Administration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU4

First Published: 2021-02-22

Last Modified: 2024-02-13

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: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

CONTENTS

PART I

Administration Overview

CHAPTER 1

Administration Overview

Cisco Unified CM Administration Overview

Cisco Unified CM Administration, a web-based application, is the main administration and configuration interface for Cisco Unified Communications Manager. You can use Cisco Unified CM Administration to configure a wide range of items for your system including general system components, features, server settings, call routing rules, phones, end users, and media resources.

Configuration Menus

The configuration windows for Cisco Unified CM Administration are organized under the following menus:

- System—Use the configuration windows under this menu to configure general system settings such as server information, NTP settings, Date and Time groups, Regions, DHCP, LDAP integration, and enterprise parameters.
- Call Routing-—Use the configuration windows under this tab to configure items related to how Cisco Unified Communications Manager routes calls, including route patterns, route groups, hunt pilots, dial rules, partitions, calling search spaces, directory numbers, and transformation patterns.
- Media Resources—Use the configuration windows under this tab to configure items such as media resource groups, conference bridges, annunciators, and transcoders.
- Advanced Features—Use the configuration windows under this tab to configure features such as voice-mail pilots, message waiting, and call control agent profiles.
- Device—Use the configuration windows under this tab to set up devices such as phones, IP phone services, trunks, gateways, softkey templates, and SIP profiles.
- Application—Use the configuration windows under this tab to download and install plug-ins such as Cisco Unified JTAPI, Cisco Unified TAPI, and the Cisco Unified Real-Time Monitoring Tool.

- User Management—Use the configuration windows under the User Management tab to configure end users and application users for your system.
- Bulk Administration-—Use the Bulk Administration Tool to import and configure large numbers of end users or devices at a time.
- Help—Click this menu to access the online help system. The online help system contains documentation that will assist you in configuring settings for the various configuration windows on your system.

Operating System Administration Overview

Use Cisco Unified Communications Operating System Administration to configure and manage your operating system and perform the following administration tasks:

- Check software and hardware status
- Check and update IP addresses
- Ping other network devices
- Manage NTP servers
- Upgrade system software and options
- Manage node security, including IPsec and certificates
- Manage remote support accounts
- Restart the system

Operating System Status

You can check the status of various operating system components, including the following:

- Clusters and nodes
- Hardware
- Network
- System
- Installed software and options

Operating System Settings

You can view and update the following operating system settings:

- IP—Updates the IP addresses and DHCP client settings that ypu entered when the application was installed.
- NTP Server settings—Configures the IP addresses of an external NTP server; adds an NTP server.
- SMTP settings—Configures the simple mail transfer protocol (SMTP) host that the operating system will use for sending email notifications.

Operating System Security Configuration

You can manage security certificates and IPsec settings. From the **Security** menu, you can choose the following security options:

- Certificate Management—Manages certificates and certificate signing requests (CSRs). You can display, upload, download, delete, and regenerate certificates. Through certificate management, you can also monitor the expiration dates of the certificates on the node.

- IPsec Management—Displays or updates existing IPsec policies; sets up new IPsec policies and associations.

Software Upgrades

You can upgrade the software version that is running on the operating system or to install specific software options, including Cisco Unified Communications Operating System locale installers, dial plans, and TFTP server files.

From the **Install/Upgrade** menu option, you can upgrade system software from either a local disc or a remote server. The upgraded software is installed on the inactive partition, and you can then restart the system and switch partitions, so the system starts running on the newer software version. For more information, see the *Upgrade Guide for the Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Note You must perform all software installations and upgrades through the software upgrade features that are included in the Cisco Unified Communications Operating System interface and the CLI. The system can upload and process only software that is Cisco Systems approved. You cannot install or use third-party or Windows-based software applications.

Services

The application provides the following operating system utilities:

- Ping—Checks connectivity with other network devices.
- Remote Support—Sets up an account that Cisco support personnel can use to access the system. This account automatically expires after the number of days that you specify.

CLI

You can access the CLI from the Operating System or through a secure shell connection to the server. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Authenticated Network Time Protocol Support

With Cisco Unified Communications Manager release 12.0 (1), the authenticated Network Time Protocol (NTP) capability for Unified Communications Manager is supported. This support is added to secure the NTP server connection to Unified Communications Manager. In the previous releases, the Unified Communications Manager connection to the NTP server was not secure.

This feature is based on symmetric key-based authentication and is supported by NTPv3 and NTPv4 servers. Unified Communications Manager supports only SHA1-based encryption. The SHA1-based symmetric key support is available from NTP version 4.2.6 and above.

- Symmetric Key
- No Authentication

You can check the authentication status of the NTP servers through administration CLI or **NTP Server List** page of the **Cisco Unified OS Administration** application.

Auto Key Authenticated Network Time Protocol Support

Cisco Unified Communications Manager also supports Network Time Protocol (NTP) authentication through Auto-key functionality (Public Key Infrastructure- based authentication). This feature is applicable only on the publisher node.

Redhat recommends symmetric key authentication over autokey. For more information, see https://access.redhat.com/support/cases/#/case/01871532.

This feature is added, as PKI-based authentication is mandatory for Common Criteria certification.

You can configure the PKI-based authentication with the IFF identity scheme on the NTP server only if you enable common criteria mode on the Cisco Unified Communication Manager.

You can enable either symmetric key or PKI-based NTP authentication on Cisco Unified Communications Manager.

If you try to enable the symmetric key on the PKI enabled server, the following warning message is displayed:

Warning NTP authentication using Autokey is currently enabled and must be disabled before the symmetric key is enabled. Use the command 'utils ntp auth auto-key disable' to disable NTP authentication, then retry this command.

If you try to enable the Autokey on the symmetric key enabled server, the following warning message is displayed:

Warning NTP authentication using symmetric key is currently enabled and must be disabled before Autokey is enabled. Use the command 'utils ntp auth symmetric-key disable' to disable NTP authentication, then retry this command.

Note NTP servers require ntp version 4 and the rpm version ntp-4.2.6p5-1.el6.x86_64.rpm and above.

You can check the authentication status of the NTP servers through administration CLI or NTP Server List page of the Cisco Unified OS Administration application.

Cisco Unified Serviceability Overview

Cisco Unified Serviceability is a web-based troubleshooting tool that provides a host of services, alarms, and tools that assist administrators in managing their systems. Among the features that Cisco Unified Serviceability offers to administrators are:

- Start and Stop Services—Administrators can set up an assortment of services that help administrators manage their systems. For example, you can start the Cisco CallManager Serviceability RTMT service thereby allowing administrators to use the Real-Time Monitoring Tool to monitor the health of your system.

- SNMP—SNMP facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.
- Alarms—Alarms provide information on the runtime status and state of your system, so that you can troubleshoot problems that are associated with your system.
- Traces—Trace tools help you to troubleshooting issues with voice applications.
- Cisco Serviceability Reporter—The Cisco Serviceability Reporter generates daily reports in Cisco Unified Serviceability.
- SNMP—SNMP facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.
- CallHome—Configure the Cisco Unified Communications Manager Call Home feature, allowing Cisco Unified Communications Manager to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server

Additional Administrative Interfaces

Using Cisco Unified Serviceability, you can start services that allow you to use the following additional administrative interfaces:

- Real-Time Monitoring Tool—The Real-Time Monitoring Tool is a web-based interface that helps you to monitor the health of your system. Using RTMT, you can view alarms, counters and reports that contain detailed information on the health of your system.
- Dialed Number Analyzer—The Dialed Number Analyzer is a web-based interface that helps administrators to troubleshoot issues with the dial plan.
- Cisco Unified CDR Analysis and Reporting—CDR Analysis and Reporting collects call details records showing the details of the calls that are placed on your system.

For details about how to use Cisco Unified Serviceability, see the *Cisco Unified Serviceability Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Cisco Unified Reporting Overview

The Cisco Unified Reporting web application generates consolidated reports for troubleshooting or inspecting cluster data. You can access the application at the Unified Communications Manager and Unified Communications Manager IM and Presence Service consoles.

This tool provides an easy way to take a snapshot of cluster data. The tool gathers data from existing sources, compares the data, and reports irregularities. When you generate a report in Cisco Unified Reporting, the report combines data from one or more sources on one or more servers into one output view. For example, you can view the following reports to help you administer your system:

- Unified CM Cluster Overview—View this report to get a snapshot of your cluster, including Cisco Unified Communications Manager and IM and Presence Service versions, server hostnames, and hardware details.

- Phone Feature List—View this report if you are configuring features. This report provides a list of which phones support which Cisco Unified Communications Manager features.
- Unified CM Phones Without Lines—View this report to see which phones in your cluster do not have a phone line.

For a full list of reports offered through Cisco Unified Reporting, as well as instructions on how to use the application, see the *Cisco Unified Reporting Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Disaster Recovery System Overview

The Disaster Recovery System (DRS), which can be invoked from Cisco Unified Communications Manager Administration, provides full data backup and restore capabilities. The Disaster Recovery System allows you to perform regularly scheduled automatic or user-invoked data backups.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores the `drfDevice.xml` and `drfSchedule.xml` files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup and restore functions.
- Scheduled backups.
- Archive backups to a physical tape drive or remote SFTP server.

Bulk Administration Tool Overview

In Cisco Unified CM Administration, uses the Bulk Administration menu and submenu options to configure entities in Unified Communications Manager through use of the Bulk Administration Tool.

The Unified Communications Manager Bulk Administration Tool (BAT), a web-based application, lets administrators perform bulk transactions to the Unified Communications Manager database. BAT lets you add, update, or delete a large number of similar phones, users, or ports at the same time. When you use Cisco Unified CM Administration, each database transaction requires an individual manual operation, while BAT automates the process and achieves faster add, update, and delete operations.

You can use BAT to work with the following types of devices and records:

- Add, update, and delete Cisco IP Phones, gateways, phones, computer telephony interface (CTI) ports, and H.323 clients
- Add, update, and delete users, user device profiles, Cisco Unified Communications Manager Assistant managers and assistants
- Add or delete Forced Authorization Codes and Client Matter Codes
- Add or delete call pickup groups
- Populate or depopulate the Region Matrix

- Insert, delete, or export the access list
- Insert, delete, or export remote destinations and remote destination profiles
- Add Infrastructure Devices

For details on how to use the Bulk Administration Tool, refer to the *Bulk Administration Guide for Cisco Unified Communications Manager*.

CHAPTER 2

Getting Started

Sign In to Adminstrative Interfaces

Use this procedure to sign in to any of the administrative interfaces in your system.

Procedure

Step 1 Open the Unified Communications Manager interface in your web browser.

Step 2 Choose the administration interface from the **Navigation** drop-down list.

Step 3 Click **Go**.

Step 4 Enter your username and password.

Step 5 Click **Login**.

Reset the Administrator or Security Password

If you lose the administrator password and cannot access your system, use this procedure to reset the password.

Note For password changes on IM and Presence nodes, stop the Cisco Presence Engine service in all IM and Presence nodes before resetting the administrator password. After the password reset, restart the Cisco Presence Engine service in all the nodes. Make sure that you perform this task during maintenance because you may face presence issues when the PE is stopped.

Before you begin

- You require physical access to the node on which you perform this procedure.

- At any point, when you are requested to insert CD or DVD media, you must mount the ISO file through the vSphere client for the VMWare server. See "Adding DVD or CD Drives to a Virtual Machine" https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html for guidance.
- The security password on all nodes in a cluster must match. Change the security password on all machines, or the cluster nodes will not communicate.

Procedure

Step 1 Sign in to the CLI on the publisher node with the following username and password:

a) Username: **`pwrecovery`**

b) Password: **`pwreset`**

Step 2 Press any key to continue.

Step 3 If you have a valid CD/DVD in the disk drive or you mounted an ISO file, remove it from the VMWare client.

Step 4 Press any key to continue.

Step 5 Insert a valid CD or DVD into the drive or mount the ISO file.

Note For this test, you must use a disk or ISO file that is data only.

Step 6 After the system verifies the last step, you are prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.

Note You must reset each node in a cluster after you change its security password. Failure to reboot the nodes causes system service problems and problems with the administration windows on the subscriber nodes.

Step 7 Enter the new password, and then reenter it to confirm.

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

Step 8 After the system verifies the strength of the new password, the password is reset, and you are prompted to press any key to exit the password reset utility.

If you want to set up a different administrator password, use the CLI command **set password**. For more information, see the *Command Line Interface Reference Guide for CiscoUnified Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Shut Down or Restart the System

Use this procedure if you need to shut down or restart your system, for example, after you make a configuration change.

Before you begin

If the server is forced to shutdown and restart from your virtual machine, the file system may become corrupted. Avoid a forced shutdown; instead, wait for the server to shutdown properly after this procedure or after you run **utils system shutdown** from the CLI.

Note If you force shutdown or restart the virtual machine from VMware administration tools (vCenter or Embedded Host Client):

- From 12.5(1)SU4 or later, the Unified Communications Manager and IM and Presence Service will gracefully shutdown/restart and this will be displayed in the system-history.log

Caution Unified Communications Manager and IM and Presence Service identifies an ungraceful shutdown/restart. A rebuild of such systems is highly recommended to ensure that there are no negative impacts such as corruption of configuration data or the filesystem itself. The administrator is notified on GUI and CLI login and a SyslogSeverityMatchFound alert is triggered until the system is rebuilt or upgraded. For more information on rebuild instruction, see Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Settings** > **Version**.

Step 2 Perform one of the following actions:

- Click **Shutdown** to stop all processes and shut down the system.
- Click **Restart** to stop all processes and restart the system.

PART II

Manage Users

CHAPTER 3

Manage User Access

User Access Overview

Manage user access to Cisco Unified Communications Manager by configuring the following items:

- Access Control Groups
- Roles
- User Rank

Access Control Group Overview

An access control group is a list of users and the roles that are assigned to those users. When you assign an end user, application user, or administrator user to an access control group, the user gains the access permissions of the roles that are associated to the group. You can manage system access by assigning users with similar access needs to an access control group with only the roles and permissions that they need.

There are two types of access control groups:

- Standard Access Control Groups—These are predefined default groups with role assignments that meet common deployment needs. You cannot edit the role assignments in a standard group. However, you can add and delete users, in addition to editing the User Rank requirement. For a list of standard access control groups, and their associated roles, see Standard Roles and Access Control Groups, on page 29.

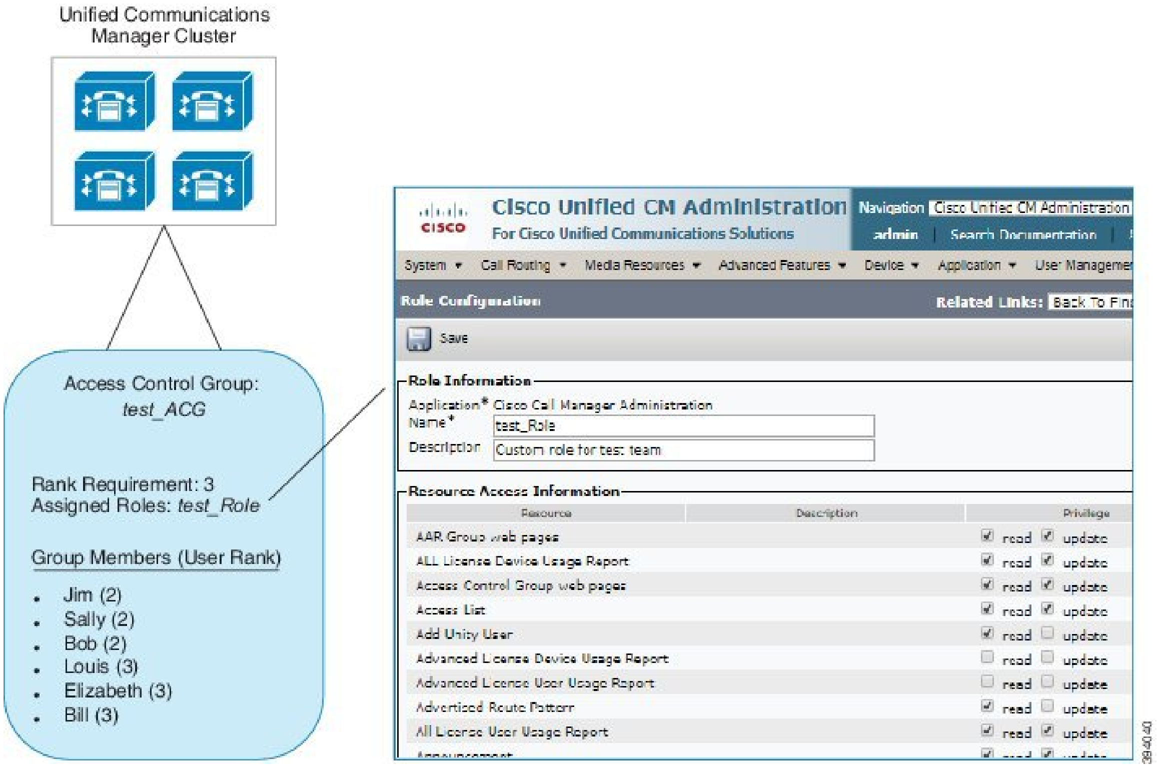
- Custom Access Control Groups—Create your own access control groups when none of the standard groups contain the role permissions that meet your needs.

The User Rank framework provides a set of controls over the access control groups to which a user can be assigned. To be assigned to an access control group, a user must meet the minimum rank requirement for that group. For example, end users whom have a User Rank of 4 can be assigned only to access control groups with minimum rank requirements between 4 and 10. They cannot be assigned to groups with a minimum rank of 1.

Example - Role Permissions with Access Control Groups

The following example illustrates a cluster where the members of a testing team are assigned to access control group **test_ACG**. The screen capture on the right displays the access settings of test_Role, which is the role that is associated to the access control group. Also note that the access control group has a minimum rank requirement of 3. All of the group members must have a rank between 1-3 to be able to join the group.

Figure 1: Role Permissions with Access Control Groups


Unified Communications Manager Cluster
Access Control Group: test_ACG
Rank Requirement: 3
Assigned Roles: test_Role
Group Members (User Rank)
Jim (2)
Sally (2)
Bob (2)
Louis (3)
Elizabeth (3)
Bill (3)
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin
Search Documentation
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Managemer
Role Configuration
Related Links: Back To Fin
Save
394040

Role Information

Application* Cisco Call Manager Administration
Name* test_Role
Description Custom role for test team

Resource Access Information

Resource	Description	Privilege
AAR Group web pages		☑ read ☑ update
ALL License Device Usage Report		☑ read ☑ update
Access Control Group web pages		☑ read ☑ update
Access List		☑ read ☑ update
Add Unity User		☑ read □ update
Advanced License Device Usage Report		□ read □ update
Advanced License User Usage Report		□ read □ update
Advertised Route Pattern		☑ read □ update
All License User Usage Report		☑ read ☑ update
Announcement		☑ read ☑ update

Roles Overview

Users obtain system access privileges via the roles that are associated to the access control group of which the user is a member. Each role contains a set of permissions that is attached to a specific resource or application, such as Cisco Unified CM Administration or CDR Analysis and Reporting. For an application such as Cisco Unified CM Administration, the role may contain permissions that let you view or edit specific GUI pages in the application. There are three levels of permissions that you can assign to a resource or application:

- Read—Allows a user to view settings for a resource.
- Update—Allows a user to edit settings for a resource.
- No Access—If a user has neither Read or Update access, the user has no access to view or edit settings for a given resource.

Role Types

When provisioning users, you must decide what roles you want to apply and then assign users to an access control group that contains the role. There are two main types of roles in Cisco Unified Communications Manager:

- Standard roles—These are preinstalled default roles that are designed to meet the needs of common deployments. You cannot edit permissions for standard roles.
- Custom roles—Create custom roles when no standard roles have the privileges you need. In addition, if you need a more granular level of access control, you can apply advanced settings to control an administrator's ability to edit key user settings. See the below section for details.

Advanced Role Settings

For custom roles, you can add a detailed level of control to selected fields on the **Application User Configuration** and **End User Configuration** windows.

The **Advanced Role Configuration** window lets you configure access to Cisco Unified CM Administration while restricting access for tasks such as:

- Adding users
- Editing passwords
- Editing user ranks
- Editing access control groups

The following table details more controls that you can apply with this configuration:

Table 1: Advanced Resource Access Information

Advanced Resource	Access Control
Permission Information	Controls the ability to add or edit access control groups: • **View**—User can view access control groups, but cannot add, edit, or delete access control groups. • **Update**—User can add, edit, or delete access control groups. **Note** When both the values are not selected, the **Permission Information** section is not available. **Note** If you choose **View**, the **User can update Permissions Information for own user** field is set to **No** and is disabled. If you want to be able to edit this field, you must set the **Permission Information** field to **Update**.

Advanced Resource	Access Control
User can update Permissions Information for own user	Controls a user's ability to edit their own access permissions: • **Yes**—User can update their own Permission Information. • **No**—User cannot update their own Permission Information. However, the user can view or modify the permission information of same or lower ranked users. **Note** The **User can update Permissions Information for own user** field is set to **No** and is disabled if the **Permission Information Update** check box is not selected.
User Rank	Controls the ability to change the user rank: • **View**—User can view the user rank, but cannot change the user rank. • **Update**—User can change the user rank. **Note** When both the values are not selected, the **User Rank** section is not available. **Note** If you choose **View**, the **User can update User Rank for own user** field is set to **No** and is disabled. If you want to be able to edit this field, you must set the **User Rank** field to **Update**.
User can update User Rank for own user	Controls a user's ability to edit their own user rank: • **Yes**—User can update their own User Rank. • **No**—User cannot update their own User Rank. However, the user can view or modify the rank of same or lower ranked users. **Note** The **User can update User Rank for own user** field is set to **No** and is disabled, if the **User Rank Update** check box is not selected.
Add New Users	Controls the ability to add a new user: • **Yes**—User can add a new user. • **No**—The **Add New** button is not available.
Password	Controls the ability to change the password: • **Yes**—User can change the user passwords under **Application User Information** section. • **No**—The **Password** and **Confirm Password** under **Application User Information** section is not available.

User Rank Overview

The User Rank hierarchy provides a set of controls over which access control groups an administrator can assign to an end user or application user.

When provisioning end users or application users, administrators can assign a user rank for the user. Administrators can also assign a user rank requirement for each access control group. When adding users to access conttrol groups, administrators can assign users only to the groups where the user's User Rank meets the group's rank requirement. For example, an administrator can assign a user whom has a User Rank of 3 to access control groups that have a User Rank requirement between 3 and 10. However, an administrator cannot assign that user to an access control group that has a User Rank requirement of 1 or 2.

Administrators can create their own user rank hierarchy within the **User Rank Configuration** window and can use that hierarchy when provisioning users and access control groups. Note that if you don't configure a user rank hierarchy, or if you simply don't specify the User Rank setting when provisioning users or access conrol groups, all users and access control groups are assigned the default User Rank of 1 (the highest rank possible).

User Access Prerequisites

Make sure to review your user needs so that you know what level of access your users require. You will want to assign roles that have the access privileges your users require, but which do not provide access to systems that they should not be able to access.

Before you create new roles and acess control groups, review the list of standard roles and access control groups to verify whether an existing access control group has the roles and access permissions that you need. For details, see Standard Roles and Access Control Groups, on page 29.

User Access Configuration Task Flow

Complete the following tasks to configure user access.

Before you begin

If you want to use default roles and access control groups then you can skip tasks for creating customized roles and access control groups. You can assign your users to the existing default access control groups.

Procedure

	Command or Action	Purpose
Step 1	Configure User Rank Hierarchy, on page 20	Set up the user rank hierarchy. Note that if you skip this task, all users and access control groups get assigned the default user rank of 1 (the highest rank).
Step 2	Create a Custom Role, on page 20	Create custom roles if the default roles don't have the access permissions you need.
Step 3	Configure Advanced Role for Administrators, on page 21	Optional. Advanced permissions in a custom role let you control an administrator’s ability to edit key user settings.
Step 4	Create Access Control Group, on page 22	Create custom access control groups if the default groups don't have the role assignments you need.

	Command or Action	Purpose
Step 5	Assign Users to Access Control Group, on page 22	Add or delete users from a standard or custom access control group.
Step 6	Configure Overlapping Privilege Policy for Access Control Groups, on page 23	Optional. This setting is used if users are assigned to multiple access control groups with conflicting permissions.

Configure User Rank Hierarchy

Use this procedure to create a custom user rank hierarchy.

Note If you don't configure a user rank hierarchy, all users and access control groups get assigned a user rank of 1 (the highest possible rank) by default.

Procedure

Step 1 From Cisco Unified CM Administration, choose**User Management** > **User Settings** > **User Rank**.

Step 2 Click **Add New**.

Step 3 From the **User Rank** drop-down menu, select a rank setting between 1–10. The highest rank is 1.

Step 4 Enter a **Rank Name** and **Description**.

Step 5 Click **Save**.

Step 6 Repeat this procedure to add additional user ranks.
You can assign the user rank to users and access control groups to control which groups a user can be assigned to.

Create a Custom Role

Use this procedure to create a new role with customized privileges. You may want to do this if there are no standard roles with the exact privileges that you need. There are two ways to create a role:

- Use the **Add New** button to create and configure the new role from scatch.
- Use the **Copy** button if an existing role has access privileges that are close to what you need. You can copy the privileges of the existing role to a new role that is editable.

Procedure

Step 1 In Cisco Unified CM Administration, click **User Management** > **User Settings** > **Role**.

Step 2 Do either of the following:

- To create a new role, click **Add New**. Choose the **Application** with which this role associates, and click **Next**.
- To copy settings from an existing role, click **Find** and open the existing role. Click **Copy** and enter a name for the new role. Click **OK**.

Step 3 Enter a **Name** and **Description** for the role.

Step 4 For each resource, check the boxes that apply:

- Check the **Read** check box if you want users to be able to view settings for the resource.
- Check the **Update** check box if you want users to be able to edit setttings for the resource.
- Leave both check boxes unchecked to provide no access to the resource.

Step 5 Click **Grant access to all** or **Deny access to all** button to grant or remove privileges to all resources that display on a page for this role.

Note If the list of resources displays on more than one page, this button applies only to the resources that display on the current page. You must display other pages and use the button on those pages to change the access to the resources that are listed on those pages.

Step 6 Click **Save**.

Configure Advanced Role for Administrators

Advanced Role Configuration lets you edit permissions for a custom role at a more granular level. You can control an administrator’s ability to edit the following key settings in the **End User Configuration** and **Application User Configuration** windows:

- Editing User Ranks
- Editing Access Control Group assignments
- Adding new users
- Editing user passwords

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Role**.

Step 2 Click **Find** and select a custom role.

Step 3 From **Related Links**, select **Advanced Role Configuration** and click **Go**.

Step 4 From the **Resource Web Page**, select **Application User Web Pages** or **User Web Pages**.

Step 5 Edit the settings. Refer to the online help for help with the fields and their settings.

Step 6 Click **Save**.

Create Access Control Group

Use this procedure if you need to create a new access control group. You may want to do this if no standard group has the roles and access privileges you need. There are two ways to create a customized group:

- Use the **Add New** button to create and configure the new access control group from scatch.
- Use the **Copy** button if an existing group has role assignments that are close to what you need. You can copy the settings from the existing group to a new and editable group.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Groups.**

Step 2 Do either of the following:

- To create a new group from scratch, click **Add New**.
- To copy settings from an existing group, click **Find** and open the existing access control group. Click **Copy** and enter a name for the new group. Click **OK**.

Step 3 Enter a **Name** for the access control group.

Step 4 From the **Available for Users with User Rank as** drop-down, select the minimum User Rank a user must meet to be assigned to this group. The default user rank is 1.

Step 5 Click **Save**.

Step 6 Assign roles to the access control group. The roles you select will be assigned to group members:

a) From **Related Links**, select **Assign Role to Access Control Group**, and click **Go**.
b) Click **Find** to search for existing roles.
c) Check the roles that you want to add and click **Add Selected**.
d) Click **Save**.

What to do next

Assign Users to Access Control Group, on page 22

Assign Users to Access Control Group

Add or delete users from a standard or custom access control group. .

Note You can add only those users whose user rank is the same or higher than the minimum user rank for the access control group.

Note If you are syncing new users from a company LDAP Directory, and your rank hierarchy and access control groups are created with the appropriate permissions, you can assign the group to synced users as a part of the LDAP sync. For details on how to set up an LDAP directory sync, see the *System Configuration Guide for Cisco Unified Communications Manager.*

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The **Find and List Access Control Group** window appears.

Step 2 Click **Find** and select the access control group for which you want to update the list of users.

Step 3 From the **Available for Users with User Rank as** drop-down, select the rank requirement that users must meet to be assigned to this group.

Step 4 In the **User** section, click **Find** to display the list of users.

Step 5 If you want to add end users or application users to the access control group, do the following:

a) Click **Add End Users to Access Control Group** or **Add App Users to Access Control Group**.
b) Select the users whom you want to add.
c) Click **Add Selected**.

Step 6 If you want to delete users from the access control group:

a) Select the users whom you want to delete.
b) Click **Delete Selected**.

Step 7 Click **Save**.

Configure Overlapping Privilege Policy for Access Control Groups

Configure how Cisco Unified Communications Manager handles overlapping user privileges that can result from access control group assignments. This is to cover situations where an end user is assigned to multiple access control groups, each with conflicting roles and privilege settings.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **User Management Parameters**, configure one of the following values for the **Effective Access Privileges For Overlapping User Groups and Roles** as follows:

- **Maximum**—The effective privilege represents the maximum of the privileges of all the overlapping access control groups. This is the default option.
- **Minimum**—The effective privilege represents the minimum of the privileges of all the overlapping access control groups.

Step 3 Click **Save**.

View User Privilege Report

Perform the following procedure to view the User Privilege report for either an existing end user or an existing application user. The User Privilege report displays the access control groups, roles, and access privileges that are assigned to an end user or application user.

Procedure

Step 1 In Cisco Unified CM Administration, perform either of the following steps:

- For end users, choose **User Management** > **End User**.
- For application users, choose **User Management** > **Application User**.

Step 2 Click **Find** and select the user for whom you want to view access privileges

Step 3 From the **Related Links** drop-down list, choose the **User Privilege Report** and click **Go**.
The User Privilege window appears.

Create Custom Help Desk Role Task Flow

Some companies want their help desk personnel to have privileges to be able to perform certain administrative tasks. Follow the steps in this task flow to configure a role and access control group for help desk team members that allows them to perform tasks such as adding a phone and adding an end user.

Procedure

	Command or Action	Purpose
Step 1	Create Custom Help Desk Role, on page 25	Create a custom role for help desk team members and assign the role privileges for items such as adding new phones and adding new users.
Step 2	Create Custom Help Desk Access Control Group, on page 25	Create a new access control group for the Help Desk role.
Step 3	Assign Help Desk Role to Access Control Group, on page 25	Assign the Help Desk role to the Help Desk access control group. Any users assigned to this access control group will be assigned the privileges of the Help Desk role.
Step 4	Assign Help Desk Members to Access Control Group, on page 26	Assign help desk team members with the privileges of the custom help desk role.

Create Custom Help Desk Role

Perform this procedure to create a custom help desk role that you can assign to help desk members in your organization.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **User Settings** > **Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list, choose the application that you want to assign to this role. For example, **Cisco CallManager Administration**.

Step 4 Click **Next**.

Step 5 Enter the **Name** of the new role. For example, `Help Desk`.

Step 6 Under **Read and Update Privileges** select the privileges that you want to assign for help desk users. For example, if you want help desk members to be able to add users and phones, check the **Read** and **Update** check boxes for User web pages and Phone web pages.

Step 7 Click **Save**.

What to do next

Create Custom Help Desk Access Control Group, on page 25

Create Custom Help Desk Access Control Group

Before you begin

Create Custom Help Desk Role, on page 25

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Add New**.

Step 3 Enter a name for the access control group. For example, `Help_Desk`.

Step 4 Click **Save**.

What to do next

Assign Help Desk Role to Access Control Group, on page 25

Assign Help Desk Role to Access Control Group

Perform the following steps to configure the Help Desk access control group with the privileges from the Help Desk role.

Before you begin

Create Custom Help Desk Access Control Group, on page 25

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group**.

Step 2 Click **Find** and select the access control group that you created for Help Desk.
The **Access Control Group Configuration** window displays.

Step 3 In the **Related Links** drop-down list box, choose the **Assign Role to Access Control Group** option and click **Go**.
The **Find and List Roles** popup displays.

Step 4 Click the **Assign Role to Group** button.

Step 5 Click **Find** and select the Help Desk role.

Step 6 Click **Add Selected**.

Step 7 Click **Save**.

What to do next

Assign Help Desk Members to Access Control Group, on page 26

Assign Help Desk Members to Access Control Group

Before you begin

Assign Help Desk Role to Access Control Group, on page 25

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Access Control Group.**

Step 2 Click **Find** and select the custom Help Desk access control group that you created.

Step 3 Perform either of the following steps:

- If your help desk team members are configured as end users, click **Add End Users to Group**.
- If your help desk team members are configured as application users, click **Add App Users to Group**.

Step 4 Click **Find** and select your help desk users.

Step 5 Click **Add Selected**.

Step 6 Click **Save**.
Cisco Unified Communications Manager assigns your help desk team members with the privileges of the custom help desk role that you created.

Delete Access Control Group

Use the following procedure to delete an access control group entirely.

Before you begin

When you delete an access control group, Cisco Unified Communications Manager removes all access control group data from the database. Ensure you are aware which roles are using the access control group.

Procedure

Step 1 Choose **User Management** > **User Settings** > **Access Control Group**.

The **Find and List Access Control Groups** window appears.

Step 2 Find the access control group that you want to delete.

Step 3 Click the name of the access control group that you want to delete.

The access control group that you chose appears. The list shows the users in this access control group in alphabetical order.

Step 4 If you want to delete the access control group entirely, click **Delete**.

A dialog box appears to warn you that you cannot undo the deletion of access control groups.

Step 5 To delete the access control group, click **OK** or to cancel the action, click **Cancel**. If you click **OK**, Cisco Unified Communications Manager removes the access control group from the database.

Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.

Disable Inactive User Accounts

Use the following procedure to disable the inactive user accounts using Cisco Database Layer Monitor service.

Cisco Database Layer Monitor changes the user account status to inactive during scheduled maintenance tasks if you have not logged in to Cisco Unified Communications Manager within a specified number of days. Disabled users are audited automatically in the subsequent audit logs.

Before you begin

Enter the **Maintenance Time** for the selected server in the Cisco Database Layer Monitor service (**System** > **Service Parameters**).

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list box, choose a server.

Step 3 From the **Service** drop-down list box, choose the **Cisco Database Layer Monitor** parameter.

Step 4 Click **Advanced**.

Step 5 In the **Disable User Accounts unused for (days)** field, enter the number of days. For example, 90. The system uses the entered value as a threshold to declare the account status as inactive. To turn-off auto disable, enter the value as 0.

Note This is a required field. The default and minimum value is 0 and the unit is days.

Step 6 Click **Save**.
The user gets disabled if remained inactive within the configured number of days (for example, 90 days). An entry is made in the audit log and it displays the message as: “`<userID>` user is marked inactive”.

Set up a Remote Account

Configure a remote account in the Unified Communications Manager so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Remote Support**.

Step 2 In the **Account Name** field, enter a name for the remote account.

Step 3 In the **Account Duration** field, enter the account duration in days.

Step 4 Click **Save**.
The system generates an encrypted pass phrase.

Step 5 Contact Cisco support to provide them with the remote support account name and pass phrase.

Standard Roles and Access Control Groups

The following table summarizes the standard roles and access control groups that come preconfigured on Cisco Unified Communications Manager. The privileges for a standard role are configured by default. In addition, the access control groups that are associated with a standard role are also configured by default.

For both standard roles and the associated access control group, you cannot edit any of the privileges, or the role assignments.

Table 2: Standard Roles, Privileges, and Access Control Groups

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard AXL API Access	Allows access to the AXL database API	Standard CCM Super Users
Standard AXL API Users	Grants login rights to execute AXL APIs.	
Standard AXL Read Only API Access	Allows you to execute AXL read only APIs (list APIs, get APIs, executeSQLQuery API) by default.	
Standard Admin Rep Tool Admin	Allows you to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).	Standard CAR Admin Users, Standard CCM Super Users
Standard Audit Log Administration	Allows you to perform the following tasks for the audit logging feature : • View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability • View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in the Real-Time Monitoring Tool • View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability • View and update the associated alert in the RTMT	Standard Audit Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Admin Users	Grants log-in rights to Cisco Unified Communications Manager Administration.	Standard CCM Admin Users, Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Monitoring, Standard CCM Super Users, Standard CCM Server Maintenance, Standard Packet Sniffer Users
Standard CCM End Users	Grant an end user log-in rights to the Cisco Unified Communications Self Care Portal	Standard CCM End Users
Standard CCM Feature Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View, delete, and insert the following items by using the Bulk Administration Tool: • Client matter codes and forced authorization codes • Call pickup groups • View and configure the following items in Cisco Unified Communications Manager Administration: • Client matter codes and forced authorization codes • Call park • Call pickup • Meet-Me numbers/patterns • Message Waiting • Cisco Unified IP Phone Services • Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles	Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Gateway Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure gateway templates in the Bulk Administration Tool • View and configure gatekeepers, gateways, and trunks	Standard CCM Gateway Administration
Standard CCM Phone Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and export phones in the Bulk Administration Tool • View and insert user device profiles in the Bulk Administration Tool • View and configure the following items in Cisco Unified Communications Manager Administration: • BLF speed dials • CTI route points • Default device profiles or default profiles • Directory numbers and line appearances • Firmware load information • Phone button templates or softkey templates • Phones • Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window	Standard CCM Phone Administration

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM Route Plan Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure application dial rules • View and configure calling search spaces and partitions • View and configure dial rules, including dial rule patterns • View and configure hunt lists, hunt pilots, and line groups • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report • View and configure time period and time schedule • View and configure translation patterns	
Standard CCM Service Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: • Annunciators, conference bridges, and transcoders • audio sources and MOH servers • Media resource groups and media resource group lists • Media termination point • Cisco Unified Communications Manager Assistant wizard • View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool	Standard CCM Server Maintenance

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCM System Management	Allows you to perform the following tasks in Cisco Unified Communications Manager Administration: • View and configure the following items: • Automate Alternate Routing (AAR) groups • Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups • Date and time groups • Device defaults • Device pools • Enterprise parameters • Enterprise phone configuration • Locations • Network Time Protocol (NTP) servers • Plug-ins • Security profiles for phones that run Skinny Call Control Protocol (SCCP) or Session Initiation Protocol (SIP); security profiles for SIP trunks • Survivable Remote Site Telephony (SRST) references • Servers • View and configure the Job Scheduler windows in the Bulk Administration Tool	Standard CCM Server Maintenance
Standard CCM User Privilege Management	Allows you to view and configure application users in Cisco Unified Communications Manager Administration.	
Standard CCMADMIN Administration	Allows you access to all aspects of the CCMAdmin system	
Standard CCMADMIN Administration	Allows you to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Super Users

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CCMADMIN Administration	Allows you to view and configure information in the Dialed Number Analyzer.	
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	
Standard CCMADMIN Read Only	Allows you to view configurations in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.	Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring
Standard CCMADMIN Read Only	Allows you to analyze routing configurations in the Dialed Number Analyzer.	
Standard CCMUSER Administration	Allows access to the Cisco Unified Communications Self Care Portal.	Standard CCM End Users
Standard CTI Allow Call Monitoring	Allows CTI applications/devices to monitor calls	Standard CTI Allow Call Monitoring
Standard CTI Allow Call Park Monitoring	Allows CTI applications/devices to use call park. **Important** The maximum number of opened lines and park lines must not exceed 65,000. If the total exceeds 65,000, remove the Standard CTI Allow Call Park Monitoring role from the application user or reduce the number of park lines that are configured.	Standard CTI Allow Call Park Monitoring
Standard CTI Allow Call Recording	Allows CTI applications/devices to record calls	Standard CTI Allow Call Recording
Standard CTI Allow Calling Number Modification	Allows CTI applications to transform calling party numbers during a call	Standard CTI Allow Calling Number Modification
Standard CTI Allow Control of All Devices	Allows control of all CTI-controllable devices	Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones Supporting Connected Xfer and conf	Allows control of all CTI devices that supported connected transfer and conferencing	Standard CTI Allow Control of Phones supporting Connected Xfer and conf

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard CTI Allow Control of Phones Supporting Rollover Mode	Allows control of all CTI devices that supported Rollover mode	Standard CTI Allow Control of Phones supporting Rollover Mode
Standard CTI Allow Reception of SRTP Key Material	Allows CTI applications to access and distribute SRTP key material	Standard CTI Allow Reception of SRTP Key Material
Standard CTI Enabled	Enables CTI application control	Standard CTI Enabled
Standard CTI Secure Connection	Enables a secure CTI connection to Cisco Unified Communications Manager	Standard CTI Secure Connection
Standard CUReporting	Allows application users to generate reports from various sources	
Standard CUReporting	Allows you to view, download, generate, and upload reports in Cisco Unified Reporting	Standard CCM Administration Users, Standard CCM Super Users
Standard EM Authentication Proxy Rights	Manages Cisco Extension Mobility (EM) authentication rights for applications; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant and Cisco Web Dialer)	Standard CCM Super Users, Standard EM Authentication Proxy Rights
Standard Packet Sniffing	Allows you to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing).	Standard Packet Sniffer Users
Standard RealtimeAndTraceCollection	Allows an you to access Cisco Unified Serviceability and the Real-Time Monitoring Tool view and use the following items: • Simple Object Access Protocol (SOAP) Serviceability AXL APIs • SOAP Call Record APIs • SOAP Diagnostic Portal (Analysis Manager) Database Service • configure trace for the audit log feature • configure Real-Time Monitoring Tool, including collecting traces	Standard RealtimeAndTraceCollection

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY	Allows you to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool: • Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability) • Audit Trace (marked as read/view only) • SNMP-related windows (Cisco Unified Serviceability) • Trace Configuration and Troubleshooting of Trace Configuration (Cisco Unified Serviceability) • Log Partition Monitoring • Alert Configuration (RTMT), Profile Configuration (RTMT), and Trace Collection (RTMT) Allows you to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service. For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource. For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource.	Standard CCM Server Monitoring, Standard CCM Super Users
Standard SERVICEABILITY Administration	A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window.	
Standard SERVICEABILITY Administration	Allows you to administer all aspects of serviceability for the Dialed Number Analyzer.	
Standard SERVICEABILITY Administration	Allows you to view and configure all windows in Cisco Unified Serviceability and Real-Time Monitoring Tool. (Audit Trace supports viewing only.) Allows you to view and use all SOAP Serviceability AXL APIs.	

Standard Role	Privileges/Resources for the Role	Associated Standard Access Control Group(s)
Standard SERVICEABILITY Read Only	Allows you to view all serviceability-related data for components in the Dialed Number Analyzer.	Standard CCM Read Only
Standard SERVICEABILITY Read Only	Allows you to view configuration in Cisco Unified Serviceability and Real-Time Monitoring Tool. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an you to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.	
Standard System Service Management	Allows you to view, activate, start, and stop services in Cisco Unified Serviceability.	
Standard SSO Config Admin	Allows you to administer all aspects of SAML SSO configuration	
Standard Confidential Access Level Users	Allows you to access all the Confidential Access Level Pages	Standard Cisco Call Manager Administration
Standard CCMADMIN Administration	Allows you to administer all aspects of CCMAdmin system	Standard Cisco Unified CM IM and Presence Administration
Standard CCMADMIN Read Only	Allows read access to all CCMAdmin resources	Standard Cisco Unified CM IM and Presence Administration
Standard CUReporting	Allows application users to generate reports from various sources	Standard Cisco Unified CM IM and Presence Reporting

CHAPTER 4

Manage End Users

End User Overview

When administering an up and running system, you may need to make updates to the list of configured end users in your system. This includes:

- Setting up a new user
- Setting up a phone for a new end user
- Changing passwords or PINs for an end user
- Enable end users for IM and Presence Service

The **End User Configuration** window in Cisco Unified CM Administration allows you to add, search, display, and maintain information about Unified CM end users. You can also use the **Quick User/Phone Add** window to quickly configure a new end user and configure a new phone for that end user.

End User Management Tasks

Procedure

	Command or Action	Purpose
Step 1	Configure User Templates, on page 40	If you have not configured your system with user profiles or feature group templates that includes universal line and device templates, perform these tasks to set them up. You can apply these templates to any new end users in order to quickly configure new users and phones.
Step 2	Add a new end user using one of the following methods	If you have configured and if your system is synchronized with a company LDAP directory,

	Command or Action	Purpose
	- Import an End User from LDAP, on page 44 - Add an End User Manually, on page 45	you can import the new end user directly from LDAP. Else, you can add and configure the end user manually.
Step 3	Assign a phone to a new or existing end user by performing either of the following tasks: - Add New Phone for End User , on page 46 - Move an Existing Phone to a End User, on page 47	You can use the 'Add New Phone' procedure to configure a new phone for the end user using settings from a universal device template. You can also use the 'Move' procedure to assign an existing phone that has already been configured.
Step 4	Change the End User PIN, on page 47	(Optional) To change the pin for an end user in Cisco Unified Communications Manager Administration.
Step 5	Change the End User Password, on page 48	(Optional) To change the password for an end user in Cisco Unified Communications Manager Administration.
Step 6	Create a Cisco Unity Connection Voice Mailbox, on page 48	(Optional) To create individual Cisco Unity Connection voice mailboxes in Cisco Unified Communications Manager Administration.

Configure User Templates

Perform the following tasks to set up a user profile and feature group template. When you add a new end user, you can use the line and device settings to quickly configure the end user and any phones for the end user.

Procedure

	Command or Action	Purpose
Step 1	Configure Universal Line Template, on page 41	Configure universal line templates with common settings that are typically applied to a directory number.
Step 2	Configure Universal Device Template, on page 41	Configure universal device templates with common settings that are typically applied to a phone.
Step 3	Configure User Profiles, on page 42	Assign universal line and universal device templates to a user profile. If you have the self-provisioning feature configured, you can enable self-provisioning for the users who use this profile.
Step 4	Configure Feature Group Template, on page 43	Assign the user profile to a feature group template. For LDAP Synchronized Users, the

	Command or Action	Purpose
		feature group template associates the user profile settings to the end user.

Configure Universal Line Template

Universal Line Templates make it easy to apply common settings to newly assigned directory numbers. Configure different templates to meet the needs of different groups of users.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Line Template**.

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Universal Line Template Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 If you are deploying Global Dial Plan Replication with alternate numbers expand the **Enterprise Alternate Number** and **+E.164 Alternate Number** sections and do the following:

a) Click the **Add Enterprise Alternate Number** button and/or **Add +E.164 Alternate Number** button.
b) Add the **Number Mask** that you want to use to assign to your alternate numbers. For example, a 4-digit extension might use 5XXXX as an enterprise number mask and 1972555XXXX as an +E.164 alternate number mask.
c) Assign the partition where you want to assign alternate numbers.
d) If you want to advertise this number via ILS, check the **Advertise Globally via ILS** check box. Note that if you are using advertised patterns to summarize a range of alternate numbers, you may not need to advertise individual alternate numbers.
e) Expand the **PSTN Failover** section and choose the **Enterprise Number** or **+E.164 Alternate Number** as the PSTN failover to use if normal call routing fails.

Step 5 Click **Save**.

What to do next

Configure Universal Device Template, on page 41

Configure Universal Device Template

Universal device templates make it easy to apply configuration settings to newly provisioned devices. The provisioned device uses the settings of the universal device template. You can configure different device templates to meet the needs of different groups of users. You can also assign the profiles that you’ve configured to this template.

Before you begin

Configure Universal Line Template, on page 41

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Click **Add New**.

Step 3 Enter the following mandatory fields:

a) Enter a **Device Description** for the template.
b) Select a **Device Pool** type from the drop-down list.
c) Select a **Device Security Profile** from the drop-down list.
d) Select a **SIP Profile** from the drop-down list.
e) Select a **Phone Button Template** from the drop-down list.

Step 4 Complete the remaining fields in the **Universal Device Template Configuration** window. For field descriptions, see the online help.

Step 5 Under **Phone Settings**, complete the following optional fields:

a) If you configured a **Common Phone Profile**, assign the profile.
b) If you configured a **Common Device Configuration**, assign the configuration.
c) If you configured a **Feature Control Policy**, assign the policy.

Step 6 Click **Save**.

What to do next

Configure User Profiles, on page 42

Configure User Profiles

Assign universal line and universal device template to users through the User Profile. Configure multiple user profiles for different groups of users. You can also enable self-provisioning for users who use this service profile.

Before you begin

Configure Universal Device Template, on page 41

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **User Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the user profile.

Step 4 Assign a **Universal Device Template** to apply to users' **Desk Phones**, **Mobile and Desktop Devices**, and **Remote Destination/Device Profiles**.

Step 5 Assign a **Universal Line Template** to apply to the phone lines for users in this user profile.

Step 6 If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

a) Check the **Allow End User to Provision their own phones** check box.

b) In the **Limit Provisioning once End User has this many phones** field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.

c) Check the **Allow Provisioning of a phone already assigned to a different End User** check box to determine whether the user who is associated with this profile has the permission to migrate or reassign a device that is already owned by another user. By default, this check box is unchecked.

Step 7 If you want Cisco Jabber users who are associated with this user profile, to be able to use the Mobile and Remote Access feature, check the **Enable Mobile and Remote Access** check box.

Note

- By default, this check box is selected. When you uncheck this check box, the **Client Policies** section is disabled, and No Service client policy option is selected by default.
- This setting is mandatory only for Cisco Jabber users whom are using OAuth Refresh Logins. Non-Jabber users do not need this setting to be able to use Mobile and Remote Access. Mobile and Remote Access feature is applicable only for the Jabber Mobile and Remote Access users and not to any other endpoints or clients.

Step 8 Assign the Jabber policies for this user profile. From the **Desktop Client Policy**, and **Mobile Client Policy** drop-down list, choose one of the following options:

- No Service—This policy disables access to all Cisco Jabber services.
- IM & Presence only—This policy enables only instant messaging and presence capabilities.
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

Note Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

Step 9 If you want the users in this user profile to set the maximum login time for Extension Mobility or Extension Mobility Cross Cluster through Cisco Unified Communications Self Care Portal, check the **Allow End User to set their Extension Mobility maximum login time** check box.

Note By default **Allow End User to set their Extension Mobility maximum login time** check box is unchecked.

Step 10 Click **Save**.

What to do next

Configure Feature Group Template, on page 43

Configure Feature Group Template

Feature group templates aid in your system deployment by helping you to quickly configure phones, lines, and features for your provisioned users. If you are syncing users from a company LDAP directory, configure a feature group template with the User Profile and Service Profile that you want users synced from the directory to use. You can also enable the IM and Presence Service for synced users through this template.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Feature Group Template**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the Feature Group Template.

Step 4 Check the **Home Cluster** check box if you want to use the local cluster as the home cluster for all users whom use this template.

Step 5 Check the **Enable User for Unified CM IM and Presence** check box to allow users whom use this template to exchange instant messaging and presence information.

Step 6 From the drop-down list, select a **Services Profile** and **User Profile**.

Step 7 Complete the remaining fields in the **Feature Group Template Configuration** window. Refer to the online help for field descriptions.

Step 8 Click **Save**.

What to do next

Add a new end user. If your system is integrated with a company LDAP directory, you can import the user directly from an LDAP directory. Otherwise, create the end user manually.

- Import an End User from LDAP, on page 44
- Add an End User Manually, on page 45

Import an End User from LDAP

Perform the following procedure to manually import a new end user from a company LDAP directory. If your LDAP synchronization configuration includes a feature group template with a user profile that includes universal line and device templates and a DN pool, the import process automatically configures the end user and primary extension.

Note You cannot add new configurations (for example, adding a feature group template) into an LDAP directory sync after the initial sync has occurred. If you want to edit an existing LDAP sync, you must either use Bulk Administration, or configure a new LDAP sync.

Before you begin

Before you begin this procedure make sure that you have already synchronized Cisco Unified Communications Manager with a company LDAP directory. The LDAP synchronization must include a feature group template with universal line and device templates.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select the LDAP directory to which the user is added.

Step 3 Click **Perform Full Sync**.
Cisco Unified Communications Manager synchronizes with the external LDAP directory. Any new end users in the LDAP directory are imported into the Cisco Unified Communications Manager database.

What to do next

If the user is enabled for self-provisioning, the end user can use the Self-Provisioning Interactive Voice Response (IVR) to provision a new phone. Otherwise, perform one of the following tasks to assign a phone to the end user:

- Add New Phone for End User , on page 46
- Move an Existing Phone to a End User, on page 47

Add an End User Manually

Perform the following procedure to add new end user and configure them with an access control group and a primary line extension.

Note Make sure that you have already set up an access control groups that has the role permissions to which you want to assign your user. For details, see the "Manage User Access" chapter.

Before you begin

Verify that you have a user profile configured that includes a universal line template. If you need to configure a new extension, Cisco Unified Communications Manager uses the settings from the universal line template to configure the primary extension.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick User/Phone Add**.

Step 2 Enter the **User ID** and **Last Name**.

Step 3 From the **Feature Group Template** drop-down list, select a feature group template.

Step 4 Click **Save**.

Step 5 From the **User Profile** drop-down list, verify that the selected user profile includes a universal line template.

Step 6 From the **Access Control Group Membership** section, click the + icon.

Step 7 From the **User is a member of** drop-down list, select an access control group.

Step 8 Under **Primary Extension**, click the + icon.

Step 9 From the **Extension** drop-down list, select a DN that displays as **(available)**.

Step 10 If all line extensions display as **(used)**, perform the following steps:

a) Click the **New...** button.
The **Add New Extension** popup displays.

b) In the **Directory Number** field, enter a new line extension.
c) From the **Line Template** drop-down list, select a universal line template.
d) Click **OK**.
Cisco Unified Communications Manager configures the directory number with the settings from the universal line template.

Step 11 (Optional) Complete any additional fields in the **Quick User/Phone Add Configuration** window.

Step 12 Click **Save**.

What to do next

Perform one of the following procedures to assign a phone to this end user:

- Add New Phone for End User , on page 46
- Move an Existing Phone to a End User, on page 47

Add New Phone for End User

Perform the following procedure to add a new phone for a new or existing end user. Make sure that the user profile for the end user includes a universal device template. Cisco Unified Communications Manager uses the universal device template settings to configure the phone.

Before you begin

Perform one of the following procedures to add an end user:

- Add an End User Manually, on page 45
- Import an End User from LDAP, on page 44

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the end user for whom you want to add a new phone.

Step 3 Click the **Manage Devices**.
The Manage Devices window appears.

Step 4 Click **Add New Phone**.
The Add Phone to User popup displays.

Step 5 From the **Product Type** drop-down list, select the phone model.

Step 6 From the **Device Protocol** drop-down list select SIP or SCCP as the protocol.

Step 7 In the **Device Name** text box, enter the device MAC address.

Step 8 From the **Universal Device Template** drop-down list, select a universal device template.

Step 9 If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10 If you want to use Extension Mobility to access the phone, check the **In Extension Mobility** check box.

Step 11 Click **Add Phone**.

The Add New Phone popup closes. Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12 If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the **Phone Configuration** window.

Move an Existing Phone to a End User

Perform this procedure to move an existing phone to a new or existing end user.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the user to whom you want to move an existing phone.

Step 3 Click the **Manage Devices** button.

Step 4 Click the **Find a Phone to Move To This User** button.

Step 5 Select the phone that you want to move to this user.

Step 6 Click **Move Selected**.

Change the End User PIN

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user from the list.
The **End User Configuration** window is displayed.

Step 3 In the **PIN** field, double-click the existing PIN, which is encrypted, and enter the new PIN. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 4 In the **Confirm PIN** field, double-click the existing, encrypted PIN and enter the new PIN again.

Step 5 Click **Save**.

Note You can login to Extension Mobility, Conference Now, Mobile Connect, and Cisco Unity Connection voicemail with the same end user PIN, if **End User Pin synchronization** checkbox is enabled in the **Application Server Configuration** window for Cisco Unity Connection. End users can use the same PIN to log in to Extension Mobility and to access their voicemail.

Change the End User Password

You cannot change an end user password when LDAP authentication is enabled.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user from the list.
The **End User Configuration** window is displayed.

Step 3 In the **Password** field, double-click the existing password, which is encrypted, and enter the new password. You must enter at least the minimum number of characters that are specified in the assigned credential policy (1-127 characters).

Step 4 In the **Confirm Password** field, double-click the existing, encrypted password and enter the new password again.

Step 5 Click **Save**.

Create a Cisco Unity Connection Voice Mailbox

Before you begin

- You must configure Cisco Unified Communications Manager for voice messaging. For more information about configuring Cisco Unified Communications Manager to use Cisco Unity Connection, see the *System Configuration Guide for Cisco Unified Communications Manager* at:

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- You must associate a device and a Primary Extension Number with the end user.

- You can use the import feature that is available in Cisco Unity Connection instead of performing the procedure that is described in this section. For information about how to use the import feature, see the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user from the list.
The **End User Configuration** window is displayed.

Step 3 Verify that a primary extension number is associated with this user.

Note You must define a primary extension; otherwise, the Create Cisco Unity User link does not appear in the **Related Links** drop-down list.

Step 4 From the **Related Links** drop-down list, choose the Create Cisco Unity User link, and then click **Go**.

The Add Cisco Unity User dialog box appears.

Step 5 From the **Application Server** drop-down list, choose the Cisco Unity Connection server on which you want to create a Cisco Unity Connection user, and then click **Next**.

Step 6 From the **Subscriber Template** drop-down list, choose the subscriber template that you want to use.

Step 7 Click **Save**.

The mailbox is created. The link in the **Related Links** drop-down list changes to Edit Cisco Unity User in the **End User Configuration** window. In Cisco Unity Connection Administration, you can now view the user that you created.

Note After you integrate the Cisco Unity Connection user with the Cisco Unified Communications Manager end user, you cannot edit fields in Cisco Unity Connection Administration such as Alias (User ID in Cisco Unified CM Administration), First Name, Last Name, and Extension (Primary Extension in Cisco Unified CM Administration). You can only update these fields in Cisco Unified CM Administration.

CHAPTER 5

Manage Application Users

Application Users Overview

The **Application User Configuration** window in Cisco Unified CM Administration allows the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager application users.

Cisco Unified CM Administration includes the following application users by default:

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

Note Administrator users in the Standard CCM Super Users group can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting with a single sign-on to one of the applications.

Application Users Task Flow

Procedure

	Command or Action	Purpose
Step 1	Add New Application User, on page 52	Add a new application user.
Step 2	Associate Devices with Application Users, on page 53	Assign devices to associate with an application user.
Step 3	Add Administrator User to Cisco Unity or Cisco Unity Connection, on page 53	Add a user as an administrator user to Cisco Unity or Cisco Unity Connection. You configure the application user in Cisco Unified CM Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.
Step 4	Change Application User Password, on page 54	Change an application user password.
Step 5	Manage Application User Password Credential Information, on page 54	Change or view credential information, such as the associated authentication rules, the associated credential policy, or the time of last password change for an application user.

Add New Application User

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **Application User** .

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Application User Configuration** window. See the online help for information about the fields and their configuration options.

Step 4 Click **Save**.

What to do next

Associate Devices with Application Users, on page 53

Associate Devices with Application Users

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.

Step 3 In the **Available Devices** list, choose a device that you want to associate with the application user and click the **Down arrow** below the list. The selected device moves to the **Controlled Devices** list.

Note To limit the list of available devices, click the **Find more Phones** or **Find more Route Points** button.

Step 4 If you click the **Find more Phones** button, the **Find and List Phones** window displays. Perform a search to find the phones to associate with this application user.

Repeat the preceding steps for each device that you want to assign to the application user.

Step 5 If you click the **Find more Route Points** button, the **Find and List CTI Route Points** window displays. Perform a search to find the CTI route points to associate with this application user.

Repeat the preceding steps for each device that you want to assign to the application user.

Step 6 Click **Save**.

Add Administrator User to Cisco Unity or Cisco Unity Connection

If you are integrating Cisco Unified Communications Manager with Cisco Unity Connection 7.x or later, you can use the import feature that is available in Cisco Unity Connection 7.x or later instead of performing the procedure that is described in the this section. For information on how to use the import feature, see the *User Moves, Adds, and Changes* Guide for Cisco Unity Connection 7.x or later at

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

When the Cisco Unity or Cisco Unity Connection user is integrated with the Cisco Unified CM Application User, you cannot edit the fields. You can only update these fields in Cisco Unified Communications Manager Administration.

Cisco Unity and Cisco Unity Connection monitor the synchronization of data from Cisco Unified Communications Manager. You can configure the sync time in Cisco Unity Administration or Cisco Unity Connection Administration on the tools menu.

Before you begin

Ensure that you have defined an appropriate template for the user that you plan to push to Cisco Unity or Cisco Unity Connection

The **Create Cisco Unity User** link displays only if you install and configure the appropriate Cisco Unity or Cisco Unity Connection software. See the applicable *Cisco Unified Communications Manager Integration*

Guide for Cisco Unity or the applicable *Cisco Unified Communications Manager SCCP Integration Guide* for Cisco Unity Connection at

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.

Step 3 From the **Related Links** drop-down list, choose the **Create Cisco Unity Application User** link and click **Go**.
The Add **Cisco Unity User** dialog displays.

Step 4 From the **Application Server** drop-down list, choose the Cisco Unity or Cisco Unity Connection server on which you want to create a Cisco Unity or Cisco Unity Connection user and click **Next**.

Step 5 From the **Application User Template** drop-down list, choose the template that you want to use.

Step 6 Click **Save**.
The administrator account gets created in Cisco Unity or Cisco Unity Connection. The link in Related Links changes to **Edit Cisco Unity User** in the **Application User Configuration** window. You can now view the user that you created in Cisco Unity Administration or Cisco Unity Connection Administration.

Change Application User Password

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.
The **Application User Configuration** window displays information about the chosen application user.

Step 3 In the **Password** field, double click the existing, encrypted password and enter the new password.

Step 4 In the **Confirm Password** field, double click the existing, encrypted password and enter the new password again.

Step 5 Click **Save**.

Manage Application User Password Credential Information

Perform the following procedure to manage credential information for an application user password. This allows you to perform administrative duties such as locking a password, applying a credential policy to a password, or viewing information such as the time of the last failed login attempt.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **Application User**.
The **Find and List Users** window appears.

Step 2 To select an existing user, specify the appropriate filters in the **Find User Where** field, select **Find** to retrieve a list of users, and then select the user from the list.
The **Application User Configuration** window displays information about the chosen application user.

Step 3 To change or view password information, click the **Edit Credential** button next to the **Password** field.
The user **Credential Configuration** is displayed.

Step 4 Configure the fields on the **Credential Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 If you have changed any settings, click **Save**.

PART III

Manage Devices

CHAPTER 6

Manage Phones

Phone Management Overview

This chapter describes how to manage the phones in your network. The topics describe tasks such as adding new phones, moving existing phones to another user, locking phones and resetting phones.

The Cisco IP Phone Administration Guide for your phone model contains configuration information specific to the phone model.

Phone Button Template

Phone button template is created based on the phone models. Some phone models do not use any specific phone button template but some phone models require specific templates, either individual template or device default template.

The **Phone Template Selection for Non-Size Safe Phone** and **Auto Registration Legacy Mode** enterprise parameter on **Enterprise Parameters Configuration** page specifies the type of phone button template used. See the online help for more information about the fields.

Table 3: Phone Button Templates in Different Scenarios

Phone Template Selection for Non-Size Safe Phone	Auto Registration Legacy Mode	Phone
Create an Individual Template	False	Individual phone button template is created when adding a phone through Universal Device Template.
Use Template From Device Defaults	False	Individual phone button template is not created, it takes the phone button template from Device defaults.

Phone Template Selection for Non-Size Safe Phone	Auto Registration Legacy Mode	Phone
Use Template From Device Defaults	True	The values for Device Pool, Phone Template, Calling Search Space, Phone Button Template is taken from Device defaults.
Create an Individual Template	True	The values for Device Pool, Phone Template, Calling Search Space, Phone Button Template is taken from Device defaults. Individual templates are not created. Auto Registration Legacy Mode has the priority.

Phone Management Tasks

Procedure

	Command or Action	Purpose
Step 1	Add New Phone from Template with or Without an End User, on page 61	Add a new phone from universal device template with or without an end user.
Step 2	Add Phone Manually, on page 61	Add a new phone for an end user without device template.
Step 3	Add a New Phone from Template with an End User, on page 62	Add a new phone for an end user and assign a universal device template.
Step 4	Move an Existing Phone, on page 69	Move a configured phone to a different end user.
Step 5	Find an Actively Logged-In Device , on page 69	Search for a specific device or list all devices for which users are actively logged in.
Step 6	Find a Remotely Logged-In Device , on page 70	Search for a specific device or list all devices for which users are logged in remotely.
Step 7	Remotely Lock a Phone, on page 71	Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.
Step 8	Reset a Phone to Factory Defaults , on page 72	Reset a phone to its factory settings.

	Command or Action	Purpose
Step 9	Phone Lock/Wipe Report , on page 72	Search for devices that have been remotely locked and/or remotely reset to factory default settings.
Step 10	View LSC Status and Generate a CAPF Report for a Phone, on page 73	Search for LSC expiry status on phones, and also generate a CAPF report.

Add Phone Manually

Perform the following procedure to add a new phone manually with a user.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device** > **Phone** > **Find and List Phones**.

Step 2 From **Find and List Phones** page, click **Add New** to manually add a phone.

Add a New Phone page is displayed.

From **Add a New Phone** page, if you click "click here to add a new phone using a Universal Device Template" hyper link, the page is redirected to the **Add a New Phone** page to add a phone from the template with or without adding a user. See Add New Phone from Template with or Without an End User, on page 61 for more information.

Step 3 From the **Phone Type** drop-down list, select the phone model.

Step 4 Click **Next**.
The **Phone Configuration** page is displayed.

Step 5 On **Phone Configuration** page, enter the values in the required fields. See online help for more information on fields.

For additional information about the fields in the Product Specific Configuration area, see the *Cisco IP Phone Administration Guide* for your phone model.

Step 6 Click **Save** to save the phone configuration.

What to do next

Move an Existing Phone to a End User, on page 47

Add New Phone from Template with or Without an End User

Perform the following procedure to add a new phone from the template with or without adding a user. Cisco Unified Communications Manager uses the universal device template settings to configure the phone.

Before you begin

Ensure that you have configured a universal device template in Cisco Unified Communications Manager.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device** > **Phone** > **Find and List Phones**.

Step 2 From **Find and List Phones** page, click **Add New From Template** to add a phone from device template with or without adding an end user.

Add a New Phone page is displayed.

From **Add a New Phone** page, if you click "click here to enter all phone settings manually" hyper link, the page is redirected to the existing **Add a New Phone** page to manually add a phone. See Add Phone Manually, on page 61for more information.

Step 3 From the **Phone Type (and Protocol)** drop-down list, select the phone model.

The protocol drop-down displays only when the phone supports multiple protocols.

Step 4 In the **Name or MAC Address** text box, enter the name or MAC address.

Step 5 From the **Device Template** drop-down list, select a universal device template.

Step 6 From the **Directory Number (Line 1)** drop-down list, select a directory number.

If the directory numbers in the drop-down list exceeds the maximum drop-down limit, the **Find** tab is displayed. Click **Find**, a pop-up dialog box opens with Find Directory Number criteria.

Step 7 (Optional) Click **New**, enter Directory Number, and select a Universal Line template, if you want to create a new directory number and assign it to the device.

You can alternately create a phone using a user associated Directory Number, go to **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 8 (Optional) From the **User** drop-down list, select the end user for whom you want to add a new phone.

Note It is mandatory to select the user for Cisco Dual Mode (mobile) devices.

If the number of end users in the drop-down list exceeds the maximum drop-down limit, the **Find** tab is displayed. Click **Find**, a pop-up dialog box opens with Find end user criteria.

Step 9 Click **Add**.

Note For Non-Size safe phones, the phone templates are created based on the selection of **Phone Template Selection for Non-Size Safe Phone** and **Auto Registration Legacy Mode** parameters on **Enterprise Parameters Configuration** page.

Add Successful message is displayed. Cisco Unified Communications Manager adds the phone and **Phone Configuration** page is displayed. See the online help for more information about the fields on **Phone Configuration** page.

What to do next

Move an Existing Phone to a End User, on page 47

Add a New Phone from Template with an End User

Perform the following procedure to add a new phone for an end user.

Before you begin

The end user for whom you are adding the phone has a user profile set up that includes a universal device template. Cisco Unified Communications Manager uses the settings from the universal device template to configure the phone.

- End User Management Tasks, on page 39

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the end user for whom you want to add a new phone.

Step 3 Click the **Manage Devices**.
The Manage Devices window appears.

Step 4 Click **Add New Phone**.
The Add Phone to User popup displays.

Step 5 From the **Product Type** drop-down list, select the phone model.

Step 6 From the **Device Protocol** drop-down list select SIP or SCCP as the protocol.

Step 7 In the **Device Name** text box, enter the device MAC address.

Step 8 From the **Universal Device Template** drop-down list, select a universal device template.

Step 9 If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10 If you want to use Extension Mobility to access the phone, check the **In Extension Mobility** check box.

Step 11 Click **Add Phone**.
The Add New Phone popup closes. Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12 If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the **Phone Configuration** window.

Collaboration Mobile Convergence Virtual Device Overview

A CMC device is a virtual device which represents the Remote destination associated to it. When an Enterprise phone calls to the CMC device, call gets redirected to the Remote destination.This feature aims at creating a device type **Collaboration Mobile Convergence** that is identical to Spark Remote Device with few customization and provides the following benefits.

- Supports native mobile devices on Cisco Unified Communications Manager with similar functionality to a Spark Remote Devices.
- Takes advantage of as a Spark-RD with capability that includes future development feature parity.
- Allows customization for mobile specific use cases such as call move from Mobile to Deskphone, Deskphone to Mobile. (Add deskpickup timer on Identity page and enable via product support feature setting).
- CMC devices can be included in hunt groups.
- Capable of Shared line with Spark Remote Device.

- License - Count as a separate device for license usage perspective. Any multi-device license bundle should support CMC-RD.

Licensing adjustment for CMC RD device

When a new CMC device is added, it consumes licenses based on the Number/Type of devices associated to the User. The type of license consumed by a CMC device depends on the number of devices the End user associated with it have.

- If you are deploying a CMC device only, use an Enhanced License
- If you are deploying a CMC device and a Spark RD, use an Enhanced License
- If a CMC and a physical device: Enhanced Plus License
- If a CMC, a Spark RD and a physical device: Enhanced Plus License

Add a Collaboration Mobile Convergence Virtual Device

Perform the following procedure to add a Cisco Collaboration Mobile Convergence (CMC) Remote Device for an end user.

Before you begin

The end user for whom you are adding the phone must have a user profile set up that includes a universal device template. Cisco Unified Communications Manager uses the settings from the universal device template to configure the phone.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Phone** .

Step 2 Click the **Add New** button.

Step 3 Click the **Click here to enter all phone settings manually** link.
The **Add a New Phone** window appears.

Step 4 From the **Phone Type** drop-down list, select Cisco Collaboration Mobile Convergence and click **Next**.
The **Phone Configuration** window appears.

Step 5 From the **Owner User ID** drop-down, select the End User who will own the device.

Step 6 From the **Device Pool** drop-down, select the Device Pool.

Step 7 Click **Save** .
A warning message pops up to click on the **Apply Config** button to have the changes take effect. Click **Ok**. Device gets added successfully.

Step 8 To configure **Directory Number**, Click on the CMC device that is added, enter the **Directory Number** and Click **Save**.

Step 9 To add a new **Remote Destination** for the CMC device that is added, click on the link in the Identity box.

Step 10 In the Remote Destination Configuration window, enter the **Name**, **Destination number** and Click **Save**.

Note For one CMC device that is added, only one Remote Destination can be added.

Step 11 To update the existing Remote Destination, enter the **New Name** and Click **Save**.

Step 12 To delete existing Remote Destination, Click the Delete button in the menu.
A message from webpage appears confirming the permanent deletion. Click **Ok**

Step 13 To delete CMC device from the Device Page, Select the **Device** Check box and Click **Delete Selected** from the menu.

CMC RD Feature Interactions

Table 4: CMC RD Feature Interactions

Feature	Interaction
Shared Line handling	• In a set up where you have a shared desk phone with a CMC RD and Spark RD associated , when a user calls from an enterprise phone to a CMC Device DN, all the three - CMC RD, Spark RD and the Shared desk phone rings. • Answering from any of the remote destinations displays the message “Remote in Use” on the shared desk phone. • Answering from any of the shared desk phone disconnects both remote destination phones (CMC RD and Spark RD phones).
CMC Device to work in Call Manager Group (CMG) Setup	• When a CMC device is associated with a Call Manager group, it always runs on primary server and runs on the next active secondary server of the Call Manager Group only if the primary server is down. • If the primary server goes down mid call, then the ongoing call is still preserved and after the call ends, the CMC device registers to secondary server. **Note** When the call is in preserved mode, media between the phones still remains active, but no other actions can be performed except disconnecting the call. • If the Primary server was down initially and call was initiated while the CMC device was registered to Secondary server and then the Primary server comes up during ongoing call, the call will go into preservation mode and after the call ends the CMC device registers to Primary server.

Feature	Interaction
Call Anchoring	All the basic incoming calls from the CMC device and Number to Remote Destination calls are anchored in the enterprise network. When the CMC Remote Device is configured, users can place and receive calls from their mobile device with all calls being anchored to the enterprise: • A user can dial directly to a CMC Remote destination from an Enterprise number.The call is anchored in the enterprise network. In this scenario, the desk phone(shared line of CMC device) does not ring, but remains in **Remote in Use** state. • A user can dial from CMC Remote destination to any Enterprise number. The call is anchored. In this scenario, the desk phone (shared line of CMC device) remains in **Remote in Use** state.
Single Number Reach	• In the Remote Destination configuration page, if the **Enable Single Number Reach** checkbox is unchecked, the call do not get extended to the CMC RD and the call gets rejected. • The incoming calls from Remote Destination and the outbound **Number to Remote Destination** calls do not get affected irrespective of the **Enable Single Number Reach** checkbox selection. • If there is shared desk phone with the CMC device and if the **Enable Single Number Reach** checkbox is unchecked, then the call gets extended to the shared desk phone but not to the CMC RD. **Note** If the **Single Number Reach Voicemail Policy** is set to **user control** the mobility destination number will **NOT** be triggered in the event of a **Blind transfer** to the primary extension. Only the primary extension will be triggered. **User control** setting supports consult transfers. **Timer Control** Voice mail avoidance policy supports both Consult and Blind transfer.

Feature	Interaction
Call Routing based on Time of Day (ToD)	• You can use the Time of Day configurations for the Remote Destination to set up a ring schedule (for example, you can configure specific times such as Monday - Friday between 9 am and 5 pm). Calls will only be redirected to your Remote Destination at those times. Call from the Enterprise phone to CMC number gets routed based on the Ring Schedule fixed in the Remote Destination configuration page. Ring Schedule can be specified as below: • **All the Time** – Call gets routed at any time. There is no restrictions. • **Day(s) of the week** – Calls get routed only on the selected specific day. • **Specific time** - Calls get routed only in the selected office hours. Make sure to select the Time Zone. • When receiving a call during the Ring schedule, call from the Enterprise phone to CMC number gets routed based on the call number or pattern added in the Allowed access list or Blocked access list in the Remote Destination configuration page. • **Allowed access list**- Destination rings only if the caller number or pattern is in the Allowed access list. • **Blocked access list**- Destination do not ring if the caller number or pattern is in the Blocked access list. **Note** At any point of time, only Allowed access list or Blocked access list can be used.
User Locale settings	The CMC Virtual Device uses the locale settings that are configured in the Phone Configuration window to determine locale for the phone display and phone announcements. This policy works for regular calls, and for calls to a Conference Now number. For the announcement part, when calling (any enterprise phone) and called (CMC device) phone with same language selected in User locale settings, the announcement on both calling and Remote Destination is based on the User Locale settings selected in the Phone configuration page. **Note** For example, when calling from a **Remote Destination** which is associated with a CMC device, to a **Conference Now number**, the announcement is based on the User Locale settings selected in the Phone configuration page of the CMC device.

Feature	Interaction
New Access code for HLogin and HLogout	This functionality helps the administrator to set the Hunt Group Login and Logout number for the CMC device using the added service parameters: • Enterprise Feature Access number for Hunt group Login. • Enterprise Feature Access number for Hunt group Logout. When a user enters the Hlogin number from the RD associated to a CMC device, only then the calls will get redirected to the RD on dialing the hunt pilot number associated with the CMC device. When a user enters the Hlogout number from the RD associated to a CMC device, then the calls will not get redirected to the RD on dialing the hunt pilot number associated with the CMC device. By default the CMC device is Hloggedin. In either case, a direct call to the CMC device is not affected.
CMC Remote Destination call extention based on **delay before ringer timer** configured in Database	**If delay before ringing timer in DB is configured as 5000** • When called from an Enterprise phone to CMC number, the shared line rings and the call reaches the Remote Destination after five seconds. • When called from an Enterprise phone to CMC number, if the shared line answers the call before five seconds, the call do not get extended to Remote Destination. • When called from Enterprise phone to CMC number, the shared line rings and if the calling party disconnects the call before five seconds, the call do not get extended to Remote Destination. **If delay before ringing timer in DB is configured as 0** Any call from Enterprise phone to CMC number will alert the Remote Destination and the shared line at the same time.
Bulk Administration Tool (BAT) Support	BAT support is provided for CMC device

CMC RD Feature Restriction

Table 5: CMC RD Feature Restrictions

Feature	Restriction
CMC Remote Destination Association	The following restrictions apply: • You can associate a CMC device to one remote destination only. . • If the end user is deleted, then its associated CMC device and the RD (Remote Destination) is also deleted. **Note** Even if the **Enable Mobility** check box is checked or unchecked, the CMC and the RD is unaffected. The CMC device is not deleted. **Note** Cisco Unified Communications Manager does not support call handle preservation for CMC devices.

Move an Existing Phone

Perform the following procedure to move a configured phone to an end user.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the user to whom you want to move an existing phone.

Step 3 Click the **Manage Devices** button.

Step 4 Click the **Find a Phone to Move To This User** button.

Step 5 Select the phone that you want to move to this user.

Step 6 Click **Move Selected**.

Find an Actively Logged-In Device

The Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster features keep a record of the devices to which users are actively logged in. For the Cisco Extension Mobility feature, the actively logged-in device report tracks the local phones that are actively logged in by local users; for the Cisco Extension Mobility

Cross Cluster feature, the actively logged-in device report tracks the local phones that are actively logged in by remote users.

Unified Communications Manager provides a specific search window for searching for devices to which users are logged in. Follow these steps to search for a specific device or to list all devices for which users are actively logged in.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 Select the **Actively Logged In Device Report** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 3 To find all actively logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

a) From the first drop-down list, select a search parameter.
b) From the second drop-down list, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **(+)** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **(–)** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 4 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Find a Remotely Logged-In Device

The Cisco Extension Mobility Cross Cluster feature keeps a record of the devices to which users are logged in remotely. The Remotely Logged In Device report tracks the phones that other clusters own but that are actively logged in by local users who are using the EMCC feature.

Unified Communications Manager provides a specific search window for searching for devices to which users are logged in remotely. Follow these steps to search for a specific device or to list all devices for which users are logged in remotely.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 Select **Remotely Logged In Device** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 3 To find all remotely logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

a) From the first drop-down list, select a search parameter.
b) From the second drop-down list, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **(+)** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **(–)** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Remotely Lock a Phone

Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.

If a phone supports the Remote Lock feature, a **Lock** button appears in the top right hand corner.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote lock.

Step 4 On the **Phone Configuration** window, click **Lock**.

If the phone is not registered, a popup window displays to inform you that the phone will be locked the next time it is registered. Click **Lock**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgement.

Reset a Phone to Factory Defaults

Some phones support a remote wipe feature. When you remotely wipe a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

If a phone supports the remote wipe feature, a **Wipe** button appears in the top right hand corner.

⚠ **Caution** This operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 In the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote wipe.

Step 4 In the **Phone Configuration** window, click **Wipe**.

If the phone is not registered, a popup window displays to inform you that the phone will be wiped the next time it is registered. Click **Wipe**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgment.

Phone Lock/Wipe Report

Unified Communications Manager provides a specific search window for searching for devices which have been remotely locked and/or remotely wiped. Follow these steps to search for a specific device or to list all devices which have been remotely locked and/or remotely wiped.

Procedure

Step 1 Choose **Device** > **Phone**.

The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select the **Phone Lock/Wipe Report** from the **Related Links** drop-down list in the upper right corner of the window and click **Go**.

Step 3 To find all remotely locked or remotely wiped device records in the database, ensure that the text box is empty; go to Step 4.

To filter or search records for a specific device:

a) From the first drop-down list, select the device operation type(s) to search.
b) From the second drop-down list, select a search parameter.
c) From the third drop-down list, select a search pattern.
d) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

View LSC Status and Generate a CAPF Report for a Phone

Use this procedure to monitor Locally Significant Certificate (LSC) expiry information from within the Cisco Unified Communications Manager interface. The following search filters display the LSC information:

- LSC Expires—Displays the LSC expiry date on the phone.
- LSC Issued By—Displays the name of the issuer which can either be CAPF or third party.
- LSC Issuer Expires By—Displays the expiry date of the issuer.

Note The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to “NA” when there is no LSC issued on a new device.

The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to “ Unknown” when the LSC is issued to a device before the upgrade to Cisco Unified Communications Manager 11.5(1).

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the first **Find Phone where** drop-down list, choose one of the following criteria:

- LSC Expires
- LSC Issued By
- LSC Issuer Expires By

From the second **Find Phone where** drop-down list, choose one of the following criteria:

- is before
- is exactly
- is after
- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Click **Find**.
A list of discovered phones displays.

Step 4 From the **Related Links** drop-down list, choose the **CAPF Report in File** and click **Go**.
The report gets downloaded.

CHAPTER 7

Manage Device Firmware

Device Firmware Updates Overview

Device loads are the software and firmware for devices such as IP phones, telepresence systems, and others that are provisioned by and register to Cisco Unified Communications Manager. During installation or upgrade, Cisco Unified Communications Manager includes the latest loads available based on when the version of Cisco Unified Communications Manager was released. Cisco regularly releases updated firmware to introduce new features and software fixes and you may wish to update your phones to a newer load without waiting for a Cisco Unified Communications Manager upgrade that includes that load.

Before endpoints can upgrade to a new version of software, the files required by the new load must be made available for download at a location the endpoints have access to. The most common location is the Cisco UCM node with the Cisco TFTP service activated, called the "TFTP server". Some phones also support using an alternate download location, called a "load server".

If you want to get a list, view, or download files that already in the tftp directory on any server you can use the CLI command file list tftp to see the files in the TFTP directory, file view tftp to view a file, and file get tftp to get a copy of a file in the TFTP directory. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. You may also use a web browser to download any TFTP file by going to the URL "http://<tftp_server>:6970/<filename>".

Tip You can apply a new load to a single device before configuring it as a systemwide default. This method is useful for testing purposes. Remember, however, that all other devices of that type use the old load until you update the systemwide defaults with the new load.

Install a Device Pack or Individual Firmware

Install a device package to introduce new phone types and upgrade the firmware for multiple phone models.

- Individual firmware for existing devices can be installed or upgraded with the following options: Cisco Options Package (COP) files—The COP file contains the firmware files and the database updates so when installed on Publisher, it updates the default firmware apart from installing the firmware files.
- Firmware files only—It is supplied in a zip file, contains individual device firmware files that should be manually extracted and uploaded to the appropriate directory on the TFTP servers.

Note Refer to the README file for installation instructions that are specific to the COP or Firmware files package.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Install/Upgrade**.

Step 2 Fill in the applicable values in the Software Location section and click **Next**.

Step 3 In the **Available Software** drop-down list, select the device package file and click **Next**.

Step 4 Verify that the MD5 value is correct, and then click **Next**.

Step 5 In the warning box, verify that you selected the correct firmware, and then click **Install**.

Step 6 Check that you received a success message.

Note Skip to Step 8 if you are rebooting the cluster.

Step 7 Restart the **Cisco TFTP** service on all nodes where the service is running.

Step 8 Reset the affected devices to upgrade the devices to the new load.

Step 9 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults** and manually change the name of the load file (for specific devices) to the new load.

Step 10 Click **Save**, and then reset the devices.

Step 11 Restart the **Cisco Tomcat** service on all cluster nodes.

Step 12 Do one of the following:

- If you are running 11.5(1)SU4 or lower, 12.0(1) or 12.0(1)SU1, reboot the cluster.
- If you are running an 11.5(x) release at 11.5(1)SU5 or higher, or any release higher at 12.0(1)SU2 or higher, reboot the **Cisco CallManager** service on the publisher node. However, if you are running the **Cisco CallManager** service on subscriber nodes only, you can skip this task.

Potential Issues with Firmware Installs

Here are some potential issues that you may run across after installing a device pack:

Issue	Cause/Resolution
New devices won't register	This could occur due from a device type mismatch. This can be caused by: • The device was added in the Phone Configuration window using the wrong device type. For example, Cisco DX80 was selected as the phone type instead of Cisco TelePresence DX80. Reconfigure the device with the correct device type. • The **Cisco CallManager** service doesn't know about the new device type. In this case, restart the **Cisco CallManager** service on the publisher node.
Endpoints aren't upgrading to the new firmware	**Possible reasons:** • The device pack wasn't installed on the TFTP server. As a result, the firmware isn't available for download by the phones. • The **Cisco TFTP** service wasn't restarted after the install so the service doesn't know about the new files. Make sure to install the device pack on the TFTP server.
Phone Configuration window in Cisco Unified CM Administration shows broken links where the icon image should be for a new device type	Restart the **Cisco Tomcat** service on all nodes from the CLI.

Remove Unused Firmware from the System

The **Device Load Management** window allows you to delete unused firmware (device loads) and associated files from the system to increase disk space. For example, you can delete unused loads before an upgrade to prevent upgrade failures due to insufficient disk space. Some firmware files may have dependent files that are not listed in the **Device Load Management** window. When you delete a firmware, the dependent files are also deleted. However, the dependent files are not deleted if they are associated with additional firmware.

Note You must delete unused firmware separately for each server in the cluster.

Before you begin

Caution Before you delete unused firmware, ensure that you are deleting the right loads. The deleted loads cannot be restored without performing a DRS restore of the entire cluster. We recommend that you take a backup before deleting the firmware.

Ensure that you do not delete files for devices that use multiple loads of files. For example, certain CE endpoints use multiple loads. However, only one load is referenced as **In Use** in the **Device Load Management** window.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Software Upgrades** > **Device Load Management**.

Step 2 Specify the search criteria and click **Find**.

Step 3 Select the device load that you want to delete. You can select multiple loads if required.

Step 4 Click **Delete Selected Loads**.

Step 5 Click **OK**.

Set up Default Firmware for a Phone Model

Use this procedure to set the default firmware load for a specific phone model. When a new phone registers, Cisco Unified Communications Manager tries to send the default firmware to the phone, unless the phone configuration specifies has an overriding firmware load specified in the **Phone Configuration** window.

Note For an individual phone, the setting of the **Phone Load Name** field in the **Phone Configuration** window overrides the default firmware load for that particular phone.

Before you begin

Make sure that the firmware is loaded onto the TFTP server.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Defaults**.
The **Device Defaults Configuration** window appears displaying the default firmware loads for the various phone models that Cisco Unified Communications Manager supports. The firmware appears in the **Load Information** column.

Step 2 Under **Device Type**, locate the phone models for which you want to assign the default firmware.

Step 3 In the accompanying **Load Information** field, enter the firmware load.

Step 4 (Optional) Enter the default **Device Pool** and default **Phone Template** for that phone model.

Step 5 Click **Save**.

Set the Firmware Load for a Phone

Use this procedure to assign a firmware load for a specific phone. You may want to do this if you want to use a different firmware load than the default that is specified in the **Device Defaults Configuration** window.

Note If you wish to assign a version for many phones you can use the Bulk Administration Tool to configure the **Phone Load Name** field using a CSV file or query. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select an individual phone.

Step 3 In the **Phone Load Name** field, enter the name of the firmware. For this phone, the firmware load specified here overrides the default firmware load that is specified in the **Device Defaults Configuration** window.

Step 4 Complete any remaining fields in the **Phone Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

Step 6 Click **Apply Config** to push the changed fields to the phone.

Using a Load Server

If you want phones to download firmware updates from a server that is not the TFTP server you may configure a "load server" on the phone's **Phone Configuration** page. A load server may be another Cisco Unified Communications Manager or a third-party server. A third-party server must be capable of providing any files the phone requests through HTTP on TCP Port 6970 (preferred) or the UDP-based TFTP protocol. Some phone models such as the DX family Cisco TelePresence devices only support HTTP for firmware updates.

Note If you wish to assign a load server for many phones you can use the Bulk Administration Tool to configure the **Load Server** field using a CSV file or query. For details, see the *Bulk Administration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select an individual phone.

Step 3 In the **Load Server** field, enter the IP Address or hostname of the alternate server.

Step 4 Complete any remaining fields in the **Phone Configuration** window. For help with the fields and their settings, see the online help.

Step 5 Click **Save**.

Step 6 Click **Apply Config** to push the changed fields to the phone.

Find Devices with Non-default Firmware Loads

The Firmware Load Information window in Unified Communications Manager enables you to quickly locate devices that are not using the default firmware load for their device type.

Note Each device can have an individually assigned firmware load that overrides the default.

Use the following procedure to locate devices that are not using the default firmware load.

Procedure

Step 1 Choose **Device** > **Device Settings** > **Firmware Load Information**.

The page updates to display a list of device types that require firmware loads. For each device type, the Devices Not Using Default Load column links to configuration settings for any devices that use a non-default load.

Step 2 To view a list of devices of a particular device type that are using a non-default device load, click the entry for that device type in the Devices Not Using Default Load column.

The window that opens lists the devices of a particular device type that are not running the default firmware load.

CHAPTER 8

Manage Infrastructure Devices

Manage Infrastructure Overview

This chapter provides tasks to manage network infrastructure devices such as switches and wireless access points as a part of the Location Awareness feature. When Location Awareness is enabled, the Cisco Unified Communications Manager database saves status information for the switches and access points in your network, including the list of endpoints that currently associate to each switch or access point.

The endpoint to infrastructure device mapping helps Cisco Unified Communications Manager and Cisco Emergency Responder to determine the physical location of a caller. For example, if a mobile client places an emergency call while in a roaming situation, Cisco Emergency Responder uses the mapping to determine where to send emergency services.

The Infrastructure information that gets stored in the database also helps you to monitor your infrastructure usage. From the Unified Communications Manager interface, you can view network infrastructure devices such as switches and wireless access points. You can also see the list of endpoints that currently associate to a specific access point or switch. If infrastructure devices are not being used, you can deactivate infrastructure devices from tracking.

Manage Infrastructure Prerequisites

You must configure the Location Awareness feature before you can manage wireless infrastructure within the Cisco Unified Communications Manager interface. For your wired infrastructure, the feature is enabled by default.

For configuration details, see "Configure Location Awareness" chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.

You must also install your network infrastructure. For details, see the hardware documentation that comes with your infrastructure devices such as wireless LAN controllers, Access Points, and Switches.

Manage Infrastructure Task Flow

Complete the following tasks to monitor and manage your network infrastructure devices.

Procedure

	Command or Action	Purpose
Step 1	View Status for Infrastructure Device, on page 82	Get the current status of a wireless access point or ethernet switch, including the list of associated endpoints.
Step 2	Deactivate Tracking for Infrastructure Device, on page 82	If you have a switch or access point that is not being used, mark the device inactive. The system will stop updating the status or the list of associated endpoints for the infrastructure device.
Step 3	Activate Tracking for Deactivated Infrastructure Devices, on page 83	Initiate tracking for an inactive infrastructure device. Cisco Unified Communications Manager begins updating the database with the status and the list of associated endpoints for the infrastructure device.

View Status for Infrastructure Device

Use this procedure to get the current status of an infrastructure device such as a wireless access point or an ethernet switch. Within the Cisco Unified Communications Manager interface, you can view the status for an access point or switch and see the current list of associated endpoints.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find**.

Step 3 Click on the switch or access point for which you want the status.
The **Switches and Access Point Configuration** window displays the current status including the list of endpoints that currently associate to that access point or switch.

Deactivate Tracking for Infrastructure Device

Use this procedure to remove tracking for a specific infrastructure device such as a switch or access point. You may want to do this for switches or access points that are not being used.

Note If you remove tracking for an infrastructure device, the device remains in the database, but becomes inactive. Cisco Unified Communications Manager no longer updates the status for the device, including the list of endpoints that associate to the infrastructure device. You can view your inactive switches and access points from the **Related Links** drop-down in the **Switches and Access Points** window.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 Click **Find** and select the switch or access point that you want to stop tracking.

Step 3 Click **Deactivate Selected**.

Activate Tracking for Deactivated Infrastructure Devices

Use this procedure to initiate tracking for an inactive infrastructure device that has been deactivated. Once the switch or access point becomes active, Cisco Unified Communications Manager begins to dynamically track the status, including the list of endpoints that associate to the switch or access point.

Before you begin

Location Awareness must be configured. For details, see the "Location Awareness" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points**.

Step 2 From **Related Links**, choose **Inactive Switches and Access Points** and click **Go**.
The **Find and List Inactive Switches and Access Points** window displays infrastructure devices that are not being tracked.

Step 3 Select the switch or access point for which you want to initiate tracking.

Step 4 Click **Reactivate Selected**.

PART IV

Manage the System

CHAPTER 9

Monitor System Status

View Cluster Nodes Status

Use this procedure to show information about the nodes in your cluster.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **Cluster**.

Step 2 Review the fields in the **Cluster** window. See the online help for more information about the fields.

View Hardware Status

Use this procedure to show the hardware status and information about hardware resources in your system.

Procedure

Step 1 From the Cisco Unified Operating System Administration, select **Show** > **Hardware**.

Step 2 Review the fields in the **Hardware Status** window. See the online help for more information about the fields.

View Network Status

Use this procedure to show the network status of your system, such as ethernet and DNS information.

The network status information that is displayed depends on whether Network Fault Tolerance is enabled:

- If Network Fault Tolerance is enabled, Ethernet port 1 automatically manages network communications if Ethernet port 0 fails.
- If Network Fault Tolerance is enabled, network status information is displayed for the network ports Ethernet 0, Ethernet 1, and Bond 0.
- If Network Fault Tolerance is not enabled, status information is displayed for only Ethernet 0.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **Network**.

Step 2 Review the fields in the **Network Configuration** window. See the online help for more information about the fields.

View Installed Software

Use this procedure to show information about software versions and installed software packages.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **Software**.

Step 2 Review the fields in the **Software Packages** window. See the online help for more information about the fields.

View System Status

Use this procedure to show the overall system status, such as information about locales, up time, CPU use, and memory use.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **System**.

Step 2 Review the fields in the **System Status** window. See the online help for more information about the fields.

View IP Preferences

Use this procedure to show a list of registered ports are available to the system.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Show** > **IP Preferences**.

Step 2 (Optional) To filter or search records, perform one of the following tasks:

- From the first list, select a search parameter.
- From the second list, select a search pattern.
- Specify the appropriate search text, if applicable.

Step 3 Click **Find**.

Step 4 Review the fields that appear in the **System Status** window. See the online help for more information about the fields.

View Last Login Details

When end users (with either local and LDAP credentials) and administrators log in to web applications for Cisco Unified Communications Manager or IM and Presence Service, the main application window displays the last successful and unsuccessful login details.

Users logging in using SAML SSO feature can only view the last successful system login information. The user can refer to the Identity Provider (IdP) application to track the unsuccessful SAML SSO login information.

The following web applications display the login attempt information:

- Cisco Unified Communications Manager:
  - Cisco Unified CM Administration
  - Cisco Unified Reporting
  - Cisco Unified Serviceability
- IM and Presence Service
  - Cisco Unified CM IM and Presence Administration
  - Cisco Unified IM and Presence Reporting
  - Cisco Unified IM and Presence Serviceability

Only administrators can login and view the last login details for the following web applications in Cisco Unified Communications Manager:

- Disaster Recovery System
- Cisco Unified OS Administration

Ping a Node

Use the Ping Utility to ping another node in the network. These results can help you verify or troubleshoot device connectivity.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Ping**.

Step 2 Configure the fields on the **Ping Configuration** window. See the online help for more information about the fields and their configuration options.

Step 3 Choose **Ping**.

The ping results are displayed.

Display Service Parameters

You may need to compare all service parameters that belong to a particular service on all servers in a cluster. You may also need to display only out-of-sync parameters (that is, service parameters for which values differ from one server to another) or parameters that have been modified from the suggested value.

Use the following procedure to display the service parameters for a particular service on all servers in a cluster.

Procedure

Step 1 Choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose a server.

Step 3 From the Service drop-down list box, choose the service for which you want to display the service parameters on all servers in a cluster.

Note The Service Parameter Configuration window displays all services (active or not active).

Step 4 In the Service Parameter Configuration window that displays, choose Parameters for All Servers in The Related Links Drop-down List Box; then, click Go.

The Parameters for All Servers window displays. For the current service, the list shows all parameters in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click on the server name or on the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Parameters for All Servers windows.

Step 5 If you need to display out-of-sync service parameters, choose Out of Sync Parameters for All Servers in the Related Links drop-down list box, then click Go.

The Out of Sync Parameters for All Servers window displays. For the current service, service parameters that have different values on different servers display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that contain this parameter displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click the server name or the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Out of Sync Parameters for All Servers windows.

Step 6 If you need to display service parameters that have been modified from the suggested value, choose Modified Parameters for All Servers in the Related Links drop-down list box; then, click Go.

The Modified Parameters for All Servers window displays. For the current service, service parameters that have values that differ from the suggested values display in alphabetical order. For each parameter, the suggested value displays next to the parameter name. Under each parameter name, a list of servers that have different values from the suggested values displays. Next to each server name, the current value for this parameter on this server displays.

For a given parameter, click the server name or the current parameter value to link to the corresponding service parameter window to change the value. Click Previous and Next to navigate between Modified Parameters for All Servers windows.

Configure Network DNS

Use this procedure to set your network DNS

Note You can also assign a DNS primary and secondary server via the DHCP Configuration window in Cisco Unified CM Administration.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 If you want to assign a DNS server, run one of the following commandson the publisher node:

- To assign the primary DNS server**run set network dns primary <ip_address>**
- To assign the secondary DNS server**run the set network dns secondary <ip_address>**

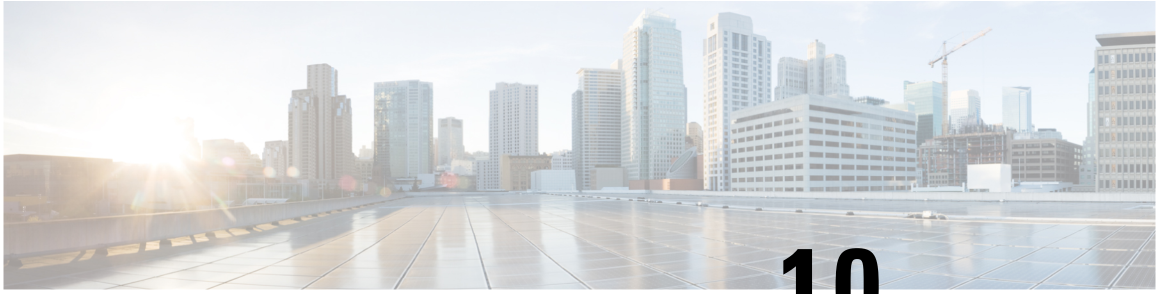
Step 3 To assign additional DNS option **run the set network dns options [timeout| seconds] [attempts| number] [rotate].**

- Timeout Sets the DNS timeout
- Seconds is the number of seconds for the timeout
- Attempts Sets the number of times to attempt a DNS request
- Number specifies the number of attempts

- Rotate causes the system to rotate among the configured DNS servers and distribute the load

For example, set network dns options timeout 60 attempts 4 rotate

The server reboots after you run this command.



CHAPTER 10

Alarms

Overview

Cisco Unified Serviceability and Cisco Unified IM and Presence Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting and also applies to clusters.

You can configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from Debug to Emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDL trace log file (for Cisco CallManager and CTIManager services only), or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure and that are specified in the routing list in the alarm definition (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or write the alarm information to its final destination (such as a log file).

You can configure alarms for services, such as Cisco Database Layer Monitor, on a particular node, or you configure alarms for a particular service on all nodes in the cluster.

Note Cisco Unity Connection SNMP does not support traps.

Tip For the Remote Syslog Server, do not specify a Unified Communications Manager server, which cannot accept syslog messages from other servers.

You use the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool (Unifed RTMT) to collect alarms that get sent to an SDL trace log file (for Cisco CallManager and CTIManager services only). You use the SysLog Viewer in Unifed RTMT to view alarm information that gets sent to the local syslog.

Alarm Configuration

You can configure alarms for services, such as Cisco Database Layer Monitor, in Cisco Unified Serviceability. Then, you configure the location or locations, such as Syslog Viewer (local syslog), where you want the system to send the alarm information. With this option, you can do the following:

- Configure alarms for services on a particular server or on all servers (Unified Communications Manager clusters only)
- Configure different remote syslog servers for the configured services or servers
- Configure different alarm event level settings for different destinations

Cisco Syslog Agent enterprise parameters in Cisco Unified Communications Manager Administration allow you to forward all alarms that meet or exceed the configured threshold to a remote syslog server with these two settings: remote syslog server name and syslog severity. To access these Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting** > **Enterprise Parameters**.
Cisco IM and Presence	In Cisco Unified Communications Manager IM and Presence Administration, choose **System** > **Enterprise Parameters**.

The alarms include system (OS/hardware platform), application (services), and security alarms.

Note If you configure both the Cisco Syslog Agent alarm enterprise parameters and application (service) alarms in Cisco Unified Serviceability, the system can send the same alarm to the remote syslog twice.

If local syslog is enabled for an application alarm, the system sends the alarm to the enterprise remote syslog server only when the alarm exceeds both the local syslog threshold and the enterprise threshold.

If remote syslog is also enabled in Cisco Unified Serviceability, the system forwards the alarm to the remote syslog server by using the application threshold that is configured in Cisco Unified Serviceability, which may result in the alarm being sent to the remote syslog server twice.

The event level/severity settings provide a filtering mechanism for the alarms and messages that the system collects. This setting helps to prevent the Syslog and trace files from becoming overloaded. The system forwards only alarms and messages that exceed the configured threshold.

For more information about the severity levels attached to alarms and events, see the Alarm Definitions, on page 95.

Alarm Definitions

Used for reference, alarm definitions describe alarm messages: what they mean and how to recover from them. You search the Alarm Definitions window for alarm information. When you click any service-specific alarm definition, a description of the alarm information (including any user-defined text that you have added) and a recommended action display.

You can search for alarm definitions of all alarms that display in the Serviceability GUI. To aid you with troubleshooting problems, the definitions, which exist in a corresponding catalog, include the alarm name, description, explanation, recommended action, severity, parameters and monitors.

When the system generates an alarm, it uses the alarm definition name in the alarm information, so you can identify the alarm. In the alarm definition, you can view the routing list, which specifies the locations where the system can send the alarm information. The routing list may include the following locations, which correlate to the locations that you can configure in the Alarm Configuration window:

- Unified Communications Manager only: SDL - The system sends the alarm information to the SDL trace if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- SDI - The system sends the alarm information to the SDI trace if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- Sys Log - The system sends the alarm information to the remote syslog server if you enable the alarm for this option, specify an event level in the Alarm Configuration window, and enter a server name or IP address for the remote syslog server.
- Event Log - The system sends the alarm information to the local syslog, which you can view in the SysLog Viewer in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT), if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- Data Collector - The system sends the alarm information to the real-time information system (RIS data collector) for alert purposes only. You cannot configure this option in the Alarm Configuration window.
- SNMP Traps - System generates an SNMP trap. You cannot configure this option in the Alarm Configuration window.

Tip If the SNMP Traps location displays in the routing list, the system forwards the alarm information to the CCM MIB SNMP agent, which generates traps according to the definition in CISCO-CCM-MIB.

The system sends an alarm if the configured alarm event level for the specific location in the Alarm Configuration window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the Alarm Configuration window, you configure the alarm event level for the specific destination as Warning, Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, the system does not send the alarm to the corresponding location.

For each alarm definition, you can include an additional explanation or recommendation. All administrators have access to the added information. You directly enter information into the User Defined Text pane that displays in the Alarm Details window. Standard horizontal and vertical scroll bars support scrolling. Cisco Unified Serviceability adds the information to the database.

Alarm Information

You view alarm information to determine whether problems exist. The method that you use to view the alarm information depends on the destination that you chose when you configured the alarm. You can view alarm information that is sent to the SDL trace log file (Unified Communications Manager) by using the Trace and Log Central option in Unified RTMT or by using a text editor. You can view alarm information that gets sent to local syslog by using the SysLog Viewer in Unified RTMT.

Set Up Alarms

Perform the following steps to configure alarms.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, Cisco Unity Connection Administrationor Cisco Unified IM and Presence Administration, configure the Cisco Syslog Agent enterprise parameters to send system, application (services), and security alarms/messages to a remote syslog server that you specify. Skip this step to configure application (services) alarms/messages in Cisco Unified Serviceability.

Step 2 In Cisco Unified Serviceability, configure the servers, services, destinations, and event levels for the applications (services) alarm information that you want to collect.

Step 3 (Optional) Add a definition to an alarm.

- All services can go to the SDI log (but must be configured in Trace also).
- All services can go to the SysLog Viewer.
- Unified Communications Manager only: Only the Cisco CallManager and CiscoCTIManager services use the SDL log.
- To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name. If you do not configure the remote server name, Cisco Unified Serviceability does not send the Syslog messages to the remote syslog server.

Tip Do not configure a Unified Communications Manager server as a remote Syslog server.

Step 4 If you chose an SDL trace file as the alarm destination, collect traces and view the information with the Trace and Log Central option in Unified RTMT.

Step 5 If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in Unified RTMT.

Step 6 See the corresponding alarm definition for the description and recommended action.

Alarm Service Setup

Syslog Agent Enterprise Parameters

You can configure the Cisco Syslog Agent enterprise parameters to send system, application, and security alarms/messages that exceed the configured threshold to a remote syslog server that you specify. To access the Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting** > **Enterprise Parameters**.
Cisco IM and Presence	In Cisco Unified Communications Manager IM and Presence Administration, choose **System** > **Enterprise Parameters**.

Next, configure the remote syslog server names (Remote Syslog Server Name 1, Remote Syslog Server Name 2, Remote Syslog Server Name 3, Remote Syslog Server Name 4, and Remote Syslog Server Name 5) and syslog severity. Ensure that you specify valid IP addresses while configuring the server names. The syslog severity is applicable to all the remote syslog servers that you configure. Then click **Save**. For the valid values to enter, click the **?** button. If no server name is specified, Cisco Unified Serviceability does not send the Syslog messages.

Caution While configuring remote syslog servers in Unified Communications Manager, do not add duplicate entries for remote syslog server names. If you add duplicate entries, the Cisco Syslog Agent will ignore the duplicate entries while sending messages to the remote syslog servers.

Note Do not configure a Unified Communications Manager as a remote syslog server. The Unified Communications Manager node does not accept Syslog messages from another server.

Set Up Alarm Service

This section describes how to add or update an alarm for a feature or network service that you manage through Cisco Unified Serviceability.

Note Cisco recommends that you do not change SNMP Trap and Catalog configurations.

Cisco Unity Connection also uses alarms, which are available in Cisco Unity Connection Serviceability. You cannot configure alarms in Cisco Unity Connection Serviceability. For details, see the *Cisco Unity Connection Serviceability Administration Guide*.

Refer to your online OS documentation for more information on how to use your standard registry editor.

Procedure

Step 1 Choose **Alarm** > **Configuration**.

The Alarm Configuration window displays.

Step 2 From the Server drop-down list, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Service Group drop-down list, choose the category of service, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.

Tip For a list of services that correspond to the service groups, see Service groups.

Step 4 From the Service drop-down list, choose the service for which you want to configure the alarm; then, click **Go**.

Only services that support the service group and your configuration display.

Tip The drop-down list displays active and inactive services.

In the Alarm Configuration window, a list of alarm monitors with the event levels displays for the chosen service. In addition, the Apply to All Nodes check box displays.

Step 5 Unified Communications Manager only: If you want to do so, you can apply the alarm configuration for the service to all nodes in the cluster by checking the **Apply to All Nodes** check box, provided your configuration supports clusters.

Step 6 Configure the settings, as described in Alarm configuration settings, which includes descriptions for monitors and event levels.

Step 7 To save your configuration, click the **Save** button.

Note To set the default, click the **Set Default** button; then, click **Save**.

What to do next

Tip The system sends the alarm if the configured alarm event level for the specific destination in the Alarm Configuration window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the Alarm Configuration window, you configure the alarm event level for the specific destination as Warning, Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, which are higher severity levels, the system does not send the alarm to the corresponding location.

To access the alarm definitions for the Cisco Extension Mobility Application service, Cisco Unified Communications Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer service, choose the **JavaApplications** catalog in the Alarm Messages Definitions window described in Alarm definitions.

Set Up Alarm Services That Use Cisco Tomcat

The following services use Cisco Tomcat for alarm generation:

- Cisco Extension Mobility Application
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer

The system login alarm AuthenticationFailed also uses Cisco Tomcat. To generate alarms for these services, perform the following procedure.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Alarm** > **Configuration**.

Step 2 From the Server drop-down list, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Services Group drop-down list, choose **Platform Services**; then, click **Go**.

Step 4 From the Services drop-down list, choose **CiscoTomcat**; then, click **Go**.

Step 5 Unified Commuications Manager only: If you want to do so, you can apply the alarm configuration for the service to all nodes in the cluster by checking the **Apply to All Nodes** check box, if your configuration supports clusters.

Step 6 Configure the settings, as described in Alarm configuration settings, which includes descriptions for monitors and event levels.

Step 7 To save your configuration, click the **Save** button.

Service Groups

The following table lists the services that correspond to the options in the Service Group drop-down list in the Alarm Configuration window.

Note Not all listed service groups and services apply to all system configurations.

Table 6: Service Groups in Alarm Configuration

Service Group	Services
CM Services	Cisco CTIManager, Cisco CallManager, Cisco DHCP Monitor Service, Cisco Dialed Number Analyzer, Cisco Dialed Number Analyzer Server, Cisco Extended Functions, Cisco IP Voice Media Streaming App, Cisco Messaging Interface, Cisco Headset Service, and Cisco TFTP
CTI Services	Cisco IP Manager Assistant and Cisco WebDialer Web Service
CDR Services	Cisco CAR Scheduler, Cisco CDR Agent, and Cisco CDR Repository Manager

Service Group	Services
Database and Admin Services	Cisco Bulk Provisioning Service and Cisco Database Layer Monitor
Performance and Monitoring Services	Cisco AMC Service and Cisco RIS Data Collector
Security Services	Cisco Certificate Authority Proxy Function and Cisco Certificate Expiry Monitor
Directory Services	Cisco DirSync
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master
System Services	Cisco Trace Collection Service
Platform Services	Cisco Tomcat and Cisco Smart License Manager
Location base Tracking Services	Cisco Wireless Controller Synchronization Service

Alarm Configuration Settings

The following table describes all alarm configuration settings, even though the service may not support the settings.

Table 7: Alarm Configuration Settings

Name	Description
Server	From the drop-down list, choose the server (node) for which you want to configure the alarm; then, click **Go**.
Service Group	Cisco Unity Connection supports only the following service groups: Database and Admin Services, Performance and Monitoring Services, Backup and Restore Services, System Services, and Platform Services. From the drop-down list, choose the category of services, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.

Name	Description
Service	From the Service drop-down list, choose the service for which you want to configure the alarm; then, click **Go**. Only services that support the service group and your configuration display. **Tip** The drop-down list displays both active and inactive services.
Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service only: Apply to All Nodes	To apply the alarm settings for the service to all nodes in a cluster, check the check box.
Enable Alarm for Local Syslogs	The SysLog viewer serves as the alarm destination. The program logs errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Name	Description
Enable Alarm for Remote Syslogs	The Syslog file serves as the alarm destination. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. If this destination is enabled and no server name is specified, Cisco Unified Serviceability does not send the Syslog messages. The configured AMC primary and failover collectors use the remote syslog settings. The remote syslog settings used by the collectors are those configured on the respective individual nodes. If the remote syslog is only configured on AMC primary collector without configuring remote syslog on AMC failover collector and failover occurs in AMC primary collector, then no remote syslogs will be generated. You must configure exactly the same settings on all nodes, to send the remote syslog alarms to the same remote syslog server. When failover occurs in AMC controller or when the collector configuration changes to a different node, the remote syslog settings on a backup or newly configured node is used. To prevent too many alarms flooding the system, you can check the **Exclude End Point Alarms** check box. This ensures that the endpoint phone-related events get logged into a separate file. **Exclude End Point Alarms** check box is displayed only for the CallManager services, and is not checked by default. You need to check the **Apply to All Nodes** also, when you check this check box. The configuration options for endpoint alarms are listed in Alarm configuration settings. **Tip** Do not specify a Unified Communications Manager or a Cisco Unified Communications Manager IM and Presence Service node as the destination because the node does not accept syslog messages from another node.
Remote Syslog Servers	In each of the Server Name 1, Server Name 2, Server Name 3, Server Name 4, and Server Name 5 fields, enter the name or IP address of the remote syslog server that you want to use to accept syslog messages. For example, if you want to send the alarms to Cisco Unified Operations Manager, specify the Cisco Unified Operations Manager as the server name. **Tip** Do not specify a Unified Communications Manager or a Cisco Unified Communications Manager IM and Presence Service node as the destination because the node does not accept syslog messages from another node.

Name	Description
Enable Alarm for SDI Trace	The SDI trace library serves as the alarm destination. To log alarms, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see Set up trace parameters.
Unified Communications Manager and Unified Communications Manager BE only: Enable Alarm for SDL Trace	The SDL trace library serves as the alarm destination. This destination applies only to the Cisco CallManager service and the CTIManager service. Configure this alarm destination by using Trace SDL configuration. To log alarms in the SDL trace log file, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see the Set up trace parameters.
Alarm Event Level	From the drop-down list, choose one of the following options: **Emergency** This level designates system as unusable. **Alert** This level indicates that immediate action is needed. **Critical** The system detects a critical condition. **Error** This level signifies that error condition exists. **Warning** This level indicates that a warning condition is detected. **Notice** This level designates a normal but significant condition. **Informational** This level designates information messages only. **Debug** This level designates detailed event information that Cisco Technical Assistance Center engineers use for debugging.

The following tables describe the default alarm configuration settings.

	Local Syslogs	Remote Syslogs	SDI Trace	SDL Trace
Enable Alarm	Checked	Unchecked	Checked	Checked
Alarm Event Level	Error	Disabled	Error	Error

Exclude End Point Alarms	Local Syslog	Alternate Syslog	Remote Syslog	Syslog Severity and Strangulate Alert	Syslog Traps
Checked	No	Yes	No	No	No
Unchecked	No	Yes	Yes	Yes	Yes

Alarm Definitions and User-Defined Description Additions

This section provides procedural information to search, view, and create user information for alarm definitions that display in the Serviceability interface.

View Alarm Definitions and Add User-Defined Descriptions

This section describes how to search for and view an alarm definitions.

Tip Unified Communications Manager and Cisco Unity Connection only: You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability. You cannot add user-defined descriptions to alarm definitions in Cisco Unity Connection Serviceability.

Cisco Unity Connection also uses certain alarm definitions in Cisco Unified Serviceability, and they must be viewed in Cisco Unified Serviceability. Be aware that alarms that are associated with the catalogs in System catalogs are available for viewing.

Before you begin

Review the description of alarm definition catalogs.

Procedure

Step 1 Select **Alarm** > **Definitions**.

Step 2 Perform one of the following actions:

- Select an alarm as follows:
  - Select an alarm catalog from the **Find alarms where** drop-down list, for example, a System Alarm catalog or IM and Presence alarm catalog.
  - Select the specific catalog name from the **Equals** drop-down list.
- Enter the alarm name in the **Enter Alarm Name** field.

Step 3 Select **Find**.

Step 4 Perform one of the following actions if multiple pages of alarm definitions exist:

- To select another page, select the appropriate navigation button at the bottom of the **Alarm Message Definitions** window.

- To change the number of alarms that display in the window, select a different value from the **Rows per Page** drop-down list.

Step 5 Select the alarm definition for which you want alarm details.

Step 6 Enter text in the **User Defined Text** field if you want to add information to the alarm, and then select **Save**.

Tip If you add text in the **User Defined Text** field, you can select **Clear All** at any time to delete the information that you entered.

Step 7 Select **Save**.

Step 8 Select **Back to Find/List Alarms** from the Related Links drop-down list if you want to return to the **Alarm Message Definitions** window.

Step 9 Select **Go**.

System Alarm Catalog Descriptions

The following table contains the System Alarm Catalog alarm descriptions. The System Alarm Catalog supports Unified Communications Manager and Cisco Unity Connection.

Table 8: System Catalogs

Name	Description
ClusterManagerAlarmCatalog	All cluster manager alarm definitions that are related to the establishmen associations between servers in a cluster.
DBAlarmCatalog	All Cisco database alarm definitions
DRFAlarmCatalog	All Disaster Recovery System alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Java Applications alarm definitions. **Tip** You cannot configure JavaApplications alarms by using the configuration GUI. For Unified Communications Manager Unity Connection, you generally configure these alarms to g Logs; for Unified Communications Manager, you can confi alarms to generate SNMP traps to integrate with CiscoWork Management Solution. Use the registry editor that is provid operating system to view or change alarm definitions and p
EMAlarmCatalog	Alarms for Extension Mobility
LoginAlarmCatalog	All login-related alarm definitions
LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All Cisco Unified Real-Time Monitoring Tool alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess p thread statistic counters together with all the process statistic counters.

Name	Description
ServiceManagerAlarmCatalogs	All service manager alarm definitions that are related to the activation, deac starting, restarting, and stopping of services.
TFTPAlarmCatalog	All Cisco TFTP alarm definitions
TVSAlarmCatalog	Alarms for Trust Verification Service
TestAlarmCatalog	All alarm definitions that are used for sending test alarms through SNMP tr the command line interface (CLI). For information on the CLI, refer to the *Line Interface Reference Guide for Cisco Unified Solutions*. **Tip** Cisco Unity Connection SNMP does not support traps in either Communications Manager and Cisco Unity Connection system
CertMonitorAlarmCatalog	All certificate expiration definitions.
CTLproviderAlarmCatalog	Alarms for Certificate Trust List (CTL) Provider service
CDPAlarmCatalog	Alarms for Cisco Discovery Protocol (CDP) service
IMSAlarmCatalog	All user authentication and credential definitions.
SLMAlarmCatalog	Alarms for Cisco Smart Licensing

CallManager Alarm Catalog Descriptions

The information in this section does not apply to Cisco Unity Connection.

The following table contains the CallManager Alarm Catalog descriptions.

Table 9: CallManager Alarm Catalog

Name	Description
CallManager	All Cisco CallManager service alarm definitions
CDRRepAlarmCatalog	All CDRRep alarm definitions
CARAlarmCatalog	All CDR analysis and reporting alarm definitions
CEFAlarmCatalog	All Cisco Extended Functions alarm definitions
CMIAlarmCatalog	All Cisco messaging interface alarm definitions
CtiManagerAlarmCatalog	All Cisco computer telephony integration (CTI) manager alarm definitions
IpVmsAlarmCatalog	All IP voice media streaming applications alarm definitions
TCDSRVAlarmCatalog	All Cisco telephony call dispatcher service alarm definitions
Phone	Alarms for phone-related tasks, such as downloads
CAPFAlarmCatalog	Alarms for Certificate Authority Proxy Function (CAPF) service

Name	Description
SAMLSSOAlarmCatalog	Alarms for SAML Single Sign On feature.

IM and Presence Alarm Catalog Descriptions

The following table contains the IM and Presence Service Alarm Catalog description.

Table 10: IM and Presence Service Alarm Catalog

Name	Description
CiscoUPSConfigAgent	All Config Agent alarms that notify the IM and Presence Service SIP Proxy of configuration changes in the IM and Presence Service IDS database.
CiscoUPInterclusterSyncAgent	All Intercluster Sync Agent alarms that synchronize end user information between IM and Presence Service clusters for intercluster routing.
CiscoUPSPresenceEngine	All Presence Engine alarms that collect information regarding the availability status and communications capabilities of a user.
CiscoUPSSIPProxy	All SIP Proxy alarms that are related to routing, requestor identification, and transport interconnection.
CiscoUPSSOAP	All simple object access protocol (SOAP) alarms that provide a secure SOAP interface to and from external clients using HTTPS.
CiscoUPSSyncAgent	All Sync Agent alarms that keep the IM and Presence Service data synchronized with Unified Communications Manager data.
CiscoUPXCP	All XCP alarms that collect information on the status of XCP components and services on IM and Presence Service.
CiscoUPServerRecoveryManager	All server recovery manager alarms that relate to the failover and fallback process between nodes in a presence redundancy group.
CiscoUPReplWatcher	All ReplWatcher alarms that monitor IDS Replication State.
CiscoUPXCPConfigManager	All Cisco XCP Config Manager alarm definitions that relate to XCP components.

Alarm information, which includes an explanation and recommended action, also includes the application name, server name, and other information, to help you perform troubleshooting, even for problems that are not on your local IM and Presence Service node.

For more information about the alarms that are specific to the IM and Presence Service, see *System Error Messages for IM and Presence on Cisco Unified Communications Manager*.

Default Alarms in CiscoSyslog File

The following table contains the description of the default alarms that are triggered in the CiscoSyslog file without any alarm configurations:

Table 11: Default Alarms in CiscoSyslog File

Name	Description
CLM_IPSecCertUpdated	The IPSec self-signed cert from a peer node in the cluster has been imported due to a change.
CLM_IPAddressChange	The IP address of a peer node in the cluster has changed.
CLM_PeerState	The ClusterMgr session state with another node in the cluster has changed to the current state.
CLM_MsgIntChkError	ClusterMgr has received a message which has failed a message integrity check. This can be an indication that another node in the cluster is configured with the wrong security password.
CLM_UnrecognizedHost	ClusterMgr has received a message from an IP address which is not configured as a node in this cluster.
CLM_ConnectivityTest	Cluster Manager detected a network error.
ServiceActivated	This service is now activated.
ServiceDeactivated	This service is now deactivated.
ServiceActivationFailed	Failed to activate this service.
ServiceDeactivationFailed	Failed to deactivate this service.
ServiceFailed	The Service has terminated abruptly. Service Manager will try to restart it.
ServiceStartFailed	Failed to start this service. Service Manager will attempt to start the service again.
ServiceStopFailed	Unable to stop the specified service after serveral retries. The service will be marked stopped.
ServiceRestartFailed	Unable to restart the specified service.
ServiceExceededMaxRestarts	Service failed to start, even after the max restarts attempts.

Name	Description
FailedToReadConfig	Failed to read configuration file. Configuration file might be corrupted.
MemAllocFailed	Failure to allocate memory.
SystemResourceError	System call failed.
ServiceManagerUnexpectedShutdown	Service Manager restarted successfully after an unexpected termination.
OutOfMemory	The process has requested memory from the operating system, and there was not enough memory available.
CREATE-DST-RULE-FILE-CLI	New DST rules file is generated from cli. Phones need to be restarted.Not restarting the phones would result in wrong DST start / stop dates.
CREATE-DST-RULE-FILE-BOOTUP	New DST rules file is generated during bootup. Phones need to be restarted.Not restarting the phones would result in wrong DST start / stop dates.
CREATE-DST-RULE-FILE-CRON	New DST rules file is generated from cron. Phones need to be restarted.Not restarting the phones would result in wrong DST start / stop dates.
PermissionDenied	An operation could not be completed because the process did not have authority to perform it.
ServiceNotInstalled	An executable is trying to start but cannot because it is not configured as a service in the service control manager. The service name is %s.
ServiceStopped	A service has stopped.
ServiceStarted	A service has started.
ServiceStartupFailed	A service has started.
FileWriteError	Failed to write into the primary file path.

CHAPTER 11

Audit Logs

Audit Logs

With audit logging, configuration changes to the system get logged in separate log files for auditing.

Audit Logging (Standard)

When audit logging is enabled, but the detailed audit logging option is not selected, the system is configured for standard audit logging.

With standard audit logging, configuration changes to the system get logged in separate log files for auditing. The Cisco Audit Event Service, which displays under Control Center - Network Services in the serviceability GUI, monitors and logs any configuration changes to the system that are made by a user or as a result of the user action.

You access the **Audit Log Configuration** window in the serviceability GUI to configure the settings for the audit logs.

Standard audit logging contains the following parts:

- Audit logging framework - The framework comprises an API that uses an alarm library to write audit events into audit logs. An alarm catalog that is defined as GenericAlarmCatalog.xml applies for these alarms. Different system components provide their own logging.

  The following example displays an API that a Unified Communications Manager component can use to send an alarm:

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207
Severity: 3
EventType: ServiceStatusUpdated
ResourceAccessed: CCMService
EventStatus: Successful
Description: CallManager Service status is stopped
```

- Audit event logging - An audit event represents any event that is required to be logged. The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

Tip Be aware that audit event logging is centralized and enabled by default. An alarm monitor called Syslog Audit writes the logs. By default, the logs are configured to rotate. If the AuditLogAlarmMonitor cannot write an audit event, the AuditLogAlarmMonitor logs this failure as a critical error in the syslog file. The Alert Manager reports this error as part of a SeverityMatchFound alert. The actual operation continues even if the event logging fails. All audit logs get collected, viewed, and deleted from Trace and Log Central in the Cisco Unified Real-Time Monitoring Tool.

Cisco Unified Serviceability Standard Events Logging

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR management. (Cisco Unified Communications Manager only)
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node. (Unified Communications Manager only)

Cisco Unified Real-Time Monitoring Tool Standard Events Loggin

Cisco Unified Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration
- Alert suspension
- E-mail configuration
- Set node alert status
- Alert addition
- Add alert action
- Clear alert
- Enable alert
- Remove alert action
- Remove alert

Unified Communications Manager Standard Events Logging

Cisco CDR Analysis and Reporting (CAR) creates audit logs for these events:

- Loader scheduling
- Daily, weekly, and monthly reports scheduling
- Mail parameters configuration
- Dial plan configuration
- Gateway configuration
- System preferences configuration
- Autopurge configuration
- Rating engine configurations for duration, time of day, and voice quality
- QoS configurations
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configuration

Cisco Unified CM Administration Standard Events Logging

The following events get logged for various components of Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and Unified Communications Manager server additions or deletions)

Cisco Unified Communications Self Care Portal Standard Events Logging

User logging (user login and user logout) events are logged for Cisco Unified Communications Self Care Portal.

Command-Line Interface Standard Events Logging

All commands issued via the command-line interface are logged (for both Unified Communications Manager and Cisco Unity Connection).

Cisco Unity Connection Administration Standard Events Logging

Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts)

- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony
- Task management (enabling or disabling a task)
- Bulk Administration Tool (bulk creates, bulk deletes)
- Custom Keypad Map (map updates)

Cisco Personal Communications Assistant (Cisco PCA) Standard Events Logging

The Cisco Personal Communications Assistant client logs the following events:

- User logging (user logins and user logouts)
- All configuration changes made via the Messaging Assistant

Cisco Unity Connection Serviceability Standard Events Logging

Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

Cisco Unity Connection Clients that Use the Representational State Transfer APIs Events Logging

Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface.

Cisco Unified IM and Presence Serviceability Standard Events Logging

Cisco Unified IM and Presence Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service
- Changes in trace configurations and alarm configurations
- Changes in SNMP configurations
- Review of any report in the Serviceability Reports Archive (this log gets viewed on the reporter node)

Cisco Unified IM and Presence Real-Time Monitoring Tool Standard Events Logging

Cisco Unified IM and Presence Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration
- Alert suspension

- E-mail configuration
- Set node alert status
- Alert addition
- Add alert action
- Clear alert
- Enable alert
- Remove alert action
- Remove alert

Cisco IM and Presence Administration Standard Events Logging

The following events get logged for various components of Cisco Unified Communications Manager IM and Presence Administration:

- Administrator logging (logins and logouts on IM and Presence interfaces such as Administration, OS Administration, Disaster Recovery System, and Reporting)
- User role membership updates (user added, user deleted, user role updated)
- Role updates (new roles added, deleted, or updated)
- Device updates (phones and gateways)
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, hostnames, Ethernet settings, and IM and Presence server additions or deletions)

IM and Presence Application Standard Events Logging

The following events get logged by the various components of the IM and Presence Application:

- End user logging on IM clients (user logins, user logouts, and failed login attempts)
- User entry to and exit from IM Chat Rooms
- Creation and destruction of IM Chat Rooms

Command Line Interface Standard Events Logging

All commands issued through the command line interface are logged.

Audit Logging (Detailed)

Detailed audit logging is an optional feature that logs additional configuration modifications that are not stored in standard (default) audit logs. In addition to all of the information that is stored in standard audit logs, detailed audit logging also includes configuration items that were added, updated, and deleted, including the modified values. Detailed audit logging is disabled by default, but you can enable it in the **Audit Log Configuration** window.

Audit Log Types

System Audit Logs

System audit logs track activities such as the creation, modification, or deletion of Linux OS users, log tampering, and any changes to file or directory permissions. This type of audit log is disabled by default due to the high volume of data gathered. To enable this function, you must manually enable utils auditd using the CLI. After you have enabled the system audit log feature, you can collect, view, download, or delete selected logs through Trace & Log Central from the Real-Time Monitoring Tool. System audit logs take on the format of `vos-audit.log`.

For information about how to enable this feature, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. For information about how to access collected logs from the Real-Time Monitoring Tool, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* .

Application Audit Logs

The Application Audit logs monitor and record any configuration changes to the system that were made by a user or as a result of the user action.

Note The Application Audit Logs (Linux auditd) can be enabled or disabled only through the CLI. Other than the collection of vos-audit.log through the Real-Time Monitoring Tool, you can not change any settings for this type of audit log.

Database Audit Logs

Database Audit Logs track all activities associated with access to the Informix Database, such as logins.

Audit Log Configuration Task Flow

Complete the following tasks to configure audit logging.

Procedure

	Command or Action	Purpose
Step 1	Set up Audit Logging, on page 117	Set up your audit log configuration in the Audit Log Configuration window. You can configure whether you want to use remote audit logging and whether you want the Detailed Audit Logging option.
Step 2	Configure Remote Audit Log Transfer Protocol, on page 118	Optional. If you have remote audit logging configured, configure the transfer protocol. The system default in normal operating mode is UDP, but you can also configure TCP or TLS
Step 3	Configure Email Server for Alert Notifications, on page 118	Optional. In RTMT, set up the email server for email alerts.

	Command or Action	Purpose
Step 4	Enable Email Alerts, on page 118	Optional. Set up one of the following email alerts: • If you have remote audit logging configured with TCP, set up the email notification for the **TCPRemoteSyslogDeliveryFailed** alert. • If you have remote audit logging configured with TLS, set up the email notification for the **TLSRemoteSyslogDeliveryFailed** alert.
Step 5	Configure Remote Audit Logging for Platform Logs, on page 119	Set up remote audit logging for platform audit logs and remote server logs. For these types of audit logs, you must configure a FileBeat client and external logstash server.

Set up Audit Logging

Before you begin

For remote audit logging, you must have already set up your remote syslog server and configured IPSec between each cluster node and the remote syslog server, including connections to any gateways in between. For IPSec configuration, see the *Cisco IOS Security Configuration Guide*.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Tools** > **Audit Log Configuration**.

Step 2 From the **Server** drop-down menu, select any server in the cluster and click **Go**.

Step 3 To log all cluster nodes, check the **Apply to All Nodes** check box.

Step 4 In the **Server Name** field, enter the IP Address or fully qualified domain name of the remote syslog server.

Step 5 Optional. To log configuration updates, including items that were modified, and the modified values, check the **Detailed Audit Logging** check box.

Step 6 Complete the remaining fields in the **Audit Log Configuration** window. For help with the fields and their descriptions, see the online help.

Step 7 Click **Save**.

What to do next

Configure Remote Audit Log Transfer Protocol, on page 118

Configure Remote Audit Log Transfer Protocol

Use this procedure to change the transfer protocol for remote audit logs. The system default is UDP, but you can reconfigure to TCP or TLS.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils remotesyslog show protocol** command to confirm which protocol is configured.

Step 3 If you need to change the protocol on this node, do the following:

- To configure TCP, run the **utils remotesyslog set protocol tcp** command.
- To configure UDP, run the **utils remotesyslog set protocol udp** command.
- To configure TLS, run the **utils remotesyslog set protocol tls** command.

Note In Common Criteria Mode, strict host name verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

Step 4 If you changed the protocol, restart the node.

Step 5 Repeat this procedure for all Unified Communications Manager and IM and Presence Service cluster nodes.

What to do next

Configure Email Server for Alert Notifications, on page 118

Configure Email Server for Alert Notifications

Use this procedure to set up your email server for alert notifications.

Procedure

Step 1 In the Real-Time Monitoring Tool's System window, click **Alert Central**.

Step 2 Choose **System** > **Tools** > **Alert** > **Config Email Server**.

Step 3 In the **Mail Server Configuration** popup, enter the details for the mail server.

Step 4 Click **OK**.

What to do next

Enable Email Alerts, on page 118

Enable Email Alerts

If you have remote audit logging with TCP or TLS configured, use this procedure to set up an email alert to notify you of transmission failures.

Procedure

Step 1 In the Real-Time Monitoring Tool **System** area, click **Alert Central**.

Step 2 In the **Alert Central** window,

- If you have remote audit logging with TCP, select **TCPRemoteSyslogDeliveryFailed**
- If you have remote audit logging with TLS, select **TLSRemoteSyslogDeliveryFailed**

Step 3 Choose **System** > **Tools** > **Alert** > **Config Alert Action**.

Step 4 In the **Alert Action** popup, select **Default** and click **Edit**.

Step 5 In the **Alert Action** popup, **Add** a recipient.

Step 6 In the popup window, enter the address where you want to send email alerts and click **OK**.

Step 7 In the **Alert Action** popup, make sure that the address appears under **Recipients** and that the **Enable** check box is checked.

Step 8 Click **OK**.

Configure Remote Audit Logging for Platform Logs

Complete these tasks to add remote audit logging support for platform audit logs, remote support logs, and Bulk Administration csv files. For these types of logs, the FileBeat client and logstash server get used.

Before you begin

Make sure that you have set up an external logstash server.

Procedure

	Command or Action	Purpose
Step 1	Configure Logstash Server Information, on page 119	Configure the FileBeat client with the external logstash server details, such as IP addresses, ports and file types.
Step 2	Configure the FileBeat Client, on page 120	Enable the FileBeat client for remote audit logging.

Configure Logstash Server Information

Use this procedure to configure the FileBeat client with the external logstash server information, such as IP address, port number, and downloadable file types.

Before you begin

Make sure that you have set up your external logstash server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat configure** command.

Step 3 Follow the prompts to configure the logstash server details.

Configure the FileBeat Client

Use this procedure to enable or disable the FileBeat client for uploads of platform audit logs, remote support logs, and Bulk Administration csv files.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils FileBeat status** command to confirm whether the FileBeat client is enabled.

Step 3 Run one of the following commands:

- To enable the client, run the **utils FileBeat enable** command.
- To disable the client, run the **utils FileBeat disable** command.

Note TCP is the default transfer protocol.

Step 4 Optional. If you want to use TLS as the transfer protocol, do the following:

- To enable TLS as the transfer protocol, run the **utils FileBeat tls enable** command.
- To disable TLS as the transfer protocol, run the **utils FileBeat tls disable** command.

Note To use TLS, a security certificate has to be uploaded from logstash server to the tomcat trust store on Unified Communications Manager and IM and Presence service.

Step 5 Repeat this procedure on each node.

Do not run any of these commands on all nodes simultaneously.

Audit Log Configuration Settings

Before You Begin

Be aware that only a user with an audit role can change the audit log settings. By default, for Unified Communications Manager, the CCMAdministrator possesses the audit role after fresh installs and upgrades. The CCMAdministrator can assign any user that has auditing privileges to the Standard Audit Users group in the User Group Configuration window in Cisco Unified Communications Manager Administration. If you want to do so, you can then remove CCMAdministrator from the Standard Audit Users group.

For IM and Presence Service, the administrator possesses the audit role after fresh installs and upgrades, and can assign any user that has auditing privileges to the Standard Audit Users group.

For Cisco Unity Connection, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role. You can also remove the Audit Administrator role from this account.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified Real-Time Monitoring Tool, IM and Presence Real-Time Monitoring Tool, Trace Collection Tool, Real-Time Monitoring Tool (RTMT) Alert Configuration, Control Center - Network Services in the serviceability user interface, RTMT Profile Saving, Audit Configuration in the serviceability user interface, and a resource that is called Audit Traces.

The Standard Audit Log Configuration role is to provide the ability to delete audit logs and to read/update access to Cisco Unified RTMT, Trace Collection Tool, RTMT Alert Configuration, Control Center - Network Services in Cisco Unified Serviceability, RTMT Profile Saving, Audit Configuration in Cisco Unified Serviceability, and a resource that is called Audit Traces.

The Audit Administrator role in Cisco Unity Connection provides the ability to view, download and delete audit logs in Cisco Unified RTMT.

For information on roles, users, and user groups in Unified Communications Manager, refer to the *Administration Guide for Cisco Unified Communications Manager*.

For information on roles and users in Cisco Unity Connection, refer to the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

For information on roles, users, and user groups in IM and Presence, refer to *Configuration and Administration of IM and Presence Service on Unified Communications Manager*.

The following table describes the settings that you can configure in the Audit Log Configuration window in Cisco Unified Serviceability.

Table 12: Audit Log Configuration Settings

Field	Description
Select Server	
Server	Choose the server (node) where you want to configure audit logs; then, click **Go**.
Apply to All Nodes	If you want to apply the audit log configuration to all nodes in the cluster, check the **Apply to all Nodes** check box.
Application Audit Log Settings	

Field	Description
Enable Audit Log	When you check this check box, an audit log gets created for the application audit log. For Unified Communications Manager, the application audit log supports configuration updates for Unified Communications Manager user interfaces, such as Cisco Unified Communications Manager Administration, Cisco Unified RTMT, Cisco Unified Communications Manager CDR Analysis and Reporting, and Cisco Unified Serviceability. For IM and Presence Service, the application audit log supports configuration updates for IM and Presence user interfaces, such as Cisco Unified Communications Manager IM and Presence Administration, Cisco Unified IM and Presence Real-Time Monitoring Tool, and Cisco Unified IM and Presence Serviceability. For Cisco Unity Connection, the application audit log supports configuration updates for Cisco Unity Connection user interfaces, including Cisco Unity Connection Administration, Cisco Unity Connection Serviceability, Cisco Personal Communications Assistant, and clients that use the Connection REST APIs. This setting displays as enabled by default. **Note** The Network Service Audit Event Service must be running.
Enable Purging	The Log Partition Monitor (LPM) looks at the Enable Purging option to determine whether it needs to purge audit logs. When you check this check box, LPM purges all the audit log files in RTMT whenever the common partition disk usage goes above the high water mark; however, you can disable purging by unchecking the check box. If purging is disabled, the number of audit logs continues to increase until the disk is full. This action could cause a disruption of the system. A message that describes the risk of disabling the purge displays when you uncheck the Enable Purging check box. Be aware that this option is available for audit logs in an active partition. If the audit logs reside in an inactive partition, the audit logs get purged when the disk usage goes above the high water mark. You can access the audit logs by choosing **Trace and Log Central** > **Audit Logs** in RTMT. **Note** The Network Service Cisco Log Partitions Monitoring tool must be running.
Enable Log Rotation	The system reads this option to determine whether it needs to rotate the audit log files or it needs to continue to create new files. The maximum number of files cannot exceed 5000. When the Enable Rotation check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files is reached. **Tip** When log rotation is disabled (unchecked), audit log ignores the Maximum No. of Files setting.

Field	Description
Detailed Audit Logging	When this check box is checked, the system is enabled for detailed audit logs. Detailed audit logs provide the same items as regular audit logs, but also include configuration changes. For example, the audit log includes items that were added, updated, and deleted, including the modified values.
Server Name	Enter the name or IP address of the remote syslog server that you want to use to accept syslog messages. If server name is not specified, Cisco Unified IM and Presence Serviceability does not send the syslog messages. Do not specify a Unified Communications Manager node as the destination because the Unified Communications Manager node does not accept syslog messages from another server. This applies to IM and Presence Service only.
Remote Syslog Audit Event Level	Select the desired syslog messages severity for the remote syslog server. All the syslog messages with selected or higher severity level are sent to the remote syslog. This applies to IM and Presence Service only.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting specifies 250. The maximum number specifies 5000.
Maximum File Size	Enter the maximum file size for the audit log. The file size value must remain between 1MB and 10MB. You must specify a number between 1 and 10.
Warning Threshold for Approaching Log Rotation Overwrite (%)	The system can alert you when the audit logs are approaching the level where they will be overwritten. Use this field to set the threshold at which the system sends you an alert. For example, if you use the default settings of 250 files of 2 MB and a warning threshold of 80%, the system sends you an alarm when 200 files (80%) of audit logs have accumulated. If you want to keep the audit history, you can use RTMT to retrieve the logs before the system overwrites them. RTMT provides an option to delete the files after you collect them. Enter a value between 1 and 99%. The default is 80%. When you set this field, you must also check the **Enable Log Rotation** option. **Note** The total disk space allocated to audit logs is the Maximum No. of Files multiplied by the Maximum File Size. If the size of audit logs on the disk exceeds this percentage of total disk space allocated, the system raises an alarm in Alert Central.
Database Audit Log Filter Settings	
Enable Audit Log	When you check this check box, an audit log gets created for the Unified Communications Manager and Cisco Unity Connection databases. Use this setting in conjunction with the Debug Audit Level setting, which allows you create a log for certain aspects of the database.

Field	Description
Debug Audit Level	This setting allows you to choose which aspects of the database you want to audit in the log. From the drop-down list box, choose one of the following options. Be aware that each audit log filter level is cumulative. • **Schema** - Tracks changes to the setup of the audit log database (for example, the columns and rows in the database tables). • **Administrative Tasks** - Tracks all administrative changes to the Unified Communications Manager system (for example, any changes to maintain the system) plus all **Schema** changes. **Tip** Most administrators will leave the Administrative Tasks setting disabled. For users who want auditing, use the Database Updates level. • **Database Updates** - Tracks all changes to the database plus all **schema** changes and all **administrative tasks** changes. • **Database Reads** - Tracks every read to the system, plus all schema changes, administrative tasks changes, and database updates changes. **Tip** Choose the Database Reads level only when you want to get a quick look at the Unified Communications Manager, IM and Presence Service, or Cisco Unity Connection system. This level uses significant amounts of system resources and should be used only for a short time.
Enable Audit Log Rotation	The system reads this option to determine whether it needs to rotate the database audit log files or it needs to continue to create new files. When the Audit Enable Rotation option check box is checked, the system begins to overwrite the oldest audit log files after the maximum number of files gets reached. When this setting check box is unchecked, audit log ignores the Maximum No. of Files setting.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. Ensure that the value that you enter for the Maximum No. of Files setting is greater than the value that you enter for the No. of Files Deleted on Log Rotation setting. You can enter a number from 4 (minimum) to 40 (maximum).
No. of Files Deleted on Log Rotation	Enter the maximum number of files that the system can delete when database audit log rotation occurs. The minimum that you can enter in this field is 1. The maximum value is 2 numbers less than the value that you enter for the Max No. of Files setting; for example, if you enter 40 in the Maximum No. of Files field, the highest number that you can enter in the No. of Files Deleted on Log Rotation field is 38.
Set to Default	The **Set to Default** button specifies the default values. It is recommended to set the audit logs to default mode unless it is required to be set to a different level for detailed troubleshooting. The **Set to Default** option minimizes the disk space utilized by log files.

⚠ **Caution** When enabled, database logging can generate large amounts of data in a short period, particularly if the debug audit level is set to **Database Updates** or **Database Reads**. This can result in a significant performance impact during heavy usage periods. In general, we recommend that you keep database logging disabled. If you do need to enable logging to track changes in the database, we recommend that you do so only for short periods of time, by using the **Database Updates** level. Similarly, administrative logging does impact on the overall performance of the web user interface, especially when polling database entries (for example, pulling up 250 devices from the database).

CHAPTER 12

Call Home

Call Home

This chapter provides an overview of the Unified Communications Manager Call Home service and describes how to configure the Unified Communications Manager Call Home feature. The Call Home feature allows to communicate and send the diagnostic alerts, inventory, and other messages to the Smart Call Home back-end server.

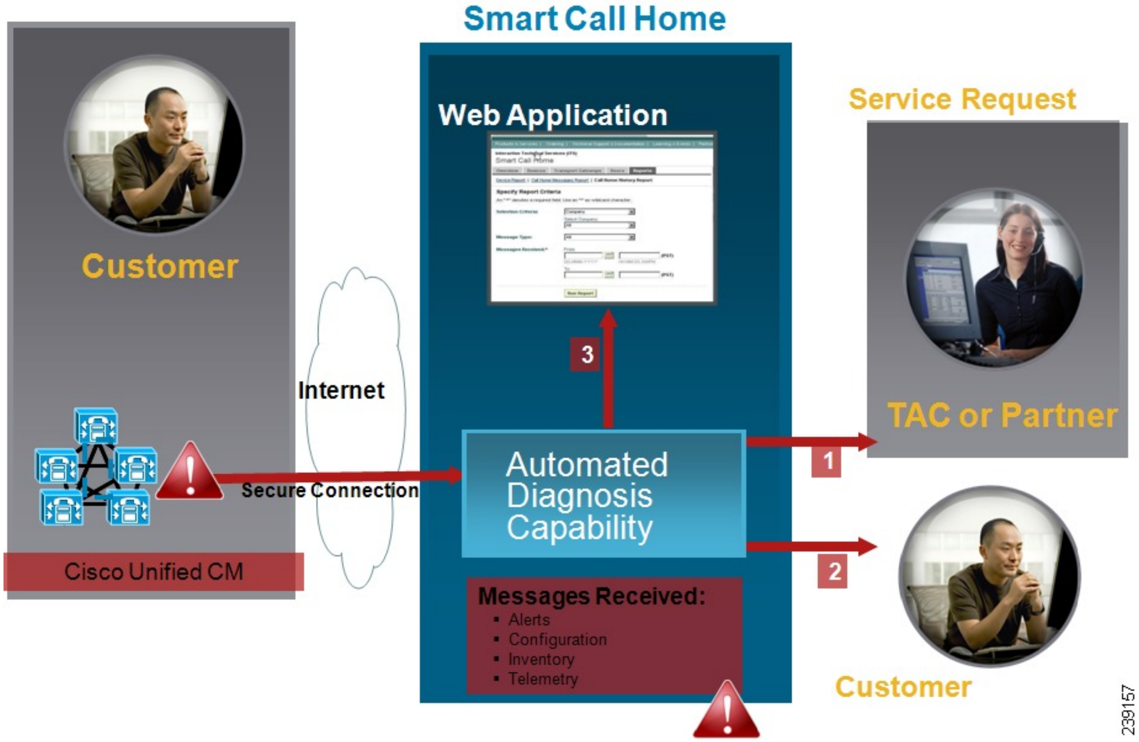
Smart Call Home

Smart Call Home provides proactive diagnostics, real-time alerts, and remediation on a range of Cisco devices for higher network availability and increased operational efficiency. It accomplishes the same by receiving and analyzing the diagnostic alerts, inventory, and other messages from Smart Call Home enabled Unified Communications Manager. This particular capability of Unified Communications Manager is called as Unified Communications Manager Call Home.

Smart Call Home offers:

- Higher network availability through proactive, fast issue resolution by:
  - Identifying issues quickly with continuous monitoring, real-time, proactive alerts, and detailed diagnostics.
  - Making you aware of potential problems by providing alerts that are specific to only those types of devices in the network. Resolving critical problems faster with direct, automatic access to experts at Cisco Technical Assistance Center (TAC).
- Increased operational efficiency by providing customers the ability to:
  - Use staff resources more efficiently by reducing troubleshooting time.
- Fast, web-based access to needed information that provides customers the ability to:
  - Review all Call Home messages, diagnostics, and recommendations in one place.
  - Check Service Request status quickly.
  - View the most up-to-date inventory and configuration information for all Call Home devices.

Figure 2: Cisco Smart Call Home Overview



Smart Call Home contains modules that perform the following tasks:

- Notify Customer of Call Home messages.
- Provide impact analysis and remediation steps.

For more information about Smart Call Home, see the Smart Call Home page at this location:

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Information for Smart Call Home Certificates Renewal

From Cisco Release 10.5(2) onwards, administrators have to manually upload the new certificates for any renewal request to continue support for Smart Call Home feature. You can upload certificates through Cisco Unified Operating System Administration web GUI. Go to **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**. Choose **tomcat-trust** as the Certificate Purpose, and upload the certificate from the saved destination.

The following certificate with extension .PEM should be uploaded to tomcat-trust.

Note Ensure that the administrator copy the entire string and include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----, paste it into a text file, and save it with the extension .PEM.

-----BEGIN CERTIFICATE-----

MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x

```
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----
```

Anonymous Call Home

The Anonymous Call Home feature is a sub-feature of the Smart Call Home feature that allows Cisco to anonymously receive inventory and telemetry messages. Enable this feature to keep your identification anonymous.

The following are the characteristics of Anonymous Call Home:

- The Unified Communications Manager sends only inventory and telemetry messages and not diagnostic and configuration information to Smart Call Home back-end.
- It will not send any user related information (for example, registered devices and upgrade history).
- Anonymous call home option does not require registration or entitlement for Smart Call Home feature with Cisco.
- The inventory and telemetry messages are sent periodically (first day of every month) to the Call Home back-end.
- **Include Trace logs and Diagnostic Information** option is disabled if Cisco Unified Communications Manager is configured to use Anonymous Call Home.

Inventory messages contains information about the cluster, nodes, and license.

The following table lists the inventory messages for Smart Call Home and Anonymous Call Home.

Table 13: Inventory Messages for Smart Call Home and Anonymous Call Home

Inventory messages	Smart Call Home	Anonymous Call Home
Contact Email	Applicable	Not Applicable
Contact Phone number	Applicable	Not Applicable
Street Address	Applicable	Not Applicable
Server Name	Applicable	Not Applicable
Server IP Address	Applicable	Not Applicable
Licence Server	Applicable	Not Applicable
OS Version	Applicable	Applicable
Model	Applicable	Applicable
Serial Number	Applicable	Applicable
CPU Speed	Applicable	Applicable
RAM	Applicable	Applicable
Storage Partition	Applicable	Applicable
Firmware version	Applicable	Applicable
BIOS Version	Applicable	Applicable

Inventory messages	Smart Call Home	Anonymous Call Home
BIOS Information	Applicable	Applicable
Raid Configuration	Applicable	Applicable
Active Services	Applicable	Applicable
Publisher Name	Applicable	Not Applicable
Publisher IP	Applicable	Not Applicable
Product ID	Applicable	Applicable
Active Version	Applicable	Applicable
Inactive Version	Applicable	Applicable
Product Short name	Applicable	Applicable

Telemetry messages contain information about the number of devices (IP phones, gateways, conference bridge, and so on) for each device type that is available on a Unified Communications Manager cluster. The telemetry data contains the device count for the entire cluster.

The following table lists the telemetry messages for Smart Call Home and Anonymous Call Home.

Table 14: Telemetry Messages for Smart Call Home and Anonymous Call Home

Telemetry messages	Smart Call Home	Anonymous Call Home
Contact Email	Applicable	Not Applicable
Contact Phone number	Applicable	Not Applicable
Street Address	Applicable	Not Applicable
Server name	Applicable	Not Applicable
CM User Count	Applicable	Not Applicable
Serial Number	Applicable	Applicable
Publisher name	Applicable	Not Applicable
Device count and Model	Applicable	Applicable
Phone User Count	Applicable	Applicable
CM Call Activity	Applicable	Applicable
Registered Device count	Applicable	Not Applicable
Upgrade history	Applicable	Not Applicable

Telemetry messages	Smart Call Home	Anonymous Call Home
System Status	Applicable for Host name, Date, Locale, Product Version, OS Version, Licence MAC, Up Time, MP Stat, Memory Used, Disk Usage, Active and Inactive partition used, and DNS	Applicable for Date, Locale, Product Version, OS Version, Licence MAC, Up Time, Memory Used, Disk Usage, and Active and Inactive partition used

Configuration messages contain information about the row count for each database table that is related to a configuration. The configuration data consists of table name and row count for each table across the cluster.

Smart Call Home Interaction

If you have a service contract directly with Cisco Systems, you can register Unified Communications Manager for the Cisco Smart Call Home service. Smart Call Home provides fast resolution of system problems by analyzing Call Home messages that are sent from Unified Communications Manager and providing background information and recommendations.

The Unified Communications Manager Call Home feature delivers the following messages to the Smart Call Home back-end server:

- Alerts - Contain alert information for various conditions related to environment, hardware failure, and system performance. The alerts may be generated from any node within the Unified Communications Manager cluster. The alert details contain the node and other information required for troubleshooting purposes, depending on the alert type. See topics related to Smart call home interaction for alerts that are sent to the Smart Call Home back-end server.

The following are the alerts for Smart Call Home.

By default, Smart Call Home processes the alerts once in 24 hours. Repeated occurrence of the same alert within the span of 24 hours in mixed cluster (Unified Communication Manager and Cisco Unified Presence) and is not processed by Smart Call Home.

Important The collected information is deleted from the primary AMC server after 48 years. By default, Unified Communications Manager publisher is the primary AMC server.

- **Performance Alerts**
  - CallProcessingNodeCPUPegging
  - CodeYellow
  - CPUPegging
  - LowActivePartitionAvailableDiskSpace
  - LowAvailableVirtualMemory
  - LowSwapPartitionAvailableDiskSpace
- **Database - Related Alerts**

  - DBReplicationFailure

- **Failed Calls Alerts**
  - MediaListExhausted
  - RouteListExhausted
- **Crash - Related Alerts**
  - Coredumpfilefound
  - CriticalServiceDown

The configuration, inventory, and telemetry messages are sent periodically (first day of every month) to the Call Home back-end. The information in these messages enables TAC to provide timely and proactive service to help customers manage and maintain their network.

Prerequisites for Call Home

To support the Unified Communications Manager Call Home service, you require the following:

- A Cisco.com user ID associated with a corresponding Unified Communications Manager service contract.
- It is highly recommended that both the Domain Name System (DNS) and Simple Mail Transfer Protocol (SMTP) servers are setup for the Unified Communications Manager Call Home feature.
  - DNS setup is required to send the Call Home messages using Secure Web (HTTPS).
  - SMTP setup is required to send the Call Home messages to Cisco TAC or to send a copy of the messages to a list of recipients through email.

Access Call Home

To access Unified Communications Manager Call Home, go to Cisco Unified Serviceability Administration and choose **CallHome** (**Cisco Unified Serviceability** > **CallHome** > **Call Home Configuration**).

Call Home Settings

The following table lists the default Unified Communications Manager Call Home settings.

Table 15: Default Call Home Settings

Parameter	**Default**
Call Home	Enabled
Send Data to Cisco Technical Assistance Center (TAC) using	Secure Web (HTTPS)

If default Smart Call Home configuration is changed during installation, then the same settings reflect in the Call Home user interface.

Note You must need to have a SMTP setup if you choose **Email** as the transport method and SMTP setup is not a required for **Secure Web (HTTPS)** option.

Call Home Configuration

In Cisco Unified Serviceability, choose **Call Home** > **Call Home Configuration**.

The Call Home Configuration window appears.

Note You can also configure the Cisco Smart Call Home while installing the Unified Communications Manager.

The Smart Call Home feature is enabled if you configure Smart Call Home option during installation. If you select **None**, a reminder message is displayed, when you log in to Cisco Unified Communications Manager Administration. Instructions to configure Smart Call Home or disable the reminder using Cisco Unified Serviceability is provided.

The following table describes the settings to configure the Unified Communications Manager Call Home.

Table 16: Unified Communications Manager Call Home Configuration Settings

Field Name	Description
Call Home Message Schedule	Displays the date and time of the last Call Home messages that were sent and the next message that is scheduled.

Field Name	Description
Call Home*	From the drop-down list, select one of the following options: • **None**: Select this option if you want to enable or disable the Call Home. A reminder message appears `Smart Call Home is not configured. To configure Smart Call Home or disable the reminder, please go to Cisco Unified Serviceability > Call Home or click here` on the administrator page. • **Disabled**: Select this option if you want to disable Call Home. • **Enabled (Smart Call Home)**: This option is enabled, if you have selected Smart Call Home during installation. When you select this option, all the fields under **Customer Contact Details** are enabled. With the same configuration, the options in **Send Data** are also enabled. • **Enabled (Anonymous Call Home)**: Select this option if you want to use Call Home in anonymous mode. When you select this option, all the fields under **Customer Contact Details** is disabled. With the same configuration, the Send a copy to the following email addresses (separate multiple addresses with comma) field in **Send Data** is enabled, and Include Trace logs and Diagnostics Information is disabled on Call Home page. **Note** If you enable Anonymous Call Home, the server sends usage statistics to Cisco systems from the server. This information helps Cisco to understand user experience about the product and to drive product direction.
Customer Contact Details	
Email Address*	Enter the contact email address of the customer. This is a mandatory field.
Company	(Optional) Enter the name of the company. You can enter up to 255 characters.
Contact Name	(Optional) Enter the contact name of the customer. You can enter up to 128 characters. The contact name can contain alphanumeric characters and some special characters like dot (.), underscore (_) and, hyphen (-).
Address	(Optional) Enter the address of the customer. You can enter up to 1024 characters.
Phone	(Optional) Enter the phone number of the customer.
Send Data	

Field Name	Description
Send Data to Cisco Technical Assistance Center (TAC) using	This is a Mandatory field. From the drop-down list, select one of the following options to send Call Home messages to Cisco TAC: • **Secure Web (HTTPS)**: Select this option if you want to send the data to Cisco TAC using secure web. • **Email**: Select this option if you want to send the data to Cisco TAC using email. For email, the SMTP server must be configured. You can see the Host name or IP address of the SMTP server that is configured. **Note** A warning message displays if you have not configured the SMTP server. • **Secure Web (HTTPS) through Proxy**: Select this option if you want to send the data to Cisco TAC through proxy. Currently, we do not support Authentication at the proxy level. The following fields appear on configuring this option: • **HTTPS Proxy IP/Hostname***: Enter the proxy IP/Hostname. • **HTTPS Proxy Port***: Enter the proxy port number to communicate.
Send a copy to the following email addresses (separate multiple addresses with comma)	Check this check box to send a copy of the Call Home messages to the specified email addresses. You can enter up to a maximum of 1024 characters.
Include Trace logs and Diagnostic Information	Check this check box to activate the Unified Communications Manager to collect logs and diagnostics information. **Note** This option is active only if the Smart Call Home is enabled. The message contains diagnostic information collected at the time of alert along with trace message. If the trace size is less than 3 MB, then the traces will be encoded and sent as part of alert message and if the traces are more than 3 MB then the path of the trace location is displayed in the alert message.
Save	Saves your Call Home configuration. **Note** After you save your Call Home Configuration, an End User License Agreement (EULA) message appears. If you are configuring for the first time, you must accept the license agreement. **Tip** To deactivate the Call Home service that you activated, select the **Disabled** option from the drop-down list and click **Save**.
Reset	Resets to last saved configuration.

Field Name	Description
Save and Call Home Now	Saves and sends the Call Home messages. **Note** A message appears **Call Home Configuration saved and all Call Home Messages sent successfully** if the messages are sent successfully.

Limitations

The following limitations apply when Unified Communications Manager or Cisco Unified Presence server is down or unreachable:

- Smart Call Home fails to capture the date and time of the last Call Home messages sent and the next message scheduled, until the server is reachable.
- Smart Call Home does not send the Call Home messages, until the server is reachable.
- Smart Call Home will be unable to capture license information in the inventory mail when the publisher is down.

The following limitations are due to Alert Manager and Collector (AMC):

- If an alert occurs on node A and the primary AMC server (by default, publisher) is restarted, and if the same alert occurs within a span of 24 hours on the same node, Smart Call Home resends the alert data from node A. Smart Call Home cannot recognize the alert that has already occurred because the primary AMC was restarted.
- If an alert occurs on node A and if you change the primary AMC server to another node, and if the same alert occurs within a span of 24 hours on the same node, Smart Call Home recognizes it as a fresh alert on node A and sends the alert data.
- The traces that are collected on the primary AMC server may reside on the primary AMC server for a maximum of 60 hours in few scenarios.

The following are the limitations in the mixed cluster (Unified Communications Manager and IM and Presence) scenario:

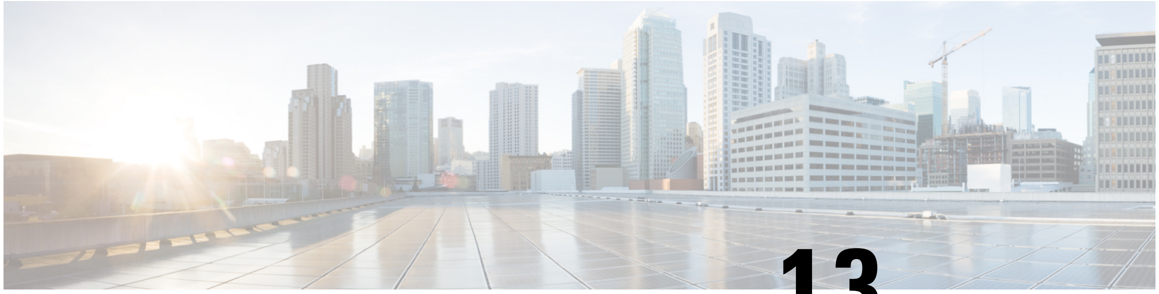
- Alerts like **CallProcessingNodeCpuPegging**, **Media List Exhausted**, **Route List Exhausted** are not applicable to IM and Presence.
- If the user changes primary AMC server to IM and Presence, then Smart Call Home cannot generate Custer Overview reports for **Media List Exhausted** and **Route List Exhausted.**
- If the user changes primary AMC server to IM and Presence, then Smart Call Home cannot generate Overview reports for **DB Replication** alert.

References for Call Home

For more information about Smart Call Home, refer the following URL:

- Smart Call Home Service Introduction

  http://www.cisco.com/en/US/products/ps7334/serv_home.html



CHAPTER 13

Serviceability Connector

Serviceability Connector Overview

You can ease the collection of logs with the Webex Serviceability service. The service automates the tasks of finding, retrieving, and storing diagnostic logs and information.

This capability uses the *Serviceability Connector* deployed on your premises. Serviceability Connector runs on a dedicated host in your network ('connector host'). You can install the connector on either of these components:

- Enterprise Compute Platform (ECP)—Recommended

  ECP uses Docker containers to isolate, secure, and manage its services. The host and the Serviceability Connector application install from the cloud. You don't need to manually upgrade them to stay current and secure.

Important We recommend use of ECP. Our future development will focus on this platform. Some new features won't be available if you install the Serviceability Connector on an Expressway.

- Cisco Expressway

You can use the Servicability Connector for these purposes:

- Automated log and system information retrieval for service requests
- Log collection of your Unified CM clusters in a Cloud-Connected UC deployment

You can use the same Serviceability Connector for both use cases.

Benefits of Using Serviceability Service

The service offers these benefits:

- Speeds up the collection of logs. TAC engineers can retrieve relevant logs as they perform the diagnosis of the problem. They can avoid the delays of requesting extra logs and waiting for their manual collection and delivery. This automation can take days off your problem resolution time.
- Works with TAC's Collaboration Solution Analyser and its database of diagnostic signatures. The system automatically analyses logs, identifies known issues, and recommends known fixes or workarounds.

Differences to Other Hybrid Services

You deploy and manage Serviceability Connectors through Control Hub like other Expressway-based Hybrid Services, such as Hybrid Calendar Service and Hybrid Call Service. But, there are important differences.

This service doesn't have features for users. The TAC is the predominant user of this service. While it can benefit organizations that use other Hybrid Services, organizations that don't use other Hybrid Services are its common users.

If you already have your organization configured in Control Hub, you can enable the service through your existing organization administrator account.

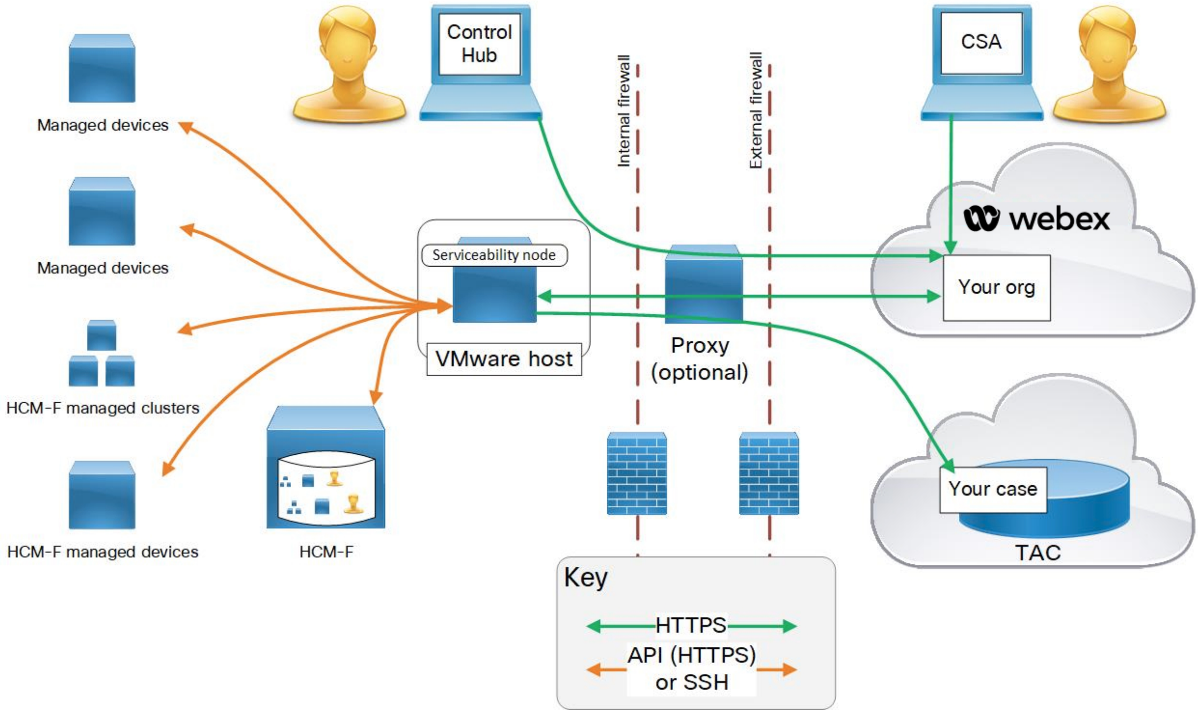
The Serviceability Connector has a different load profile from connectors that provide features directly to users. The connector is always available, so that TAC can collect data when necessary. But, it doesn't have a steady load over time. The TAC representatives manually initiate data collection. They negotiate an appropriate time for the collection to minimize the impact on other services provided by the same infrastructure.

Short Description of How it Works

1. Your administrators work with Cisco TAC to deploy Serviceability service. See Deployment Architecture for TAC Case, on page 141.
2. TAC learns of a problem with one of your Cisco devices (when you open a case).
3. TAC representative uses the Collaborations Solution Analyzer (CSA) web interface to request Serviceability Connector to collect data from relevant devices.
4. Your Serviceability Connector translates the request into API commands to collect the requested data from the managed devices.
5. Your Serviceability Connector collects, encrypts, and uploads that data over an encrypted link to Customer eXperience Drive (CXD), and associates the data with your Service Request.
6. The data is analyzed against the TAC database of more than 1000 diagnostic signatures.
7. The TAC representative reviews the results, checking the original logs if necessary.

Deployment Architecture for TAC Case

Figure 3: Deployment with Service Connector on Expressway



Element	Description
Managed devices	Includes any devices that you want to supply logs from to Serviceability Service. You can add up to 150 locally managed devices with one Serviceability connector. You can import information from HCM-F (Hosted Collaboration Mediation Fulfillment) about HCS customers' managed devices and clusters (with larger numbers of devices, see https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service). The service currently works with the following devices: • Hosted Collaboration Mediation Fulfillment (HCM-F) • Cisco Unified Communications Manager • Cisco Unified CM IM and Presence Service • Cisco Expressway Series • Cisco TelePresence Video Communication Server (VCS) • Cisco Unified Contact Center Express (UCCX) • Cisco Unified Border Element (CUBE) • Cisco BroadWorks Application Server (AS) • Cisco BroadWorks Profile Server (PS) • Cisco BroadWorks Messaging Server (UMS) • Cisco BroadWorks Execution Server (XS) • Cisco Broadworks Xtended Services Platform (XSP)
Your administrator	Uses Control Hub to register a connector host and enable Serviceability Service. The URL is https://admin.webex.com and you need your “organization administrator” credentials.
Connector host	An Enterprise Compute Platform (ECP) or Expressway that hosts the Management connector and the Serviceability Connector. • **Management Connector** (on ECP or Expressway) and the corresponding Management Service (in Webex) manage your registration. They persist the connection, update connectors when required, and report status and alarms. • **Serviceability Connector**—A small application that the connector host (ECP or Expressway) downloads from Webex after you enable your organization for Serviceability service.
Proxy	(Optional) If you change the proxy configuration after starting Serviceability Connector, then also restart the Serviceability Connector.
Webex cloud	Hosts Webex, Webex calling, Webex meetings, and Webex Hybrid Services.

Element	Description
Technical Assistance Center	Contains: • TAC representative using CSA to communicate with your Serviceability Connectors through Webex cloud. • TAC case management system with your case and associated logs that Serviceability Connector collected and uploaded to Customer eXperience Drive.

TAC Support for Serviceability Connector

For more details on Serviceability Connector, see https://www.cisco.com/go/serviceability or contact your TAC representative.

CHAPTER 14

Simple Network Management Protocol

Simple Network Management Protocol Support

SNMP, an application layer protocol, facilitates the exchange of management information among network devices, such as nodes and routers. As part of the TCP/IP suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

You use the serviceability GUI to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. The SNMP settings that you configure apply to the local node; however, if your system configuration supports clusters, you can apply settings to all servers in the cluster with the "Apply to All Nodes" option in the SNMP configuration windows.

Tip Unified Communications Manager only: SNMP configuration parameters that you specified in Cisco Unified CallManager or Unified Communications Manager 4.X do not migrate during a Unified Communications Manager 6.0 and later upgrade. You must perform the SNMP configuration procedures again in Cisco Unified Serviceability.

SNMP supports IPv4 and IPv6, the CISCO-CCM-MIB includes columns and storage for both IPv4 and IPv6 addresses, preferences, and so on.

SNMP Basics

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- Managed device - A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  Unified Communications Manager and IM and Presence Service only: In a configuration that supports clusters, the first node in the cluster acts as the managed device.

- Agent - A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.

  The master agent and subagent components are used to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the master agent contains a few Management Information Base (MIB) variables that relate to MIB-II. The master agent also connects and disconnects subagents after the subagent completes necessary tasks. The SNMP master agent listens on port 161 and forwards SNMP packets for Vendor MIBs.

  The Unified Communications Manager subagent interacts with the local Unified Communications Manager only. The Unified Communications Manager subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

  The IM and Presence Service subagent interacts with the local IM and Presence Service only. The IM and Presence Service subagents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

- Network Management System (NMS) - An SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. The following NMSs are supported:

  - CiscoWorks LAN Management Solution
  - HP OpenView
  - Third-party applications that support SNMP and Unified Communications Manager SNMP interfaces

SNMP Management Information Base

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

Observe the following limitations:

- Unified Communications Manager does not support CISCO-UNITY-MIB.
- Cisco Unity Connection does not support CISCO-CCM-MIB.
- IM and Presence Service does not support CISCO-CCM-MIB and CISCO-UNITY-MIB.

The SNM) extension agent resides in the server and exposes the CISCO-CCM-MIB, which provides detailed information about devices that are known to the server. In the case of a cluster configuration, the SNMP extension agent resides in each server in the cluster. The CISCO-CCM-MIB provides device information such as device registration status, IP address, description, and model type for the server (not the cluster, in a configuration that supports clusters).

The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

Use the CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables the SNMP managed device to advertise themself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

Note The CISCO-CDP-MIB is dependent on the presence of the following MIBs: CISCO-SMI, CISCO-TC, CISCO-VTP-MIB.

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun

- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

Table 17: SYSAPPL-MIB Commands

Command	Description
Device-Related Queries	
sysApplInstallPkgVersion	Provides the version number that the software manufacturer assigned to the application package.
sysApplElmPastRunUser	Provides the process owner's login name (for example, root).
Memory, Storage, and CPU-Related Queries	
sysApplElmPastRunMemory	Provides the last-known total amount of real system memory measured in kilobytes that was allocated to this process before it terminated.
sysApplElmtPastRunCPU	Provides the last known number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may increment by more than one centi-second in one centi-second of real (wall clock) time.
sysApplInstallElmtCurSizeLow	Provides the current file size modulo 2^32 bytes. For example, for a file with a total size of 4,294,967,296 bytes this variable would have a value of 0; for a file with a total size of 4,294,967,295 bytes this variable would be 4,294,967,295.
sysApplInstallElmtSizeLow	Provides the installed file size modulo 2^32 bytes. This is the size of the file on disk immediately after installation. For example, for a file with a total size of 4,294,967,296 bytes this variable would have a value of 0; for a file with a total size of 4,294,967,295 bytes this variable would be 4,294,967,295.
sysApplElmRunMemory	Provides the total amount of real system memory, measured in kilobytes, that is currently allocated to this process.

sysApplElmRunCPU	Provides the number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
Process-Related Queries	
sysApplElmtRunState	Provides the current state of the running process. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5).
sysApplElmtRunNumFiles	Provides the number of regular files currently opened by the process. Transport connections (sockets) should *not* be included in the calculation of this value, nor should operating-system-specific special file types.
sysApplElmtRunTimeStarted	Provides the time the process was started.
sysApplElmtRunMemory	Provides the total amount of real system memory, measured in kilobytes, that is currently allocated to this process.
sysApplElmtPastRunInstallID	Provides the index into the installed element table. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a previously executed process.
sysApplElmtPastRunUser	Provides the process owner's login name (for example, root).
sysApplElmtPastRunTimeEnded	Provides the time the process ended.
sysApplElmtRunUser	Provides the process owner's login name (for example, root).
sysApplRunStarted	Provides the date and time that the application was started.

sysApplElmtRunCPU	Provides the number of centi-seconds of the total system CPU resources consumed by this process. **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
Software Component-Related Queries	
sysApplInstallPkgProductName	Provides the name that the manufacturer assigned to the software application package.
sysApplElmtRunParameters	Provides the starting parameters for the process.
sysApplElmtRunName	Provides the full path and filename of the process. For example, '/opt/MYYpkg/bin/myyproc' would be returned for process 'myyproc' whose execution path is 'opt/MYYpkg/bin/myyproc'.
sysApplInstallElmtName	Provides the name of this element, which is contained in the application.
sysApplElmtRunUser	Provides the process owner's login name (for example, root).
sysApplInstallElmtPath	Provides the full path to the directory where this element is installed. For example, the value would be '/opt/EMPuma/bin' for an element installed in the directory '/opt/EMPuma/bin'. Most application packages include information about the elements that are contained in the package. In addition, elements are typically installed in subdirectories under the package installation directory. In cases where the element path names are not included in the package information itself, the path can usually be determined by a simple search of the subdirectories. If the element is not installed in that location and no other information is available to the agent implementation, then the path is unknown and null is returned.

sysApplMapInstallPkgIndex	Provides the value of this object and identifies the installed software package for the application of which this process is a part. Provided that the parent application of the process can be determined, the value of this object is the same value as the sysApplInstallPkgIndex for the entry in the sysApplInstallPkgTable that corresponds to the installed application of which this process is a part. If, however, the parent application cannot be determined (for example, the process is not part of a particular installed application), the value for this object is then '0', signifying that this process cannot be related back to an application, and in turn, an installed software package.
sysApplElmtRunInstallID	Provides the index into the sysApplInstallElmtTable. The value of this object is the same value as the sysApplInstallElmtIndex for the application element of which this entry represents a running instance. If this process cannot be associated with an installed executable, the value should be '0'.
sysApplRunCurrentState	Provides the current state of the running application instance. The possible values are running(1), runnable(2) but waiting for a resource such as CPU, waiting(3) for an event, exiting(4), or other(5). This value is based on an evaluation of the running elements of this application instance (see sysApplElmRunState) and their Roles as defined by sysApplInstallElmtRole. An agent implementation may detect that an application instance is in the process of exiting if one or more of its REQUIRED elements are no longer running. Most agent implementations will wait until a second internal poll is completed to give the system time to start REQUIRED elements before marking the application instance as exiting.
sysApplInstallPkgDate	Provides the date and time this software application was installed on the host.
sysApplInstallPkgVersion	Provides the version number that the software manufacturer assigned to the application package.

sysApplInstallElmtType	Provides the type of element that is part of the installed application.
Date/Time-Related Queries	
sysApplElmtRunCPU	The number of centi-seconds of the total system CPU resources consumed by this process **Note** On a multiprocessor system, this value may have been incremented by more than one centi-second in one centi-second of real (wall clock) time.
sysApplInstallPkgDate	Provides the date and time this software application is installed on the host.
sysApplElmtPastRunTimeEnded	Provides the time the process ended.
sysApplRunStarted	Provides the date and time that the application was started.

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

Table 18: MIB-II Commands

Command	Description
Device-Related Queries	
sysName	Provides an administratively assigned name for this managed node. By convention, this name is the fully qualified domain name of the node. If the name is unknown, the value is the zero-length string.

sysDescr	Provides a textual description of the entity. This value should include the full name and version identification of the system hardware type, software operating-system, and networking software.
SNMP Diagnostic Queries	
sysName	Provides an administratively assigned name for this managed node. By convention, this name is the fully-qualified domain name of the node. If the name is unknown, the value is the zero-length string.
sysUpTime	Provides the time (in hundredths of a second) since the network management portion of the system was last reinitialized.
snmpInTotalReqVars	Provides the total number of MIB objects that were retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpOutPkts	Provides the total number of SNMP Messages that were passed from the SNMP entity to the transport service.
sysServices	Provides a value that indicates the set of services that this entity potentially offers. The value is a sum. This sum initially takes the value zero, then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which is a host offering application services would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). **Note** In the context of the Internet suite of protocols, calculate: layer 1 physical (for example, repeaters), layer 2 datalink/subnetwork (for example, bridges), layer 3 internet (supports IP), layer 4 end-to-end (supports TCP), layer 7 applications (supports SMTP). For systems including OSI protocols, you can also count layers 5 and 6.

snmpEnableAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. **Note** Cisco strongly recommends that this object be stored in nonvolatile memory so that it remains constant across reinitializations of the network management system.
Syslog-Related Queries	
snmpEnabledAuthenTraps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. **Note** Cisco strongly recommends that this object be stored in a nonvolatile memory so that it remains constant across reinitializations of the network management system.
Date/Time-Related Queries	
sysUpTime	Provides the time (in hundredths of a second) since the network management portion of the system was last reinitialized.

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

Table 19: HOST-RESOURCES MIB Commands

Command	Description
Device-Related Queries	

hrFSMountPoint	Provides the path name of the root of this file system.
hrDeviceDescr	Provides a textual description of this device, including the device manufacturer and revision, and optionally, the serial number.
hrStorageDescr	Provides a description of the type and instance of the storage.
Memory, Storage, and CPU Related Queries	
hrMemorySize	Provides the amount of physical read-write main memory, typically RAM, that the host contains.
hrStorageSize	Provides the size of the storage, in units of hrStorageAllocationUnits.This object is writable to allow remote configuration of the size of the storage area in those cases where such an operation makes sense and is possible on the underlying system. For example, you can modify the amount of main memory allocated to a buffer pool or the amount of disk space allocated to virtual memory.
Process-Related Queries	
hrSWRunName	Provides a textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known. If this software is installed locally, it must be the same string as used in the corresponding hrSWInstalledName.
hrSystemProcesses	Provides the number of process contexts that are currently loaded or running on this system.
hrSWRunIndex	Provides a unique value for each piece of software that is running on the host. Wherever possible, use the native, unique identification number of the system.
Software Component-Related Queries	
hrSWInstalledName	Provides a textual description of this installed piece of software, including the manufacturer, revision, the name by which it is commonly known, and optionally, the serial number.
hrSWRunPath	Provides a description of the location of long-term storage (for example, a disk drive) from which this software was loaded.
Date/Time-Related Queries	
hrSystemDate	Provides the host local date and time of day.

hrFSLastPartialBackupDate	Provides the last date at which a portion of this file system was copied to another storage device for backup. This information is useful for ensuring that backups are being performed regularly. If this information is not known, then this variable will have the value corresponding to January 1, year 0000, 00:00:00.0, which is encoded as (hex)'00 00 01 01 00 00 00 00'.

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

Note The CISCO-SYSLOG-MIB is dependent on the presence of the CISCO-SMI MIB.

Table 20: CISCO-SYSLOG-MIB Commands

Command	Description
Syslog-Related Queries	
clogNotificationEnabled	Indicates whether clogMessageGenerated notifications will be sent when the device generates a syslog message. Disabling notifications does not prevent syslog messages from being added to the clogHistoryTable.
clogMaxSeverity	Indicates which syslog severity levels will be processed. The agent will ignore any syslog message with a severity value greater than this value. **Note** Severity numeric values increase as their severity decreases. For example, error (4) is more severe than debug (8).

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

The CISCO-CCM-MIB contains both dynamic (real-time) and configured (static) information about the Unified Communications Manager and its associated devices, such as phones, gateways, and so on, that are visible on this Unified Communications Manager node. Simple Network Management Protocol (SNMP) tables contain information such as IP address, registration status, and model type.

SNMP supports IPv4 and IPv6, the CISCO-CCM-MIB includes columns and storage for both IPv4 and IPv6 addresses, preferences, and so on.

Note Unified Communications Manager supports this MIB in Unified Communications Manager systems. IM and Presence Service and Cisco Unity Connection do not support this MIB.

To view the support lists for the CISCO-CCM-MIB and MIB definitions, go to the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

To view MIB dependencies and MIB contents, including obsolete objects, across Unified Communications Manager releases, go to the following link: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

Dynamic tables get populated only if the Cisco CallManager service is up and running (or the local Cisco CallManager service in the case of a Unified Communications Manager cluster configuration); static tables get populated when the Cisco CallManager SNMP Service is running.

Table 21: Cisco-CCM-MIB Dynamic Tables

Table(s)	Contents
ccmTable	This table stores the version and installation ID for the local Unified Communications Manager. The table also stores information about all the Unified Communications Manager in a cluster that the local Unified Communications Manager knows about but shows “unknown” for the version detail. If the local Unified Communications Manager is down, the table remains empty, except for the version and installation ID values.
ccmPhoneFailed, ccmPhoneStatusUpdate, ccmPhoneExtn, ccmPhone, ccmPhoneExtension	For the Cisco Unified IP Phone, the number of registered phones in ccmPhoneTable should match Unified Communications Manager/RegisteredHardware Phones perfmon counter. The ccmPhoneTable includes one entry for each registered, unregistered, or rejected Cisco Unified IP Phone. The ccmPhoneExtnTable uses a combined index, ccmPhoneIndex and ccmPhoneExtnIndex, for relating the entries in the ccmPhoneTable and ccmPhoneExtnTable.
ccmCTIDevice, ccmCTIDeviceDirNum	The ccmCTIDeviceTable stores each CTI device as one device. Based on the registration status of the CTI Route Point or CTI Port, the ccmRegisteredCTIDevices, ccmUnregisteredCTIDevices, and ccmRejectedCTIDevices counters in the Unified Communications Manager MIB get updated.
ccmSIPDevice	The CCMSIPDeviceTable stores each SIP trunk as one device.

Table(s)	Contents
ccmH323Device	The ccmH323DeviceTable contains the list of H.323 devices for which Unified Communications Manager contains information (or the local Unified Communications Manager in the case of a cluster configuration). For H.323 phones or H.323 gateways, the ccmH.323DeviceTable contains one entry for each H.323 device. (The H.323 phone and gateway do not register with Unified Communications Manager. Unified Communications Manager generates the H.323Started alarm when it is ready to handle calls for the indicated H.323 phone and gateway.) The system provides the gatekeeper information as part of the H.323 trunk information.
ccmVoiceMailDevice, ccmVoiceMailDirNum	For Cisco uOne, ActiveVoice, the ccmVoiceMailDeviceTable includes one entry for each voice-messaging device. Based on the registration status, the ccmRegisteredVoiceMailDevices, ccmUnregisteredVoiceMailDevices, and ccmRejectedVoiceMailDevices counters in the Cisc MIB get updated.
ccmGateway	The ccmRegisteredGateways, ccmUnregistered gateways, and ccmRejectedGateways keep track of the number of registered gateway devices or ports, number of unregistered gateway devices or ports, and number of rejected gateway devices or ports, respectively. Unified Communications Manager generates alarms at the device or port level. The ccmGatewayTable, based on CallManager alarms, contains device- or port-level information. Each registered, unregistered, or rejected device or port has one entry in ccmGatewayTable. The VG200 with two FXS ports and one T1 port has three entries in ccmGatewayTable. The ccmActiveGateway and ccmInActiveGateway counters track number of active (registered) and lost contact with (unregistered or rejected) gateway devices or ports. Based on the registration status, ccmRegisteredGateways, ccmUnregisteredGateways, and ccmRejectedGateways counters get updated.
ccmMediaDeviceInfo	The table contains a list of all media devices which have tried to register with the local Unified Communications Manager at least once.
ccmGroup	This tables contains the Unified Communications Manager groups in a Unified Communications Manager cluster.
ccmGroupMapping	This table maps all Unified Communications Manager's in a cluster to a Unified Communications Manager group. The table remains empty when the local Unified Communications Manager node is down.

Table 22: CISCO-CCM-MIB Static Tables

Table(s)	Content
ccmProductType	The table contains the list of product types that are supported with Unified Communications Manager (or cluster, in the case of a Unified Communications Manager cluster configuration), including phone types, gateway types, media device types, H.323 device types, CTI device types, voice-messaging device types, and SIP device types.
ccmRegion, ccmRegionPair	ccmRegionTable contains the list of all geographically separated regions in a Cisco Communications Network (CCN) system. The ccmRegionPairTable contains the list of geographical region pairs for a Unified Communications Manager cluster. Geographical region pairs are defined by Source region and Destination region.
ccmTimeZone	The table contains the list of all time zone groups in a Unified Communications Manager cluster.
ccmDevicePool	The tables contains the list of all device pools in a Unified Communications Manager cluster. Device pools are defined by Region, Date/Time Group, and Unified Communications Manager Group.

Note ‘The “ccmAlarmConfigInfo” and “ccmQualityReportAlarmConfigInfo” groups in the CISCO-CCM-MIB define the configuration parameters that relate to the notifications that are described.

CISCO-UNITY-MIB

The CISCO-UNITY-MIB uses the Connection SNMP Agent to get information about Cisco Unity Connection.

To view the CISCO-UNITY-MIB definitions, go to the following link and click **SNMP V2 MIBs**:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note Cisco Unity Connection supports this MIB. Unified Communications Manager and IM and Presence Service do not support this MIB.

The Connection SNMP Agent supports the following objects.

Table 23: CISCO-UNITY-MIB Objects

Object	Description
ciscoUnityTable	This table contains general information about the Cisco Unity Connection servers such as hostname and version number.
ciscoUnityPortTable	This table contains general information about the Cisco Unity Connection voice messaging ports.
General Unity Usage Info objects	This group contains information about capacity and utilization of the Cisco Unity Connection voice messaging ports.

SNMP Configuration Requirements

The system provides no default SNMP configuration. You must configure SNMP settings after installation to access MIB information. Cisco supports SNMP V1, V2c, and V3 versions.

SNMP agent provides security with community names and authentication traps. You must configure a community name to access MIB information. The following table provides the required SNMP configuration settings.

Table 24: SNMP Configuration Requirements

Configuration	Cisco Unified Serviceability Page
V1/V2c Community String	**SNMP** > **V1/V2c** > **Community String**
V3 Community String	**SNMP** > **V3** > **User**
System Contact and Location for MIB2	**SNMP** > **SystemGroup** > **MIB2 System Group**
Trap Destinations (V1/V2c)	**SNMP** > **V1/V2c** > **Notification Destination**
Trap Destinations (V3)	**SNMP** > **V3** > **Notification Destination**

SNMP Version 1 Support

SNMP Version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP).

The SNMPv1 SMI defines highly structured tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed, so SNMP can retrieve or alter an entire row with a supported command.

With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

In the serviceability GUI, you configure SNMPv1 support in the **V1/V2c Configuration** window.

SNMP Version 2c Support

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in

SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

The Inform operation in SNMPv2c allows one NMS to send trap information to another NMS and to then receive a response from the NMS.

In the serviceability GUI, you configure SNMPv2c support in the **V1/V2c Configuration** window.

SNMP Version 3 Support

SNMP Version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the requested objects). To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

Note From Release 12.5(1)SU1 onwards, the MD5 or DES encryption methods are not supported in Unified Communications Manager. You can choose either SHA or AES as the authentication protocols while adding an SNMPv3 user.

Instead of using community strings like SNMPv1 and v2, SNMPv3 uses SNMP users.

In the serviceability GUI, you configure SNMPv3 support in the **V3Configuration** window.

SNMP Services

The services in the following table support SNMP operations.

Note SNMP Master Agent serves as the primary service for the MIB interface. You must manually activate Cisco CallManager SNMP service; all other SNMP services should be running after installation.

Table 25: SNMP Services

MIB	Service	Window
CISCO-CCM-MIB	Cisco CallManager SNMP service	**Cisco Unified Serviceability** > **Tools** > **Control Center - Feature Services**. Choose a server; then, choose Performance and Monitoring category.

MIB	Service	Window
SNMP Agent	SNMP Master Agent	**Cisco Unified Serviceability** > **Tools** > **Control Center - Network Services.** Choose a server; then, choose Platform Services category. **CiscoUnifiedIM and Presence Serviceability** > **Tools** > **Control Center - Network Services.** Choose a server; then, choose Platform Services category.
CISCO-CDP-MIB	CiscoCDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
Hardware MIBs	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	**Cisco Unity Connection Serviceability** > **Tools** > **Service Management.** Choose a server; then, choose Base Services category.

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the Unified Communications Manager or Cisco Unity Connection network. Do not stop the services unless your technical support team tells you to do so.

SNMP Community Strings and Users

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. You configure SNMP community strings for SNMPv1 and v2c only.

SNMPv3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

In the serviceability GUI, no default community string or user exists.

SNMP Traps and Informs

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination, whereas informs do receive acknowledgments. You configure the notification destinations by using the SNMP Notification Destination Configuration windows in the serviceability GUI.

Note Unified Communications Manager supports SNMP traps in Unified Communications Manager and IM and Presence Service systems.

For SNMP notifications, the system sends traps immediately if the corresponding trap flags are enabled. In the case of the syslog agent, alarms and system level log messages get sent to syslog daemon for logging. Also, some standard third-party applications send the log messages to syslog daemon for logging. These log messages get logged locally in the syslog files and also get converted into SNMP traps/notifications.

The following list contains Unified Communications Manager SNMP trap/inform messages that are sent to a configured trap destination:

- Unified Communications Manager failed
- Phone failed
- Phones status update
- Gateway failed
- Media resource list exhausted
- Route list exhausted
- Gateway layer 2 change
- Quality report
- Malicious call
- Syslog message generated

Tip Before you configure notification destination, verify that the required SNMP services are activated and running. Also, make sure that you configured the privileges for the community string/user correctly.

You configure the SNMP trap destination by choosing **SNMP** > **V1/V2** > **Notification Destination** or **SNMP** > **V3** > **Notification Destination** in the serviceability GUI.

The following table provides information about trap/inform parameters that you configure on the Network Management System (NMS). You can configure the values in the table by issuing the appropriate commands on the NMS, as described in the SNMP product documentation that supports the NMS.

Note All the parameters that are listed in the table are part of CISCO-CCM-MIB except for the last two parameters. The last two, clogNotificationsEnabled and clogMaxSeverity, comprise part of CISCO-SYSLOG-MIB.

For IM and Presence Service, you configure only clogNotificationsEnabled and clogMaxSeverity trap/inform parameters on the NMS.

Table 26: Cisco Unified Communications Manager Trap/Inform Configuration Parameters

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	Keep the default specification.

Parameter Name	Default Value	Generated Traps	Configuration Recommendations
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Although you can configure a CiscoATA 186 device as a phone in Cisco Unified Communications Manager Administration, when Unified Communications Manager sends SNMP traps for the CiscoATA device, it sends a gateway type trap; for example, ccmGatewayFailed.	None. The default specifies this trap as enabled.
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	Set the ccmPhoneStatusUpdateAlarmInterval to a value between 30 and 3600.
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	Set the ccmPhoneFailedAlarmInterval to a value between 30 and 3600.
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	None. The default specifies this trap as enabled.
ccmQualityReportAlarmEnable	True	This trap gets generated only if the CiscoExtended Functions service is activated and running on the server, or, in the case of a cluster configuration (Unified Communications Manager only), on the local Unified Communications Manager server. ccmQualityReport	None. The default specifies this trap as enabled.
clogNotificationsEnabled	False	clogMessageGenerated	To enable trap generation, set clogNotificationsEnable to True.
clogMaxSeverity	Warning	clogMessageGenerated	When you set clogMaxSeverity to warning, a SNMP trap generates when applications generate a syslog message with at least a warning severity level.

SFTP Server Support

For internal testing, we use the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Table 27: SFTP Server Support

SFTP Server	Support Description
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Emergency Responder and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Emergency Responder to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided and third party tested. Version compatibility depends on the third-party test. Refer to the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager.
SFTP Server from another Third Party	These servers are third party provided and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Emergency Responder versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

SNMP Configuration Task Flow

Complete these tasks to configure the Simple Network Management Protocol. Make sure that you know which SNMP version you are going to configure as the tasks may vary. You can choose from SNMP V1, V2c, or V3..

Before you begin

Install and configure the SNMP Network Management System.

Procedure

	Command or Action	Purpose
Step 1	Activate SNMP Services, on page 166	Confirm that essential SNMP services are running.
Step 2	Complete one of the following tasks, according to your SNMP version: • Configure SNMP Community String, on page 167 • Configure an SNMP User, on page 169	For SNMP V1 or V2, configure a community string. For SNMP V3, configure an SNMP User.

	Command or Action	Purpose
Step 3	Get Remote SNMP Engine ID, on page 172	For SNMP V3, obtain the address of the remote SNMP engine, which is required in Notification Destination configuration. **Note** This procedure is mandatory for SNMP V3, but is optional for SNMP V1 or V2c.
Step 4	Configure SNMP Notification Destination, on page 173	For all SNMP versions, configure a Notification Destination for SNMP Traps and Informs.
Step 5	Configure MIB2 System Group, on page 177	Configure a system contact and system location for the MIB-II system group.
Step 6	CISCO-SYSLOG-MIB Trap Parameters, on page 178	Configure trap settings for CISCO-SYSLOG-MIB.
Step 7	CISCO-CCM-MIB Trap Parameters, on page 179	Unified Communications Manager only: Configure trap settings for CISCO-CCM-MIB.
Step 8	Restart SNMP Master Agent, on page 179	After completing your SNMP configuration, restart the SNMP Master Agent.
Step 9	On the SNMP Network Management System, configure the Unified Communications Manager trap parameters.	

Activate SNMP Services

Use this procedure to ensure that SNMP Services are up and running.

Procedure

Step 1 Log in to Cisco Unified Serviceability.

Step 2 Confirm that the **Cisco SNMP Master Agent** network service is running. The service is on by default.

a) Choose **Tools** > **Control Center - Network Services**.
b) Choose the publisher node and click **Go**.
c) Verify that the **Cisco SNMP Master Agent** service is running.

Step 3 Start the **Cisco Call Manager SNMP Service**.

a) Choose **Control Center** > **Service Activation**.
b) From the **Server** drop-down, choose the publisher node and click **Go**.
c) Confirm that the **Cisco Call Manager SNMP Service** is running. If it's not running, check the corresponding check box and click **Save**.

What to do next

If you are configuring SNMP V1 or V2c, Configure SNMP Community String, on page 167.

If you are configuring SNMP V3, Configure an SNMP User, on page 169.

Configure SNMP Community String

If you are deploying SNMP V1 or V2c, use this procedure to set up an SNMP community string.

Note This procedure is required for SNMP V1 or V2c. For SNMP V3, configure an SNMP User instead of a community string.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Snmp** > **V1/V2c** > **Community String**.

Step 2 Select a **Server** and click **Find** to search for existing community strings. Optionally, you can enter search parameters to locate a specific community string.

Step 3 Do either of the following:

- To edit an existing SNMP community string, select the string.
- To add a new community string, click **Add New**.

Note To delete an existing community string, select the string and click **Delete Selected**. After you delete the user, restart the Cisco SNMP Master Agent.

Step 4 Enter the **Community String Name**.

Step 5 Complete the fields in the **SNMP Community String Configuration** window. For help with the fields and their settings, see Community String Configuration Settings, on page 168.

Step 6 From the **Access Privileges** drop-down, configure the privileges for this community string.

Step 7 If you want these settings to apply to all cluster nodes, check the **Apply to All Nodes** check box.

Step 8 Click **Save**.

Step 9 Click **OK** to restart the SNMP master agent service and effect the changes.

What to do next

Configure SNMP Notification Destination, on page 173

Community String Configuration Settings

The following table describes the community string configuration settings.

Table 28: Community String Configuration Settings

Field	Description
Server	This setting in the Community String configuration window displays as read only because you specified the server choice when you performed the procedure in find a community string. To change the server for the community string, perform the find a community string procedure.
Community String	Enter a name for the community string. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Choose community string names that are hard for outsiders to figure out. When you edit a community string, you cannot change the name of the community string.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click this button.
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Hostname/IPv4/IPv6 Address field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets and click **Insert**. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334. Repeat this process for each address from which you want to accept SNMP packets. To delete an address, choose that address from the Host IPv4/IPv6 Addresses list box and click **Remove**.

Field	Description
Access Privileges	From the drop-down list box, select the appropriate access level from the following list: **ReadOnly** The community string can only read the values of MIB objects. **ReadWrite** The community string can read and write the values of MIB objects. **ReadWriteNotify** The community string can read and write the values of MIB objects and send MIB object values for a trap and inform messages. **NotifyOnly** The community string can only send MIB object values for a trap and inform messages. **ReadNotifyOnly** The community string can read values of MIB objects and also send the values for trap and inform messages. **None** The community string cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, configure a community string with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges. IM and Presence Service does not support ReadNoticyOnly.
Apply To All Nodes	To apply the community string to all nodes in the cluster, check this check box. This field applies to Unified Communications Manager and IM and Presence Service clusters only.

Configure an SNMP User

If you are deploying SNMP V3, use this procedure to set up an SNMP User.

Note This procedure is required for SNMP V3 only. For SNMP V1 or V2c, configure a community string instead.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Snmp** > **V3** > **User**.

Step 2 Select a **Server** and click **Find** to search for existing SNMP users. Optionally, you can enter search parameters to locate a specific user.

Step 3 Do either of the following::

- To edit an existing SNMP user, select the user.
- To add a new SNMP user, click **Add New**.

Note To delete an existing user, select the user and click **Delete Selected**. After you delete the user, restart the Cisco SNMP Master Agent.

Step 4 Enter the **SNMP User Name**.

Step 5 Enter the SNMP User configuration settings. For help with the fields and their settings, see SNMP V3 User Configuration Settings, on page 170.

Tip Before you save the configuration, you can click the **Clear All** button at any time to delete all information that you entered for all settings in the window.

Step 6 From the **Access Privileges** drop-down, configure the access privileges that you want to assign to this user.

Step 7 If you want to apply this configuration to all cluster nodes, check the **Apply to all Nodes** check box.

Step 8 Click **Save**.

Step 9 Click **OK** to restart the SNMP Master Agent.

Note To access the server with the user that you configured, make sure that you configure this user on the NMS with the appropriate authentication and privacy settings.

What to do next

Get Remote SNMP Engine ID, on page 172

SNMP V3 User Configuration Settings

The following table describes the SNMP V3 user configuration settings.

Table 29: SNMP V3 User Configuration Settings

Field	Description
Server	This setting displays as read only because you specified the server when you performed the find notification destination procedure. To change the server where you want to provide access, perform the procedure to find an SNMP user.
User Name	In the field, enter the name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS). For existing SNMP users, this setting displays as read only.

Field	Description
Authentication Required	To require authentication, check the check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol. The password must contain at least 8 characters. **Note** If FIPS mode or Enhanced Security Mode is enabled, choose **SHA** as the protocol.
Privacy Required	If you checked the Authentication Required check box, you can specify privacy information. To require privacy, check the check box, enter the password in the Password and Reenter Password fields, and check the protocol check box. The password must contain at least 8 characters. **Note** If FIPS mode or Enhanced Security Mode is enabled, choose **AES128** as the protocol.
Accept SNMP Packets from any host	To accept SNMP packets from any host, click the radio button.
Accept SNMP Packets only from these hosts	To accept SNMP packets from specific hosts, click the radio button. In the Hostname/IPv4/IPv6 Address field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets and click **Insert**. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334. Repeat this process for each address from which you want to accept SNMP packets. To delete an address, choose that address from the Host IPv4/IPv6 Addresses list box and click **Remove**.

Field	Description
Access Privileges	From the drop-down list box, choose one of the following options for the access level: **ReadOnly** You can only read the values of MIB objects. **ReadWrite** You can read and write the values of MIB objects. **ReadWriteNotify** You can read and write the values of MIB objects and send MIB object values for a trap and inform messages. **NotifyOnly** You can only send MIB object values for trap and inform messages. **ReadNotifyOnly** You can read values of MIB objects and also send the values for trap and inform messages. **None** You cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
Apply To All Nodes	To apply the user configuration to all nodes in the cluster, check this check box. This applies to Unified Communications Manager and IM and Presence Service clusters only.

Get Remote SNMP Engine ID

If you are deploying SNMP V3, use this procedure to obtain the remote SNMP engine ID, which is required for Notification Destination configuration.

Note This procedure is mandatory for SNMP V3, but is optional for SNMP V1 or 2C.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the `utils snmp walk 1` CLI command.

Step 3 Enter the configured community string (with SNMP V1/V2) or configured user (with SNMP V3).

Step 4 Enter the ip address of the server. For example, enter `127.0.0.1` for localhost.

Step 5 Enter `1.3.6.1.6.3.10.2.1.1.0` as the Object ID (OID).

Step 6 For the file, enter `file`.

Step 7 Enter `y`.

The HEX-STRING that the system outputs represents the Remote SNMP Engine ID.

Step 8 Repeat this procedure on each node where SNMP is running.

What to do next

Configure SNMP Notification Destination, on page 173

Configure SNMP Notification Destination

Use this procedure to configure a Notification Destination for SNMP Traps and Informs. You can use this procedure for either SNMP V1, V2c, or V3.

Before you begin

If you haven't set up an SNMP community string or SNMP user yet, complete one of these tasks:

- For SNMP V1/V2, see Configure SNMP Community String, on page 167
- For SNMP V3, see Configure an SNMP User, on page 169

Procedure

Step 1 From Cisco Unifeid Serviceability, choose one of the following:

- For SNMP V1/V2, choose **Snmp** > **V1/V2** > **Notification Destination**
- For SNMP V3, choose **Snmp** > **V3** > **Notification Destination**

Step 2 Select a **Server** and click **Find** to search for existing SNMP Notification Destinations. Optionally, you can enter search parameters to locate a specific destination.

Step 3 Do either of the following::

- To edit an existing SNMP notification destination, select the notification destination.
- To add a new SNMP notification destination, click **Add New**.

Note To delete an existing SNMP notification destination, select the destination and click **Delete Selected**. After you delete the user, restart the **Cisco SNMP Master Agent**.

Step 4 From the **Host IP Addresses** drop-down, select an existing address or click **Add New** and enter a new host IP address.

Step 5 SNMP V1/V2 only. From the **SNMP Version** field, check the V1 or V2C radio buttons, depending on whether you are configuring SNMP V1 or V2c.

Step 6 For SNMP V1/V2, complete these steps:

a) SNMP V2 only. From the **Notification Type** drop-down, select **Inform** or **Trap**.

b) Select the **Community String** that you configured.

Step 7 For SNMP V3, complete these steps:

a) From the **Notification Type** drop-down select **Inform** or **Trap**.

b) From the **Remote SNMP Engine ID** drop-down, select an existing Engine ID or select **Add New** and enter a new ID.

c) From the **Security Level** drop-down, assign the appropriate security level.

Step 8 If you want to apply this configuration to all cluster nodes, check the **Apply to all Nodes** check box.

Step 9 Click **Insert**.

Step 10 Click **OK** to restart the SNMP Master Agent.

Example

Note For field description help in the Notification Destination Configuration window, see one of the following topics:

- Notification Destination Settings for SNMP V1 and V2c, on page 174
- Notification Destination Settings for SNMP V3, on page 175

What to do next

Configure MIB2 System Group, on page 177

Notification Destination Settings for SNMP V1 and V2c

The following table describes the notification destination configuration settings for SNMP V1/V2c.

Table 30: Notification Destination Configuration Settings for SNMP V1/V2c

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure to find a notification destination. To change the server for the notification destination, perform the procedure to find a community string.
Host IPv4/IPv6 Addresses	From the drop-down list box, select the Host IPv4/IPv6 address of the trap destination or click **Add New**. If you click **Add New**, enter the IPv4/IPv6 address of the trap destination in the Host IPv4/IPv6 Address field. For existing notification destinations, you cannot modify the host IP address configuration.

Field	Description
Host IPv4/IPv6 Address	In the field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334.
Port Number	In the field, enter the notification-receiving port number on the destination server that receives SNMP packets.
V1 or V2c	From the SNMP Version Information pane, click the appropriate SNMP version radio button, either V1 or V2c, which depends on the version of SNMP that you are using. • If you choose V1, configure the community string setting. • If you choose V2c, configure the notification type setting and then configure the community string.
Community String	From the drop-down list box, choose the community string name to be used in the notification messages that this host generates. Only community strings with minimum notify privileges (ReadWriteNotify or Notify Only) display. If you have not configured a community string with these privileges, no options appear in the drop-down list box. If necessary, click **Create New uiCommunity String** to create a community string. IM and Presence only: Only community strings with minimum notify privileges (ReadWriteNotify, ReadNotifyOnly, or Notify Only) display. If you have not configured a community string with these privileges, no options appear in the drop-down list box. If necessary, click **Create New Community String** to create a community string.
Notification Type	From the drop-down list box, choose the appropriate notification type.
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Notification Destination Settings for SNMP V3

The following table describes the notification destination configuration settings for SNMP V3.

Table 31: Notification Destination Configuration Settings for SNMP V3

Field	Description
Server	This setting displays as read only because you specified the server when you performed the procedure to find an SNMP V3 notification destination. To change the server for the notification destination, perform the procedure to find an SNMP V3 notification destination and select a different server.

Field	Description
Host IPv4/IPv6 Addresses	From the drop-down list box, select the Host IPv4/IPv6 address of the trap destination or click **Add New**. If you click **Add New**, enter the IPv4/IPv6 address of the trap destination in the Host IPv4/IPv6 Address field. For existing notification destinations, you cannot modify the host IP address configuration.
Host IPv4/IPv6 Address	In the field, enter either IPv4 or IPv6 address from which you want to accept SNMP packets. The IPv4 address is in dotted decimal format. For example, 10.66.34.23. The IPv6 address is in colon separated hexadecimal format. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 2001:0db8:85a3::8a2e:0370:7334.
Port Number	In the field, enter the notification-receiving port number on the destination server.
Notification Type	From the drop-down list box, choose **Inform** or **Trap**. **Tip** Cisco recommends that you choose the Inform option. The Inform function retransmits the message until it is acknowledged, thus, making it more reliable than traps.
Remote SNMP Engine Id	This setting displays if you chose Inform from the Notification Type drop-down list box. From the drop-down list box, choose the engine ID or choose **Add New**. If you chose Add New, enter the ID in the Remote SNMP Engine Id field, which requires a hexidecimal value.
Security Level	From the drop-down list box, choose the appropriate security level for the user. **noAuthNoPriv** No authentication or privacy configured. **authNoPriv** Authentication configured, but no privacy configured. **authPriv** Authentication and privacy configured.
User Information pane	From the pane, perform one of the following tasks to associate or disassociate the notification destination with the user. **1.** To create a new user, click **Create New User**. **2.** To modify an existing user, click the radio button for the user and then click **Update Selected User**. **3.** To delete a user, click the radio button for the user and then click **Delete Selected User**. The users that display vary depending on the security level that you configured for the notification destination.

Field	Description
Apply To All Nodes	To apply the notification destination configuration to all nodes in the cluster, check this check box. This applies to Cisco Unified Communications Manager and IM and Presence Service clusters only.

Configure MIB2 System Group

Use this procedure to configure a system contact and system location for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and SanJose, Bldg 23, 2nd floor, for the system location. You can use this procedure for SNMP V1, V2, and V3.

Procedure

Step 1 From cisco Unified Serviceability, choose **Snmp** > **SystemGroup** > **MIB2 System Group**.

Step 2 From the **Server** drop-down select a node and click **Go**.

Step 3 Complete the **System Contact** and **System Location** fields.

Step 4 If you want these settings to apply to all cluster nodes, check the **Apply to All Nodes** check box.

Step 5 Click **Save**.

Step 6 Click **OK** to restart the SNMP master agent service

Example

Note For field description help, see MIB2 System Group Settings, on page 177

Note You can click **Clear All** to clear the fields. If you click **Clear All** followed by**Save**, the record is deleted.

MIB2 System Group Settings

The following table describes the MIB2 System Group configuration settings.

Table 32: MIB2 System Group Configuration Settings

Field	Description
Server	From the drop-down list box, choose the server for which you want to configure contacts, and then click **Go**.
System Contact	Enter a person to notify when problems occur.

Field	Description
System Location	Enter the location of the person that is identified as the system contact.
Apply To All Nodes	Check to apply the system configuration to all of the nodes in the cluster. This applies to Unified Communications Manager and IM and Presence Service clusters only.

CISCO-SYSLOG-MIB Trap Parameters

Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system:

- Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to True by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to True from the linux command line using:

  ```
  snmpset -c <community string>-v2c
  <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
  ```

  You can also use any other SNMP management application for the SNMP Set operation.

- Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

  ```
  snmpset-c public-v2c
  <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>
  ```

  Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.

  Severity values are as follows:

  - 1: Emergency
  - 2: Alert
  - 3: Critical
  - 4: Error
  - 5: Warning
  - 6: Notice
  - 7: Info
  - 8: Debug)

  You can also use any other SNMP management application for the SNMP Set operation.

Note Before logging, Syslog truncates any trap message data that is larger than the specified Syslog buffer size. The Syslog trap message length limitation equals 255 bytes.

CISCO-CCM-MIB Trap Parameters

- Set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

  ```
  snmpset -c <community string> -v2c
  <transmitter ipaddress> 1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
  ```

  You can also use any other SNMP management application for the SNMP Set operation.

- Set ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) to a value in the range 30-3600 by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using:

  ```
  snmpset -c <community string> -v2c
  <transmitter ipaddress> 1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
  ```

  You can also use any other SNMP management application for the SNMP Set operation.

CISCO-UNITY-MIB Trap Parameters

Cisco Unity Connection only: The Cisco Unity Connection SNMP Agent does not enable trap notifications, though traps can be triggered by Cisco Unity Connection alarms. You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability, on the **Alarm** > **Definitions** screen.

You can configure trap parameters by using the CISCO-SYSLOG-MIB.

Related Topics

CISCO-SYSLOG-MIB Trap Parameters, on page 178

Restart SNMP Master Agent

After you complete all of your SNMP configurations, restart the SNMP Master Agent service.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Network Services**.

Step 2 Choose a **Server** and click **Go**.

Step 3 Select the **SNMP Master Agent**.

Step 4 Click **Restart**.

SNMP Trap Settings

Use CLI commands to set the configurable SNMP trap settings. SNMP trap configuration parameters and recommended configuration tips are provided for CISCO-SYSLOG-MIB, CISCO-CCM-MIB, and CISCO-UNITY-MIB.

Configure SNMP Traps

Use this procedure to configure SNMP traps.

Before you begin

Configure your system for SNMP. For details, see SNMP Configuration Task Flow, on page 165.

Make sure that the **Access Privileges** for either the SNMP community string (for SNMP V1/V2), or the SNMP user (for SNMP V3) are set to one of the following settings: **ReadWriteNotify**, **ReadNotify**, **NotifyOnly**.

Procedure

Step 1 Log in to CLI and run the `utils snmp test` CLI command to verify that SNMP is running.

Step 2 Follow Generate SNMP Traps, on page 180 to generate specific SNMP traps (for example, the ccmPhoneFailed or MediaResourceListExhausted traps).

Step 3 If the traps do not generate, perform the following steps:

- In Cisco Unified Serviceability, choose **Alarm** > **Configuration** and select **CM Services** and **Cisco CallManager**.
- Check the **Apply to All Nodes** check box.
- Under Local Syslogs, set the Alarm Event Level drop-down list box to **Informational**.

Step 4 Reproduce the traps and check if the corresponding alarm is logged in CiscoSyslog file.

Generate SNMP Traps

This section describes the process for generating specific types of SNMP traps. SNMP must be set up and running on the server in order for the individual traps to generate. Follow Configure SNMP Traps, on page 180 for instructions on how to set up your system to generate SNMP traps.

Note The processing time for individual SNMP traps varies depending on which trap you are attempting to generate. Some SNMP traps may take up to a few minutes to generate.

Table 33: Generate SNMP Traps

SNMP Traps	Process
ccmPhoneStatusUpdate	To trigger the ccmPhoneStatusUpdate trap: 1. In the ccmAlarmConfig Info mib table, set ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 or higher. 2. Log in to Cisco Unified Communications Manager Administration. 3. For a phone that is in service and that is registered to Unified Communications Manager, reset the phone. The phone deregisters, and then reregisters, generating the ccmPhoneStatusUpdate trap.
ccmPhoneFailed	To trigger the ccmPhoneFailed trap: 1. In the ccmAlarmConfigInfo mib table, set ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 or higher. 2. In Cisco Unified Communications Manager Administration, change the MAC address of the phone to an invalid value. 3. In Cisco Unified Communications Manager Administration, reregister the phone. 4. Set the phone to point to the TFTP server A and plug the phone into a different server.
ccmGatewayFailed	To trigger the ccmGatewayFailed SNMP trap: 1. Confirm that ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) is set to true. 2. In Cisco Unified Communications Manager Administration, change the MAC address of the gateway to an invalid value. 3. Reboot the gateway.
ccmGatewayLayer2Change	To trigger the ccmGatewayLayer2Change trap on a working gateway where layer 2 is monitored (for example, the MGCP backhaul load): 1. In the ccmAlarmConfig Info mib table, set ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true. 2. In Cisco Unified Communications Manager Administration, change the MAC address of the gateway to an invalid value. 3. Reset the gateway.

SNMP Traps	Process
MediaResourceListExhausted	To trigger a MediaResourceListExhausted trap: **1.** In Cisco Unified Communications Manager Administration, create a media resource group that contains one of the standard Conference Bridge resources (CFB-2). **2.** Create a media resource group list that contains the media resource group that you created. **3.** In the Phone Configuration window, set the Media Resource Group List field to the media resource group list that you have created. **4.** Stop the IP Voice Media Streaming service. This action causes the ConferenceBridge resource (CFB-2) to stop working. **5.** Make conference calls with phones that use the media resource group list. The "No Conference Bridge available" message appears in the phone screen.
RouteListExhausted	To trigger a RouteListExhausted trap: **1.** Create a route group that contains one gateway. **2.** Create a route group list that contains the route group that you just created. **3.** Create a unique route pattern that routes a call through the route group list. **4.** Deregister the gateway. **5.** Dial a number that matches the route pattern from one of the phones.
MaliciousCallFailed	To trigger a MaliciousCallFailed trap: **1.** Create a softkey template that includes all available "MaliciousCall" softkeys. **2.** Assign the new softkey template to phones in your network and reset the phones. **3.** Place a call between the phones. **4.** During the call, select the "MaliciousCall" softkey.

SNMP Traps	Process
ccmCallManagerFailed	1. Run the `show process list` CLI command to get the Process Identifier (PID) of the CallManager application ccm. This command returns a number of processes and their PIDs. You must obtain the PID for ccm specifically since this is the PID that you must stop in order to generate the alarm. 2. Run the `delete process <pid>` crash CLI command 3. Run the CLI command. The CallManager Failed Alarm is generated when internal errors are generated. These internal errors may include an internal thread quitting due to the lack of CPU, pausing the CallManager server for more than 16 seconds, and timer issues. You cannot manually generate this alarm. **Note** Generating a ccmCallManagerFailed alarm or trap shuts down the CallManager service and generates a core file. To avoid confusion, Cisco recommends that you delete the core file immediately.
syslog messages as traps	To receive syslog messages above a particular severity as traps, set the following two mib objects in the clogBasic table: 1. Set clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true(1). Default value is false(2). For example, snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 2. Set the clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) to a level that is greater than the level at which you want your traps to be produced. The default value is warning (5). All syslog messages with alarm severity lesser than or equal to the configured severity level are sent as traps. For example, snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP Trace Configuration

For Unified Communications Manager, you can configure trace for the Cisco CallManager SNMP agent in the Trace Configuration window in Cisco Unified Serviceability by choosing the Cisco CallManager SNMP Service in the Performance and Monitoring Services service group. A default setting exists for all the agents. For Cisco CDP Agent and Cisco Syslog Agent, you use the CLI to change trace settings, as described in the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For Cisco Unity Connection, you can configure trace for the Cisco Unity Connection SNMP agent in the Trace Configuration window in Cisco Unity Connection Serviceability by choosing the Connection SNMP Agent component.

Troubleshooting SNMP

Review this section for troubleshooting tips. Make sure that all of the feature and network services are running.

Problem

You cannot poll any MIBs from the system.

This condition means that the community string or the snmp user is not configured on the system or they do not match with what is configured on the system. By default, no community string or user is configured on the system.

Solution

Check whether the community string or snmp user is properly configured on the system by using the SNMP configuration windows.

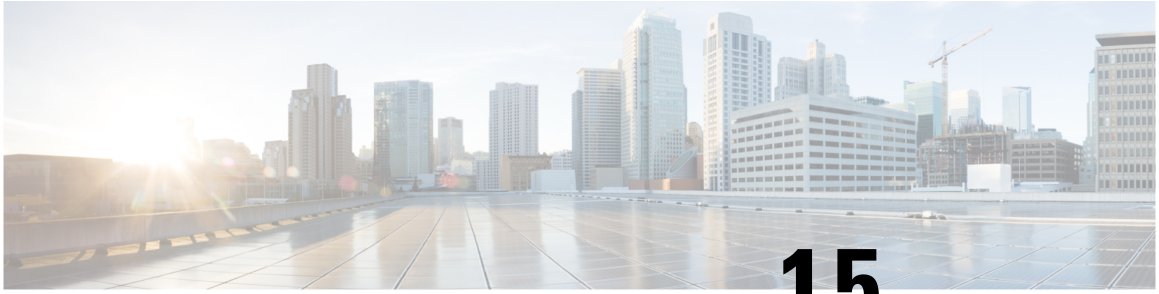
Problem

You cannot receive any notifications from the system.

This condition means that the notification destination is not configured correctly on the system.

Solution

Verify that you configured the notification destination properly in the Notification Destination (V1/V2c or V3) Configuration window.



CHAPTER 15

Services

Feature Services

Use the Serviceability GUI to activate, start, and stop Cisco Unified Communications Manager and IM and Presence services. Activation turns on and starts a service. You must manually activate the feature service for all features that you want to use. For service-activation recommendations, see topics related to service activation.

Note If you try to access a Unified Communications Manager server from an IM and Presence node or vice versa, you may encounter the following error: "Connection to the Server cannot be established (unable to access Remote Node)" . If this error message appears, see the *Administration Guide for Cisco Unified Communications Manager* .

Note Devices using IM and Presence are configured to use a Postgres external database to support persistent chat, compliance, and file transfer. However, the connection between IM and Presence server and Postgres is not secured and the data passes without any check. For the services or devices that do not support TLS, there is another way to provide secure communication by configuring IP Sec, which is a standard protocol for secure communications by authenticating and encrypting each IP packet of a communication session.

After you activate a service in the **Service Activation** window, you do not need to start it in the **Control Center - Feature Services** window. If the service does not start for any reason, you must start it in the **Control Center - Feature Services** window.

After the system is installed, it does not automatically activate feature services, You need to activate the feature service to use your configuration features, for example, the Serviceability Reports Archive feature.

Unified Communications Manager and Cisco Unified IM and Presence Service only: If you are upgrading Unified Communications Manager, those services that you activated on the system before the upgrade automatically start after the upgrade.

After you activate feature services, you can modify service parameter settings using the administrative GUI for your product:

- Cisco Unified Communications Manager Administration
- Cisco Unity Connection Administration

Feature Services Categories

In Cisco Unified Serviceability, the **Service Activation** window and the **Control Center - Feature Services** window categorize feature services into the following groups:

- Database and administration services
- Performance and monitoring services
- CM services
- CTI services
- CDR services
- Security services
- Directory services
- Voice quality reporter services

In Cisco Unified IM and Presence Serviceability, the **Service Activation** window and the **Control Center - Feature Services** window categorize feature services into the following groups:

- Database and administration services
- Performance and monitoring services
- IM and Presence Service services

Database and Administration Services

Locations Bandwidth Manager

This service is not supported by IM and Presence Service.

The Locations Bandwidth Manager service assembles a network model from configured Location and Link data in one or more clusters, determines the Effective Paths between pairs of Locations, determines whether to admit calls between a pair of Locations based on the availability of bandwidth for each type of call, and deducts (reserves) bandwidth for the duration of each call that is admitted.

Cisco AXL Web Service

The Cisco AXL Web Service allows you to modify database entries and execute stored procedures from client-based applications that use AXL.

In an IM and Presence Service system, this service supports both Unified Communications Manager and Cisco Unity Connection.

Cisco UXL Web Service

This service is not supported by IM and Presence Service.

The TabSync client in Cisco IP Phone Address Book Synchronizer uses the Cisco UXL Web Service for queries to the Unified Communications Manager database, which ensures that Cisco IP Phone Address Book Synchronizer users have access only to end-user data that pertains to them. The Cisco UXL Web Service performs the following functions:

- Conducts authentication checks by verifying the end-user username and password when an end user logs in to Cisco IP Phone Address Book Synchronizer.
- Conducts a user authorization check by only allowing the user that is currently logged in to Cisco IP Phone Address Book Synchronizer to perform functions such as listing, retrieving, updating, removing, and adding contacts.

Cisco Bulk Provisioning Service

This service does not support Cisco Unity Connection.

If your configuration supports clusters (Unified Communications Manager only), you can activate the Cisco Bulk Provisioning Service only on the first server. If you use the Unified Communications Manager Bulk Administration Tool to administer phones and users, you must activate this service.

Cisco TAPS Service

This service does not support Cisco Unity Connection or IM and Presence Service.

The Cisco Tools for Auto-Registered Phones Support (TAPS) Service supports the Cisco Unified Communications Manager Auto-Register Phone Tool, which allows a user to upload a customized configuration on an auto registered phone after a user responds to Interactive Voice Response (IVR) prompts.

If your configuration supports clusters (Unified Communications Manager only), you activate this service on the first server. When you want to create dummy MAC addresses for the tool, ensure that the Cisco Bulk Provisioning Service is activated on the same server.

Tip The Cisco Unified Communications Manager Auto-Register Phone Tool relies on Cisco Customer Response Solutions (CRS). Before the tool can work as designed, verify that the CRS server is configured and running, as described in the CRS documentation.

Platform Administrative Web Service

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Important Do not activate the Platform Administrative Web Service on the PAWS-M server.

Performance and monitoring services

Cisco Serviceability Reporter

The Cisco Serviceability Reporter service generates daily reports. For details, see topics that are related to the serviceability reports archive.

If your configuration supports clusters (Unified Communications Manager only), this service is installed on all the Unified Communications Manager servers in the cluster. Reporter generates reports once a day based on logged information. You can access the reports that Reporter generates in Cisco Unified Serviceability from the Tools menu. Each summary report comprises different charts that display the statistics for that particular report. After you activate the service, report generation may take up to 24 hours.

Related Topics

Serviceability Reports Archive, on page 269

Cisco CallManager SNMP Service

This service does not support IM and Presence Service and Cisco Unity Connection.

This service, which implements the CISCO-CCM-MIB, provides SNMP access to provisioning and statistics information that is available for Unified Communications Manager.

If your configuration supports clusters (Unified Communications Manager only), activate this service on all servers in the cluster.

CM Services

This section describes the CM Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CallManager

The Cisco CallManager Service provides software-only call processing as well as signaling and call control functionality for Unified Communications Manager.

Tip

Unified Communications Manager clusters only: Before you activate this service, verify that the Unified Communications Manager server displays in the Find and List Cisco Unified Communications Manager's window in Cisco Unified Communications Manager Administration. If the server does not display, add the Unified Communications Manager server before you activate this service. For information on how to find and add the server, see the *Administration Guide for Cisco Unified Communications Manager* .

Unified Communications Manager clusters only: If you deactivate the Cisco CallManager or CTIManager services in Service Activation, the Unified Communications Manager server where you deactivated the service no longer exists in the database, which means that you cannot choose that Unified Communications Manager server for configuration operations in Cisco Unified Communications Manager Administration because it does not display in the graphical user interface (GUI). If you then reactivate the services on the same Unified Communications Manager server, the database creates an entry for Unified Communications Manager again and adds a "CM_" prefix to the server name or IP address; for example, if you reactivate the Cisco CallManager or CTIManager service on a server with an IP address of 172.19.140.180, then CM_172.19.140.180 displays in Cisco Unified Communications Manager Administration. You can now choose the server, with the new "CM_" prefix, in Cisco Unified Communications Manager Administration.

The following services rely on Cisco CallManager service activation:

- CM Services
- CDR Services

Cisco TFTP

Cisco Trivial File Transfer Protocol (TFTP) builds and serves files that are consistent with the trivial file transfer protocol, a simplified version of FTP. Cisco TFTP serves embedded component executable, ringer files, and device configuration files.

Unified Communications Manager only: A configuration file includes a list of Unified Communications Manager's to which devices (telephones and gateways) make connections. When a device boots, the component queries a Dynamic Host Configuration Protocol (DHCP) server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. The device requests a configuration file from the TFTP server. The configuration file contains a list of Unified Communications Manager's and the TCP port through which the device connects to those Unified Communications Manager's. The configuration file contains a list of Unified Communications Managers and the TCP port through which the device connects to those Unified Communications Manager's.

Cisco Messaging Interface

The Cisco Messaging Interface allows you to connect a simplified message desk interface (SMDI)-compliant external voice-messaging system with the Cisco Unified Communications Manager. The SMDI defines a way for a phone system to provide a voice-messaging system with the information that is needed to intelligently process incoming calls.

Cisco Unified Mobile Voice Access Service

The Cisco Unified Voice Access Service starts the mobile voice access capability within Cisco Unified Mobility; mobile voice access, which is an integrated voice response (IVR) system, allows Cisco Unified Mobility users to perform the following tasks:

- Make calls from the cellular phone as if the call originated from the desk phone.
- Turn Cisco Unified Mobility on.
- Turn Cisco Unified Mobility off.

Cisco IP Voice Media Streaming App

The Cisco IP Voice Media Streaming Application service provides voice media streaming functionality for Unified Communications Manager for use with Media Termination Point (MTP), conferencing, music on hold (MOH), and annunciator. The Cisco IP Voice Media Streaming Application relays messages from Unified Communications Manager to the IP voice media streaming driver, which handles Real-Time Protocol (RTP) streaming.

The Cisco IP Voice Media Streaming Application service does not generate the Call Management Record (CMR) files for call legs that involve any IP Voice Media Streaming Application components like conference, MOH, annunciator, or MTP.

Cisco CTIManager

The Cisco CTI Manager contains the CTI components that interact with applications. This service allows applications to monitor or control phones and virtual devices to perform call control functionality.

Unified Communications Manager clusters only: With CTI Manager, applications can access resources and functionality of all Unified Communications Manager's in the cluster and have improved failover capability. Although one or more CTI Managers can be active in a cluster, only one CTI Manager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTI Managers; however, an application can use only one connection at a time to open a device with media termination.

Cisco Extension Mobility

This service, which supports the Cisco Extension Mobility feature, performs the login and automatic logout functionality for the feature.

Cisco Dialed Number Analyzer

The Cisco Dialed Number Analyzer service supports Unified Communications Manager Dialed Number Analyzer. When activated, this application consumes a lot of resources, so activate this service only during off-peak hours when minimal call-processing interruptions may occur.

Unified Communications Manager clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

Cisco Dialed Number Analyzer Server

The Cisco Dialed Number Analyzer Server service along with the Cisco Dialed Number Analyzer service supports Cisco Unified Communications Manager Dialed Number Analyzer. This service needs to be activated only on the node that is dedicated specifically for the Cisco Dialed Number Analyzer service.

Unified Communications Manager clusters only: Cisco does not recommend that you activate the service on all the servers in a cluster. Cisco recommends that you activate this service only on one of the servers of a cluster where call-processing activity is the least.

Cisco DHCP Monitor Service

Cisco DHCP Monitor Service monitors IP address changes for IP phones in the database tables. When a change is detected, it modifies the /etc./dhcpd.conf file and restarts the DHCPD daemon.

Cisco Intercluster Lookup Service

The Intercluster Lookup Service (ILS) runs on a cluster-wide basis. ILS allows you to create networks of remote Unified Communications Manager clusters. The ILS cluster discovery feature allows Unified Communications Manager to connect to remote clusters without the need for an administrator having to manually configure connections between each cluster. The ILS Global Dial Plan Replication feature enables clusters in the ILS network with the ability to exchange global dial plan data with the other clusters in an ILS network.

ILS can be activated from the ILS Configuration window that can be accessed in Cisco Unified Communications Manager Administration by selecting **Advanced Features** > **ILS Configuration**.

Cisco UserSync Service

Cisco UserSync service synchronizes the data from Unified Communications Manager end-user table to the LDAP database.

Cisco UserLookup Web Service

Cisco UserLookup Web service routes the commercial calls (calls through external gateways) to an alternate internal number of the called party in order to avoid the commercial cost of calling an external number.

If a caller within a Unified Communications Manager network makes a call on an external number, Unified Communications Manager checks if an internal number exists for the called party in the LDAP database. If an internal number exists, the call is routed to that internal number. If the internal number is not found in the LDAP database, the call is routed to the original (external) number.

Cisco Headset Service

Cisco Headset Service enables you to manage inventory, configuration updates, and diagnostics data of your Cisco Headset if you use compatible Cisco IP Phones, Cisco Jabber, or other Cisco devices.

Note Cisco Headset service should be activated on all the Unified Communications Manager nodes wherever Cisco CallManager service is already running. Ensure that you activate the Cisco Headset service on the Unified Communications Manager nodes where you want to administer headsets using the Cisco Unified CM Administration interface. The Cisco CallManager service will be automatically activated when you enable the Cisco Headset service. Deactivate the Cisco CallManager service if you do not need it.

IM and Presence Services

IM and Presence services apply only to IM and Presence Service.

Cisco SIP Proxy

The Cisco SIP Proxy service is responsible for providing the SIP registrar and proxy functionality. This includes request routing, requestor identification, and transport interconnection.

Cisco Presence Engine

The Cisco Presence Engine collects, aggregates, and distributes user capabilities and attributes using the standards-based SIP and SIMPLE interface. It collects information about the availability status and communications capabilities of a user.

Cisco XCP Text Conference Manager

The Cisco XCP Text Conference Manager supports the chat feature. The chat feature allows users to communicate with each other in online chat rooms. It supports chat functionality using ad hoc (temporary) and permanent chat rooms, which remain on a Cisco-supported external database until they are deleted.

Cisco XCP Web Connection Manager

The Cisco XCP Web Connection Manager service enables browser-based clients to connect to IM and Presence Service.

Cisco XCP Connection Manager

The Cisco Unified Presence XCP Connection Manager enables XMPP clients to connect to the Cisco Unified Presence server.

Cisco XCP SIP Federation Connection Manager

The Cisco XCP SIP Federation Connection Manager supports interdomain federation with Microsoft OCS over the SIP protocol. You must also turn on this service when your deployment contains an intercluster connection between an IM and Presence Service Release 9.0 cluster, and a Cisco Unified Presence Release 8.6 cluster.

Cisco XCP XMPP Federation Connection Manager

The Cisco XCP XMPP Federation Connection Manager supports interdomain federation with third party enterprises such as IBM Lotus Sametime, Cisco Webex Meeting Center, and GoogleTalk over the XMPP protocol, as well as supports interdomain federation with another IM and Presence Service enterprise over the XMPP protocol.

Cisco XCP Message Archiver

The Cisco XCP Message Archiver service supports the IM Compliance feature. The IM Compliance feature logs all messages sent to and from the IM and Presence Service server, including point-to-point messages, and messages from ad hoc (temporary) and permanent chat rooms for the Chat feature. Messages are logged to an external Cisco-supported database.

Cisco XCP Directory Service

The Cisco XCP Directory Service supports the integration of XMPP clients with the LDAP directory to allow users to search and add contacts from the LDAP directory.

Cisco XCP Authentication Service

The Cisco XCP Authentication Service handles all authentication requests from XMPP clients that are connecting to IM and Presence Service.

CTI Services

This section describes the CTI Services and does not apply to Cisco Unity Connection or IM and Presence Service.

Cisco IP Manager Assistant

This service supports Cisco Unified Communications Manager Assistant. After service activation, Cisco Unified Communications Manager Assistant enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support.

The feature comprises a call-routing service, enhancements to phone capabilities for the manager, and desktop interfaces that are primarily used by the assistant.

The service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets on the basis of preconfigured call filters. The manager can change the call routing dynamically; for example, by pressing a softkey on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Unified Communications Manager users comprise managers and assistants. The routing service intercepts manager calls and routes them appropriately. An assistant user handles calls on behalf of a manager.

Cisco WebDialer Web Service

Cisco WebDialer Web Service for Cisco Unified Communications Manager Systems

Cisco Web Dialer provides click-to-dial functionality. It allows users inside a Unified Communications Manager cluster to initiate a call to other users inside or outside the cluster by using a web page or a desktop application. Cisco Web Dialer provides a web page that enables users to call each other within a cluster. Cisco Web Dialer comprises two components: WebDialer servlet and Redirector servlet.

The Redirector servlet provides the ability for third-party applications to use Cisco Web Dialer. The Redirector servlet finds the appropriate Unified Communications Manager cluster for the Cisco Web Dialer user and redirects the request to the Cisco Web Dialer in that cluster. The Redirector functionality applies only for HTTP/HTML-based WebDialer client applications because it is not available for Simple Object Access Protocol (SOAP)-based WebDialer applications.

Self-Provisioning IVR

With the introduction of Self-Provisioning IVR Service, the autoregistered IP phones on the Unified Communications Manager are assigned to users quickly with less effort. When you dial the CTI RP DN, that is configured on the Self-Provisioning page, from an extension of a user that uses the IVR service, the phone connects to the Self-Provisioning IVR application and prompts you to provide the Self-Service credentials. Based on the validation of the Self-Service credentials that you provide, the IVR service assigns the autoregistered IP phones to the users.

You can configure self-provisioning even if the service is deactivated, but the administrator cannot assign IP phones to users using the IVR service. By default, this service is deactivated.

To enable the Self-Provisioning IVR service, you must also enable the Cisco CTI Manager service.

For more information about how to configure self-provisioning, see the *Administration Guide for Cisco Unified Communications Manager* .

CDR Services

This section describes the CDR Services and does not apply to IM and Presence Service and Cisco Unity Connection.

CAR Web Service

The Cisco CAR Web Service loads the user interface for CAR, a web-based reporting application that generates either CSV or PDF reports by using CDR data.

Cisco SOAP - CDRonDemand Service

The Cisco SOAP - CDRonDemand Service, a SOAP/HTTPS-based service, runs on the CDR Repository server. It receives SOAP requests for CDR filename lists that are based on a user-specified time interval (up to a maximum of 1 hour) and returns a list of filenames that fit the time duration that is specified in the request. This service also receives requests for delivery of a specific CDR/CMR file with the filename and the transfer method (SFTP/FTP, server name, login info, directory) that is specified in the request.

If you are using a third-party billing application that accesses CDR data through an HTTPS/SOAP interface, activate this service.

For Unified Communications Manager Release 12.x and later releases, CDR onDemand Service is not enabled by default. If you want to enable the CDR onDemand service, the service should be activated manually. Execute the following command at the root level to activate the CDR onDemand service: `/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8443`.

Security Services

This section describes the Security Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CTL Provider

Unified Communications Manager only: The Cisco Certificate Trust List (CTL) Provider service, which runs with local system account privileges, works with the Cisco CTL Provider Utility, a client-side plug-in, to change the security mode for the cluster from nonsecure to mixed mode. When you install the plug-in, the Cisco CTL Provider service retrieves a list of all Unified Communications Manager and Cisco TFTP servers in the cluster for the CTL file, which contains a list of security tokens and servers in the cluster.

You can install and configure the Cisco CTL Client or the CLI command set **utils ctl**, and then activate this service for the clusterwide security mode to change from nonsecure to secure.

After you activate the service, the Cisco CTL Provider service reverts to the default CTL port, which is2444. If you want to change the port, see the *Cisco Unified Communications Manager Security Guide* for more information.

Cisco Certificate Authority Proxy Function (CAPF)

Working in conjunction with the Cisco Certificate Authority Proxy Function (CAPF) application, the CAPF service can perform the following tasks, depending on your configuration:

- Issue locally significant certificates to supported Cisco Unified IP Phone models.
- Upgrade existing certificates on the phones.
- Retrieve phone certificates for troubleshooting.
- Delete locally significant certificates on the phone.

Note Unified Communications Manager only: When you view real-time information in the Real-Time Monitoring Tool (RTMT), the CAPF service displays only for the first server.

Directory Services

This section describes the Directory Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco DirSync

Unified Communications Manager: The Cisco DirSync service ensures that the Unified Communications Manager database stores all user information. If you use an integrated corporate directory, for example, Microsoft Active Directory or Netscape/iPlanet Directory, with Unified Communications Manager, the Cisco DirSync service migrates the user data to the Unified Communications Manager database. The Cisco DirSync service does not synchronize the passwords from the corporate directory.

Note Users with duplicate email IDs are not synchronized and the administrator receives no notification about the list of users which are not synced. These IDS are shown in the DirSync error logs from Unified RTMT.

Cisco Unity Connection: When Cisco Unity Connection is integrated with an LDAP directory, the Cisco DirSync service synchronizes a small subset of user data (first name, last name, alias, phone number, and so on) in the Unified Communications Manager database on the Cisco Unity Connection server with the corresponding data in the LDAP directory. Another service (CuCmDbEventListener) synchronizes data in the Cisco Unity Connection user database with data in the Unified Communications Manager database. When a Cisco Unity Connection cluster is configured, the Cisco DirSync service runs only on the publisher server.

Location Based Tracking Services

This section describes Location Based Tracking Services.

Cisco Wireless Controller Synchronization Service

This service supports the Location Awareness feature, which provides a status of your network's wireless access points and associated mobile devices.

This service must be running to synchronize Unified Communications Manager with a Cisco wireless access point controller. When the service is running, and synchronization is configured, Unified Communications Manager syncs its database with a Cisco wireless access point controller and saves status information for the wireless access points that the controller manages. You can schedule syncs to occur at regular intervals so that the information stays current.

Note Make sure that this service is running when adding a new Cisco wireless access point controller.

Voice Quality Reporter Services

This section describes the Voice Quality Reporter Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco Extended Functions

The Cisco Extended Functions service provides support for Unified Communications Manager voice-quality features, including Quality Report Tool (QRT). For more information about individual features, see the *System Configuration Guide for Cisco Unified Communications Manager* and the *Cisco Unified IP PhoneAdministrationGuide for Cisco Unified Communications Manager*.

Network Services

Installed automatically, network services include services that the system requires to function, for example, database and platform services. Because these services are required for basic functionality, you cannot activate them in the Service Activation window. If necessary, for example, for troubleshooting purposes, you may need to stop and start (or restart) a network service in the Control Center - Network Services window.

After the installation of your application, network services start automatically, as noted in the Control Center - Network Services window. The serviceability GUI categorizes services into logical groups.

Performance and Monitoring Services

Cisco CallManager Serviceability RTMT

The Cisco CallManager Serviceability RTMT servlet supports the IM and Presence Real-Time Monitoring Tool (RTMT), which allows you to collect and view traces, view performance monitoring objects, work with alerts, and monitor system performance and performance counters, and so on.

Cisco RTMT Reporter Servlet

The Cisco RTMT Reporter servlet allows you to publish reports for RTMT.

Cisco Log Partition Monitoring Tool

The Cisco Log Partition Monitoring Tool service supports the Log Partition Monitoring feature, which monitors the disk usage of the log partition on a node (or all nodes in the cluster) by using configured thresholds and a polling interval.

Cisco Tomcat Stats Servlet

The Cisco Tomcat Stats Servlet allows you to monitor the Tomcat perfmon counters by using RTMT or the CLI. Do not stop this service unless you suspect that this service is using too many resources, such as CPU time.

Cisco RIS Data Collector

The Real-Time Information Server (RIS) maintains real-time information such as device registration status, performance counter statistics, critical alarms generated, and so on. The Cisco RIS Data Collector service provides an interface for applications, such as the IM and Presence Real-Time Monitoring Tool (RTMT), SOAP applications, and so on, to retrieve the information that is stored in all RIS nodes in the cluster.

Cisco AMC Service

Used for the Real-Time Monitoring Tool (RTMT), this service, Alert Manager and Collector service, allows RTMT to retrieve real-time information that exists on the server (or on all servers in the cluster).

Cisco Audit Event Service

The Cisco Audit Event Service monitors and logs any administrative configuration change to the Unified Communications Manager or IM and Presence system by a user or as a result of the user action. The Cisco Audit Event Service also monitors and logs end user events such as login, logout, and IM chat room entry and exit.

Backup and Restore Services

Cisco DRF Master

This does not apply to IM and Presence Service.

The CiscoDRF Master Agent service supports the DRF Master Agent, which works with the Disaster Recovery System GUI or CLI to schedule backups, perform restorations, view dependencies, check status of jobs, and cancel jobs, if necessary. The Cisco DRF Master Agent also provides the storage medium for the backup and restoration process.

Cisco DRF Local

The Cisco DRF Local service supports the Cisco DRF Local Agent, which acts as the workhorse for the DRF Master Agent. Components register with the Cisco DRF Local Agent to use the disaster recovery framework. The Cisco DRF Local Agent executes commands that it receives from the Cisco DRF Master Agent. Cisco DRF Local Agent sends the status, logs, and command results to the Cisco DRF Master Agent.

System Services

Cisco CallManager Serviceability

The Cisco CallManager Serviceability service supports Cisco Unified Serviceability and the IM and Presence Service serviceability GUIs, which are web application/interfaces that you use to troubleshoot issues and manage services. This service, which is installed automatically, allows you access to the serviceability GUIs. If you stop this service on the server, you cannot access the serviceability GUI when you browse into that server.

Cisco CDP

Cisco Discovery Protocol (CDP) advertises the voice application to other network management applications, so the network management application, for example, SNMP or Cisco Unified Operations Manager, can perform network management tasks for the voice application.

Cisco Trace Collection Servlet

The Cisco Trace Collection Servlet, along with the Cisco Trace Collection Service, supports trace collection and allows users to view traces by using RTMT. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Cisco Trace Collection Service

The Cisco Trace Collection Service, along with the Cisco Trace Collection Servlet, supports trace collection and allows users to view traces by using the RTMT client. If you stop this service on a server, you cannot collect or view traces on that server.

For SysLog Viewer and Trace and Log Central to work in RTMT, the Cisco Trace Collection Servlet and the Cisco Trace Collection Service must run on the server.

Tip If necessary, Cisco recommends that, to reduce the initialization time, you restart the Cisco Trace Collection Service before you restart Cisco Trace Collection Servlet.

Platform Services

A Cisco DB

A Cisco DB service supports the Progres database engine on Unified Communications Manager. On IM and Presence Service, A Cisco DB service supports the IDS database engine.

A Cisco DB Replicator

Unified Communications Manager and IM and Presence only: The A Cisco DB Replicator service ensures database configuration and data synchronization between the first and subsequent servers in the cluster.

Cisco Tomcat

The Cisco Tomcat service supports the web server.

SNMP Master Agent

This service, which acts as the agent protocol engine, provides authentication, authorization, access control, and privacy functions that relate to SNMP requests.

Tip After you complete SNMP configuration in the serviceability GUI, you must restart the SNMP Master Agent service in the **Control Center—Network Features** window.

MIB2 Agent

This service provides SNMP access to variables, which are defined in RFC 1213, that read and write variables, for example, system, interfaces, and IP.

Host Resources Agent

This service provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. This service implements the HOST-RESOURCES-MIB.

Native Agent Adaptor

This service, which supports vendor Management Information Bases (MIBs), allows you to forward SNMP requests to another SNMP agent that runs on the system.

For IM and Presence Service and Unified Communications Manager, this service will not be present if installed on a Virtual Machine.

System Application Agent

This service provides SNMP access to the applications that are installed and executing on the system. This implements the SYSAPPL-MIB.

Cisco CDP Agent

This service uses the Cisco Discovery Protocol to provide SNMP access to network connectivity information on the node. This service implements the CISCO-CDP-MIB.

Cisco Syslog Agent

This service supports gathering of syslog messages that various Unified Communications Manager components generate. This service implements the CISCO-SYSLOG-MIB.

Caution Stopping any SNMP service may result in loss of data because the network management system no longer monitors the network. Do not stop the services unless your technical support team tells you to do so.

Cisco Certificate Change Notification

This service keeps certificates of components like Tomcat, CallManager, and XMPP automatically synchronized across all nodes in the cluster. When the service is stopped and you regenerate certificates, then you have to manually upload them to Certificate Trust on the other nodes.

Platform Administrative Web Service

The Platform Administrative Web Service is a Simple Object Access Protocol (SOAP) API that can be activated on Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems to allow the PAWS-M server to upgrade the system.

Important Do not activate the Platform Administrative Web Service on the PAWS-M server.

Platform Communication Web Service

Platform Communication Web Service is a Representational State Transfer Protocol (REST) API which runs on Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection systems.

Note You cannot start or stop the **Platform Communication Web Service** manually.

Cisco Certificate Expiry Monitor

This service periodically checks the expiration status of certificates that the system generates and sends notification when a certificate is close to its expiration date. For Unified Communications Manager, you manage the certificates that use this service in Cisco Unified Operating System Administration. For IM and Presence Service, you manage the certificates that use this service in Cisco Unified IM and Presence Operating System Administration.

Cisco Smart License Manager

Cisco Smart License Manager is a network service that runs only on the publisher. It manages all the Cisco Smart Licensing operations on the Unified Communications Manager publisher. Cisco Smart License Manager service reports the product's license or entitlement usage to Cisco Smart Software Manager or Cisco Smart Software Manager satellite and gets the authorization status from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Security Services

Cisco Certificate Enrollment Service

This service creates an online connection between an online third-party CA and the Certificate Authority Proxy Function. This service must be activated in order to use an Online CA with the Certificate Authority Proxy Function for signing LSC certificates.

Cisco Trust Verification Service

This service is not supported by IM and Presence Service.

Cisco Trust Verification Service is a service running on a CallManager server or a dedicated server, that authenticates certificates on behalf of phones and other endpoints. It associates a list of roles for the owner of the certificate. A certificate or the owner can be associated with one or many roles.

The protocol between phones and Trust Verification Service allows phones to request for verification. Trust Verification Service validates the certificate and returns a list of roles associated with it. The protocol allows Trust Verification Service to authenticate a request and conversely, a phone to authenticate the response from Trust Verification Service. The protocol protects the integrity of the request and the response. Confidentiality of the request and the response is not required.

Multiples instances of Cisco Trust Verification Service run on different servers in the cluster to provide scalability. These servers may or may not be the same as the ones hosting the Cisco Unified CallManager. Phones obtain a list of Trust Verification Services in the network and connect to one of them using a selection algorithm (example: Round Robin). If the contacted Trust Verification Service does not respond, the phone switches to the next Trust Verification Service in the list.

Database Services

Cisco Database Layer Monitor

The Cisco Database Layer Monitor service monitors aspects of the database layer. This service handles change notification and monitoring.

Note Unified Communications Manager uses Automatic Update Statistics, an intelligent statistics update feature that monitors the changes that are made in the database tables and updates only tables that need statistic updates. This feature saves considerable bandwidth, especially on VMware deployments of Unified Communications Manager. Automatic Update Statistics is the default indexing method.

SOAP Services

Cisco SOAP-Real-Time Service APIs

IM and Presence Service only: The Cisco SOAP-Real-Time Service APIs support client login and third-party APIs for presence data.

Unified Communications Manager and Cisco Unity Connection only: The Cisco SOAP-Real-Time Service APIs allow you to collect real-time information for devices and CTI applications. This service also provides APIs for activating, starting, and stopping services.

Cisco SOAP-Performance-Monitoring APIs

The Cisco SOAP-Performance-Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs; for example, you can monitor memory information per service, CPU usage, and performance monitoring counters.

Cisco SOAP-Log-Collection APIs

The Cisco SOAP-Log-Collection APIs service allows you to collect log files and to schedule collection of log files on a remote SFTP server. Examples of log files that you can collect include syslog, core dump files, and Cisco application trace files.

SOAP-Diagnostic Portal Database Service

The Cisco Unified Real-Time Monitoring Tool (RTMT) uses the SOAP-Diagnostic Portal Database Service to access the RTMT Analysis Manager hosting database. RTMT gathers call records based on operator-defined filter selections. If this service is stopped, RTMT cannot collect the call records from the database.

CM Services

This section describes the Unified Communications Manager CM Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CallManager Personal Directory

The Cisco CallManager Personal Directory service supports Cisco Personal Directory.

In a Cisco Business Edition 5000 system, this service supports Unified Communications Manager only.

Cisco Extension Mobility Application

The Cisco Extension Mobility Application service allows you to define login settings such as duration limits on phone configuration for the Cisco Extension Mobility feature.

Unified Communications Manager only: The Cisco Extension Mobility feature allows users within a Unified Communications Manager cluster to temporarily configure another phone in the cluster as their own phone by logging in to that other phone. After a user logs in, the phone adopts the personal phone numbers, speed dials, services links, and other user-specific properties of the user. After logout, the phone adopts the original user profile.

Cisco CallManager Cisco IP Phone Services

The Cisco CallManager Cisco IP Phone Service initializes the service URLs for the Cisco Unified IP Phone services that you configured in Cisco Unified Communications Manager Administration.

In a Cisco Business Edition 5000 system, this service supports Unified Communications Manager only.

Cisco User Data Services

Cisco User Data Services provides Cisco Unified IP Phones with the ability to access user data from the Cisco Unified Communications Manager database. Cisco User Data Services provides support for Cisco Personal Directory.

Cisco Push Notification Service

The Cisco Push Notification Service provides functionality to send push notification for incoming calls to Apple iOS devices from Cisco Unified Communications Manager. This service relays push notification messages from the Cisco CallManager service to the Cisco Collaboration Cloud. This service also manages the access tokens used to send push notifications.

Cisco Headset Service

Cisco Headset Service enables you to manage inventory, configuration updates, and diagnostics data of your Cisco Headset if you use compatible Cisco IP Phones, Cisco Jabber, or other Cisco devices.

Note Cisco Headset service should be activated on all the Unified Communications Manager nodes wherever Cisco CallManager service is already running. Ensure that you activate the Cisco Headset service on the Unified Communications Manager nodes where you want to administer headsets using the Cisco Unified CM Administration interface. The Cisco CallManager service will be automatically activated when you enable the Cisco Headset service. Deactivate the Cisco CallManager service if you do not need it.

IM and Presence Service Services

IM and Presence Service services apply only to IM and Presence Service.

Cisco Login Datastore

The Cisco Login Datastore is a real-time database for storing client sessions to the Cisco Client Profile Agent.

Cisco Route Datastore

The Cisco Route Datastore is a real-time database for storing a cache of route information and assigned users for the Cisco SIP Proxy and the Cisco Client Profile Agent.

Cisco Config Agent

The Cisco Configuration Agent is a change-notification service that notifies the Cisco SIP Proxy of configuration changes in the IM and Presence Service IDS database.

Cisco Sync Agent

The Cisco Sync Agent keeps IM and Presence data synchronized with Unified Communications Manager data. It sends SOAP requests to the Unified Communications Manager for data of interest to IM and Presence and subscribes to change notifications from Unified Communications Manager and updates the IM and Presence IDS database.

Cisco OAM Agent

The Cisco OAM Agent service monitors configuration parameters in the IM and Presence Service IDS database that are of interest to the Presence Engine. When a change is made in the database, the OAM Agent writes a configuration file and sends an RPC notification to the Presence Engine.

Cisco Client Profile Agent

The Cisco Client Profile Agent service provides a secure SOAP interface to or from external clients using HTTPS.

Cisco Intercluster Sync Agent

The Cisco Intercluster Sync Agent service provides the following: DND propagation to Unified Communications Manager and syncs end user information between IM and Presence Service clusters for intercluster SIP routing.

Cisco XCP Router

The XCP Router is the core communication functionality on the IM and Presence Service server. It provides XMPP-based routing functionality on IM and Presence Service; it routes XMPP data to the other active XCP services on IM and Presence Service, and it accesses SDNS to allow the system to route XMPP data to IM and Presence Service users. The XCP router manages XMPP sessions for users, and routes XMPP messages to and from these sessions.

After IM and Presence Service installation, the system turns on Cisco XCP Router by default.

Note If you restart the Cisco XCP Router, IM and Presence Service automatically restarts all active XCP services. Note that you must select the Restart option to restart the Cisco XCP Router; this is not the same as turning off and turning on the Cisco XCP Router. If you turn off the Cisco XCP Router, rather than restart this service, IM and Presence Service stops all other XCP services. Subsequently when you turn on the XCP router, IM and Presence Service does not automatically turn on the other XCP services; you need to manually turn on the other XCP services.

Cisco XCP Config Manager

The Cisco XCP Config Manager service monitors the configuration and system topology changes made through the administration GUI (as well as topology changes that are synchronized from an InterCluster Peer) that affect other XCP components (for example, Router and Message Archiver), and updates these components as needed. The Cisco XCP Config Manager service creates notifications for the administrator indicating when an XCP component requires a restart (due to these changes), and it automatically clears the notifications after the restarts are complete.

Cisco Server Recovery Manager

The Cisco Server Recovery Manager (SRM) service manages the failover between nodes in a presence redundancy group. The SRM manages all state changes in a node; state changes are either automatic or initiated by the administrator (manual). Once you turn on high availability in a presence redundancy group, the SRM on each node establishes heartbeat connections with the peer node and begins to monitor the critical processes.

Cisco IM and Presence Data Monitor

The Cisco IM and Presence Data Monitor monitors IDS replication state on the IM and Presence Service. Other IM and Presence services are dependent on the Cisco IM and Presence Data Monitor. These dependent services use the Cisco service to delay startup until such time as IDS replication is in a stable state.

The Cisco IM and Presence Data Monitor also checks the status of the Cisco Sync Agent sync from Unified Communications Manager. Dependent services are only allowed to start after IDS replication has set up and the Sync Agent on the IM and Presence database publisher node has completed its sync from Unified Communications Manager. After the timeout has been reached, the Cisco IM and Presence Data Monitor on the Publisher node will allow dependent services to start even if IDS replication and the Sync Agent have not completed.

On the subscriber nodes, the Cisco IM and Presence Data Monitor delays the startup of feature services until IDS replication is successfully established. The Cisco IM and Presence Data Monitor only delays the startup of feature services on the problem subscriber node in a cluster, it will not delay the startup of feature services on all subscriber nodes due to one problem node. For example, if IDS replication is successfully established on node1 and node2, but not on node3, the Cisco IM and Presence Data Monitor allows feature services to start on node1 and node2, but delays feature service startup on node3.

Cisco Presence Datastore

The Cisco Presence Datastore is a real-time database for storing transient presence data and subscriptions.

Cisco SIP Registration Datastore

The Cisco Presence SIP Registration Datastore is a real-time database for storing SIP Registration data.

Cisco RCC Device Selection

The Cisco RCC Device Selection service is the Cisco IM and Presence user device selection service for Remote Call Control.

CDR Services

This section describes the CDR Services and does not apply to IM and Presence Service and Cisco Unity Connection.

Cisco CDR Repository Manager

This service maintains and moves the generated Call Detail Records (CDRs) that are obtained from the Cisco CDR Agent service. In a system that supports clusters (Unified Communications Manager only), the service exists on the first server.

Cisco CDR Agent

Note Unified Communications Manager supports Cisco CDR Agent in Cisco Unified Communications Manager systems.

This service does not support IM and Presence Service and Cisco Unity Connection.

The Cisco CDR Agent service transfers CDR and CMR files that are generated by Unified Communications Manager from the local host to the CDR repository server, where the CDR Repository Manager service runs over a SFTP connection.

This service transfers CDR and CMR files generated from the local host to the CDR repository server in a cluster. The CDR Agent in the CDR Repository Node standalone server transfers the files that are generated by the standalone server to the Cisco CDR Repository Manager over a SFTP connection. The CDR Agent maintains and moves the files.

For this service to work, activate the Cisco CallManager service on the server and ensure that it is running. If your configuration supports clusters (Unified Communications Manager only), activate the Cisco CallManager service on the first server.

Cisco CAR Scheduler

The Cisco CDR Analysis and Reporting (CAR) Scheduler service does not support IM and Presence Service and Cisco Unity Connection.

The Cisco CAR Scheduler service allows you to schedule CAR-related tasks; for example, you can schedule report generation or CDR file loading into the CAR database.

Cisco SOAP-CallRecord Service

The Cisco SOAP-CallRecord service runs by default on the publisher as a SOAP server, so that the client can connect to CAR database through the SOAP API. This connection happens through the use of the CAR connector (with a separate CAR IDS instance).

Cisco CAR DB

Cisco CAR DB manages the Informix instance for the CAR database, which allows Service Manager to start or stop this service and to bring up or shut down the CAR IDS instance respectively. This is similar to the Unified Communications Manager database that is used to maintain the CCM IDS instance.

The Cisco CAR DB service is activated on the publisher by default. The CAR DB instances are installed and actively run on the publisher, to maintain the CAR database. This network service is used only on the publisher and is not available on the subscribers.

Admin Services

This section describes the Admin Services and does not apply to Cisco Unity Connection.

Cisco CallManager Admin

The Cisco CallManager Admin service is not supported by IM and Presence Service and Cisco Unity Connection.

The Cisco CallManager Admin service supports Cisco Unified Communications Manager Administration, the web application/interface that you use to configure Unified Communications Manager settings. After the Unified Communications Manager installation, this service starts automatically and allows you to access the graphical user interface (GUI). If you stop this service, you cannot access the Cisco Unified Communications Manager Administration graphical user interface when you browse into that server.

Cisco IM and Presence Admin

The Cisco IM and Presence Admin service is not supported by Unified Communications Manager and Cisco Unity Connection.

The Cisco IM and Presence Admin service supports Cisco Unified Communications Manager IM and Presence Administration, the web application/interface that you use to configure IM and Presence Service settings. After the IM and Presence Service installation, this service starts automatically and allows you to access the GUI. If you stop this service, you cannot access the Cisco Unified Communications Manager IM and Presence Administration GUI when you browse into that server.

Services setup

Control Center

From Control Center in the serviceability GUI, you can view status and start and stop one service at a time. To start, stop, and restart network services, access the Control Center - Network Services window. To start, stop, and restart feature services, access the Control Center - Feature Services window.

Tip Use the Related Links drop-down list box and the Go button to navigate to Control Center and Service Activation windows.

Unified Communications Manager and IM and Presence only: In a cluster configuration, you can view status and start and stop services for one server in the cluster at a time.

Unified Communications Manager only: Starting and stopping a feature service causes all Cisco Unified IP Phones and gateways that are currently registered to that service to fail over to their secondary service. Devices and phones need to restart only if they cannot register with their secondary service. Starting and stopping a service may cause other installed applications (such as a conference bridge or Cisco Messaging Interface) that are homed to that Unified Communications Manager to start and stop as well.

Caution Unified Communications Manager only: Stopping a service also stops call processing for all devices that the service controls. When a service is stopped, calls from an IP phone to another IP phone stay up; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also stay up, but other types of calls drop.

Set Up Services

You can perform the following tasks when working with services:

Procedure

Step 1 Activate the feature services that you want to run.

Step 2 Configure the appropriate service parameters.

Step 3 If necessary, troubleshoot problems by using the serviceability GUI trace tools.

Service Activation

Note You can activate or deactivate multiple feature services or choose default services to activate from the Service Activation window in the serviceability GUI. You can view, start, and stop Unified Communications Manager services from an IM and Presence node and vice versa. You may encounter the following error: "Connection to the Server cannot be established (unable to access Remote Node)". If this error message appears, see the *Administration Guide for Cisco Unified Communications Manager*.

Note Starting with Unified Communications Manager Release 6.1.1, end users can no longer access Cisco Unified Serviceability to start and stop services.

Feature services are activated in automatic mode and the serviceability GUI checks for service dependencies based on a single-node configuration. When you choose to activate a feature service, you are prompted to select all the other services, if any, that depend on that service to run. When you click **Set Default**, the serviceability GUI chooses those services that are required to run on the server.

Unified Communications Manager and IM and Presence Service only: Even in a configuration that supports clusters, this process is based on a single-server configuration.

Activating a service automatically starts the service. You start and stop services from Control Center.

ClusterServiceActivationRecommendationsforCiscoUnifiedCommunications Manager

Before you activate services in a cluster, review the following table, which provides service recommendations for multiserver Unified Communications Manager configurations.

Table 34: Cisco Unified Communications Manager Service Activation Recommendations

Service/Servlet	Activation Recommendations
CM Services	
Cisco CallManager	This service supports Unified Communications Manager. In the Control Center - Network Services, ensure that the Cisco RIS Data Collector service Database Layer Monitor service are running on the node. **Tip** Before you activate this service, verify that the Unified Communications Mana server displays in the Unified Communications Manager Find/List window in Ci Unified Communications Manager Administration. If the server does not displ add the Unified Communications Manager server before you activate this servi For information on how to add a server, see the *System Configuration Guide fo Cisco Unified Communications Manager*.
Cisco Messaging Interface	Activate only if using an SMDI integration to a third-party Voicemail system using a server-attached USB-to-serial adapter.
Cisco Unified Mobile Voice Access Service	For mobile voice access to work, you must activate this service on the first node in the clus after you configure the H.323 gateway to point to the first VXML page. In addition, make s that the Cisco CallManager and the Cisco TFTP services run on one server in the cluster, no necessarily the same server where the Cisco Unified Mobile Voice Access Service runs.
Cisco IP Voice Media Streaming App	If you have more than one node in the cluster, activate on one or two servers per cluster. Yo may activate on a node that is dedicated specifically for music on hold. This service requires you activate Cisco TFTP on one node in the cluster. Do not activate this service on the first n or on any nodes that run the Cisco CallManager service.
Cisco CTIManager	Activate on each node to which JTAPI/TAPI applications will connect. CTIManager activa requires the Cisco CallManager service also to be activated on the node. See topics related CM services for more information on CTIManager and Cisco CallManager services interac
Cisco Extension Mobility	Activate on all nodes in the cluster.
Cisco Extended Functions	Activate this service, which supports the Quality Report Tool (QRT), on one or more servers run the Cisco RIS Data Collector. Make sure that you activate the Cisco CTIManager servic a node in the cluster.
Cisco DHCP Monitor Service	When the DHCP Monitor service is enabled, it detects changes in the database that affect II addresses for the IP phones, modifies the /etc/dhcpd.conf file, and stops and restarts the DH daemon with the updated configuration file. Activate this service on the node that has DHC enabled.

Service/Servlet	Activation Recommendations
Cisco Location Bandwidth Manager	If you plan to use Cisco Location Call Admission Control functionality to manage band allocation for audio and video calls, you must activate this service. This service works i conjunction with the Cisco CallManager service. It is recommended to run the Cisco Lo Bandwidth Manager on the same server that runs the Cisco CallManager service. If the L Bandwidth Manager is not running on the same server as the CallManager service, ensu you configure the Location Bandwidth Manager Group correctly.
Cisco Intercluster Lookup Service	If you plan to propagate the URI and numeric routing information between multiple Un Communications Manager clusters, you must activate this service on the publisher of th that participates in this exchange.
Cisco Dialed Number Analyzer Server	If you have more than one node in the cluster, activate this service on one node that is d specifically for the Cisco Dialed Number Analyzer service.
Cisco Dialed Number Analyzer	If you are planning to use Unified Communications Manager Dialed Number Analyzer, this service. This service may consume a lot of resources, so only activate this service o node with the least amount of call-processing activity or during off-peak hours.
Cisco TFTP	If you have more than one node in the cluster, activate this service on one node that is d specifically for the Cisco TFTP service. Configure Option 150 if you activate this servi more than one node in the cluster.
Cisco Headset Service	Activate this service if you plan to manage your Cisco headsets from Unified Communi Manager. **Note** Cisco Headset service should be activated on all the Unified Communicatio Manager nodes wherever Cisco CallManager service is already running. E that you activate the Cisco Headset service on the Unified Communications M nodes where you want to administer headsets using the Cisco Unified CM Administration interface. The Cisco CallManager service will be automati activated when you enable the Cisco Headset service. Deactivate the Cisco CallManager service if you do not need it.
CTI Services	
Cisco IP Manager Assistant	If you are planning to use Cisco Unified Communications Manager Assistant, activate thi on any two servers (Primary and Backup) in the cluster. Ensure that Cisco CTI Manage is activated in the cluster. See the *Feature Configuration Guide for Cisco Unified Communications Manager* for details on Cisco IP Manager Assistant.
Cisco WebDialer Web Service	Activate on one node per cluster.
Self-Provisioning IVR	To enable the Self-Provisioning IVR service, you must also enable the Cisco CTI Manage You can configure self-provisioning even if the service is deactivated, but the administr cannot assign IP phones to users using the IVR service. By default, this service is deact
CDR Services	

Service/Servlet	Activation Recommendations
Cisco SOAP-CDRonDemand Service	You can activate the Cisco SOAP-CDROnDemand Service only on the first server, and it requ that the Cisco CDR Repository Manager and Cisco CDR Agent services are running on the s server. For Unified Communications Manager Release 12.x and later releases, CDR onDemand Ser is not enabled by default. If you want to enable the CDR onDemand service, the service sho be activated manually. Execute the following command at the root level to activate the CDI onDemand service: `/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8`
Cisco CAR Web Service	You can activate the Cisco CAR Web Service only on the first server, and it requires that th Cisco CAR Scheduler service is activated and running on the same server and that the CDR Repository Manager service also is running on the same server.
Database and Admin Services	
Cisco AXL Web Service	Following installation, Cisco AXL Web Service is enabled by default on all cluster nodes. C recommends that you always leave the service activated on the publisher node. This ensures you are able to configure products that are dependent on AXL, such as Unified Provisionin Manager. Based on your needs, you can activate or deactivate the service on specific subscriber node Cisco Unified Serviceability under Feature Services.
Cisco Bulk Provisioning Service	You can activate the Cisco Bulk Provisioning Service only on the first node. If you use the I Administration Tool (BAT) to administer phones and users, you must activate this service.
Cisco UXL Web Service	This service performs authentication and user authorization checks. The TabSync client in C IP Phone Address Book Synchronizer uses the Cisco UXL Web Service for queries to the C Unified Communications Manager database. If you plan to use the Cisco IP Phone Address Book Synchronizer, you must activate this ser on one node, preferably publisher. If you are not using Cisco IP Phone Address Book Synchron then Cisco recommends that you deactivate this service . By default, this service is deactiva
Cisco Platform Administrative Web Service	You must activate this service if you plan to use a Cisco Prime Collaboration Deployment (P server to manage upgrades, switch version, restart or readdress operations. Platform Administra Web Service (PAWS) allows SOAP communication between the Call Manager and Prime Collaboration Deployment (PCD). If you have more than one node in the cluster, you must acti this service on each server in the cluster.
Cisco TAPS Service	Before you can use the Cisco Unified Communications Manager Auto-Register Phone Tool, must activate this service on the first node. When you create dummy MAC addresses for th Cisco Unified Communications Manager Auto-Register Phone Tool, ensure that the Cisco I Provisioning Service is activated on the same node.
Performance and Monitoring Services	
Cisco Serviceability Reporter	Activate on only the first node. **Note** The service only generates reports on the first node even if you activate the serv on other nodes.

Service/Servlet	Activation Recommendations
Cisco CallManager SNMP Service	If you use SNMP, activate this service on all servers in the cluster.
Security Services	
Cisco CTL Provider	Activate on all servers in the cluster.
Cisco Certificate Authority Proxy Function (CAPF)	Activate on only the first node.
Directory Services	
Cisco DirSync	Activate only on the first node.

Cluster Service Activation Recommendations for IM and Presence Service

Caution Before you turn on any services for a feature, you must complete all the required configuration on IM and Presence for that feature. See the relevant documentation for each IM and Presence feature.

Before you turn on services in a cluster, review the following table, which provides service recommendations for multinode IM and Presence configurations.

Table 35: IM and Presence Service Activation Recommendations

Service/Servlet	Recommendations
Database and Admin Services	
Cisco AXL Web Service	Following installation, Cisco AXL Web Service is enabled by default on all cluster nodes. Cisco recommends that you always leave the service activated on the IM and Presence Service database publisher node. This ensures that you are able to configure products that are dependent on AXL. If intercluster communication is configured, this service must be enabled on both nodes in the sub-cluster where remote peers are configured to sync from. If this service is not enabled on both nodes presence and IM capabilities will be lost in failover scenarios. Based on your needs, you can activate or deactivate the service on specific IM and Presence subscriber nodes in Cisco Unified Serviceability under Feature Services.

Service/Servlet	Recommendations
Cisco Bulk Provisioning Service	• You turn on the Cisco Bulk Provisioning Service only on the first node. • If you use the Bulk Administration Tool (BAT) to administer users, you must turn on this service.
Performance and Monitoring Services	
Cisco Serviceability Reporter	Turn on this service on the publisher node only. **Note** The service only generates reports on the publisher node even if you turn on the service on other nodes.
IM and Presence Services	
Cisco SIP Proxy	Turn on this service on all nodes in the cluster.
Cisco Presence Engine	Turn on this service on all nodes in the cluster.
Cisco Sync Agent	Turn on this service on all nodes in the cluster.
Cisco XCP Text Conference Manager	• Turn on this service if you deploy the chat feature on IM and Presence. • Turn on this service on each node that runs the chat feature. **Note** The permanent chat feature requires an external database. If you enable the permanent chat feature, you must also configure an external database before starting the Text Conference Manager service. The Text Conference Manager service will not start if the permanent chat feature is enabled and an external database is not configured. See the *Database Setup Guide for IM and Presence on Unified Communications Manager*.
Cisco XCP Web Connection Manager	• Turn on this service if you integrate web clients with IM and Presence. • Turn on this service on all nodes in the cluster.
Cisco XCP Connection Manager	• Turn on this service if you integrate XMPP clients with IM and Presence. • Turn on this service on all nodes in the cluster.

Service/Servlet	Recommendations
Cisco XCP SIP Federation Connection Manager	Turn on this service if you deploy any of the following configurations: • Interdomain federation over the SIP protocol on IM and Presence. Turn on this service on each node that runs SIP federation. • Intercluster deployment between a IM and Presence Release 9.x cluster and a Cisco Unified Presence Release 8.6(x) cluster. Turn on this service on all nodes in the Release 9.x cluster.
Cisco XCP XMPP Federation Connection Manager	• Turn on this service only if you deploy interdomain federation over the XMPP protocol on IM and Presence. • Turn on this service on each node that runs XMPP federation. **Note** Before you turn on the XMPP Federation Connection Manager service on a node, you must turn on XMPP Federation in Cisco Unified Communications Manager IM and Presence Administration on that node. See *Interdomain Federation for IM and Presence on Unified Communications Manager*.
Cisco XCP Message Archiver	• Turn on this service if you deploy the Compliance feature on IM and Presence. • Turn on this service on any node that runs the IM Compliance feature. **Note** If you turn on the Message Archiver before you configure an external database, the service will not start. Also, if the external database is not reachable, the service will not start. See the *Database Setup Guide for IM and Presence on Unified Communications Manager*.

Service/Servlet	Recommendations
Cisco XCP Directory Service	• Turn on this service if you integrate XMPP clients on IM and Presence with an LDAP directory. • Turn on this service on all nodes in the cluster. **Note** If you turn on the Directory Service before you configure the LDAP contact search settings for third-party XMPP clients, the service will start, and then stop again. See *Configuration and Administration of IM and Presence Service on Unified Communications Manager*.
Cisco XCP Authentication Service	• Turn on this service if you integrate XMPP clients with IM and Presence. • Turn on this service on all nodes in the cluster.

Activate Feature Services

You activate and deactivate feature services in the **Service Activation** window in the serviceability GUI. Services that display in the **Service Activation** window do not start until you activate them.

You can activate and deactivate only features services (not network services). You may activate or deactivate as many services as you want at the same time. Some feature services depend on other services, and the dependent services get activated before the feature service activates.

Tip Unified Communications Manager and IM and Presence Service only: Before you activate services in the Service Activation window, review topics related to cluster service activation recommendations.

Procedure

Step 1 Choose **Tools** > **Service Activation**.

The **Service Activation** window displays.

Step 2 Select the server (node) from the **Server** drop-down list, and then click **Go**.

You can access Unified Communications Manager services from an IM and Presence Service node and vice versa. You may encounter the following error when trying to access a remote node: "Connection to the Server cannot be established (unable to connect to Remote Node)". If this error message appears, see the *Administration Guide for Cisco Unified Communications Manager*.

Step 3 Perform one of the following actions to turn on or turn off services:

a) To turn on the default services required to run on a single server, select **Set to Default**.

Note This option selects default services based on the configuration of a single server, and checks for service dependencies.

b) To turn on all services, check **Check All Services**.
c) To turn on a specific service, check the check box for the service that you want to turn on
d) To turn off a service, uncheck the check box for the services that you want to turn off.

Step 4 Unified Communications Manager and IM and Presence Service only: For a cluster configuration, review the cluster service activation recommendations, and then check the check boxes next to the services that you want to activate.

Step 5 After you check the check boxes for the services that you want to activate, click **Save**.

Tip To deactivate services that you activated, uncheck the check boxes next to the services that you want to deactivate; then, click **Save**.

Tip To obtain the latest status of the services, click the **Refresh** button.

Related Topics

Cluster Service Activation Recommendations for Cisco Unified Communications Manager, on page 208
Cluster Service Activation Recommendations for IM and Presence Service, on page 211

Start, Stop, and Restart Services in Control Center or CLI

To perform these tasks, the serviceability GUI provides two Control Center windows. To start, stop, and restart network services, access the **Control Center—Network Services** window. To start, stop, and restart feature services, access the **Control Center—Feature Services** window.

Tip Use the **Related Links** list box and the **Go** button to navigate to Control Center and Service Activation windows.

Start, Stop, and Restart Services in Control Center

Control Center in the serviceability GUI allows you to:

- view status
- refresh status
- start, stop, and restart feature and network services on a particular server, or for a server in a cluster in a cluster configuration

When a service is stopping, you cannot start it until after the service is stopped.

Caution Unified Communications Manager only: Stopping a service also stops call processing for all devices that the service controls. When a service is stopped, calls from an IP phone to another IP phone remain connected; calls in progress from an IP phone to a Media Gateway Control Protocol (MGCP) gateway also remain connected, but other types of calls get dropped.

Procedure

Step 1 Depending on the service type that you want to start/stop/restart/refresh, perform one of the following tasks:

- Choose **Tools** > **Control Center - Feature Services**.

  Tip Before you can start, stop, or restart a feature service, it must be activated.

- Choose **Tools** > **Control Center - Network Services**.

Step 2 Choose the server from the Server drop-down list, and then click **Go**.

The window displays the following items:

- The service names for the server that you chose.
- The service group.
- The service status, for example, Started, Running, Not Running, and so on. (Status column).
- The exact time that the service started running. (Start Time column).
- The amount of time that the service has been running. (Up Time column).

Step 3 Perform one of the following tasks:

- Click the radio button next to the service that you want to start, and then click **Start**. The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to stop, and then click **Stop**. The Status changes to reflect the updated status.
- Click the radio button next to the service that you want to restart, and then click **Restart**. A message indicates that restarting may take a while. Click **OK**.
- Click **Refresh** to get the latest status of the services.
- To go to the **Service Activation** window or to the other Control Center window, choose an option from the Related Links drop-down list, and then click **Go**.

Start, Stop, and Restart Services Using Command Line Interface

You can start and stop some services through the CLI. For a list of services that you can start and stop through the CLI and for information on how to perform these tasks, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Tip You must start and stop most services from Control Center in the serviceability GUI.

CHAPTER 16

Trace

Trace

Cisco Unified Serviceability provides trace tools to assist you in troubleshooting issues with your voice application. Cisco Unified Serviceability supports SDI (System Diagnostic Interface) trace, SDL (Signaling Distribution Layer) trace (for Cisco CallManager and Cisco CTIManager services, applicable to Unified Communications Manager only), and Log4J trace (for Java applications).

You use the Trace Configuration window to specify the level of information that you want traced as well the type of information that you want to be included in each trace file.

Unified Communications Manager only: If the service is a call-processing application such as Cisco CallManager or Cisco CTIManager, you can configure a trace on devices such as phones and gateway.

Unified Communications Manager only: In the Alarm Configuration window, you can direct alarms to various locations, including SDL trace log files. If you want to do so, you can configure trace for alerts in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT).

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool.

Cisco Unified IM and Presence Serviceability provides trace tools to assist you in troubleshooting issues with your instant messaging and presence application. Cisco Unified IM and Presence Serviceability supports:

- SDI trace
- Log4J trace (for Java applications)

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files). You can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

In the **Alarm Configuration** window, you can direct alarms to various locations. If you want to do so, you can configure trace for alerts in the IM and Presence Unified RTMT.

After you have configured information that you want to include in the trace files for the various services, you can collect and view trace files by using the Trace and Log Central option in the Unified RTMT. You can configure trace parameters for any feature or network service that is available on any IM and Presence node in the cluster. Use the **Trace Configuration** window to specify the parameters that you want to trace for troubleshooting problems. If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the **Troubleshooting Trace Setting** window.

Note Enabling Trace decreases system performance; therefore, enable Trace only for troubleshooting purposes. For assistance in using Trace, contact Cisco Technical Assistance Center (TAC).

Trace Configuration

You can configure trace parameters for any feature or network service that displays in the Serviceability interface. If you have clusters, you can configure trace parameters for any feature or network service that is available on any server in the cluster. Use the Trace Configuration window to specify the parameters that you want to trace for troubleshooting problems.

You can configure the level of information that you want traced (debug level), what information you want to trace (trace fields), and information about the trace files (such as number of files per service, size of file, and time that the data is stored in the trace files). If you have clusters, you can configure trace for a single service or apply the trace settings for that service to all servers in the cluster.

If you want to use predetermined troubleshooting trace settings rather than choosing your own trace fields, you can use the Troubleshooting Trace window. For more information on troubleshooting trace, see Trace settings.

After you have configured information that you want to include in the trace files for the various services, you can collect trace files by using the trace and log central option in Unified RTMT. For more information regarding trace collection, see Trace collection.

Trace Settings

The Troubleshooting Trace Settings window allows you to choose the services for which you want to set predetermined troubleshooting trace settings. In this window, you can choose a single service or multiple services and change the trace settings for those services to the predetermined trace settings. If you have clusters, you can choose the services on different servers in the cluster, so the trace settings of the chosen services get changed to the predetermined trace settings. You can choose specific activated services for a single server, all activated services for the server, specific activated services for all servers in the cluster, or all activated services for all servers in the cluster. In the window, N/A displays next to inactive services.

Note The predetermined troubleshooting trace settings for a feature or network service include SDL, SDI, and Log4j trace settings. Before the troubleshooting trace settings are applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings are restored.

When you open the Troubleshooting Trace Settings window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. In the Troubleshooting Trace Settings window, you can reset the trace settings to the original settings.

After you apply Troubleshooting Trace Setting to a service, the Trace Configuration window displays a message that troubleshooting trace is set for that service. From the Related Links drop-down list box, you can choose the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the Trace Configuration window displays all the settings as read-only, except for some parameters of trace output settings, for example, Maximum No. of Files. You can modify these parameters even after you apply troubleshooting trace settings.

Trace Collection

Use Trace and Log Central, an option in the Cisco Unified Real-Time Monitoring Tool, to collect, view, and zip various service traces or other log files. With the Trace and Log Central option, you can collect SDL/SDI traces, Application Logs, System Logs (such as Event View Application, Security, and System logs), and crash dump files.

Tip Do not use Windows NotePad to view collected trace files to view collected trace files, because Windows NotePad does not properly display line breaks.

Note Unified Communications Manager only: For devices that support encryption, the Secure Real-time Transport Protocol (SRTP) keying material does not display in the trace file.

For more information about trace collection, see *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Called Party Tracing

Called Party Tracing allows you to configure a directory number or list of directory numbers that you want to trace. You can request on-demand tracing of calls using the Session Trace Tool.

For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Set Up Trace Configuration

The following procedure provides an overview of the steps to configure and collect trace for feature and network services in the Serviceability interface.

Procedure

Step 1 Configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service) by performing one of these steps:

- Cisco Unified Communications Manager Administration and Cisco Unified IM and Presence: Select **System** > **ServiceParameters** and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).

- Cisco Unity Connection only: Select **System Settings** > **Service Parameters**in Cisco Unity Connection Administration and configure the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).

Step 2 Configure the trace setting for the service for which you want to collect traces. If you have clusters, you can configure trace for the service on one server or on all servers in the cluster.

To configure trace settings, choose what information you want to include in the trace log by choosing the debug level and trace fields.

If you want to run predetermined traces on services, set troubleshooting trace for those services.

Step 3 Install the Cisco Unified Real-Time Monitoring Tool on a local PC.

Step 4 If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert in Unified RTMT.

You can find the LogFileSearchStringFound alarm in the LpmTctCatalog. (Select**Alarms** > **Definitions**. In the Find alarms where drop-down list box, choose the **System Alarm Catalog**; in the Equals drop-down list box, choose **LpmTctCatalog**).

Step 5 If you want to automatically capture traces for alerts such as CriticalServiceDownand CodeYellow, check the **Enable Trace Download** check box in the Set Alert/Properties dialog box for the specific alert in Unified RTMT; configure how often that you want the download to occur.

Step 6 Collect the traces.

Step 7 View the log file in the appropriate viewer.

Step 8 If you enabled troubleshooting trace, reset the trace settings services, so the original settings are restored.

Note Leaving troubleshooting trace enabled for a long time increases the size of the trace files and may affect the performance of the services.

Configure Trace

This section provides information for configuring trace settings.

Note Enabling trace decreases system performance; therefore, enable trace only for troubleshooting purposes. For assistance in using trace, contact your technical support team.

Set Up Trace Parameters

This section describes how to configure trace parameters for feature and network services that you manage through the Serviceability GUI.

Tip For Cisco Unity Connection, you may need to run trace in Cisco Unified Serviceability and Cisco Unity Connection Serviceability to troubleshoot Cisco Unity Connection issues. For information on how to run trace in Cisco Unity Connection Serviceability, refer to the *Cisco Unity Connection Serviceability Administration Guide* .

Procedure

Step 1 Select **Trace** > **Configuration**.

The Trace Configuration window displays.

Step 2 From the Server drop-down list box, select the server that is running the service for which you want to configure trace; then, click **Go**.

Step 3 From the Service Group drop-down list box, select the service group for the service that you want to configure trace; then, click **Go**.

Tip The Service Groups in Trace Configuration table lists the services and trace libraries that correspond to the options that display in the Service Group drop-down list box.

Step 4 From the Service drop-down list box, select the service for which you want to configure trace and, click **Go**.

The drop-down list box displays active and inactive services.

Tip Cisco Unity Connection only: For the Cisco CallManager and CTIManager services, you can configure SDL trace parameters. To do so, open the Trace Configuration window for one of those services, and click the **Go** button that is next to the Related Links drop-down list box.

If you configured Troubleshooting Trace for the service, a message displays at the top of the window that indicates that the Troubleshooting Traces feature is set, which means that the system disables all fields in the Trace Configuration window except for Trace Output Settings. To configure the Trace Output Settings, go to Step 11. To reset Troubleshooting Trace, see the Set up troubleshooting trace settings.

The trace parameters display for the service that you chose. In addition, the Apply to All Nodes check box displays (Unified Communications Manager only).

Step 5 Unified Communications Manager and IM and Presence only: If you want to do so, you can apply the trace settings for the service or trace library to all servers in the cluster by checking the **Apply to All Nodes** check box; that is, if your configuration supports clusters.

Step 6 Check the **Trace On** check box.

Step 7 Cisco Unity Connection only: If you are configuring SDL trace parameters, go to Step 10.

Step 8 Select the level of information that you want traced from the **Debug Trace Level** list box, as described in Debug trace level settings.

Step 9 Check the **Trace Fields** check box for the service that you chose, for example, Cisco Log Partition Monitoring Tool Trace Fields.

Step 10 If the service does not have multiple trace settings where you can specify the traces that you want to activate, check the **Enable All Trace** check box. If the service that you chose has multiple trace settings, check the check boxes next to the trace check boxes that you want to enable, as described in Trace field descriptions.

Step 11 To limit the number and size of the trace files, specify the trace output setting. See Trace Ouput Settings for descriptions.

Step 12 To save your trace parameters configuration, click the **Save** button.

The changes to trace configuration take effect immediately for all services except Cisco Messaging Interface (Unified Communications Manager only). The trace configuration changes for Cisco Messaging Interface take effect in 3 to 5 minutes.

Note To set the default, click the **Set Default** button.

Service Groups in Trace Configuration

The following table lists the services and trace libraries that correspond to the options in the Service Group drop-down list box in the Trace Configuration window.

Table 36: Service Groups in Trace Configuration

Service Group	Services and Trace Libraries	Notes
Unified Communications Manager CM Services	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP Phone Service • Cisco DHCP Monitor Service • Cisco Dialed Number Analyzer • Cisco Dialed Number Analyzer Server • Cisco Extended Functions, Cisco Extension Mobility • Cisco Extension Mobility Application • Cisco IP Voice Media Streaming App • Cisco Messaging Interface • Cisco TFTP • Cisco Unified Mobile Voice Access Service	For most services in the CM Services group, you run trace for specific components, instead of enabling all trace for the service. The Trace field descriptions lists the services for which you can run trace for specific components.
Unified Communications Manager CTI Services	• Cisco IP Manager Assistant • Cisco Web Dialer Web Service	For these services, you can run trace for specific components, instead of enabling all trace for the service; see the Trace field descriptions.

Service Group	Services and Trace Libraries	Notes
Unified Communications Manager CDR Services	• Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler • Cisco Unified Communications Manager CDR Analysis and Reporting Web Service • Cisco CDR Agent • Cisco CDR Repository Manager	You enable all trace for each service, instead of running trace for specific components. In Cisco Unified Communications Manager CDR Analysis and Reporting, when reports are run that call stored procedures, Cisco Unified Communications Manager CDR Analysis and Reporting checks the configured debug trace level for the Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler service and the Cisco Unified Communications Manager CDR Analysis and Reporting Web Service in the Trace Configuration window before stored procedure logging begins. For pregenerated reports, Cisco Unified Communications Manager CDR Analysis and Reporting checks the level for the Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler service; for on-demand reports, Cisco Unified Communications Manager CDR Analysis and Reporting checks the level for the Cisco Unified Communications Manager CDR Analysis and Reporting Web Service. If you choose Debug from the Debug Trace Level drop-down list box, stored procedure logging gets enabled and continues until you choose another option from the drop-down list box. The following Cisco Unified Communications Manager CDR Analysis and Reporting reports use stored procedure logging: Gateway Utilization report, Route and Line Group Utilization report, Route/Hunt List Utilization report, Route Pattern/Hunt Pilot Utilization report, Conference Call Details report, Conference Call Summary report, Conference Bridge Utilization report, Voice Messaging Utilization report, and the CDR Search report.

Service Group	Services and Trace Libraries	Notes
IM and Presence Services	• Cisco Client Profile Agent • Cisco Config Agent • Cisco Intercluster Sync Agent • Cisco Login Datastore • Cisco OAM Agent • Cisco Presence Datastore • Cisco Presence Engine • Cisco IM and Presence Data Monitor • Cisco Route Datastore • Cisco SIP Proxy • Cisco SIP Registration Datastore • Cisco Server Recovery Manager • Cisco Sync Agent • Cisco XCP Authentication Service • Cisco XCP Config Manager • Cisco XCP Connection Manager • Cisco XCP Directory Service • Cisco XCP Message Archiver • Cisco XCP Router • Cisco XCP SIP Federation Connection Manager • Cisco XCP Text Conference Manager • Cisco XCP Web Connection Manager • Cisco XCP XMPP Federation Connection Manager	See topics related to feature and network services in Cisco Unified IM and Presence Serviceability for a description of these services. • For these services, you should enable all trace for the service, instead of running trace for specific components.

Service Group	Services and Trace Libraries	Notes
Database and Admin Services	Unified Communications Manager and Cisco Unity Connection: - Cisco AXL Web Service - Cisco CCM DBL Web Library - Cisco CCMAdmin Web Service - Cisco CCMUser Web Service - Cisco Database Layer Monitor - Cisco UXL Web Service Unified Communications Manager - Cisco Bulk Provisioning Service - Cisco GRT Communications Web Service - Cisco Role-based Security - Cisco TAPS Service - Cisco Unified Reporting Web Service IM and Presence Services: - Cisco AXL Web Service - Cisco Bulk Provisioning Service - Cisco CCMUser Web Service - Cisco Database Layer Monitor - Cisco GRT Communications Web Service - Cisco IM and Presence Admin - Cisco Unified Reporting Web Service - Platform Administrative Web Service	Choosing the Cisco CCM DBL Web Library option activates the trace for database access for Java applications. For database access for C++ applications, activate trace for Cisco Database Layer Monitor, as described in the Cisco Extended Functions trace fields. Choosing the Cisco Role-based Security option, which supports Unified Communications Manager, activates trace for user-role authorization. For most services in the Database and Admin Services group, you enable all trace for the service/library, instead of enabling trace for specific components. For Cisco Database Layer Monitor, you can run trace for specific components. **Note** You can control logging for services in the Cisco Unified IM and Presence Serviceability UI. To change the log level, select the System Services group and Cisco CCMService Web Service.

Service Group	Services and Trace Libraries	Notes
Performance and Monitoring Services	Unified Communications Manager and Cisco Unity Connection: • Cisco AMC Service • Cisco CCM NCS Web Library • CCM PD Web Service • Cisco CallManager SNMP Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco Audit Event Service • Cisco RisBean Library Unified Communications Manager: • Cisco CCM PD Web Service IM and Presence Services: • Cisco AMC Service • Cisco Audit Event Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco RisBean Library	Choosing the Cisco CCM NCS Web Library option activates trace for database change notification for the Java client. Choosing the Cisco Unity RTMT Web Service option activates trace for the Unity RTMT servlets; running this trace creates the server-side log for Unity RTMT client queries.
Unified Communications Manager Security Services	• Cisco CTL Provider • Cisco Certificate Authority Proxy Function • Cisco Trust Verification Service	You enable all trace for each service, instead of running trace for specific components.
Unified Communications Manager Directory Services	Cisco DirSync	You enable all trace for this service, instead of running trace for specific components.
Backup and Restore Services	• Cisco DRF Local • Unified Communications Manager and Cisco Unity Connection only: Cisco DRF Master	You enable all trace for each service, instead of running trace for specific components.

Service Group	Services and Trace Libraries	Notes
System Services	Unified Communications Manager: • Cisco CCMRealm Web Service • Cisco CCMService Web Service • Cisco Common User Interface • Cisco Trace Collection Service IM and Presence Services: • Cisco CCMService Web Service • Cisco Trace Collection Service	Choosing the Cisco CCMRealm Web Service option activates trace for login authentication. Choosing the Cisco Common User Interface option activates trace for the common code that multiple applications use; for example, Cisco Unified Operating System Administration and Cisco Unified Serviceability. Choosing the Cisco CCMService Web Service option activates trace for the Cisco Unified Serviceability web application (GUI). You enable all trace for each option/service, instead of running trace for specific components.
SOAP Services	• CiscoSOAP Web Service • CiscoSOAPMessage Service	Choosing the Cisco SOAP Web Service option activates the trace for the AXL Serviceability API. You enable all trace for this service, instead of running trace for specific components.
Platform Services	Cisco Unified OS Admin Web Service	The Cisco Unified OS Admin Web Service supports Cisco Unified Operating System Administration, which is the web application that provides management of platform-related functionality such as certificate management, version settings, and installations and upgrades. You enable all trace for this service, instead of running trace for specific components.

Debug Trace Level Settings

The following table describes the debug trace level settings for services.

Table 37: Debug Trace Levels for Services

Level	Description
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.
Special	Traces all Error conditions plus process and device initialization messages.
State Transition	Traces all Special conditions plus subsystem state transitions that occur during normal operation. Traces call-processing events.
Significant	Traces all State Transition conditions plus media layer events that occur during normal operation.

Level	Description
Entry/Exit	**Note** Not all services use this trace level. Traces all Significant conditions plus entry and exit points of routines.
Arbitrary	Traces all Entry/Exit conditions plus low-level debugging information.
Detailed	Traces all Arbitrary conditions plus detailed debugging information.

The following table describes the debug trace level settings for servlets.

Table 38: Debug Trace Levels for Servlets

Level	Description
Fatal	Traces very severe error events that may cause the application to abort.
Error	Traces alarm conditions and events. Used for all traces that are generated in abnormal path.
Warn	Traces potentially harmful situations.
Info	Traces the majority of servlet problems and has a minimal effect on system performance.
Debug	Traces all State Transition conditions plus media layer events that occur during normal operation. Trace level that turns on all logging.

Trace Field Descriptions

For some services, you can activate trace for specific components, instead of enabling all trace for the service. The following list includes the services for which you can activate trace for specific components. Clicking one of the cross-references takes you to the applicable section where a description displays for each trace field for the service. If a service does not exist in the following list, the Enable All Trace check box displays for the service in the Trace Configuration window.

The following services are applicable to Unified Communications Manager and Cisco Unity Connection:

- Database layer monitor trace fields
- Cisco RIS data collector trace fields

The following services are applicable to Unified Communications Manager:

- Cisco CallManager SDI trace fields
- Cisco CallManager SDL trace fields

- Cisco CTIManager SDL trace fields
- Cisco Extended Functions trace fields
- Cisco Extension Mobility trace fields
- Cisco IP manager assistant trace fields
- Cisco IP voice media streaming app trace fields
- Cisco TFTP trace fields
- Cisco Web Dialer web service trace fields

Database Layer Monitor Trace Fields

The following table describes the Cisco Database Layer Monitor trace fields. The Cisco Database Layer Monitor service supports Unified Communications Manager and Cisco Unity Connection.

Table 39: Cisco Database Layer Monitor Trace Fields

Field Name	Description
Enable DB Library Trace	Activates database library trace for C++ applications.
Enable Service Trace	Activates service trace.
Enable DB Change Notification Trace	Activates the database change notification traces for C++ applications.
Enable Unit Test Trace	Do not check this check box. Cisco engineering uses it for debugging purposes.

Cisco RIS Data Collector Trace Fields

The following table describes the Cisco RIS Data Collector trace fields. The Cisco RIS Data Collector service supports Unified Communications Manager and Cisco Unity Connection.

Table 40: Cisco RIS Data Collector Trace Fields

Field Name	Description
Enable RISDC Trace	Activates trace for the RISDC thread of the RIS data collector service (RIS).
Enable System Access Trace	Activates trace for the system access library in the RIS data collector.
Enable Link Services Trace	Activates trace for the link services library in the RIS data collector.
Enable RISDC Access Trace	Activates trace for the RISDC access library in the RIS data collector.

Field Name	Description
Enable RISDB Trace	Activates trace for the RISDB library in the RIS data collector.
Enable PI Trace	Activates trace for the PI library in the RIS data collector.
Enable XML Trace	Activates trace for the input/output XML messages of the RIS data collector service.
Enable Perfmon Logger Trace	Activates trace for the troubleshooting perfmon data logging in the RIS data collector. Used to trace the name of the log file, the total number of counters that are logged, the names of the application and system counters and instances, calculation of process and thread CPU percentage, and occurrences of log file rollover and deletion.

Cisco CallManager SDI Trace Fields

The following table describes the Cisco CallManager SDI trace fields. The Cisco CallManager service supports Unified Communications Manager.

Table 41: Cisco CallManager SDI Trace Fields

Field Name	Description
Enable H245 Message Trace	Activates trace of H245 messages.
Enable DT-24+/DE-30+ Trace	Activates the logging of ISDN type of DT-24+/DE-30+ device traces.
Enable PRI Trace	Activates trace of primary rate interface (PRI) devices.
Enable ISDN Translation Trace	Activates ISDN message traces. Used for normal debugging.
Enable H225 & Gatekeeper Trace	Activates trace of H.225 devices. Used for normal debugging.
Enable Miscellaneous Trace	Activates trace of miscellaneous devices. **Note** Do not check this check box during normal system operation.
Enable Conference Bridge Trace	Activates trace of conference bridges. Used for normal debugging.

Field Name	Description
Enable Music on Hold Trace	Activates trace of music on hold (MOH) devices. Used to trace MOH device status such as registered with Unified Communications Manager, unregistered with Unified Communications Manager, and resource allocation processed successfully or failed.
Enable Unified CM Real-Time Information Server Trace	Activates Unified Communications Manager real-time information traces that the real-time information server uses.
Enable SIP Stack Trace	Activates trace of SIP stack. The default is enabled.
Enable Annunciator Trace	Activates trace for the annunciator, a SCCP device that uses the Cisco IP Voice Media Streaming Application service to enable Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices.
Enable CDR Trace	Activates traces for CDR.
Enable Analog Trunk Trace	Activates trace of all analog trunk (AT) gateways.
Enable All Phone Device Trace	Activates trace of phone devices. Trace information includes SoftPhone devices. Used for normal debugging.
Enable MTP Trace	Activates trace of media termination point (MTP) devices. Used for normal debugging.
Enable All Gateway Trace	Activates trace of all analog and digital gateways.
Enable Forward and Miscellaneous Trace	Activates trace for call forwarding and all subsystems that are not covered by another check box. Used for normal debugging.
Enable MGCP Trace	Activates trace for media gateway control protocol (MGCP) devices. Used for normal debugging.
Enable Media Resource Manager Trace	Activates trace for media resource manager (MRM) activities.
Enable SIP Call Processing Trace	Activates trace for SIP call processing.
Enable SCCP Keep Alive Trace	Activates trace for SCCP keepalive trace information in the Cisco CallManager traces. Because each SCCP device reports keepalive messages every 30 seconds, and each keepalive message creates 3 lines of trace data, the system generates a large amount of trace data when this check box is checked.

Field Name	Description
Enable SIP Keep Alive (REGISTER Refresh) Trace	Activates trace for SIP keepalive (REGISTER refresh) trace information in the Cisco CallManager traces. Because each SIP device reports keepalive messages every 2 minutes, and each keepalive message can create multiple lines of trace data, the system generates a large amount of trace data when this check box is checked.

Cisco CallManager SDL Trace Fields

The following table describes the Cisco CallManager SDL trace filter settings. The Cisco CallManager service supports Unified Communications Manager.

Note Cisco recommends that you use the defaults unless a Cisco engineer instructs you to do otherwise.

Table 42: Cisco CallManager SDL Configuration Trace Filter Settings

Setting Name	Description
Enable all Layer 1 traces.	Activates traces for Layer 1.
Enable detailed Layer 1 traces.	Activates detailed Layer 1 traces.
Enable all Layer 2 traces.	Activates traces for Layer 2.
Enable Layer 2 interface trace.	Activates Layer 2 interface traces.
Enable Layer 2 TCP trace.	Activates Layer 2 Transmission Control Program (TCP) traces.
Enable detailed dump Layer 2 trace.	Activates detailed traces for dump Layer 2.
Enable all Layer 3 traces.	Activates traces for Layer 3.
Enable all call control traces.	Activates traces for call control.
Enable miscellaneous polls trace.	Activates traces for miscellaneous polls.
Enable miscellaneous trace (database signals).	Activates miscellaneous traces such as database signals.
Enable message translation signals trace.	Activates traces for message translation signals.
Enable UUIE output trace.	Activates traces for user-to-user informational element (UUIE) output.
Enable gateway signals trace.	Activates traces for gateway signals.
Enable CTI trace.	Activates CTI trace.

Setting Name	Description
Enable network service data trace	Activates network service data trace.
Enable network service event trace	Activates network service event trace.
Enable ICCP admin trace	Activates ICCP administration trace.
Enable default trace	Activates default trace.

The following table describes the Cisco CallManager SDL configuration characteristics.

Table 43: Cisco CallManager SDL Configuration Trace Characteristics

Characteristics	Description
Enable SDL link states trace.	Activates trace for intracluster communication protocol (ICCP) link state.
Enable low-level SDL trace.	Activates trace for low-level SDL.
Enable SDL link poll trace.	Activates trace for ICCP link poll.
Enable SDL link messages trace.	Activates trace for ICCP raw messages.
Enable signal data dump trace.	Activates traces for signal data dump.
Enable correlation tag mapping trace.	Activates traces for correlation tag mapping.
Enable SDL process states trace.	Activates traces for SDL process states.
Disable pretty print of SDL trace.	Disables trace for pretty print of SDL. Pretty print adds tabs and spaces in a trace file without performing post processing.
Enable SDL TCP event trace.	Activates SDL TCP event trace.

Cisco CTIManager SDL Trace Fields

The following table describes the Cisco CTIManager SDL configuration trace filter settings. The Cisco CTIManager service supports Unified Communications Manager.

Tip Cisco recommends that you use the defaults unless a Cisco engineer instructs you to do otherwise.

Tip When you choose the CTIManager service from the Service Groups drop-down list box, the Trace Configuration window displays for SDI traces for this service. To activate SDI trace for the Cisco CTI Manager service, check the **Enable All Trace** check box in the Trace Configuration window for the Cisco CTIManager service. To access the SDL Configuration window, choose **SDL Configuration** from the Related Links drop-down list box; the settings that are described in Cisco CTIManager SDL Configuration Trace Filter Settings table and Cisco CTIManager SDL Configuration Trace Characteristics table display.

Table 44: Cisco CTIManager SDL Configuration Trace Filter Settings

Setting Name	Description
Enable miscellaneous polls trace.	Activates traces for miscellaneous polls.
Enable miscellaneous trace (database signals).	Activates miscellaneous traces such as database signals.
Enable CTI trace.	Activates CTI trace.
Enable Network Service Data Trace	Activates network service data trace.
Enable Network Service Event Trace	Activates network service event trace.
Enable ICCP Admin Trace	Activates ICCP administration trace.
Enable Default Trace	Activates default trace.

The following table describes the Cisco CTIManager SDL configuration trace characteristics.

Table 45: Cisco CTIManager SDL Configuration Trace Characteristics

Characteristics	Description
Enable SDL link states trace.	Activates trace for ICCP link state.
Enable low-level SDL trace.	Activates trace for low-level SDL.
Enable SDL link poll trace.	Activates trace for ICCP link poll.
Enable SDL link messages trace.	Activates trace for ICCP raw messages.
Enable signal data dump trace.	Activates traces for signal data dump.
Enable correlation tag mapping trace.	Activates traces for correlation tag mapping.
Enable SDL process states trace.	Activates traces for SDL process states.
Disable pretty print of SDL trace.	Disables trace for pretty print of SDL. Pretty print adds tabs and spaces in a trace file without performing post processing.
Enable SDL TCP Event trace	Activates SDL TCP event trace.

Cisco Extended Functions Trace Fields

The following table describes the Cisco Extended Functions trace fields. The Cisco Extended Functions service supports Unified Communications Manager.

Table 46: Cisco Extended Functions Trace Fields

Field Name	Description
Enable QBE Helper TSP Trace	Activates telephony service provider trace.

Field Name	Description
Enable QBE Helper TSPI Trace	Activates QBE helper TSP interface trace.
Enable QRT Dictionary Trace	Activates quality report tool service dictionary trace.
Enable DOM Helper Traces	Activates DOM helper trace.
Enable Redundancy and Change Notification Trace	Activates database change notification trace.
Enable QRT Report Handler Trace	Activates quality report tool report handler trace.
Enable QBE Helper CTI Trace	Activates QBE helper CTI trace.
Enable QRT Service Trace	Activates quality report tool service related trace.
Enable QRT DB Traces	Activates QRT DB access trace.
Enable Template Map Traces	Activates standard template map and multimap trace.
Enable QRT Event Handler Trace	Activates quality report tool event handler trace.
Enable QRT Real-Time Information Server Trace	Activates quality report tool real-time information server trace.

Cisco Extension Mobility Trace Fields

The following table describes the Cisco Extension Mobility trace fields. The Cisco Extension Mobility service supports Unified Communications Manager.

Table 47: Cisco Extension Mobility Trace Fields

Field Name	Description
Enable EM Service Trace	Activates trace for the extension mobility service.

Tip When you activate trace for the Cisco Extension Mobility Application service, you check the Enable All Trace check box in the Trace Configuration window for the Cisco Extension Mobility Application service.

Cisco IP Manager Assistant Trace Fields

The following table describes the Cisco IP Manager Assistant trace fields. The Cisco IP Manager Assistant service supports Cisco Unified Communications Manager Assistant.

Table 48: Cisco IP Manager Assistant Trace Fields

Field Name	Description
Enable IPMA Service Trace	Activates trace for the Cisco IP Manager Assistant service.

Field Name	Description
Enable IPMA Manager Configuration Change Log	Activates trace for the changes that you make to the manager and assistant configurations.
Enable IPMA CTI Trace	Activates trace for the CTI Manager connection.
Enable IPMA CTI Security Trace	Activates trace for the secure connection to CTIManager.

Cisco IP Voice Media Streaming App Trace Fields

The information in this section does not apply to Cisco Unity Connection.

The following table describes the Cisco IP Voice Media Streaming App trace fields. The Cisco IP Voice Media Streaming App service supports Unified Communications Manager.

Table 49: Cisco IP Voice Media Streaming Application Trace Fields

Field Name	Description
Enable Service Initialization Trace	Activates trace for initialization information.
Enable MTP Device Trace	Activates traces to monitor the processed messages for media termination point (MTP).
Enable Device Recovery Trace	Activates traces for device-recovery-related information for MTP, conference bridge, and MOH.
Enable Skinny Station Messages Trace	Activates traces for skinny station protocol.
Enable WinSock Level 2 Trace	Activates trace for high-level, detailed WinSock-related information.
Enable Music On Hold Manager Trace	Activates trace to monitor MOH audio source manager.
Enable Annunciator Trace	Activates trace to monitor annunciator.
Enable DB Setup Manager Trace	Activates trace to monitor database setup and changes for MTP, conference bridge, and MOH.
Enable Conference Bridge Device Trace	Activates traces to monitor the processed messages for conference bridge.
Enable Device Driver Trace	Activates device driver traces.
Enable WinSock Level 1 Trace	Activates trace for low-level, general, WinSock-related information.
Enable Music on Hold Device Trace	Activates traces to monitor the processed messages for MOH.
Enable TFTP Downloads Trace	Activates trace to monitor the download of MOH audio source files.

Cisco TFTP Trace Fields

The following table describes the Cisco TFTP trace fields. The Cisco TFTP service supports Unified Communications Manager.

Table 50: Cisco TFTP Trace Fields

Field Name	Description
Enable Service System Trace	Activates trace for service system.
Enable Build File Trace	Activates trace for build files.
Enable Serve File Trace	Activates trace for serve files.

Cisco Web Dialer Web Service Trace Fields

The following table describes the Cisco Web Dialer Web Service trace fields. The Cisco Web Dialer Web Service supports Unified Communications Manager.

Table 51: Cisco Web Dialer Web Service Trace Fields

Field Name	Description
Enable Web Dialer Servlet Trace	Activates trace for Cisco Web Dialer servlet.
Enable Redirector Servlet Trace	Activates trace for the Redirector servlet.

IM and Presence SIP Proxy Service Trace Filter Settings

The following table below describes the service trace filter settings for the IM and Presence SIP Proxy.

Table 52: IM and Presence SIP Proxy Service Trace Filter Settings

Parameter	Description
Enable Access Log Trace	This parameter enables the proxy access log trace; the first line of each SIP message received by the proxy is logged.
Enable Authentication Trace	This parameter enables tracing for the Authentication module.
Enable CALENDAR Trace	This parameter enables tracing for the Calendar module.
Enable CTI Gateway Trace	This parameter enables tracing for the CTI Gateway.
Enable Enum Trace	This parameter enables tracing for the Enum module.
Enable Method/Event Routing Trace	This parameter enables tracing for the Method/Event routing module.

Parameter	Description
Enable Number Expansion Trace	This parameter enables tracing for the Number Expansion module.
Enable Parser Trace	This parameter enables tracing of parser information related to the operation of the per-sipd child SIP parser.
Enable Privacy Trace	This parameter enables tracing for information about processing of PAI, RPID, and Diversion headers in relation to privacy requests.
Enable Registry Trace	This parameter enables tracing for the Registry module.
Enable Routing Trace	This parameter enables tracing for the Routing module.
Enable SIPUA Trace	This parameter enables tracing for the SIP UA application module.
Enable Server Trace	This parameter enables tracing for the Server.
Enable SIP Message and State Machine Trace	This parameter enables tracing for information related to the operation of the per-sipd SIP state machine.
Enable SIP TCP Trace	This parameter enables tracing for information related to the TCP transport of SIP messages by TCP services.
Enable SIP TLS Trace	This parameter enables tracing for information related to the TLS transport of SIP messages by TCP services.
Enable SIP XMPP IM Gateway Trace	This parameter enables trace for the SIP XMPP IM Gateway.
Enable Presence Web Service Trace	This parameter enables tracing for the Presence Web Service.

IM and Presence Trace Field Descriptions

The following tables provide field descriptions for the services that support trace activation of specific components. For some services, you can activate trace for specific component instead of enabling all trace for the service. If a service is not included in this chapter, Enable All Trace displays for the service in the Trace Configuration window.

Cisco Access Log Trace Fields

The following table describes the Cisco Access Log trace fields.

Table 53: Access Log Trace Fields

Field Name	Description
Enable Access Log Trace	Turns on Access Log trace.

Cisco Authentication Trace Fields

The following table describes the Cisco Authentication trace fields.

Table 54: Authentication Trace Fields

Field Name	Description
Enable Authentication Trace	Turns on authentication trace.

Cisco Calendar Trace Fields

The following table describes the Cisco Calendar trace fields.

Table 55: Calendar Trace Fields

Field Name	Description
Enable Calendar Trace	Turns on Calendar trace.

Cisco CTI Gateway Trace Fields

The following table describes the Cisco CTI Gateway trace fields.

Table 56: CTI Gateway Trace Fields

Field Name	Description
Enable CTI Gateway Trace	Turns on CTI Gateway trace.

Cisco Database Layer Monitor Trace Fields

The following table describes the Cisco Database Layer Monitor trace fields.

Table 57: Cisco Database Layer Monitor Trace Fields

Field Name	Description
Enable DB Library Trace	Turns on database library trace for C++ applications.
Enable Service Trace	Turns on service trace.
Enable DB Change Notification Trace	Activates the database change notification traces for C++ applications.
Enable Unit Test Trace	Do not check. Cisco engineering uses it for debugging purposes.

Cisco Enum Trace Fields

The following table describes the Cisco Enum trace fields.

Table 58: Enum Trace Fields

Field Name	Description
Enable Enum Trace	Turns on Enum trace.

Cisco Method/Event Trace Fields

The following table describes the Cisco Method/Event trace fields.

Table 59: Method/Event Trace Fields

Field Name	Description
Enable Method/Event Trace	Turns on Method/Event trace.

Cisco Number Expansion Trace Fields

The following table describes the Cisco Number Expansion trace fields.

Table 60: Number Expansion Trace Fields

Field Name	Description
Enable Number Expansion Trace	Activates number expansion trace.

Cisco Parser Trace Fields

The following table describes the Cisco Parser trace fields.

Table 61: Parser Trace Fields

Field Name	Description
Enable Parser Trace	Activates parser trace.

Cisco Privacy Trace Fields

The following table describes the Cisco Privacy trace fields.

Table 62: PrivacyTrace Fields

Field Name	Description
Enable Privacy Trace	Activates Privacy trace.

Cisco Proxy Trace Fields

The following table describes the Cisco proxy trace fields.

Table 63: Proxy Trace Fields

Field Name	Description
Add Proxy	Turns on Proxy trace.

Cisco RIS Data Collector Trace Fields

The following table describes the Cisco RIS Data Collector trace fields.

Table 64: Cisco RIS Data Collector Trace Fields

Field Name	Description
Enable RISDC Trace	Activates trace for the RISDC thread of the RIS data collector service (RIS).
Enable System Access Trace	Activates trace for the system access library in the RIS data collector.
Enable Link Services Trace	Activates trace for the link services library in the RIS data collector.
Enable RISDC Access Trace	Activates trace for the RISDC access library in the RIS data collector.
Enable RISDB Trace	Activates trace for the RISDB library in the RIS data collector.
Enable PI Trace	Activates trace for the PI library in the RIS data collector.
Enable XML Trace	Activates trace for the input/output XML messages of the RIS data collector service.
Enable Perfmon Logger Trace	Activates trace for the troubleshooting perfmon data logging in the RIS data collector. Used to trace the name of the log file, the total number of counters that are logged, the names of the application and system counters and instances, calculation of process and thread CPU percentage, and occurrences of log file rollover and deletion.

Cisco Registry Trace Fields

The following table describes the Cisco Registry trace fields.

Table 65: Registry Trace Fields

Field Name	Description
Enable Registry Trace	Activates Registry trace.

Cisco Routing Trace Fields

The following table describes the Cisco Routing trace fields.

Table 66: Routing Trace Fields

Field Name	Description
Enable Routing Trace	Activates Routing trace.

Cisco Server Trace Fields

The following table describes the Cisco Server trace fields.

Table 67: Server Trace Fields

Field Name	Description
Enable Server Trace	Activates Server trace.

Cisco SIP Message and State Machine Trace Fields

The following table describes the Cisco SIP Message and State Machine trace fields.

Table 68: SIP Message and State Machine Trace Fields

Field Name	Description
Enable SIP Message and State Machine Trace	Activates SIP Message and State Machine trace.

Cisco SIP TCP Trace Fields

The following table describes the Cisco SIP TCP trace fields.

Table 69: SIP TCP Trace Fields

Field Name	Description
Enable SIP TCP Trace	Activates SIP TCP trace.

Cisco SIP TLS Trace Fields

The following table describes the Cisco SIP TLS trace fields.

Table 70: SIP TLS Trace Fields

Field Name	Description
Enable SIP TLS Trace	Activates SIP TLS trace.

Cisco Web Service Trace Fields

The following table describes the Cisco Web Service trace fields.

Table 71: Web Service Trace Fields

Field Name	Description
Enable Presence Web Service Trace	Activates Presence Web Service trace.

Trace Output Settings

The following table contains the trace log file descriptions.

Caution When you change either the Maximum No. of Files or the Maximum File Size settings in the Trace Configuration window, the system deletes all service log files except for the current file, that is, if the service is running; if the service has not been activated, the system deletes the files immediately after you activate the service. Before you change the Maximum No. of Files setting or the Maximum File Size setting, download and save the service log files to another server if you want to keep a record of the log files; to perform this task, use Trace and Log Central in Unity RTMT.

Table 72: Trace Output Settings

Field	Description
Maximum number of files	This field specifies the total number of trace files for a given service. Cisco Unified Serviceability automatically appends a sequence number to the filename to indicate which file it is, for example, cus299.txt. When the last file in the sequence is full, the trace data begins writing over the first file. The default varies by service.
Maximum file size (MB)	This field specifies the maximum size of the trace file in megabytes. The default varies by service.

Trace Setting Troubleshooting

Troubleshoot Trace Settings Window

The **Troubleshooting Trace Settings** window allows you to select the services in the Serviceability GUI for which you want to set predetermined troubleshooting trace settings. In this window, you can select the services on different nodes in the cluster. This populates the trace settings changes for all the services you choose. You can select specific active services for a single node, all active services for the node, specific active services for all nodes in the cluster, or all active services for all nodes in the cluster. In the window, N/A displays next to inactive services.

Note For IM and Presence the predetermined troubleshooting trace settings for an IM and Presence feature or network service include SDI and Log4j trace settings. Before the troubleshooting trace settings are applied, the system backs up the original trace settings. When you reset the troubleshooting trace settings, the original trace settings are restored.

When you open the **Troubleshooting Trace Settings** window after you apply troubleshooting trace settings to a service, the service that you set for troubleshooting displays as checked. In the **Troubleshooting Trace Settings** window, you can reset the trace settings to the original settings.

After you apply Troubleshooting Trace Setting to a service, the **Trace Configuration** window displays a message that troubleshooting trace is set for that service. From the **Related Links** list box, you can select the Troubleshooting Trace Settings option if you want to reset the settings for the service. For the given service, the **Trace Configuration** window displays all the settings as read-only, except for some parameters of trace output settings, for example, Maximum No. of Files.

Troubleshoot Trace Settings

Before you begin

Review the tasks Set up trace configuration and Set up trace parameters.

Procedure

Step 1 Select **Trace** > **Troubleshooting Trace Settings**.

Step 2 Select the server where you want to troubleshoot trace settings from the **Server** list box.

Step 3 Select **Go**.

A list of services display. The services that are not active display as N/A.

Step 4 Perform one of the following actions:

a) To monitor specific services on the node that you selected from the **Server** list box, check the service in the **Services** pane.

   For example, the Database and Admin Services, Performance and Monitoring Services, or the Backup and Restore Services pane (and so on).

   This task affects only the node that you selected from the **Server** list box.

b) To monitor all services on the node that you selected from the **Server** list box, check **Check All Services**.

c) Cisco Unified Communications Manager and IM and Presence clusters only: To monitor specific services on all nodes in a cluster, check **Check Selected Services on All Nodes**.

   This setting applies for all nodes in the cluster where the service is active.

d) Unified Communications Manager and IM and Presence clusters only: To monitor all services for all nodes in the cluster, check **Check All Services on All Nodes**.

Step 5 Select **Save**.

Step 6 Select one of the following buttons to restore the original trace settings:

a) **Reset Troubleshooting Traces**—Restores the original trace settings for the services on the node that you chose in the Server list box; also displays as an icon that you can select.
b) Unified Communications Manager and IM and Presence clusters only: **Reset Troubleshooting Traces On All Nodes**—Restores the original trace settings for the services on all nodes in the cluster.

The Reset Troubleshooting Traces button displays only if you have set troubleshooting trace for one or more services.

Note Leaving troubleshooting trace enabled for a long time increases the size of the trace files and may affect the performance of the services.

After you select the **Reset** button, the window refreshes and the service check boxes display as unchecked.

CHAPTER 17

View Usage Records

Usage Records Overview

Cisco Unified Communications Manager provides records that allow you to see how configured items are used in your system. Configured items include devices, as well as system-level settings such as device pools, date and time groups, and route plans.

Dependency Records

Use dependency records for the following purposes:

- Find information about system-level settings, such as servers, device pools, and date and time groups.
- Determine the records in the database that use other records. For example, you can determine which devices, such as CTI route points or phones, use a particular calling search space.
- Show dependencies between records before you delete any records. For example, before you delete a partition, use dependency records to see which calling search spaces (CSSs) and devices are associated with it. You can then reconfigure the settings to remove the dependency.

Route Plan Reports

The route plan report allows you to view either a partial or full list of numbers, routes, and patterns that are configured in the system. When you generate a report, you can access the configuration window for each item by clicking the entry in the Pattern/Directory Number, Partition, or Route Detail columns of the report.

In addition, the route plan report allows you to save report data into a.CSV file that you can import into other applications. The.CSV file contains more detailed information than the web pages, including directory numbers for phones, route patterns, pattern usage, device name, and device description.

Cisco Unified Communications Manager uses the route plan to route both internal calls and external public switched telephone network (PSTN) calls. Because you might have several records in your network, Cisco Unified Communications Manager Administration lets you locate specific route plan records on the basis of specific criteria.

Usage Report Tasks

Procedure

	Command or Action	Purpose
Step 1	To view route plan records and use them to manage unassigned directory numbers, see the following procedures: • View Route Plan Records, on page 248 • Save Route Plan Reports, on page 249 • Delete Unassigned Directory Numbers, on page 249 • Update Unassigned Directory Numbers, on page 250	Use these procedures to locate specific route plan records, save the records in a .CSV file, and manage unassigned directory numbers.
Step 2	To use dependency records, see the following procedures: • View Dependency Records, on page 251	Use these procedures to find information about system-level settings and show dependencies between records in the database.

Route Plan Reports Task Flow

Procedure

	Command or Action	Purpose
Step 1	View Route Plan Records, on page 248.	View route plan records and generate customized route plan reports.
Step 2	Save Route Plan Reports, on page 249.	View route plan reports in a.csv file format.
Step 3	Delete Unassigned Directory Numbers, on page 249.	Delete an unassigned directory number from the route plan report.
Step 4	Update Unassigned Directory Numbers, on page 250.	Update the settings of an unassigned directory number from the route plan report.

View Route Plan Records

This section describes how to view route plan records. Because you might have several records in your network, Cisco Unified Communications Manager Administration lets you locate specific route plan records on the basis of specific criteria. Use the following procedure to generate customized route plan reports.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.

Step 2 To find all records in the database, ensure the dialog box is empty and proceed to step 3.

To filter or search records

a) From the first drop-down list box, select a search parameter.
b) From the second drop-down list box, select a search pattern.
c) Specify the appropriate search text, if applicable.

Step 3 Click **Find**.

All or matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Step 4 From the list of records that display, click the link for the record that you want to view.

The window displays the item that you choose.

Save Route Plan Reports

This section contains information on how to view route plan reports in a.csv file.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.

Step 2 Choose **View In File** from the **Related Links** drop-down list on the **Route Plan Report** window and click **Go**.

From the dialog box that appears, you can either save the file or import it into another application.

Step 3 Click **Save**.

Another window displays that allows you to save this file to a location of your choice.

Note You may also save the file as a different file name, but the file name must include a.CSV extension.

Step 4 Choose the location in which to save the file and click **Save**. This action should save the file to the location that you designated.

Step 5 Locate the.CSV file that you just saved and double-click its icon to view it.

Delete Unassigned Directory Numbers

This section describes how to delete an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device or a phone gets deleted, the directory number still exists in the Cisco Unified Communications Manager database. To delete the directory number from the database, use the Route Plan Report window.

Procedure

Step 1 Choose Call **Call Routing** > **Route Plan Report**.

Step 2 In the Route Plan Report window, use the three drop-down lists to specify a route plan report that lists all unassigned DNs.

Step 3 Three ways exist to delete directory numbers:

a) Click the directory number that you want to delete. When the Directory Number Configuration window displays, click Delete.
b) Check the check box next to the directory number that you want to delete. Click Delete Selected.
c) To delete all found unassigned directory numbers, click Delete All Found Items.

A warning message verifies that you want to delete the directory number.

Step 4 To delete the directory number, click OK. To cancel the delete request, click Cancel.

Update Unassigned Directory Numbers

This section describes how to update the settings of an unassigned directory number from the route plan report. Directory numbers get configured and removed in the Directory Number Configuration window of Cisco Unified Communications Manager Administration. When a directory number gets removed from a device, the directory number still exists in the Cisco Unified Communications Manager database. To update the settings of the directory number, use the Route Plan Report window.

Procedure

Step 1 Choose **Call Routing** > **Route Plan Report**.

Step 2 In the **Route Plan Report** window, use the three drop-down lists to specify a route plan report that lists all unassigned DNs.

Step 3 Click the directory number that you want to update.

Note You can update all the settings of the directory number except the directory number and partition.

Step 4 Make the required updates such as calling search space or forwarding options.

Step 5 Click **Save**.

The Directory Number Configuration window redisplays, and the directory number field is blank.

Dependency Records Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Dependency Records, on page 251.	Use this procedure to enable or disable dependency records. This procedure runs at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and CPU requirements of other applications.
Step 2	View Dependency Records, on page 251.	After you enable dependency records, you can access them from the configuration windows on the interface.

Configure Dependency Records

Use dependency records to view relationships between records in the Cisco Unified Communications Manager database. For example, before you delete a partition, use dependency records to see which calling search spaces (CSSs) and devices are associated with it.

⚠ **Caution** Dependency records cause high CPU usage. This procedure runs at below-normal priority and may take time to complete due to dial plan size and complexity, CPU speed, and CPU requirements of other applications.

If you have dependency records enabled and your system is experiencing CPU usage issues, you can disable dependency records.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Scroll to the **CCMAdmin Parameters** section and from the **Enable Dependency Records** drop-down list, choose one of the following options:

- **True**—Enable dependency records.
- **False**—Disable dependency records.

Based on the option you choose, a dialog box appears with a message about the consequences of enabling or disabling the dependency records. Read the message before you click **OK** in this dialog box.

Step 3 Click **OK**.

Step 4 Click **Save**.
The `Update Successful` message appears confirming the change.

View Dependency Records

After you enable dependency records, you can access them from the configuration windows on the interface.

Before you begin

Configure Dependency Records, on page 251

Procedure

Step 1 From Cisco Unified CM Administration, navigate to the configuration window for the records that you want to view.

Example:

To view dependency records for a device pool, select **System** > **Device Pool**.

Note You cannot view dependency records from the **Device Defaults** and **Enterprise Parameters Configuration** windows.

Step 2 Click **Find**.

Step 3 Click one of the records.
The configuration window appears.

Step 4 From the **Related Links** list box, choose **Dependency Records** box, and click **Go**.

Note If you have not enabled the dependency records, the **Dependency Records Summary** window displays a message, not the information about the record.

The **Dependency Records Summary** window appears showing the records that are used by other records in the database.

Step 5 Select one of the following dependency record buttons in this window:

- **Refresh**—Update the window with current information.
- **Close**—Close the window without returning to the configuration window in which you clicked the Dependency Records link.
- **Close and Go Back**—Close the window and returns to the configuration window in which you clicked the Dependency Records link.

CHAPTER 18

Manage Enterprise Parameters

Enterprise Parameters Overview

Enterprise parameters provide default settings that apply to all devices and services across the entire cluster. For example, your system uses the enterprise parameters to set the initial values of its device defaults.

You cannot add or delete enterprise parameters, but you can update existing enterprise parameters. The configuration window lists enterprise parameters under categories; for example, CCMAdmin parameters, CCMUser parameters, and CDR parameters.

You can view detailed descriptions for enterprise parameters on the **Enterprise Parameters Configuration** window.

⚠ **Caution** Many of the enterprise parameters do not require changes. Do not change an enterprise parameter unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) advises you on the change.

View Enterprise Parameter Information

Access information about enterprise parameters through embedded content in the **Enterprise Parameter Configuration** window.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Perform one of the following tasks:

- To view the description of a particular enterprise parameter, click the parameter name.
- To view the descriptions of all the enterprise parameters, click **?**.

Update Enterprise Parameters

Use this procedure to open the **Enterprise Parameter Configuration** window and configure system-level settings.

Caution Many of the enterprise parameters do not require changes. Do not change an enterprise parameter unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) advises you on the change.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Choose the desired values for the enterprise parameters that you want to change.

Step 3 Click **Save**.

What to do next

Apply Configuration to Devices, on page 254

Apply Configuration to Devices

Use this procedure to update all affected devices in the cluster with the settings you configured.

Before you begin

Update Enterprise Parameters, on page 254

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Verify your changes, and then click **Save**.

Step 3 Choose one of the following options:

- Click **Apply Config** if you want your system to determine which devices to reboot. In some cases, a device may not need a reboot. Calls in progress may be dropped but connected calls will be preserved unless the device pool includes SIP trunks.
- Click **Reset** if you want to reboot all devices in your cluster. We recommend that you perform this step during off-peak hours.

Step 4 After you read the confirmation dialog, click **OK**.

Restore Default Enterprise Parameters

Use this procedure if you want to reset the enterprise parameters to the default settings. Some enterprise parameters contain suggested values, as shown in the column on the configuration window; this procedure uses these values as the default settings.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Click **Set to Default**.

Step 3 After you read the confirmation prompt, click **OK**.

CHAPTER 19

Manage the Server

Manage the Server Overview

This chapter describes how to manage the properties of the Cisco Unified Communications Manager node, view the Presence Server status and configure a host name for the Unified Communications Manager server.

Server Deletion

This section describes how to delete a server from the Cisco Unified Communications Manager database and how to add a deleted server back to the Cisco Unified Communications Manager cluster.

In Cisco Unified Communications Manager Administration, you cannot delete the first node of the cluster, but you can delete subsequent nodes. Before you delete a subsequent node in the Find and List Servers window, Cisco UnifiedCM Administration displays the following message: “You are about to permanently delete one or more servers. This action cannot be undone. Continue?”. If you click OK, the server gets deleted from the Cisco UnifiedCM database and is not available for use.

Tip When you attempt to delete a server from the Server Configuration window, a message that is similar to the one in the preceding paragraph displays. If you click OK, the server gets deleted from the Cisco UnifiedCM database and is not available for use.

Before you delete a server, consider the following information:

- Cisco Unified Communications Manager Administration does not allow you to delete the first node in the cluster, but you can delete any subsequent node.

- Cisco recommends that you do not delete any node that has Cisco Unified Communications Manager running on it, especially if the node has devices, such as phones, registered with it.
- Although dependency records exist for the subsequent nodes, the records do not prevent you from deleting the node.
- If any call park numbers are configured for Cisco Unified Communications Manager on the node that is being deleted, the deletion fails. Before you can delete the node, you must delete the call park numbers in Cisco Unified Communications Manager Administration.
- If a configuration field in Cisco Unified Communications Manager Administration contains the IP address or host name for a server that you plan to delete, update the configuration before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server; for example, if you enter the IP address or host name for a service parameter, enterprise parameter, service URL, directory URL, IP phone service, and so on, update this configuration before you delete the server.
- If an application GUI, for example, Cisco Unity, Cisco Unity Connection, and so on, contains the IP address or host name for the server that you plan to delete, update the configuration in the corresponding GUIs before you delete the server. If you do not perform this task, features that rely on the configuration may not work after you delete the server.
- The system may automatically delete some devices, such as MOH servers, when you delete a server.
- Before you delete a node, Cisco recommends that you deactivate the services that are active on the subsequent node. Performing this task ensures that the services work after you delete the node.
- Changes to the server configuration do not take effect until you restart Cisco Unified Communications Manager. For information on restarting the Cisco CallManager service, see the *Cisco Unified Serviceability Administration Guide*.
- To ensure that database files get updated correctly, you must reboot the cluster after you delete a server, Presence, or application server.
- After you delete the node, access Cisco Unified Reporting to verify that Cisco Unified Communications Manager removed the node from the cluster. In addition, access Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes by using the CLI.

Note When a subscriber node is removed from a cluster, its certificates still exist in publisher and other nodes. Admin has to manually remove:

- the certificate of the subscriber node removed from the trust-store of the individual cluster members.
- the certificates of each of the other cluster members from the trust-store of the removed subscriber node.

Delete Unified Communications Manager Node from Cluster

Use this procedure to delete a Cisco Unified Communications Manager node from the cluster.

Procedure

Step 1 From Cisco Unified CM Administration choose **System** > **Server**.

Step 2 Click **Find** and select the node you want to delete.

Step 3 Click **Delete**.

Step 4 Click **OK** when a warning dialog box indicates that this action cannot be undone.

Step 5 Shut down the host VM for the node you have unassigned.

Delete IM and Presence Node From Cluster

Follow this procedure if you need to safely remove an IM and Presence Service node from its presence redundancy group and cluster.

Caution Removing a node will cause a service interruption to users on the remaining node(s) in the presence redundancy group. This procedure should only be performed during a maintenance window.

Procedure

Step 1 On the **Cisco Unified CM Administration > System > Presence Redundancy Groups** page, disable High Availability if it is enabled.

Step 2 On the **Cisco Unified CM Administration** > **User Management** > **Assign Presence Users** page, unassign or move all the users off the node that you want to remove.

Step 3 To remove the node from its presence redundancy group, choose **Not-Selected** from the Presence Server drop down list on the presence redundancy group's **Presence Redundancy Group Configuration** page. Select **OK** when a warning dialog box indicates that services in the presence redundancy group will be restarted as a result of unassigning the node.

Note You cannot delete the publisher node directly from a presence redundancy group. To delete a publisher node, first unassign users from the publisher node and delete the presence redundancy group completely.

However, you can add the deleted IM and Presence node back into the cluster. For more information on how to add the deleted nodes, see Add Deleted Server Back in to Cluster, on page 260. In this scenario, the **DefaultCUPSubcluster** is created automatically when the deleted publisher node is added back to the server in the **System > Server** screen in the Cisco Unified CM Administration console.

Step 4 In Cisco Unified CM Administration, delete the unassigned node from the **System** > **Server**. Click **OK** when a warning dialog box indicates that this action cannot be undone.

Step 5 Shut down the host VM or server for the node you have unassigned.

Step 6 Restart the **Cisco XCP Router** on all nodes.

Add Deleted Server Back in to Cluster

If you delete a subsequent node (subscriber) from Cisco Unified Communications Manager Administration and you want to add it back to the cluster, perform the following procedure.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, add the server by choosing **System** > **Server**.

Step 2 After you add the subsequent node to Cisco Unified Communications Manager Administration, perform an installation on the server by using the disk that Cisco provided in the software kit for your version.

Tip Make sure that the version that you install matches the version that runs on the publisher node. If the version that is running on the publisher does not match your installation file, choose the Upgrade During Install option during the installation process. For details, see the *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*.

Step 3 After you install Cisco UnifiedCM, configure the subsequent node, as described in the installation documentation that supports your version of Cisco UnifiedCM.

Step 4 Access the Cisco Unified Reporting, RTMT, or the CLI to verify that database replication is occurring between existing nodes; if necessary, repair database replication between the nodes.

Add Node to Cluster Before Install

Use Cisco Unified Communications Manager Administration to add a new node to a cluster before installing the node. The server type you select when adding the node must match the server type you install.

You must configure a new node on the first node using Cisco Unified Communications Manager Administration before you install the new node. To install a node on a cluster, see the *Cisco Unified Communications Manager Installation Guide*.

For Cisco Unified Communications Manager Video/Voice servers, the first server you add during an initial installation of the Cisco Unified Communications Manager software is designated the publisher node. All subsequent server installations or additions are designated as subscriber nodes. The first Cisco Unified Communications Manager IM and Presence node you add to the cluster is designated the IM and Presence Service database publisher node.

Note You cannot use Cisco Unified Communications Manager Administration to change the server type after the server has been added. You must delete the existing server instance, and then add the new server again and choose the correct server type setting.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window displays.

Step 2 Click **Add New**.

The **Server Configuration - Add a Server** window displays.

Step 3 From the **Server Type** drop-down list box, choose the server type that you want to add, and then click **Next**.

- CUCM Video/Voice
- CUCM IM and Presence

Step 4 In the **Server Configuration** window, enter the appropriate server settings.

For server configuration field descriptions, see Server Settings.

Step 5 Click **Save**.

View Presence Server Status

Use Cisco Unified Communications Manager Administration to view the status of critical services and self-diagnostic test results for the IM and Presence Service node.

Procedure

Step 1 Select **System** > **Server**.

The **Find and List Servers** window appears.

Step 2 Select the server search parameters, and then click **Find**.

Matching records appear.

Step 3 Select the IM and Presence server that is listed in the **Find and List Servers** window.

The **Server Configuration** window appears.

Step 4 Click on the Presence Server Status link in the IM and Presence Server Information section of the **Server Configuration** window.

The **Node Details** window for the server appears.

Configure Ports

Use this procedure to change the port settings used for connections such as SCCP device registration, SIP device registration, and MGCP gateway connections.

Note Normally, you need not change the default port settings. Use this procedure only if you really want to change the defaults.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, select **System** > **Cisco Unified CM**.
The **Find and List Cisco Unified CMs** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.
All matching Cisco Unified Communications Managers are displayed.

Step 3 Select the **Cisco Unified CM** that you want to view.
The **Cisco Unified CM Configuration** window appears.

Step 4 Navigate to the **Cisco Unified Communications Manager TCP Port Settings for this Server** section.

Step 5 Configure the port settings for the Cisco Unified Communications Manager.

See Port Settings, on page 262 information about the fields and their configuration options.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Step 8 Click **OK**.

Port Settings

Field	Description
Ethernet Phone Port	The system uses this TCP port to communicate with the Cisco Unified IP Phones (SCCP only) on the network. • Accept the default port value of 2000 unless this port is already in use on your system. Choosing 2000 identifies this port as non-secure. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
MGCP Listen Port	The system uses this TCP port to detect messages from its associated MGCP gateway. • Accept the default port of 2427 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.

Field	Description
MGCP Keep-alive Port	The system uses this TCP port to exchange keepalive messages with its associated MGCP gateway. • Accept the default port of 2428 unless this port is already in use on your system. • Ensure all port entries are unique. • Valid port numbers range from 1024 to 49151.
SIP Phone Port	This field specifies the port number that Unified Communications Manager uses to listen for SIP line registrations over TCP and UDP.
SIP Phone Secure Port	This field specifies the port number that the system uses to listen for SIP line registrations over TLS.
SIP Phone OAuth Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations from Jabber On-Premise devices over TLS (Transport Layer Security). The default value is 5090. Range is 1024 to 49151.
SIP Mobile and Remote Access OAuth Port	This field specifies the port number that Cisco Unified Communications Manager uses to listen for SIP line registrations from Jabber over Expressway through MTLS (Mutual Transport Layer Security). The default value is 5091. Range is 1024 to 49151.

Hostname Configuration

The following table lists the locations where you can configure a host name for the Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Table 73: Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System** > **Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for a server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation wizard	You can add the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Hostname field **Settings** > **IP** > **Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric
set network hostname hostname Command Line Interface	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

  After you install the Unified Communications Manager publisher node, the host name for the publisher automatically displays in this field. Before you install a Unified Communications Manager subscriber node, enter either the IP address or the host name for the subscriber node in this field on the Unified Communications Manager publisher node.

  In this field, configure a host name only if Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

Tip In addition to configuring Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the installation of the Unified Communications Manager publisher node, you enter the host name, which is mandatory, and IP address of the publisher node to configure network information; that is, if you want to use static networking.

  During the installation of a Unified Communications Manager subscriber node, you enter the hostname and IP address of the Unified Communications Manager publisher node, so that Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber node. When the Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

kerneldump Utility

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiring a secondary server.

In a Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade the Unified Communications Manager from supported appliance releases.

Important Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The *command line interface* (CLI) for the *Cisco Unified Communications Operating System* can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Working with Files That Are Collected by the Utility

To view the crash information from the kerneldump utility, use the *Cisco Unified Real-Time Monitoring Tool* or the *Command Line Interface* (CLI). To collect the kerneldump logs by using the *Cisco Unified Real-Time Monitoring Tool*, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Kerneldump logs check box. For more information on collecting files using *Cisco Unified Real-Time Monitoring Tool*, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the kerneldump logs, use the “file” CLI commands on the files in the crash directory. These are found under the “activelog” partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump logs to the local server or to an external server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kerneldump enable` CLI command.

- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3 Reboot the server.

Example

Note If you need to disable the kerneldump utility, you can run the `utils os kernelcrash disable` CLI command to disable the local server for core dumps and the `utils os kerneldump ssh disable <ip_address>` CLI command to disable the utility on the external server.

What to do next

Configure an email alert in the Real-Time Monitoring Tool to be advised of core dumps. For details, see Enable Email Alert for Core Dump, on page 266

Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information on the kerneldump utility and troubleshooting.

Enable Email Alert for Core Dump

Use this procedure to configure the Real-Time Monitoring Tool to email the administrator whenever a core dump occurs.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.
b) Follow the prompts and **Add** a Recipient email address. When this alert is triggered, the default action is to email this address.
c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.
b) Enter the e-mail server and port information to send email alerts.
c) Enter the **Send User Id**.
d) Click **OK**.

PART V

Manage Reports

CHAPTER 20

Cisco Serviceability Reporter

Serviceability Reports Archive

The Cisco Serviceability Reporter service generates daily reports containing charts that display a summary of the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

Using the serviceability GUI, view reports from **Tools** > **Serviceability Reports Archive**. You must activate the Cisco Serviceability Reporter service before you can view reports. After you activate the service, report generation may take up to 24 hours.

The reports contain 24-hour data for the previous day. A suffix that is added to the report names shows the date for which Reporter generated them; for example, AlertRep_mm_dd_yyyy.pdf. The Serviceability Reports Archive window uses this date to display the reports for the relevant date only. The reports generate from the data that is present in the log files, with the timestamp for the previous day. The system considers log files for the current date and the previous two days for collecting data.

The time that is shown in the report reflects the server “System Time.”

You can retrieve log files from the server while you are generating reports.

Note The Cisco Unified Reporting web application provides snapshot views of data into one output and runs data checks. The application also allows you to archive generated reports. See the *Cisco Unified Reporting Administration Guide* for more information.

Serviceability Report Archive Considerations for Cluster Configurations

This section applies to Unified Communications Manager and IM and Presence Service only.

- Because the Cisco Serviceability Reporter is only active on the first server, at any time, Reporter generates reports only on the first server, not the other servers.
- The time that is shown in the report reflects the first server “System Time.” If the first server and subsequent servers are in different time zones, the first server “System Time” shows in the report.

- The time zone differences between the server locations in a cluster are taken into account when data is collected for the reports.
- You can select log files from individual servers or from all servers in the cluster when you generate reports.
- Cisco Unified Reporting web application output and data checks include cluster data from all accessible servers.

Cisco Serviceability Reporter Configuration Task Flow

Complete these tasks to set up daily system reports via the Cisco Serviceability Reporter.

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco Serviceability Reporter, on page 270	For daily reports to generate, the **Cisco Serviceability Reporter** service must be running.
Step 2	Configure Cisco Serviceability Reporter Settings, on page 271	Configure scheduling settings for the Cisco Serviceability Reporter.
Step 3	View Daily Report Archive, on page 271	Once the system is generating daily reports, use this task to view daily reports in a PDF file.

Activate the Cisco Serviceability Reporter

Use this procedure to turn on daily system reporting with the **Cisco Serviceability Reporter**. For reports to generate, the service must be **Activated**.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 Select the **Server** and click **Go**.

Step 3 Under **Performance and Monitoring Services**, check the status of the **Cisco Serviceability Reporter** service.

Step 4 If the service is deactivated, check the adjacent radio button, and click **Save**.

Note Reports generate daily. It may take up to 24 hours for the first reports to generate.

Configure Cisco Serviceability Reporter Settings

Configure scheduling settings for the daily reports that the Cisco Serviceability Reporter generates.

Procedure

Step 1 From Cisco Unified CM Administration chose **System** > **Service Parameters**.

Step 2 Select the **Server** on which the Cisco Serviceability Reporter is running.

Step 3 From the **Service** drop-down, select the Cisco Serviceability Reporter.

Step 4 Configure settings for the following service parameters:

- **RTMT Reporter Designated Node**—Specifies the designated node on which RTMT Reporter runs. Cisco recommends that you assign a non-call processing node.
- **Report Generation Time**—The number of minutes after midnight that reports generate. The range is 0 – 1439 with a default setting of 30 minutes.
- **Report Deletion Age**—The number of days that reports are saved on the disk. The range is 0 - 30 with a default setting of 7 days.

Step 5 Click **Save**.

View Daily Report Archive

Once the Cisco Serviceability Reporter is generating daily reports, use this procedure to view reports in a PDF file.

Procedure

Step 1 Choose **Tools** > **Serviceability Reports Archive**.

Step 2 Choose the month and year for which you want to display reports.
A list of days that correspond to the month displays.

Step 3 Click the the day for which you want to view generated reports.

Step 4 Click on the report that you want to view.

Note To view PDF reports, Acrobat Reader must be installed on your machine. You can download Acrobat Reader by clicking the link at the bottom of the **Serviceability Reports Archive** window.

Daily Report Summary

The Cisco Serviceability Reporter generates the following system reports daily:

- Device Statistics Report
- Server Statistics Report

- Service Statistics Report
- Call Activities Report
- Alert Summary Report
- Performance Protection Report

Device Statistics Report

The Device Statistics Report does not apply to IM and Presence Service and Cisco Unity Connection.

The Device Statistics Report provides the following line charts:

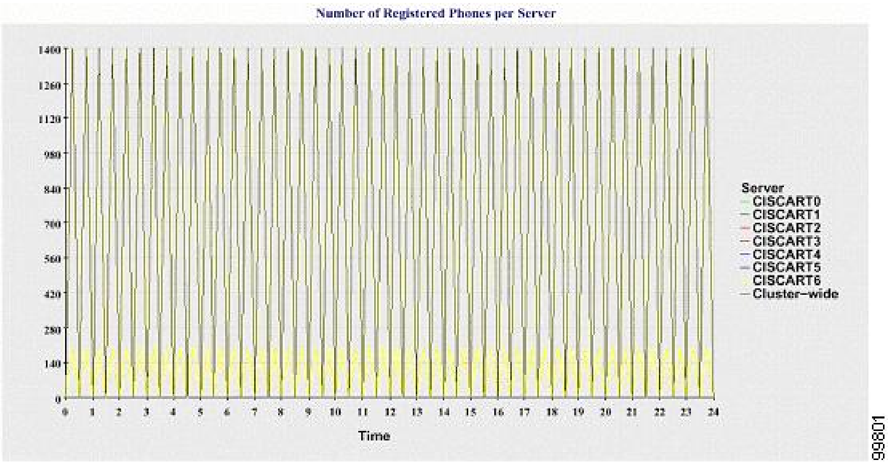
- Number of Registered Phones per Server
- Number of H.323 Gateways in the Cluster
- Number of Trunks in the Cluster

Number of Registered Phones Per Server

A line chart displays the number of registered phones for each Unified Communications Manager server (and cluster in a Unified Communications Manager cluster configuration). Each line in the chart represents the data for a server for which data is available, and one extra line displays the clusterwide data (Unified Communications Manager clusters only). Each data value in the chart represents the average number of phones that are registered for a 15-minute duration. If a server shows no data, Reporter does not generate the line that represents that server. If no data exists for the server (or for all servers in a Unified Communications Manager cluster configuration), for registered phones, Reporter does not generate the chart. The message “No data for Device Statistics report available” displays.

Figure 4: Line Chart That Depicts Number of Registered Phones Per Server

The following figure shows an example of a line chart representing the number of registered phones per Unified Communications Manager server in a Unified Communications Manager cluster configuration.

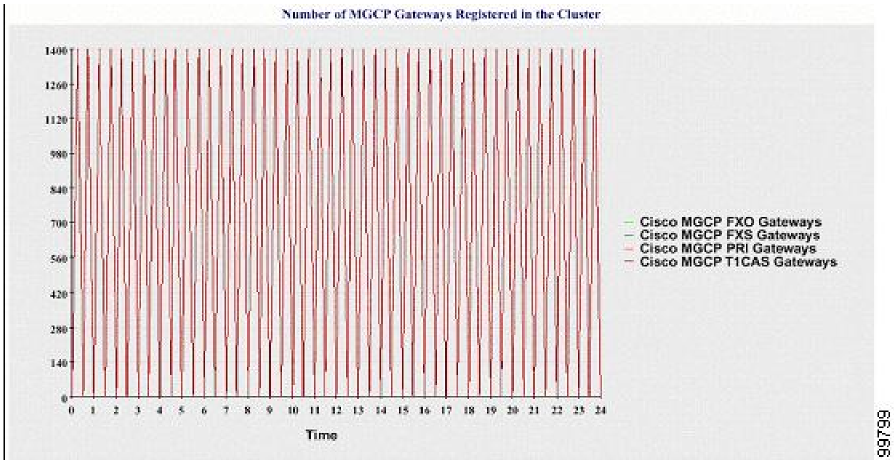


Number of MGCP Gateways Registered in the Cluster

A line chart displays the number of registered MGCP FXO, FXS, PRI, and T1CAS gateways. Each line represents data only for the Unified Communications Manager server (or cluster in a Unified Communications Manager cluster configuration); so, four lines show server (or clusterwide) details for each gateway type. Each data value in the chart represents the average number of MGCP gateways that are registered for a 15-minute duration. If no data exists for a gateway for the server (or all the servers in a cluster), Reporter does not generate the line that represents data for that particular gateway. If no data exists for all gateways for the server (or for all servers in a cluster), Reporter does not generate the chart.

Figure 5: Line Chart That Depicts Number of Registered Gateways Per Cluster

The following figure shows an example of a line chart representing the number of registered gateways per cluster, in a Unified Communications Manager cluster configuration.

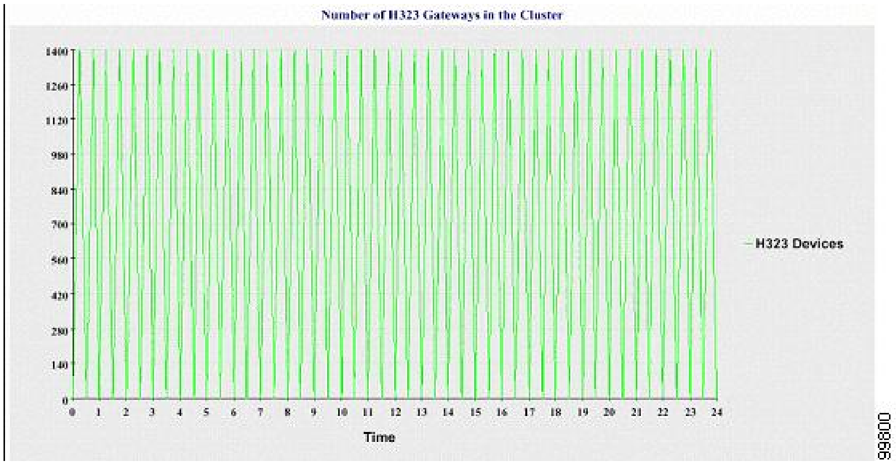


Number of H.323 Gateways in the Cluster

A line chart displays the number of H.323 gateways. One line represents the details of the H.323 gateways (or the clusterwide details in a Unified Communications Manager cluster configuration). Each data value in the chart represents the average number of H.323 gateways for a 15-minute duration. If no data exists for H.323 gateways for the server (or for all servers in a cluster), Reporter does not generate the chart.

Figure 6: Line Chart That Depicts Number of Registered H.323 Gateways Per Cluster

The following figure shows an example line chart representing the number of H.323 gateways per cluster in a Unified Communications Manager cluster configuration.

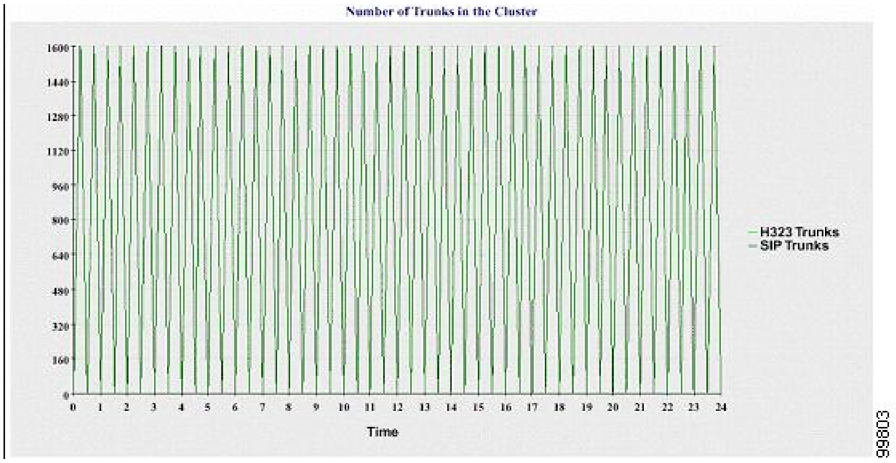


Number of Trunks in the Cluster

A line chart displays the number of H.323 and SIP trunks. Two lines represent the details of the H.323 trunks and SIP trunks (or the clusterwide details in a Unified Communications Manager cluster configuration). Each data value in the chart represents the average number of H.323 and SIP trunks for a 15-minute duration. If no data exists for H.323 trunks for the server (or for all servers in a cluster), Reporter does not generate the line that represents data for the H.323 trunks. If no data exists for SIP trunks for the server (or for all servers in the cluster), Reporter does not generate the line that represents data for SIP trunks. If no data exists for trunks at all, Reporter does not generate the chart.

Figure 7: Line Chart That Depicts Number of Trunks Per Cluster

The following figure shows an example line chart representing the number of trunks per cluster in a Unified Communications Manager cluster configuration.



The server (or each server in the cluster) contains log files that match the filename pattern DeviceLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Number of registered phones on the server (or on each server in a Unified Communications Manager cluster)
- Number of registered MGCP FXO, FXS, PRI, and T1CAS gateways on the server (or on each server in a Unified Communications Manager cluster)

- Number of registered H.323 gateways on the server (or on each server in a Unified Communications Manager cluster)
- Number of SIP trunks and H.323 trunks

Server Statistics Report

The Server Statistics Report provides the following line charts:

- Percentage of CPU per Server
- Percentage of Memory Usage per Server
- Percentage of Hard Disk Usage of the Largest Partition per Server

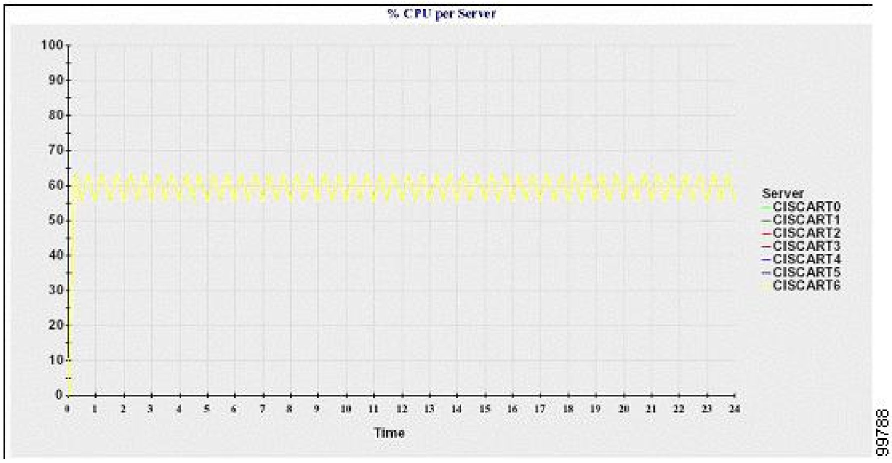
Cluster-specific statistics are only supported by Unified Communications Manager and IM and Presence Service.

Percentage of CPU Per Server

A line chart displays the percentage of CPU usage for the server (or for each server in a cluster). The line in the chart represents the data for the server (or one line for each server in a cluster) for which data is available. Each data value in the chart represents the average CPU usage for a 15-minute duration. If no data exists for the server (or for any one server in a cluster), Reporter does not generate the line that represents that server. If there are no lines to generate, Reporter does not create the chart. The message “No data for Server Statistics report available” displays.

Figure 8: Line Chart That Depicts the Percentage of CPU Per Server

The following figure shows a line chart example representing the percentage of CPU usage per server in a Unified Communications Manager cluster configuration.

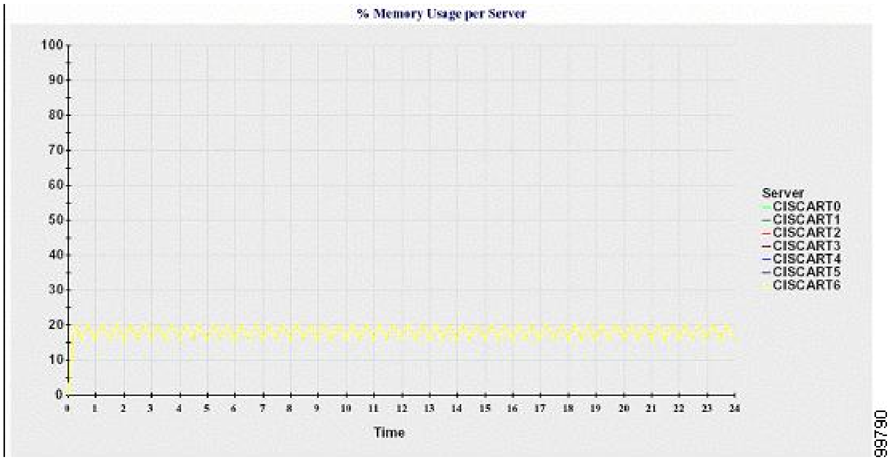


Percentage of Memory Usage Per Server

A line chart displays the percentage of Memory Usage for the Unified Communications Manager server (%MemoryInUse). In a Unified Communications Manager cluster configuration, there is one line per server in the cluster for which data is available. Each data value in the chart represents the average memory usage for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any server in a cluster configuration, Reporter does not generate the line that represents that server.

Figure 9: Line Chart That Depicts Percentage of Memory Usage Per Server

The following figure shows a line chart example representing the percentage of memory usage per Unified Communications Manager server in a cluster configuration.

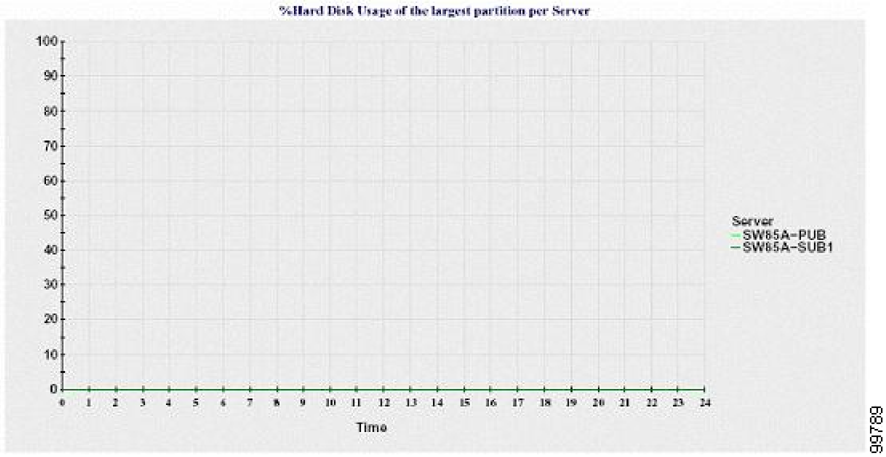


Percentage of Hard Disk Usage of the Largest Partition Per Server

A line chart displays the percentage of disk space usage for the largest partition on the server (%DiskSpaceInUse), or on each server in a cluster configuration. Each data value in the chart represents the average disk usage for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a cluster configuration, Reporter does not generate the line that represents that server.

Figure 10: Line Chart That Depicts Percentage of Hard Disk Usage of the Largest Partition Per Server

The following figure shows a line chart example representing the percentage of hard disk usage for the largest partition per server in a Unified Communications Manager cluster configuration.



The server (or each server in a cluster configuration) contains log files that match the filename pattern ServerLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Percentage of CPU usage on the server (or each server in a cluster)

- Percentage of Memory usage (%MemoryInUse) on the server (or on each server in a cluster)
- Percentage of Hard disk usage of the largest partition (%DiskSpaceInUse) on the server (or on each server in a cluster)

Service Statistics Report

The Service Statistics Report does not support IM and Presence Service and Cisco Unity Connection.

The Service Statistics Report provides the following line charts:

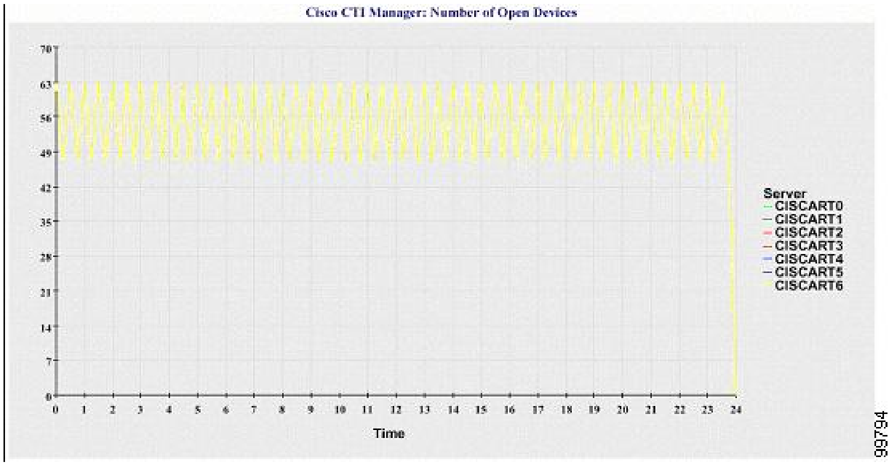
- Cisco CTI Manager: Number of Open Devices
- Cisco CTI Manager: Number of Open Lines
- Cisco TFTP: Number of Requests
- Cisco TFTP: Number of Aborted Requests

Cisco CTI Manager: Number of Open Devices

A line chart displays the number of CTI Open Devices for the CTI Manager (or for each CTI Manager in a Unified Communications Manager cluster configuration). Each line chart represents the data for the server (or on each server in a Unified Communications Manager cluster) on which service is activated. Each data value in the chart represents the average number of CTI open devices for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server. The message “No data for Service Statistics report available” displays.

Figure 11: Line Chart That Depicts Cisco CTI Manager: Number of Open Devices

The following figure shows a line chart example representing the number of open devices per Cisco CTI Manager in a Unified Communications Manager cluster configuration.

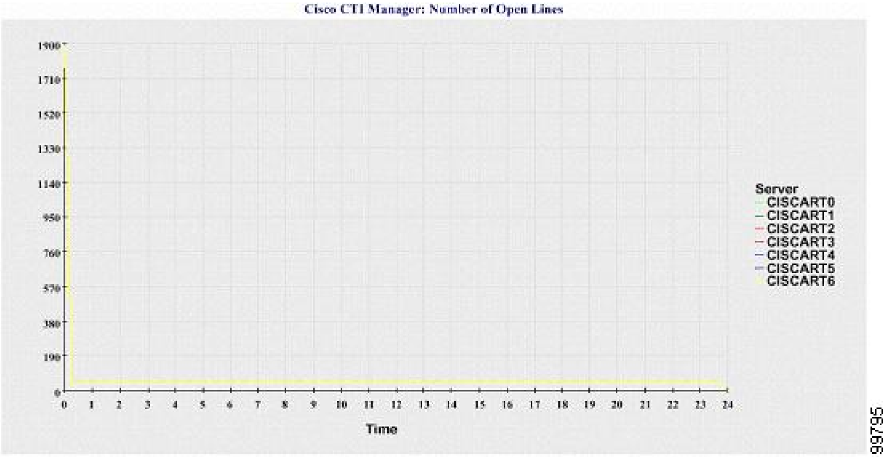


Cisco CTI Manager: Number of Open Lines

A line chart displays the number of CTI open lines for the CTI Manager (or per CTI Manager in a Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Unified Communications Manager cluster configuration) where the Cisco CTI Manager service is activated. Each data value in the chart represents the average number of CTI open lines for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 12: Line Chart That Depicts Cisco CTI Manager: Number of Open Lines

The followings figure shows a line chart example representing the number of open lines per Cisco CTI Manager in a Unified Communications Manager cluster configuration.

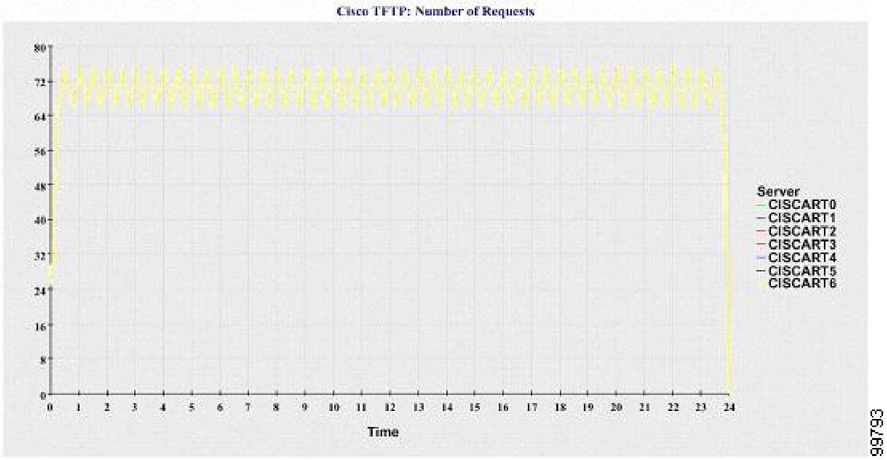


Cisco TFTP: Number of Requests

A line chart displays the number of Cisco TFTP requests for the TFTP server (or per TFTP server in a Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Unified Communications Manager cluster) where the Cisco TFTP service is activated. Each data value in the chart represents the average number of TFTP requests for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 13: Line Chart That Depicts Cisco TFTP: Number of Requests

The following figure shows a line chart example representing the number of Cisco TFTP requests per TFTP server.

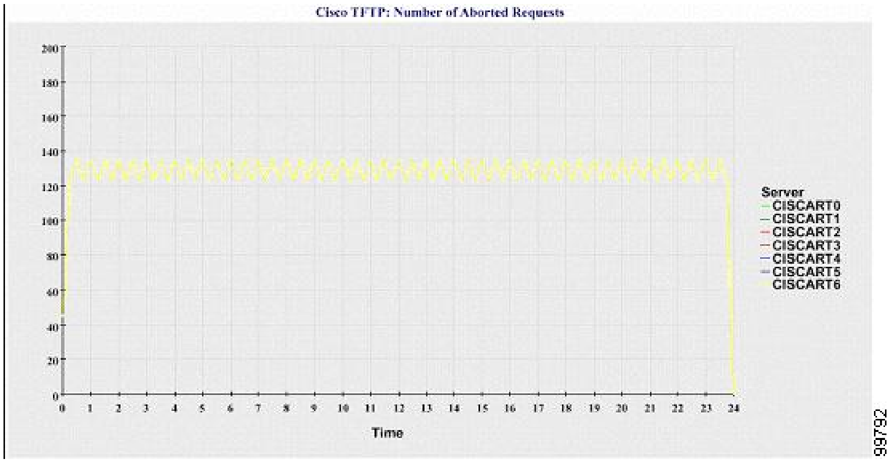


Cisco TFTP: Number of Aborted Requests

A line chart displays the number of Cisco TFTP requests that were aborted for the TFTP server (or per TFTP server in a Unified Communications Manager cluster configuration). A line in the chart represents the data for the server (or one line for each server in a Unified Communications Manager cluster) where the Cisco TFTP service is activated. Each data value in the chart represents the average of TFTP requests that were aborted for a 15-minute duration. If no data exists, Reporter does not generate the chart. If no data exists for any one server in a Unified Communications Manager cluster configuration, Reporter does not generate the line that represents that server.

Figure 14: Line Chart That Depicts Cisco TFTP: Number of Aborted Requests

The following figure shows a line chart example that represents the number of Cisco TFTP requests that were aborted per TFTP server.



The server (or each server in a Unified Communications Manager cluster) contains log files that match the filename pattern ServiceLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- For each CTI Manager - Number of open devices
- For each CTI Manager - Number of open lines
- For each Cisco TFTP server - TotalTftpRequests
- For each Cisco TFTP server - TotalTftpRequestsAborted

Call Activities Report

The Call Activities Report does not support IM and Presence Service and Cisco Unity Connection.

The Call Activities Report provides the following line charts:

- Unified Communications Manager Call Activity for a cluster
- H.323 Gateways Call Activity for the Cluster
- MGCP Gateways Call Activity for the Cluster
- MGCP Gateways
- Trunk Call Activity for the Cluster

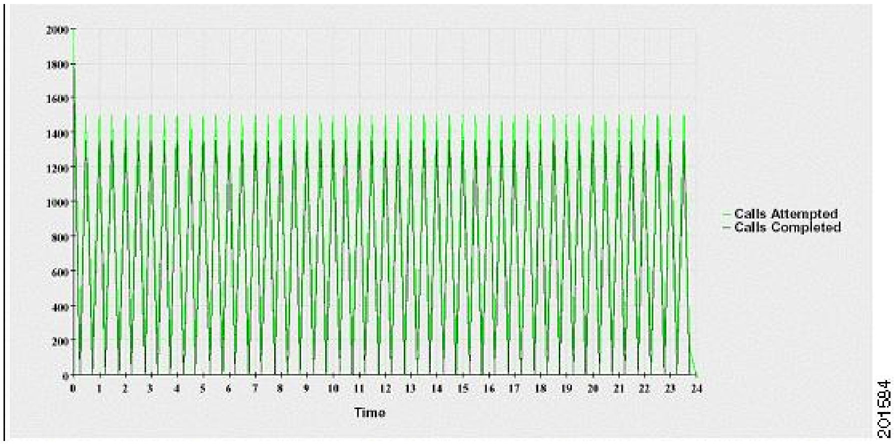
Cisco Unified Communications Manager Call Activity for the Cluster

A line chart displays the number of Unified Communications Manager calls that were attempted and calls that were completed. In a Unified Communications Manager cluster configuration, the line chart displays the number of calls attempted and completed for the entire cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. For a Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration.

If no data exists for Unified Communications Manager calls that were completed, Reporter does not generate the line that represents data for the calls that were completed. If no data exists for Unified Communications Manager calls that were attempted, Reporter does not generate the line that represents data for the calls that were attempted. In a Unified Communications Manager cluster configuration, if no data exists for a server in the cluster, Reporter does not generate the line that represents calls attempted or completed on that server. If no data exists for Unified Communications Manager call activities at all, Reporter does not generate the chart. The message “No data for Call Activities report available” displays.

Figure 15: Line Chart That Depicts Cisco Unified Communications Manager Call Activity for a Cluster

The following figure shows a line chart representing the number of attempted and completed calls for a Unified Communications Manager cluster.

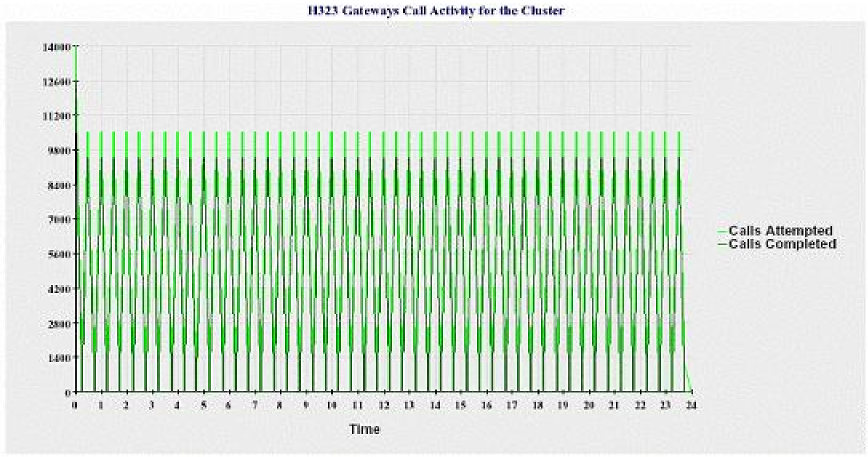


H.323 Gateways Call Activity for the Cluster

A line chart displays the number of calls that were attempted and calls that were completed for H.323 gateways. In a Unified Communications Manager cluster configuration, the line chart displays the number of calls attempted and completed for the entire cluster. The chart comprises two lines, one for the number of calls that were attempted and another for the number of calls that were completed. For a Unified Communications Manager cluster configuration, each line represents the cluster value, which equals the sum of the values for all the servers in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were attempted or calls that were completed for a 15-minute duration. If no data exists for H.323 gateways calls that were completed, Reporter does not generate the line that represents data for calls that were completed. If no data exists for H.323 gateways calls that were attempted, Reporter does not generate the line that represents data for calls that were attempted. In a Unified Communications Manager cluster configuration, if no data exists for a server in the cluster, Reporter does not generate the line that represents calls attempted or completed on that server. If no data exists for H.323 gateways call activities at all, Reporter does not generate the chart.

Figure 16: Line Chart That Depicts H.323 Gateways Call Activity for the Cluster

The following figure shows a line chart representing the H.323 gateway call activity for a Unified Communications Manager cluster.

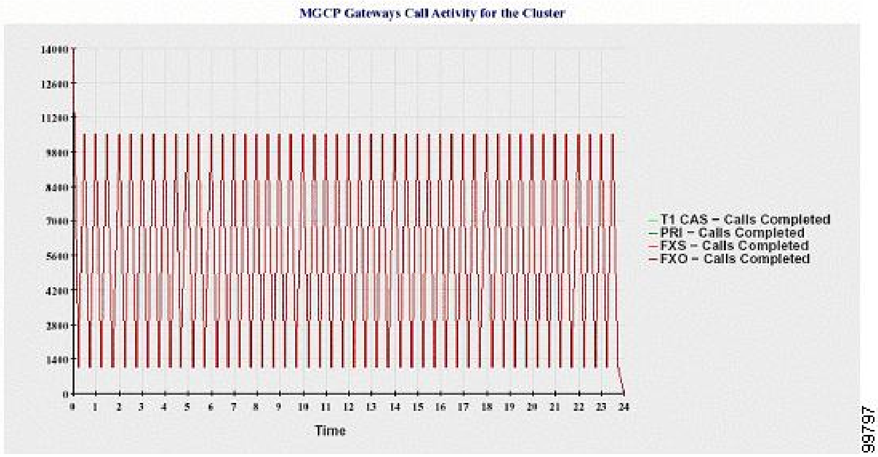


MGCP Gateways Call Activity for the Cluster

A line chart displays the number of calls that were completed in an hour for MGCP FXO, FXS, PRI, and T1CAS gateways. In a Unified Communications Manager cluster configuration, the chart displays the number of calls that were completed for the entire Unified Communications Manager cluster. The chart comprises four lines at the most, one for the number of calls that were completed for each of the gateway types (for which data is available). Each data value in the chart represents the total number of calls that were completed for a 15-minute duration. If no data exists for a gateway, Reporter does not generate the line that represents data for calls that were completed for a particular gateway. If no data exists for all gateways, Reporter does not generate the chart.

Figure 17: Line Chart That Depicts MGCP Gateways Call Activity for the Cluster

The following figure shows a line chart representing the MGCP gateways call activity for a Unified Communications Manager cluster.

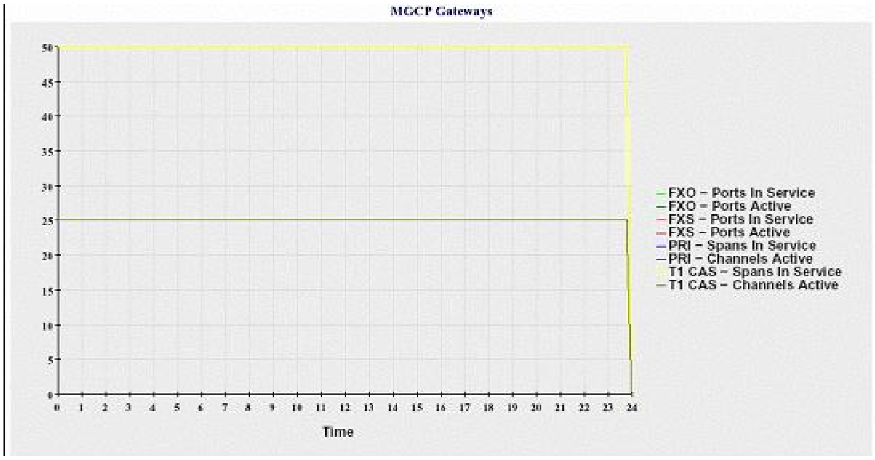


MGCP Gateways

A line chart displays the number of Ports In Service and Active Ports for MGCP FXO, FXS gateways and the number of Spans In Service or Channels Active for PRI, T1CAS gateways. For a Unified Communications Manager cluster configuration, the chart displays the data for the entire Unified Communications Manager cluster. The chart comprises eight lines, two lines each for the number of Ports In Service for MGCP FXO and FXS, and two lines each for the number of Active Ports for MGCP FXO and FXS. Four more lines for the number of Spans In Service and Channels Active for PRI and T1CAS gateways exist. For a Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all servers in the cluster (for which data is available). Each data value in the chart represents the total Number of Ports In Service, Number of Active Ports, Spans In Service or Channels Active for a 15-minute duration. If no data exists for the number of Spans In Service or the Channels Active for a gateway (MGCP PRI, T1CAS) for all servers, Reporter does not generate the line that represents data for that particular gateway.

Figure 18: Line Chart That Depicts MGCP Gateways

The following figure shows a line chart representing the MGCP gateways.

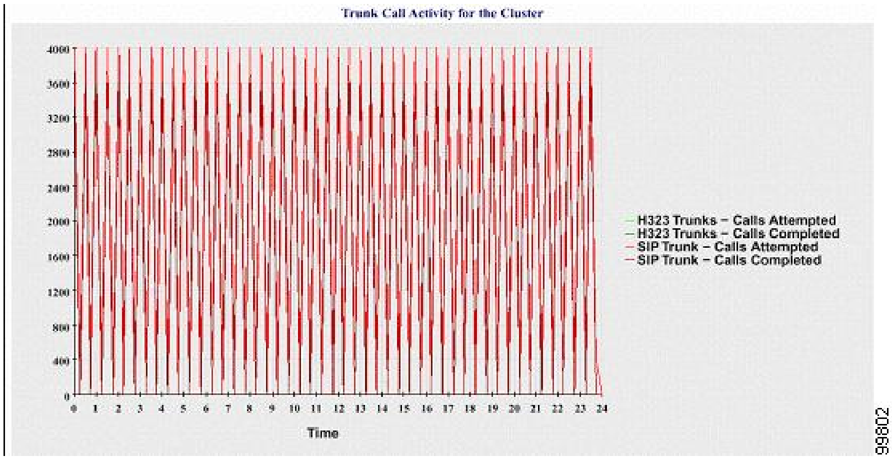


Trunk Call Activity for the Cluster

A line chart displays the number of calls that were completed and calls that were attempted in an hour for SIP trunk and H.323 trunk. For a Unified Communications Manager cluster configuration, the chart displays the number of calls that were completed and calls that were attempted for the entire Unified Communications Manager cluster. The chart comprises four lines, two for the number of calls that were completed for each SIP and H.323 trunk (for which data is available) and two for the number of calls that were attempted. For a Unified Communications Manager cluster configuration, each line represents the cluster value, which is the sum of the values for all nodes in the cluster (for which data is available). Each data value in the chart represents the total number of calls that were completed or number of calls that were attempted for a 15-minute duration. If no data exists for a trunk, Reporter does not generate the line that represents data for the calls that were completed or the calls that were attempted for that particular trunk. If no data exists for both trunk types, Reporter does not generate the chart.

Figure 19: Line Chart That Depicts Trunk Call Activity for the Cluster

The following figure shows a line chart representing the trunk call activity for a Unified Communications Manager cluster.



The server (or each server in a Unified Communications Manager cluster configuration) contains log files that match the filename pattern CallLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Calls that were attempted and calls that were completed for Unified Communications Manager (or for each server in a Unified Communications Manager cluster)
- Calls that were attempted and calls that were completed for the H.323 gateways (or for the gateways in each server in a Unified Communications Manager cluster)
- Calls that were completed for the MGCP FXO, FXS, PRI, and T1CAS gateways (or for the gateways in each server in a Unified Communications Manager cluster)
- Ports in service, active ports for MGCP FXO and FXS gateways and spans in service, channels active for PRI, and T1CAS gateways (in each server in a Unified Communications Manager cluster)
- Calls that were attempted and calls that were completed for H.323 trunks and SIP trunks

Alert Summary Report

The Alert Summary Report provides the details of alerts that are generated for the day.

Cluster-specific statistics are supported only by Unified Communications Manager and IM and Presence Service.

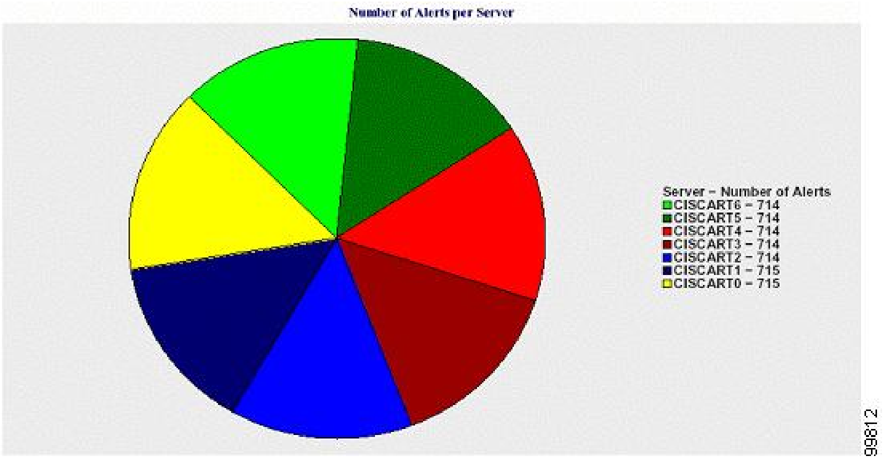
Number of Alerts Per Server

A pie chart provides the number of alerts per node in a cluster. The chart displays the serverwide details of the alerts that are generated. Each sector of the pie chart represents the number of alerts generated for a particular server in the cluster. The chart includes as many number of sectors as there are servers (for which Reporter generates alerts in the day) in the cluster. If no data exists for a server, no sector in the chart represents that server. If no data exists for all servers, Reporter does not generate the chart. The message “No alerts were generated for the day” displays.

Cisco Unity Connection only: A pie chart provides the number of alerts for the server. The chart displays the serverwide details of the alerts that are generated. If no data exists for the server, Reporter does not generate the chart. The message “No alerts were generated for the day” displays.

The following chart shows a pie chart example that represents the number of alerts per server in a Unified Communications Manager cluster.

Figure 20: Pie Chart That Depicts Number of Alerts Per Server

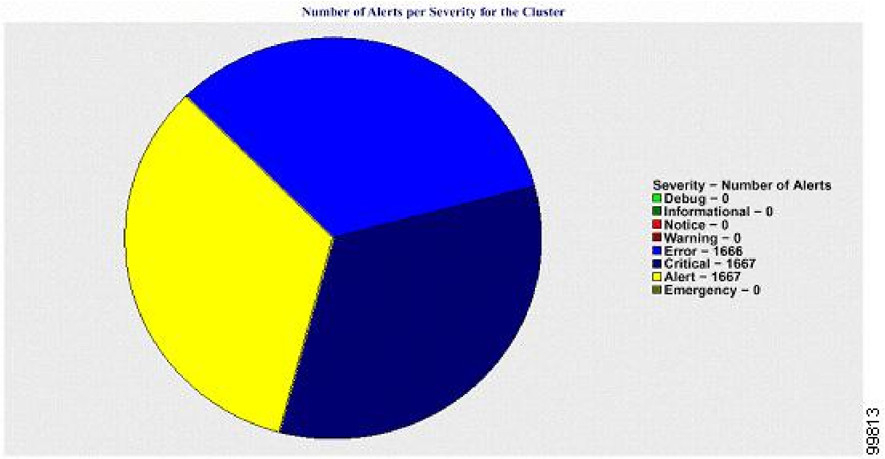


Number of Alerts Per Severity for the Cluster

A pie chart displays the number of alerts per alert severity. The chart displays the severity details of the alerts that are generated. Each sector of the pie chart represents the number of alerts that are generated of a particular severity type. The chart provides as many number of sectors as there are severities (for which Reporter generates alerts in the day). If no data exists for a severity, no sector in the chart represents that severity. If no data exists, Reporter does not generate the chart.

The following chart shows a pie chart example that represents the number of alerts per severity for a Unified Communications Manager cluster.

Figure 21: Pie Chart That Depicts Number of Alerts Per Severity for the Cluster

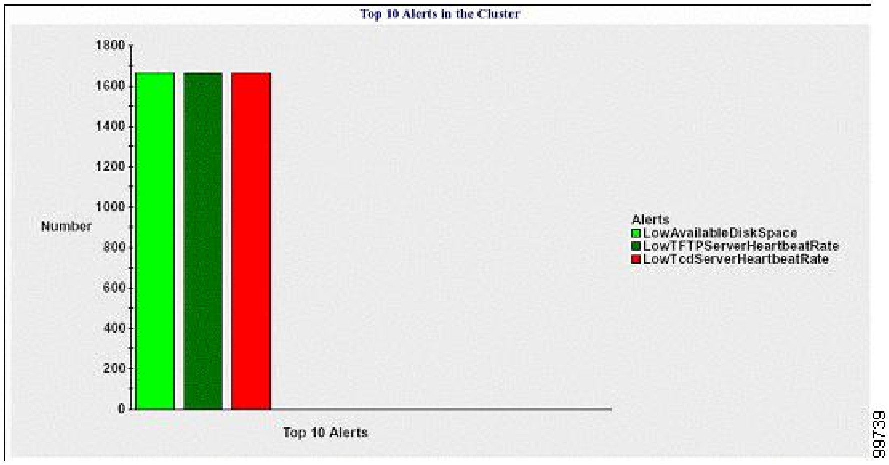


Top Ten Alerts in the Cluster

A bar chart displays the number of alerts of a particular alert type. The chart displays the details of the alerts that are generated on the basis of the alert type. Each bar represents the number of alerts for an alert type. The chart displays details only for the first ten alerts based on the highest number of alerts in descending order. If no data exists for a particular alert type, no bar represents that alert. If no data exists for any alert type, RTMT does not generate the chart.

The following chart shows a bar chart example that represents the top ten alerts in a Unified Communications Manager cluster.

Figure 22: Bar Chart That Depicts Top 10 Alerts in the Cluster



The server (or each server in a cluster) contains log files that match the filename pattern AlertLog_mm_dd_yyyy_hh_mm.csv. The following information exists in the log file:

- Time - Time at which the alert occurred
- Alert Name - Descriptive name
- Node Name - Server on which the alert occurred
- Monitored object - The object that is monitored
- Severity - Severity of this alert

Performance Protection Report

The Performance Protection Report does not support IM and Presence Service and Cisco Unity Connection.

The Performance Protection Report provides a summary that comprises different charts that display the statistics for that particular report. Reporter generates reports once a day on the basis of logged information.

The Performance Protection Report provides trend analysis information on default monitoring objects for the last seven that allows you to track information about Cisco Intercompany Media Engine. The report includes the Cisco IME Client Call Activity chart that shows the total calls and fallback call ratio for the Cisco IME client.

The Performance Protection report comprises the following charts:

- Cisco Unified Communications Manager Call Activity
- Number of registered phones and MGCP gateways
- System Resource Utilization

- Device and Dial Plan Quantities

Cisco Unified Communications Manager Call Activity

A line chart displays the hourly rate of increase or decrease for number of calls that were attempted and calls that were completed as the number of active calls. For a Unified Communications Manager cluster configuration, the data is charted for each server in the cluster. The chart comprises three lines, one for the number of calls that were attempted, one for the calls that were completed, and one for the active calls. If no data exists for call activity, Reporter does not generate the chart.

Number of Registered Phones and MGCP Gateways

A line chart displays the number of registered phones and MGCP gateways. For a Unified Communications Manager cluster configuration, the chart displays the data for each server in the cluster.The chart comprises two lines, one for the number of registered phones and another for the number of MGCP gateways. If no data exists for phones or MGCP gateways, Reporter does not generate the chart.

System Resource Utilization

A line chart displays the CPU load percentage and the percentage of memory that is used (in bytes) for the server (or for the whole cluster in a Unified Communications Manager cluster configuration). The chart comprises two lines, one for the CPU load and one for the memory usage. In a Unified Communications Manager cluster, each line represents the cluster value, which is the average of the values for all the servers in the cluster (for which data is available). If no data exists for phones or MGCP gateways, Reporter does not generate the chart.

Device and Dial Plan Quantities

Two tables display information from the Unified Communications Manager database about the numbers of devices and number of dial plan components. The device table shows the number of IP phones, Cisco Unity Connection ports, H.323 clients, H.323 gateways, MGCP gateways, MOH resources, and MTP resources. The dial plan table shows the number of directory numbers and lines, route patterns, and translation patterns.

CHAPTER 21

Cisco Unified Reporting

Consolidated Data Reporting

The Cisco Unified Reporting web application, which is accessed at the Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service consoles, generates consolidated reports for troubleshooting or inspecting cluster data.

Note Unless stated otherwise, the information, notes, and procedures in this guide apply to Unified Communications Manager and the IM and Presence Service.

This tool provides an easy way to take a snapshot of cluster data. The tool gathers data from existing sources, compares the data, and reports irregularities. When you generate a report in Cisco Unified Reporting, the report combines data from one or more sources on one or more servers into one output view. For example, you can view a report that shows the *hosts* file for all servers in the cluster.

The Cisco Unified Reporting web application deploys to all nodes in a cluster at installation time. Reports are generated from database records.

Note On Cisco Business Edition 5000 servers, the Cisco Unified Reporting application captures data for Unified Communications Manager only. Due to size constraints, the application does not capture data for Cisco Unity Connection. You can use the tool to gather important information about your Unified Communications Manager installation.

Data Sources Used to Generate Reports

The application captures information from any of the following sources on the publisher node and each subscriber node.

- RTMT counters
- CDR_CAR (Unified Communications Manager only)
- Unified Communications Manager DB (Unified Communications Manager only)
- IM and Presence DB (IM and Presence Service only)
- disk files
- OS API calls
- network API calls
- prefs
- CLI
- RIS

The report includes data for all active clusters that are accessible at the time that you generate the report. If the database on the publisher node is down, you can generate a report for the active nodes. The Report Descriptions report in the System Reports list provides the information sources for a report.

Supported Output Format

This release supports HTML/CSV output for reports. You can identify a report in Cisco Unified Reporting by the report name and the date-and-time stamp. The application stores a local copy of the most recent report for you to view. You can download the local copy of the most recent report or a new report to your hard disk, as described in “Download new report.” After you download a report, you can rename downloaded files or store them in different folders for identification purposes.

System Requirements

Cisco Tomcat Service

Cisco Unified Reporting runs as an application on the Cisco Tomcat service, which activates when you install Unified Communications Manager and the IM and Presence Service. Ensure that these products are running on all nodes in the cluster.

HTTPS

The report subsystem gathers information from other nodes by using an RPC mechanism via HTTPS. Ensure the HTTPS port is open and the Cisco Tomcat service is running on the node to successfully generate a report.

To enable HTTPS, you must download a certificate that identifies the node during the connection process. You can accept the node certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that node. The trust folder stores the certificates for all your trusted sites. For more information about HTTPS, see the “Introduction” chapter in the *Cisco Unified Communications Manager Administration Guide*.

To access the application, you access the Administration interface in a browser window. Cisco Unified Reporting uses HTTPS to establish a secure connection to the browser.

Required Access Permissions

The Cisco Unified Reporting application uses the Cisco Tomcat service to authenticate users before allowing access to the web application. Only authorized users can access the Cisco Unified Reporting application. For Unified Communications Manager, by default, only administrator users in the Standard CCM Super Users group can access Cisco Unified Reporting to view and create reports.

For Cisco Unified Communications Manager and IM and Presence Service, users in the Standard CUReporting Authentication role can access Cisco Unified Reporting.

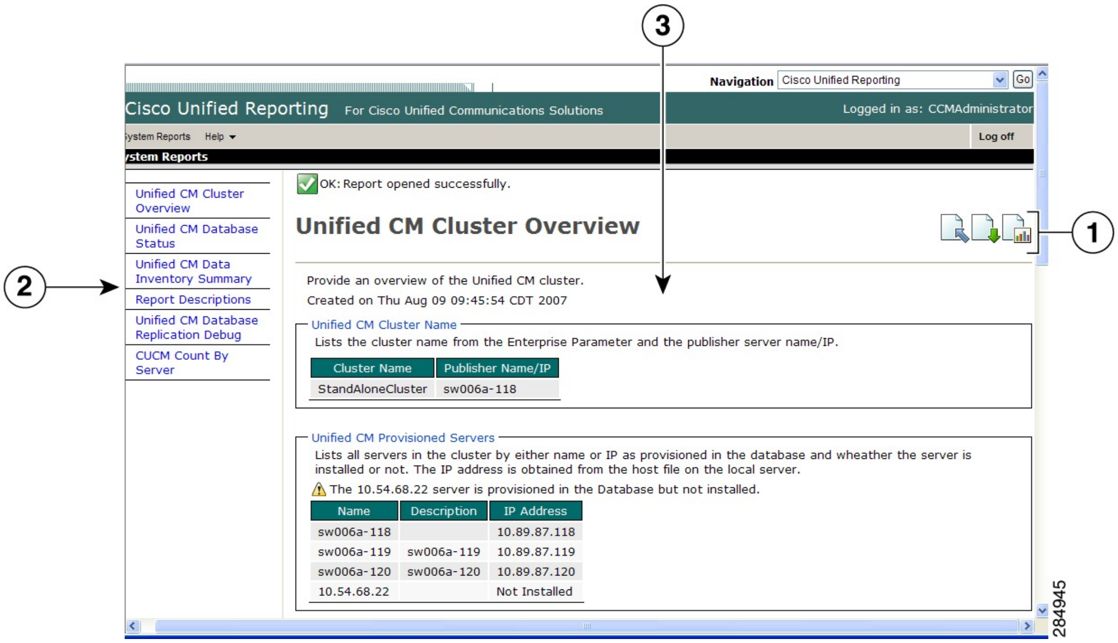
As an authorized user, you can use the Cisco Unified Reporting user interface to view reports, generate new reports, or download reports.

Note For Unified Communications Manager, administrator users in the Standard CCM Super Users group can access administrative applications in the Unified Communications Manager Administration navigation menu, including Cisco Unified Reporting, with a single sign-on to one of the applications.

UI Components

The following figure shows the UI components for Cisco Unified Reporting.

Figure 23: UI Components


3
Navigation
Cisco Unified Reporting
Go
Cisco Unified Reporting
For Cisco Unified Communications Solutions
Logged in as: CCMAdministrator
ystem Reports
Help
Log off
ystem Reports
Unified CM Cluster Overview
Unified CM Database Status
Unified CM Data Inventory Summary
Report Descriptions
Unified CM Database Replication Debug
CUCM Count By Server
1
2
284945

✓ OK: Report opened successfully.

Unified CM Cluster Overview

Provide an overview of the Unified CM cluster.

Created on Thu Aug 09 09:45:54 CDT 2007

Unified CM Cluster Name

Lists the cluster name from the Enterprise Parameter and the publisher server name/IP.

Cluster Name	Publisher Name/IP
StandAloneCluster	sw006a-118

Unified CM Provisioned Servers

Lists all servers in the cluster by either name or IP as provisioned in the database and wheather the server is installed or not. The IP address is obtained from the host file on the local server.

⚠ The 10.54.68.22 server is provisioned in the Database but not installed.

Name	Description	IP Address
sw006a-118		10.89.87.118
sw006a-119	sw006a-119	10.89.87.119
sw006a-120	sw006a-120	10.89.87.120
10.54.68.22		Not Installed

1. Upload, Download, Generate icons
2. Report List
3. Report Details

Note The report categories, available reports, and report data vary, depending on release.

Sign In From Administration Interface

Perform either of the following steps to sign in to Cisco Unified Reporting from the Administration interface.

- For Unified Communications Manager, select **Cisco Unified Reporting** from the navigation menu in the Cisco Unified CM Administration interface.
- For the IM and Presence Service, select **Cisco Unified IM and Presence Reporting** from the navigation menu in the Cisco Unified CM IM and Presence Administration interface.

Before you begin

Ensure that you are authorized to access the Cisco Unified Reporting application.

When you log in to Cisco Unified Reporting, the last successful system login attempt and the last unsuccessful system login attempt for each user along with the user id, date, time and IP address is displayed in the main Cisco Unified Reporting window.

Supported Reports

This section details the supported reports for Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service. You can identify a report in Cisco Unified Reporting by the report name and the date-and-time stamp. Cisco Unified Reporting stores a local copy of the most recent report for you to view.

Unified Communications Manager Reports

The following table describes the types of system reports that appear in Cisco Unified Reporting after you install Unified Communications Manager.

Table 74: Unified Communications Manager Reports That Appear in Cisco Unified Reporting

Report	Description
UCM Users with Out-Of-Date Credential Algorithm	Provides a list of end users' whose passwords or PINs are stored and hashed using SHA1.
Report Descriptions	Provides troubleshooting and detailed information about the reports that appear.
Security Diagnostic Tool	Provides a summary view of information about security components.

Report	Description
Unified CM Cluster Overview	Provides an overview of the Unified Communications Manager cluster. This report includes the following details: • The Unified Communications Manager or IM and Presence Service versions that are installed in the cluster • The hostname or IP address of all nodes in the cluster • A summary of hardware details
Unified CM Data Summary	Provides a summary of data that exists in the Unified Communications Manager database, according to the structure of the menus in Unified Communications Manager Administration. For example, if you configure three credential policies, five conference bridges, and ten shared-line appearances, you can see that type of information in this report.
Unified CM Database Replication Debug	Provides debugging information for database replication. **Tip** For this report, generation may spike CPU and take up to 10 seconds per node in the cluster.
Unified CM Database Status	Provides a snapshot of the health of the Unified Communications Manager database. Generate this report before an upgrade to ensure that the database is healthy.
Unified CM Device Counts Summary	Provides the number of devices by model and protocol that exist in the Unified Communications Manager database.
Unified CM Device Distribution Summary	Provides a summary of how devices are distributed throughout the cluster; for example, this report shows which devices are associated with the primary, secondary, and tertiary nodes.
Unified CM Directory URI and GDPR Duplicates	Provides a detailed list of duplicated User Directory URIs, Learned Directory URIs, Learned Numbers, and Learned Patterns on the system.
Unified CM Extension Mobility	Provides a summary of Cisco Extension Mobility usage; for example, the number of phones that have a Cisco Extension Mobility user logged in to them, the users that are associated with Cisco Extension Mobility, and so on.
Unified CM GeoLocation Policy	Provides a list of records from the GeoLocation Logical Partitioning Policy Matrix.
Unified CM GeoLocation Policy with Filter	Provides a list of records from the GeoLocation Logical Partitioning Policy Matrix for the selected GeoLocation policy.
Unified CM Lines Without Phones	Provides a list of lines that are not associated with a phone.
Unified CM Multi-Line Devices	Provides a list of phones with multiple line appearances.

Report	Description
Unified CM Phone Category	Provides a listing of phone models in a given category for use with the Universal Device Templates. When enabling self provisioning for a user, you may choose to allow any or all of these categories of phones by providing a template for each category.
Unified CM Phone Feature List	Provides a list of supported features for each device type in Unified Communications Manager Administration.
Unified CM Phone Locale Installers	Provides a list of Cisco Unified IP Phone firmware versions supported by the installed Phone Locale Packages.
Unified CM Phones With Mismatched Load	Provides a list of all phones that have a mismatched firmware load.
Unified CM Phones Without Lines	Provides a list of all phones in the Unified Communications Manager database that do not have lines that are associated with them.
Unified CM Shared Lines	Provides a list of all phones in the Unified Communications Manager database with at least one shared-line appearance.
Unified CM Table Count Summary	Provides a database-centric view of data. This report is useful for administrators or AXL API developers that understand database schema.
Unified CM User Device Count	Provides information about associated devices; for example, this report lists the number of phones with no users, the number of users with one phone, and the number of users with more than one phone.
Unified CM Users Sharing Primary Extensions	Provides a list of users that share a primary extension on the system.
Unified CM VG2XX Gateway	Provides a summary of gateway endpoint security profiles.
Unified CM Voice Mail	Provides a summary of voice-messaging-related configuration in Unified Communications Manager Administration; for example, this report lists the number of configured voicemail ports, the number of message waiting indicators, the number of configured voice messaging profiles, the number of directory numbers that are associated with voice message profiles, and so on.
Unified Confidential Access Level Matrix	Provides all information about the Confidential Access Level Matrix.

IM and Presence Service Reports

The following table describes the types of system reports that display in Cisco Unified Reporting after you install the IM and Presence Service on Unified Communications Manager.

Note From Release 10.0(1), the IM and Presence cluster information is available from the Cisco Unified Communications Manager node. From Cisco Unified Communications Manager, select **Cisco Unified Reporting** > **System Reports** > **Unified CM Cluster Overview**.

You can view and generate any of the report types in the following table.

Table 75: IM and Presence Service Reports That Display in Cisco Unified Reporting

Report	Description
IM and Presence Database Replication Debug	Provides debugging information for database replication. **Tip** For this report, generation may spike CPU and take up to 10 seconds per node in the cluster.
IM and Presence Database Status	Provides a snapshot of the health of the IM and Presence Service database. Generate this report before an upgrade to ensure that the database is healthy.
IM and Presence Table Count Summary	Provides a database-centric view of data. This report proves useful for administrators or AXL API developers that understand the database schema.
IM and Presence User Sessions Report	Provides a list of all active users signed-in sessions with one or more devices.
Presence Configuration Report	Provides configuration information about IM and Presence Service users. • Users that are synced from Cisco Unified Communications Manager • Users that are enabled for IM and Presence Service • Users that are enabled for Microsoft remote call control • Users that are enabled for calendaring information in IM and Presence Service Click **View Details** to see the list of users in sortable columns.
IM and Presence Cluster Overview	Provides an overview of the IM and Presence Service cluster. This report, for example, tells you which IM and Presence Service version is installed in the cluster, the hostname or IP address of all nodes in the cluster, a summary of hardware details, and so on.
Presence Limits Warning Report	Provides information about users that have met or exceeded the configuration limits for the maximum number of contacts or watchers. Click **View Details** to see the list of users in sortable columns.
Presence Usage Report	Provides usage information for logged-in XMPP clients and third-party APIs. Click **View Details** to see the list of XMPP clients and third-party APIs in sortable columns.

Report	Description
Report Descriptions	Provides troubleshooting and detailed information about the reports that display. This report provides descriptions for the report, for each information group, and for each data item, as well as the data sources, symptoms of related problems, and remedies.

View Report Descriptions

Cisco Unified Reporting provides report help. The Report Descriptions link provides descriptions for the report, for each information group, and for each data item, as well as the data sources, symptoms of related problems, and remedies.

Note You may still need to contact TAC for additional help on report problems.

Procedure

Step 1 Select **System Reports**.

Step 2 Select the **Report Descriptions** link in the list of reports.

Note Re-enter your Cisco Unified Communications Manager Administration login credentials if you are prompted to re-login when you select an IM and Presence Service report.

Step 3 Select the **Generate Report** icon.

The report generates and is displayed.

Generate New Report

You can generate and view a new report.

Before you begin

Ensure that the Cisco Tomcat service is running on at least one node and you are using a supported web browser to view the report.

The application notifies you if a report will take excessive time to generate or consume excessive CPU time. A progress bar displays while the report generates. The new report displays, and the date and time updates.

Procedure

Step 1 Select **System Reports** from the menu bar.

Step 2 Select a report.

Note Re-enter your Cisco Unified Communications Manager Administration login credentials if you are prompted to re-login when you select an IM and Presence Service report.

Step 3 Select the **Generate Report** (bar chart) icon in the **Reports** window.

Step 4 Select the **View Details** link to expose details for a section that does not automatically appear.

What to do next

If the report shows an unsuccessful data check for an item, select the **Report Descriptions** report and review the troubleshooting information and possible remedies. Because the report descriptions report is dynamically generated from the database, you can also generate a new report descriptions report.

View Saved Report

You can view a copy of an existing report.

Note During a fresh install or upgrade, the Cisco Unified Reporting application does not save a local copy of the most recent report.

Before you begin

Ensure that the Cisco Tomcat service is running on at least one node and you are using a supported web browser to view the report.

Procedure

Step 1 Select **System Reports** from the menu bar.

Step 2 Select the report that you want to view from the reports list.

Step 3 Select the link for the report name (dated and time stamped).

Step 4 Select the **View Details** link for details for a section that does not automatically appear.

What to do next

Download a new or saved report.

If the report shows an unsuccessful data check for an item, select the **Report Descriptions** report and review the troubleshooting information for possible remedies.

Download New Report

To download a new report, you store it locally on your hard drive. Downloading a report downloads the raw XML data file to your hard drive.

Procedure

Step 1 Generate the new report.

Step 2 After the new report appears, select the **Download Report** (green arrow) icon in the **Reports** window.

Note You do not need to click the **View Details** link for report details before you download the document. The data are captured in the downloaded file.

Step 3 Select **Save** to save the file to the location on your disk that you designate.

To change the filename or the location where your file is stored on your hard disk, enter a new location or rename the file (optional). A progress bar shows the download in progress.

The file downloads to your hard disk.

Step 4 After the download completes, select **Open** to open the XML report.

Note Do not change the contents in the XML file, or your report may not appear properly on the screen.

What to do next

To view a downloaded report file in your browser, upload the file to your node.

Note For technical assistance, you can attach the downloaded file in an e-mail or upload the file to another node.

Download Saved Report

To download saved reports, you download the report and store it locally on your hard drive. Downloading a report downloads the raw XML data file to your hard disk.

Procedure

Step 1 Open and view the details of the existing report.

Step 2 Select the **Download Report** (green arrow) icon in the **Reports** window.

Step 3 Select **Save** to save the file to the location on your disk that you designate.

To change the filename or the location where your file is stored on your hard disk, enter a new location or rename the file (optional). A progress bar shows the download in progress.

The file downloads to your hard disk.

Step 4 After the download completes, select **Open** to open the XML report.

Note Do not change the contents in the XML file, or your report may not appear properly.

What to do next

To view a downloaded report file in your browser, upload the file to your node.

Note For technical assistance, you can attach the downloaded file in an e-mail or upload the file to another node.

Upload Report

To view a downloaded report in your browser window, you must upload the report to the nodetand,.

Before you begin

Download a report to your hard drive.

Procedure

Step 1 Select **System Reports** from the menu bar.

Step 2 Access any report to display the **Upload Report** (blue arrow) icon in the **Reports** window.

Step 3 Select the **Upload Report** icon.

Step 4 To locate the .xml file, select **Browse** to navigate to its location on your hard drive.

Step 5 Select **Upload**.

Step 6 Select **Continue** to display the uploaded file in the browser window.

What to do next

You can compare an uploaded report and a newly generated report side-by-side during an upgrade.

CHAPTER 22

Configure Call Diagnostics and Quality Reporting for Cisco IP Phones

Diagnostics and Reporting Overview

Cisco Unified Communications Manager offers two options for ensuring call quality on Cisco IP Phones:

- Call Diagnostics—Call diagnostics includes generating Call Management Records (CMR) and voice quality metrics.
- Quality Report Tool QRT)—QRT is a voice-quality and general problem-reporting tool for Cisco Unified IP Phones. This tool allows users to easily and accurately report audio and other general problems with their IP phone.

Call Diagnostics Overview

You can configure Cisco IP Phones that are running SCCP and SIP to collect call diagnostics. Call diagnostics comprises Call Management Records (CMR), also called diagnostic records, and voice quality metrics.

Voice quality metrics are enabled by default and supported on most of the Cisco IP Phones. Cisco IP Phones calculate voice quality metrics based on MOS (Mean Opinion Square) value. Voice quality metrics do not account for noise or distortion, only frame loss.

The CMR records store information about the quality of the streamed audio of the call. You can configure the Unified Communications Manager to generate CMRs. This information is useful for post-processing activities such as generating billing records and network analysis.

Quality Report Tool Overview

The Quality Report Tool (QRT) is a voice-quality and general problem-reporting tool for Cisco IP Phones. This tool allows users to easily and accurately report audio and other general problems with their IP phone.

As a system administrator, you can enable QRT functionality by configuring and assigning a softkey template to display the QRT softkey on a user IP phone. You can choose from two different user modes, depending on the level of user interaction that you want with QRT. You then define how the feature works in your system by configuring system parameters and setting up Cisco Unified Serviceability tools. You can create, customize, and view phone problem reports by using the QRT Viewer application.

When users experience problems with their IP phones, they can report the type of problem and other relevant statistics by pressing the QRT softkey on the Cisco IP Phones during the On Hook or Connected call states. Users can then choose the reason code that best describes the problem that is being reported for the IP phone. A customized phone problem report provides you with the specific information.

QRT attempts to collect the streaming statistics after a user selects the type of problem by pressing the QRT softkey. A call should be active for a minimum of 5 seconds for QRT to collect the streaming statistics.

Detailed Call Reporting and Billing

The Cisco CDR Analysis and Reporting (CAR) tool generates detailed reports for quality of service, traffic, user call volume, billing, and gateways. CAR uses data from Call Detail Records (CDRs), Call Management Records (CMRs), and the Unified Communications Manager database in order to generate reports. The CAR interface can be accessed under the **Tools** menu of Cisco Unified Serviceability.

CAR is not intended to replace call accounting and billing solutions that third-party companies provide. You can find the companies that provide these solutions and that are members of the Cisco Technology Developer Program by searching the home page of the Cisco Developer Community.

For details about how to configure reporting with CAR, refer to the *Call Reporting and Billing Administration Guide for Cisco Unified Communications Manager*.

Prerequisites

Call Diagnostics Prerequisites

Check if your Cisco Unified IP Phone supports Call Diagnostics.

Use this table to determine if your phone supports Call Diagnostics. The Support for Call Diagnostics legend is as follows:

- X—Supported by phones that are running both SCCP and SIP
- S—SCCP feature only

Table 76: Device Support for Call Diagnostics

Device	Support for Call Diagnostics
Cisco Unified IP Phone 7906	X
Cisco Unified IP Phone 7911	X
Cisco Unified IP Phone 7921	X
Cisco Unified IP Phone 7931	X

Device	Support for Call Diagnostics
Cisco Unified IP Phone 7940	S
Cisco Unified IP Phone 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP Phone 7960	S
Cisco Unified IP Phone 7961	X
Cisco Unified IP Phone 7962-G	X
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7970	X
Cisco Unified IP Phone 7971	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

Quality Report Tool Prerequisites

Any Cisco IP Phone that includes the following capabilities:

- Support for softkey templates
- Support for IP phone services
- Controllable by CTI
- Contains an internal HTTP server

For more information, see the guide for your phone model.

Diagnostics and Reporting Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure Call Diagnostics, on page 302	Perform this task to configure Cisco Unified Communications Manager to generate CMRs. The CMR records store information about the

	Command or Action	Purpose
		quality of the streamed audio of the call. For more information about accessing CMRs, see the *Cisco Unified Communications Manager Call Detail Records Administration Guide* . Voice Quality Metrics are automatically enabled on the Cisco IP Phones. For more information about accessing voice quality metrics, see the Cisco Unified IP Phone Administration Guide for your phone model.
Step 2	To Configure the Quality Report Tool, on page 303, perform the following subtasks: • Configure a Softkey Template with the QRT Softkey, on page 304 • Associate a QRT Softkey Template with a Common Device Configuration, on page 305 • Add the QRT Softkey Template to a Phone, on page 306 • Configure QRT in Cisco Unified Serviceability, on page 307 • Configure the Service Parameters for the Quality Report Tool, on page 309	Configure the Quality Report Tool (QRT) so that users who experience problems with their IP phones can report the type of problem and other relevant statistics by pressing a QRT softkey.

Configure Call Diagnostics

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server on which the Cisco CallManager service is running.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.
The **Service Parameter Configuration** window appears.

Step 4 In the **Clusterwide Parameters (Device - General)** area, configure the **Call Diagnostics Enabled** service parameter. The following options are available:

- **Disabled**—CMRs are not generated.
- **Enabled Only When CDR Enabled Flag is True**—CMRs are generated only when the Call Detail Records (CDR) Enabled Flag service parameter is set to True.
- **Enabled Regardless of CDR Enabled Flag**—CMRs are generated regardless of the CDR Enabled Flag service parameter value.

Note Generating CMRs without enabling the CDR Enabled Flag service parameter can cause uncontrolled disk space consumption. Cisco recommends that you enable CDRs when CMRs are enabled.

Step 5 Click **Save**.

Configure the Quality Report Tool

Configure the Quality Report Tool (QRT) so that users who experience problems with their IP phones can report the type of problem and other relevant statistics by pressing a QRT softkey.

Procedure

	Command or Action	Purpose
Step 1	Configure a Softkey Template with the QRT Softkey, on page 304	You must configure the On Hook and Connected call states for the QRT Softkey. The following call states are also available: • Connected Conference • Connected Transfer
Step 2	(Optional) To Associate a QRT Softkey Template with a Common Device Configuration, on page 305, perform the following subtasks: • Add a QRT Softkey Template to a Common Device Configuration, on page 305 • Associate a Common Device Configuration with a Phone, on page 306	To make the softkey template available to phones, you must complete either this step or the following step. Follow this step if your system uses a **Common Device Configuration** to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.
Step 3	(Optional) Add the QRT Softkey Template to a Phone, on page 306	Use this procedure either as an alternative to associating the softkey template with the Common Device Configuration, or in conjunction with the Common Device Configuration. Use this procedure in conjunction with the Common Device Configuration if you need assign a softkey template that overrides the assignment in the Common Device Configuration or any other default softkey assignment.
Step 4	To Configure QRT in Cisco Unified Serviceability, on page 307, perform the following subtasks: • Activate the Cisco Extended Functions Service, on page 307 • Configure Alarms, on page 308 • Configure Traces, on page 308	

	Command or Action	Purpose
Step 5	(Optional) Configure the Service Parameters for the Quality Report Tool, on page 309	

Configure a Softkey Template with the QRT Softkey

You must configure the On Hook and Connected call states for the QRT Softkey. The following call states are also available:

- Connected Conference
- Connected Transfer

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Softkey Template**.

Step 2 Perform the following steps to create a new softkey template; otherwise, proceed to the next step.

a) Click **Add New**.
b) Select a default template and click **Copy**.
c) Enter a new name for the template in the **Softkey Template Name** field.
d) Click **Save**.

Step 3 Perform the following steps to add softkeys to an existing template.

a) Click **Find** and enter the search criteria.
b) Select the required existing template.

Step 4 Check the **Default Softkey Template** check box to designate this softkey template as the default softkey template.

Note If you designate a softkey template as the default softkey template, you cannot delete it unless you first remove the default designation.

Step 5 Choose **Configure Softkey Layout** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 6 From the **Select a Call State to Configure** drop-down list, choose the call state for which you want the softkey to display.

Step 7 From the **Unselected Softkeys** list, choose the softkey to add and click the right arrow to move the softkey to the **Selected Softkeys** list. Use the up and down arrows to change the position of the new softkey.

Step 8 Repeat the previous step to display the softkey in additional call states.

Step 9 Click **Save**.

Step 10 Perform one of the following tasks:

- Click **Apply Config** if you modified a template that is already associated with devices to restart the devices.

- If you created a new softkey template, associate the template with the devices and then restart them. For more information, see *Add a Softkey Template to a Common Device Configuration* and *Associate a Softkey Template with a Phone* sections.

What to do next

Perform one of the following steps:

- Add a QRT Softkey Template to a Common Device Configuration, on page 305
- Add the QRT Softkey Template to a Phone, on page 306

Associate a QRT Softkey Template with a Common Device Configuration

Optional. There are two ways to associate a softkey template with a phone:

- Add the softkey template to the Phone Configuration.
- Add the softkey template to the Common Device Configuration.

The procedures in this section describe how to associate the softkey template with a Common Device Configuration. Follow these procedures if your system uses a Common Device Configuration to apply configuration options to phones. This is the most commonly used method for making a softkey template available to phones.

To use the alternative method, see Add the QRT Softkey Template to a Phone, on page 306.

Procedure

	Command or Action	Purpose
Step 1	Add a QRT Softkey Template to a Common Device Configuration, on page 305	
Step 2	Associate a Common Device Configuration with a Phone, on page 306	

Add a QRT Softkey Template to a Common Device Configuration

Before you begin

Configure a Softkey Template with the QRT Softkey, on page 304

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Perform the following steps to create a new Common Device Configuration and associate the softkey template with it; otherwise, proceed to the next step.

a) Click **Add New**.

b) Enter a name for the Common Device Configuration in the **Name** field.

c) Click **Save**.

Step 3 Perform the following steps to add the softkey template to an existing Common Device Configuration.

a) Click **Find** and enter the search criteria.
b) Click an existing Common Device Configuration.

Step 4 In the **Softkey Template** drop-down list, choose the softkey template that contains the softkey that you want to make available.

Step 5 Click **Save**.

Step 6 Perform one of the following tasks:

- If you modified a Common Device Configuration that is already associated with devices, click **Apply Config** to restart the devices.
- If you created a new Common Device Configuration, associate the configuration with devices and then restart them.

What to do next

Associate a Common Device Configuration with a Phone, on page 306

Associate a Common Device Configuration with a Phone

Before you begin

Add a QRT Softkey Template to a Common Device Configuration, on page 305

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the phone device to add the softkey template.

Step 3 From the **Common Device Configuration** drop-down list, choose the common device configuration that contains the new softkey template.

Step 4 Click **Save**.

Step 5 Click **Reset** to update the phone settings.

Add the QRT Softkey Template to a Phone

Before you begin

Configure a Softkey Template with the QRT Softkey, on page 304

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** to display the list of configured phones.

Step 3 Choose the phone to which you want to add the phone button template.

Step 4 In the **Phone Button Template** drop-down list, choose the phone button template that contains the new feature button.

Step 5 Click **Save**.
A dialog box is displayed with a message to press **Reset** to update the phone settings.

Configure QRT in Cisco Unified Serviceability

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco Extended Functions Service, on page 307	Activate the Cisco Extended Functions Service to provide support for voice-quality features such as the Quality Report Tool.
Step 2	Configure Alarms, on page 308	Configure alarms for the QRT to log errors in the Application Logs within SysLog Viewer. This function logs alarms, provides a description of the alarms, and recommended actions. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool.
Step 3	Configure Traces, on page 308	Configure traces for the QRT to log trace information for your voice application. After configure the information that you want to include in the trace files for the QRT, you can collect and view trace files by using the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool.

Activate the Cisco Extended Functions Service

Activate the Cisco Extended Functions Service to provide support for voice-quality features such as the Quality Report Tool.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the node on which you want to activate the Cisco Extended Functions service.

Step 3 Check the **Cisco Extended Functions** check box.

Step 4 Click **Save**.

What to do next

Configure Alarms, on page 308

Configure Alarms

Configure alarms for the QRT to log errors in the Application Logs within SysLog Viewer. This function logs alarms, provides a description of the alarms, and recommended actions. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool.

Before you begin

Activate the Cisco Extended Functions Service, on page 307

Procedure

Step 1 From the Cisco Unified Serviceability, choose **Alarm** > **Configuration**.

Step 2 From the **Server** drop-down list, choose the node on which you want to configure alarms.

Step 3 From the **Service Group** drop-down list, choose **CM Services**.

Step 4 From the **Service** drop-down list, choose **Cisco Extended Functions**.

Step 5 Check the **Enable Alarm** check box for both Local Syslogs and SDI Trace.

Step 6 From the drop-down list, configure the Alarm Event Level for both Local Syslogs and SDI Trace by choosing one of the following options:

- **Emergency**—Designates the system as unusable.
- **Alert**—Indicates that immediate action is needed.
- **Critical**—The system detects a critical condition.
- **Error**—Indicates that an error condition is detected.
- **Warning**—Indicates that a warning condition is detected.
- **Notice**—Indicates that a normal but significant condition is detected.
- **Informational**—Indicates only information messages.
- **Debug**— Indicates detailed event information that Cisco Technical Assistance Center (TAC) engineers use for debugging.

The default value is **Error**.

Step 7 Click **Save**.

What to do next

Configure Traces, on page 308

Configure Traces

Configure traces for the QRT to log trace information for your voice application. After configure the information that you want to include in the trace files for the QRT, you can collect and view trace files by using the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool.

Before you begin

Configure Alarms, on page 308

Procedure

Step 1 From Cisco Unified Serviceability, choose **Trace** > **Configuration**.

Step 2 From the **Server** drop-down list, choose the node on which you want to configure traces.

Step 3 From the **Service Group** drop-down list, choose **CM Services**.

Step 4 From the **Service** drop-down list, choose **Cisco Extended Functions**.

Step 5 Check the **Trace On** check box.

Step 6 From the **Debug Trace Level** drop-down list, choose one of the following options:

- **Error**—Traces all error conditions, as well as process and device initialization messages.
- **Special**—Traces all special conditions and subsystem state transitions that occur during normal operation. Traces call-processing events.
- **State Transition**—Traces all state transition conditions and media layer events that occur during normal operation.
- **Significant**—Traces all significant conditions, as well as entry and exit points of routines. Not all services use this trace level.
- **Entry_exit**—Traces all entry and exit conditions, plus low-level debugging information.
- **Arbitrary**—Traces all Arbitrary conditions plus detailed debugging information.
- **Detailed**— Traces alarm conditions and events. Used for all traces that are generated in abnormal path. Uses minimum number of CPU cycles.

The default value is **Error**.

Tip We recommend that you check all the check boxes in this section for troubleshooting purposes.

Step 7 Click **Save**.

What to do next

(Optional) Configure the Service Parameters for the Quality Report Tool, on page 309

Configure the Service Parameters for the Quality Report Tool

Caution We recommend that you use the default service parameters settings unless the Cisco Technical Assistance Center (TAC) instructs otherwise.

Procedure

Step 1 From Cisco Unified Communications Manager Administration , choose **System** > **Service Parameters**.

Step 2 Choose the node where the QRT application resides.

Step 3 Choose the **Cisco Extended Functions** service.

Step 4 Configure the service parameters. See the Related Topics section for more information about the service parameters and their configuration options.

Step 5 Click **Save**.

Related Topics

Quality Report Tool Service Parameters, on page 310

Quality Report Tool Service Parameters

Table 77: Quality Report Tool Service Parameters

Parameter	Description
Display Extended QRT Menu Choices	Determines whether extended menu choices are presented to the user. You can choose one of the following configuration options: • Set this field to true to display extended menu choices (interview mode). • Set this field to false to not display extended menu choices (silent mode). • The recommended default value is false (silent mode).
Streaming Statistics Polling Duration	Determines the duration that is to be used for polling streaming statistics. You can choose one of the following configuration options: • Set this field to -1 to poll until the call ends. • Set this field to 0 to not poll at all. • Set it to any positive value to poll for that many seconds. Polling stops when the call ends. • The recommended default value is -1 (poll until the call ends).
Streaming Statistics Polling Frequency (seconds)	Enter the number of seconds to wait between each poll. The value ranges between 30 and 3600. The recommended default value is 30.
Maximum No. of Files	Enter the maximum number of files before the file count restarts and overwrites the old files. Valid values are between 1 and 10000. The recommended default value is 250.

Parameter	Description
Maximum No. of Lines per File	Enter the maximum number of lines in each file before starting the next file: • The value ranges between 100 and 2000. • The recommended default value specifies 2000.
CAPF Profile Instance Id for Secure Connection to CTI Manager	Enter the Instance ID of the Application CAPF Profile for application user CCMQRTSysUser that the Cisco Extended Function service will use to open a secure connection to CTI Manager. You must configure this parameter if CTI Manager Connection Security Flag is enabled. **Note** Turn on security by enabling the CTI Manager Connection Security Flag service parameter. You must restart the Cisco Extended Functions service for the changes to take effect.
CTI Manager Connection Security Flag	Choose whether security for Cisco Extended Functions service CTI Manager connection is enabled or disabled. If enabled, Cisco Extended Functions will open a secure connection to CTI Manager using the Application CAPF Profile configured for the Instance ID for application user CCMQRTSysUser. The value choices are True and False. You must choose True to enable a secure connection to CTI.

PART VI

Manage Security

CHAPTER 23

Manage SAML Single Sign-On

SAML Single Sign-On Overview

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. It is an authentication protocol used by service providers (such as Cisco Unified Communications Manager) to authenticate a user. With SAML, security authentication information is exchanged between an identity provider (IdP) and a service provider. The feature provides secure mechanisms to use common credentials and relevant information across various applications.

SAML SSO establishes a circle of trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the service provider. The service provider trusts user information of the IdP to provide access to the various services or applications.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the assertion to the service provider. Because a CoT established, the service provider trusts the assertion and grants access to the client.

Opt-In Control for Certificate-Based SSO Authentication for Cisco Jabber on iOS

This release of Cisco Unified Communications Manager introduces the opt-in configuration option to control Cisco Jabber on iOS SSO login behavior with an Identity provider (IdP). Use this option to allow Cisco Jabber to perform certificate-based authentication with the IdP in a controlled mobile device management (MDM) deployment.

You can configure the opt-in control through the **SSO Login Behavior for iOS** enterprise parameter in Cisco Unified Communications Manager.

Note Before you change the default value of this parameter, see the Cisco Jabber feature support and documentation at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html to ensure Cisco Jabber on iOS support for SSO login behavior and certificate-based authentication.

To enable this feature, see the Configure SSO Login Behavior for Cisco Jabber on iOS, on page 317 procedure.

SAML Single Sign-On Prerequisites

- DNS configured for the Cisco Unified Communications Manager cluster
- An identity provider (IdP) server
- An LDAP server that is trusted by the IdP server and supported by your system

The following IdPs using SAML 2.0 are tested for the SAML SSO feature:

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

The third-party applications must meet the following configuration requirements:

- The mandatory attribute “uid” must be configured on the IdP. This attribute must match the attribute that is used for the LDAP-synchronized user ID in Cisco Unified Communications Manager.
- The clocks of all the entities participating in SAML SSO must be synchronized. For information about synchronizing clocks, see “NTP Settings” in the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Manage SAML Single Sign-On

Enable SAML Single Sign-On

Note You cannot enable SAML SSO until the verify sync agent test succeeds.

Before you begin

- Ensure that user data is synchronized to the Unified Communications Manager database. For more information, see the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

- Verify that the Cisco Unified CM IM and Presence Service Cisco Sync Agent service successfully completed data synchronization. Check the status of this test by choosing **Cisco Unified CM IM and Presence Administration** > **Diagnostics** > **System Troubleshooter**. The "Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information)" test indicates a test passed outcome if data synchronization successfully completed.
- Ensure that at least one LDAP synchronized user is added to the Standard CCM Super Users group to enable access to Cisco Unified CM Administration. For more information, see the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
- To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO**.

Step 3 After you see warning message to notify you that all server connections will be restarted, click **Continue**.

Step 4 Click **Browse** to locate and upload the IdP metadata file.

Step 5 Click **Import IdP Metadata**.

Step 6 Click **Next**.

Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.

Step 8 Upload the server metadata on the IdP server.

Step 9 Click **Next** to continue.

Step 10 Choose an LDAP synchronized user with administrator rights from the list of valid administrator IDs.

Step 11 Click **Run Test**.

Step 12 Enter a valid username and password.

Step 13 Close the browser window after you see the success message.

Step 14 Click **Finish** and allow 1 to 2 minutes for the web applications to restart.

Configure SSO Login Behavior for Cisco Jabber on iOS

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 To configure the opt-in control, in the SSO Configuration section, choose the **Use Native Browser** option for the **SSO Login Behavior for iOS** parameter:

Note

The **SSO Login Behavior for iOS** parameter includes the following options:

- **Use Embedded Browser**—If you enable this option, Cisco Jabber uses the embedded browser for SSO authentication. Use this option to allow iOS devices prior to version 9 to use SSO without cross-launching into the native Apple Safari browser. This option is enabled by default.
- **Use Native Browser**—If you enable this option, Cisco Jabber uses the Apple Safari framework on an iOS device to perform certificate-based authentication with an Identity Provider (IdP) in the MDM deployment.

  Note

  We don't recommend to configure this option, except in a controlled MDM deployment, because using a native browser is not as secure as the using the embedded browser.

Step 3 Click **Save**.

Enable SAML Single Sign-On on WebDialer After an Upgrade

Follow these tasks to reactivate SAML Single Sign-On on Cisco WebDialer after an upgrade. If Cisco WebDialer is activated before SAML Single Sign-On is enabled, SAML Single Sign-On is not enabled on Cisco WebDialer by default.

Procedure

	Command or Action	Purpose
Step 1	Deactivate the Cisco WebDialer Service, on page 318	Deactivate the Cisco WebDialer web service if it is already activated.
Step 2	Disable SAML Single Sign-On, on page 319	Disable SAML Single Sign-On if it is already enabled.
Step 3	Activate the Cisco WebDialer Service, on page 319	
Step 4	Enable SAML Single Sign-On, on page 316	

Deactivate the Cisco WebDialer Service

Deactivate the Cisco WebDialer web service if it is already activated.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Servers** drop-down list, choose the Cisco Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, uncheck the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

What to do next

Disable SAML Single Sign-On, on page 319

Disable SAML Single Sign-On

Disable SAML Single Sign-On if it is already enabled.

Before you begin

Deactivate the Cisco WebDialer Service, on page 318

Procedure

From the CLI, run the command **utils sso disable**.

What to do next

Activate the Cisco WebDialer Service, on page 319

Activate the Cisco WebDialer Service

Before you begin

Disable SAML Single Sign-On, on page 319

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Servers** drop-down list, choose the Unified Communications Manager server that is listed.

Step 3 From **CTI Services**, check the **Cisco WebDialer Web Service** check box.

Step 4 Click **Save**.

Step 5 From Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to confirm that the CTI Manager service is active and is in start mode.

For WebDialer to function properly, the CTI Manager service must be active and in start mode.

What to do next

Enable SAML Single Sign-On, on page 316

Access the Recovery URL

Use the recovery URL to bypass SAML Single Sign-On and log in to the Cisco Unified Communications Manager Administration and Cisco Unified CM IM and Presence Service interfaces for troubleshooting. For example, enable the recovery URL before you change the domain or hostname of a server. Logging in to the recovery URL facilitates an update of the server metadata.

Note The recovery URL does not work for end users (LDAP or local) trying to log in to the Self Care portal.

Before you begin

- Only application users with administrative privileges can access the recovery URL.
- If SAML SSO is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Procedure

In your browser, enter `https://hostname:8443/ssosp/local/login`.

Update Server Metadata After a Domain or Hostname Change

After a domain or hostname change, SAML Single Sign-On is not functional until you perform this procedure.

Note If you are unable to log in to the **SAML Single Sign-On** window even after performing this procedure, clear the browser cache and try logging in again.

Before you begin

If the recovery URL is disabled, it does not appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: **utils sso recovery-url enable**.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

```
https://<Unified CM-server-name>
```

where `<Unified CM-server-name>` is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run Test**.

Step 8 Enter a valid User ID and password.

Step 9 After you see the success message, close the browser window.

Update Server Metadata After Deleting a Server

After a server is deleted from the cluster in a clusterwide SSO integration, re-import of metadata is mandatory to avoid index mismatch with IdP.

Before you begin

Note If the recovery URL is disabled, it does not appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: **utils sso recovery-url enable**.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

```
https://<Unified CM-server-name>
```

where `<Unified CM-server-name>` is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco Unified CM Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run Test**.

Step 8 Enter a valid User ID and password.

Step 9 After you see the success message, close the browser window.

Manually Provision Server Metadata

To provision a single connection in your Identity Provider for multiple UC applications, you must manually provision the server metadata while configuring the Circle of Trust between the Identity Provider and the Service Provider. For more information about configuring the Circle of Trust, see the IdP product documentation.

The general URL syntax is as follows:

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

Procedure

To provision the server metadata manually, use the Assertion Customer Service (ACS) URL.

Example:

Sample ACS URL: `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com" index="0"/>`

CHAPTER 24

Manage Certificates

Certificates Overview

Your system uses self-signed- and third-party-signed certificates. Certificates are used between devices in your system to securely authenticate devices, encrypt data, and hash the data to ensure its integrity from source to destination. Certificates allow for secure transfer of bandwidth, communication, and operations.

The most important part of certificates is that you know and define how your data is encrypted and shared with entities such as the intended website, phone, or FTP server.

When your system trusts a certificate, this means that there is a preinstalled certificate on your system which states it is fully confident that it shares information with the correct destination. Otherwise, it terminates the communication between these points.

In order to trust a certificate, trust must already be established with a third-party certificate authority (CA).

Your devices must know that they can trust both the CA and intermediate certificates first, before they can trust the server certificate presented by the exchange of messages called the secure sockets layer (SSL) handshake.

Note EC-based certificates for Tomcat are supported. This new certificate is called tomcat-ECDSA. For further information, see the Enhanced TLS Encryption on IM and Presence Service section of the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

EC Ciphers on the Tomcat interface are disabled by default. You can enable them using the **HTTPS Ciphers** enterprise parameter on Cisco Unified Communications Manager or on IM and Presence Service. If you change this parameter the Cisco Tomcat service must be restarted on all nodes.

For further information on EC-based certificates see, ECDSA Support for Common Criteria for Certified Solutions in the Release Notes for Cisco Unified Communications Manager and IM and Presence Service.

Third-Party Signed Certificate or Certificate Chain

Upload the certificate authority root certificate of the certificate authority that signed an application certificate. If a subordinate certificate authority signs an application certificate, you must upload the certificate authority root certificate of the subordinate certificate authority. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates.

You can upload certificate authority root certificates and application certificates by using the same **Upload Certificate** dialog box. When you upload a certificate authority root certificate or certificate chain that contains only certificate authority certificates, choose the certificate name with the format certificate type-trust. When you upload an application certificate or certificate chain that contains an application certificate and certificate authority certificates, choose the certificate name that includes only the certificate type.

For example, choose **tomcat-trust** when you upload a Tomcat certificate authority certificate or certificate authority certificate chain; choose **tomcat** or **tomcat-ECDSA** when you upload a Tomcat application certificate or certificate chain that contains an application certificate and certificate authority certificates.

When you upload a CAPF certificate authority root certificate, it is copied to the CallManager-trust store, so you do not need to upload the certificate authority root certificate for CallManager separately.

Note Successful upload of third-party certificate authority signed certificate deletes a recently generated CSR that was used to obtain a signed certificate and overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Note The system automatically replicates tomcat-trust, CallManager-trust and Phone-SAST-trust certificates to each node in the cluster.

Note You can upload a directory trust certificate to tomcat-trust, which is required for the DirSync service to work in secure mode.

Third-Party Certificate Authority Certificates

To use an application certificate that a third-party certificate authority issues, you must obtain both the signed application certificate and the certificate authority root certificate from the certificate authority or PKCS#7 certificate chain (distinguished encoding rules [DER]), which contains both the application certificate and certificate authority certificates. Retrieve information about obtaining these certificates from your certificate authority. The process varies among certificate authorities. The signature algorithm must use RSA encryption.

Cisco Unified Communications Operating System generates CSRs in privacy enhanced mail (PEM) encoding format. The system accepts certificates in DER and PEM encoding formats and PKCS#7 Certificate chain in PEM format. For all certificate types except certificate authority proxy function (CAPF), you must obtain and upload a certificate authority root certificate and an application certificate on each node.

For CAPF, obtain and upload a certificate authority root certificate and an application certificate only on the first node. CAPF and Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the certificate authority. If your certificate authority does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, as follows:

- The CAPF CSR uses the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Key Usage:
Digital Signature, Certificate Sign
```

- The CSRs for Tomcat and Tomcat-ECDSA, use the following extensions:

Note Tomcat or Tomcat-ECDSA does not require the key agreement or IPsec end system key usage.

```
X509v3 Extended Key Usage:
 TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System

 X509v3 Key Usage:
 Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for IPsec use the following extensions:

```
 X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for Unified Communications Manager use the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

- The CSRs for the IM and Presence Service cup and cup-xmpp certificates use the following extensions:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement,
```

Note You can generate a CSR for your certificates and have them signed by a third party certificate authority with a SHA256 signature. You can then upload this signed certificate back to Unified Communications Manager, allowing Tomcat and other certificates to support SHA256.

Certificate Signing Request Key Usage Extensions

The following tables display key usage extensions for Certificate Signing Requests (CSRs) for both Unified Communications Manager and the IM and Presence Service CA certificates.

Table 78: Cisco Unified Communications Manager CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF (publisher only)	N	Y			Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	N	Y	Y		Y	Y	Y		

Table 79: IM and Presence Service CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

Note Ensure that ‘Data Encipherment’ bit is not changed or removed as part of the CA-signing certificate process.

Show Certificates

Use the filter option on the Certificate List page, to sort and view the list of certificates, based on their common name, expiry date, key type, and usage. The filter option thus allows you to sort, view, and manage your data effectively.

From Unified Communications Manager Release 14, you can choose the usage option to sort and view the list of identity or trust certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The Certificate List page appears.

Step 2 From the **Find Certificate List where** drop-down list, choose the required filter option, enter the search item in the **Find** field, and click the **Find** button.

For example, to view only identity certificates, choose **Usage** from the **Find Certificate List where** drop-down list, enter Identity in the **Find** field, and click the **Find** button.

Download Certificates

Use the download certificates task to have a copy of your certificate or upload the certificate when you submit a CSR request.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Specify search criteria and then click **Find**.

Step 3 Choose the required file name and Click **Download**.

Install Intermediate Certificates

To install an intermediate certificate, you must install a root certificate first and then upload the signed certificate. This step is required only if the certificate authority provides a signed certificate with multiple certificates in the certificate chain.

Procedure

Step 1 From Cisco Unified OS Administration, click **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate / Certificate Chain**.

Step 3 Choose the appropriate trust store from the **Certificate Purpose** drop-down list to install the root certificate.

Step 4 Enter the description for the certificate purpose selected.

Step 5 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse** and navigate to the file; then click **Open**.

Step 6 Click **Upload**.

Step 7 Access the Cisco Unified Intelligence Center URL using the FQDN after you install the customer certificate. If you access the Cisco Unified Intelligence Center using an IP address, you will see the message “Click here to continue”, even after you successfully install the custom certificate.

Note
- TFTP service should be restarted when a Tomcat certificate is uploaded. Else, the TFTP continues to offer the old cached self-signed tomcat certificate.
- Uploading certificates from phone edge trust should be done from publisher.

Delete a Trust Certificate

A trusted certificate is the only type of certificate that you can delete. You cannot delete a self-signed certificate that is generated by your system.

Caution Deleting a certificate can affect your system operations. It can also break a certificate chain if the certificate is part of an existing chain. Verify this relationship from the username and subject name of the relevant certificates in the **Certificate List** window. You cannot undo this action.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note

- If you delete the "CAPF-trust", "tomcat-trust", "CallManager-trust", or "Phone-SAST-trust" certificate type, the certificate is deleted across all servers in the cluster.
- Deletion of certificates from phone edge trust should be done from publisher.
- If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across the cluster.

Regenerate a Certificate

We recommend you to regenerate certificates before they expire. You will receive warnings in RTMT (Syslog Viewer) and an email notification when the certificates are about to expire.

However, you can also regenerate an expired certificate. Perform this task after business hours, because you must restart phones and reboot services. You can regenerate only a certificate that is listed as type "cert" in Cisco Unified OS Administration

⚠ **Caution** Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Enter search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the **Certificate List** window.

Click **Regenerate** button in certificate details page, a self-signed certificate with the same key length is regenerated.

Note When regenerating a certificate, the **Certificate Description** field is not updated until you close the **Regeneration** window and open the newly generated certificate.

Click **Generate Self-Signed Certificate** to regenerate a self-signed certificate with a new key length of 3072 or 4096.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate. See Certificate Names and Descriptions, on page 330 for more information.

Step 5 Update the CTL file (if configured) after you regenerate the CAPF, ITLRecovery Certificates or CallManager Certificates.

Note After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register.

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 80: Certificate Names and Descriptions

Name	Description	Services to be Restarted
tomcat tomcat-ECDSA	This certificate is used by WebServices, Cisco DRF Services, and Cisco CallManager Services when SIP Oauth mode is enabled.	Cisco Tomcat Services, Cisco CallManager Service.
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	Cisco Call Manager Service and other relevant services including Cisco CTI Manager - update CTL file if the server is in secure mode. CallManager-ECDSA - Cisco CallManager Service.
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode)	N/A
TVS	This is used by Trust verification service, which acts as a secondary trust verification mechanism for the phones in case the server certificate changes.	N/A

Important This note is applicable for Release 14SU2 only.

For Release 14SU2, Cisco DRF services needs restart post tomcat-ECDSA certificate regeneration or upload. Restart is not needed post tomcat RSA certificate operations.

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the **AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.
b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.
b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Note Restart the Cisco CallManager Service on all nodes in the cluster after the keys are reassigned.

Upload Certificate or Certificate Chain

Upload any new certificates or certificate chains that you want your system to trust.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse**, navigate to the file, and then click **Open**.

Step 5 To upload the file to the server, click **Upload File**.

Note Restart the affected service after uploading the certificate. When the server comes back up you can access the CCMAdmin or CCMUser GUI to verify your newly added certificates in use.

Manage Third-Party Certificate Authority Certificates

This task flow provides an overview of the third-party certificate process, with references to each step in the sequence. Your system supports certificates that a third-party certificate authority issues with a PKCS # 10 certificate signing request (CSR).

Procedure

	Command or Action	Purpose
Step 1	Generate a Certificate Signing Request, on page 333	Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.
Step 2	Download a Certificate Signing Request, on page 333	Download the CSR after you generate it and have it ready to submit to your certificate authority.
Step 3	See your certificate authority documentation.	Obtain application certificates from your certificate authority.
Step 4	See your certificate authority documentation.	Obtain a root certificate from your certificate authority.
Step 5	Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store , on page 334	Add the root certificate to the trust store. Perform this step when using a certificate authority-signed CAPF certificate.
Step 6	Upload Certificate or Certificate Chain, on page 331	Upload the certificate authority root certificate to the node.
Step 7	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file.	See the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

	Command or Action	Purpose
		Rerun the CTL client (if configured) after you upload the third-party signed CAPF or CallManager certificate.
Step 8	Restart a Service, on page 334	Restart the services that are affected by the new certificate. For all certificate types, restart the corresponding service (for example, restart the Cisco Tomcat service if you updated the Tomcat or Tomcat-ECDSA certificate).

Generate a Certificate Signing Request

Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.

Note If you generate a new CSR, you overwrite any existing CSRs.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Generate CSR**.

Step 3 Configure fields on the **Generate Certificate Signing Request** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Generate**.

Download a Certificate Signing Request

Download the CSR after you generate it and have it ready to submit to your certificate authority.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Download CSR**.

Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Click **Download CSR**.

Step 5 (Optional) If prompted, click **Save**.

Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store

Add the root certificate to the Unified Communications Manager trust store when using a Certificate Authority-Signed CAPF Certificate.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 In the **Upload Certificate/Certificate Chain** popup window, choose **CallManager-trust** from the **Certificate Purpose** drop-down list and browse to the certificate authority-signed CAPF root certificate.

Step 4 Click **Upload** after the certificate appears in the **Upload File** field.

Restart a Service

Use this procedure if your system requires that you restart any feature or network services on a particular node in your cluster.

Procedure

Step 1 Depending on the service type that you want to restart, perform one of the following tasks:

- Choose **Tools** > **Control Center - Feature Services**.
- Choose **Tools** > **Control Center - Network Services**.

Step 2 Choose your system node from the **Server** drop-down list, and then click **Go**.

Step 3 Click the radio button next to the service that you want to restart, and then click **Restart**.

Step 4 After you see the message that indicates that the restart will take some time, click **OK**.

Certificate Revocation through Online Certificate Status Protocol

Unified Communications Manager provisions the OCSP for monitoring certificate revocation. System checks for the certificate status to confirm validity at scheduled intervals and every time there is, a certificate uploaded.

The Online Certificate Status Protocol (OCSP) helps administrators manage their system's certificate requirements. When OCSP is configured, it provides a simple, secure, and automated method to check certificate validity and revoke expired certificates in real-time.

For FIPS deployments with Common Criteria mode enabled, OCSP also helps your system comply with Common Criteria requirements.

Validation Checks

Unified Communications Manager checks the certificate status and confirms validity.

The certificates are validated as follows:

- Unified Communications Manager uses the Delegated Trust Model (DTM) and checks the Root CA or Intermediate CA for the OCSP signing attribute. The Root CA or the Intermediate CA must sign the OCSP Certificate to check the status. If the delegated trust model fails, Unified Communications Manager falls back to the Trust Responder Model (TRP) and uses a designated OCSP response signing certificate from an OCSP server to validate certificates.

Note OCSP Responder must be running to check the revocation status of the certificates.

- Enable OCSP option in the **Certificate Revocation** window to provide the most secure means of checking certificate revocation in real-time. Choose from options to use the OCSP URI from a certificate or from the configured OCSP URI. For more information on manual OCSP configuration, see Configure Certificate Revocation via OCSP.

Note In case of leaf certificates, TLS clients like syslog, FileBeat, SIP, ILS, LBM, and so on send OCSP requests to the OCSP responder and receives the certificate revocation response in real-time from the OCSP responder.

One of the following status is returned for the certificate once the validations are performed and the Common Criteria mode is ON.

- **Good --**The **good** state indicates a positive response to the status inquiry. At a minimum, this positive response indicates that the certificate is not revoked, but does not necessarily mean that the certificate was ever issued or that the time at which the response was produced is within the certificate's validity interval. Response extensions may be used to convey additional information on assertions made by the responder regarding the status of the certificate such as positive statement about issuance, validity, etc.
- **Revoked** --The **revoked** state indicates that the certificate has been revoked (either permanantly or temporarily (on hold)).
- **Unknown --** The **unknown** state indicates that the OCSP responder doesn't know about the certificate being requested.

Note In Common Criteria mode, the connection fails in both **Revoked** as well as **Unknown** case whereas the connection would succeed in **Unknown** response case when Common Criteria is not enabled.

Certificate Monitoring Task Flow

Complete these tasks to configure the system to monitor certificate status and expiration automatically.

- Email you when certificates are approaching expiration.
- Revoke expired certificates.

Procedure

	Command or Action	Purpose
Step 1	Configure Certificate Monitor Notifications, on page 336	Configure automatic certificate monitoring. The system periodically checks certificate statuses and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 337	Configure the OCSP so that the system revokes expired certificates automatically.

Configure Certificate Monitor Notifications

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.

Note The **Cisco Certificate Expiry Monitor** network service must be running. This service is enabled by default, but you can confirm the service is running in Cisco Unified Serviceability by choosing **Tools** > **Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).

Step 2 Choose **Security** > **Certificate Monitor**.

Step 3 In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.

Step 4 In the **Notification Frequency** fields, enter the frequency of notifications.

Step 5 Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations..

Step 6 Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.

Step 7 In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.

Step 8 Click **Save**.

Note The certificate monitor service runs once every 24 hours by default. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

What to do next

Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, seeConfigure Certificate Revocation via OCSP, on page 337

Configure Certificate Revocation via OCSP

Enable the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically.

Before you begin

Make sure that your system has the certificates that are required for OCSP checks. You can use Root or Intermediate CA certificates that are configured with the OCSP response attribute or you can use a designated OCSP signing certificate that has been uploaded to the tomcat-trust.

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).

Step 2 Choose **Security** > **Certificate Revocation**.

Step 3 Check the **Enable OCSP** check box, and perform one of the following tasks:

- If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.
- If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.

Step 4 Check the **Enable Revocation Check** check box.

Step 5 Complete the **Check Every** field with the interval period for revocation checks.

Step 6 Click **Save**.

Step 7 Optional. If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long-lived connections:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.

c) Configure a value for the **Validity Check Frequency** parameter.

Note The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

d) Click **Save**.

Troubleshoot Certificate Errors

Before you begin

If you encounter an error when you attempt to access Unified Communications Manager services from an IM and Presence Service node or IM and Presence Service functionality from a Unified Communications Manager node, the source of the issue is the tomcat-trust certificate. The error message `Connection to the Server cannot be established (unable to connect to Remote Node)` appears on the following Serviceability interface windows:

- **Service Activation**
- **Control Center - Feature Services**
- **Control Center - Network Services**

Use this procedure to help you resolve the certificate error. Start with the first step and proceed, if necessary. Sometime, you may only have to complete the first step to resolve the error; in other cases, you have to complete all the steps.

Procedure

Step 1 From Cisco Unified OS Administration, verify that the required tomcat-trust certificates are present: **Security** > **Certificate Management**.

If the required certificates are not present, wait 30 minutes before checking again.

Step 2 Choose a certificate to view its information. Verify that the content matches with the corresponding certificate on the remote node.

Step 3 From the CLI, restart the Cisco Intercluster Sync Agent service: **utils service restart Cisco Intercluster Sync Agent**.

Step 4 After the Cisco Intercluster Sync Agent service restarts, restart the Cisco Tomcat service: **utils service restart Cisco Tomcat**.

Step 5 Wait 30 minutes. If the previous steps do not address the certificate error and a tomcat-trust certificate is present, delete the certificate. After you delete the certificate, you must manually exchange it by downloading the Tomcat and Tomcat-ECDSA certificate for each node and uploading it to its peers as a tomcat-trust certificate.

Step 6 After the certificate exchange is complete, restart Cisco Tomcat on each affected server: **utils service restart Cisco Tomcat**.

CHAPTER 25

Manage Bulk Certificates

Manage Bulk Certificates

Use bulk certificate management if you want to share a set of certificates between clusters. This step is required for system functions that require established trust between clusters, such as extension mobility cross cluster.

Procedure

	Command or Action	Purpose
Step 1	Export Certificates, on page 339	This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.
Step 2	Import Certificates, on page 340	Import the certificates back into the home and remote (visiting) clusters.

Export Certificates

This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management**.

Step 2 Configure the settings for a TFTP server that both the home and remote clusters can reach. See the online help for information about the fields and their configuration options.

Step 3 Click **Save**.

Step 4 Click **Export**.

Step 5 In the **Bulk Certificate Export** window, choose **All** for the **Certificate Type** field.

Step 6 Click **Export**.

Step 7 Click **Close**.

Note When the bulk certificate export is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

The above steps are performed when certificates are self-signed and there is no common trust in another cluster. If there is a common trust or the same signer then the export of ALL certificates is not needed.

Import Certificates

Import the certificates back into the home and remote (visiting) clusters.

Note Import of certificate using bulk certificate management causes phones to reset.

Before you begin

Before the Import button appears, you must complete the following activities:

- Export the certificates from at least two clusters to the SFTP server.
- Consolidate the exported certificates.

Procedure

Step 1 From From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management** > **Import** > **Bulk Certificate Import**.

Step 2 From the **Certificate Type** drop-down list, choose **All**.

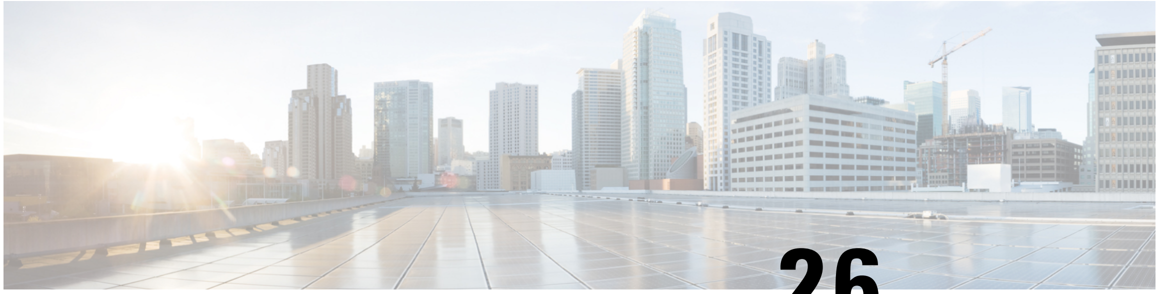
Step 3 Choose **Import**.

Note When the bulk certificate import is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

Note The following types of certificates determines phones that are restarted:

- Callmanager - ALL phones only IF TFTP service is activated on the node the certificate belongs.
- TVS - SOME phones based on Callmanager group membership.
- CAPF - ALL phones only IF CAPF is activated.



CHAPTER 26

Manage IPSec Policies

IPsec Policies Overview

IPsec is a framework that ensures private, secure communications over IP networks through the use of cryptographic security services. IPsec policies are used to configure IPsec security services. The policies provide varying levels of protection for most traffic types in your network. You can configure IPsec policies to meet the security requirements of a computer, organizational unit (OU), domain, site, or global enterprise.

Configure IPsec Policies

Note

- Because any changes that you make to an IPsec policy during a system upgrade will be lost, don't modify or create IPsec policies during an upgrade.
- IPsec requires bidirectional provisioning, or one peer for each host (or gateway).
- When you provision the IPsec policy on two Unified Communications Manager nodes with one IPsec policy protocol set to “ANY” and the other IPsec policy protocol set to “UDP” or “TCP”, the validation can result in a false negative if run from the node that uses the “ANY” protocol.
- IPsec, especially with encryption, affects the performance of your system.
- After the Unified CM node reboot, if the IPsec connection isn't up, ensure that you restart the IPsec service using the command **utils ipsec restart** to establish the IPsec connection successfully. This workaround is to mitigate any issues with IPsec service restart before the network connectivity is established.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSec Configuration**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **IPSEC Policy Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 (Optional) To validate IPsec, choose **Services** > **Ping**, check the **Validate IPsec** check box, and then click **Ping**.

Manage IPsec Policies

Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution Any changes that you make to the existing IPsec certificate because of hostname, domain, or IP address changes require you to delete the IPsec policies and recreate them, if certificate names are changed. If certificate names are unchanged, then after importing the remote node's regenerated certificate, the IPsec policies must be disabled and enabled.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **IPSEC Configuration**.

Step 2 To display, enable, or disable a policy, follow these steps:

a) Click the policy name.
b) To enable or disable the policy, check or uncheck the **Enable Policy** check box.
c) Click **Save**.
d) If you disable the policy, you must run the **utils ipsec restart** command for the disable changes to take effect.

Step 3 To delete one or more policies, follow these steps:

a) Check the check box next to each policy that you want to delete.

   You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.

b) Click **Delete Selected**.

CHAPTER 27

Manage Credential Policies

Credential Policy and Authentication

The authentication function authenticates users, updates credential information, tracks and logs user events and errors, records credential change histories, and encrypts or decrypts user credentials for data storage.

The system always authenticates application user passwords and end user PINs against the Unified Communications Manager database. The system can authenticate end user passwords against the corporate directory or the database.

If your system is synchronized with the corporate directory, either the authentication function in Unified Communications Manager or lightweight directory access protocol (LDAP) can authenticate the password:

- With LDAP authentication enabled, user passwords and credential policies do not apply. These defaults are applied to users that are created with directory synchronization (DirSync service).
- When LDAP authentication is disabled, the system authenticates user credentials against the database. With this option, you can assign credential policies, manage authentication events, and administer passwords. End users can change passwords and PINs through the phone user interfaces.

Credential policies do not apply to operating system users or CLI users. These administrators use standard password verification procedures that the operating system supports.

After users are configured in the database, the system stores a history of user credentials in the database to prevent users from entering previous information when users are prompted to change their credentials.

JTAPI and TAPI Support for Credential Policies

Because the Cisco Unified Communications Manager Java telephony applications programming interface (JTAPI) and telephony applications programming interface (TAPI) support the credential policies that are assigned to application users, developers must create applications that respond to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Applications use an API to authenticate with the database or corporate directory, regardless of the authentication model that an application uses.

For more information about JTAPI and TAPI for developers, see the developer guides at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Configure a Credential Policy

Credential policies apply to application users and end users. You assign a password policy to end users and application users and a PIN policy to end users. The Credential Policy Default Configuration lists the policy assignments for these groups. When you add a new user to the database, the system assigns the default policy. You can change the assigned policy and manage user authentication events.

Note Ensure that the Inactive Days Allowed parameter under the Credential Policy Settings is set to 0 (unlimited) for CTI application users. Else, the application users unexpectedly become inactive and the CTI applications may fail to connect to Unified CM after restart.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing credential policy.
- Click **Add New** to create a new credential policy.

Step 3 Complete the fields in the **Credential Policy Configuration** window. See the online help for more information about the fields and their configuration settings.

Step 4 Click **Save**.

Configure a Credential Policy Default

At installation, Cisco Unified Communications Manager assigns a static default credential policy to user groups. It does not provide default credentials. Your system provides options to assign new default policies and to configure new default credentials and credential requirements for users.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.

Step 2 From the **Credential Policy** drop-down list box, choose the credential policy for this group.

Step 3 Enter the password in both the **Change Credential** and **Confirm Credential** configuration windows.

Step 4 Check the **User Cannot Change** check box if you do not want your users to be able to change this credential.

Step 5 Check the **User Must Change at Next Login** check box if you want to use this credential as a temporary credential that an end user must change the next time that they login.

Note Please note that, if you check this box, your users are unable to change PIN using Personal Directory service.

Step 6 If you do not want the credential to expire, check the **Does Not Expire** check box.

Step 7 Click **Save**.

Monitor Authentication Activity

The system shows the most current authentication results, such as last hack attempt time, and counts for failed logon attempts.

The system generates log file entries for the following credential policy events:

- Authentication success
- Authentication failure (bad password or unknown)
- Authentication failure because of
  - Administrative lock
  - Hack lock (failed logon lockouts)
  - Expired soft lock (expired credential)
  - Inactive lock (credential not used for some time)
  - User must change (credential set to user must change)
  - LDAP inactive (switching to LDAP authentication and LDAP not active)
- Successful user credential updates
- Failed user credential updates

Note If you use LDAP authentication for end user passwords, LDAP tracks only authentication successes and failures.

All event messages contain the string “ims-auth” and the user ID that is attempting authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End Users**.

Step 2 Enter search criteria, click **Find**, and then choose a user from the resulting list.

Step 3 Click **Edit Credential** to view the user's authentication activity.

What to do next

You can view log files with the Cisco Unified Real-Time Monitoring Tool (Unified RTMT). You can also collect captured events into reports. For detailed steps about how to use Unified RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Credential Caching

Enable credential caching to increase system efficiency. Your system does not have to perform a database lookup or invoke a stored procedure for every single login request. An associated credential policy is not enforced until the caching duration expires.

This setting applies to all Java applications that invoke user authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Perform the following tasks as needed:

- Set the **Enable Caching** enterprise parameter to **True**. With this parameter enabled, Cisco Unified Communications Manager uses cached credentials for up to 2 minutes.
- Set the **Enable Caching** enterprise parameter to **False** to disable caching, so that the system does not use cached credentials for authentication. The system ignores this setting for LDAP authentication. Credential caching requires a minimal amount of additional memory per user.

Step 3 Click **Save**.

Manage Session Termination

Administrators can use this procedure to terminate a user's active sign-in session specific to each node.

Note

- An administrator with privilege level 4 only can terminate the sessions.
- Session Management terminates the active sign-in sessions on a particular node. If the administrator wants to terminate all the user sessions across different nodes, then the administrator has to sign-in to each node and terminate the sessions.

This applies to the following interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications Self Care Portal
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

Procedure

Step 1 From Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration, choose **Security** > **Session Management**.
The Session Management window is displayed.

Step 2 Enter the user ID of the active signed-in user in the **User ID** field.

Step 3 Click **Terminate Session**.

Step 4 Click **OK**.

If the terminated user refreshes the signed-in interface page, then the user is signed out. An entry is made in the audit log and it displays the terminated `userID`.

PART VII

IP Address, Hostname and Domain Name Changes

CHAPTER 28

Pre-Change Tasks and System Health Checks

Pre-Change Tasks

IP Address, Hostname, and Other Network Identifier Changes

You can change the network-level IP address and hostname name of nodes in your deployment for a variety of reasons, including moving the node from one cluster to another or resolving a duplicate IP address problem. The IP address is the network-level Internet Protocol (IP) associated with the node, and the Hostname is the network-level hostname of the node.

Note All Unified Communications products such as Cisco Unified Communications Manager, Cisco Unity Connections, and Cisco IM and Presence, and so on, have only one interface. Thus, you can assign only one IP address for each of these products.

For changes to other network identifiers, such as the node name and domain name, see the following resources:

- System Configuration Guide for Cisco Unified Communications Manager
- *Configuration and Administration Guide for the IM and Presence Service*
- *Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service*

For IM and Presence Service, instructions to change the node name and the network-level DNS default domain name for the node are also included in this document.

IM and Presence Service Node Name and Default Domain Name Changes

The node name is configured using Cisco Unified CM Administration GUI and must be resolvable from all other IM and Presence Service nodes and from all client machines. Therefore, the recommended node name value is the network FQDN of the node. However, both IP address and hostname are also supported as values for the node name in certain deployments. See the Hostname Configuration, on page 263 for more information about node name recommendations and the supported deployment types.

The network-level DNS default domain name of the node is combined with the hostname to form the Fully Qualified Domain Name (FQDN) for the node. For example, a node with hostname “imp-server” and domain “example.com” has an FQDN of “imp-server.example.com”.

Do not confuse the network-level DNS default domain of the node with the enterprise-wide domain of the IM and Presence Service application.

- The network-level DNS default domain is used only as a network identifier for the node.
- The enterprise-wide IM and Presence Service domain is the application-level domain that is used in the end-user IM address.

You can configure the enterprise-wide domain using either Cisco Unified CM IM and Presence Administration GUI or Cisco Unified Communications Manager Administration. See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for more information about enterprise-wide domains and the supported deployment types.

Hostname Configuration

The following table lists the locations where you can configure a host name for the Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.

Table 81: Host Name Configuration in Cisco Unified Communications Manager

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
Host Name/ IP Address field **System** > **Server** in Cisco Unified Communications Manager Administration	You can add or change the host name for a server in the cluster.	2-63	alphabetic	alphanumeric
Hostname field Cisco Unified Communications Manager installation wizard	You can add the host name for a server in the cluster.	1-63	alphabetic	alphanumeric
Hostname field **Settings** > **IP** > **Ethernet** in Cisco Unified Communications Operating System	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Host Name Location	Allowed Configuration	Allowed Number of Characters	Recommended First Character for Host Name	Recommended Last Character for Host Name
set network hostname hostname Command Line Interface	You can change, not add, the host name for a server in the cluster.	1-63	alphabetic	alphanumeric

Tip The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.

  After you install the Unified Communications Manager publisher node, the host name for the publisher automatically displays in this field. Before you install a Unified Communications Manager subscriber node, enter either the IP address or the host name for the subscriber node in this field on the Unified Communications Manager publisher node.

  In this field, configure a host name only if Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

Tip In addition to configuring Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the installation of the Unified Communications Manager publisher node, you enter the host name, which is mandatory, and IP address of the publisher node to configure network information; that is, if you want to use static networking.

  During the installation of a Unified Communications Manager subscriber node, you enter the hostname and IP address of the Unified Communications Manager publisher node, so that Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber node. When the Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

Procedure workflows

Cisco Unified Communications Manager Workflow

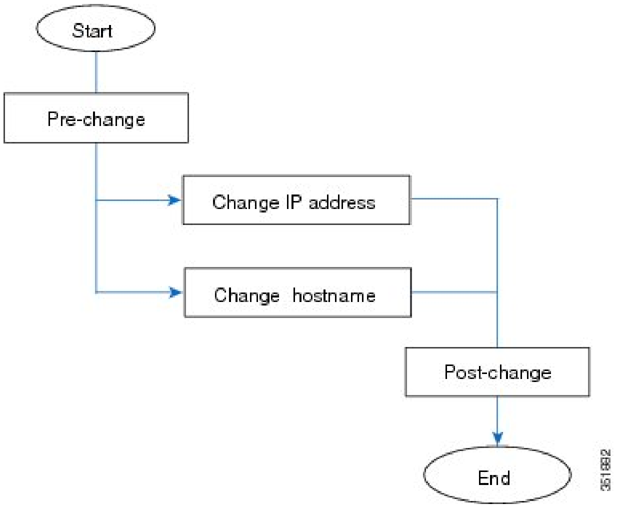
This document provides detailed procedures for the following tasks for Cisco Unified Communications Manager nodes:

- Change the IP address of a node
- Change the hostname of a node

Task lists are provided for each of these procedures that summarize the steps to perform.

Note You must complete all pre-change tasks and system health checks before you make these changes, and you must complete the post-change tasks after you make any of these changes.

Figure 24: Cisco Unified Communications Manager Workflow



IM and Presence Service Workflow

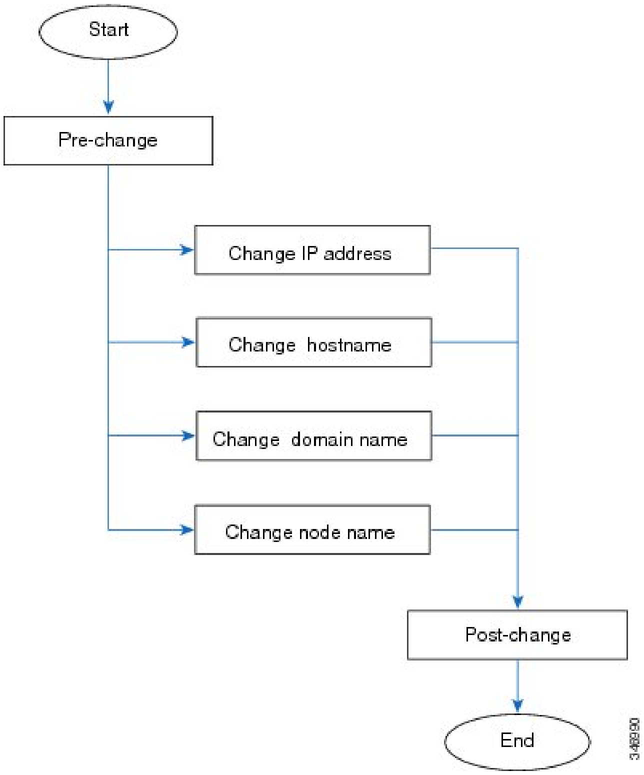
This document provides detailed procedures for the following tasks for IM and Presence Service nodes:

- Change the IP address of a node
- Change the hostname of a node
- Change the DNS default domain name
- Change the node name of a node

Task lists are provided for each of these procedures that summarize the steps to perform.

Note You must complete all pre-change tasks and system health checks before you make these changes, and you must complete the post-change tasks after you make any of these changes.

Figure 25: IM and Presence Service Workflow



Pre-Change Tasks for Cisco Unified Communications Manager Nodes

The following procedure explains the tasks to change the IP address and hostname for Cisco Unified Communications Manager nodes. You must perform these procedures during a scheduled maintenance window.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Procedure

Step 1 If you have DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that forward and reverse records (for example, A record and PTR record) are configured and that the DNS is reachable and working.

Step 2 Check for any active ServerDown alerts to ensure that all servers in the cluster are up and available. Use either the Cisco Unified Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) on the first node.

a) To check using Unified RTMT, access Alert Central and check for ServerDown alerts.

b) To check using the CLI on the first node, enter the following CLI command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 3 Check the database replication status of all Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. For IM and Presence Service, check the database replication status on the database publisher node using the CLI if you have more than one node in your deployment. Use either Unified RTMT or the CLI. All nodes should show a status of 2.

a. To check by using RTMT, access the Database Summary and inspect the replication status.

b. To check by using the CLI, enter **utils dbreplication runtimestate**.

Step 4 Enter the CLI command utils diagnose as shown in the following example to check network connectivity and DNS server configuration.

Example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network : Passed
Diagnostics Completed
admin:
```

Step 5 In Cisco Unified Reporting, generate the Unified CM Database Status report. Look for any errors or warnings in this report.

Step 6 In Cisco Unified Reporting, generate the Unified CM Cluster Overview report. Look for any errors or warnings in this report.

Step 7 From Cisco Unified Communications Manager Administration on the first node, select **System** > **Server** and click **Find**. A list of all servers in the cluster displays. Retain this list of servers for future reference. Ensure that you save an inventory of both the hostname and IP address of each node in your cluster.

Step 8 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Administration Guide for Cisco Unified Communications Manager*

Step 9 If you are changing the hostname, disable SAML single sign-on (SSO). For more information about SAML SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 10 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide*.

Note To avoid unnecessary delays, you must update the CTL file with the new IP address of your TFTP servers before you change the IP address of the TFTP servers. If you do not perform this step, you will have to update all secure IP phones manually.

Note All IP phones that support security always download the CTL file, which includes the IP address of the TFTP servers with which the phones are allowed to communicate. If you change the IP address of one or more TFTP servers, you must first add the new IP addresses to the CTL file so that the phones can communicate with their TFTP server.

Pre-Change Setup Tasks for IM and Presence Service Nodes

Perform the applicable pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Note You do not need to perform the steps to verify that the Cisco AXL Web service and the IM and Presence Cisco Sync Agent services are started unless you are changing the domain name or the node name. See the pre-change task list for a complete list of the tasks to perform.

Procedure

Step 1 Check the database replication status on all nodes in the cluster to ensure that all servers are replicating database changes successfully.

For IM and Presence Service, check the database replication status on the database publisher node using the CLI if you have more than one node in your deployment.

Use either Unified RTMT or the CLI. All nodes should show a status of **2**.

a) To check by using RTMT, access the Database Summary and inspect the replication status.
b) To check by using the CLI, enter `utils dbreplication runtimestate`.

For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 2 Enter the CLI command `utils diagnose` as shown in the following example to check network connectivity and DNS server configuration.

Example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
admin:
```

Step 3 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 4 Disable High Availability (HA) on all presence redundancy groups. For information on Presence Redundancy Groups configuration, see the "Configure Presence Redundancy Groups" chapter in the *System Configuration Guide for Cisco Unified Communications Manager*.

Note

- Before you disable HA, take a record of the number of users in each node and subcluster. You can find this information in the **System** > **Presence Topology** window of Cisco Unified CM IM and Presence Administration.
- After you disable HA, wait at least 2 minutes for the settings to sync across the cluster before completing any further changes.

Step 5 If you are changing the hostname, disable SAML single sign-on (SSO). For more information about SAML SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 6 If you have intercluster peers configured in your deployment, perform the following tasks:

a) For each cluster where the IM and Presence database publisher node that you are changing is an intercluster peer, remove the publisher’s cluster from the list of intercluster peers.

Example:

ClusterA, ClusterB and ClusterC are all intercluster peers. You want to change the hostname on the publisher node of ClusterA. You must first remove the ClusterA publisher node from the list of intercluster peers on both ClusterB and ClusterC.

b) Restart the Cisco Intercluster Sync Agent on the publisher and subscriber nodes of the first presence redundancy group in each cluster.

Step 7 Compile a list of all services that are currently activated. Retain these lists for future reference.

a) To view the list of activated network services using Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services**.
b) To view the list of activated feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**.

Step 8 Stop all feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**. The order in which you stop feature services is not important.

Tip You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically stopped for these name changes.

Step 9 Stop the following network services that are listed under the IM and Presence Service services group using Cisco Unified Serviceability when you select **Tools** > **Control Center - Network Services**.

You must stop these IM and Presence Service network services in the following order:

a. Cisco Config Agent
b. Cisco Intercluster Sync Agent
c. Cisco Client Profile Agent
d. Cisco OAM Agent
e. Cisco XCP Config Manager
f. Cisco XCP Router
g. Cisco Presence Datastore
h. Cisco SIP Registration Datastore
i. Cisco Login Datastore
j. Cisco Route Datastore
k. Cisco Server Recovery Manager
l. Cisco IM and Presence Data Monitor

Step 10 Verify that the Cisco AXL Web Service is started on the Cisco Unified Communications Manager publisher node using Cisco Unified Serviceability, **Tools** > **Control Center - Feature Services**.

Note Perform this step only if you are changing the domain name or node name.

Step 11 Verify that the IM and Presence Cisco Sync Agent service has started and that synchronization is complete.

Note Perform this step only if you are changing the domain name or node name.

a) To verify using Cisco Unified Serviceability, perform the following steps:

1. Select **Tools** > **Control Center - Network Services**.
2. Select the IM and Presence database publisher node.
3. Select **IM and Presence Service Services**.
4. Verify that the Cisco Sync Agent service has started.
5. From the Cisco Unified CM IM and Presence Administration GUI, select **Diagnostics** > **System Dashboard** > **Sync Status**.
6. Verify that synchronization is complete and that no errors display in the synchronization status area.

b) To verify using the Cisco Unified CM IM and Presence Administration GUI on the IM and Presence database publisher node, select **Diagnostics** > **System Dashboard**.

CHAPTER 29

IP Address and Hostname Changes

Change IP Address and Hostname Task List

The following table lists the tasks to perform to change the IP address and hostname for Cisco Unified Communications Manager and IM and Presence Service nodes.

Table 82: Change IP Address and Hostname Task List

Item	Task
1	Perform the pre-change tasks and system health checks.
2	Change the IP address or hostname for the node using either the Command Line Interface (CLI) or the Unified Operating System GUI. For IM and Presence Service nodes, observe the following conditions: • Change the IP address and hostname for the database publisher node before you change any subscriber nodes. • You can change the IP address and hostname for all subscriber nodes simultaneously or one at a time. **Note** After you change the IP address or hostname of an IM and Presence Service node, you must change the Destination Address value for the SIP publish trunk on Cisco Unified Communications Manager. See the post-change task list.
3	Perform the post-change tasks.

Change IP Address or Hostname Through OS Admin GUI

You can use Cisco Unified Operating System Administration to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Unified Communications Manager and IM and Presence Service clusters.

Changing the hostname through **set network hostname** command triggers an automatically self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you need to have them re-signed.

Changing only the IP address using the **set network hostname** command causes all devices in the cluster to reset so that they can download an updated ITL file. Certificates are not updated.

Note Changing the hostname does not trigger the ITL recovery certificates regeneration.

Caution

- Through Cisco Unified Operating System Administration, we recommend that you change only one of these settings at a time. To change both the IP address and hostname at the same time, use the CLI command **set network hostname**.
- If the Unified Communications Manager cluster security is operating in mixed mode, secure connections to this node will fail after changing the hostname, or IP address until you run the CTL client and update the CTL file or run **utils ctl update CTLFile** if you used the tokenless CTL feature.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Note In case you must change the vNIC from vcenter, use the CLI command **set network hostname**.

Procedure

Step 1 From Cisco Unified Operating System Administration, select **Settings** > **IP** > **Ethernet**

Step 2 Change the hostname, IP address, and if necessary, the default gateway.

Step 3 Click **Save**.

Node services automatically restart with the new changes. Restarting services ensures the proper update and service-restart sequence for the changes to take effect.

Changing the hostname triggers an automatically self-signed certificate regeneration and causes all devices in the cluster to reset so they can download an updated ITL file. Changing the hostname does not trigger the ITL recovery certificates regeneration.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address.

If your cluster is using CA-signed certificates, you need to have them re-signed.

Run the CTL Client to update the CTL file if you used that process to put your cluster into mixed mode. If you used the tokenless CTL feature, then run the CLI command **utils ctl update CTLFile**

Change IP Address or Hostname Through Unified CM Administration GUI

You can use Cisco Unified CM Administration to change the IP address or hostname, which is defined in the database, for the publisher and subscriber nodes. Doing this ensures that the hostname entries are uniform with the system-defined hostname or IP values.

Changing the IP address or hostname triggers an automatically self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you must have them re-signed.

Caution

- A change of the hostname or IP address requires the system services to be restarted. Hence, refrain from making this change during normal operating hours.
- Through Cisco Unified CM Administration, we recommend that you change only one of these settings at a time. To change both the IP address and hostname at the same time, use the CLI command **set network hostname**.
- If the Unified Communications Manager cluster security is operating in mixed mode, secure connections to this node will fail after changing the hostname, or IP address until you run the CTL client and update the CTL file or run **utils ctl update CTLFile** if you used the tokenless CTL feature.
- If the hostname or IP address that is defined on the Cisco Unified OS Administration and Cisco Unified CM Administration pages do not match, the applications are unable to fetch the correct phone status. Also, due to certificate mismatch, TLS handshake fails. Hence, ensure that the IP address and hostname entries in both the Cisco Unified OS Administration and the Cisco Unified CM Administration pages are alike.

Before you begin

Perform the prechange tasks and system health checks on your deployment.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Server**.

The **Find and List Servers** window appears.

Step 2 To get a list of all servers, click **Find**.

Step 3 From the list, click the server for which you want to modify the hostname.

Step 4 In the **Host Name/IP Address*** field, enter the new host name or the IP address and click **Save**.

Step 5 Using the Admin CLI GUI, reboot the node using the **utils system restart** CLI command.

Change IP Address or Hostname Through CLI

You can use the CLI to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Cisco Unified Communication Manager and IM and Presence Service clusters.

Changing the hostname triggers an automatically self-signed certificate regeneration. This causes all devices in the cluster to reset so that they can download an updated ITL file. If your cluster is using CA-signed certificates, you must have them re-signed. Changing the hostname does not trigger the ITL recovery certificates regeneration.

⚠ **Caution** If the Cisco Unified Communications Manager cluster security is operating in mixed mode, secure connections to this node will fail after changing the hostname, or IP address until you run the CTL client and update the CTL file or run **utils ctl update CTLFile** if you used the tokenless CTL feature.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log in to the CLI of the node that you want to change.

Step 2 Enter `set network hostname`.

Step 3 Follow the prompts to change the hostname, IP address, or default gateway.

a) Enter the new hostname and press **Enter**.
b) Enter `yes` if you also want to change the IP address; otherwise, go to Step 4.
c) Enter the new IP address.
d) Enter the subnet mask.
e) Enter the address of the gateway.

Step 4 Verify that all your input is correct and enter `yes` to start the process.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address.

If your cluster is using CA-signed certificates, you must have them re-signed.

Run the CTL Client to update the CTL file if you used that process to put your cluster into mixed mode. If you used the tokenless CTL feature, then run the CLI command **utils ctl update CTLFile**

Example CLI Output for Set Network Hostname

Note In case you need to change the vNIC from vcenter, update the vNIC after the step `calling 4 of 5 component notification script: regenerate_all_certs.sh` as displayed in the following output.

```
 admin:set network hostname

ctrl-c: To quit the input.

         ***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=======================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=======================================================

Security Warning : This operation will regenerate
       all CUCM Certificates including any third party
       signed Certificates that have been uploaded.

Enter the hostname:: newHostname

Would you like to change the network ip address at this time [yes]::


Warning: Do not close this window until command finishes.



ctrl-c: To quit the input.
```

```
           ***   W A R N I N G   ***
=======================================================
 Note: Please verify that the new ip address is unique
       across the cluster.
=======================================================

Enter the ip address:: 10.10.10.28
Enter the ip subnet mask:: 255.255.255.0
Enter the ip address of the gateway:: 10.10.10.1
Hostname:       newHostname
IP Address:     10.10.10.28
IP Subnet Mask: 255.255.255.0
Gateway:        10.10.10.1

Do you want to continue [yes/no]? yes



calling 1 of 5 component notification script: ahostname_callback.sh
Info(0): Processnode query returned =
name
==========
bldr-vcm18
updating server table from:'oldHostname', to: 'newHostname'
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
Going to trigger /usr/local/cm/bin/dbl updatefiles --remote=newHostname,oldHostname

calling 2 of 5 component notification script: clm_notify_hostname.sh  notification
Verifying update across cluster nodes...
platformConfig.xml is up-to-date: bldr-vcm21

cluster update successfull
calling 3 of 5 component notification script: drf_notify_hostname_change.py
calling 4 of 5 component notification script: regenerate_all_certs.sh
calling 5 of 5 component notification script: update_idsenv.sh
calling 1 of 2 component notification script: ahostname_callback.sh
Info(0): Processnode query returned =
name
====
Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=10.10.10.28,10.67.142.24
calling 2 of 2 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Shutting down interface eth0:
```

Change IP Address Only

You can change the IP address of a node by using the CLI.

If the node is defined by hostname or FQDN, you must update only the DNS before you make the change (if DNS is used).

Note For IM and Presence Service:

- Change and verify the IM and Presence database publisher node first.
- You can change the IM and Presence Service subscriber nodes simultaneously or one at a time.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log into the CLI of the node that you want to change.

Step 2 Enter **`set network ip eth0`** ***`new-ip_address new_netmask new_gateway`*** to change the IP address of the node.

Note Changing IP addres only with **set network ip eth0** command does not trigger Certificate Regeneration.

where *`new_ip_address`* specifies the new server IP address, *`new_netmask`* specifies the new server network mask and *`new_gateway`* specifies the gateway address.

The following output displays:

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1

WARNING: Changing this setting will invalidate software license
on this server. The license will have to be re-hosted.

Continue (y/n)?
```

Step 3 Verify the output of the CLI command. Enter **`yes`**, and then press **Enter** to start the process.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Example Output for Set Network IP Address

Note In case you need to change the vNIC from vcenter, update the vNIC after the step `calling 3 of 6 component notification script: aetc_hosts_verify.sh` as displayed in the following output.

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1
```

```
           ***   W A R N I N G   ***

This command will restart system services
=======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=======================================================


Continue (y/n)?y
calling 1 of 6 component notification script: acluster_healthcheck.sh
calling 2 of 6 component notification script: adns_verify.sh
No Primary DNS server defined
No Secondary DNS server defined
calling 3 of 6 component notification script: aetc_hosts_verify.sh
calling 4 of 6 component notification script: afupdateip.sh
calling 5 of 6 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using 10.77.30.33:
name
====
calling 6 of 6 component notification script: clm_notify_hostname.sh
```

Change DNS IP Address Using CLI

You can use CLI to change the DNS IP Address for publisher and subscriber nodes in your deployment. This procedure applies to both publisher and subscriber nodes on Unified Communications Manager and IM and Presence Service clusters.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log in to the CLI of the node that you want to change.

Step 2 Enter `set network dns primary/secondary <new IP address of the DNS>`

Note If you change the IP address for the DNS servers, you must reboot the server through the **utils system restart** CLI command.

The following ouput displays:

```
admin:set network dns primary/secondary <new IP address of DNS>
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity
```

Step 3 Verify the output of the CLI command. Enter **`Yes`** and then press **Enter** to start the process.

CHAPTER 30

Domain Name and Node Name Changes

Domain Name Change

Administrators can modify the network-level DNS default domain that is associated with an IM and Presence Service node or group of nodes.

The enterprise-wide IM and Presence Service domain does not need to align with the DNS default domain of any IM and Presence Service node. To modify the enterprise-wide domain for your deployment, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager Configuration and Administration Guide for the IM and Presence Service*.

Caution Changing the default domain on any node in an IM and Presence Service cluster will result in node restarts and interruptions to presence services and other system functions. Because of this impact to the system, you must perform this domain change procedure during a scheduled maintenance window.

When you change the default domain name for a node, all third-party signed security certificates are automatically overwritten with new self-signed certificates. If you want to have those certificates re-signed by your third-party Certificate Authority, you must manually request and upload the new certificates. Service restarts may be required to pick up these new certificates. Depending on the time that is required to request new certificates, a separate maintenance window may be required to schedule the service restarts.

Note New certificates cannot be requested in advance of changing the default domain name for the node. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the node and the node has been rebooted.

IM and Presence Service Default Domain Name Change Tasks

The following table contains the step-by-step instructions for modifying the network-level DNS default domain name associated with an IM and Presence Service node or group of nodes. The detailed instructions for this procedure specify the exact order of steps for performing the change on multiple nodes within the cluster.

If you are performing this procedure across multiple clusters, you must complete the changes sequentially on one cluster at a time.

Note You must complete each task in this procedure in the exact order presented in this workflow.

Procedure

Step 1 Complete the pre-change tasks on all applicable nodes within the cluster. Some of the pre-change tasks may apply only to the IM and Presence database publisher node and can be skipped if you are modifying a subscriber node.

Step 2 Update the DNS records for the IM and Presence Service node on all applicable nodes within the cluster. Also update SRV, Forward (A), and Reverse (PTR) records as appropriate to incorporate the new node domain.

Step 3 Update the IM and Presence Service node name on all applicable nodes within the cluster using Cisco Unified Communications Manager Administration.

Note This step is mandatory for the FQDN node name format. It is not applicable if the node name is an IP address or a Hostname.

- If the node name is an FQDN, then it references the old node domain name. Therefore, you must update the node name such that the FQDN value reflects the new domain name.
- If the node name is an IP address or hostname, then the domain is not referenced and therefore no changes are required.

Step 4 Update the DNS domain on all applicable nodes using the Command Line Interface (CLI). The CLI command makes the required domain change on the node operating system and triggers an automatic reboot of each node.

Step 5 Restart the 'A Cisco DB' service of all the nodes in the cluster after the domain name update to ensure that operating system configuration files on all nodes pick up the DNS domain name change that is associated with the modified nodes.

Note Verify that the system is working properly. If you observe any replication issues, ensure that you restart all the nodes in the cluster.

Step 6 Verify database replication using the CLI. See topics related to performing system health checks and troubleshooting database replication for details. After all system files are synchronized within the cluster, you must verify database replication.

Step 7 Regenerate security certificates on the node.

- The Subject Common Name on all IM and Presence Service security certificates is set to the node FQDN. Therefore, to incorporate the new node domain, all certificates are automatically regenerated after a DNS domain change.

- Any certificates that were previously signed by a certificate.

Step 8 Complete the post-change tasks for all applicable nodes within the cluster to ensure that the cluster is fully operational.

Update DNS Records

Because you are changing the DNS domain for the node, you must also update any existing DNS records associated with that node. This includes the following types of records:

- A records
- PTR records
- SRV records

If multiple nodes within a cluster are being modified, you must complete the following procedure for each of these nodes.

If you are modifying the IM and Presence database publisher node, you must complete this procedure on the IM and Presence database publisher node first before repeating on any applicable IM and Presence Service subscriber nodes.

Note

- These DNS records must be updated during the same maintenance window as the DNS domain change itself on the node.
- Updating the DNS records before the scheduled maintenance window may adversely affect IM and Presence Service functionality.

Before you begin

Perform all pre-change tasks and the applicable system health checks on your deployment.

Procedure

Step 1 Remove the old DNS forward (A) record for the node from the old domain.

Step 2 Create a new DNS forward (A) record for the node within the new domain.

Step 3 Update the DNS reverse (PTR) record for the node to point to the updated Fully Qualified Domain Name (FQDN) of the node.

Step 4 Update any DNS SRV records that point to the node.

Step 5 Update any other DNS records that point to the node.

Step 6 Verify that all the above DNS changes have propagated to all other nodes within the cluster by running the following Command Line Interface (CLI) command on each node:

a) To validate the new A record, enter **`utils network host new-fqdn`**, where `new-fqdn` is the updated FQDN of the node.

Example:

```
admin: utils network host server1.new-domain.com
Local Resolution:
server1.new-domain.com resolves locally to 10.53.50.219

External Resolution:
server1.new-domain.com has address 10.53.50.219
```

b) To validate the updated PTR record, enter **`utils network host ip-addr`**, where `ip-addr` is the IP address of the node.

```
admin: utils network host 10.53.50.219
Local Resolution:
10.53.50.219 resolves locally to server1.new-domain.com

External Resolution:
server1.new-domain.com has address 10.53.50.219
219.50.53.10.in-addr.arpa domain name pointer server1.new-domain.com.
```

Note At this point in the procedure, the **Local Resolution** result for the IP address will continue to point to the old FQDN value until the DNS domain is changed on the node.

c) To validate any updated SRV records, enter **`utils network host srv-name srv`**, where `srv-name` is the SRV record.

Example:

_xmpp-server SRV record lookup example.

```
admin: utils network host _xmpp-server._tcp.galway-imp.com srv
Local Resolution:
Nothing found

External Resolution:
_xmpp-server._tcp.sample.com has SRV record 0 0 5269 server1.new-domain.com.
```

What to do next

Update the IM and Presence Service node name.

Update Node Name in FQDN Value

If the node name defined for the node in the Presence Topology window on the Cisco Unified CM IM and Presence Administration GUI is set to the Fully Qualified Domain Name (FQDN) of the node, then it references the old domain name. Therefore you must update the node name to reference the new domain name.

Note This procedure is only required if the node name value for this node is set to FQDN. If the node name matches the IP address or the hostname of the node, then this procedure is not required.

If multiple nodes within a cluster are being modified, you must complete the following procedure sequentially for each of these nodes.

If the IM and Presence database publisher node is being modified, you must complete this procedure for the IM and Presence Service subscriber nodes first, before completing the procedure on the publisher node.

Before you begin

Update the DNS records for the node.

Procedure

Step 1 Modify the node name for the IM and Presence Service node.

a) Sign in to Cisco Unified Communications Manager Administration.
b) Select **System** > **Server**.
c) Search for and select the node.
d) Update the **Fully Qualified Domain Name/IP Address** field so that the FQDN references the new domain value. For example, update the **Fully Qualified Domain Name/IP Address** value from `server1.old-domain.com` to `server1.new-domain.com`.
e) Select **Save**.

Step 2 Verify that the Application Server entry for this node has been updated to reflect the new node name on the **Presence Topology** window of the Cisco Unified CM IM and Presence Administration GUI.

a) Sign in to Cisco Unified Communications Manager Administration and select **System** > **Application Server**.
b) Click **Find**, if required, on the **Find and List Application Servers** window.
c) Ensure that an entry exists for the updated node name in the list of Application Servers.

Note Do not continue if there is no entry for this node or if there is an entry but it reflects the old node name for the node.

What to do next

Update the DNS domain on all applicable nodes.

Update DNS Domain

You can change the DNS domain of the IM and Presence Service node using the Command Line Interface (CLI).

The enterprise-wide IM and Presence Service domain does not need to align with the network-level DNS default domain of any IM and Presence Service node. To modify the enterprise-wide domain for your deployment, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

If you are modifying multiple nodes within a cluster, then you must complete the following procedure sequentially for each node.

If you are modifying the IM and Presence database publisher node, then you must first complete this procedure on the database publisher node before you modify any subscriber nodes.

Before you begin

Update the IM and Presence Service node name.

Procedure

Step 1 Sign in to the CLI on the node and enter **`set network domain new-domain`**, where `new-domain` is the new domain value to be set.

Example:

```
admin: set network domain new-domain.com

*** W A R N I N G ***
Adding/deleting or changing domain name on this server will break
database replication. Once you have completed domain modification
on all systems that you intend to modify, please reboot all the
servers in the cluster. This will ensure that replication keeps
working correctly. After the service is rebooted, please
confirm that there are no issues reported on the Cisco Unified
Reporting report for Database Replication.

The server will now be rebooted. Do you wish to continue.

Security Warning : This operation will regenerate
all CUP Certificates including any third party
signed Certificates that have been uploaded.

Continue (y/n)?
```

Step 2 Enter **`y`** and press **Return** to confirm the domain change and restart of the node or enter **`n`** to cancel.

Tip When the node name change is complete, all certificates are regenerated on the node. If any of those certificates were signed by a third-party Certificate Authority, then you must re-request those signed certificates later in the procedure.

Step 3 After the node restarts, enter `show network eth0` to confirm the domain name change has taken effect.

Example:

The new domain in the following example is new-domain.com.

```
admin: show network eth0
Ethernet 0
DHCP         : disabled       Status      : up
IP Address   : 10.53.50.219   IP Mask     : 255.255.255.000
Link Detected: yes            Mode        : Auto disabled, Full, 1000 Mbits/s
Duplicate IP : no

DNS
Primary  : 10.53.51.234       Secondary   : Not Configured
Options  : timeout:5 attempts:2
Domain   : new-domain.com
Gateway  : 10.53.50.1 on Ethernet 0
```

Step 4 Repeat the previous steps on all applicable nodes in the cluster.

What to do next

Reboot all nodes in the cluster.

Cluster Nodes Considerations

You can use the Command Line Interface (CLI) to restart the "A Cisco DB" service in the nodes in your cluster.

After you change the domain name and the node reboots, you need to restart the 'A Cisco DB' service of all the nodes in the cluster, including those nodes that have automatically rebooted, starting with the Unified CM publisher and then for all the subscribers as the published database comes up. This ensures that the Operating System configuration files on all nodes are aligned with the new domain values.

Verify that the system is working properly. If you observe any replication issues, ensure that you restart all the nodes in the cluster.

Initiate the reboot process on the IM and Presence database publisher node first. When the database publisher node has restarted, proceed to reboot the remaining IM and Presence Service subscriber nodes in any order.

Before you begin

Ensure that the DNS domain name of the node was changed.

Procedure

Step 1 Reboot the IM and Presence database publisher node using the CLI. Enter **`utils system restart`**.

Example:

```
admin: utils system restart
Do you really want to restart ?
Enter (yes/no)?
```

Step 2 Enter **`yes`** and press **Return** to restart.

Step 3 Wait until you see the following message that indicates the IM and Presence database publisher node has restarted.

Example:

```
Broadcast message from root (Wed Oct 24 16:14:55 2012):

The system is going down for reboot NOW!
Waiting .

Operation succeeded

restart now.
```

Step 4 Sign in to the CLI on each IM and Presence Service subscriber node and enter `utils system restart` to reboot each subscriber node.

Note After several minutes of trying to stop services, the CLI may ask you to force a restart. If this occurs, enter `yes`.

What to do next

Verify database replication. See topics related to system health checks for more information.

Regenerate Security Certificates

The Fully Qualified Domain Name (FQDN) of the node is used as Subject Common Name in all IM and Presence Service security certificates. Therefore, when the DNS domain is updated on a node, all security certificates are automatically regenerated.

If any certificates were signed by a third-party Certificate Authority, then you must manually generate new Certificate Authority signed certificates.

If you are modifying multiple nodes within a cluster, you must complete the following procedure for each node.

Note New certificates cannot be requested in advance of changing the default domain name for the node. Certificate Signing Requests (CSRs) can only be generated after the domain has been changed on the node and the node has been rebooted.

Before you begin

Verify database replication to ensure that database replication is successfully established on all nodes.

Procedure

Step 1 If a certificate must be signed by a third-party Certificate Authority, sign in to the Cisco Unified Operating System Administration GUI and perform the required steps for each relevant certificate.

Step 2 After you upload the signed certificate, you may need to restart services on the IM and Presence Service node.

The required service restarts are as follows:

- Tomcat certificate: Restart the tomcat service by running the following Command Line Interface (CLI) command:

  ```
  utils service restart Cisco Tomcat
  ```

- Cup-xmpp certificate: Restart the Cisco XCP Router service from the Cisco Unified Serviceability GUI.
- Cup-xmpp-s2s certificate: Restart the Cisco XCP Router service from the Cisco Unified Serviceability GUI.

Note

- These actions restart the affect service. Therefore, depending on the time lag in acquiring the signed certificates, you may need to schedule the restarts for a later maintenance window. In the meantime, the self-signed certificates will continue to be presented on the relevant interfaces until the services are restarted.
- If a certificate is not specified in the preceding list, no service restarts are required for that certificate.

What to do next

Perform the post-change task list on all applicable nodes within the cluster.

Node Name Change

You can modify the node name that is associated with an IM and Presence Service node or group of nodes. The updates are displayed on the **Server Configuration** window of Cisco Unified Communications Manager Administration.

Use these procedures for the following node name change scenarios:

- IP address to hostname
- IP address to Fully Qualified Domain Name (FQDN)
- hostname to IP address
- hostname to FQDN
- FQDN to hostname
- FQDN to IP address

For more information about node name recommendations, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

⚠

Caution Use this procedure to change the node name only for an IM and Presence Service node where there are no network-level changes needed. Perform the procedures that are specific to changing the network IP address, hostname, or the domain name in that case. You must perform this node name change procedure during a scheduled maintenance window. Changing the node name on any node in an IM and Presence Service cluster will result in node restarts and interruptions to presence services and other system functions.

IM and Presence Service Node Name Change Task List

The following table contains the step-by-step instructions to change the node name that is associated with an IM and Presence Service node or group of nodes. The detailed instructions for this procedure specify the exact order of steps for performing the change.

If you are performing this procedure across multiple clusters, complete all the sequential steps to change the node name on one cluster at a time.

Table 83: Change IM and Presence Service Node Name Task List

Item	Task
1	Complete the pre-change tasks on all applicable nodes within the cluster. Some of the pre-change tasks may apply only to the IM and Presence database publisher node and can be skipped if you are modifying a subscriber node.
2	Update the IM and Presence Service node name using Cisco Unified Communications Manager Administration.
3	Verify the node name updates and ensure that the node name change is synchronized with IM and Presence Service.
4	Verify database replication using the Command Line Interface (CLI) after the node name updates are complete. Ensure that the new node names have replicated across the cluster and that database replication is operational on all nodes.
5	Complete the post-change tasks list on the updated nodes and verify that the node is fully functional.

Update Node Name

If multiple nodes within a cluster are being modified, you must complete the following procedure sequentially for each node.

If the IM and Presence database publisher node is being modified, you must complete this procedure for the IM and Presence Service subscriber nodes first, before completing the procedure on the publisher node.

Note For IM and Presence nodes, it's recommended to use a fully qualified domain name. However, IP addresses and hostnames are also supported.

Before you begin

Perform all pre-change tasks and the applicable system health checks for your deployment.

Procedure

Step 1 Sign in to Cisco Unified CMAdministration.

Step 2 Select **System** > **Server**.

Step 3 Select the node that you want to modify.

Step 4 Update the **Host Name/IP Address** field with the new node name.

Note Ensure you upload the newly generated SP metadata to the IDP server.

Step 5 If multiple nodes within a cluster are being modified, repeat this procedure for each node.

Note If you update the IM and Presence Service node name and you also have third-party compliance configured, you must update the compliance server to use the new realm which is based on the node name. This configuration update is made on the third-party compliance server. The new realm will be displayed on the **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Compliance** > **Compliance Settings** window.

What to do next

Verify the node name change.

Verify Node Name Changes Using CLI

You can verify that the new node name has replicated across the cluster using the Command Line Interface (CLI).

Procedure

Step 1 Enter `run sql name select from processnode` to validate that the new node name has replicated correctly on each node in the cluster.

Example:

```
admin:run sql select name from processnode
name
=====================
EnterpriseWideData
server1.example.com
server2.example.com
server3.example.com
server4.example.com
```

Step 2 Verify that there is an entry for each node in the cluster that specifies the new node name. No old node name should appear in the output.

a) If the output is as expected, then validation has passed and you do not need to validate database replication for the nodes.

b) If any new node names are missing or if there are peferences to old node names, then continue to Step 3.

Step 3 To troubleshoot missing node names or old node names that appear for the node, perform the following actions:

a) For an IM and Presence database publisher node, check if the sync agent is running ok and verify that there are no errors in the sync agent status using the dashboard on the Cisco Unified CM IM and Presence Administration GUI.

b) For subscriber nodes, perform the validate database replication procedure.

Verify Node Name Changes Using Cisco Unified CM IM and Presence Administration

For IM and Presence Service nodes only, verify that the application server entry for this node has been updated to reflect the new node name on Cisco Unified CM IM and Presence Administration GUI.

Before you begin

Update the IM and Presence Service node name.

Procedure

Step 1 Sign in to the Cisco Unified CM IM and Presence Administration GUI.

Step 2 Select **System** > **Presence Topology**.

Step 3 Verify that the new node name appears in the **Presence Topology** pane.

What to do next

Verify database replication.

Update Domain Name for Cisco Unified Communications Manager

You can use the Command Line Interface (CLI) to change the domain name for Cisco Unified Communications Manager. Update the DNS domain name on all applicable nodes using the CLI. The CLI command makes the required domain name change on the node and triggers an automatic reboot for each node.

If the Unified CM cluster security mode is non-secure and you are updating or changing the domain, then as a part of domain changes all certificates will be regenerated. To make sure that the ITLs are updated on the phones, perform the following steps needed prior to updating the domain name:

1. Ensure that all phones are online and registered so that they can process the updated ITLs. For phones that are not online when this procedure is performed, the ITL must be deleted manually.
2. Set the **Prepare Cluster for Rollback to pre-8.0 enterprise** parameter to **True**. All phones automatically reset and download an ITL file that contains empty Trust Verification Services (TVS) and TFTP certificate sections.
3. On the phone, select **Settings > Security > Trust List > ITL File** to verify that the TVS and TFTP certificate sections of the ITL file are empty.
4. Change the domain of the server and let the phones configured for rollback register to the cluster.
5. After all the phones have successfully registered to the cluster, set the enterprise parameter **Prepare Cluster for Rollback to pre-8.0** to **False**.

Before you begin

- Ensure to enable the DNS before changing the domain name.
- Sign in to Cisco Unified Communications Manager Administration and navigate to the **System > Server Fields** page. If this server configuration settings page has an existing hostname entry, you should first change the hostname entry of the domain name.
- Perform all pre-change tasks and the applicable system health checks. See the Related Topic section for more information.

Procedure

Step 1 Log in to Command Line Interface.

Step 2 Enter **run set network domain <new_domain_name>**.
The command prompts for a system reboot.

Step 3 Click **Yes** to reboot the system.
The new domain name gets updated after the system is rebooted.

Step 4 Enter the command **show network eth0** to check if the new domain name is updated after the reboot.

Step 5 Repeat this procedure for all cluster nodes.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

CHAPTER 31

Post Change Tasks And Verification

Post-Change Tasks Cisco Unified Communications Manager Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Procedure

Step 1 If you have DNS configured anywhere on the Cisco Unified Communications Manager servers, ensure that a forward and reverse lookup zone has been configured and that the DNS is reachable and working.

Step 2 Check for any active ServerDown alerts to ensure that all servers in the cluster are up and available. Use either the Cisco Unified Real-Time Monitoring Tool (RTMT) or the command line interface (CLI) on the first node.

a) To check using Unified RTMT, access Alert Central and check for ServerDown alerts.

b) To check using the CLI on the first node, enter the following CLI command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 3 Check the database replication status on all nodes in the cluster to ensure that all servers are replicating database changes successfully.

For IM and Presence Service, check the database replication status on the database publisher node using the CLI if you have more than one node in your deployment.

Use either Unified RTMT or the CLI. All nodes should show a status of **2**.

a) To check by using RTMT, access the Database Summary and inspect the replication status.
b) To check by using the CLI, enter **`utils dbreplication runtimestate`**.

For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 4 Enter the CLI command **`utils diagnose`** as shown in the following example to check network connectivity and DNS server configuration.

Example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
admin:
```

If you are performing the pre-change system health checks, you are done; otherwise, continue to perform the post-change verification steps.

Step 5 Verify that the new hostname or IP address appears on the Cisco Unified Communications Manager server list. In Cisco Unified Communications Manager Administration, select **System** > **Server**.

Note Perform this step only as part of the post-change tasks.

Step 6 Verify that changes to the IP address, hostname, or both are fully implemented in the network. Enter the CLI command **`show network cluster`** on each node in the cluster.

Note Perform this step only as part of the post-change tasks.

The output should contain the new IP address or hostname of the node.

Example:

```
admin:show network cluster
10.63.70.125 hippo2.burren.pst hippo2 Subscriber cups DBPub authenticated
10.63.70.48 aligator.burren.pst aligator Publisher callmanager DBPub
authenticated using TCP since Wed May 29 17:44:48 2013
```

Step 7 Verify that changes to the hostname are fully implemented in the network. Enter the CLI command **`utils network host`** <***new_hostname***> on each node in the cluster.

Note Perform this step only as part of the post-change tasks.

The output should confirm that the new hostname resolves locally and externally to the IP address.

Example:

```
admin:utils network host hippo2
Local Resolution:
hippo2.burren.pst resolves locally to 10.63.70.125

External Resolution:
hippo2.burren.pst has address 10.63.70.125
```

tasks.

Step 8 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file and then restart all nodes in the cluster before you perform the system health checks and other post-change tasks.

For more information, see the Certificate and ITL Regeneration for Multi-Server Cluster Phones, on page 389 section.

Step 9 If you enabled cluster security using Certificate Trust List (CTL) files and USB eTokens, you must regenerate the Initial Trust List (ITL) file and the certificates in the ITL if you changed the IP address or hostname for Release 8.0 or later nodes. Skip this step if you have not enabled cluster security using Certificate Trust List (CTL) files and USB eTokens.

Step 10 Run a manual DRS backup and ensure that all nodes and active services back up successfully.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

Step 11 Update all relevant IP phone URL parameters.

Step 12 Update all relevant IP phone services using Cisco Unified Communications Manager Administration. Choose **System** > **Enterprise Parameters**.

Step 13 Update Unified RTMT custom alerts and saved profiles.

- Unified RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- Unified RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Step 14 If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Step 15 Check and make any required configuration changes to other associated Cisco Unified Communications components.

The following is a partial list of some of the components to check:

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 trunks
- IOS Gatekeepers
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- DHCP Scopes for IP phones

- SFTP servers that are used for Cisco Unified Communications Manager trace collection for CDR export, or as a DRS backup destination
- IOS hardware resources (conference bridge, media termination point, transcoder, RSVP agent) that register with Cisco Unified Communications Manager
- IPVC video MCUs that register or integrate with Cisco Unified Communications Manager
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Associated routers and gateways

Note Consult the documentation for your product to determine how to make any required configuration changes.

Security enabled cluster tasks for Cisco Unified Communications Manager nodes

Initial Trust List and Certificate Regeneration

If you change the IP address or the hostname of a server in a Cisco Unified Communications Manager Release 8.0 or later cluster, the Initial Trust List (ITL) file and the certificates in the ITL are regenerated. The regenerated files do not match the files stored on the phones.

Note If you enable cluster security using Certificate Trust List (CTL) files and USB eTokens, it is not necessary to perform the steps in the following procedure because trust is maintained by the eTokens and the eTokens are not changed.

If cluster security is not enabled, perform the steps in the Single-server cluster or Multi-server cluster procedures to reset the phones.

Regenerate certificates and ITL for single-server cluster phones

If you change the IP address or the hostname of the server in a Cisco Unified Communications Manager Release 8.0 or later single-server cluster and you are using ITL files, perform the following steps to reset the phones.

Enable rollback prior to changing the IP address or hostname of the server.

Procedure

Step 1 Ensure that all phones are online and registered so that they can process the updated ITLs. For phones that are not online when this procedure is performed, the ITL must be deleted manually.

Step 2 Set the Prepare Cluster for Rollback to pre-8.0 enterprise parameter to True. All phones automatically reset and download an ITL file that contains empty Trust Verification Services (TVS) and TFTP certificate sections.

Step 3 On the phone, select **Settings** > **Security** > **Trust List** > **ITL File** to verify that the TVS and TFTP certificate sections of the ITL file are empty.

Step 4 Change the IP address or hostname of the server and let the phones configured for rollback register to the cluster.

Step 5 After all the phones have successfully registered to the cluster, set the enterprise parameter Prepare Cluster for Rollback to pre-8.0 to **False**.

What to do next

If you use CTL files or tokens, re-run the CTL client after you change the IP address or hostname of the server, or after you change the DNS domain name.

Certificate and ITL Regeneration for Multi-Server Cluster Phones

In a multi-server cluster, the phones should have primary and secondary TVS servers to validate the regenerated ITL file and certificates. If a phone can not contact the primary TVS server (due to recent configuration changes), it will fall back to the secondary server. The TVS servers are identified by the CM Group assigned to the phone.

In a multi-server cluster, ensure that you change the IP address or hostname on only one server at a time. If you use CTL files or tokens, re-run the CTL client or the CLI command set **utils ctl** after you change the IP address or hostname of the server, or after you change the DNS domain name.

Post-Change Tasks for IM and Presence Service Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment.

⚠

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Procedure

Step 1 Verify that changes to the hostname or IP address are updated on the Cisco Unified Communications Manager server.

Step 2 Check network connectivity and DNS server configuration on the node that was changed.

Note If you changed the IP address to a different subnet, ensure that your network adapter is now connected to the correct VLAN. Also, if the IM and Presence Service nodes belong to different subnets after the IP address change, ensure that the Routing Communication Type field of the Cisco XCP Router service parameter is set to Router to Router. Otherwise, the Routing Communication Type field should be set to Multicast DNS.

Step 3 Verify that the changes to the IP address, hostname, or both are fully implemented in the network.

Step 4 If you changed the hostname, verify that the hostname change has been fully implemented in the network.

Step 5 Verify that database replication has been successfully established. All nodes should show a status of 2 and be Connected. If replication is not set up, see topics related to troubleshooting database replication.

Step 6 If you disabled SAML single sign-on (SSO), you can enable it now. For more information about SAML SSO, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Step 7 If you changed the hostname, you must ensure that the cup, cup-xmpp and Tomcat certificates contain the new hostname.

a) From the Cisco Unified OS Administration GUI, select **Security** > **Certificate Management**.
b) Verify that the names of the trust certificates contain the new hostname.
c) If the certificates do not contain the new hostname, regenerate the certificates.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 8 If the IP address for a node has changed, update Cisco Unified Real-Time Monitoring Tool (RTMT) custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server address. You must delete and re-add these counters and then save the profile to update it to the new address.

Step 9 Check and make any required configuration changes to other associated Cisco Unified Communications components, for example, SIP trunks on Cisco Unified Communications Manager.

Step 10 Start all network services that are listed under the CUP Services group using Cisco Unified Serviceability, select **Tools** > **Control Center - Network Services**.

Tip You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Network services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all network services are started.

You must start the CUP Services network services in the following order:

a. Cisco IM and Presence Data Monitor
b. Cisco Server Recovery Manager
c. Cisco Route Datastore
d. Cisco Login Datastore
e. Cisco SIP Registration Datastore
f. Cisco Presence Datastore
g. Cisco XCP Config Manager
h. Cisco XCP Router
i. Cisco OAM Agent

j. Cisco Client Profile Agent
k. Cisco Intercluster Sync Agent
l. Cisco Config Agent

Step 11 Start all feature services using Cisco Unified Serviceability, select **Tools** > **Control Center - Feature Services**. The order in which you start feature services is not important.

Tip You do not need to complete this step if you are changing the IP address, hostname, or both the IP address and hostname. Feature services are automatically started for these name changes. However, if some services do not automatically start after the change, complete this step to ensure that all feature services are started.

Step 12 Confirm that your Cisco Jabber sessions have been recreated before you re-enable High Availability. Otherwise, Jabber clients whose sessions are created will be unable to connect.

Run the `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI command on all cluster nodes. The number of active sessions should match the number of users that you recorded when you disabled high availability. If it takes more than 30 minutes for your sessions to start, you may have a larger system issue.

Step 13 Enable High Availability (HA) on all presence redundancy groups if you disabled HA during the pre-change setup.

Step 14 Verify that IM and Presence Service is functioning properly after the changes.

a) From the Cisco Unified Serviceability GUI, select **System** > **Presence Topology**.

- If HA is enabled, verify that all HA nodes are in the Normal state.
- Verify that all services are started.

b) Run the System Troubleshooter from the Cisco Unified CM IM and Presence Administration GUI and ensure that there are no failed tests. Select **Diagnostics** > **System Troubleshooter**.

Step 15 You must run a manual Disaster Recovery System backup after you change the IP address or hostname of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

CHAPTER 32

Troubleshooting Address Change Issues

Troubleshoot Cluster Authentication

You can troubleshoot cluster authentication issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`show network eth0 [detail]`** to verify network configuration.

Step 2 Enter **`show network cluster`** to verify the network cluster information.

- If the output displays incorrect publisher information, enter the **`set network cluster publisher [hostname/IP address]`** CLI command on the subscriber node to correct the information.
- If you are on a publisher node, and the `show network cluster` CLI command displays incorrect subscriber information, login to Cisco Unified Communications Manager Administration and choose **System** > **Server** to check the output.
- If you are on a subscriber node and the `show network cluster` output displays incorrect publisher information, use the `set network cluster publisher [hostname | IP_address]` CLI command to change the publisher hostname or IP address.

Troubleshoot Database Replication

You can use the Command Line Interface (CLI) to troubleshoot database replication on the nodes in your cluster.

- Verify that database replication is in a correct state in the cluster.

- Repair and reestablish database replication for the nodes.
- Reset database replication.

For more information about these commands or using the CLI, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Verify Database Replication

Use the Command Line Interface (CLI) to check the database replication status for all nodes in the cluster. Verify that the Replication Setup (RTMT) & Details shows a value of **2**. Anything other than 2 means that there is a problem with database replication and that you need to reset replication for the node. See topics related to database replication examples for example output.

Procedure

Step 1 Enter **`utils dbreplication runtimestate`** on the first node to check database replication on all nodes in the cluster.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

Tip If replication is not set up for the nodes in your cluster, you can reset database replication for the nodes using the CLI. For more information, see topics related to resetting database replication using the CLI.

Example:

```
admin: utils dbreplication runtimestate

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-09-26-15-18
     Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
     Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from PUB (2 Servers):

                         PING        REPLICATION REPL. DBver& REPL. REPLICATION
SETUP
SERVER-NAME IP ADDRESS   (msec) RPC? STATUS      QUEUE TABLES LOOP? (RTMT) &
details
----------- ------------ ------ ---- ----------- ----- ------ -----
-----------------
server1     100.10.10.17 0.052  Yes  Connected   0     match  Yes   (2) PUB Setup
 Completed
server2     100.10.10.14 0.166  Yes  Connected   0     match  Yes   (2) Setup
Completed
```

Step 2 Verify the output.

The output should show a replication status of **Connected** and a replication setup value of **(2) Setup Complete** for each node. This means that the replication network within the cluster is functioning properly. If the output results are different, proceed to troubleshoot and repair database replication.

Example Database Replication CLI Output

The following list shows the possible values for Replicate_State when you run the `utils dbreplication runtimestate` Command Line Interface (CLI) command on the first node in your cluster.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

- 0 - Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
- 1 - Replicates have been created, but their count is incorrect.
- 2 - Replication is good.
- 3 - Replication is bad in the cluster.
- 4 - Replication setup did not succeed.

Note It is important to verify that the Replication Setup (RTMT) & Details shows a value of `2`. Anything other than 2 means that there is a problem with database replication and that you need to reset replication. For information about resolving database replication issues, see topics related to troubleshooting database replication.

Example CLI Output for Cisco Unified Communications Manager Node

In this example, the Replication Setup (RTMT) & Details shows a value of `2`. Replication is good.

```
admin: utils dbreplication runtimestate
Server Time: Mon Jun 1 12:00:00 EDT 2013

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-06-01-12-00
   Last Sync Result: SYNC COMPLETED on 672 tables out of 672
   Sync Status: NO ERRORS
   Use CLI to see detail: 'file view activelog
cm/trace/dbl/2013_06_01_12_00_00_dbl_repl_output_Broadcast.log'

DB Version: ccm10_0_1_10000_1
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from uc10-pub (2 Servers):

                        PING       Replication  REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) RPC? Group ID     (RTMT) & Details
----------- ---------- ------ ---- ----------- -------------------
uc10-pub    192.0.2.95 0.040  Yes    (g_2)      (2) Setup Completed
uc10-sub1   192.0.2.96 0.282  Yes    (g_3)      (2) Setup Completed
```

Example CLI Output for IM and Presence Service Node

In this example, the Replication Setup (RTMT) & Details shows a value of 2. Replication is good.

```
admin: utils dbreplication runtimestate
Server Time: Mon Jun 1 12:00:00 EDT 2013

DB and Replication Services: ALL RUNNING

Cluster Replication State: Replication status command started at: 2012-02-26-09-40

   Replication status command COMPLETED 269 tables checked out of 269
   No Errors or Mismatches found.
   Use 'file view activelog
cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out' to see the details

DB Version: ccm8_6_3_10000_23
Number of replicated tables: 269

Cluster Detailed View from PUB (2 Servers):

                       PING       REPLICATION   REPL. DBver&  REPL.  REPLICATION
 SETUP
SERVER-NAME IP ADDRESS (msec) RPC? STATUS        QUEUE TABLES  LOOP? (RTMT) &
details
----------- ------------ ------ ---- ----------- ----- ------- -----
-----------------
gwydla020218 10.53.46.130 0.038 Yes Connected    0     match   Yes   (2) PUB Setup
 Completed
gwydla020220 10.53.46.133 0.248 Yes Connected    128   match   Yes   (2) Setup
Completed
```

Repair Database Replication

Use the Command Line Interface (CLI) to repair database replication.

Procedure

Step 1 Enter `utils dbreplication repair all` on the first node to attempt to repair database replication.

For IM and Presence Service, repair the database replication status from the database publisher node if you have more than one node in your deployment.

Depending on the size of the database, it may take several minutes to repair database replication. Proceed to the next step to monitor the progress of database replication repair.

Example:

```
admin:utils dbreplication repair all
-------------------- utils dbreplication repair --------------------

Replication Repair is now running in the background.
Use command 'utils dbreplication runtimestate' to check its progress

Output will be in file cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out
```

```
Please use "file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out " command to see the
output
```

Step 2 Enter `utils dbreplication runtimestate` on the first node to check the progress of replication repair.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

The bolded text in the example replication output highlights the final status of the replication repair.

Example:

```
admin:utils dbreplication runtimestate

DB and Replication Services: ALL RUNNING

Cluster Replication State: Replication repair command started at: 2013-05-11-12-33

     Replication repair command COMPLETED 269 tables processed out of 269
     No Errors or Mismatches found.

     Use 'file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out' to see the details

DB Version: ccm8_6_4_98000_192
Number of replicated tables: 269

Cluster Detailed View from PUB (2 Servers):

                         PING        REPLICATION REPL. DBver& REPL. REPLICATION
SETUP
SERVER-NAME IP ADDRESS   (msec) RPC? STATUS      QUEUE TABLES LOOP? (RTMT) &
details
----------- ------------ ------ ---- ----------- ----- ------ -----
-----------------
server1     100.10.10.17 0.052  Yes  Connected   0     match  Yes   (2) PUB Setup
 Completed
server2     100.10.10.14 0.166  Yes  Connected   0     match  Yes   (2) Setup
Completed
```

a) If replication repair runs to completion without any errors or mismatches, run the procedure to verify the node name change again to validate that the new node name is now correctly replicated.
b) If errors or mismatches are found, there may be a transient mismatch between nodes. Run the procedure to repair database replication again.

Note If, after several attempts to repair replication, mismatches or errors are being reported, contact your Cisco Support Representative to resolve this issue.

Step 3 Enter `utils dbreplication reset all` on the first node to attempt to reestablish replication.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in the deployment.

Depending on the size of the database, it may take several minutes to over an hour for replication to be fully reestablished. Proceed to the next step to monitor the progress of database replication reestablishment.

Example:

```
admin:utils dbreplication reset all
This command will try to start Replication reset and will return in 1-2 minutes.
Background repair of replication will continue after that for 1 hour.
Please watch RTMT replication state. It should go from 0 to 2. When all subs
have an RTMT Replicate State of 2, replication is complete.
If Sub replication state becomes 4 or 1, there is an error in replication setup.
Monitor the RTMT counters on all subs to determine when replication is complete.
Error details if found will be listed below
OK [10.53.56.14]
```

Step 4 Enter `utils dbreplication runtimestate` on the first node to monitor the progress of the attempt to reestablish database replication.

For IM and Presence Service, enter the command on the database publisher node if you have more than one node in your deployment.

Replication is considered to be reestablished when all nodes show a replication status of **Connected** and a replication setup value of **(2) Setup Complete**.

Example:

```
admin: utils dbreplication runtimestate

DDB and Replication Services: ALL RUNNING

DB CLI Status: No other dbreplication CLI is running...

Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-09-26-15-18
     Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257
     Sync Errors: NO ERRORS

DB Version: ccm9_0_1_10000_9000
Number of replicated tables: 257
Repltimeout set to: 300s

Cluster Detailed View from newserver100 (2 Servers):
                           PING      REPLICATION REPL. DBver& REPL. REPLICATION
 SETUP
SERVER-NAME IP ADDRESS     (msec) RPC? STATUS      QUEUE TABLES LOOP? (RTMT) &
details
----------- -------------- ------ ---- ----------- ----- ------ -----
-----------------
server1     100.10.10.201  0.038  Yes  Connected   0     match  Yes   (2) PUB
Setup Completed
server2     100.10.10.202  0.248  Yes  Connected   0     match  Yes   (2) Setup
Completed
server3     100.10.10.203  0.248  Yes  Connected   0     match  Yes   (2) Setup
Completed
server4     100.10.10.204  0.248  Yes  Connected   0
```

a) If replication is reestablished, run the procedure to verify the node name change again to validate that the new node name is now correctly replicated.

b) If replication does not recover, contact your Cisco Support Representative to resolve this issue.

Caution Do not proceed beyond this point if database replication is broken.

Reset Database Replication

Reset database replication if replication is not set up for the nodes in your cluster. You can reset database replication using the command line interface (CLI).

Before you begin

Check database replication status for all nodes in the cluster. Verify that the Replication Setup (RTMT) & Details shows a value of `2`. Anything other than 2 means that there is a problem with database replication and that you need to reset replication for the node.

Procedure

Step 1 Reset replication on nodes in your cluster. Do one of the following:

a) For Unified Communications Manager, enter **`utils db replication reset all`**.

Before you run this CLI command on any Cisco Unified Communications Manager nodes, first run the command **`utils dbreplication stop`** on all subscriber nodes that are reset, and then on the publisher server. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

b) For IM and Presence Service, enter **`utils db replication reset all`** on the database publisher node to reset all IM and Presence Service nodes in the cluster.

Tip You can enter a specific hostname instead of **all** to reset database replication on only that node. For more information, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Step 2 Enter **`utils dbreplication runtimestate`** to check the database replication status.

For IM and Presence Service, run the CLI command on the IM and Presence database publisher node

Troubleshoot Network

You can troubleshoot network issues on nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`show network eth0 [detail]`** to verify network configuration.

Step 2 If any of the fields are missing, then reset the network interface.

a) Enter **`set network status eth0 down`**.
b) Enter **`set network status eth0 up`**.

Step 3 Verify the IP address, mask, and gateway.

Ensure that these values are unique across the network.

Network Time Protocol troubleshooting

Troubleshoot NTP on Subscriber Nodes

You can troubleshoot Network Time Protocol (NTP) issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **`show network eth0 [detail]`** to verify network configuration.

Step 2 Enter **`utils ntp status`** to verify NTP status.

Step 3 Enter **`utils ntp restart`** to Restart NTP.

Step 4 Enter **`show network cluster`** to verify the network cluster.

If the output displays incorrect publisher information, use the **`set network cluster publisher [hostname/IP_address]`** CLI command to reset the publisher.

Troubleshoot NTP on Publisher Nodes

You can troubleshoot Network Time Protocol (NTP) issues on publisher nodes using the Command Line Interface (CLI).

Procedure

	Command or Action	Purpose
Step 1	Enter **`show network eth0 [detail]`** to verify network configuration.	
Step 2	Enter **`utils ntp status`** to verify NTP status.	
Step 3	Enter **`utils ntp restart`** to Restart NTP.	
Step 4	Enter **`utils ntp server list`** to verify NTP servers.	To add or delete an NTP server, use the **`utils ntp server [add/delete]`** CLI command.

PART VIII

Disaster Recovery

CHAPTER 33

Back Up the System

Backup Overview

Cisco recommends performing regular backups. You can use the Disaster Recovery System (DRS) to do a full data backup for all servers in a cluster. You can set up automatic backups or invoke a backup at any time.

The Disaster Recovery System performs a cluster-level backup, which means that it collects backups for all servers in a Cisco Unified Communications Manager cluster to a central location and archives the backup data to physical storage device. Backup files are encrypted and can be opened only by the system software.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

When you perform a system data restoration, you can choose which nodes in the cluster you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks.
- A distributed system architecture for performing backup functions.
- Scheduled backups or manual (user-invoked) backups.
- It archives backups to a remote sftp server.

The table displays the features and components that the Disaster Recovery System can back up and restore. For each feature that you choose, the system backs up all its components automatically.

Table 84: Cisco Unified CM Features and Components

Feature	Components
CCM - Unified Communications Manager	Unified Communications Manager database
	Platform
	Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)
	Call Detail Records (CDRs)
	CDR Reporting and Analysis (CAR)

Table 85: IM and Presence Features and Components

Feature	Components
IM and Presence Service	IM and Presence database
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	Platform
	Reporter (Serviceability Reporter)
	CUP SIP Proxy
	XCP
	CLM
	Bulk Tool (BAT)
	Preference
	tct (trace collection tool)

Backup Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The software version saved in the backup file must match the version that is running on the cluster nodes.

  The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail. Ensure that you backup the system whenever you upgrade the software version so that the version saved in the backup file matches the version that is running on the cluster nodes.
- Be aware the DRS encryption depends on the cluster security password. When running the backup, DRS generates a random password for encryption and then encrypts the random password with the cluster security password. If the cluster security password ever gets changed between the backup and this restore, you will need to know what the password was at the time of the backup in order to use that backup file to restore your system or take a backup immediately after the security password change/reset.
- If you want to back up to a remote device, make sure that you have an SFTP server set up. For more information on the available SFTP servers, see SFTP Servers for Remote Backups , on page 411

Backup Task Flow

Complete these tasks to configure and run a backup. Do not perform any OS Administration tasks while a backup is running. This is because Disaster Recovery System blocks all OS Administration requests by locking platform API. However, Disaster Recovery System does not block most CLI commands, because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

	Command or Action	Purpose
Step 1	Configure Backup Devices, on page 406	Specify the devices on which to back up data.
Step 2	Estimate Size of Backup File, on page 407	Estimate size of backup file created on the SFTP device.
Step 3	Choose one of the following options: • Configure a Scheduled Backup, on page 407 • Start a Manual Backup, on page 409	Create a backup schedule to back up data on a schedule. Optionally, run a manual backup.

	Command or Action	Purpose
Step 4	View Current Backup Status, on page 409	Optional. Check the Status of the Backup. While a backup is running, you can check the status of the current backup job.
Step 5	View Backup History, on page 410	Optional. View Backup History

Configure Backup Devices

You can configure up to 10 backup devices. Perform the following steps to configure the location where you want to store backup files.

Before you begin

- Ensure you have write access to the directory path in the SFTP server to store the backup file.
- Ensure that the username, password, server name, and directory path are valid as the DRS Master Agent validates the configuration of the backup device.

Note Schedule backups during periods when you expect less network traffic.

Procedure

Step 1 From Disaster Recovery System, select **Backup** > **Backup Device**.

Step 2 In the **Backup Device List** window, do either of the following:

- To configure a new device, click **Add New**.
- To edit an existing backup device, enter the search criteria, click Find, and **Edit Selected**.
- To delete a backup device, select it in the **Backup Device** list and click **Delete Selected**.

You cannot delete a backup device that is configured as the backup device in a backup schedule.

Step 3 Enter a backup name in the **Backup Device Name** field.

The backup device name contains only alphanumeric characters, spaces (), dashes (-) and underscores (_). Do not use any other characters.

Step 4 In the **Select Destination** area, under **Network Directory** perform the following:

- In the **Host name/IP Address** field, enter the hostname or IP address for the network server.
- In the **Path name** field, enter the directory path where you want to store the backup file.
- In the **User name** field, enter a valid username.
- In the **Password** field, enter a valid password.
- From the **Number of backups to store on Network Directory** drop-down list, choose the required number of backups.

Step 5 Click **Save**.

What to do next

Estimate Size of Backup File, on page 407

Estimate Size of Backup File

Cisco Unified Communications Manager will estimate the size of the backup tar, only if a backup history exists for one or more selected features.

The calculated size is not an exact value but an estimated size of the backup tar. Size is calculated based on the actual backup size of a previous successful backup and may vary if the configuration changed since the last backup.

You can use this procedure only when the previous backups exist and not when you back up the system for the first time.

Follow this procedure to estimate the size of the backup tar that is saved to a SFTP device.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Select Features** area, select the features to back up.

Step 3 Click **Estimate Size** to view the estimated size of backup for the selected features.

What to do next

Perform one of the following procedures to backup your system:

- Configure a Scheduled Backup, on page 407
- Start a Manual Backup, on page 409

Configure a Scheduled Backup

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Be aware that your backup .tar files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along with the backup .tar files. You must remember this security password or take a backup immediately after the security password change or reset.

Caution Schedule backups during off-peak hours to avoid call processing interruptions and impact to service.

Before you begin

Configure Backup Devices, on page 406

Procedure

Step 1 From the Disaster Recovery System, choose **Backup** **Scheduler**.

Step 2 In the **Schedule List** window, do one of the following steps to add a new schedule or edit an existing schedule.

- To create a new schedule, click **Add New**.
- To configure an existing schedule, click the name in the Schedule List column.

Step 3 In the **scheduler** window, enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 4 Select the backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Features** area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 Choose the frequency at which you want the backup to occur in the **Frequency** area. The frequency can be set to Once Daily, Weekly, and Monthly. If you choose **Weekly**, you can also choose the days of the week when the backup will occur.

Tip To set the backup frequency to **Weekly**, occurring Tuesday through Saturday, click **Set Default**.

Step 8 To update these settings, click **Save**.

Step 9 Choose one of the following options:

- To enable the selected schedules, click **Enable Selected Schedules**.
- To disable the selected schedules, click **Disable Selected Schedules**.
- To delete the selected schedules, click **Delete Selected**.

Step 10 To enable the schedule, click **Enable Schedule**.

The next backup occurs automatically at the time that you set.

Note Ensure that all servers in the cluster are running the same version of Cisco Unified Communications Manager or Cisco IM and Presence Service and are reachable through the network. Servers that are not reachable at the time of the scheduled backup will not get backed up.

What to do next

Perform the following procedures:

- Estimate Size of Backup File, on page 407
- (Optional) View Current Backup Status, on page 409

Start a Manual Backup

Before you begin

- Ensure that you use a network device as the storage location for the backup files. Virtualized deployments of Unified Communications Manager do not support the use of tape drives to store backup files.
- Ensure that all cluster nodes have the same installed version of Cisco Unified Communications Manager or IM and Presence Service.
- The backup process can fail due to non availability of space on a remote server or due to interruptions in the network connectivity. You need to start a fresh backup after addressing the issues that caused the backup to fail.
- Ensure that there are no network interruptions.
- Configure Backup Devices, on page 406
- Estimate Size of Backup File, on page 407
- Make sure that you have a record of the cluster security password. If the cluster security password changes after you complete this backup, you will need to know the password or you will not be able to use the backup file to restore your system.

Note While a backup is running, you cannot perform any tasks in Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration because Disaster Recovery System locks the platform API to block all requests. However, Disaster Recovery System does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Manual Backup**.

Step 2 In the **Manual Backup** window, select a backup device from the **Backup Device Name** area.

Step 3 Choose a feature from the **Select Features** area.

Step 4 Click **Start Backup.**

What to do next

(Optional) View Current Backup Status, on page 409

View Current Backup Status

Perform the following steps to check the status of the current backup job.

⚠

Caution Be aware that if the backup to the remote server is not completed within 20 hours, the backup session times out and you must begin a fresh backup.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **Current Status**.

Step 2 To view the backup log file, click the log filename link.

Step 3 To cancel the current backup, click **Cancel Backup**.

Note The backup cancels after the current component completes its backup operation.

What to do next

View Backup History, on page 410

View Backup History

Perform the following steps to view the backup history.

Procedure

Step 1 From the Disaster Recovery System, select **Backup** > **History**.

Step 2 From the **Backup History** window, you can view the backups that you have performed, including filename, backup device, completion date, result, version, features that are backed up, and failed features.

Note The **Backup History** window displays only the last 20 backup jobs.

Backup Interactions and Restrictions

- Backup Restrictions , on page 411

Backup Restrictions

The following restrictions apply to backups:

Table 86: Backup Restrictions

Restriction	Description
Cluster Security Password	We recommend that you run a backup whenever you change the cluster security password. Backup encryption uses the cluster security password to encrypt data on the backup file. If you edit the cluster security password after a backup file is created, you will not be able to use that backup file to restore data unless you remember the old password.
Certificate Management	The Disaster Recovery System (DRS) uses an SSL-based communication between the Master Agent and the Local Agent for authentication and encryption of data between the Cisco Unified Communications Manager cluster nodes. DRS makes use of the IPsec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore(hostname.pem) file from the Certificate Management pages, then DRS will not work as expected. If you delete the IPSEC-trust file manually, you must ensure that you upload the IPSEC certificate to the IPSEC-trust. For more details, see the “Certificate management” section in the *Security Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

SFTP Servers for Remote Backups

To back up data to a remote device on the network, you must have an SFTP server that is configured. For internal testing, Cisco uses the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Use the information in the following table to determine which SFTP server solution to use in your system.

Table 87: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Unified Communications Manager and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Unified Communications Manager to ensure that the versions are compatible.

SFTP Server	Information
SFTP Server from a Technology Partner	These servers are third party provided and third party tested. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Unified Communications Manager for which versions are compatible: https://marketplace.cisco.com
SFTP Server from another Third Party	These servers are third party provided and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Unified Communications Manager versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Cipher Support

For Unified Communications Manager 11.5, Unified Communications Manager advertises the following CBC and CTR ciphers for SFTP connections:

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

Note Make sure that the backup SFTP Server supports one of these ciphers to communicate with Unified Communications Manager.

From Unified Communications Manager 12.0 release onwards, CBC ciphers are not supported. Unified Communications Manager supports and advertises only the following CTR ciphers:

- aes256-ctr
- aes128-ctr
- aes192-ctr

Note Make sure that the backup SFTP Server supports one of these CTR ciphers to communicate with Unified Communications Manager.

CHAPTER 34

Restore the System

Restore Overview

The Disaster Recovery System (DRS) provides a wizard to walk you through the process of restoring your system.

The backup files are encrypted and only the DRS system can open them to restore the data. The Disaster Recovery System includes the following capabilities:

- A user interface for performing restore tasks.
- A distributed system architecture for performing restore functions.

Master Agent

The system automatically starts the Master Agent service on each node of the cluster, but the Master Agent is functional only on the publisher node. The Master Agents on the subscriber nodes do not perform any functions.

Local Agents

The server has a Local Agent to perform backup and restore functions.

Each node in a Cisco Unified Communications Manager cluster, including the node that contains the Master Agent, must have its own Local Agent to perform backup and restore functions.

Note

By default, a Local Agent automatically gets started on each node of the cluster, including IM and Presence nodes.

Restore Prerequisites

- Make sure that you meet the version requirements:
  - All Cisco Unified Communications Manager cluster nodes must be running the same version of the Cisco Unified Communications Manager application.
  - All IM and Presence Service cluster nodes must be running the same version of the IM and Presence Service application.
  - The version saved in the backup file must match the version that is running on the cluster nodes.

  The entire version string must match. For example, if the IM and Presence database publisher node is at version 11.5.1.10000-1, then all IM and Presence subscriber nodes must be 11.5.1.10000-1, and the backup file must also be must be 11.5.1.10000-1. If you try to restore the system from a backup file that does not match the current version, the restore will fail.
- Make sure that the IP address, hostname, DNS configuration and deployment type for the server matches the IP address, hostname, DNS configuration and deployment type that are stored on the backup file.
- If you have changed the cluster security password since the backup was run, make sure that you have a record of the old password, or the restore will fail.

Re-enable SAML SSO after Restore

Important

This section is applicable for Release 12.5(1)SU7 only.

After restoring the system using DRS, SAML SSO can be disabled on any of the nodes in the cluster intermittently. To re-enable SAML SSO on the affected nodes, you must perform the following:

1. From Cisco Unified CM Administration, choose **System** > **SAML Single Sign On**.
2. Click **Run SSO Test**.
3. After you see the **"SSO Test Succeeded!"** message, close the browser window; click **Finish**.

Note

Cisco Tomcat restarts during SAML SSO re-enabling process. It will not have any impact on the nodes where SAML SSO is already enabled.

Restore Task Flow

During the restore process, do not perform any tasks with Cisco Unified Communications Manager OS Administration or Cisco Unified IM and Presence OS Administration.

Procedure

	Command or Action	Purpose
Step 1	Restore the First Node Only, on page 415	(Optional) Use this procedure only to restore the first publisher node in the cluster.
Step 2	Restore Subsequent Cluster Node, on page 417	(Optional) Use this procedure to restore the subscriber nodes in a cluster.
Step 3	Restore Cluster in One Step After Publisher Rebuilds, on page 418	(Optional) Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt.
Step 4	Restore Entire Cluster, on page 420	(Optional) Use this procedure to restore all nodes in the cluster, including the publisher node. If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you may need to rebuild all nodes in the cluster.
Step 5	Restore Node Or Cluster to Last Known Good Configuration, on page 421	(Optional) Use this procedure only if you are restoring a node to a last known good configuration. Do not use this after a hard drive failure or other hardware failure.
Step 6	Restart a Node, on page 421	Use this procedure to restart a node.
Step 7	Check Restore Job Status, on page 422	(Optional) Use this procedure to check the restore job status.
Step 8	View Restore History, on page 423	(Optional) Use this procedure to view the restore history.

Restore the First Node Only

If you are restoring the first node after a rebuild, you must configure the backup device.

This procedure is applicable to the Cisco Unified Communications Manager First Node, also known as the publisher node. The other Cisco Unified Communications Manager nodes and all the IM and Presence Service nodes are considered as secondary nodes or subscribers.

Before you begin

If there is an IM and Presence Service node in the cluster, ensure that it is running and accessible when you restore the first node. This is required so that a valid backup file can be found during the procedure.

Procedure

Step 1 From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window, **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 Choose the features that you want to restore.

Note The features that you have selected for backup will be displayed.

Step 8 Click **Next**. The Restore Wizard Step 4 window displays.

Step 9 Select the Perform file integrity check using the SHA1 Message Digest checkbox if you want to run a file integrity check.

Note The file integrity check is optional and is only needed in the case of SFTP backups.

Be aware that the file integrity check process consumes a significant amount of CPU and network bandwidth, which slows down the restore process.

We can use SHA-1 for message digest verification in FIPS mode as well. SHA-1 is allowed for all non-digital signature uses in the hash functions applications like HMAC and Random Bit Generation that are not used for digital signatures. For instance, SHA-1 can still be used to compute a checksum. Only for signature generation and verification, we can't use SHA-1.

Step 10 Select the node to restore.

Step 11 Click **Restore** to restore the data.

Step 12 Click **Next**.

Step 13 When you are prompted to select the nodes to restore, choose only the first node (the publisher).

Caution Do not select the subsequent (subscriber) nodes in this condition as this will result in failure of the restore attempt.

Step 14 (Optional) From the **Select Server Name** drop-down list, select the subscriber node from which you want to restore the publisher database. Ensure that the subscriber node that you chose is in-service and connected to the cluster.
The Disaster Recovery System restores all non database information from the backup file and pulls the latest database from the chosen subscriber node.

Note This option appears only if the backup file that you selected includes the CCMDB database component. Initially, only the publisher node is fully restored, but when you perform Step 14 and restart the subsequent cluster nodes, the Disaster Recovery System performs database replication and fully synchronizes all cluster node databases. This ensures that all cluster nodes are using current data.

Step 15 Click **Restore**.

Step 16 Your data is restored on the publisher node. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Note Restoring the first node restores the whole Cisco Unified Communications Manager database to the cluster. This may take up to several hours based on number of nodes and size of database that is being restored. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 17 When the **Percentage Complete** field on the **Restore Status** window, shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note If you are restoring a Cisco Unified Communications Manager node only, the Cisco Unified Communications Manager and IM and Presence Service cluster must be restarted.

If you are restoring an IM and Presence Service Publisher node only, the IM and Presence Service cluster must be restarted.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 422
- To restart a node, see Restart a Node, on page 421

Restore Subsequent Cluster Node

This procedure is applicable to the Cisco Unified Communications Manager subscriber (subsequent) nodes only. The first Cisco Unified Communications Manager node installed is the publisher node. All other Cisco Unified Communications Manager nodes, and all IM and Presence Service nodes are subscriber nodes.

Follow this procedure to restore one or more Cisco Unified Communications Manager subscriber nodes in the cluster.

Before you begin

Before you perform a restore operation, ensure that the hostname, IP address, DNS configuration, and deployment type of the restore matches the hostname, IP address, DNS configuration, and deployment type of the backup file that you want to restore. Disaster Recovery System does not restore across different hostnames, IP addresses, DNS configurations and deployment types.

Ensure that the software version that is installed on the server matches the version of the backup file that you want to restore. Disaster Recovery System supports only matching software versions for restore operations. If you are restoring the subsequent nodes after a rebuild, you must configure the backup device.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window, **Select Backup Device** area, choose the backup device from which to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, select the features that you want to restore.

Note Only the features that were backed up to the file that you chose display.

Step 7 Click **Next**. The Restore Wizard Step 4 window displays.

Step 8 In the **Restore Wizard Step 4** window, when you are prompted to choose the nodes to restore, select only the subsequent nodes.

Step 9 Click **Restore**.

Step 10 Your data is restored on the subsequent nodes. For more information about how to view the status of the restore, see the What to Do Next section.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Step 11 When the **Percentage Complete** field on the **Restore Status** window shows 100%, restart the secondary servers you just restored. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

Note If the IM and Presence Service first node is restored. Ensure to restart the IM and Presence Service first node before you restart the IM and Presence Service subsequent nodes.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 422
- To restart a node, see Restart a Node, on page 421

Restore Cluster in One Step After Publisher Rebuilds

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore. Follow this procedure to restore the entire cluster in one step if the publisher has already been rebuilt or freshly installed.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Restore Wizard Step 1** window **Select Backup Device** area, choose the backup device from which to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file that you want to restore.

The backup filename indicates the date and time that the system created the backup file.

Choose only the backup file of the cluster from which you want to restore the entire cluster.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, select the features that you want to restore.

The screen displays only those features that were saved to the backup file.

Step 7 Click **Next**.

Step 8 In the **Restore Wizard Step 4** window, click **One-Step Restore**.

This option appears on **Restore Wizard Step 4** window only if the backup file selected for restore is the backup file of the cluster and the features chosen for restore includes the feature(s) that is registered with both publisher and subscriber nodes. For more information, see Restore the First Node Only, on page 415 and Restore Subsequent Cluster Node, on page 417.

Note If a status message indicates that *Publisher has failed to become cluster aware. Cannot start one-step restore*, you need to restore the publisher node and then the subscriber node. See the Related topics for more information.

This option allows the publisher to become cluster aware and will take five minutes to do so. Once you click on this option, a status message displays as “Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period”.

After the delay, if the publisher becomes cluster aware, a status message displays as “Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster”.

After the delay, if the publisher has not become cluster aware, a status message displays as "Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore." To restore the whole cluster in two-step (publisher and then subscriber), perform the steps mentioned in Restore the First Node Only, on page 415 and Restore Subsequent Cluster Node, on page 417.

Step 9 When you are prompted to choose the nodes to restore, choose all the nodes in the cluster.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database that is being restored.

Step 10 Click **Restore**.
Your data is restored on all the nodes of the cluster.

Step 11 When the **Percentage Complete** field on the **Restore Status window** shows 100%, restart the server. Restart of all the nodes in the cluster is required in case of restoring only to the first node. Ensure that you restart the first node before you restart the subsequent nodes. For information about how to restart the server, see the What to Do Next section.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 422

- To restart a node, see Restart a Node, on page 421

Restore Entire Cluster

If a major hard drive failure or upgrade occurs, or in the event of a hard drive migration, you have to rebuild all nodes in the cluster. Follow these steps to restore an entire cluster.

If you are doing most other types of hardware upgrades, such as replacing a network card or adding memory, you do not need to perform this procedure.

Procedure

Step 1 From Disaster Recovery System, select **Restore** > **Restore Wizard**.

Step 2 In the **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 In the **Restore Wizard Step 4** window, select all the nodes when prompted to choose restore nodes.

Step 8 Click **Restore** to restore the data.

The Disaster Recovery System restores the Cisco Unified Communications Manager database (CCMDB) on subsequent nodes automatically when you restore a first node. This may take up to several hours based on number of nodes and size of that database.

Data is restored on the all the nodes.

Note During the restore process, do not perform any tasks with Cisco Unified Communications Manager Administration or User Options.

Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 9 Restart the server once the restoration process is completed. See the What to Do Next section for more information about how to restart the server.

Note Make sure that you restart the first node before you restart the subsequent nodes.

After the first node has restarted and is running the restored version of Cisco Unified Communications Manager, restart the subsequent nodes.

Step 10 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the “utils dbreplication runtimestate” CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*. The value on each node should equal 2.

Note Database replication on the subsequent nodes may take enough time to complete after the subsequent node restarts, depending on the size of the cluster.

Tip If replication does not set up properly, use the "utils dbreplication rebuild" CLI command as described in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

What to do next

- (Optional) To view the status of the restore, see Check Restore Job Status, on page 422
- To restart a node, see Restart a Node, on page 421

Restore Node Or Cluster to Last Known Good Configuration

Follow this procedure to restore node or cluster to last known good configuration.

Before you begin

- Ensure that the restore file contains the hostname, IP address, DNS configuration, and deployment type that is configured in the backup file.
- Ensure that the Cisco Unified Communications Manager version installed on the server matches the version of the backup file that you want to restore.
- Ensure this procedure is used only to restore node to a last known good configuration.

Procedure

Step 1 From the Disaster Recovery System, choose **Restore** > **Restore Wizard**.

Step 2 In the **Select Backup Device** area, select the appropriate backup device to restore.

Step 3 Click **Next**.

Step 4 In the **Restore Wizard Step 2** window, select the backup file you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.

Step 6 In the **Restore Wizard Step 3** window, click **Next**.

Step 7 Select the appropriate node, when prompted to choose restore nodes.
Data is restored on the chosen nodes.

Step 8 Restart all nodes in the cluster. Restart the first Cisco Unified Communications Manager node before restarting the subsequent Cisco Unified Communications Manager nodes. If the cluster also has Cisco IM and Presence nodes, restart the first Cisco IM and Presence node before restarting the subsequent IM and Presence nodes. See the What to Do Next section for more information.

Restart a Node

You must restart a node after you restore data.

If you are restoring a publisher node (first node), you must restart the publisher node first. Restart subscriber nodes only after the publisher node has restarted and is successfully running the restored version of the software.

Note Do not restart IM and Presence subscriber nodes if the CUCM publisher node is offline. In such cases, the node services will fail to start because the subscriber node is unable to connect to the CUCM publisher.

Caution This procedure causes the system to restart and become temporarily out of service.

Perform this procedure on every node in the cluster that you need to restart.

Procedure

Step 1 From Cisco Unified OS Administration, select **Settings** > **Version**.

Step 2 To restart the node, click **Restart**.

Step 3 Replication will be setup automatically after cluster reboot. Check the Replication Status value on all nodes by using the **utils dbreplication runtimestate** CLI command. The value on each node should be equal 2. See Cisco Unified Communications (CallManager) Command References for more information about CLI commands.

If replication does not set up properly, use the **utils dbreplication reset** CLI command as described in the *Command Line Reference Guide for Cisco Unified Communications Solutions*.

Note Database replication on the subsequent nodes may take several hours to complete after the subsequent nodes restart, depending on the size of the cluster.

What to do next

(Optional) To view the status of the restore, see Check Restore Job Status, on page 422.

Check Restore Job Status

Follow this procedure to check the restore job status.

Procedure

Step 1 From the Disaster Recovery System, select **Restore** > **Current Status**.

Step 2 In the **Restore Status** window, click the log filename link to view the restore status.

View Restore History

Perform the following steps to view the restore history.

Procedure

Step 1 From Disaster Recovery System, choose **Restore** > **History**.

Step 2 From the **Restore History** window, you can view the restores that you have performed, including filename, backup device, completion date, result, version, features that were restored, and failed features.

The **Restore History** window displays only the last 20 restore jobs.

Data Authentication

Trace Files

The following trace file locations are used during troubleshooting or while collecting the logs.

Trace files for the Master Agent, the GUI, each Local Agent, and the JSch library get written to the following locations:

- For the Master Agent, find the trace file at platform/drf/trace/drfMA0*
- For each Local Agent, find the trace file at platform/drf/trace/drfLA0*
- For the GUI, find the trace file at platform/drf/trace/drfConfLib0*
- For the JSch, find the trace file at platform/drf/trace/drfJSch*

For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Command Line Interface

The Disaster Recovery System also provides command line access to a subset of backup and restore functions, as shown in the following table. For more information on these commands and on using the command line interface, see the *Command Line Interface Reference Guide* for Cisco Unified Communications Solutions at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html.

Table 88: Disaster Recovery System Command Line Interface

Command	Description
utils disaster_recovery estimate_tar_size	Displays estimated size of backup tar from SFTP/Local device and requires one parameter for feature list

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface
utils disaster_recovery jschLogs	Enables or disables JSch library logging
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore
utils disaster_recovery status	Displays the status of ongoing backup or restore job
utils disaster_recovery show_backupfiles	Displays existing backup files
utils disaster_recovery cancel_backup	Cancels an ongoing backup job
utils disaster_recovery show_registration	Displays the currently configured registration
utils disaster_recovery device add	Adds the network device
utils disaster_recovery device delete	Deletes the device
utils disaster_recovery device list	Lists all the devices
utils disaster_recovery schedule add	Adds a schedule
utils disaster_recovery schedule delete	Deletes a schedule
utils disaster_recovery schedule disable	Disables a schedule
utils disaster_recovery schedule enable	Enables a schedule
utils disaster_recovery schedule list	Lists all the schedules
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface.
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and nodes to restore.
utils disaster_recovery status	Displays the status of ongoing backup or restore job.
utils disaster_recovery show_backupfiles	Displays existing backup files.

Command	Description
utils disaster_recovery cancel_backup	Cancels an ongoing backup job.
utils disaster_recovery show_registration	Displays the currently configured registration.

Alarms and Messages

Alarms and Messages

The Disaster Recovery System issues alarms for various errors that could occur during a backup or restore procedure. The following table provides a list of Cisco Disaster Recovery System alarms.

Table 89: Disaster Recovery System Alarms and Messages

Alarm Name	Description	Explanation
DRFBackupDeviceError	DRF backup process has problems accessing device.	DRS backup process encoun while it was accessing devic
DRFBackupFailure	Cisco DRF Backup process failed.	DRS backup process encoun
DRFBackupInProgress	New backup cannot start while another backup is still running	DRS cannot start new backup backup is still running.
DRFInternalProcessFailure	DRF internal process encountered an error.	DRS internal process encoun
DRFLA2MAFailure	DRF Local Agent cannot connect to Master Agent.	DRS Local Agent cannot con Agent.
DRFLocalAgentStartFailure	DRF Local Agent does not start.	DRS Local Agent might be c
DRFMA2LAFailure	DRF Master Agent does not connect to Local Agent.	DRS Master Agent cannot co Agent.
DRFMABackupComponentFailure	DRF cannot back up at least one component.	DRS requested a component data; however, an error occur backup process, and the comp get backed up.
DRFMABackupNodeDisconnect	The node that is being backed up disconnected from the Master Agent prior to being fully backed up.	While the DRS Master Agen a backup operation on a Cisc Communications Manager n disconnected before the back completed.

Alarm Name	Description	Explanation
DRFMARestoreComponentFailure	DRF cannot restore at least one component.	DRS requested a component to r data; however, an error occurred restore process, and the compone get restored.
DRFMARestoreNodeDisconnect	The node that is being restored disconnected from the Master Agent prior to being fully restored.	While the DRS Master Agent wa a restore operation on a Cisco U Communications Manager node, disconnected before the restore c completed.
DRFMasterAgentStartFailure	DRF Master Agent did not start.	DRS Master Agent might be dov
DRFNoRegisteredComponent	No registered components are available, so backup failed.	DRS backup failed because no r components are available.
DRFNoRegisteredFeature	No feature got selected for backup.	No feature got selected for backu
DRFRestoreDeviceError	DRF restore process has problems accessing device.	DRS restore process cannot reac device.
DRFRestoreFailure	DRF restore process failed.	DRS restore process encountere
DRFSftpFailure	DRF SFTP operation has errors.	Errors exist in DRS SFTP opera
DRFSecurityViolation	DRF system detected a malicious pattern that could result in a security violation.	The DRF Network Message con malicious pattern that could resu security violation like code injec directory traversal. DRF Networl has been blocked.
DRFTruststoreMissing	The IPsec truststore is missing on the node.	The IPsec truststore is missing or DRF Local Agent cannot connect Agent.
DRFUnknownClient	DRF Master Agent on the Pub received a Client connection request from an unknown server outside the cluster. The request has been rejected.	The DRF Master Agent on the Pu a Client connection request from unknown server outside the clus request has been rejected.
DRFBackupCompleted	DRF backup completed successfully.	DRF backup completed successf
DRFRestoreCompleted	DRF restore completed successfully.	DRF restore completed successf
DRFNoBackupTaken	DRF did not find a valid backup of the current system.	DRF did not find a valid backup current system after an Upgrade/ or Fresh Install.
DRFComponentRegistered	DRF successfully registered the requested component.	DRF successfully registered the component.
DRFRegistrationFailure	DRF Registration operation failed.	DRF Registration operation faile component due to some internal

Alarm Name	Description	Explanation
DRFComponentDeRegistered	DRF successfully deregistered the requested component.	DRF successfully deregistered component.
DRFDeRegistrationFailure	DRF deregistration request for a component failed.	DRF deregistration request fo failed.
DRFFailure	DRF Backup or Restore process has failed.	DRF Backup or Restore proc encountered errors.
DRFRestoreInternalError	DRF Restore operation has encountered an error. Restore cancelled internally.	DRF Restore operation has e error. Restore cancelled inter
DRFLogDirAccessFailure	DRF could not access the log directory.	DRF could not access the log
DRFDeRegisteredServer	DRF automatically de-registered all the components for the server.	The server may have been di from the Unified Communica cluster.
DRFSchedulerDisabled	DRF Scheduler is disabled because no configured features are available for backup.	DRF Scheduler is disabled b configured features are availa
DRFSchedulerUpdated	DRF Scheduled backup configuration is updated automatically due to feature de-registration.	DRF Scheduled backup conf updated automatically due to de-registration

License Reservation

License Reservation

Important The below license feature table is supported till Unified CM 14SU1 release.

Follow the below steps, after performing the restore operation on the Specific License Reservation enabled Unified Communications Manager.

Table 90: Disaster Recovery System for License Reservation

State after Restore	Product on CSSM	Solution
UNREGISTERED	Yes	Contact Cisco to remove the product from CSSM and do register from the product.
	No	Nothing required

State after Restore	Product on CSSM	Solution
RESERVATION IN PROGRESS	Yes	Do either of the below procedures: Procedure-1: **1.** Get the authorization code for the product from CSSM. **2.** Run the below CLI by giving the authorization code **license smart reservation return-authorization "<authorization-code>"**. Procedure-2: **1.** Contact Cisco to remove the product from CSSM.
	No	Execute the CLI from the product **license smart reservation cancel**.
REGISTERED	Yes	**1.** Execute the below CLI **license smart reservation return** from the product. A reservation return code will be printed on the console. **2.** Enter the reservation return code on CSSM to remove the product.
	No	Execute the CLI from the product **license smart reservation return**.

Restore Interactions and Restrictions

Restore Restrictions

The following restrictions apply to using Disaster Recovery System to restore Cisco Unified Communications Manager or IM and Presence Service

Table 91: Restore Restrictions

Restriction	Description
Export Restricted	You can restore the DRS backup from a restricted version only to a restricted version and the backup from an unrestricted version can be restored only to an unrestricted version. Note that if you upgrade to the U.S. export unrestricted version of Cisco Unified Communications Manager, you will not be able to later upgrade to or be able to perform a fresh install of the U.S. export restricted version of this software

Restriction	Description
Platform Migrations	You cannot use the Disaster Recovery System to migrate data between platforms (for example, from Windows to Linux or from Linux to Windows). A restore must run on the same product version as the backup. For information on data migration from a Windows-based platform to a Linux-based platform, see the *Data Migration Assistant User Guide*.
HW Replacement and Migrations	When you perform a DRS restore to migrate data to a new server, you must assign the new server the identical IP address and hostname that the old server used. Additionally, if DNS was configured when the backup was taken, then the same DNS configuration must be present prior to performing a restore. For more information about replacing a server, refer to the *Replacing a Single Server or Cluster for Cisco Unified Communications Manager guide*. In addition, you must run the Certificate Trust List (CTL) client after a hardware replacement. You must run the CTL client if you do not restore the subsequent node (subscriber) servers. In other cases, DRS backs up the certificates that you need. For more information, see the “Installing the CTL Client” and “Configuring the CTL Client ” procedures in the *Cisco Unified Communications Manager Security Guide*.
Extension Mobility Cross Cluster	Extension Mobility Cross Cluster users who are logged in to a remote cluster at backup shall remain logged in after restore.

Note DRS backup/restore is a high CPU-oriented process. Smart Licence Manager is one of the components that are backed-up and restored. During this process Smart License Manger service is restarted. You can expect high resource utilization so recommended to schedule the process during maintenance period.

After successfully restoring the Cisco Unified Communications server components, register the Cisco Unified Communications Manager with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. If the product is already registered before taking the backup, then reregister the product for updating the license information.

For more information on how to register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite, see the *System Configuration Guide for Cisco Unified Communications Manager* for your release.

Troubleshooting

DRS Restore to Smaller Virtual Machine Fails

Problem

A database restore may fail if you restore an IM and Presence Service node to a VM with smaller disks.

Cause

This failure occurs when you migrate from a larger disk size to a smaller disk size.

Solution

Deploy a VM for the restore from an OVA template that has 2 virtual disks.

PART IX

Troubleshooting

CHAPTER 35

Troubleshooting Overview

This section provides the necessary background information and available resources to troubleshoot the Unified Communications Manager.

Cisco Unified Serviceability

Cisco Unified Serviceability, a web-based troubleshooting tool for Unified Communications Manager, provides the following functionality to assist administrators troubleshoot system problems:

- Saves Unified Communications Manager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Unified Communications Manager services trace information to various log files for troubleshooting. Administrators can configure, collect, and view trace information.
- Monitors real-time behavior of the components in a Unified Communications Manager cluster through the real-time monitoring tool (RTMT).
- Generates reports for Quality of Service, traffic, and billing information through Unified Communications Manager CDR Analysis and Reporting (CAR).
- Provides feature services that you can activate, deactivate, and view through the Service Activation window.
- Provides an interface for starting and stopping feature and network services.
- Archives reports that are associated with Cisco Unified Serviceability tools.
- Allows Unified Communications Manager to work as a managed device for SNMP remote management and troubleshooting.
- Monitors the disk usage of the log partition on a server (or all servers in the cluster).

Access Cisco Unified Serviceability from the Cisco Unified Communications Manager Administration window by choosing Cisco Unified Serviceability from the Navigation drop-down list box. Installing the Unified Communications Manager software automatically installs Cisco Unified Serviceability and makes it available.

See *Cisco Unified Serviceability Administration Guide* for detailed information and configuration procedures on the serviceability tools.

Cisco Unified Communications Operating System Administration

Cisco Unified Communications Operating System Administration allows you to perform the following tasks to configure and manage the *Cisco Unified Communications Operating System*:

- Check software and hardware status.
- Check and update IP addresses.
- Ping other network devices.
- Manage Network Time Protocol servers.
- Upgrade system software and options.
- Restart the system.

Refer to the Administration Guide for Cisco Unified Communications Manager for detailed information and configuration procedures on the serviceability tools.

General Model of Problem Solving

When troubleshooting a telephony or IP network environment, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

The following steps provide guidelines to use in the problem-solving process.

Procedure

1. Analyze the network problem and create a clear problem statement. Define symptoms and potential causes.
2. Gather the facts that you need to help isolate possible causes.
3. Consider possible causes based on the facts that you gathered.
4. Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only one variable.
5. Implement the action plan; perform each step carefully while testing to see whether the symptom disappears.
6. Analyze the results to determine whether the problem has been resolved. If the problem was resolved, consider the process complete.
7. If the problem has not been resolved, create an action plan based on the next most probable cause on your list. Return to 4, on page 434 and repeat the process until the problem is solved.

Make sure that you undo anything that you changed while implementing your action plan. Remember that you want to change only one variable at a time.

Note If you exhaust all the common causes and actions (either those outlined in this document or others that you have identified in your environment), contact Cisco TAC.

Network Failure Preparation

You can always recover more easily from a network failure if you are prepared ahead of time. To determine if you are prepared for a network failure, answer the following questions:

- Do you have an accurate physical and logical map of your internetwork that outlines the physical location of all of the devices on the network and how they are connected as well as a logical map of network addresses, network numbers, and subnetworks?
- Do you have a list of all network protocols that are implemented in your network for each of the protocols implemented and a list of the network numbers, subnetworks, zones, and areas that are associated with them?
- Do you know which protocols are being routed and the correct, up-to-date configuration information for each protocol?
- Do you know which protocols are being bridged? Are any filters configured in any of these bridges, and do you have a copy of these configurations? Is this applicable to Unified Communications Manager?
- Do you know all the points of contact to external networks, including any connections to the Internet? For each external network connection, do you know what routing protocol is being used?
- Has your organization documented normal network behavior and performance, so you can compare current problems with a baseline?

If you can answer yes to these questions, faster recovery from a failure results.

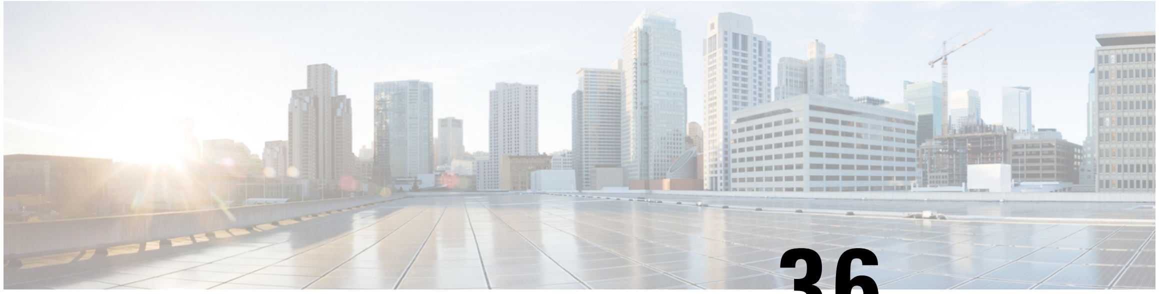
Where to Find More Information

Use the following links for information on various IP telephony topics:

- For further information about related Cisco IP telephony applications and products, see the *Cisco Unified Communications Manager Documentation Guide*. The following URL shows an example of the path to the documentation guide:

  https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html
- For documentation related to Cisco Unity, see the following URL: *https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html*
- For documentation related to Cisco Emergency Responder, see the following URL: *https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html*

- For documentation related to Cisco Unified IP Phone, see the following URL: *https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html*
- For information on designing and troubleshooting IP telephony networks, see the Cisco IP Telephony Solution Reference Network Design Guides that are available at: *https://www.cisco.com/go/srnd*



CHAPTER 36

Troubleshooting Tools

This section addresses the tools and utilities that you use to configure, monitor, and troubleshoot Unified Communications Manager and provides general guidelines for collecting information to avoid repetitive testing and recollection of identical data.

Note To access some of the URL sites that are listed in this document, you must be a registered user, and you must be logged in.

Cisco Unified Serviceability Troubleshooting Tools

Refer to the *Cisco Unified Serviceability Administration Guide* for detailed information of the following different types of tools that Cisco Unified Serviceability provides to monitor and analyze the various Unified Communications Manager systems.

Table 92: Serviceability Tools

Term	Definition
Cisco Unified Real-Time Monitoring Tool (RTMT)	This tool provides real-time information about Unified Communications Manager devices and performance counters and enables you to collect traces. Performance counters can be system-specific or Unified Communications Manager specific. Objects comprise the logical groupings of like counters for a specific device or feature, such as Cisco Unified IP Phones or Unified Communications Manager System Performance. Counters measure various aspects of system performance. Counters measure statistics such as the number of registered phones, calls that are attempted and calls in progress.
Alarms	Administrators use alarms to obtain the run-time status and state of the Unified Communications Manager system. Alarms contain information about system problems such as explanation and recommended action. Administrators search the alarm definitions database for alarm information. The alarm definition contains a description of the alarm and recommended actions.
Trace	Administrators and Cisco engineers use trace files to obtain specific information about Unified Communications Manager service problems. Cisco Unified Serviceability sends configured trace information to the trace log file. Two types of trace log files exist: SDI and SDL. Every service includes a default trace log file. The system traces system diagnostic interface (SDI) information from the services and logs run-time events and traces to a log file. The SDL trace log file contains call-processing information from services such as Cisco CallManager and Cisco CTIManager. The system traces the signal distribution layer (SDL) of the call and logs state transitions into a log file. **Note** In most cases, you will only gather SDL traces when Cisco Technical Assistance Center (TAC) requests you to do so.
Quality Report Tool	This term designates voice quality and general problem-reporting utility in Cisco Unified Serviceability.
Serviceability Connector	The Cisco Webex Serviceability service increases the speed with which Cisco technical assistance staff can diagnose issues with your infrastructure. It automates the tasks of finding, retrieving, and storing diagnostic logs and information into an SR case. The service also triggers analysis against diagnostic signatures so that TAC can more efficiently identify and resolve issues with your on-premises equipment.

Command Line Interface

Use the command line interface (CLI) to access the Unified Communications Manager system for basic maintenance and failure recovery. Obtain access to the system by either a hard-wired terminal (a system monitor and keyboard) or by performing a SSH session.

The account name and password get created at install time. You can change the password after install, but you never can change the account name.

A command represents a text instruction that caused the system to perform some function. Commands may be stand alone, or they can have mandatory or optional arguments or options.

A level comprises a collection of commands; for example, show designates a level, whereas show status specifies a command. Each level and command also includes an associated privilege level. You can execute a command only if you have sufficient privilege level.

For complete information on the Unified Communications Manager CLI command set, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

kerneldump Utility

The kerneldump utility allows you to collect crash dump logs locally on the affected machine without requiring a secondary server.

In a Unified Communications Manager cluster, you only need to ensure the kerneldump utility is enabled on the server before you can collect the crash dump information.

Note Cisco recommends that you verify the kerneldump utility is enabled after you install Unified Communications Manager to allow for more efficient troubleshooting. If you have not already done so, enable the kerneldump utility before you upgrade the Unified Communications Manager from supported appliance releases.

Important Enabling or disabling the kerneldump utility will require a reboot of the node. Do not execute the enable command unless you are within a window where a reboot would be acceptable.

The *command line interface* (CLI) for the *Cisco Unified Communications Operating System* can be used to enable, disable, or check the status of the kerneldump utility.

Use the following procedure to enable the kernel dump utility:

Working with Files That Are Collected by the Utility

To view the crash information from the kerneldump utility, use the *Cisco Unified Real-Time Monitoring Tool* or the *Command Line Interface* (CLI). To collect the kerneldump logs by using the *Cisco Unified Real-Time Monitoring Tool*, choose the Collect Files option from Trace & Log Central. From the Select System Services/Applications tab, choose the Kerneldump logs check box. For more information on collecting files using *Cisco Unified Real-Time Monitoring Tool*, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

To use the CLI to collect the kerneldump logs, use the “file” CLI commands on the files in the crash directory. These are found under the “activelog” partition. The log filenames begin with the IP address of the kerneldump client and end with the date that the file is created. For more information on the file commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Enable the Kerneldump Utility

Use this procedure to enable the kerneldump utility. In the event of a kernel crash, the utility provides a mechanism for collecting and dumping the crash. You can configure the utility to dump logs to the local server or to an external server.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Complete either of the following:

- To dump kernel crashes on the local server, run the `utils os kerneldump enable` CLI command.
- To dump kernel crashes to an external server, run the `utils os kerneldump ssh enable <ip_address>` CLI command with the IP address of the external server.

Step 3 Reboot the server.

Example

Note If you need to disable the kerneldump utility, you can run the `utils os kernelcrash disable` CLI command to disable the local server for core dumps and the `utils os kerneldump ssh disable <ip_address>` CLI command to disable the utility on the external server.

What to do next

Configure an email alert in the Real-Time Monitoring Tool to be advised of core dumps. For details, see Enable Email Alert for Core Dump, on page 266

Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information on the kerneldump utility and troubleshooting.

Enable Email Alert for Core Dump

Use this procedure to configure the Real-Time Monitoring Tool to email the administrator whenever a core dump occurs.

Procedure

Step 1 Select **System** > **Tools** > **Alert** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard prompts to set your preferred criteria:

a) In the **Alert Properties: Email Notification** popup, make sure that **Enable Email** is checked and click **Configure** to set the default alert action, which will be to email an administrator.

b) Follow the prompts and **Add** a Recipient email address. When this alert is triggered, the default action is to email this address.

c) Click **Save**.

Step 4 Set the default Email server:

a) Select **System** > **Tools** > **Alert** > **Config Email Server**.

b) Enter the e-mail server and port information to send email alerts.

c) Enter the **Send User Id**.

d) Click **OK**.

Network Management

Use the network management tools for Unified Communications Manager remote serviceability.

- System Log Management
- Cisco Discovery Protocol Support
- Simple Network Management Protocol support

Refer to the documentation at the URLs provided in the sections for these network management tools for more information.

System Log Management

Although it can be adapted to other network management systems, Cisco Syslog Analysis, which is packaged with Resource Manager Essentials (RME), provides the best method to manage Syslog messages from Cisco devices.

Cisco Syslog Analyzer serves as the component of Cisco Syslog Analysis that provides common storage and analysis of the system log for multiple applications. The other major component, Syslog Analyzer Collector, gathers log messages from Unified Communications Manager servers.

These two Cisco applications work together to provide a centralized system logging service for Cisco Unified Communications Solutions.

Refer to the following URL for RME documentation: *http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml*

Cisco Discovery Protocol Support

The Cisco Discovery Protocol Support enables discovery of Unified Communications Manager servers and management of those servers.

Refer to the following URL for RME documentation: *http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml*

Simple Network Management Protocol Support

Network management systems (NMS) use SNMP, an industry-standard interface, to exchange management information between network devices. A part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network comprises three key components: managed devices, agents, and network management systems.

- A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.
- An agent, as network management software, resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP.
- A network management system comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. The following NMSs share compatibility with Unified Communications Manager:
  - CiscoWorks Common Services Software
  - HP OpenView
  - Third-party applications that support SNMP and Unified Communications Manager SNMP interfaces

Sniffer Traces

Typically, you collect sniffer traces by connecting a laptop or other sniffer-equipped device on a Catalyst port that is configured to span the VLAN or port(s) (CatOS, Cat6K-IOS, XL-IOS) that contains the trouble information. If no free port is available, connect the sniffer-equipped device on a hub that is inserted between the switch and the device.

Tip To help facilitate reading and interpreting of the traces by the TAC engineer, Cisco recommends using Sniffer Pro software because it is widely used within the TAC.

Have available the IP/MAC addresses of all equipment that is involved, such as IP phones, gateways, Unified Communications Managers, and so on.

Debugs

The output from **debug** privileged EXEC commands provides diagnostic information about a variety of internetworking event that relate to protocol status and network activity in general.

Set up your terminal emulator software (such as HyperTerminal), so it can capture the debug output to a file. In HyperTerminal, click **Transfer**; then, click **Capture Text** and choose the appropriate options.

Before running any IOS voice gateway debugs, make sure that **`servicetimestampsdebugdatetimemsec`** is globally configured on the gateway.

Note Avoid collecting debugs in a live environment during operation hours.

Preferably, collect debugs during non-working hours. If you must collect debugs in a live environment, configure `no logging console` and `loggingbuffered`. To collect the debugs, use `show log`.

Because some debugs can be lengthy, collect them directly on the console port (default `logging console`) or on the buffer (`logging buffer`). Collecting debugs over a Telnet session may impact the device performance, and the result could be incomplete debugs, which requires that you re-collect them.

To stop a debug, use the `no debug all` or `undebug all` commands. Verify that the debugs have been turned off by using the command `show debug`.

Cisco Secure Telnet

Cisco Secure Telnet allows Cisco Service Engineers (CSE) transparent firewall access to the Unified Communications Manager node on your site. Using strong encryption, *Cisco Secure Telnet* enables a special Telnet client from Cisco Systems to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and troubleshooting of your Unified Communications Manager nodes, without requiring firewall modifications.

Note Cisco provides this service only with your permission. You must ensure that a network administrator is available at your site to help initiate the process.

Packet Capture

This section contains information about packet capture.

Related Topics

Packet Capturing Overview, on page 443
Configuration Checklist for Packet Capturing, on page 444
Adding an End User to the Standard Packet Sniffer Access Control Group , on page 445
Configuring Packet-Capturing Service Parameters, on page 445
Configuring Packet Capturing in the Phone Configuration Window, on page 446
Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 446
Packet-Capturing Configuration Settings, on page 448
Analyzing Captured Packets, on page 449

Packet Capturing Overview

Because third-party troubleshooting tools that sniff media and TCP packets do not work after you enable encryption, you must use Unified Communications Manager to perform the following tasks if a problem occurs:

- Analyze packets for messages that are exchanged between Unified Communications Manager and the device [Cisco Unified IP Phone (SIP and SCCP), Cisco IOS MGCP gateway, H.323 gateway, H.323/H.245/H.225 trunk, or SIP trunk].
- Capture the Secure Real Time Protocol (SRTP) packets between the devices.
- Extract the media encryption key material from messages and decrypt the media between the devices.

Tip Performing this task for several devices at the same time may cause high CPU usage and call-processing interruptions. Cisco strongly recommends that you perform this task when you can minimize call-processing interruptions.

For more information, see the Security Guide for Cisco Unified Communications Manager.

Configuration Checklist for Packet Capturing

Extracting and analyzing pertinent data includes performing the following tasks.

Procedure

1. Add end users to the Standard Packet Sniffer Users group.
2. Configure packet capturing service parameters in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration; for example, configure the Packet Capture Enable service parameter.
3. Configure packet capturing settings on a per-device basis in the Phone or Gateway or Trunk Configuration window.

   Note Cisco strongly recommends that you do not enable packet capturing for many devices at the same time because this task may cause high CPU usage in your network.

4. Capture SRTP packets by using a sniffer trace between the affected devices. Refer to the documentation that supports your sniffer trace tool.
5. After you capture the packets, set the Packet Capture Enable service parameter to False.
6. Gather the files that you need to analyze the packets.
7. Cisco Technical Assistance Center (TAC) analyzes the packets. Contact TAC directly to perform this task.

Related Topics

Adding an End User to the Standard Packet Sniffer Access Control Group , on page 445
Analyzing Captured Packets, on page 449
Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 446
Configuring Packet Capturing in the Phone Configuration Window, on page 446
Configuring Packet-Capturing Service Parameters, on page 445
Packet-Capturing Configuration Settings, on page 448

Adding an End User to the Standard Packet Sniffer Access Control Group

End users that belong to the Standard Packet Sniffer Users group can configure the Packet Capture Mode and Packet Capture Duration settings for devices that support packet capturing. If the user does not exist in the Standard Packet Sniffer Access Control Group, the user cannot initiate packet capturing.

The following procedure, which describes how to add an end user to the Standard Packet Sniffer Access Control Group, assumes that you configured the end user in Cisco Unified Communications Manager Administration, as described in the Administration Guide for Cisco Unified Communications Manager.

Procedure

1. Find the access control group, as described in the Administration Guide for Cisco Unified Communications Manager.
2. After the Find/List window displays, click the **Standard Packet Sniffer Users** link.
3. Click the **Add Users to Group** button.
4. Add the end user, as described in the Administration Guide for Cisco Unified Communications Manager.
5. After you add the user, click **Save**.

Configuring Packet-Capturing Service Parameters

To configure parameters for packet capturing, perform the following procedure:

Procedure

1. In Unified Communications Manager, choose **System** > **Service Parameters**.
2. From the Server drop-down list box, choose an Active server where you activated the Cisco CallManager service.
3. From the Service drop-down list box, choose the **Cisco CallManager (Active)** service.
4. Scroll to the TLS Packet Capturing Configuration pane and configure the packet capturing settings.

Tip For information on the service parameters, click the name of the parameter or the question mark that displays in the window.

Note For packet capturing to occur, you must set the Packet Capture Enable service parameter to True.

5. For the changes to take effect, click **Save**.
6. You can continue to configure packet-capturing.

Related Topics

Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 446

Configuring Packet Capturing in the Phone Configuration Window, on page 446

Configuring Packet Capturing in the Phone Configuration Window

After you enable packet capturing in the Service Parameter window, you can configure packet capturing on a per-device basis in the Phone Configuration window of Cisco Unified Communications Manager Administration.

You enable or disable packet capturing on a per-phone basis. The default setting for packet capturing equals None.

Caution Cisco strongly recommends that you do not enable packet capturing for many phones at the same time because this task may cause high CPU usage in your network.

If you do not want to capture packets or if you completed the task, set the Packet Capture Enable service parameter to False.

To configure packet capturing for phones, perform the following procedure:

Procedure

1. Before you configure the packet-capturing settings, see the topics related to packet capturing configuration.
2. Find the SIP or SCCP phone, as described in the System Configuration Guide for Cisco Unified Communications Manager.
3. After the Phone Configuration window displays, configure the troubleshooting settings, as described in Packet-Capturing Configuration Settings.
4. After you complete the configuration, click **Save**.
5. In the Reset dialog box, click **OK**.

Tip Although Cisco Unified Communications Manager Administration prompts you to reset the device, you do not need to reset the device to capture packets.

Additional Steps

Capture SRTP packets by using a sniffer trace between the affected devices.

After you capture the packets, set the Packet Capture Enable service parameter to False.

Related Topics

Analyzing Captured Packets, on page 449
Configuration Checklist for Packet Capturing, on page 444

Configuring Packet Capturing in Gateway and Trunk Configuration Windows

The following gateways and trunks support packet capturing in Unified Communications Manager.

- Cisco IOS MGCP gateways
- H.323 gateways

- H.323/H.245/H.225 trunks
- SIP trunks

Tip Cisco strongly recommends that you do not enable packet capturing for many devices at the same time because this task may cause high CPU usage in your network.

If you do not want to capture packets or if you completed the task, set the Packet Capture Enable service parameter to False.

To configure packet-capturing settings in the Gateway or Trunk Configuration window, perform the following procedure:

Procedure

1. Before you configure the packet-capturing settings, see the topics related to packet capturing configuration.
2. Perform one of the following tasks:
   - Find the Cisco IOS MGCP gateway, as described in the System Configuration Guide for Cisco Unified Communications Manager.
   - Find the H.323 gateway, as described in the System Configuration Guide for Cisco Unified Communications Manager.
   - Find the H.323/H.245/H.225 trunk, as described in the System Configuration Guide for Cisco Unified Communications Manager.
   - Find the SIP trunk, as described in the System Configuration Guide for Cisco Unified Communications Manager.
3. After the configuration window displays, locate the Packet Capture Mode and Packet Capture Duration settings.

   Tip If you located a Cisco IOS MGCP gateway, ensure that you configured the ports for the Cisco IOS MGCP gateway, as described in the Administration Guide for Cisco Unified Communications Manager. The packet-capturing settings for the Cisco IOS MGCP gateway display in the Gateway Configuration window for endpoint identifiers. To access this window, click the endpoint identifier for the voice interface card.
4. Configure the troubleshooting settings, as described in Packet-Capturing Configuration Settings.
5. After you configure the packet-capturing settings, click **Save**.
6. In the Reset dialog box, click **OK**.

   Tip Although Cisco Unified Communications Manager Administration prompts you to reset the device, you do not need to reset the device to capture packets.

Additional Steps

Capture SRTP packets by using a sniffer trace between the affected devices.

After you capture the packets, set the Packet Capture Enable service parameter to False.

Related Topics

- Analyzing Captured Packets, on page 449
- Configuration Checklist for Packet Capturing, on page 444

Packet-Capturing Configuration Settings

The following table describes the Packet Capture Mode and Packet Capture Duration settings when configuring packet capturing for gateways, trunks, and phones.

Setting	Description
Packet Capture Mode	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box: • **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, Unified Communications Manager sets the Packet Capture Mode to None. • **Batch Processing Mode**— Unified Communications Manager writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Unified Communications Manager, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Unified Communications Manager stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message. The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file. **Tip** Before you contact TAC, you must capture the SRTP packets by using a sniffer trace between the affected devices.
Packet Capture Duration	This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes. To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

Related Topics

Configuring Packet Capturing in Gateway and Trunk Configuration Windows, on page 446
Configuring Packet Capturing in the Phone Configuration Window, on page 446

Analyzing Captured Packets

Cisco Technical Assistance Center (TAC) analyzes the packets by using a debugging tool. Before you contact TAC, capture SRTP packets by using a sniffer trace between the affected devices. Contact TAC directly after you gather the following information:

- Packet Capture File—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**, where you browse into the server and locate the packet-capture file by month, date, and year (mm-dd-yyyy)
- Key for the file—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**, where you browse into the server and locate the key by month, date, and year (mm-dd-yyyy)
- User name and password of end user that belongs to the Standard Packet Sniffer Users group

For more information, see Security Guide for Cisco Unified Communications Manager.

Common Troubleshooting Tasks, Tools, and Commands

This section provides a quick reference for commands and utilities to help you troubleshoot a Unified Communications Manager server with root access disabled. The following table provides a summary of the CLI commands and GUI selections that you can use to gather information troubleshoot various system problems.

Table 93: Summary of CLI Commands and GUI Selections

Information	Linux Command	Serviceability GUI Tool	CLI commands
CPU usage	top	RTMT Go to View tab and select **Server** > **CPU and Memory**	Processor CPU usage: show perf query class Processor Process CPU Usage for all processes: show perf query counter Process “% CPU Time” Individual process counter details (including CPU usage) show perf query instance <Process task_name>
Process state	ps	RTMT Go to View tab and select **Server** > **Process**	show perf query counter Process “Process Status”
Disk usage	df/du	RTMT Go to View tab and select **Server** > **Disk Usage**	show perf query counter Partition“% Used” or show perf query class Partition

Information	Linux Command	Serviceability GUI Tool	CLI commands
Memory	free	RTMT Go to View tab and select **Server** > **CPU and Memory**	show perf query class Memory
Network status	netstats		show network status
Reboot server	reboot	Log in to Platform Web page on the server Go to **Server** > **Current Version**	utils system restart
Collect Traces/logs	Sftp, ftp	RTMT Go to Tools tab and select **Trace** > **Trace & Log Central**	List file: file list Download files: file get View a file: file view

The following table provides a list of common problems and tools to use to troubleshoot them.

Table 94: Troubleshooting Common Problems with CLI Commands and GUI Selections

Task	GUI Tool	CLI commands
Accessing the database	none	Log in as admin and use any of the following **show** commands: • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* To run a SQL command, use the **run** command: • run sql <sql command>
Freeing up disk space **Note** You can only delete files from the Log partition.	Using the RTMT client application, go to the **Tools** tab and select **Trace & Log Central** > **Collect Files**. Choose the criteria to select the files you want to collect, then check the option **Delete Files**. This will delete the files on the Unified Communications Manager server after downloading the files to your PC.	file delete
Viewing core files	You cannot view the core files; however, you can download the Core files by using the RTMT application and selecting **Trace & Log Central** > **Collect Crash Dump**.	utils core [options.]

Task	GUI Tool	CLI commands
Rebooting the Unified Communications Manager server	Log in to Platform on the server and go to **Restart** > **Current Version**.	utils system restart
Changing debug levels for traces	Log in to *Cisco Unity Connection Serviceability* Administration at `https://<server_ipaddress>:8443/ccmservice/` and choose **Trace** > **Configuration**.	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
Looking at netstats	none	show network status

Troubleshooting Tips

The following tips may help you when you are troubleshooting the Unified Communications Manager.

Tip Check the release notes for Unified Communications Manager for known problems. The release notes provide descriptions and workaround solutions for known problems.

Tip Know where your devices are registered.

Each Unified Communications Manager log traces files locally. If a phone or gateway is registered to a particular Unified Communications Manager, the call processing gets done on that Unified Communications Manager if the call is initiated there. You will need to capture traces on that Unified Communications Manager to debug a problem.

A common mistake involves having devices that are registered on a subscriber server but are capturing traces on the publisher server. These trace files will be nearly empty (and definitely will not have the call in them).

Another common problem involves having Device 1 registered to CM1 and Device 2 registered to CM2. If Device 1 calls Device 2, the call trace occurs in CM1, and, if Device 2 calls Device 1, the trace occurs in CM2. If you are troubleshooting a two-way calling issue, you need both traces from both Unified Communications Managers to obtain all the information that is needed to troubleshoot.

Tip Know the approximate time of the problem.

Multiple calls may have occurred, so knowing the approximate time of the call helps TAC quickly locate the trouble.

You can obtain phone statistics on a Cisco Unified IP Phone 79xx by pressing the **i** or**?** button twice during an active call.

When you are running a test to reproduce the issue and produce information, know the following data that is crucial to understanding the issue:

- Calling number/called number
- Any other number that is involved in the specific scenario
- Time of the call

Note Remember that time synchronization of all equipment is important for troubleshooting.

If you are reproducing a problem, make sure to choose the file for the timeframe by looking at the modification date and the time stamps in the file. The best way to collect the right trace means that you reproduce a problem and then quickly locate the most recent file and copy it from the Unified Communications Manager server.

Tip Save the log files to prevent them from being overwritten.

Files will get overwritten after some time. The only way to know which file is being logged to is to choose **View** > **Refresh** on the menu bar and look at the dates and times on the files.

System History Log

This system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, and DRS backups and DRS restores, as well as switch version and reboot history.

Related Topics

System History Log Overview, on page 453
System History Log Fields, on page 454
Accessing the System History Log, on page 455

System History Log Overview

The system history log exists as a simple ASCII file, **system-history.log**, and the data does not get maintained in the database. Because it does not get excessively large, the system history file does not get rotated.

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success, failure, or cancellation of every software upgrade (Cisco option files and patches).
- Logs every DRS backup and restore that is performed.
- Logs every invocation of Switch Version that is issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown that is issued through either the CLI or the GUI.
- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot is the result of a manual reboot, power cycle, or kernel panic.

- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. You can access the log from the CLI by using the **file** commands or from the Real Time Monitoring Tool (RTMT).

System History Log Fields

The log displays a common header that contains information about the product name, product version, and kernel image; for example:

```
=======================================
Product Name - Unified Communications Manager
Product Version - 7.1.0.39000-9023
Kernel Image - 2.6.9-67.EL
=======================================
```

Each system history log entry contains the following fields:

timestamp userid action description start/result

The system history log fields can contain the following values:

- *timestamp*—Displays the local time and date on the server with the format *mm/dd/yyyy hh:mm:ss*.
- *userid*—Displays the user name of the user who invokes the action.
- *action*—Displays one of the following actions:
  - Install
  - Windows Upgrade
  - Upgrade During Install
  - Upgrade
  - Cisco Option Install
  - Switch Version
  - System Restart
  - Shutdown
  - Boot
  - DRS Backup
  - DRS Restore
- *description*—Displays one of the following messages:
  - *Version*: Displays for the Basic Install, Windows Upgrade, Upgrade During Install, and Upgrade actions.
  - *Cisco Option file name*: Displays for the Cisco Option Install action.

- *Timestamp*: Displays for the DRS Backup and DRS Restore actions.
- *Active version to inactive version*: Displays for the Switch Version action.
- *Active version*: Displays for the System Restart, Shutdown, and Boot actions.

- *result*—Displays the following results:
  - Start
  - Success or Failure
  - Cancel

The following shows a sample of the system history log.

```
admin:file dump install system-history.log=======================================
Product Name -    Cisco Unified Communications Manager
Product Version - 6.1.2.9901-117
Kernel Image -    2.4.21-47.EL.cs.3BOOT
=======================================
07/25/2008 14:20:06 | root: Install 6.1.2.9901-117 Start
07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start
07/30/2008 10:08:56 | root: Upgrade 6.1.2.9901-126 Start
07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126 Success
07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Start

07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Success

07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start
08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126 Start
```

Accessing the System History Log

You can use either the CLI or RTMT to access the system history log.

Using the CLI

You can access the system history log by using the CLI **file** command; for example:

- **file view install system-history.log**
- **file get install system-history.log**

For more information on the CLI **file** commands, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Using RTMT

You can also access the system history log by using RTMT. From the Trace and Log Central tab, choose **Collect Install Logs**.

For more information about using RTMT, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Audit Logging

Centralized audit logging ensures that configuration changes to the Unified Communications Manager system gets logged in separate log files for auditing. An audit event represents any event that is required to be logged. The following Unified Communications Manager components generate audit events:

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Unified Real-Time Monitoring Tool*
- *Cisco Unified Communications Operating System*
- *Disaster Recovery System*
- Database
- Command Line Interface
- Remote Support Account Enabled (CLI commands issued by technical supports teams)

In *Cisco Business Edition 5000*, the following Cisco Unity Connection components also generate audit events:

- Cisco Unity Connection Administration
- *Cisco Personal Communications Assistant* (Cisco PCA)
- Cisco Unity Connection Serviceability
- Cisco Unity Connection clients that use the Representational State Transfer (REST) APIs

The following example displays a sample audit event:

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful
 Description: Call Manager Service status is stopped App ID:Cisco Tomcat Cluster
 ID:StandAloneCluster Node ID:sa-cm1-3
```

Audit logs, which contain information about audit events, get written in the common partition. The Log Partition Monitor (LPM) manages the purging of these audit logs as needed, similar to trace files. By default, the LPM purges the audit logs, but the audit user can change this setting from the Audit User Configuration window in Cisco Unified Serviceability. The LPM sends an alert whenever the common partition disk usage exceeds the threshold; however, the alert does not have the information about whether the disk is full because of audit logs or trace files.

Tip The Cisco Audit Event Service, which is a network service that supports audit logging, displays in Control Center—Network Services in Cisco Unified Serviceability. If audit logs do not get written, then stop and start this service by choosing **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.

All audit logs get collected, viewed and deleted from Trace and Log Central in the *Cisco Unified Real-Time Monitoring Tool*. Access the audit logs in RTMT in Trace and Log Central. Go to **System** > **Real-Time Trace** > **Audit Logs** > **Nodes**. After you select the node, another window displays **System** > **Cisco Audit Logs**.

The following types of audit logs display in RTMT:

- Application log
- Database log
- Operating system log
- Remote SupportAccEnabled log

Application Log

The application audit log, which displays in the AuditApp folder in RTMT, provides configuration changes for Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, the *CLI*, *Cisco Unified Real-Time Monitoring Tool* (RTMT), *Disaster Recovery System*, and Cisco Unified CDR Analysis and Reporting (CAR). For *Cisco Business Edition 5000*, the application audit log also logs changes for Cisco Unity Connection Administration, *Cisco Personal Communications Assistant* (Cisco PCA), Cisco Unity Connection Serviceability, and clients that use the Representational State Transfer (REST) APIs.

Although the Application Log stays enabled by default, you can configure it in Cisco Unified Serviceability by choosing **Tools** > **Audit Log Configuration**. For a description of the settings that you can configure for audit log configuration, see *Cisco Unified Serviceability Administration Guide*.

If the audit logs get disabled in Cisco Unified Serviceability, no new audit log files get created.

Tip Only a user with an audit role has permission to change the Audit Log settings. By default, the CCMAdministrator has the audit role after fresh installs and upgrades. The CCMAdministrator can assign the “standard audit users” group to a new user that the CCMAdministrator specifically creates for audit purposes. The CCMAdministrator can then be removed from the audit user group. The “standard audit log configuration” role provides the ability to delete audit logs, read/update access to *Cisco Unified Real-Time Monitoring Tool*, Trace Collection Tool, RTMT Alert Configuration, the Control Center - Network Services window, RTMT Profile Saving, the Audit Configuration window, and a new resource called Audit Traces. For Cisco Unity Connection in *Cisco Business Edition 5000*, the application administration account that was created during installation has the Audit Administrator role and can assign other administrative users to the role.

Unified Communications Manager creates one application audit log file until the configured maximum file size is reached; then, it closes and creates a new application audit log file. If the system specifies rotating the log files, Unified Communications Manager saves the configured number of files. Some of the logging events can be viewed by using RTMT SyslogViewer.

The following events get logged for Cisco Unified Communications Manager Administration:

- User logging (user logins and user logouts).
- User role membership updates (user added, user deleted, user role updated).
- Role updates (new roles added, deleted, or updated).
- Device updates (phones and gateways).
- Server configuration updates (changes to alarm or trace configurations, service parameters, enterprise parameters, IP addresses, host names, Ethernet settings, and Unified Communications Manager server additions or deletions).

The following events get logged for Cisco Unified Serviceability:

- Activation, deactivation, start, or stop of a service from any Serviceability window.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR Management.
- Review of any report in the Serviceability Reports Archive. View this log on the reporter node.

RTMT logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

The following events get logged for *Unified Communications Manager CDR Analysis and Reporting*:

- Scheduling the CDR Loader.
- Scheduling the daily, weekly, and monthly user reports, system reports, and device reports.
- Mail parameters configurations.
- Dial plan configurations.
- Gateway configurations.
- System preferences configurations.
- Autopurge configurations.

- Rating engine configurations for duration, time of day, and voice quality.
- QoS configurations.
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configurations.

The following events gets logged for *Disaster Recovery System*:

- Backup initiated successfully/failed
- Restore initiated successfully/failed
- Backup cancelled successfully
- Backup completed successfully/failed
- Restore completed successfully/failed
- Save/update/delete/enable/disable of backup schedule
- Save/update/delete of destination device for backup

For *Cisco Business Edition 5000*, Cisco Unity Connection Administration logs the following events:

- User logging (user logins and user logouts).
- All configuration changes, including but not limited to users, contacts, call management objects, networking, system settings, and telephony.
- Task management (enabling or disabling a task).
- Bulk Administration Tool (bulk creates, bulk deletes).
- Custom Keypad Map (map updates)

For *Cisco Business Edition 5000*, Cisco PCA logs the following events:

- User logging (user logins and user logouts).
- All configuration changes made via the Messaging Assistant.

For *Cisco Business Edition 5000*, Cisco Unity Connection Serviceability logs the following events:

- User logging (user logins and user logouts).
- All configuration changes.
- Activating, deactivating, starting or stopping services.

For *Cisco Business Edition 5000*, clients that use the REST APIs log the following events:

- User logging (user API authentication).
- API calls that utilize Cisco Unity Connection Provisioning Interface (CUPI).

Database Log

The database audit log, which displays in the informix folder in RTMT, reports database changes. This log, which is not enabled by default, gets configured in Cisco Unified Serviceability by choosing **Tools** > **Audit Log Configuration**. For a description of the settings that you can configure for audit log configuration, see Cisco Unified Serviceability.

This audit differs from the Application audit because it logs database changes, and the Application audit logs application configuration changes. The informix folder does not display in RTMT unless database auditing is enabled in Cisco Unified Serviceability.

Operating System Log

The operating system audit log, which displays in the vos folder in RTMT, reports events that are triggered by the operating system. It does not get enabled by default. The **utils auditd** CLI command enables, disables, or gives status about the events.

The vos folder does not display in RTMT unless the audit is enabled in the CLI.

For information on the CLI, see *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Remote Support Acct Enabled Log

The Remote Support Acct Enabled audit log, which displays in the vos folder in RTMT, reports CLI commands that get issued by technical support teams. You cannot configure it, and the log gets created only if the Remote Support Acct gets enabled by the technical support team.

Verify Cisco Unified Communications Manager Services Are Running

Use the following procedure to verify which Cisco CallManager services are active on a server.

Procedure

1. From Cisco Unified Communications Manager Administration, choose **Navigation** > **Cisco Unified Serviceability**.
2. Choose **Tools** > **Service Activation**.
3. From the Servers column, choose the desired server.

   The server that you choose displays next to the Current Server title, and a series of boxes with configured services displays.

   Activation Status column displays either Activated or Deactivated in the Cisco CallManager line.

   If the **Activated** status displays, the specified Cisco CallManager service remains active on the chosen server.

   If the **Deactivated** status displays, continue with the following steps.
4. Check the check box for the desired Cisco CallManager service.
5. Click the **Update** button.

The Activation Status column displays **Activated** in the specified Cisco CallManager service line.

The specified service now shows active for the chosen server.

Perform the following procedure if the Cisco CallManager service has been in activated and you want to verify if the service is currently running.

Procedure

1. From Cisco Unified Communications Manager Administration, choose **Navigation** > **Cisco Unified Serviceability**.

   The Cisco Unified Serviceability window displays.

2. Choose **Tools** > **Control Center – Feature Services**.

3. From the Servers column, choose the server.

   The server that you chose displays next to the Current Server title, and a box with configured services displays.

   The Status column displays which services are running for the chosen server.

CHAPTER 37

Opening a Case With TAC

This section contains details on the type of information that you need when you contact TAC and information on methods of sharing information with TAC personnel.

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website remains available 24 hours a day, 365 days a year at this URL: *http://www.cisco.com/techsupport*

Using the online TAC Service Request Tool represents the fastest way to open S3 and S4 service requests. (S3 and S4 service requests specify those requests in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved by using the recommended resources, your service request will get assigned to a Cisco TAC engineer. Find the TAC Service Request Tool at this URL: *http://www.cisco.com/techsupport/servicerequest*

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL: *http://www.cisco.com/techsupport/contacts*

Information You Will Need

When you open a case with the Cisco TAC, you must provide preliminary information to better identify and qualify the issue. You may need to provide additional information, depending on the nature of the issue. Waiting to collect the following information until you have an engineer request after opening a case inevitably results in resolution delay.

Related Topics

Cisco Live!, on page 467
Cisco Secure Telnet, on page 468
General Information, on page 465
Network Layout, on page 464
Online Cases, on page 466
Problem Description, on page 465
Remote Access, on page 467
Required Preliminary Information, on page 464

Required Preliminary Information

For all issues, always provide the following information to TAC. Collect and save this information for use upon opening a TAC case and update it regularly with any changes.

Related Topics

General Information, on page 465
Network Layout, on page 464
Problem Description, on page 465

Network Layout

Provide a detailed description of the physical and logical setup, as well as all the following network elements that are involved in the voice network (if applicable):

- Unified Communications Manager(s)
    - Version (from Unified Communications Manager Administration, choose **Details**)
    - Number of Unified Communications Managers
    - Setup (stand alone, cluster)
        - Unity
    - Version (from Unified Communications Manager Administration)
    - Integration type
        - Applications
    - List of installed applications

- Version numbers of each application
    - IP/voice gateways
- OS version
- Show tech (IOS gateway)
- Unified Communications Manager load (Skinny gateway)
    - Switch
- OS version
- VLAN configuration
    - Dial plan—Numbering scheme, call routing

Ideally, submit a Visio or other detailed diagram, such as JPG. Using the whiteboard, you may also provide the diagram through a Cisco Live! session.

Problem Description

Provide step-by-step detail of actions that the user performed when the issue occurs. Ensure the detailed information includes

- Expected behavior
- Detailed observed behavior

General Information

Make sure that the following information is readily available:

- Is this a new installation?
- If this is a previous version of a Unified Communications Manager installation, has this issue occurred since the beginning? (If not, what changes were recently made to the system?)
- Is the issue reproducible?
    - If reproducible, is it under normal or special circumstances?
    - If not reproducible, is there anything special about when it does occur?
    - What is the frequency of occurrence?
- What are the affected devices?
    - If specific devices are affected (not random), what do they have in common?
    - Include DNs or IP addresses (if gateways) for all devices that are involved in the problem.
- What devices are on the Call-Path (if applicable)?

Online Cases

Opening a case online through Cisco.com gives it initial priority over all other case-opening methods. High-priority cases (P1 and P2) provide an exception to this rule.

Provide an accurate problem description when you open a case. That description of the problem returns URL links that may provide you with an immediate solution.

If you do not find a solution to your problem, continue the process of sending your case to a TAC engineer.

Serviceability Connector

Serviceability Connector Overview

You can ease the collection of logs with the Webex Serviceability service. The service automates the tasks of finding, retrieving, and storing diagnostic logs and information.

This capability uses the *Serviceability Connector* deployed on your premises. Serviceability Connector runs on a dedicated host in your network ('connector host'). You can install the connector on either of these components:

- Enterprise Compute Platform (ECP)—Recommended

  ECP uses Docker containers to isolate, secure, and manage its services. The host and the Serviceability Connector application install from the cloud. You don’t need to manually upgrade them to stay current and secure.

Important We recommend use of ECP. Our future development will focus on this platform. Some new features won't be available if you install the Serviceability Connector on an Expressway.

- Cisco Expressway

You can use the Servicability Connector for these purposes:

- Automated log and system information retrieval for service requests
- Log collection of your Unified CM clusters in a Cloud-Connected UC deployment

You can use the same Serviceability Connector for both use cases.

Benefits of Using Serviceability Service

The service offers these benefits:

- Speeds up the collection of logs. TAC engineers can retrieve relevant logs as they perform the diagnosis of the problem. They can avoid the delays of requesting extra logs and waiting for their manual collection and delivery. This automation can take days off your problem resolution time.

- Works with TAC’s Collaboration Solution Analyser and its database of diagnostic signatures. The system automatically analyses logs, identifies known issues, and recommends known fixes or workarounds.

TAC Support for Serviceability Connector

For more details on Serviceability Connector, see https://www.cisco.com/go/serviceability or contact your TAC representative.

Cisco Live!

Cisco Live!, a secure, encrypted Java applet, allows you and your Cisco TAC engineer to work together more effectively by using Collaborative Web Browsing / URL sharing, whiteboard, Telnet, and clipboard tools.

Access Cisco Live! at the following URL:

```
http://c3.cisco.com/
```

Remote Access

Remote access provides you with the ability to establish Terminal Services (remote port 3389), HTTP (remote port 80), and Telnet (remote port 23) sessions to all the necessary equipment.

Caution When you are setting up dial-in, do not use **login:cisco** or **password:cisco** because they constitute a vulnerability to the system.

You may resolve many issues very quickly by allowing the TAC engineer remote access to the devices through one of the following methods:

- Equipment with public IP address.
- Dial-in access—In decreasing order of preference: analog modem, Integrated Services Digital Network (ISDN) modem, virtual private network (VPN).
- Network Address Translation (NAT)—IOS and private Internet exchange (PIX) to allow access to equipment with private IP addresses.

Ensure that firewalls do not obstruct IOS traffic and PIX traffic during engineer intervention and that all necessary services, such as Terminal Services, start on the servers.

Note TAC handles all access information with the utmost discretion, and no changes will get made to the system without customer consent.

Cisco Secure Telnet

Cisco Secure Telnet offers Cisco Service Engineers (CSE) transparent firewall access to Unified Communications Manager servers on your site.

Cisco Secure Telnet works by enabling a Telnet client inside the Cisco Systems firewall to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and maintenance of your Unified Communications Manager servers without requiring firewall modifications.

Note Cisco accesses your network only with your permission. You must provide a network administrator at your site to help initiate the process.

Firewall Protection

Virtually all internal networks use firewall applications to restrict outside access to internal host systems. These applications protect your network by restricting IP connections between the network and the public Internet.

Firewalls work by automatically blocking TCP/IP connections that are initiated from the outside, unless the software is reconfigured to allow such access.

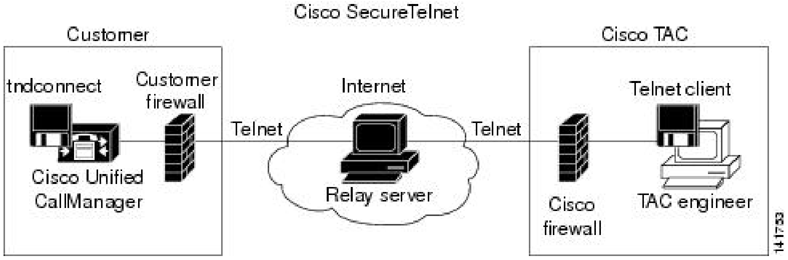
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

Cisco Secure Telnet Design

Cisco Secure Telnet takes advantage of the fact that Telnet connections can easily be initiated from behind a firewall. Using an external proxy machine, the system relays TCP/IP communications from behind your firewall to a host behind another firewall at the *Cisco Technical Assistance Center* (TAC).

Using this relay server maintains the integrity of both firewalls while secure communication between the shielded remote systems get supported.

Figure 26: Cisco Secure Telnet System



Cisco Secure Telnet Structure

The external relay server establishes the connection between your network and Cisco Systems by building a Telnet tunnel. This enables you to transmit the IP address and password identifier of your Unified Communications Manager server to your CSE.

Note The password comprises a text string upon which your administrator and the CSE mutually agree.

Your administrator starts the process by initiating the Telnet tunnel, which establishes a TCP connection from inside your firewall out to the relay server on the public Internet. The Telnet tunnel then establishes another connection to your local Telnet server, creating a two-way link between the entities.

Note The Telnet client at the Cisco TAC runs in compliance with systems that run on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco Communications Manager at your site accepts the password, the Telnet client that is running at the Cisco TAC connects to the Telnet daemon that is running behind your firewall. The resulting transparent connection allows the same access as if the machine were being used locally.

After the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Unified Communications Manager server.

You can view the commands that the CSE sends and the responses that your Unified Communications Manager server issues, but the commands and responses may not always be completely formatted.

Set up a Remote Account

Configure a remote account in the Unified Communications Manager so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Remote Support**.

Step 2 In the **Account Name** field, enter a name for the remote account.

Step 3 In the **Account Duration** field, enter the account duration in days.

Step 4 Click **Save**.
The system generates an encrypted pass phrase.

Step 5 Contact Cisco support to provide them with the remote support account name and pass phrase.