# Cisco Hosted Collaboration Mediation Fulfillment Maintain and Operate Guide, Release 10.6(1)

**First Published:** June 30, 2015

**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

# CONTENTS

# Preface



## Purpose

This document provides instructions for maintaining and operating Cisco Hosted Collaboration Mediation Fulfillment in Cisco Hosted Collaboration Solution (HCS).

## Audience

This document provides information for service providers who are responsible for maintaining and operating Cisco Hosted Collaboration Mediation Fulfillment in Cisco HCS. This guide requires knowledge of Cisco HCS. This guide includes information on routine maintenance for Cisco Hosted Collaboration Mediation Fulfillment and provides descriptions and procedural tasks that you complete by using the Cisco Hosted Collaboration Mediation Fulfillment administrative interface.

## Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |

| Convention | Description |
|---|---|
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier font` | Terminal sessions and information the system displays appear in `courier` font. |
| **`Bold Courier`** font | **`Bold Courier`** font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |
| ... | An ellipsis (three consecutive non-bolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Non-printing characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

# Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

CHAPTER 1

# Maintenance Overview



## Administrative Interface

The Cisco Hosted Collaboration Mediation Fulfillment administrative interface includes the following administrative interfaces:

**Service Inventory**

Cisco Hosted Collaboration Mediation Fulfillment supports Service Inventory, an application that periodically queries the Cisco Unified Communications Domain Manager server and reports the current operating state of the underlying Unified Communications applications. In addition, Service Inventory can generate reports directly from Cisco Unified Communications Manager and Cisco Unity Connection application servers for customers that are provisioned in Cisco Hosted Collaboration Mediation Fulfillment that do not have a Unified Communications Domain Manager configured. The data provides information about customers, subscribers, devices, and other details that are currently provisioned for Cisco HCS through Unified Communications Domain Manager or the appropriate UC application. The service provider uses this data to generate billing records for end customers as part of regular business processes. Service Inventory also can report on the overall state of the system.

The Service Inventory administrative interface allows you to schedule, configure, and generate Service Inventory billing reports, which use a Cisco common format. The generated reports are backed up for a configured amount of time, which is 60 days by default. Service Inventory automatically transfers the report files at regular intervals to the remote SFTP servers that you configure in the Service Inventory administrative interface. If report generation fails, Service Inventory sends you an email failure notification if you provide an email address.

Service Inventory provides both Scheduled and On Demand reports. Scheduled reports are run daily at a chosen time, configured in the Service Inventory administrative interface. On Demand reporting consists of Inventory and Location reports, that can be run at any time to allow the administrator to generate reports without having to alter the reporting schedule. The Inventory report is equivalent to a scheduled Service Inventory report. Location Summary reports generate a report to indicate the number of devices and subscribers per location. For On Demand Service Inventory reports, a check box is available for "Each Reseller & Customer" and "Generate XLS Report". Upon selecting "Each Reseller & Customer" you will have Aggregate reports generated for each Customer & Reseller in the system. Each Customer/Reseller will have a Summary,

Detailed & MACD report generated as well as a Service Provider level Summary Report. Upon selecting "Generate XLS Report" checkbox, an excel-formatted report is generated. Location reports require an Inventory report (.si) to be available on the system or an error will be generated.

Both Scheduled and On Demand reports require that either CUCDM, UCAPP, or CUCDM&UCAPP be chosen as the report source, the default being CUCDM. Selecting CUCDM as the source generates a ".si" report and summary reports will be generated from Cisco Unified Communication Domain Manager. If UCAPP is chosen as the report source, ".ucsi" and ".simacd" reports will be generated from a Cisco Unified Communication application, provided a Cisco Unified Communication application has been configured directly in Cisco Hosted Collaboration Mediation Fulfillment, without using Cisco Unified Communication Domain Manager). If CUCDM&UCAPP is chosen as the report source, ".si", ".ucsi", and ".simacd" reports will be generated.

**Infrastructure Manager**

Infrastructure Manager allows you to provision and query the Cisco HCS Shared Data Repository (SDR). The Cisco HCS Shared Data Repository provides configuration information for Cisco Hosted Mediation Fulfillment Service Assurance. The Cisco HCS Shared Data Repository is a repository of data that represents the Cisco HCS configuration of data centers, customers and management components in the service provider's network. This repository is then used by HCM-Service Assurance to provide more effective, detailed, and accurate operational alarms and events.

Cisco HCS License Manager is a part of Infrastructure Manager and provides centralized license management for Cisco HCS. Cisco HLM leverages the functionality of a UC component called Prime License Manager. Cisco HLM extends the functionality of Prime License Manager for use in the service provider space beyond the scope of a single enterprise.

**Node Manager**

The Node Manager application allows you to manage your Cisco Hosted Collaboration Mediation Fulfillment platform by adding, editing and deleting Cisco Hosted Collaboration Mediation Fulfillment Cluster Nodes.

**Platform Manager**

The Platform Manager administrative interface, a UC application platform management client, allows you to start upgrades for Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unity Connection in the Cisco Hosted Collaboration Solution. It allows you to configure the server inventory for the system as well as select, schedule, and monitor upgrades of one or more servers across one or more clusters. In the Platform Manager administrative interface, you can also create groups of servers to help manage multiple clients and applications. From the administrative interface, you can schedule restarts for servers and schedule tasks for switching to the active version (active partition). You can also automate backup tasks of your system using the Backup Schedule feature.

**Note** Management of UC Applications, Release 10.5(2) or later, is handled by Cisco Prime Collaboration Deployment (PCD). Cisco Prime Collaboration Deployment is an application that is designed to assist in the management of Unified Communications (UC) applications. It allows you to perform tasks such as migration of older software versions of clusters to new virtual machines, fresh installs, and upgrades on existing clusters.

Details on available PCD features, along with installation, configuration and administration, best practices, and troubleshooting information can be found in the PCD Deployment Guide at:http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html and in the PCD Release Notes at: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html.

# Browser support

From any networked device with a supported web browser, you can browse into a server that is running the Cisco Hosted Collaboration Mediation Fulfillment administrative interface and log in with administrative privileges.

The Cisco Hosted Collaboration Mediation Fulfillment administrative interface uses HTTPS, or HTTP over Secure Sockets Layer (SSL), to secure communication between the browser and the web server. HTTPS uses certificates to ensure server identities and to secure the browser connection. HTTPS uses a public key to encrypt the data, including the user login and password, during transport over the Internet. To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server 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 server. For more information on how your browser supports HTTPS, refer to the documentation for your browser.

For browser compatibility information, refer to *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.

CHAPTER 2

# Perform Routine Maintenance



# Maintenance Tools and Utilities

## Service Inventory

### General Settings for Service Inventory Setup

In the Service Inventory administrative interface, you manage credentials and configure general settings for Service Inventory on the Configuration page. The following table provides a list of settings that you configure on the Configuration page.

**Tip** Service Inventory works with Cisco Unified Communications Domain Manager or two UC Applications - Cisco Unified Communications Manager and Cisco Unity Connection. For Service Inventory to work, make sure that you configure Cisco Unified Communications Domain Manager or the supported UC Application in the Infrastructure Manager administrative interface.

**Important** Service Inventory can generate reports only from a Cisco Unified Communications Manager and Cisco Unity Connection running UC Application Software Version 8.6(2) or later.

In the Service Inventory administrative interface, click **Configuration**. Enter the configuration for the settings in the following table; then click **Save**.

*Table 1: Settings for Configuration Page in Service Inventory*

| Field | Description |
|---|---|
| Service Inventory Settings<br>Use this section to configure a Service Inventory server. | |
| Hostname | Enter the hostname of the Service Inventory server. The Service Inventory hostname must be entered as an IP address or a fully qualified domain name.<br>**Note** If the Cisco Unified Communications Domain Manager server is not configured with DNS enabled, enter an IP address in the Hostname field. |
| Port | Enter the SFTP port number that is used by the Cisco Unified Communications Domain Manager server to send the requested SI billing data to this Service Inventory server. The default is 22. |
| Username | Cisco Unified Communications Domain Manager uses the username, adminsftp, to transfer data to the Service Inventory application. You cannot update this field. |
| Password | Enter the password for the adminsftp user account. This step is required as an identity confirmation for security purposes. This password is the same as the HCS administrator password that you set up during the Cisco HCM-F installation (or changed after installation). |
| Service Provider SFTP and Remote Backup SFTP Settings<br>Use this section to configure and enable transfer of Service Inventory reports to remote SFTP servers. Remote SFTP servers configured on this page also serve as the destination of files when you initiate a transfer from the Backup page.<br>You must configure a primary remote SFTP server. If you want to do so, you may configure a secondary remote SFTP server. If you configure the secondary remote SFTP server, the generated report files get sent to the location for the secondary remote SFTP server in addition to the primary remote SFTP location.<br>**Note** The Backup page sends selected files to the primary SFTP server but not the backup server, while scheduled jobs send files to both servers. | |
| Hostname | Enter the hostname of the primary remote SFTP server. |
| Port | Enter a port number for the primary remote SFTP server or use the default, which is 22. |
| Username | Enter a valid username to access the remote SFTP server. |
| Password | Enter the password to access the remote SFTP server. |
| Destination Path | Enter a path on the SFTP server where the billing files will be stored. |
| Retry Count | Set the number of times the Service Inventory service will attempt to transfer billing reports if the SFTP transfer does not succeed on the first try.<br>**Tip** The Retry Count and Maximum File Size that you specified under the Remote SFTP Server settings also apply to the Remote Backup SFTP Server settings. |

| Field | Description |
|---|---|
| Maximum File Size (MB) | Enter the maximum individual file size (in MB) for Service Inventory reports that are transferred to remote SFTP servers. The Service Inventory application will split and rename files to meet this size requirement before transfer. The maximum value you can enter is 2047 MB. |
| Local Settings<br>Use this section to configure the local settings for report backup retention, for log trace levels, to enable report customization and to set up the failure notification email feature. | |
| Local Backup Retention period (days) | Set the number of days that you want to retain backup copies of generated Service Inventory reports. Enter between 30 and 60, with 60 being the default. |
| Log Trace Level | Set the log trace level. Available trace levels are Fatal, Error, Warning, Informational, and Detailed. |
| Enable Report Customization | Check to enable additional customization of Service Inventory reports. Verify that an appropriate Cisco Advanced Services application plug-in is installed. Service Inventory application executes the plug-in to provide additional report customization after basic processing if this option is enabled and the plug-in is installed. |
| Failure Notification<br>The Service Inventory service provides the ability to send email notifications in the event of application errors and failures. This notification service is optional, but is used if configured.<br>**Tip** For email notification to work, you must use DNS. | |
| SMTP Hostname | Enter the outbound SMTP hostname or use the default of local host. |
| SMTP Port | Enter the SMTP port number or use the default, which is 25. |
| Email Address (From) | Enter the outbound email address. |
| Email Address (To) | Enter the inbound email address. |

## Infrastructure Manager for Service Inventory Support Setup

Service Inventory can generate reports from Cisco Unified Communications Domain Manager. If you use Unified Communications Domain Manager with Service Inventory, verify that a managed Unified Communications Domain Manager application instance is configured within Infrastructure Manager.

Service Inventory can also generate reports directly from a supported UC Application, Cisco Unified Communications Manager and Cisco Unity Connection application servers for customers that are provisioned in Cisco HCM-F that do not have a Unified Communications Domain Manager configured. If you do not have a Unified Communications Domain Manager configured, you need to add a Cisco Unified Communications Manager and Cisco Unity Connection application server manually to run a Service Inventory report.

Cisco Unified Communications Domain Manager should appear on the Management Network page in the Infrastructure Manager administrative interface (**Application Management** > **Management Application**). If you determine that an instance does not exist, configure the settings in the following table.

***Table 2: Settings for Unified Communications Domain Manager 8.1.x in Infrastructure Manager (Management Application Page)***

| Field | Description |
|---|---|
| **General Information** | |
| Application Type | From the drop-down list box, select **CUCDM 8.1.x**. |
| Name | Enter the name of the Cisco Unified Communications Domain Manager. |
| API Version | Select the API version.<br>**Note** If you are integrating with a CUCDM version prior to 8.1.2, the API version must be set to 8.0. The API version can be set to either 8.0 or 8.1 when integrating with CUCDM 8.1.2. Also note that if the 8.0 API version is configured, SIP Trunk will not be synced, and only location name will be synced for Customer Location. |
| Port | Enter a SOAP port number for the Cisco Unified Communications Domain Manager platform. The default port is 8181. |
| Description | Enter a description for the Unified Communications Domain Manager. |
| Auto Link to Virtual Machine | Check this check box to automatically link to the virtual machine. |
| Virtual Machine | Enter the location of the virtual machine where Unified Communications Domain Manager is installed. |
| Host ID | Enter the unique host identifier for the Cisco Unified Communications Domain Manager platform.<br>**Tip** Service Inventory requires a value of 1 or greater. |
| Routing ID | Enter the route identifier for the Cisco Unified Communications Domain Manager platform.<br>**Note** You can choose to use a unique identifier based on information already within your provisioning system instead of the default hierarchical name-based routing based on the infrastructure configuration in SDR. |

| Field | Description |
|---|---|
| Sync Enabled | Check this check box to enable synchronization of data from Cisco Unified Communications Domain Manager. For synchronization to work, make sure that the Cisco HCS CUCDMSync service is activated and running on the Cisco HCM-F platform.<br><br>Unchecking this check box disables automatic synchronization. If you do not enable sync, you must perform a manual sync before a Service Inventory report can be generated. Verify that the Service Provider name in the Administration page in Infrastructure Manager matches the name that is configured in Cisco Unified Communications Domain Manager. |
| Sync Interval (Minutes) | Enter how often you want the Cisco HCS CUCDMSync service to attempt to synchronize the data from Cisco Unified Communications Domain Manager. For example, if you enter 15, the service attempts to synchronize the data every 15 minutes.<br><br>This setting works only if you checked the Sync Enabled check box and the Cisco HCS CUCDM Sync service is activated and running on the Cisco HCM-F platform. |
| **Credentials** | |
| Credentials Type | From the drop-down list box, select **ADMIN**. |
| User ID | Ensure you have created a webservice user on Unified Communications Domain Manager release 8.1(x) (superuser role). This is the User ID to access Unified Communications Domain Manager. |
| Password and Re-enter Password | Enter the password for the User ID. Re-enter the same password for the User ID. |
| Access Type | Service Inventory requires Read Only, but you can select either option. |
| Network Addresses | |
| Network Space | From the drop-down list box, select **Service Provider Space**. |
| IPv4 Address | If your Unified Communications Domain Manager platform uses IPv4, enter the IPv4 address for the Unified Communications Domain Manager platform. |
| IPv6 Address | If your Unified Communications Domain Manager platform uses IPv6, enter the IPv6 address for the Unified Communications Domain Manager platform. |
| Hostname | If you use DNS, enter the hostname for the Unified Communications Domain Manager platform. |

| Field | Description |
|---|---|
| Domain | Enter the domain for the Unified Communications Domain Manager platform. |
| SRV Address | This setting does not apply to Service Inventory. |

***Table 3: Settings for Unified Communications Domain Manager 10.x in Infrastructure Manager (Management Application Page)***

| Field | Description |
|---|---|
| **General Information** | |
| Application Type | From the drop-down list box, select **CUCDM**. |
| Name | Enter the name of the Cisco Unified Communications Domain Manager. |
| Description | Enter a description for the Unified Communications Domain Manager. |
| Auto Link to Virtual Machine | Check this check box to automatically link to the virtual machine. |
| Virtual Machine | Enter the location of the virtual machine where Unified Communications Domain Manager is installed. |
| **Credentials** | |
| Credentials Type | From the drop-down list box, select **ADMIN**. |
| User ID | Enter the User ID that is used to access Unified Communications Domain Manager. Service Inventory uses the 'hcsadmin' user for querying Cisco Unified Communications Domain Manager. |
| Password and Re-enter Password | Enter the password for the User ID. Re-enter the same password for the User ID. |
| Access Type | Service Inventory requires Read Only, but you can select either option. |
| **Network Addresses** | |
| Network Space | From the drop-down list box, select **Service Provider Space**. |
| IPv4 Address | If your Unified Communications Domain Manager platform uses IPv4, enter the IPv4 address for the Unified Communications Domain Manager platform. |
| IPv6 Address | If your Unified Communications Domain Manager platform uses IPv6, enter the IPv6 address for the Unified Communications Domain Manager platform. |

| Field | Description |
|---|---|
| Hostname | If you use DNS, enter the hostname for the Unified Communications Domain Manager platform. |
| Domain | Enter the domain for the Unified Communications Domain Manager platform. |
| SRV Address | This setting does not apply to Service Inventory. |

To configure both Cisco Unified Communications Manager and Cisco Unity Connection, go to the Customer Management page in the Infrastructure Manager administrative interface (**Customer Management** > **Customer**).

## Report Generation for Service Inventory

At the time that is specified in the Service Inventory configuration, Service Inventory sends a real-time query request to Cisco Unified Communications Domain Manager and all Cisco HCM-F provisioned UC Applications that are assigned to customers that are not associated with a Cisco Unified Communications Domain Manager.

Cisco Unified Communications Domain Manager generates the necessary files and sends the files to Service Inventory through SFTP.

Service Inventory processes the files or messages, including but not limited to backing up the files for troubleshooting purposes, creating the report, and transferring the report to the SFTP servers that are configured in the Service Inventory administrative interface.

Service Inventory supports Partitioned Unity Connection.

**Example**: Customer A - Sharedent 1 and Customer B - Sharedent 2.

Customer A and B are sharing the partitioned unity connection application.

The generated report contains data for the previous 24 hours, up to and including the end time that you specify on the Overview page in the Service Inventory administrative interface.

**Note** The first SI report (OnDemand or Scheduled) with Cisco Unified Communications Domain Manager 10.x will not have MACD reported. The subsequent reports will have MACD in the "si" report.

## Generated Reports

In the Service Inventory administrative interface, the Backup page displays a list of generated report files. The Backup page displays the file name, date, and file size for the generated report. Filter the results by selecting an option from the Show drop-down list box or by clicking one of the columns on the page.

**Tip** The configuration for the Local Backup Retention Period setting on the Configuration page determines the files that appear in the list on the Backup page. Service Inventory deletes reports based on the value that you configure for this setting. For example, if you configure this setting as 35, and the report is 36 days old, the report name does not appear in the list.

## On Demand Reporting

Service Inventory provides On Demand Inventory and Location reporting. These On Demand reports allow the administrator to generate reports at any time without having to alter the reporting schedule. Location Summary reports generate a report to indicate the number of devices and subscribers per location.

For On Demand Service Inventory reports, a check box is available for "Each Reseller & Customer" and "Generate XLS Report". Upon selecting "Each Reseller & Customer" you will have Aggregate reports generated for each Customer & Reseller in the system. Each Customer/Reseller will have a Summary, Detailed & MACD report generated as well as a Service Provider level Summary Report. Upon selecting "Generate XLS Report" checkbox, an excel-formatted report is generated. For this release, the report extension is .xlsm and for other releases, the report extension is .xlsx.

**Note** You must generate an inventory report (.si) before you can generate a location report. If you try and generate a location report first, you will receive an error.

Both Scheduled and On Demand reports require that either CUCDM, UCAPP, or CUCDM&UCAPP be chosen as the report source, the default being CUCDM. Selecting CUCDM as the source generates a ".si" report and summary reports will be generated from Cisco Unified Communication Domain Manager. If UCAPP is chosen as the report source, ".ucsi" and ".simacd" reports will be generated from a Cisco Unified Communication application, provided Cisco Unified Communication application has been configured in Cisco Unified Communcations Domain Manager and provisioned in Cisco Hosted Collaboration Mediation Fulfillment & synced with Cisco Unified Communications Manager). If CUCDM&UCAPP is chosen as the report source, ".si", ".ucsi", and ".simacd" reports will be generated.

The following table describes the fields to configure On Demand Reporting.

| Field | Description |
|---|---|
| System Time | Click the refresh button to acquire the system time. |
| Type of report to generate | Generated report type (Location Report or Inventory Report). |
| Report Source | Report Source will either be CUCDM, UCAPP, or CUCDM&UCAPP |
| Report Format Version | Version report format (8.6.2, 9.0.1, 9.1.1, 9.1.2, 10.0.1, 10.1.2, 10.6.1). |
| Report must include information up to (GMT) | Report will contain data up to a specified time period (listed in 15 minute intervals). |
| **Create separate report files for: (checkboxes)** | |

| Field | Description |
|---|---|
| Service Provider | Systemwide service providers' report (selected by default). |
| Each reseller and customer | Report created for each reseller and customer. |
| Generate XLS Report | Report created in XLS Format. |

In a deployment where UCDM 8.1(x) and UCDM 10 co-exist, a report will be generated for both UCDM 8.1(x) and UCDM 10. The report file name for UCDM 8.1(x) will have a tag of "+CUCDM+" and the UCDM 10 tag will be "+CUCDM2+".

The below report format is common for the Service Inventory and the Location report generates with any source (CUCDM or UCAPP).

Report generated Year-Month-Date followed by the time- GMT timezone.

The following are example file names:

CUCDM 8.1.4 customers: 20140804131528GMT+1+CUCDM+1+1.si

CUCDM 10 customers: 20140804131528GMT+1+CUCDM2+1+1.si

## Location Reporting

Location Reporting provides details of each customer's internal hierarchy and locations as modeled by Cisco Unified Communications Domain Manager. The report should be executed on demand through the Service Inventory user interface or the Cisco Hosted Collaboration Mediation Fulfillment Northbound Interface and then transferred to the service provider's primary SFTP location. A previously generated Service Inventory report file is used as the source file to generate the data in the Location report.

**Note** Location reports require that at least one Inventory report request has been executed.

## Customer and Reseller Reports

For both Scheduled & On Demand Service Inventory reports, a check box is available for "Each Reseller & Customer". Upon selecting this check box you will have Aggregate reports generated for each Customer & Reseller in the system. Each Customer/Reseller will have a Summary, Detailed and MACD report generated as well as a service provider level Summary Report.

### *Detailed Reporting*

Detailed Aggregate level reports compliment existing service inventory (.si) reports by generating detailed information for both Cisco Unified Communications Domain Manager and Cisco Unified Communication application based configurations. Aggregate reporting at any level will have detailed report data for its customers only.

The status of a generated report can be viewed in **Infrastructure Manager > Administration > Jobs**.

**Note** Only customer level detailed reports are generated for Cisco UC application based configurations.

### *Summary Reporting*

Summary reporting gives the high level information of Cisco HCS Service Inventory customers along with the subscribers and devices. When aggregate level reporting is enabled in the Service Inventory configuration, summary reports along with other aggregate level reports are generated and saved to the Cisco Hosted Collaboration Mediation Fulfillment server. The Service Inventory configuration can also be completed through the Cisco Hosted Collaboration Mediation Fulfillment Northbound Interface.

Summary reports will get generated at different aggregate levels for multiple providers, each reseller and each customer present in Cisco Unified Communications Domain Manager and non Cisco Unified Communications Domain Manager deployment(UC Deployment). In a Hybrid deployment model, Service Inventory pulls inventory data directly from the UC Applications created on Cisco Hosted Collaboration Mediation Fulfillment and puts them into a report. A message is sent to get an inventory report, which Service Inventory then takes and formats based on the version's format specification. This generates a single summary report using data from both Cisco Unified Communications Domain Manager and Unified Communication applications.

### *MACD (Move-Add-Change-Delete) Reporting*

MACD reports are generated for both Cisco Unified Communications Domain Manager-based and Cisco Unified Communication Application-based configurations. However, Cisco Unified Communication Application-based reports are not generated at the reseller level.

## Report Matrix

***Table 4: Report Matrix***

| Report Version | CUCDM 8.x | CUCDM 10.x | UC APP | Comments |
|---|---|---|---|---|
| 8.6.2 | Yes | Yes | No | Report from CUCDM 10.x is as close as possible to CUCDM 8.x. (The only exception is the features/feature groups where in 10.x, it is based on actual features that are enabled.) |
| 9.0.1 | Yes | Yes | No | Report from CUCDM 10.x is as close as possible to CUCDM 8.x. (The only exception is the features/feature groups where in 10.x, it is based on actual features that are enabled.) |
| 9.1.1 | No | No | Yes | This report appears only when the report source is selected as UC APP. |
| 9.1.2 | No | No | Yes | This report appears only when the report source is selected as UC APP. |
| 9.2.1 | Yes | No | No | This report version is purely from CUCDM 8.x, as we cannot provide the Connected Location and Fake Phone info in CUCDM 10.x. |
| 9.2.2 | No | Yes | No | This report appears only when the report source is selected as CUCDM 10.x. |

| Report Version | CUCDM 8.x | CUCDM 10.x | UC APP | Comments |
|---|---|---|---|---|
| 10.0.1 | Yes | Yes | No | From CUCDM 10.x we generate 10.0.1 format. For CUCDM 8.x we generate the latest report version available (9.2.1) from CUCDM 8.x. |
| 10.1.2 | Yes | Yes | No | From CUCDM 10.x we generate 10.1.2 format. For CUCDM 8.x we generate the latest report version available (9.2.1) from CUCDM 8.x. |
| 10.6.1 | Yes | Yes | No | From CUCDM 10.x we generate 10.6.1 format. For CUCDM 8.x we generate the latest report version available (9.2.1) from CUCDM 8.x. |

## Report Combinations

### Cisco HCS Deployment with Cisco Unified Communications Domain Manager 8.x

| Source of Report | Report Version selected | | | | | |
|---|---|---|---|---|---|---|
| | **8.6.2** | **9.0.1** | **9.1.1** | **9.2.1** | **9.1.2** | **9.2.2** |
| **UCAPP** | N/A | N/A | UCApp report “.ucsi” is generated of report version 9.1.1 | N/A | UCApp report “.ucsi” is generated with report version 9.1.2 | N/A |
| **CUCDM** | CUCDM “.si” report is generated of report version 8.6.2 | CUCDM “.si” report is generated of report version 9.0.1 | N/A | CUCDM “.si” report is generated of report version 9.2.1 | N/A | CUCDM “.si” report is generated with report version 9.2.2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **CUCDM & UCAPP** | CUCDM “.si” report is generated of report version 8.6.2<br>AND<br>UCApp report “.ucsi” is generated of report version 9.1.1<br>. | CUCDM “.si” report is generated of report version 9.0.1<br>AND<br>UCApp report“ .ucsi” is generated of report version 9.1.1 | N/A | CUCDM “.si” report is generated of report version 9.2.1<br>AND<br>UCApp report “.ucsi” is generated of report version 9.1.1 | N/A | CUCDM “.si” report is generated of report version 9.2.2<br>AND<br>CUCDM “.si” report is generated of report version 9.2.2 |

### Deployment with Cisco Unified Communications Domain Manager 10.x

| **Source of Report** | **Report Version selected** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **8.6.2** | **9.0.1** | **9.1.1** | **9.2.1** | **9.2.2** | **10.0.1** | **10.1.2** | **10.6.1** |
| **UCAPP** | N/A | N/A | UCApp report ".ucsi" is generated of report version 9.1.1 | N/A | N/A | N/A | N/A | N/A |
| **CUCDM** | CUCDM ".si" report is generated of report version 8.6.2. | CUCDM ".si" report is generated of report version 9.0.1 . | CUCDM ".si" report is generated of report version 9.2.1 | N/A | CUCDM “.si” report is generated of report version 9.2.2 | CUCDM ".si" report is generated of report version 10.0.1 | CUCDM ".si" report is generated of report version 10.1.2 | CUCDM “.si” report is generated with report version 10.6.1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **CUCDM & UCAPP** | CUCDM ".si" report is generated of report version 8.6.2<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1<br>. | CUCDM ".si" report is generated of report version 9.0.1<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | N/A | CUCDM ".si" report is generated of report version 9.2.1<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | CUCDM “.si” report is generated with report version 9.2.2<br>AND<br>UCApp report “.ucsi” is generated with report version 9.1.2 | CUCDM ".si" report is generated of report version 10.0.1<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | CUCDM ".si" report is generated of report version 10.1.2<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | UCApp report “.ucsi” is generated with report version 9.1.2<br>AND<br>UCApp report “.ucsi” is generated with report version 9.1.2 |

### Deployment without Cisco Unified Communications Domain Manager 10.x/8.x

| **Source of Report** | **Report Version selected** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **8.6.2** | **9.0.1** | **9.1.1** | **9.2.1** | **9.2.2** | **10.0.1** | **10.1.2** | **10.6.1** |
| **UCAPP** | N/A | N/A | UCApp report ".ucsi" is generated of report version 9.1.1 | N/A | N/A | N/A | N/A | N/A |
| **CUCDM** | CUCDM ".si" report is generated of report version 8.6.2 from both the CUCDM's are generated | CUCDM ".si" report is generated of report version 9.0.1 from both the CUCDM's are generated | N/A | CUCDM ".si" report is generated of report version 9.2.1 from both the CUCDM's are generated | CUCDM “.si” report is generated of report version 9.2.2 from both the CUCDM's are generated | CUCDM ".si" report is generated of report version 10.0.1 from CUCDM 10.x and report version of 9.2.1 from CUCDM 8.x are generated | CUCDM ".si" report is generated of report version 10.1.2 from CUCDM 10.x and report version of 9.2.1 from CUCDM 8.x are generated | CUCDM “.si” report is generated with report version 10.6.1from CUCDM 10.x and report version of 9.2.2 from CUCDM 8.x are generated |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **CUCDM & UCAPP** | CUCDM ".si" report is generated of report version 8.6.2 from both the CUCDM's are generated<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | CUCDM ".si" report is generated of report version 9.0.1 from both the CUCDM's are generated<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | N/A | CUCDM ".si" report is generated of report version 9.2.1 from both the CUCDM's are generated<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | CUCDM ".si "report is generated with report version 9.2.2 from both the CUCDM's are generated<br>AND<br>UCApp report ".ucsi" is generated with report version 9.1.2 | CUCDM ".si" report is generated of report version 10.0.1 from CUCDM 10.x and report version of 9.2.1 from CUCDM 8.x are generated<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | CUCDM ".si" report is generated of report version 10.1.2 from CUCDM 10.x and report version of 9.2.1 from CUCDM 8.x are generated<br>AND<br>UCApp report ".ucsi" is generated of report version 9.1.1 | CUCDM ".si "report is generated with report version 10.6.1 from CUCDM 10.x and report version of 9.2.2 from CUCDM 8.x are generated<br>AND<br>UCApp report ".ucsi" is generated with report version 9.1.2 |

# Infrastructure Manager

Infrastructure Manager allows you to provision and query the Cisco HCS Shared Data Repository. The Cisco HCS Shared Data Repository provides configuration information for HCM-Service Assurance. The Cisco HCS Shared Data Repository is a repository of data that represents the Cisco HCS configuration of Data Centers, customers, and management components in the service provider's network. This repository is then used by HCM-Service Assurance to provide more effective, detailed, and accurate operational alarms and events.

## Jobs

The Jobs Summary page displays a list of the last 400 automatic and manual jobs added to your Cisco HCM-F as well as basic details about each one.

**Note** A purge of the job list occurs every 24 hours.

### Jobs Field Descriptions

| Field | Description |
|---|---|
| Job Type | Displays the job type. |
| Description | Displays the job description. |
| Job Entity | Displays the job entity. |
| Entity Name | Displays entity name. |
| Date/Time Initiated | Displays the initiated job date and time. |
| Status | Displays the job status. If the Job Status is In Progress or Fail, hover the cursor over the info circle and more information is given as well as recommended actions. |
| Actions | Displays the available job actions. |

## Failed or Cancelled Jobs

**Checking the Job Status**

To view the job status, navigate to Administration > Jobs in Infrastructure Manager in HCM-F GUI. For Infrastructure Provisioning Adapter (IPA) jobs, the Job Type is "Provisioning", the Description is "IPA Provisioning Request", and the Entity Name is the name of the customer. The job status table is displayed and will remain until deleted or automatically removed.

Additional status information and recommended actions for the job can be seen by hovering over the job details icon. If the IPA service is stopped or restarted while a job is in-progress, the job status will be marked as failed when IPA resumes.

**Note** Cancelling a job is supported with no rollback support. If the job is already in progress, remaining tasks of the job are cancelled and you must manually delete any Virtual Machines created as part of provisioning the job.

**Canceling the job**

You can cancel queued or in-progress jobs by clicking the cancel button under the actions column for the job status page in the HCM-F GUI. The job will immediately be cancelled and marked as such after the GUI refreshes. No new vCenter tasks will begin for that job, but any current operations in the vCenter will continue until they are completed or are cancelled by the user. The user must manually clean up any Virtual Machines from the job just as in the case of a failed job. Any queued jobs for the customer will run immediately. Cisco recommends that the user cancels the queued jobs prior to cancelling the active job if an entire customer's provisioning needs to be stopped.

**Failed/cancelled jobs**

If the job fails, the user must clean up any Virtual Machines from the job and resubmit the job. Failures in the preliminary validation phase do not leave behind any Virtual Machines. If the job fails or is cancelled during the identity process, the cloned Virtual Machines may still have the identity (hostname, IP address) of the template. You must power off or remove these Virtual Machines before attempting to clone again from the same template. Subsequent jobs will time out while waiting for the node to come online if there is a conflict.

## Service Provider

The service provider page displays the details of the service provider in your Cisco HCS.

**Note** If CUCDMSync is enabled and successful, customer equipment is added, edited, and deleted through the CUCDMSync.

### Service Provider Field Descriptions

## Settings

The settings page provides thresholds for Cisco Prime Collaboration assignments that you can configure the maximum number of customers and devices each Cisco Prime Collaboration can service. The settings page also allows the administrator to specify warning thresholds.

When a maximum is reached, you can make no further assignments to that Cisco Prime Collaboration. When a warning threshold is reached, the Usage is highlighted on the Management Application page.

### Settings Field Descriptions

| Field | Description |
|---|---|
| Maximum number of customers | Displays the maximum number of customers . |
| Customer warning threshold (% of maximum) | Displays the warning threshold for the number of customers. |
| Maximum number of devices | Displays the maximum number of devices. |
| Device warning threshold (% of maximum) | Displays the warning threshold for the number of devices. |

## Diagnostics

Diagnostics allows you to get real time status and statistics from running services, run real time tests to make sure services are working properly and if not, indicate recommended actions for administrators.

These diagnostic reports can also be accessed from the command line interface. For more information on CLI diagnostic commands, see *Cisco Hosted Collaboration Mediation Fulfillment Command Line Interface Reference Guide, Release 10.6(1)*.

***Table 5: Diagnostics Field Descriptions***

| Field | Description |
|---|---|
| Diagnostic | Allows a selection of the type of diagnostics to run. |
| Request Diagnostics | Button to click to submit the diagnostic request. |

## API Gateway Diagnostic Report

### API Gateway Proxy web service

The following table outlines the diagnostic report for the API Gateway Proxy web service.

| Property Name | Property Value Description |
|---|---|
| Start Time | Timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |
| Maximum Memory | The maximum memory allocated for the service. |
| Free Memory | The free memory available for the service. |
| Percent Free Memory | The free memory available for the service in percent. |
| Global Address and Http Port | The global address and http port advertised by API Gateway Proxy if configured. |

***Table 6: Routing Counters***

| Property Name | Property Value Description |
|---|---|
| Number of Routes by RoutingId | Number of Routes that are routed based on routing ID. |
| Number of Routes by Cluster | Number of Routes that are routed based on customer name and cluster name. |
| Number of Routes by Cluster and Node | Number of Routes that are routed based on customer name, cluster name and node name. |
| Number of Routes by Domain Manager | Number of Routes that are routed based on domain manager name. |

| Property Name | Property Value Description |
|---|---|
| Number of Clusters that aren't associated with a Customer | Number of clusters that are not associated with a customer. |
| Number of Invalid Routes | Number of routes that are not configured correctly. |

Each area has its own set of counters, but the property names and descriptions are the same.

***Table 7: CUCM, CUCxn, CUP, HCS, CUCDM, CCDM, and Total Counters***

| Property Name | Property Value Description |
|---|---|
| Northbound Rxd (North ==> Proxy) | Displays the number of messages received from the clients. |
| Northbound Txd (North <== Proxy) | Displays the number of messages transmitted to the clients. |
| Southbound Txd (Proxy ==> South) | Displays the number of messages transmitted to the Cisco Unified Communications Manager applications. |
| Southbound Rxd (Proxy <== South) | Displays the number of messages received from the Cisco Unified Communications Manager applications. |
| AsyncNorthbound Txd (North <== Proxy | Displays the number of asynchronous messages transmitted to the clients. |
| AsyncSouthbound Rxd (Proxy <== South) | Displays the number of asynchronous messages received from the Cisco Unified Communications Manager applications. |
| Southbound Failures | Displays the number of messages that API Gateway Proxy failed to transmit to the Cisco Unified Communications Manager applications. |
| Northbound Failures | Displays the number of messages that API Gateway Proxy failed to transmit to the client. |
| Routing Failures | Displays the number of messages that API Gateway Proxy failed to route. |

***Table 8: Database Pulse Detector Diagnostics***

| Property Name | Property Value Description |
|---|---|
| Database State | Whether the database is up or down. |
| Last Test Time | The time of the last test. |
| Currently Sleeping for (Ms) | The time in Ms that the database has been inactive. |

| Property Name | Property Value Description |
|---|---|
| Registered Callback Handlers | The number of registered callback handlers |
| Running Callback Handlers | The number of active callback handlers. |
| initialDatabaseTestDelayMs | The time in MS to delay the initial database test. |
| periodicTestDelayWhenDBIsDownMs | The periodic time in MS to delay the database test when the database is down. |
| periodicTestDelayWhenDBIsUpMs | The periodic time in MS to delay the database test when the database is up. |
| dieWhenDatabaseComesUp | Determines if the Database Pulse Detector will die once the database comes up for the first time. |
| sessionName | DBPulseDetector |
| logger | com.cisco.hcs.apigw |

## CHPA Diagnostic Report

### CHPA Agent Properties

The following tables outlines the diagnostic report for the Cisco HCS Provisioning Adapter service.

***Table 9: CHPA AgentRouteBuilder Properties***

| Property Name | Property Value Description |
|---|---|
| CHPA AgentRouteBuilder Status | Signifies the health of the agent; options are Red, Yellow, or Green. |
| Recommended Action | Recommended action to correct last failure. If "Unknown", then no failures to report. |
| Configured CHPA Agents | The number of CHPA Agents configured. |
| Device AgentInstanceMap Size | The number of application instances managed. |

***Table 10: CHPA Agent Properties***

| Property Name | Property Value Description |
|---|---|
| Agent Instance Id | Internal Id of the agent. |
| Agent Status | Signifies the health of the agent; options are Red, Yellow, or Green. |
| Creation Time | Date and time the agent was created. |
| # of App Instances Managed | Number of application instances that are managed by the agent. |

| Property Name | Property Value Description |
|---|---|
| Connection Table Size | The size of the connection table. |
| Total Success | Total number of requests sent to application instances that were successful. |
| Total Failures | Total number of requests sent to application instances that were un-successful. |
| Last Success Time | Date and time the last successful request was made to an application instance. |
| Last Failure Time | Date and time the last unsuccessful request was made to an application instance. If this time is equal to the agent's creation time, then no failures have occurred. |
| Last Failure Appinst | The last Application Instance that encountered a failure. If "Unknown", then no failures to report. |
| Last Failure Reason | The reason for the last failure. If "Unknown", then no failures to report. |
| Last Failure (Recommended Action) | Recommended action to correct last failure. If "Unknown", then no failures to report. |

## CUCDMSync Diagnostic Report

### Cisco HCS CUCDMSync

The following tables outline the diagnostic report for the Cisco HCS CUCDMSync service.

**Note** Cisco recommends that you do not configure this manually. For customers on Cisco Unified Communications Domain Manager 8.1(x), please use CUCDMSync to configure. For customers on Cisco Unified Communications Domain Manager 10.1(x), the information will be pushed from the Cisco Unified Communications Domain Manager Server to the Cisco HCM-F server and does not require configuration.

***Table 11: CUCDMSync Service Diagnostic Properties***

| Property Name | Property Value Description |
|---|---|
| CUCDMSync Status | Signifies the health of the CUCDMSync, options are Red, Yellow, or Green. |
| Status Info | Job status info for the CUCDMSync, field is empty if no job has started for this application. |
| Recommended Action | Job recommended action for the CUCDMSync, field is empty if no job has started for this application. |
| Sync Interval | The time between each CUCDMSync request. |

| Property Name | Property Value Description |
|---|---|
| Health Interval | A time interval used by the CUCDMSync service to calculate when to perform self diagnostics to detect and correct service-threatening events, such as unresponsive sync agents. This value can not be altered by the administrator. |
| Next Auto-Sync | The time until the next CUCDMSync request. (Only displayed in the diagnostics GUI if Auto-Sync is enabled. If the Sync Interval value shows "Disabled," then Next-Auto Sync will not be displayed.) |
| Number of attempted syncs | The number of attempted CUCDMSync requests. |
| Last Success Sync | The date and time of the last successful CUCDMSync request. |
| Last Error Sync | The date and time of the last error from the CUCDMSync request. |
| Last Error Reason | A description of the possible errors and a list of recommended actions to resolve the error. |
| Number of failed agents | The number of failed agents. |
| Time of last failed agents | The date and time of the last failed agent. |

***Table 12: Connection Pools Properties***

| Property Name | Property Value Description |
|---|---|
| CUCDM Active Connections | The number of currently active Cisco Unified Communications Domain Manager connections. |
| CUCDM Idle Connections | The number of currently idle Cisco Unified Communications Domain Manager connections. |
| SDR Active Sessions | The number of currently active SDR connections. |
| SDR Idle Sessions | The number of currently idle SDR connections. |

The following fields appear in the GUI only after a sync has been performed on your HCM-F.

***Table 13: CUCDMSync Cluster Agent Diagnostic Properties***

| Property Name | Property Value Description |
|---|---|
| Agent Instance ID | The unique ID for the CUCDMSync agent. |
| Agent Status | Signifies the health of the CUCDMSync Agent, options are Red, Yellow, or Green. |
| Work done | The number of syncs performed. |

| Property Name | Property Value Description |
|---|---|
| Number of Errors | The number of errors for the CUCDMSync cluster agent. |
| SDR Session | The name of the SDR session. |
| CUCDM Connection | The connection of the Cisco Unified Communications Domain Manager. |

## DMA-SA Diagnostic Report

### DMA-SA (Domain Manager Adapter - Service Assurance)

The following table outlines the diagnostic reports for the DMA-SA service.

DMA-SA Diagnostic Properties

| Property Name | Property Value Description |
|---|---|
| Default | No service specific info available |
| Total devices | The total number of devices |
| Devices Provisioned Successfully | The total number of devices successfully provisioned |
| Devices Pending | The total number of devices in the process of being provisioned |
| DmReceiver Queue | The number of messages the dispatcher (an internal component of DMA-SA) has received and yet to process |
| SDR CNF in service | SDR CNF (Change Notification Framework) must be in service for this component to work. If the value is false, then something is wrong and new users cannot be added |
| Total Pushed Entities | The total number of users |
| Provisioned Successfully | The total number of users successfully provisioned |
| Pending | The total number of users in the process of being provisioned |
| Receiver Queue | The number of messages the dispatcher (an internal component of DMA-SA) has received and yet to process |
| Devices | The number of devices configured on the HCM-F to be monitored by this Prime Collab out of the maximum devices allowed to be monitored by a single Prime Collab |

| Property Name | Property Value Description |
|---|---|
| Customers | The number of customers configured on the HCM-F with devices to be monitored by this Prime Collab out of the maximum customers allowed for a single Prime Collab |
| Subscribers | is the number of registered end-user subscribers on all the call managers monitored by this Prime Collab out of the maximum allowed. |
| Items In Progress | is the number of devices that are currently in the process being added to or removed from this Prime Collab. |

## Fulfillment Diagnostic Report

### Fulfillment

The following tables outline the diagnostic report for the Cisco HCS Fulfillment service.

***Table 14: Session Pool Manager***

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |
| Session Name | The name of the session created for this pool. |
| Min Sessions | The minimum number of sessions for this pool. |
| Max Sessions | The maximum number of sessions for this pool. |
| Allocated Sessions | The number of sessions allocated for this pool. |
| Max Allocated Sessions | The maximum number of allocated sessions allowed for this pool. |
| Periodic Time to test DB (ms) | The time in milliseconds to retest the database connection. |
| Free Sessions | The number of free sessions in the pool. |
| Used Sessions | The number of used sessions in the pool. |
| Stale Sessions | The number of stale sessions in the pool. |
| Rebuild Session Pool count | The number of times the pool has been rebuilt. |
| Pool Starter last ran | The time and date that the pool starter was last ran. This indicates when the pool noticed the database was down. |

| Property Name | Property Value Description |
|---|---|
| Stale Session Reader last ran | The time and date that the stale session reader was last ran. This indicates when the pool noticed the database was down. |

*Table 15: Service Level Information*

| Property Name | Property Value Description |
|---|---|
| Derby Status | The current status of the Derby status seen by this agent. |
| SDR Status | The status of SDR seen by this agent. |
| CHPA Status | The status of the CHPA service seen by this agent. |
| DMASA Status | DMASA status monitored by Fulfillment. |
| SDRCNF Status | SDRCNF status monitored by Fulfillment. |
| Expected Number of Agents | The expected number of active agents in Fulfillment Service. |
| Number of active agents | The actual number of active agents in Fulfillment Service. |

*Table 16: Fulfillment Diagnostics Status Count*

| Property Name | Property Value Description |
|---|---|
| GREEN | The number of agents whose status is GREEN (no issues). |
| YELLOW | The number of agents whose status is YELLOW (minor issues encountered, but nothing alarming or show-stopping. |
| RED | The number of agents whose status is RED (major issues have been encountered). |
| Total Count | The total number of agents that exist in Fulfillment Service. |

*Table 17: Fulfillment Job Status Count*

| Property Name | Property Value Description |
|---|---|
| <current job status; field entry will vary. Example: NO JOB> | The number of agents whose job is in that state. |
| Total Count | A count of all agents, with or without jobs. |

*Table 18: Fulfillment Diagnostics Status Agents List*

| Property Name | Property Value Description |
|---|---|
| GREEN | Names of agents whose status is GREEN. |
| YELLOW | Names of agents whose status is YELLOW. |
| RED | Names of agents whose status is RED. |

*Table 19: Fulfillment Job Status Agents List*

| Property Name | Property Value Description |
|---|---|
| <current job status; field entry will vary. Example: NO JOB> | The list of agents whose job is in that state. |

The following tables outline the diagnostic report for Cisco HCS Fulfillment service SDR Link Agent Route Builder

*Table 20: SDR Link Agent Route Builder Properties*

| Property Name | Property Value Description |
|---|---|
| Status | Status of the application. |
| Number of Agents | Number of agents associated to the application. |

The following table outlines the diagnostic report for the Cisco HCS Fulfillment application properties, for example the ESXi Host Blade, Customer, Cisco Prime Unified Operations Manager, or Application Instance Virtual Machine properties.

*Table 21: Application Properties*

| Property Name | Property Value Description |
|---|---|
| Audit List Size | The number of links that the agent needs to retry. |

*Table 22: ApplicationInstanceVirtualMachine Auto Linked Status*

| Property Name | Property Value Description |
|---|---|
| Application Configured for Manual VM Link | The number of application instances and virtual machines that have been configured to be manually linked. |

| Property Name | Property Value Description |
|---|---|
| Application Configured for Auto-VM Link | The number of application instances and virtual machines that have been configured to be auto linked. |
| Application Auto Linked to VM | The number of application instances and virtual machines that have been auto linked. |
| Application NOT Auto Linked to VM | The number of application instances and virtual machines that could not be auto linked. |
| List of Applications Configured for Manual VM Link | The list of application instances and virtual machines that have been configured to be manually linked. |
| List of Applications Configured for Auto VM Link | The list of application instances and virtual machines that have been configured to be auto linked. |
| List of Applications Auto Linked to VM | The list of application instances and virtual machines that have been auto linked. |
| List of Applications NOT Auto Linked to VM | The list of application instances and virtual machines that could not be auto linked. |

## HLM Diagnostic Report

### Cisco HCS License Manager Service

The following tables outline the diagnostic report for the Cisco HCS License Manager service.

***Table 23: HCS License Manager Properties***

| Property Name | Property Value Description |
|---|---|
| Last Audit Performed | Date and time that the last audit was performed. |

***Table 24: HLM Core Agent Specific Properties***

| Property Name | Property Value Description |
|---|---|
| HCM-F Global Deployment Mode | The deployment mode of the HCM-F. |
| # of License Managers | The number of License Managers. |
| # of Assigned Clusters | The number of assigned clusters. |

## NBI Diagnostic Report

### Cisco HCS North Bound Interface Web Service

The following tables outline the diagnostic reports for the Cisco HCS North Bound Interface Web service.

*Table 25: NBI Web Services Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |

*Table 26: Session Pool Manager Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |
| Session Name | The name of the session created for this pool. |
| Min Sessions | The minimum number of sessions for this pool. |
| Max Sessions | The maximum number of sessions for this pool. |
| Allocated Sessions | The number of sessions allocated for this pool. |
| Max Allocated Sessions | The maximum number of sessions allowed to be allocated for this pool. |
| Periodic Time to test DB (ms) | The time in milliseconds to retest the database connection. |
| Free Sessions | The number of free sessions in pool. |
| Used Sessions | The number of used sessions in pool. |
| Stale Sessions | The number of stale sessions in pool. |
| Pool Starter last ran | The time and date that the pool starter was last ran. This indicates when the pool noticed the database was down. |
| Stale Session Reader last ran | The time and date that the stale session reader was last ran. This indicates when the pool noticed the database was down. |

## NBIRESTFF Diagnostic Report

### North Bound Interface REST FF Diagnostic Report

The following table outlines the diagnostic report for the North Bound Interface REST FF web service.

*Table 27: NBI Web Services Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |

*Table 28: Session Pool Manager Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |
| Session Name | The name of the session created for this pool. |
| Min Sessions | The minimum number of sessions for this pool. |
| Max Sessions | The maximum number of sessions for this pool. |
| Allocated Sessions | The number of sessions allocated for this pool. |
| Max Allocated Sessions | The maximum number of sessions allowed to be allocated for this pool. |
| Periodic Time to test DB (ms) | The time in milliseconds to retest the database connection. |
| Free Sessions | The number of free sessions in pool. |
| Used Sessions | The number of used sessions in pool. |
| Stale Sessions | The number of stale sessions in pool. |
| Pool Starter last ran | The time and date that the pool starter was last ran. This indicates when the pool noticed the database was down. |
| Stale Session Reader last ran | The time and date that the stale session reader was last ran. This indicates when the pool noticed the database was down. |

## NBIRESTSDR Diagnostic Report

### North Bound Interface REST SDR Diagnostic Report

The following table outlines the diagnostic report for the North Bound Interface REST SDR web service.

*Table 29: NBI Web Services Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |

*Table 30: Session Pool Manager Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the web service has been running. |
| Session Name | The name of the session created for this pool. |
| Min Sessions | The minimum number of sessions for this pool. |
| Max Sessions | The maximum number of sessions for this pool. |
| Allocated Sessions | The number of sessions allocated for this pool. |
| Max Allocated Sessions | The maximum number of sessions allowed to be allocated for this pool. |
| Periodic Time to test DB (ms) | The time in milliseconds to retest the database connection. |
| Free Sessions | The number of free sessions in pool. |
| Used Sessions | The number of used sessions in pool. |
| Stale Sessions | The number of stale sessions in pool. |
| Pool Starter last ran | The time and date that the pool starter was last ran. This indicates when the pool noticed the database was down. |
| Stale Session Reader last ran | The time and date that the stale session reader was last ran. This indicates when the pool noticed the database was down. |

## SDRCNF Diagnostic Report

### SDRCNF AgentRouteBuilder Properties

The following tables outline the diagnostic reports for the Cisco HCS SDR Change Notification service

*Table 31: Service Level Properties*

| Property Name | Property Value Description |
|---|---|
| SDRCNF AgentRouteBuilder Status | The current health of the service (Red, Yellow, or Green) based on its ability to produce and send notifications. |
| Recommended Action | The action recommended to repair the service if the status is Yellow or Red. This is based on the results of service initialization, checking the SDR status, and automatically auditing the service. |
| Start Time | Provides a timestamp of when the service was started. |
| Up Time | The amount of time the service has been running. |
| Configured SDRCNF Agents | The number of agents configured to handle incoming subscription requests. |
| Device AgentInstanceMap Size | The number of SDRCNF agents in operation. |
| SDR Status | The status of SDR. If not healthy, the service will not be able to produce notifications and will be placed in the RED state. |
| Last Audit Time | Provides a timestamp of when the last service audit was executed. |
| Last Audit Result | Provides the result of the last audit (success or failure). |
| Last Audit Error | Details the error if the last audit failed. |

*Table 32: Resource Properties*

| Property Name | Property Value Description |
|---|---|
| Sessions | The number of SDR sessions used to create subscriptions. |
| Subscriptions | The number of independent subscriptions to change notifications. |
| Subscription Specifications | The number of unique sets of subscriptions. Many subscriptions can share the same specification. |
| Triggers | The number of database triggers currently active for the service. |
| Dynamic Topics | The number of messaging topics created to send change notifications to the subscribers. |

*Table 33: Processor Properties*

| Property Name | Property Value Description |
|---|---|
| Transaction Chunks | The number of transaction chunks from the database waiting to be processed. |
| Ready Transactions | The number of ready transactions waiting to be processed. |

| Property Name | Property Value Description |
|---|---|
| Ready Notifications | The number of notifications waiting to be sent to subscribers. |

*Table 34: Agent Level Properties*

| Property Name | Property Value Description |
|---|---|
| Agent Instance ID | Internal Id of the agent. |
| Agent Status | Signifies the health of the agent; options are Red, Yellow, or Green. |
| Creation Time | Provides a timestamp of when the agent was configured. |
| Total Success | The total number of successful subscription requests handled by this agent. |
| Total Failures | The total number of failed subscription requests handled by this agent. |
| Last Success Time | Date and time of the last failed subscription request. |
| Last Failure Time | Date and time of the last failed subscription request. |
| Last Failure Reason | The reason for the last failure subscription request. |
| Last Failure (Recommended Action) | The recommended action to repair the last failed subscription request. |

## SI Diagnostic Report

### Cisco HCS Service Inventory

The following tables outline the diagnostic report for the Cisco HCS Service Inventory services.

*Table 35: SI Status*

| Property Name | Property Value Description |
|---|---|
| Date of Last Report | The day and time of the last report. Also shows if the report has not been run yet. |
| Status of Last Report | Whether the report succeeded or failed. |
| Alarm Code | The type of failure/alarm if the report failed. |

*Table 36: SI Agent Route Builder Properties*

| Property Name | Property Value Description |
|---|---|
| Start Time | The day and time that the SI Agent Route Builder started. |

| Property Name | Property Value Description |
|---|---|
| Up Time | The total time (hh:mm:ss) that SI Agent Route Builder has been up. |

*Table 37: SI General Agent Properties*

| Property Name | Property Value Description |
|---|---|
| Agent Status | Agent Status options are Green or Red. |
| Start Time | The day and time that the SI General Agent started. |
| Up Time | The total time (hh:mm:ss) that SI General Agent has been up. |

*Table 38: SI Scheduler Properties*

| Property Name | Property Value Description |
|---|---|
| Scheduler Enabled | Whether or not the scheduler is enabled. |
| Current State | The current state may be Idle or Active. |
| Report Execution Time | The time the report ran (24-hour mode). |
| Report End Time | SI reports on provisioning up until this time. |
| Report Version | The software version for which the report is run. |

*Table 39: SI General Properties*

| Property Name | Property Value Description |
|---|---|
| Number of Backup Days | The number of days for which Backup occurs. |
| Custom Report Enabled | Whether or not Custom Report is enabled. |
| Backup File Count | The number of backup files created. |

*Table 40: SI Host Properties*

| Property Name | Property Value Description |
|---|---|
| SI Host | The name of the SI Host. |
| SI Port | The number of the SI port in use. |
| SI User | The name of the SI user. |

*Table 41: SI SFTP Host Properties*

| Property Name | Property Value Description |
|---|---|
| SFTP Host | The name of the SFTP Host. |
| SFTP Port | The number of the SFTP port in use. |
| SFTP User | The name of the SFTP user. |
| SFTP Destination Path | The SFTP Destination Path. |
| SFTP Max File Size | The maximum SFTP file size allowed. |
| SFTP Retry Count | A count of the number of SFTP retries. |

*Table 42: SI UC App Data Collection Manager Properties*

| Property Name | Property Value Description |
|---|---|
| Total Customers to Process | The total number of UC Customers the UCDCM is processing. |
| Number Message Managers | The number of Message Managers available for processing. |
| Number Messages per Manager | The number of messages a Message Manager can handle at a time. |

## UCPA Diagnostic Report

### UCPA Agent Properties

The following tables outline the diagnostic report for the Cisco HCS Unity Connection Provisioning Adapter service.

*Table 43: UCPA AgentRouteBuilder Properties:*

| Property Name | Property Value Description |
|---|---|
| ucpa AgentRouteBuilder Status | Signifies the health of the agent; options are Red, Yellow, or Green. |
| Recommended Action | Recommended action to correct last failure. If "Unknown," then no failures to report. |
| Configured ucpa Agents | The number of UCPA Agents configured. |
| Device AgentInstanceMap Size | The number of application instances managed. |

*Table 44: UCPA Agent Properties:*

| Property Name | Property Value Description |
|---|---|
| Agent Instance Id | Internal Id of the agent. |
| Agent Status | Signifies the health of the agent; options are Red, Yellow, or Green. |
| Creation Time | Date and time the agent was created. |
| Total Success | Total number of requests sent to application instances that were successful. |
| Total Failures | Total number of requests sent to application instances that were un-successful. |
| Last Success Time | Date and time the last successful request was made to an application instance. |
| Last Failure Time | Date and time the last unsuccessful request was made to an application instance. If this time is equal to the agent's creation time, then no failures have occurred. |
| Last Failure Reason | The reason for the last failure. If "Unknown," then no failures to report. |
| Last Failure (Recommended Action) | Recommended action to correct last failure. If "Unknown," then no failures to report. |

## UCSMSync Diagnostic Report

### Cisco HCS UCSMSync

The following table outlines the diagnostic report for the Cisco HCS UCSMSync service.

*Table 45: UCSManager Sync Agent Properties*

| Property Name | Property Value Description |
|---|---|
| Name | The name of the Cisco Unified Communications Manager. |
| Auto-sync | Signifies if the status of Cisco Unified Communications Manager auto-sync, options are Enabled or Disabled. |
| Overall Status | Signifies the health of the UCSMSync, options are Red, Yellow, or Green. |
| Status Info | Job status information for the UCSMSync, field is empty if no job has started for this application. |

| Property Name | Property Value Description |
|---|---|
| Recommended Action | Job recommended action for the UCSMSync, field is empty if no job has started for this application. |
| Status Details | Displays any status details, field is empty if no job has started for this application. |
| FSM State | Displays the state of the FSM. |
| Retry timer | Displays the state of the retry timer. |
| ConnectionCheck timer | Displays the state of the connection check timer. |
| UCSManager Connection | The URL used to connect to the UCS manager. |
| SDR Connection | The URL used to connect to the database. |
| Messages received | Number of messages received. |
| Diag Level | The diag level for the report. |

## VcenterSync Diagnostic Report

### Cisco HCS VCenterSync

The following table outlines the diagnostic report for the Cisco HCS VCenterSync service.

***Table 46: VCenter Sync Agent Properties***

| Property Name | Property Value Description |
|---|---|
| Name | The name of the vCenter. |
| Auto-sync | Signifies if the status of vCenter auto-sync, options are Enabled or Disabled. |
| Overall Status | Signifies the health of the VCenterSync, options are Red, Yellow, or Green. |
| Status Info | Job status info for the VCenterSync, field is empty if no job has started for this application. |
| Recommended Action | Job recommended action for the VCenter Sync, field is empty if no job has started for this application. |
| Status Details | Displays any status details, field is empty if no job has started for this application. |
| FSM State | Displays the state of the FSM. |
| Retry timer | Displays the state of the retry timer. |
| ConnectionCheck timer | Displays the state of the connection check timer. |
| VCenter Connection | The URL used to connect to the vCenter. |

| Property Name | Property Value Description |
|---|---|
| SDR Connection | The URL used to connect to the database. |
| Messages received | Number of messages received. |
| Diag Level | The diag level for the report. |

## HCS License Manager for Cisco HCM-F

### Software Requirements

Cisco HCS License Manager requires the following software to perform licensing management:

- Cisco Hosted Collaboration Mediation Fulfillment 10.1(1) or later release
- Enterprise License Manager 9.x
- Prime License Manager 10.0 or later release
- Cisco Unified Communications Manager 9x or later release
- Cisco Unity Connection 9x or later release

**Note** Cisco Unified Communications Domain Manager is not required. However it is convenient for the users to sync all of the provisioned customers and UC clusters from Cisco Unified Communications Domain Manager to SDR before performing any Cisco HCS license operation.

### License Management Overview

**Note** In this document, the term License Manager refers to both Enterprise License Manager and Prime License Manager.

HLM runs as a stand-alone Java application on the Hosted Collaboration Mediation Fulfillment platform, utilizing Cisco Hosted Collaboration Mediation Fulfillment service infrastructure and message framework. There is one HLM per install of Cisco HCS. HLM and its associated License Manager manage licenses for Cisco Unified Communications Manager, Cisco Unity Connection, and TelePresence Room.

**Note** There is no licensing requirement for Presence Service and Cisco Unified Communications Manager IM.

HLM requires that you set the Cisco HCS global deployment mode before you can create a License Manager instance in the Cisco HCS space. The Cisco HCS global deployment mode must be either Cisco HCS, Cisco HCS-Large Enterprise (HCS-LE) or Enterprise for Enterprise Agreement. The global deployment mode enforces that every assigned License Manager instance and assigned cluster must have the same deployment

mode. You cannot change the global deployment mode if there is still a License Manager instance in the Cisco HCS space.

Through the Cisco Hosted Collaboration Mediation Fulfillment NBI or GUI, an administrator can create, read, or delete a License Manager instance in Cisco HCS. A Cisco Hosted Collaboration Mediation Fulfillment administrator cannot perform any licensing management function until HLM validates its connection to the installed License Manager and its license file is uploaded. HLM exposes an interface to list all of the License Manager instances.

After the administrator successfully adds and validates a License Manager instance to the HLM, one can assign a customer to the License Manager. This action does not make all CUCM and CUC 9.x clusters within this customer to be assigned to that License Manager automatically. The administrator must assign each of the customer's CUCM or CUC 9.x cluster to an License Manager after the associated customer is assigned to that License Manager. If the customer is not assigned to any License Manager, the cluster assign fails, and the user is advised to associate the customer with an License Manager first.

The administrator can unassign a UC cluster from a License Manager through the HLM NBI or GUI.

For more information about Prime License Manager see *Cisco Prime License Manager User Guide*.

HLM supports License Report generation. The report includes all customers on the system with aggregate license consumption at the customer level.

**Note** Customers that are assigned to Enterprise Licensing Manager 9.0 are not reported. The license usage of 9.0 clusters that are assigned to Enterprise Licensing Manager 9.1 is not counted in the report either.

An optional field **Deal ID** at the customer level is included in the report. Each customer has zero or more Deal IDs that can be configured through the HCM-F GUI.

The Administrator requests the system-level Cisco HCS license report through the HLM GUI or NBI. The report request generates two files: csv, and xlsx format. Both files are saved into the HLM license report repository (/opt/hcs/hlm/reports/system) for future download. The retention period of the report is set to 60 days by default.

## Inter-Component Relationships

**Note** Ensure you sync the customer and cluster data into the SDR before performing any license operations.

### *CUCDM Sync*

HLM retrieves customer and UC cluster information from the SDR. The cluster version must be 9.0.1 or higher for HLM to import that cluster. You can update this data by a scheduled CUCDM-sync (highly recommended), a manual CUCDM-sync, or through manual provisioning using the Cisco Hosted Collaboration Mediation Fulfillment GUI or NBIs.

### Restrictions

The following restrictions apply:

- Only stand-alone License Manager is supported. Co-resident License Manager is not supported in HCS.
- The maximum cluster capacity of an Enterprise License Manager is 200.
- The maximum cluster capacity of a Prime License Manager is 1000.

- A License Manager instance cannot be created in the Cisco HCS space without a valid connection to the installed License Manager.
- A License Manager instance cannot be created in Cisco HCS if the installed License Manager has a demo license installed.
- A Cisco Unified Communication IM and Presence Service cluster cannot be assigned to a License Manager.
- An 8.x UC cluster cannot be assigned to a License Manager.
- Unity Connection 9.0(1) FCS is not supported with HLM. The user should install Cisco Unity Connection 9.0(1)ES1 or later release.
- The Cisco HCS license report retention period is set to 60 days by default. The value can be set through CLI with minimum = 1 and maximum = 120.
- The audit interval is set to four hours by default. The value can be changed through CLI with minimum = 4 and maximum = 24.
- The license report does not display the license usage of a customer that is associated with a 9.0 Enterprise License Manager. The report does not count the license usage of a customer's 9.0 clusters that are assigned to an Enterprise License Manager 9.1.

## UC Solution Impacts and Dependencies

### CUCM Interactions

- Verify and start, if necessary, the Platform Administrative Web Service in the CUCM cluster publisher.
- Configure the platform credential of the publisher.

**Note** Platform credentials are equal to the CUCM OS admin user credentials.

- If the cluster's platform credential is not found, HLM uses the default credential if one is configured.

### Unity Connection Interactions

- Verify and start, if necessary, the Platform Administrative Web Service in the CUC cluster publisher.
- Configure the platform credential of the publisher.

**Note** Platform credentials are equal to the CUC OS admin user credentials.

- If the cluster's platform credential is not found, HLM uses the default credential if one is configured.

## Limitations

- Changing an License Manager hostname or IP Address is not supported in HLM. The user is required to remove all of the clusters of the License Manager, delete the License Manager from the Cisco HCS space, then recreate a License Manager with the correct hostname or IP address.
- HLM auditing validates the connection between the License Manager instance and the installed License Manager. However, it is the Cisco Hosted Collaboration Mediation Fulfillment Administrator's responsibility to remove the License Manager instance from HLM after uninstalling the actual License Manager.

## HCS Licensing Operations

The following are the licensing operations that a user performs through HLM:

### Get/Set HCS Global Deployment Mode

Cisco HCS Global Deployment mode must be set before any HLM licensing operation is performed. The value can be either **HCS**, **HCSLE** or **Enterprise**. You can set the global deployment mode through either HLM NBI setHLMGlobalDeploymentMode or Cisco Hosted Collaboration Mediation Fulfillment License Management Setting page. The global deployment mode cannot be changed if there is still an License Manager in Cisco HCS space.

### Prime License Manager Related Operations

You can add a new License Manager instance by specifying its name, hostname, OS Administration ID, and password through either HLM NBI createPLM or **License Management >License Management Summary** page. The creation is not allowed if the connection test to the actual installed License Manager fails or the license file is still not uploaded (demo licensing). This create operation enforces the installed License Manager having the same deployment mode to Cisco HCS global deployment mode.

You can edit the version from the drop-down menu on the GUI or through NBI updatePLM to sync with the installed License Manager version.

You can remove an License Manager through either the HLM NBI deletePLM or **License Management >License Management Summary** page. You must unassign all of the clusters within an License Manager before the License Manager can be deleted. The delete operation removes the License Manager instance in Cisco HCS space, and resets the installed License Manager deployment mode to Enterprise.

### Cluster Assign/Un-Assign Operations

The Administrator can assign an eligible UC cluster to an License Manager through the HLM NBI assignCluster by specifying the cluster name and License Manager name, or by using the Cisco Hosted Collaboration Mediation Fulfillment GUI.

After the Administrator successfully assigns a cluster to an License Manager, the corresponding job is updated with status = Succeeded and a description like assigning cluster abc-cluster to License Manager xyz-plm succeeded. The assigned UC cluster's deployment mode is set to Cisco HCS global deployment mode and a new product instance is created in the License Manager inventory section. For failed assigning operations, the job is updated with status = Failed and a description like Assigning cluster abc-cluster to License Manager xyz-plm failed: fail reason.

The Administrator can unassign a cluster from an License Manager through either the HLM NBI or GUI.

After the Administrator successfully unassigns a cluster from a License Manager, the corresponding job is updated with status = Succeeded and a description like Unassigning cluster abc-cluster from License Manager xyz-plm succeeded. The unassigned UC cluster's deployment mode is reset to Enterprise and its product instance is removed from the License Manager inventory section. For failed operations, the job is updated with status = Failed and a description like Unassigning cluster abc-cluster from License Manager xyz-plm failed: fail reason.

**Note** Cluster assign and unassign operations are considered asynchronous. After receiving the request, HLM responds with a job ID before performing any licensing function. After the job is complete, HLM updates the job table in SDR with the result, such as Succeeded or Failed, and a detailed description of the operation. It usually takes about 30 to 40 minutes to complete a UC cluster assign/unassign operation. Due to the longevity of each cluster assign/unassign operation, you should not run more than 5 parallel jobs at any time to avoid potential deployment mode mismatch between UC clusters and Prime License Managers.

#### Update an Assigned Cluster's Credential

If the OS Admin credential of an assigned cluster is changed, you should reflect this change in both HLM and License Manager through the HLM NBI updateAssignedCluster with the cluster name, License Manager name, and the changed credential.

Or go into Cisco Hosted Collaboration Mediation Fulfillment GUI, locate the assigned cluster's publisher in **Application Management >Cluster Application**, then change its platform credential. Log into License Manager, find the assigned cluster in inventory, then change the credential.

#### Sync License Manager Operation

You can sync a License Manager version in HLM after the installed License Manager version is successfully switched. Go to the **PLM Edit** and click **sync** to retrieve the currently installed License Manager version.

#### Customer Deal ID

You can add, update, or delete the Deal IDs by editing the Deal IDs field in the GUI.

#### Generate HCS License Reports

Click **Request New Report** to create two HCS system-level license reports in csv and xslx format. The files should be saved to the HCS license report directory.

#### List and Download HCS License Reports

All of the Cisco HCS license reports in the repository are displayed with file name, date, and size. You can select one file at a time to download to your desktop.

## HCS License Report

### *HCS License Reports*

In HLM 10.x,, license reports displays 9.x and 10.x license versions. HLM supports system level license report generation. The report includes all customers on the system with aggregate license consumption at customer level. It supports deployment with one or multiple UC clusters and License Managers. Optional field "Deal ID" at the customer level is included in the report. Each customer has zero to multiple Deal IDs that can be configured through the Cisco Hosted Collaboration Mediation Fulfillment GUI. The Deal ID field

is free text format. Deal ID(s) come from a Cisco Account Manager who works with the service provider to develop Cisco HCS business with the specific customer. Entering the Deal IDs makes this report more useful to the service provider's business personnel responsible for monthly POS reporting to Cisco.

Request the Cisco HCS license report through the Cisco Hosted Collaboration Mediation Fulfillment GUI. The report request will generate two files: one is in csv, the other one is in xlsx format. Both files will be saved into the HLM license report repository for future download. The retention period of the report is set to 60 days by default.

The naming convention of a system level Cisco HCS license report is LicenseReport_ALL_YYYYMMDD_hhmmss.csv/xlsx , see the following examples:

- LicenseReport_ALL_20140319_185023.csv
- LicenseReport_ALL_20140319_185023.xslx

## Audit

HLM auditing is run every four hours by default to check to see if the clusters in SDR match the clusters found in an associated License Manager. There are three scenarios that can occur from this check:

1. The clusters in License Manager and SDR match and no further action needs to be taken.
2. SDR reports an additional cluster assigned to a License Manager that the License Manager does not have provisioned. In this case, HLM sends out a HLMAuditWarning alarm and adds the missing cluster(s) to the License Manager.
3. License Manager reports an additional cluster assigned to it, yet this cluster is not assigned by SDR. In this case HLM sends out a HLMAuditWarning alarm and informs the administrator to manually remove the cluster from the License Manager and to assign it through the HLM service.

After HLM auditing finishes checking for Cluster List matching, it verifies credentials for every assigned cluster provisioned in SDR and ensures that the credentials for the cluster provisioned in License Manager match.

If a mismatch is detected, HLM auditing updates the cluster credentials in License Manager to match those of SDR, keep SDR the master record. It then sends out a HLMAuditingWarning alarm noting the disparity. This happens if the username, password, or both mismatch.

This also covers the case where the Cisco HCS administrator updates the cluster credentials in SDR but does not update the assigned cluster's credentials through HLM. HLM auditing eventually detects the disparity and corrects this automatically after the auditing has run.

HLM auditing compares the version of the installed License Managers to the Prime License Manager instances in SDR. If a version mismatch is detected, HLM updates the License Manager version in SDR according to the version value of the installed Prime License Manager.

The auditing interval is set through the CLI with a value between 4 and 24 hours. The new audit interval value will be effective immediately once HLM receives the corresponding change notification. No service restart is needed to make the new interval value become effective. HLM auditing also adds a new function to check license report disk space usage. If the report repository disk space exceeds the configured value, a warning alarm HLMDiskSpaceAllotmentExceeded is sent out.

# Cisco HCM-F Real-Time Monitoring Tool

Cisco Hosted Collaboration Mediation Fulfillment (Cisco HCM-F) Real-Time Monitoring Tool (RTMT) runs as a client-side application and uses HTTPS to monitor system performance. Real-Time Monitoring Tool can connect directly to a device through HTTPS to troubleshoot system problems. Tasks such as alarm and performance monitoring updates continue to run on the server in the background even when RTMT is not connected to the server.

The Cisco Hosted Collaboration Mediation Fulfillment installation consists of one application server and may contain one or more Web Services (WS) servers. While the Real-Time Monitoring Tool can provide troubleshooting support for more than one server, you can monitor only one server in each Real-Time Monitoring Tool session

**Note** It is possible to launch more than one Real-Time Monitoring Tool session (for example, one session is connected to the Cisco Hosted Collaboration Mediation Fulfillment application server and another session is connected to an Cisco Hosted Collaboration Mediation Fulfillment Web Services server). However, multiple Real-Time Monitoring Tool sessions are not recommended by Cisco.

Real-Time Monitoring Tool allows you to perform the following tasks:

- Monitor a set of predefined management objects and performance counters that monitor the health of the server to which the Real-Time Monitoring Tool is connected.
- Configure and update alert settings for the management objects and performance counters (in the form of email messages).

  The Cisco Hosted Collaboration Mediation Fulfillment server monitors the alert conditions and generates alerts when values exceed the range defined by user-configured thresholds. The Real-Time Monitoring Tool does not need to be running on your computer in order for alerts to be generated by the server. Alerts are displayed in the Real-Time Monitoring Tool in the form of alert logs and in Alert Central.
- Collect and download or view traces and logs.
- View syslog messages in SysLog Viewer.

## Performance Monitoring

Cisco Hosted Collaboration Mediation Fulfillment updates performance monitor (perfmon) counters which contain simple, useful information about the system. You can use RTMT to monitor the performance of system components and applications by selecting, for any object, the counters to monitor. The counters available for each object are shown when you expand the object folder. RTMT periodically polls the selected counters to display data for those counters. RTMT also provides alert notifications for troubleshooting performance.

RTMT allows you to perform the following performance monitoring tasks:

- Continuously monitor a set of preconfigured objects.
- Associate counter threshold settings to alert notification. An email or popup message provides notification to the administrator.
- Save and restore settings, such as counters being monitored, threshold settings, and alert notifications, for customized troubleshooting tasks.

- Display up to six perfmon counters in one chart for performance comparisons.
- Group perfmon counters into categories, to help you troubleshoot specific performance, system, or device problems.
- Log perfmon counters locally on your computer.
- View the local or server-based performance logs.

## Performance Counter Interface

RTMT contains ready-to-view, predefined performance counters. You can also select and add counters to monitor in RTMT using performance queries.

RTMT displays performance counters in chart or table format. Chart format presents a miniature window of information. You can display a particular counter by double-clicking the counter in the perfmon monitoring pane.

Attributes for predefined performance counters, such as format and category, remain fixed. You can define attributes for counters that you configure in RTMT. Because chart view represents the default, you can configure the performance counters to display in table format when you create a category.

### *Category Tabs*

A category comprises a group of monitored performance counters. A tab in the RTMT monitoring pane contains the category name. All performance counters that are monitored in this tab belong to a category. RTMT displays any categories that you access during a RTMT session in the bottom toolbar.

The system polls the performance counters in the tab at the same rate, with each category configured to have its own polling rate.

You can create custom categories in the RTMT monitoring pane to view information that helps you troubleshoot specific performance, system, or device problems. If your system is experiencing performance problems with specific objects, create custom categories to monitor the performance of the counters within the object. If the system is experiencing problems with specific devices, create custom categories to monitor the devices in your system. In addition, you can create alert notifications for counters and gateways in these custom categories. To create custom categories, you add a new category tab. When the tab is created, you specify the specific performance counters, devices, and alerts within that tab and then save your custom category by using Profile.

### *Sample Rate*

The application polls the counters, devices, and gateway ports to gather status information.

The polling rate in each precanned monitoring window remains fixed, and the default value specifies 30 seconds. If the collecting rate for the AMC (Alert Manager and Collector) service parameter changes, the polling rate in the precanned window also updates. In addition, the local time of the RTMT client application and not the backend server time, provides the basis for the time stamp in each chart. For more information on Service Parameters, refer to *System Configuration Guide for Cisco Unified Communications Manager* or *Cisco Unity Connection System Administration Guide*.

In the RTMT monitoring pane, you configure the polling intervals for the applicable performance counters, devices, and gateway ports for each category tab that you create.

**Note** High-frequency polling rate affects the performance on the server. The minimum polling rate for monitoring a performance counter in chart view equals 5 seconds; the minimum rate for monitoring a performance counter in table view equals 1 second. The default for both specifies 10 seconds.

### *Zoom In on Perfmon Counter*

To get a closer look at perfmon counters, you can zoom in on a perfmon monitor counter in the RTMT.

**Procedure**

**Step 1** To zoom in on a counter, perform one of the following tasks:

- To zoom in predefined objects, such as System Summary, perform one of the following actions:
  - Drag the mouse over the plot area in the counter to frame the data and release the mouse button. The counter zooms in the chart.
  - Click the counter. The counter zooms in.
- To zoom counters in the Performance pane, perform one of the following actions (and resize the window, if necessary):
  - Double-click the counter that you want to zoom. The box with the counter appears highlighted and the Zoom window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.
  - Click the counter to select the counter to zoom. The box with the counter appears highlighted.
  - Right-click the counter and select **Zoom Chart** or choose **System** > **Performance** > **Zoom Chart**. The **Zoom** window launches. The minimum, maximum, average, and last fields show the values for the counter since the monitoring began for the counter.

**Step 2** To zoom out a counter, perform one of the following actions:

- To zoom out predefined objects, such as System Summary, click the counter and press **Z** in the active counter to return the counter to original size.
- To zoom out counters in the Performance pane, click **OK** to close the **Zoom** window.

### *Highlight Charts and Graphs*

The highlight feature helps to distinguish hosts and counters when multiple nodes or counters display on color-coded graphs. This feature is active in the System Summary, CPU and Memory, Disk Usage, and Performance Log Viewer windows.

**Procedure**

**Step 1** To highlight charts and graphs, perform one of the following tasks:

- To highlight charts and graphs for predefined objects, such as System Summary, right-click in a plot area to highlight the nearest data series or point.
- To highlight charts and graphs in the performance log viewer, perform one of the following tasks:
  - Right-click any color code in the table below the chart in the Performance Log Viewer and choose **Highlight** to highlight the data series for that counter.
  - Right-click any color code in the table below the chart in the Performance Log Viewer and choose **Change Color** to select a different color for the counter.

**Step 2** To return a highlighted item to its original appearance in the Performance Log Viewer, select another item to highlight.

*Counter Properties*

Counter properties allow you to display a description of the counter and configure data-sampling parameters.

The Counter Property window contains the option to configure data samples for a counter. The performance counters that display in the Unified RTMT performance monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option to view the data that a perfmon counter collected.

*Alert Notification for Counters*

When you activate the Alert Notification feature, the application notifies you of system problems. Perform the following configuration setup to activate alert notifications for a system counter:

1. From the RTMT Perfmon Monitoring pane, choose the system perfmon counter.
2. Set up an email or a message popup window for alert notification.
3. Determine the threshold for the alert (for example, an alert activates when calls in progress exceed the threshold of over 100 calls or under 50 calls).
4. Determine the frequency of the alert notification (for example, the alert occurs once or every hour).
5. Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

## Alerts for Cisco HCM-F

### RTMT Alerts

The system generates alert messages to notify the administrator when a predefined condition is met, such as when an activated service goes from up to down. The system can send alerts by email or e-page.

RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts). The Alert menu comprises the following menu options:

- Alert Central: This option comprises the history and current status of every alert in the system.

**Note** You can also access Alert Central in the QuickLaunch Channel by clicking **Tools** > **Alert Central**.

- Set Alert/Properties: This option allows you to create or modify alerts and alert properties.
- Remove Alert
- Enable Alert
- Disable Alert
- Suspend Cluster/Node Alerts: This option allows you to temporarily suspend alerts on a particular server.
- Clear Alert: This option allows you to reset an alert (change the color of an alert item to black) to signal that the alert has been handled. After an alert is raised, its color automatically changes in RTMT and stays that way until you manually clear the alert.

**Note** The manual clear alert action does not update the System Cleared Timestamp column in Alert Central. The column is updated only if the alert condition is automatically cleared.

- Clear all Alerts
- Reset All Alerts to Default Config: This option allows you to reset all the alerts to the default configuration.
- Alert Detail: This option allows you to view detailed information for alert events.
- Config Email Server: In this category, you can configure the email server to enable alerts.

**Note** To configure RTMT to send alerts using email, you must configure DNS.

- Config Alert Action: This option allows you to define the actions for specific alerts; you can configure the actions to send the alerts to specific email addresses.

In RTMT, you configure alert notification for performance monitor counter value thresholds and set alert properties such as the threshold, duration and frequency. RTMT predefined alerts are configured for performance monitor counter thresholds as well as event (alarm) notifications.

## Alert Central Displays

RTMT displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under the System, HCS, and Custom tabs.

You can enable or disable preconfigured and custom alerts in Alert Central; however, you cannot delete preconfigured alerts.

## Alert Fields

You can configure both preconfigured and user-defined alerts in RTMT. You can also disable both preconfigured and user-defined alerts. You can add and delete user-defined alerts; however, you cannot delete preconfigured alerts.

**Note** Severity levels for syslog entries match the severity level for all RTMT alerts. If RTMT issues a critical alert, RTMT identifies the corresponding syslog entry as critical.

The following table describes the fields that you can configure for each alert; users can modify preconfigured fields, unless otherwise noted.

***Table 47: Alert Customization***

| Field | Description | Comment |
|---|---|---|
| Alert Name | High-level name of the monitor item with which RTMT associates an alert | Descriptive name. For preconfigured alerts, you cannot modify this field. See topics related to Alert Central displays for a list of preconfigured alerts. |
| Description | Description of the alert | You cannot modify this field for preconfigured alerts. For a list of preconfigured alerts, See topics related to Alert Central. |
| Performance Counter(s) | Source of the performance counter | You cannot modify this field. You can associate only one instance of the performance counter with an alert. |
| Threshold | Condition to raise alert (value is...) | Specify up < - > down, less than #, %, rate greater than #, %, rate. This field is applicable only for alerts based on performance counters. |
| Value Calculated As | Method used to check the threshold condition | Specify value to be evaluated as absolute, delta (present - previous), or % delta. This field is applicable only for alerts that are based on performance counters. |
| Duration | Condition to raise alert (how long value threshold must persist before the system raises an alert) | Options include the system sending the alert immediately or after a specified time that the alert has persisted. This field is applicable only for alerts that are based on performance counters. |

| Field | Description | Comment |
|---|---|---|
| Number of Events Threshold | Raise alert only when a configurable number of events exceeds a configurable time interval (in minutes) | For ExcessiveVoiceQualityReports, the default thresholds are 10 to 60 minutes. For RouteListExhausted and MediaListExhausted, the defaults are 0 to 60 minutes. This field is applicable only for event-based alerts. |
| Alert Action ID | ID of alert action to take (system always logs alerts regardless of the alert action) | Alert action gets defined first. A blank field indicates that email is disabled. |
| Enable Alerts | Enable or disable alerts | Options include enabled or disabled. |
| Clear Alert | Resets alert (change the color of an alert item to black) to signal that the alert has been resolved | After an alert has been raised, its color automatically changes and stays that way until you manually clear the alert. Use Clear All to clear all alerts. |
| Alert Generation Rate | How often to generate an alert when alert condition persists | Specify every X minutes. (Raise alert once every X minutes if condition persists.)<br>Specify every X minutes up to Y times. (Raise alert Y times every X minutes if condition persists.) |
| User Provide Text | Administrator to append text on top of predefined alert text | N/A |
| Severity | For viewing purposes (for example, show only Severity 1 alerts) | Specify defaults that are provided for predefined (for example, Error, Warning, Information) alerts. |

## Alert Action Setup

In RTMT, you can configure alert actions for each alert that is generated and to send the alert action sent to email recipients that you specify in the alert action list.

The following table provides a list of fields that you use to configure alert actions. You can configure all fields, unless otherwise marked.

*Table 48: Alert Action Configuration*

| Field | Description | Comment |
|---|---|---|
| Alert Action ID | ID of alert action to take. | Enter a descriptive name. |
| Mail Recipients | List of email addresses. You can selectively enable or disable an individual email address in the list. | N/A |

## Automatic Trace Download Activation

Some preconfigured alerts allow you to initiate a trace download based on the occurrence of an event. You can automatically capture traces when a particular event occurs by checking the **Enable Trace Download** check box in Set Alert/Properties for the following alerts:

- CriticalServiceDown: This alert is generated when any service is down. The CriticalServiceDown alert monitors only those services that are listed in RTMT Critical Services.

**Note** The RTMT back-end service checks status (by default) every 30 seconds. If service goes down and comes back up within that period, the CriticalServiceDown alert may not be generated.

- CoreDumpFileFound: This alert is generated when RTMT back-end service detects a new Core Dump file.

**Note** You can configure both CriticalServiceDown and CoreDumpFileFound alerts to download corresponding trace files for troubleshooting purposes. This helps preserve trace files at the time of crash.

**Caution** Enabling Trace Download may affect services on the server. Configuring a high number of downloads will adversely affect quality of service on the server.

## Alert Logs

The alert log stores the alert, which is also stored in memory. The memory is cleared at regular intervals, leaving the last 30 minutes of data in memory. When the service starts/restarts, the system loads the last 30 minutes of the alert data into memory by reading from the alert logs on the server. The system sends alert data in the memory to the RTMT client on request.

Upon RTMT startup, RTMT shows all logs that occurred in the last 30 minutes (on just the server to which RTMT is connected) in the Alert History section of the Alert Central pane. The system updates the alert log periodically, and inserts new logs into the Alert History section. When the number of logs reaches 100, RTMT removes the oldest 40 logs.

The following file name format for the alert log applies: `AlertLog_MM_DD_YYYY_hh_mm.csv`.

The alert log includes the following attributes:

- Time Stamp: The time when RTMT logs the data
- Node: Server name for where RTMT raised the alert
- Alert Name: Descriptive name of the alert
- Severity: Severity of the alert
- Sent to: E-mail address to which the alert was sent
- Description: Description of the monitored object
- Alert Message: Detailed description about the alert
- Type: Type of the alert
- PollValue: Value of the monitored object where the alert condition occurred
- Action: Alert action taken
- Group ID: Identifies the source of the alert

The first line of each log file comprises the header. Details of each alert are written in a single line, separated by a comma.

## Log Partition Monitoring Tool Service

The Cisco Log Partition Monitoring Tool service, which is installed automatically with the system, uses configurable thresholds to monitor log partition disk usage on a server. The service starts automatically after system installation.

Every 5 minutes, the service uses the following configured thresholds to monitor log partition disk usage and the spare log partition on a server:

- LogPartitionLowWaterMarkExceeded (% disk space): When disk usage is above the percentage that you specify, the service sends an alarm message to syslog and an alert to RTMT Alert Central. To save the log files and regain disk space, you can use Trace & Log Central in RTMT.
- LogPartitionHighWaterMarkExceeded (% disk space): When disk usage is above the percentage that you specify, the service sends an alarm message to syslog and an alert to RTMT Alert Central.
- SparePartitionLowWaterMarkExceeded (% disk space): When disk usage is above the percentage that you specify, the service sends an alarm message to syslog and an alert to RTMT Alert Central. To save the log files and regain disk space, you can use Trace & Log Central in RTMT.
- SparePartitionHighWaterMarkExceeded (% disk space): When disk usage is above the percentage that you specify, the service sends an alarm message to syslog and an alert to RTMT Alert Central.

In addition, the Cisco Log Partition Monitoring Tool service checks the server every 5 seconds for newly created core dump files. If new core dump files exist, the service sends a CoreDumpFileFound alarm and an alert to Alert Central with information on each new core file.

To monitor the log partition, verify that the Cisco Log Partitioning Monitoring Tool service (a network service) is running on the Cisco HCM-F server. Stopping the service causes a loss of feature functionality.

When the service starts at system startup, the service checks the current disk space usage. If the percentage of disk usage is above the low-water mark, but below the high-water mark, the service sends an alarm message to syslog and generates a corresponding alert in RTMT Alert Central.

To configure the Cisco Log Partition Monitoring Tool service, set the alert properties for the LogPartitionLowWaterMarkExceeded and LogPartitionHighWaterMarkExceeded alerts in Alert Central.

To offload the log files and regain disk space on the server, use RTMT to collect the traces that you want to save.

If the percentage of disk usage is above the configured high-water mark, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark.

**Note** The Cisco Log Partition Monitoring Tool service automatically identifies the common partition that contains an active directory and an inactive directory. The active directory contains the log files for the current installed version of the software and the inactive directory contains the log files for the previous installed version of the software. If necessary, the service deletes log files in the inactive directory first. It then deletes log files in the active directory, starting with the oldest log file for every application until the disk space percentage drops below the configured low-water mark. The Cisco Log Partition Monitoring Tool service does not send an email when log partition monitoring purges the log files.

After the system determines the disk usage and performs the necessary tasks (sending alarms, generating alerts, or purging logs), log partition monitoring occurs at regular 5-minute intervals.

## Traces and Logs

### About Trace & Log Central

Trace & Log Central allows you to configure on-demand trace collection for a specific date range or absolute time. You can perform the following tasks:

- Collect trace files that contain search criteria that you specify and save the trace collection criteria for later use.
- Schedule a recurring trace collection and download the trace files to an SFTP or FTP server on your network.
- Collect a crash dump file.
- Edit the settings for traces on the server that you specify.

  **Note** Enabling trace settings decreases system performance; therefore, enable traces for troubleshooting purposes only.

- View the trace files in the appropriate viewer within RTMT or by using an external viewer.

  You can also view traces on the server without downloading the trace files by using the Remote Browse feature.

**Note** To use Trace & Log Central, ensure that RTMT can directly access the server without Network Access Translation (NAT). If NAT is set up to access devices, configure the servers with a hostname instead of an IP address and ensure that the hostnames and their routable IP addresses are in the DNS server or host file.

For devices that support encryption, the SRTP keying material does not appear in the trace file.

### Related Topics

Collect and Download Trace Files Using Query Wizard, on page 87

## Display RTMT Trace & Log Central Options

For each object listed in Trace & Log Central, you can perform the following tasks:

- Specify the services/applications for which you want traces.
- Specify the logs and servers that you want to use.
- Schedule a collection date and time.
- Configure the ability to download the files.
- Configure zip files.
- Delete collected trace files.

### Before You Begin

Cisco recommends that you import the certificates before you use the trace and log central option. If you do not import the certificates, the trace and log central option displays a security certificate for the server each time that you log in to RTMT and access Trace & Log Central. You cannot change any data that displays for the certificate.
To import the security certificates, select **System** > **Tools** > **Trace** > **Import Certificates** and then click **OK**.

### Procedure

To display the Trace & Log Central tree hierarchy, perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

### What to Do Next

After you display Trace & Log Central in RTMT, you can perform the following tasks:

- Use **Collect Files** to download services and application traces from the server.
- Use **Query Wizard** to collect and download trace files that contain search criteria that you specify. You can save your trace collection query for later use.

- Use **Schedule Collection** to create recurring trace collection. You can download the trace files to an SFTP or FTP server on your network.
- Use **Real Time Trace** to view service trace data or to view event trace data as it is collected in real time. For events, you can perform a specified action when a string matching your search criteria appears in the trace file.
- Use **Collect Crash Dump** to download a crash dump file from the server.
- Use **Collect Install Logs** to download the install logs from the server.
- Use **Audit Logs** to browse the audit logs, download the audit logs, or schedule a download of the audit logs. You can download the audit logs to an SFTP or FTP server on your network.
- Use **Remote Browse** to view the collected trace files on the server.
- Use **Local Browse** to view the trace files that you downloaded.

## Trace File Collection, Throttling, and Compression

The Collect Files option in Trace & Log Central is used to collect traces for services, applications, and system logs on the server.

**Note** The services that you have not activated are also shown, so you can collect traces for those services.

### RTMT Trace & Log Central disk I/O and CPU throttling

RTMT supports the throttling of critical Trace & Log Central operations and jobs, whether they are running on-demand, scheduled, or automatic. Throttling slows the operations when I/O utilization is in high demand for call processing, so call processing can take precedence.

When you make a request for an on-demand operation when the call processing node is running under high I/O conditions, the system displays a warning that gives you opportunity to cancel the operation. You can configure the I/O rate threshold values that control when the warning displays with the following service parameters (in Cisco RIS Data Collector service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The system compares the values of these parameters against the actual system CPU and I/OWait values. If the goal (the value of the service parameter) is lower than the actual value, the system displays the warning.

### Trace compression support

The Recoverable Outstream (ROS) library supports compressed output of trace files. Files are compressed as they are generated. The benefits of trace file compression include the following:

- Compression reduces the capacity that is required to store trace files.
- Compression reduces the disk head movement, which results in significantly improved disk I/O wait. This may prove of value when trace file demand is high.

Use the enterprise parameter Trace Compression to enable or disable trace compression. The default value for this parameter is Disabled.

**Note** File compression adds additional CPU cycles. Enabling the Trace Compression enterprise parameter can negatively affect overall call throughput by as much as 10 percent.

# Using Maintenance Tools and Utilities

## Service Inventory Tasks

### UC Application Provisioning

Service Inventory report generation for UC Applications requires some additional steps after adding a cluster in Infrastructure Manager. After the cluster application is saved in Infrastructure Manager, perform the following steps:

**Procedure**

**Step 1** Click **Add New** on the Credentials Tab.

**Step 2** Select the **Credential Type**.
**Note** **PLATFORM** and **ADMIN** are required to run the UC Application Report Collection.

**Step 3** Enter **User ID**, **Password** and **Re-enter Password** and click **Save**.

**Step 4** Repeat to add the next **Credential Type**.

**Step 5** Click on the Network Address Tab and Click **Add New**.

**Step 6** Select the **Network Space : Service Provider Space**.
**Note** This is required for both Cisco Unified Communications Manager and Cisco Unity Connection cluster applications.

**Step 7** Enter **IPV4 Address** and click **Save**.
**Note** This is required for both Cisco Unified Communications Manager and Cisco Unity Connection cluster applications.

**Step 8** Repeat all for the next cluster application.

### Set up Schedule for Daily Report Generation

The Overview page in the Service Inventory administrative interface displays the current status for Service Inventory and any events that you scheduled.

**Tip** If you do not configure the required options on the Configuration page in the Service Inventory administrative interface, the report generation fails.

If the Enable Schedule check box is unchecked, the report does not get generated at the specified time. Keep the Enable Schedule check box unchecked until you are ready to send billing files. If the Configuration page is not configured correctly, the report generation fails.

To schedule the generation of daily reports, perform the following procedure.

**Important** Service Inventory can generate reports only from a Cisco Unified Communications Manager and Cisco Unity Connection running UC Application Software Version 8.6(2) or later.

**Note** Reports are generated differently, depending on your configuration:

- If Unified Communications Domain Manager is not configured in HCM-F and customers exist in HCM-F that are not associated with Unified Communications Domain Manager, only a UC Application-based report is generated.
- If Unified Communications Domain Manager is configured and all customers are associated with Unified Communications Domain Manager in HCM-F, only a Unified Communications Domain Manager-based report is generated.
- If Unified Communications Domain Manager is configured and any customers that exist in HMC-F are not associated with Unified Communications Domain Manager, both UC Application and Unified Communications Domain Manager reports are generated.

### Procedure

**Step 1** Check **Enable Schedule**.

**Step 2** Select **Refresh** to get the most up-to-date time on the server.

**Step 3** Set a time to begin the report daily using the format HH:MM:SS (HH = hours, MM = minutes, SS = seconds).

**Note** You must enter the report times in GMT; however, you can hover over the information icon to see the GMT report time converted to local browser time.

**Step 4** Set the time that you want the reporting period to end using the format HH:MM:SS. The generated report contains data from 24 hours before the set time up to and including the set time.

**Step 5** Select the report format version that you want the SI application to deliver.

**Note** The Cisco HCS 9.0(1) report format version is compatible only with Unified Communications Domain Manager Version 8.1 and later. The Cisco HCS 8.6(2) report format version is compatible with Unified Communications Domain Manager Version 8.0 and later. If you are running an earlier version of the Unified Communications Domain Manager software, select the 8.6(2) report format version.

From the **Infrastructure Manager** > **Application Management** > **Management Application** page, be sure to select the Unified Communications Domain Manager software versions 8.0 or 8.1 for 9.0(1) and 8.6(2) HCS report formats to generate properly.

**Note** The Cisco HCS 9.1(1) report format version is only compatible with Unified Communications Domain Manager Version 8.1 and later. The Cisco HCS 9.0(1) report format version is compatible with Unified Communications Domain Manager Version 8.0 and later. If you are running an earlier version of the Unified Communications Domain Manager software, select the 8.6(2) report format version.

**Service Inventory Unified Communications Domain Manager report**

To ensure that 9.1(1) and 9.0(1) HCS report formats are generated properly, from the **Infrastructure Manager** > **Management Application** page, be sure to select the Unified Communications Domain Manager Software Version 8.0 or 8.1.

**Service Inventory UC Application report**

If a customer is provisioned in Unified Communications Domain Manager, that customer cannot be manually provisioned in Cisco HCM-F. Customers must be provisioned either in Unified Communications Domain Manager or in Cisco HCM-F. The UC Applications report is generated with report format version 9.1(1) or later.

**Service Inventory 10.0.1 Report**

If Unified Communications Domain Manager 10.x is configured, the report format version will list 10.0.1. Reports will be generated in the 10.0.1 format.

**Co-existence and Service Inventory Reports**

In a co-existing deployment, Cisco Hosted Collaboration Mediation Fulfillment can be configured to have Unified Communications Domain Manager 8.x, 10.x and UC applications. In this scenario, based on the report format selected, multiple reports will be generated.

For more information on generated reports, see the Report Combinations, on page 15.

**Step 6** Click **Save**.

## On-Demand Reports

On-Demand reports allows you to generate Inventory and Location reports immediately.

**Note** You must generate an inventory report before you can generate a location report. If you try and generate a location report first, you will receive an error.

### Creating on-demand reports

#### Procedure

**Step 1** Select the type of report you want to generate.

**Step 2** Select the Report Source as **CUCDM**, **UCAPP**, or **CUCDM&UCAPP**.

**Note**
- If you select the Report Source as CUCDM, the Report Format Versions displayed are 9.0(1), 10.1(2), 10.0(1), 8.6(2), and 9.2(1).
- If you select the Report Source as UCAPP, the Report Format Verison will auto populate as 9.1(1).
- If you select the Report Source as CUCDM&UCAPP, the Report Format Version displayed are 8.6(2), 9.0(1), 9.2(1), 10.0(1), 10.1(2).
  **Note** While generating the report, the UCApp report version 9.1(1) is also generated.

**Step 3** Select the Report Format Version from the drop-down box.

**Note** Ensure you are using the compatible versions of Service Inventory and any supported UC Application. For compatibility information, refer to the *Cisco Hosted Collaboration Solution Compatibility Matrix*.

**Note** **Service Inventory Unified Communications Domain Manager report**

You can update the version from the **Infrastructure Manager** > **Management Application** page for Unified Communications Domain Manager software.

**Service Inventory UC Application report**

If a customer is provisioned in Unified Communications Domain Manager, that customer cannot be manually provisioned in Cisco HCM-F. Customers must be provisioned either in Unified Communications Domain Manager or in Cisco HCM-F.

**Step 4** Enter the GMT time the report must include information up to, using the format HH:MM:SS.

**Step 5** Select **Each reseller and customer** or **Generate XLS Report** .

**Note** Selecting each reseller and customer generates separate Summary, Detailed & MACD report files for each reseller and customer in addition to the High Level Summary Report for Service Provider and summary report & excel report files. The Service Provider option is defaulted and cannot be changed.

Selecting Generate XLS Report generates summary report and .si report files.

**Step 6** Click **Save**.

## Transfer Report to Remote SFTP Server

You can transfer a report to the remote SFTP server that you configured on the Configuration page in the Service Inventory administrative interface. To transfer a report, perform the following procedure:

### Procedure

**Step 1** In the Service Inventory administrative interface, click **Backup**.

**Step 2** The list of generated reports appear. Locate and select the files that you want to transfer to the remote SFTP server.

**Step 3** Click **Transfer Selected Files**.

**Step 4** To view the file backup job status in the Infrastructure Manager administrative interface, select **Administration** > **Jobs**.

# General Tasks for Infrastructure Manager

The following section contains the general procedures related to Infrastructure Manager.

## Edit Component

Follow this procedure to view and edit components in Infrastructure Manager.

### Procedure

**Step 1** In the side menu, navigate to the component you want to view or edit.

**Step 2** Click the name of the component you want to view or edit.

**Step 3** Made any edit changes as required.

**Step 4** Click **Save** to commit changes or click **Cancel** to return to the previous screeen.

## Delete Component

Deleting components follows a hierarchical structure that correlates to the menu structure of Infrastructure Manager. For example, when you delete a vCenter the vCenter and associated VMware Data Centers, VMware clusters, Virtual Machines and ESXi hosts are deleted.

Follow this procedure to delete an element in Infrastructure Manager.

**Note** You cannot delete a component added through a sync service unless you disable the sync service for that component.

### Procedure

**Step 1** In the side menu, navigate to the component you want to delete.

**Step 2** Check the check box for the component you want to delete.

**Step 3** Click **Delete Selected**.

## Perform Manual Sync

Follow this procedure to perform a manual sync.

### Procedure

**Step 1** From the side menu, select **Administration** > **Sync Request**.

**Step 2** Select the Job Entity.

- Service Provider: All Data Centers and customers in the system are synced.
- Customer: Only the selected customers are synced.
- Data Center: All vCenters in the Data Center are synced.
- vCenter: Only the selected vCenters are synced.
- UCS Manager: Only the selected UCS Managers are synced.

**Step 3** Check the check box next to the name of the element you want to sync.

**Step 4** Click **Sync Request**.

## Edit Service Provider Information

Follow this procedure to edit the service provider information.

### Procedure

**Step 1** From the side menu, select **Administration** > **Service Provider**.

**Step 2** Enter the following information:

| Field | Description |
|---|---|
| Name | Enter the name of the service provider. This is a mandatory field. |
| Account Number | Enter the account number for the service provider. This is an optional field. |

**Step 3** Click **Address and Contact Information**.

**Step 4** Enter the optional information for the Address 1, Address 2, City, State, Country, Zip Code, Contact Name, Contact Telephone Number, and Contact Email fields.

**Step 5** Click **Save**.

## Display Diagnostic Reports

### utils diagnose hcs

This command enables you to diagnose problems for Cisco HCS services. The information is helpful for debugging purposes.

This command can be executed from any node in the cluster.

**Command Syntax**

**utils diagnose hcs**

**agp**

**chpa**

**cucdmsync**

**dmasa**

**fulfillment**

**hlm**

**nbi**

**si**

**sdrcnf**

**ucpa**

**ucsmsync**

**vcentersync**

**Parameters**

- **agp** displays the diagnostics information for the API Gateway Proxy service.
- **chpa** displays the diagnostics information for the Provisioning Adapter Service.
- **cucdmsync** displays the diagnostics information for the CUCDMSync Service.
- **dmaim** displays the diagnostics information for the DMA-IM.
- **fulfillment** displays the diagnostics information for the fulfillment Service.
- **hlm** displays the diagnostics information for the HCS License Manager Service.
- **nbi** displays the diagnostics information for the North Bound Interface Service.
- **si** displays the diagnostics information for the Service Inventory Service.
- **sdrcnf** displays the diagnostics information for the SDR Change Notification Service.
- **ucpa** displays the diagnostic information for the Unity Connection Provisioning Adapter. It used by Service Inventory.
- **ucsmsync** displays the diagnostics information for the UCSMSync Service.
- **vcentersync** displays the diagnostics information for the VCenterSync Service.

**Requirements**

Command privilege level: 0

Allowed during upgrade: No

### Using Infrastructure Manager Administration GUI

#### Procedure

**Step 1** From the Infrastrucute Manager interface, select **Administration** > **Diagnostics**.

**Step 2** Select the diagnostic you want from the pulldown menu and click **Request Diagnostics.**

## License Management Tasks

### Edit a License Manager

Follow this procedure to edit a License Manager.

**Note** You can only sync the License Manager version by retrieving the version of the installed License Manager.

#### Procedure

**Step 1** From the side menu, select **License Management** > **License Manager Summary**.

**Step 2** Click on the License Manager name you are editing.

**Step 3** Click the **Sync Version**.

### Prime License Manager Customers Summary Page

*Unassign License Manager Clusters*

Follow this procedure to unassign clusters from License Manager using License Management.

### Procedure

**Step 1** From the side menu, select **License Management** > **License Manager Summary**.
**Step 2** Click the customer name.
**Step 3** Click the **Clusters Managed by** dropdown.
**Step 4** Expand Unassign Clusters.
**Step 5** Select the cluster name and click **Unassign**.
**Step 6** From the side menu, select **License Management** > **License Manager Summary**.
**Step 7** Click the customer name.
**Step 8** Expand Assign Customer.
**Step 9** Select None from the drop down menu and click **Save** to unassign the customer from the License Manager.

### Request/Download a HCS License Report

**Note**

Follow this procedure to generate and download license reports using License Management.

### Procedure

**Step 1** From the side menu, select **License Management** > **License Reports**.
**Step 2** To generate a new report click **Request New Report**.
a) Click **Refresh** to see the newly generated report.
**Step 3** To download a report select the report name.
**Step 4** Click **Download CSV Format** or **Download Excel Format**.

# Cisco HCM-F Real-Time Monitoring Tool

## Launch RTMT

The RTMT application launches when you double click on the application icon or open the application, but does not work properly unless you log in on the proper type of server. In this case, a Cisco Hosted Collaboration Mediation Fulfillment (Cisco HCM-F) server.

You can connect to either the HCM-F application server or the HCM-F Web Services server. The RTMT session does not provide monitoring support for all the servers in HCM-F cluster.

**Note** You can launch more than one RTMT session, with each session connecting to a different server (for example, one session connection to the HCM-F application server and another session connection to an HCM-F Web Services server). However, multiple RTMT sessions are not recommended by Cisco.

### Before You Begin

Ensure that a Cisco CDM Database service is running on the Cisco HCM-F server to which you want to establish the RTMT connection.

### Procedure

**Step 1** To launch RTMT, perform one of the following tasks:

- On the Windows desktop, double-click the **Real-Time Monitoring Tool** icon.
  Alternatively, select **Start** > **Programs** > **Cisco** > **HCS** > **Real-Time Monitoring Tool**.

  **Note** If you are working on a Windows Vista computer, the following User Account Control popup message appears: "An unidentified program wants to access your computer." To continue, click **Allow**.

- For Linux: If a shortcut does not appear on the desktop, you can use `/opt/Cisco/HCS/JRtmt` to start the RTMT.

The Real-Time Monitoring Tool Login dialog appears.

**Step 2** In the Host IP Address field, enter either the IP address or the hostname of the Cisco HCM-F server.

**Step 3** Enter the port that the application will use to listen to the server.
The default port is 8443.

**Step 4** Check the **Secure Connection** check box.

**Step 5** Click **OK**.
If the Add Certificate to Store dialog appears, click **Accept** to continue.

The Authentication Required dialog appears.

**Step 6** In the User Name field, enter the Administrator username for the application.

**Step 7** In the Password field, enter the password for the Administrator username.
If the authentication fails or if the server is unreachable, RTMT prompts you to reenter the server and authentication details, or you can click **Cancel** to exit the application.

If authentication succeeds, RTMT launches the monitoring module from local cache or from a remote server, if the local cache does not contain a monitoring module that matches the back-end version. The Cisco HCM-F Real-Time Monitoring Tool window and the Select Configuration dialog box appear.

**Step 8** Select a profile, and then click **OK**.

# Profiles

## Add Configuration Profile

With RTMT, you can customize your monitoring window by monitoring different performance counters and then create your own configuration profiles. You can restore these monitoring windows in a single step rather than opening each window again.

You can switch between different profiles during the same RTMT session or use the configuration profile in subsequent RTMT sessions.

Follow this procedure to create a profile.

### Procedure

**Step 1** Choose **File** > **Profile**.
The Preferences dialog box appears.

**Step 2** Click **Save**.
The Save Current Configuration dialog box appears.

**Step 3** In the Configuration name field, enter a name for this particular configuration profile.

**Step 4** In the Configuration description field, enter a description of this particular configuration profile.

**Note** Profiles apply to all nodes within a cluster, but you cannot save and apply the profile to a different cluster.

The system creates the new configuration profile.

## Restore Configuration Profile

Perform the following procedure to restore a profile that you configured:

### Procedure

**Step 1** Choose **File** > **Profile**.
The Preferences dialog box appears.

**Step 2** Click the profile that you want to restore.

**Step 3** Click **Restore**.
All windows with precanned settings or performance monitoring counters for the restored configuration open.

## Delete Configuration Profile

Perform the following procedure to delete a profile that you configured:

### Procedure

**Step 1** Choose **File** > **Profile**.
The Preferences dialog box appears.

**Step 2** Click the profile that you want to delete.

**Step 3** Click **Delete**.

**Step 4** Click **Close**.

## Categories

Categories allow you to organize objects in RTMT, such as performance monitor counters and devices. For example, the default category, Perfmon Counters, allows you to monitor up to six performance monitor counters in graph format. If you want to monitor more than six counters, you must create a new category and display the data in table format.

### Create Category

In RTMT, categories (groups of counters) can help you troubleshoot specific performance, system, or device problems. Category tabs are shown at the bottom of the Performance pane.
To create a category, perform the following procedure.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Performance** > **Performance**.
- On the menu bar, choose **System** > **Performance** > **Open Performance Monitoring**.

**Step 2** On the menu bar, choose **Edit** > **New Category**

**Note** You can also right click an existing category tab and then on the menu that appears, select **New Category**.

**Step 3** Enter the name of the category.

**Step 4** If you want to display counters on this tab in table view (instead of in chart view), check the **Present Data in Table View** check box.

**Step 5** Click **OK**.
The category tab appears at the bottom of the Performance pane.

**Step 6** To save the category tab for use in a future RTMT session, on the menu bar, choose **File** > **Profile**.
The Profile dialog box appears.

**Step 7** Click **Save**.
The Save Current Configuration dialog box appears.

**Step 8** Enter a name and description for this configuration and then click **OK** to close the Save Current Configuration dialog box.

**Note** You can modify an existing configuration profile by entering the name and description of the existing profile exactly as shown in the Profile dialog box. Then click **OK**.

**Step 9** Click **Close** to close the Profile dialog box.
The new categories are saved in the RTMT profile. To view them in each future RTMT session, on the menu bar, choose **File** > **Profile**, choose the configuration and then click **Restore**.

### Rename Category

To rename a category, perform the following procedure:

#### Procedure

**Step 1** Perform one of the following tasks:

a) Right-click the category tab that you want to rename and choose **Rename Category**.
b) Click the category tab that you want to rename and choose **Edit** > **Rename Category**.

**Step 2** Enter the new name and click **OK**.
The renamed category displays at the bottom of the window.

### Delete Category

To delete a category, perform one of the following tasks:

- Right-click the category tab that you want to delete and choose **Remove Category**.
- Click the category tab that you want to delete and choose **Edit** > **Remove Category**.

## Using the HCM-F RTMT Performance Counter Monitoring

### Add Counter Using Performance Queries

You can use queries to select and display perfmon counters. You can organize the perfmon counters to display a set of feature-based counters and save it in a category. After you save your Unified RTMT profile, you can quickly access the counters in which you are interested.

Unified RTMT displays perfmon counters in chart or table format. The chart format displays the perfmon counter information by using line charts. For each category tab that you create, you can display up to six charts in the Perfmon Monitoring pane with up to three counters in one chart. After you create a category, you cannot change the display from a chart format to a table format, or vice versa.

**Tip** You can display up to three counters in one chart in the Perfmon Monitoring pane. To add another counter in a chart, click the counter and drag it to the Perfmon Monitoring pane. Repeat again to add up to three counters.

By default, Unified RTMT displays perfmon counters in a chart format. You can also choose to display the perfmon counters in a table format. To display the perfmon counters in table format, you need to check the **Present Data in Table View** check box when you create a new category.

### Procedure

**Step 1** Choose **System** > **Performance** > **Open Performance Monitoring**.

**Step 2** Click the name of the server where you want to add a counter to monitor.
The tree hierarchy expands and displays all the perfmon objects.

**Step 3** To monitor a counter in table format, continue to step 4. To monitor a counter in chart format, skip to step 9.

**Step 4** Choose **Edit** > **New Category**.

**Step 5** In the Enter Name field, enter a name for the tab.

**Step 6** To display the perfmon counters in table format, check the **Present Data in Table View** check box.

**Step 7** Click **OK**.
A new tab with the name that you entered appears at the bottom of the pane.

**Step 8** Perform one of the following actions to select one or more counters with one or more instances for monitoring in table format (skip the remaining step in this procedure):

- Double-click a single counter and select a single instance from the popup window, and then click **Add**.
- Double-click a single counter and select multiple instances from the popup window, and then, click **Add**.

**Tip** To display the counter in chart format after you display it in table format, right-click the category tab and choose **Remove Category**. The counter displays in chart format.

**Step 9** To monitor a counter in chart format, perform the following tasks:

a) Click the file icon next to the object name that lists the counters that you want to monitor.
A list of counters appears.

b) To display the counter information, either right-click the counter and click **Counter Monitoring**, double-click the counter, or drag and drop the counter into the Perfmon Monitoring pane.
The counter chart appears in the Perfmon Monitoring pane.

## Remove Counter From Performance Monitoring Pane

You can remove a counter chart (table entry) with the Remove Chart/Table Entry menu item in the Perfmon menu in the menu bar.

You can remove counters from the RTMT Perfmon Monitoring pane when you no longer need them. Follow this procedure to remove a counter from the pane.

### Procedure

Perform one of the following tasks:

- Right-click the counter that you want to remove and choose **Remove**.
- Click the counter that you want to remove and choose **Perfmon** > **Remove Chart/Table Entry**.

## Add Counter Instance

Follow this procedure to add a counter instance.

### Procedure

**Step 1** Find and display the performance monitoring counter.

**Step 2** Click the performance monitoring counter in the performance monitoring tree hierarchy and choose **System** > **Performance** > **Counter Instances**.

**Step 3** In the **Select Instance** window, click the instance, and then click **Add**.
The counter appears.

## Set Up Counter Alert Notification

Follow this procedure to configure alert notification for a counter.

**Tip** To remove the alert for the counter, right-click the counter and choose Remove Alert. The option appears gray after you remove the alert.

### Procedure

**Step 1** Find and display the performance counter.

**Step 2** From the counter chart or table, right-click the counter for which you want to configure the alert notification, and choose **Set Alert/Properties**.

**Step 3** Check the **Enable Alert** check box.

**Step 4** In the **Severity** drop-down list box, choose the severity level at which you want to be notified.

**Step 5** In the Description pane, enter a description of the alert and click **Next**.

**Step 6** Configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes. After you enter the settings in the window, click **Next** to proceed to the next panes.

**Step 7** To configure the system to send an e-mail message for the alert, check the **Enable Email** check box.

**Step 8** To trigger an alert action that is already configured, choose the alert action that you want from the **Trigger Alert Action** drop-down list box.

**Step 9** To configure a new alert action for the alert, click **Configure**.

**Note** Whenever the specified alert is triggered, the system sends the alert action.

The **Alert Action** dialog box appears.

**Step 10** To add a new alert action, click **Add**.
The Action Configuration dialog box appears.

**Step 11** In the Name field, enter a name for the alert action.

**Step 12** In the Description field, enter a description for the alert action.

**Step 13** Click **Add** to add a new e-mail recipient for the alert action.
The Input dialog box appears.

**Step 14** Enter either the e-mail or e-page address of the recipient that you want to receive the alert action notification and click **OK**

**Step 15** In the User-defined email text box, enter the text that you want to display in the e-mail message and click **Activate**.

*Counter Alert Configuration Parameters*

## Display Counter Description

The following shows how to obtain a description of the counter:

### Procedure

**Step 1** Perform one of the following tasks:

a) In the Perfmon tree hierarchy, right-click the counter for which you want property information and choose **Counter Description**.

b) In the RTMT Performance Monitoring pane, click the counter and choose **System** > **Performance** > **Counter Description** from the menu bar.

**Tip** You can display the counter description and configure data-sampling parameters.

The **Counter Property** window displays the description of the counter. The description includes the host address, the object to which the counter belongs, the counter name, and a brief overview of what the counter does.

**Step 2** To close the **Counter Property** window, click **OK**.

## Start Perfmon Counter Logging

To start logging perfmon counter data into a CSV log file, perform the following procedure:

### Procedure

**Step 1** Find and display the performance monitoring counters.

**Step 2** If you are displaying perfmon counters in the chart format, right-click the graph for which you want data sample information and choose **Start Counter(s) Logging**.
The **Counter Logging Configuration** dialog box appears.

**Step 3** If you want to log all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Start Counter(s) Logging**.
The **Counter Logging Configuration** dialog box appears.

**Step 4** In the Logger File Name field, enter a filename and click **OK**.
RTMT saves the CSV log files in the log folder in the .jrtmt directory under the user home directory. For example, in Windows, the path specifies `D:\Documents and Settings\userA\.jrtmt\log`, or in Linux, the path specifies `/users/home/.jrtmt/log`.

To limit the number and size of the files, configure the maximum file size and maximum number of files parameter in the trace output setting for the specific service in the **Trace Configuration** window of Cisco Unified Serviceability. See *Cisco Unified Serviceability Administration Guide*.

## Stop Perfmon Counter Logging

To stop logging perfmon counter data, perform the following procedure:

### Procedure

**Step 1** Find and display the performance monitoring counters.

**Step 2** If you are displaying perfmon counters in the chart format, right-click the graph for which counter logging is started and choose **Stop Counter(s) Logging**. If you want to stop logging of all counters in a screen (both chart and table view format), you can right-click the category name tab at the bottom of the window and choose **Stop Counter(s) Logging**.

## Configure Data Sample

The **Counter Property** window contains the option to configure data samples for a counter. The perfmon counters that display in the RTMT Perfmon Monitoring pane contain green dots that represent samples of data over time. You can configure the number of data samples to collect and the number of data points to show in the chart. After the data sample is configured, view the information by using the View All Data/View Current Data menu option.

Follow this procedure to configure the number of data samples to collect for a counter.

### Procedure

**Step 1** Find and display the counter.

**Step 2** Click the counter for which you want data sample information and choose **System** > **Performance** > **Monitoring Properties**.
The **Counter Property** window displays the description of the counter, as well as the tab for configuring data samples. The description includes the host address, the object to which the counter belongs, the counter name, and a brief overview of what the counter does.

**Step 3** To configure the number of data samples for the counter, click the **Data Sample** tab.

**Step 4** From the **No. of data samples** drop-down list box, choose the number of samples (between 100 and 1000).
The default specifies 100.

**Step 5** From the **No. of data points shown on chart** drop-down list box, choose the number of data points to display on the chart (between 10 and 50).
The default specifies 20.

**Step 6** Click one of the following parameters:

- Absolute: Because some counter values are accumulative, choose Absolute to display the data at its current status.
- Delta: Choose Delta to display the difference between the current counter value and the previous counter value.
- Delta Percentage: Choose Delta Percentage to display the counter performance changes in percentage.

**Step 7** To close the **Counter Property** window and return to the RTMT Perfmon Monitoring pane, click **OK**.

## View Counter Data

Follow this procedure to view the data that is collected for a performance counter.

### Procedure

**Step 1** In the RTMT Perfmon Monitoring pane, right-click the counter chart for the counter for which you want to view data samples.

**Step 2** Choose **View All Data**.
The counter chart displays all data that has been sampled. The green dots display close together.

**Step 3** Right-click the counter that currently appears.

**Step 4** Choose **View Current**.
The counter chart displays the last configured data samples that were collected.

## View Performance Monitor Log Files

You can view data in the performance monitor CSV log file by using Performance Log Viewer in RTMT or by using Performance Monitor in Windows.

You can only view log files on the server to which RTMT is connected. To view the log files on a different server, you must log out and establish a new RTMT connection to that server.

### *View Log Files on Perfmon Log Viewer*

The Performance Log Viewer displays data for counters from perfmon CSV log files in a graphical format. You can use the performance log viewer to display data from the local perfmon logs that you collected, or you can display the data from the Real-time Information Server Data Collection (RISDC) perfmon logs.

#### Before You Begin

The local perfmon logs consist of data from counters that you select and store locally on your computer.

#### Procedure

**Step 1** Select **System** > **Performance** > **Open Performance Log Viewer**.

**Step 2** Select the type of perfmon logs that you want to view:

- For RisDC Perfmon Logs, perform the following steps:
  1. Select RisDC Perfmon Logs in the Select Perfmon Log Location section.
  2. Select a node from the list box.
  3. Select **Open**.
  4. Select the file and select **Open File**.
  5. Check the counters that you want to display.
  6. Select **OK**.
- For locally stored data, perform the following actions:
  1. Select **Local Perfmon Logs**.
  2. Select **Open**.
  3. Browse to the file directory.
  4. Select the file that you are interested in viewing or enter the filename in the filename field.
  5. Select **Open**.
  6. Check the counters that you want to display.
  7. Select **OK**.

**Step 3** Select the counters that you want to display.

**Step 4** Select **OK**.
Troubleshooting Tips

- The Real-Time Monitoring Tool saves the perfmon CSV log files in the log folder in the.jrtmt directory under the user home directory. In Windows, the path specifies D:\Documents and Settings\userA\.jrtmt\log, or in Linux, the path specifies /users/home/.jrtmt/log
- The RISDC perfmon logging is also known as Troubleshooting Perfmon Data logging. When you enable RISDC perfmon logging, the server collects data that are used to troubleshoot problems. Because the IM and Presence service collects a large amount of data in a short period of time, you should limit the time that RISDC perfmon data logging (troubleshooting perfmon data logging) is enabled.
- You can order each column by selecting on a column heading. The first time that you select on a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you select the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you select the column heading one more time, the records displays in the unsorted state.

### *View Perfmon Log Files with Microsoft Performance Tool*

**Note** The method for accessing **Performance** may vary depending on the version of windows you install on your computer.

#### Procedure

**Step 1** Select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Performance**.

**Step 2** Perform the following actions in the application window:

a) Select the right mouse button.

b) Select **Properties**.

**Step 3** Select the Source tab in the System Monitor Properties dialog box.

**Step 4** Browse to the directory where you downloaded the perfmon log file and select the perfmon csv file. The log file includes the following naming convention:
PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv; for example,
PerfMon_172.19.240.80_06_15_2005_11_25.csv.

**Step 5** Select **Apply**.

**Step 6** Select **Time Range**. To specify the time range in the perfmon log file that you want to view, drag the bar to the appropriate starting and ending times.

**Step 7** To open the Add Counters dialog box, select the Data tab and select **Add**.

**Step 8** Select the perfmon object from the Performance Object drop-down list box. If an object has multiple instances, you may select **All instances** or select only the instances that you are interested in viewing.

**Step 9** You can select **All Counters** or select only the counters that you are interested in viewing.

**Step 10** Select **Add** to add the selected counters.

**Step 11** Select **Close when you finish selecting counters**.

# Setting up Alerts

## Access Alert Central and Setup Alerts

The following procedure explains how to perform the following tasks:

- access Alert Central
- sort alert information
- enable, disable, or remove an alert
- clear an alert
- view alert details

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Alert Central**.
- Choose **System** > **Tools** > **Alert** > **Alert Central**.

The Alert Central pane displays the alert status and history of the alerts that are generated by the system.

**Step 2** Perform one of the following tasks:

- Set alert properties (see Setup Alert Properties, on page 79).
- Suspend alerts (see Suspend Alerts, on page 81).
- Configure emails for alert notification (see Configure Mail Server for Alert Notification, on page 81).
- Configure alert actions (see Setup Alert Actions, on page 82).

**Step 3** To sort the alert and alert history information, click a column heading.
An up or down arrow appears in the column heading to indicate that sorting is based on that column, and that sorting is ascending (up arrow) or descending (down arrow).

To see alert history that is out of view in the pane, use the scroll bar on the right side of the Alert History pane.

**Step 4** To enable, disable, or remove an alert, perform one of the following tasks:

- Right-click the alert and choose **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish.
- Select the alert and choose **System** > **Tools** > **Alert** > **Disable/Enable (or Remove) Alert**.

**Tip** You can remove only user-defined alerts from RTMT. The Remove Alert option appears dimmed when you choose a preconfigured alert.

**Step 5** To clear either individual or collective alerts after they are resolved, perform one of the following tasks:

- Right-click the alert and choose **Clear Alert** (or **Clear All Alerts**).

- Select the alert and choose **System** > **Tools** > **Alert** > **Clear Alert** (or **Clear All Alerts**).

After you clear an alert, the color changes from red to black.

**Step 6** To reset alerts to default configuration, perform one of the following tasks:

- Right-click the alert and choose **Reset Alert to Default Config**.
- Choose **System** > **Tools** > **Alert** > **Reset all Alerts to Default Config**.

**Step 7** To view alert details, perform one of the following tasks:

- Right-click the alert and choose **Alert Detail**.
- Select the alert and choose **System** > **Tools** > **Alert** > **Alert Detail**.

After you have finished viewing the alert details, click **OK**.

## Setup Alert Properties

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Alert Central**.
- On the menu bar, choose **System** > **Tools** > **Alert** > **Alert Central**.

**Step 2** Select the alert you want to configure.

**Step 3** Perform one of the following tasks:

- Right-click the alert and choose **Set Alert/Properties**.
- Choose **System** > **Tools** > **Alert** > **Set Alert/Properties**.

The Alert Properties: General dialog box appears.

**Step 4** To enable the alert, check the **Enable Alert** check box.

**Step 5** In the **Severity** list box, choose the severity for the alert.

**Step 6** In the Enable/Disable this alert on following server(s) section (if it appears), check the **Enable** check box for the servers on which you want this alert to be enabled.
For preconfigured alerts, the Description field contains a description of the alert. The Recommended Action field describes what should be done after the alert is received. You cannot change these fields.

**Step 7** Click **Next**.
The Alert Properties: Threshold & Duration dialog box appears.

**Note** The Duration section does not appear in this dialog box if it is not relevant for the alert. In this case, the dialog box title is Alert Properties: Threshold.

**Step 8** In the Threshold section, enter the conditions that trigger the alert.

**Note** Fields appear for configuring the threshold only if threshold configuration is relevant for the alert.

**Step 9** In the Duration section (if it is shown), click one of the following radio buttons:

- **Trigger alert only when value constantly below or over threshold for:** If you want the alert to be triggered only when the value is constantly below or over the threshold for a specific number of seconds. Enter the number of seconds.
- **Trigger alert immediately:** If you want the system to trigger an alert immediately.

**Step 10** Click **Next**.
The Alert Properties: Frequency & Schedule dialog box appears.

**Step 11** In the Frequency section, click one of the following radio buttons (if they appear):

- **Trigger alert on every poll:** If you want the alert to be triggered on every poll.
- **Trigger up to <number> alerts within <number> minutes:** If you want a specific number of alerts to be triggered within a specific number of minutes, enter the number of alerts and the number of minutes.

**Step 12** In the Schedule section, click one of the following radio buttons:

- **Trigger Alert when it occurs (Non-Stop Monitoring):** If you want the alert to be triggered 24 hours a day.
- **Trigger Alert everyday (Scheduled Monitoring) between:** If you want the alert to be triggered within a specific start and stop time. Enter the start and end times.

**Step 13** Click **Next**.

**Step 14** For alerts such as CriticalServiceDown and CodeYellow that allow trace download, perform the following tasks in the Alert Properties: Trace Download dialog box (if it appears); otherwise, go to **Step 15**.

a) In the Alert Properties: Trace Download dialog box, check the **Enable Trace Download** check box.
The Trace Download Configuration dialog box appears.

b) Click the **SFTP/FTP Server** radio button.

c) Click either the **Localhost** or **SFTP/FTP Server** radio button.

d) Select FTP or SFTP as the protocol, and then enter the IP address, username, password, port, and download directory path where the trace will be saved.

e) To ensure that you have connectivity with the SFTP server, click **Test Connection**. If the connection test fails, your settings will not be saved.

f) To save the configuration and close the Trace Download Configuration dialog box, click **OK**.

g) In the Alert Properties: Trace Download Parameters dialog box, enter the number and frequency of downloads.
The number and frequency of download settings help to limit the number of trace files that are downloaded. The polling setting provides the basis for the default setting for the frequency.

**Caution** Enabling Trace Download may affect services on the server. Configuring a high number of downloads will adversely affect quality of service on the server.

h) Click **Next**.

The Alert Properties: Email Notification dialog box appears.

**Step 15** In the Alert Properties: Email Notification dialog box: If you want to enable email notification for this alert, check the **Enable Email** check box.

**Step 16** To trigger an alert action with this alert, in the Trigger Alert Action list, choose the action that you want to send.
For information about configuring alert actions, see Setup Alert Actions, on page 82.

**Step 17** Enter descriptive information about the alert in the User-defined email text box.

**Step 18** Click **Save** to save the alert configuration and close the Alert Properties dialog box.

## Suspend Alerts

You may want to temporarily suspend some or all alerts on a particular server. For example, if you are upgrading Cisco HCM-F to a newer release, you may want to suspend all alerts until the upgrade completes, so you do not receive emails or e-pages during the upgrade. The following procedure describes how to suspend alerts in Alert Central.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Alert Central**.
- On the menu bar, choose **System** > **Tools** > **Alert** > **Alert Central**.

**Step 2** Choose **System** > **Tools** > **Alert** > **Suspend Cluster/Node Alerts**.

**Step 3** Perform one of the following tasks:

- To suspend alerts on the entire server cluster, click the **Cluster Wide** radio button, and then if appropriate, check the **suspend all alerts** check box.
- To suspend alerts on specific servers, click the **Per Server** radio button and then check the **Suspend** check box for each server on which you want to suspend alerts.

**Step 4** Click **OK**.

**Note** To resume alerts, choose **System** > **Tools** > **Alert** > **Suspend Cluster/Node Alerts** again and uncheck the **Suspend** check boxes.

## Configure Mail Server for Alert Notification

Perform the following procedure to configure email information for alert notification.

**Note** To configure RTMT to send alerts using email, you must configure DNS. For information on configuring the primary and secondary DNS IP addresses and the domain name in Cisco HCM-F, see *Administration Guide for Cisco Hosted Collaboration Mediation Fulfillment*.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Alert Central**.
- On the menu bar, choose **System** > **Tools** > **Alert** > **Alert Central**.

**Step 2** Choose **System** > **Tools** > **Alert** > **Config Email Server**.
The Mail Server Configuration window appears.

**Step 3** In the Mail Server field, enter the address of the mail server.

**Step 4** In the Port field, enter the port number on the mail server.

**Step 5** In the Sender User Id field, enter the email address for the intended recipient.
By default, `RTMT_Admin@domain` is used, where `domain` is the domain of the host server.

**Step 6** Click **OK**.

## Setup Alert Actions

The following procedure describes how to create, modify, or delete alert actions.

### Procedure

**Step 1** If you came to this procedure while configuring the Alert Properties: Email Configuration dialog box, click **Configure**.
The Alert Action dialog box appears. Go to **Step 4**. Otherwise, go to **Step 2**.

**Step 2** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Alert Central**.
- On the menu bar, choose **System** > **Tools** > **Alert** > **Alert Central**.

**Step 3** Choose **System** > **Tools** > **Alert** > **Config Alert Action**.
The Alert Action dialog box appears.

**Step 4** Perform one of the following steps:

- To add a new alert action, click **Add**. The Action Configuration dialog box appears.
- To modify an existing alert action, select the alert action and then click **Edit**. The Action Configuration dialog box appears.

- To delete an alert action, select it and then click **Delete**. The selected alert action disappears from the list.

**Step 5** If you are adding a new alert action: In the Name field, enter a name for the alert action.

**Note** You cannot modify the name for an existing alert action.

**Step 6** In the Description field, enter (or modify) the description of the alert action.

**Step 7** To add an email recipient, click **Add**.
The Info dialog box appears.

**Step 8** In the Enter email/epage address field, enter an email or e-page address of the recipient that you want to receive the alert action and click **OK**.
The Action Configuration dialog box shows the recipient that you added, and the **Enable** check box is automatically checked.

**Tip** To delete an email recipient, select the recipient and click **Delete**. The recipient that you chose disappears from the recipient list.

**Step 9** When you finish adding recipients, click **OK** to close the Action Configuration dialog box.

**Step 10** Click **Close** to save and close the Alert Action dialog box.

## Setup the Global Email List for Alert Notifications

The following procedure describes how to configure all predefined alerts to send email to one or more email destinations. This procedure uses “Default,” the action that is assigned to all alerts during installation.

Follow this procedure to configure a recipient list for all predefined alerts without needing to set an action for each alert. When you add email destinations to the “Default” alert action recipient list, all predefined alerts are sent to those recipients, as long as all alerts continue to use the “Default” alert action.

To configure a new action for a specific alert, to reconfigure existing alert actions, or to disable emails for an alert, use the Set Alerts/Properties option, which appears when you right-click an alert. For more information, see Setup Alert Properties, on page 79.

Each time you update an alert action, the changes apply to all alerts that are configured with that alert action. For example, if all alerts use the “Default” alert action, updating the “Default” alert action automatically updates all alerts.

You cannot delete the “Default” alert action. For other alert actions, you can delete them only if they are not associated with other alerts. If an action is associated with multiple alerts, you must reassign a new action to those alerts before you can delete the alert action.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Alert Central**.
- On the menu bar, choose **System** > **Tools** > **Alert** > **Alert Central**.

The Alert Central monitor pane appears.

**Step 2** Click **System** > **Tools** > **Alert** > **Config Alert Action**.
The Alert Action dialog box appears.

**Step 3** In the Alert Action list, select **Default** and click **Edit**.
The Action Configuration dialog box appears.

**Step 4** If required, enter or modify the description for the "Default" action.

**Step 5** Click **Add** to add a recipient.
The Input dialog box appears.

**Step 6** Enter the email address that is to receive all alerts and click **OK**.
The email address appears in the Recipients list in the Action Configuration dialog box; the Enable check box for the recipient is checked by default.

**Note** You can disable the email recipient at any time by unchecking the **Enable** check box. To completely remove the recipient from the list, select it and click **Delete**.

**Step 7** Return to **Step 5** to add additional email recipients, if required.

**Step 8** Click **OK** to close the Action Configuration dialog box.

**Step 9** Click **Close** to close the Alert Action dialog box.

## Settings up Traces and Logs

### Collect Trace Files

Use the Collect Files object in Trace & Log Central to collect traces for services, applications, and system logs on the server. You specify the date and time range for which you want to collect traces, the directory in which to download the trace files, whether to delete the collected files from the server, and so on. The following procedure describes how to use Trace & Log Central to collect traces.

**Note** The services that you have not activated are also shown, so you can collect traces for those services.

Use Query Wizard if you want to collect trace files that contain search criteria that you specify or you want to use trace collection criteria that you saved for later use.

#### Before You Begin

Perform one or more of the following tasks:

- Configure the throttling of critical Trace & Log Central operations and jobs by setting the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service).
- Enable trace compression by setting the value of the Trace Compression enterprise parameter to Enabled.

### Procedure

**Step 1** Perform one of the following actions:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** In the Trace & Log Central list, double-click **Collect Files**.
The Collect Files window appears. The services that you have not activated are also shown, so you can collect traces for those services.

**Step 3** On the Select HCS Services/Application tab, perform one of the following tasks:

- To collect traces for the server, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for a specific server, check the check box beside the server name and click **Next**.
- To collect traces for specific HCS services and applications on a server, check the check boxes that apply and click **Next**.
- To go to the next tab without collecting traces for HCS services and applications, click **Next**.

**Step 4** On the Select System Services/Application tab, perform one of the following tasks:

- To collect traces for the server, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for a specific server, check the check box beside the server name and click **Next**.
- To collect traces for specific system services and applications on a server, check the check boxes that apply and click **Next**.
- To continue the configuration without collecting traces for system services and applications, click **Next**.

**Step 5** In the Collection Time section, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range:** Specify the time zone and the start and end dates and time for which you want to collect traces.
  By default, the default selection in the Select Reference Server Time Zone list box is the time zone on the RTMT client computer. Your alternate choice is the server time zone.

  Trace & Log Central downloads the file with a time range that is based on the selected time zone.

  To set the date range for which you want to collect traces, choose the dates in the From Date/Time and To Date/Time fields.
- **Relative Range:** Specify the number of minutes, hours, days, weeks, or months before the current time.

  **Note** RTMT returns logs of a different time stamp than that configured through the wizard. This occurs when the specified time stamp is lower than that of the existing log files. For example, log files exist on the server for a specific service from 11/24/09, and you specified the time range from 11/23/09 5:50 to 11/23/09 7:50; RTMT still returns the existing log files.

**Step 6** In the Download File Options section, in the Select Partition list box, select the partition that contains the logs for which you want to collect traces.

**Note** Cisco Unified Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive directory. For example, if you upgrade from a version of Cisco HCM-F that is running on an application server to another version, and you restart the server with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log back in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

**Step 7** To specify the directory in which to download the trace files, click **Browse**, navigate to the directory, and click **Open**.
The default path is `<rtmt_install_directory>\<server name or server IP address>\<download time>` where `<rtmt_install_directory>` is the directory in which RTMT is installed.

**Step 8** Perform one of the following steps:

- To create a zip file of the trace files that you collect, click the **Zip Files** radio button.
- To download the trace files without zipping the files, click the **Do Not Zip Files** radio button.

**Step 9** To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.

**Step 10** Click **Finish**, or to cancel the settings, click **Cancel**.
If you click Finish, RTMT displays the status of the trace file downloads in the Trace & Log Central pane as well as in the status bar at the bottom.

When the collection process is complete, the message "Completed downloading for node <Server name or IP address>" appears in the status bar at the bottom of the window.

**Step 11** To view the trace files that you collected, use Local Browse.
For more information, see Display Downloaded Trace Files using Local Browse, on page 100.

**Note** You will see a message if the service parameter values are exceeded or if the system is in code yellow.

## Collect Installation Logs

The following procedure describes how to collect installation and upgrade logs in Trace & Log Central.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

The Trace & Log Central pane appears.

**Step 2** In the Trace & Log Central list, double-click **Collect Install Logs**.
The Collect Install Logs dialog box appears.

**Step 3** In the Select Servers Options section, specify from which server you want to collect the install logs.

To collect the install logs for a particular server, check the check box beside the server name.

To collect the install logs for all servers, check the **Select All Servers** check box.

**Step 4** In the Download File Options section, specify the directory where you want to download the log file.
To specify the directory in which you want to download the log files, click **Browse**, navigate to the directory, and click **Open**. The default path is `<rtmt_install_directory>` where `<rtmt_install_directory>` is the directory where RTMT is installed.

**Step 5** Click **Finish**.

## Collect and Download Trace Files Using Query Wizard

The Query Wizard in Trace & Log Central allows you to collect and download trace files that contain search criteria that you specify. You can save the trace collection criteria for later use. To use the trace collection Query Wizard, perform the following procedure.

**Note** You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

### Before You Begin

If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** In the Trace & Log Central list, double-click **Query Wizard**.
The Query Wizard dialog box appears.

**Step 3** On the Query Wizard Options page, perform one of the following actions:

- Click **Saved Query**, and then click **Browse** to navigate to the query that you want to use.
  Choose the query and click **Open**.

  If the query was saved as a single-node generic query, the server to which RTMT is connected appears with a check mark beside the Browse button.

  If the query was saved as a regular query, all of the servers selected in the query appear with check marks. You can check or uncheck any server in the list. If you choose new servers, you must use the wizard to choose the services for that server.

- Click **Create Query**.

**Step 4** Perform one of the following tasks:

- If you selected Saved Query and want to run the query without modification, click **Run Query** and then go to **Step 19**.
- If you selected Saved Query and want to modify it, click **Next**. The HCS Services/Applications tab appears. The services that are not activated are also shown so you can collect traces for those services.
- If you selected Create Query, click **Next**. The Select HCS Services/Applications tab appears. The services that are not activated are also shown so you can collect traces for those services.

**Step 5** Perform one of the following tasks:

- To collect traces for all HCS services and applications on the server, check the **Select All Services on All Servers** check box.
- To collect traces for all HCS services and applications on a particular server, check the check box beside the server name or server IP address.
- To collect traces for specific HCS services and applications on the server, check the check boxes that apply.

**Step 6** Click **Next**.
The Select System Services/Applications tab appears.

**Step 7** Perform one of the following tasks:

- To collect traces for all system services and applications on the server, check the **Select All Services on All Servers** check box.
- To collect traces for all system services and applications on a particular server, check the check box beside the server name or server IP address.
- To collect traces for specific system services and applications on the server, check the check boxes that apply.

**Step 8** Click **Next**.
The Query File Options page appears.

**Step 9** In the Query Time Options section, specify the time range for which you want to collect traces. Choose one of the following options:

- **All Available Traces:** Choose this option to collect all the traces on the server for the services that you chose.
- **Absolute Range:** Select the time zone and the start and end dates and time for which you want to collect traces.
  By default, the default selection in the Select Reference Server Time Zone list box is the time zone on the RTMT client computer. Your alternate choice is the server time zone.

  Trace & Log Central downloads the files with a time range that is based on the selected time zone. If you have servers in different time zones, Trace & Log Central adjusts for the time change and collects the files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and

you have a second server (server x) that is in a time zone that is one hour ahead, Trace & Log Central downloads the files from 10:00 a.m. to 11:00 a.m. from server x.

To set the date range for which you want to collect traces, choose the dates in the From Date/Time and To Date/Time fields.

- **Relative Range:** Specify the time before the current time (in minutes, hours, days, weeks, or months) for which you want to collect traces.

**Step 10** To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field.

**Step 11** If you want to search for an exact match to the word or phrase that you entered, check the **Case Sensitive** check box.

**Step 12** In the Call Processing Impact Options section, in the Select Impact Level list box, select the maximum level of impact the string search activity should have on call processing.
Your choices are Low, Medium, or High. Low causes the least impact on call processing but yields slower results. High causes the most impact on call processing but yields faster results.

**Step 13** Click **Next**.
The Action Options dialog box appears.

**Step 14** Click one of the following radio buttons:

- **Trace Browse**
- **On Demand Trace Collection**
  To specify the directory in which to download the trace files and the results file, click **Browse**, navigate to the directory, and click **Open**. The default path is `<rtmt_install_directory>\<server name or server IP address>\<download time>` where `<rtmt_install_directory>` is the directory in which RTMT is installed.

  To create a zip file of the trace files that you collect, check the **Zip Files** check box.

  To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.
- **Schedule Download**
  Select the start and end dates and time.

  To configure the trace server, click the **Configure Trace Server** check box. The Trace Download Configuration dialog box appears.

  In the dialog box, configure the following FTP/SFTP parameters and then click **Test Connection** to verify that the connection is good.

  - Host IP Address
  - User Name
  - Password
  - Port
  - Download Directory Path

**Note** **Localhost** is available for Cisco Intercompany Media Engine servers only. If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command. FTP is not supported for Cisco Intercompany Media Engine.

HCM-F RTMT does not support the **Localhost** option.

When you are finished, click **OK** to close the Trace Download Configuration dialog box.

**Step 15** Perform one of the following tasks:

- To save the query so you can use it again in the future, click **Save Query**. The Save options dialog box appears. Go to **Step 16**.
- To execute the query, click **Run Query**. This option is available only if you selected **Trace Browse**. When the query completes, the Query Results folder appears in the Trace & Log Central pane, and a dialog box appears to indicate that the query execution completed. Click **Close** to close the dialog box. Go to **Step 19**.
- To download the traces now, click **Download Trace**.
  This option is available only if you selected **On Demand Trace Collection** or **Schedule Download**.

  A new appears in the Trace & Log Central pane to report the status of the download. When finished, the final message indicates successful completion of the trace download.

  You can view the downloaded trace files by using Local Browse. For more information, see Display Downloaded Trace Files using Local Browse, on page 100.

**Step 16** In the Save options dialog box, perform one of the following tasks:

- If you want to run the query on servers other than the server on which it was created, check the **Generic Query** check box. You can create a generic query only if the services that you choose exist on the other servers.
  Click either the **Single Node Query** or the **All Node Query** radio button.

  If you click the Single Node Query radio button, by default, Trace & Log Central chooses the server on which you created the query when you execute the query. If you click the All Node Query radio button, Trace & Log Central selects all servers by default.
  **Note** You can change the server selection before you actually execute the query.

- If you want to run the query only on the server on which you created it, check the **Regular Query** check box.

**Step 17** Click **Finish** to save the trace collection query.

**Step 18** Browse to the folder where you want to store the query, enter a name for the query in the File Name field, and then click **Save**.

**Step 19** After the Run Query execution completes, in the Query Result tree list, navigate to the collected trace file:

a) Double-click **Query Result**.
b) Double-click the <node> folder (where <node> is the IP address or hostname for the server that you specified).
c) Double-click each folder in the hierarchy until one or more files appear in the list in the right pane.

**Step 20** Perform one of the following tasks:

- If you want to view the trace file contents now, go to **Step 21**.

- If you want to download the trace files, go to **Step 22**.

**Step 21** To open the file in a viewer, perform the following tasks:

a) Double-click the file.
The Open With dialog box appears.

b) Select the viewer to use.

c) If desired, check the **Always use this program to open these files** check box.

d) Click **OK**.
The viewer opens to show the contents of the trace file. When you are finished reviewing the file, click **Close** to close the viewer.

**Step 22** To download the trace files, perform the following tasks:

a) Select the file, and then click **Download**.
The Select Download Options dialog box appears.

b) To specify the directory in which you want to save the files, click **Browse**, navigate to the directory, and click **Open**.
The default path is `<rtmt_install_directory>\<server name or server IP address>\<download time>` where `<rtmt_install_directory>` is the directory in which RTMT is installed.

c) To create a zip file of the trace files you are downloading, check the **Zip Files** check box.

d) To delete collected log files from the server, check the **Delete Files on Server** check box.

e) Click **Finish**.

After you download the trace files, you can view them by using Local Browse in Trace & Log Central. For more information, see Display Downloaded Trace Files using Local Browse, on page 100.

## Schedule Trace Collection

You can use the Schedule Collection option in Trace & Log Central to schedule up to six concurrent trace collections and to download the trace files to an SFTP or FTP server on your network, run another saved query, or generate a syslog file. To change a scheduled collection after you have entered it in the system, you must delete the scheduled collection and add a new collection event. To schedule trace collection, perform the following procedure.

**Note** You can schedule up to ten trace collection jobs, but only six trace collection jobs can be concurrent. That is, only six jobs can be in a running state at the same time.

### Before You Begin

If you want alarms to be sent to a trace file, choose an SDI or SDL trace file as the alarm destination in the Alarm Configuration window.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** In the Trace & Log Central list, double-click **Schedule Collection**.
The Select HCS Services/Applications tab appears.

**Note** The services that you have not activated also appear, so you can collect traces for those services.

**Step 3** Perform one of the following tasks:

- To collect traces for all HCS services and applications on the server, check the **Select All Services on All Servers** check box.
- To collect traces for all HCS services and applications on a particular server, check the check box beside the server name or server IP address.
- To collect traces for specific HCS services and applications on the server, check the check boxes that apply.

**Step 4** Click **Next**.
The Select System Services/Applications tab appears.

**Step 5** Perform one of the following tasks:

- To collect traces for all system services and applications on the server, check the **Select All Services on All Servers** check box.
- To collect traces for all system services and applications on a particular server, check the check box beside the server name or server IP address.
- To collect traces for specific system services and applications on the server, check the check boxes that apply.

**Step 6** Click **Next**.
The Schedule Options page appears.

**Step 7** Select the time zone and the start and end dates and time for which you want to collect traces.
By default, the default selection in the Select Reference Server Time Zone list box is the time zone on the RTMT client computer. Your alternate choice is the server time zone.

**Note** The trace collection completes, even if the collection goes beyond the configured end time; however, Trace & Log Central deletes this collection from the schedule.

**Step 8** In the **Scheduler Frequency** list box, choose how often you want to run the configured trace collection.

**Step 9** In the **Collect Files generated in the last** list boxes, specify the time before the current time (in minutes, hours, days, weeks, or months) for which you want to collect traces.

**Step 10** To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field.

**Step 11** If you want to search for an exact match to the word or phrase that you entered, check the **Case Sensitive** check box.

**Step 12** To create a zip file of the trace files that are collected, check the **Zip File** check box.

**Step 13** To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.

**Step 14** Check the following check boxes, as required:

- **Download Files**
  The Trace Download Configuration dialog box appears. Go to **Step 15**.
- **Run Another Query**
  Click **Browse** to locate the query that you want to run, and click **OK**.

  Trace & Log Central executes the specified query only if the first query generated results.
- **Generate Syslog** and then go to **Step 16**.

**Step 15** In the Trace Download Configuration dialog box, perform the following tasks:

a) Enter the server credentials for the server where Trace & Log Central downloads the results.
The Download Directory Path field specifies the directory in which Trace & Log Central stores collected files. By default, files are stored in the home directory of the user whose user ID you specify in the SFTP or FTP parameters fields: `/home/<user>/Trace`.

The **Localhost** option is available only for Cisco Intercompany Media Engine servers. FTP is not supported for Cisco Intercompany Media Engine.

HCM-F RTMT does not support the **Localhost** option.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

b) Click **Test Connection**.
Trace & Log Central verifies the connection to the SFTP or FTP server.

c) Click **OK**.

**Step 16** Click **Finish**.
A message indicates that the system added the scheduled trace successfully.

**Note** If RTMT cannot access the SFTP or FTP server, a message appears. Verify that you entered the correct IP address, username, and password.

**Step 17** Click **OK**.

**Step 18** To view a list of scheduled collections, choose **Tools** > **Job Status** in the QuickLaunch Channel pane.

## View Trace Collection Status

To view trace collection event status and to delete scheduled trace collections, use the following procedure.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** Double-click the **Job Status** icon.
The Job Status pane appears.

**Step 3** In the **Select a Node** list box, choose the server for which you want to view or delete trace collection events.
The list of scheduled trace collections appears.

Possible job types include Scheduled Job, OnDemand, RealTimeFileMon, and RealTimeFileSearch.

Possible statuses include Pending, Running, Cancel, and Terminated.

**Step 4** To delete a scheduled collection, choose the event that you want to delete and click **Delete**.

**Note** You can delete only the jobs with a status of Pending or Running and a job type of Schedule Task or a job type of RealTimeFileSearch.

## Collect a Crash Dump File

Perform the following procedure to collect a crash dump file:

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** In the Trace & Log Central list, double-click **Collect Crash Dump**.
The Select HCS Services/Applications tab appears.

**Note** The services that you have not activated also appear, so you can collect crash dump for those services.

**Step 3** Perform one of the following tasks:

- To collect crash dump for all HCS services and applications on the server, check the **Select All Services on All Servers** check box.
- To collect crash dump for all HCS services and applications on a particular server, check the check box beside the server name or server IP address.
- To collect crash dump for specific HCS services and applications on the server, check the check boxes that apply.

**Step 4** Click **Next**.

The Select System Services/Applications tab appears.

**Step 5** Perform one of the following tasks:

- To collect crash dump for all system services and applications on the server, check the **Select All Services on All Servers** check box.
- To collect crash dump for all system services and applications on a particular server, check the check box beside the server name or server IP address.
- To collect crash dump for specific system services and applications on the server, check the check boxes that apply.

**Step 6** Click **Next**.
The Collect File Options page appears.

**Step 7** In the Collection Time group box, specify the time range. Choose one of the following options:

- **Absolute Range:** Specify the server time zone and the time range (start and end date and time).

  By default, the default selection in the Select Reference Server Time Zone list box is the time zone on the RTMT client computer. Your alternate choice is the server time zone.

  Trace & Log Central downloads the files with a time range that is based on the selected time zone. If you have servers in different time zones, Trace & Log Central adjusts for the time change and collects the files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second server (server x) that is in a time zone that is one hour ahead, Trace & Log Central downloads the files from 10:00 a.m. to 11:00 a.m. from server x.

  To set the date range, choose the dates in the From Date/Time and To Date/Time fields.

- **Relative Range:** Specify the time before the current time (in minutes, hours, days, weeks, or months).

**Step 8** In the **Select Partition** list box, choose the partition that contains the system logs.
Cisco Unified Serviceability stores the logs for the version of application that you are logged in to in the active partition and stores the logs for the other version (if installed) in the inactive directory.

This means that when you upgrade from one version of Cisco HCM-F that is running on the Linux platform to another version, and you restart the server with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

**Step 9** To specify the directory in which you want to download the trace files, click **Browse**, navigate to the directory, and click **Open**.
The default path is `<rtmt_install_directory>\<server name or server IP address>\<download time>` where `<rtmt_install_directory>` is the directory where RTMT is installed.

**Step 10** To create a zip file of the crash dump files that you collect, click the **Zip Files** radio button.
To download the crash dump files without zipping the files, click the **Do Not Zip Files** radio button.

**Note** You cannot download a zipped crash dump file that exceeds 2 gigabytes.

**Step 11** To delete collected crash dump files from the server, check the **Delete Collected Log Files from Server** check box.

**Step 12** Click **Finish**.

A message displays that requests confirmation that you want to collect crash dump files (because doing so may affect server performance). To continue, click **OK**.

**Note** If you clicked the Zip Files radio button and the crash dump files exceed 2 gigabytes, the system displays a message that indicates that you cannot collect the crash dump file of that size. Click the **Do Not Zip Files** radio button and try the collection again.

## Collect Audit Logs

The audit user can collect, view, and delete the audit logs. The end user can view the audit logs.

**Note** Only a user with an audit role can delete the audit logs.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** In the Trace & Log Central list, double-click **Audit Logs**.
The Audit Logs dialog box appears.

**Step 3** Choose one of the following actions on the Action Options page:

- Browse Audit Logs: Go to **Step 4**.
- Download Audit Logs: Go to **Step 12**.
- Schedule Download of Audit Logs: Go to **Step 17**.

**Step 4** **To browse audit logs:** In the Audit Logs dialog box, check the **Browse Audit Logs** check box and click **Next**.
The Nodes Selection Options page appears.

**Step 5** Perform one of the following tasks:

- To collect audit logs for all servers, check the **Select All Servers** check box.
  If you have a standalone server and check the **Select All Servers** check box, the system will collect all audit logs for your standalone server.
- To collect audit logs on a particular server, check the check box beside the server name.

**Step 6** Click **Finish**.

A new tab appears in the Trace & Log Central pane, and the Result dialog box appears to indicate that the data is ready for browsing. The tab contains the Nodes folder list in the left pane, and a list of the audit log files in the right pane.

**Step 7** Click **Close** to close the Result dialog box.

**Step 8** In the Nodes list, perform the following actions:

a) Double-click the **Nodes** folder.

b) Double-click the <node> folder (where <node> is the IP address or hostname for the server that you specified).

c) Double-click each folder in the list until one or more files appear in the right pane after you double-click the AuditApp folder.

**Step 9** Perform one of the following actions:

- Open the file in a viewer. Go to **Step 10**.
- Download the audit log. Go to **Step 11**.

**Step 10** To open the file in a viewer, perform the following tasks:

a) Double-click the file.
The Open With dialog box appears.

b) Select the viewer to use.

c) If desired, check the **Always use this program to open these files** check box.

d) Click **OK**.
The viewer opens to show the contents of the audit log. When you are finished reviewing the file, click **Close** to close the viewer.

**Step 11** To download the selected audit log file, perform the following tasks:

a) Click **Download**.
The Select Download Options dialog box appears.

b) To specify the directory in which you want to download the audit log file, click **Browse**, navigate to the directory, and click **Open**.
The default is `<\Program Files\Cisco\HCS\JRtmt>`.

c) To create a zip file of the audit log files that you collect, click the **Zip all Files** radio button.
**Note** You cannot download a zipped audit log file that exceeds 2 gigabytes.

d) To delete collected audit log files from the server, check the **Delete Files on Server** check box.

e) Click **Finish** to close the Select Download Options dialog box. The Information dialog appears to indicate successful completion of the download.

**Step 12** **To download audit logs:** In the Audit Logs dialog box, check the **Download Audit Logs** check box, and click **Next**.

**Step 13** In the Nodes Selection Options section of the Audit Logs dialog box, perform one of the following actions:

- To download the audit logs for all servers, check the **Select All Servers** check box.
If you have a standalone server and check the **Select All Servers** check box, the system will download all audit logs for your standalone server.

- To download the audit logs on a particular server, check the check box beside the server name.

**Step 14** In the Collection Time section of the Audit Logs dialog box, perform one of the following tasks:

- **Absolute Range:** Select the time zone and the start and end dates and time for which you want to collect the audit logs.
  By default, the default selection in the Select Reference Server Time Zone list box is the time zone on the RTMT client computer. Your alternate choice is the server time zone.

  Trace & Log Central downloads the files with a time range that is based on the selected time zone. If you have servers in different time zones, Trace & Log Central adjusts for the time change and collects the files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second server (server x) that is in a time zone that is one hour ahead, Trace & Log Central downloads the files from 10:00 a.m. to 11:00 a.m. from server x.

  To set the date range for which you want to collect audit logs, choose the dates in the From Date/Time and To Date/Time fields.

- **Relative Range:** Specify the time before the current time (in minutes, hours, days, weeks, or months) in which to collect traces.

| Period of Time | Range |
|---|---|
| Minutes | 5 to 60 |
| Hours | 2 to 24 |
| Days | 1 to 31 |
| Weeks | 1 to 4 |
| Months | 1 to 12 |

**Step 15** In the Download File Options section, perform the following tasks:

a) Click **Browse** and specify the download directory.
b) Check the following check boxes, as required:
   **Zip all Files**

   **Delete Collected Log Files from Server**

**Step 16** Click **Finish**.
The collection status is reported in the Trace & Log Central pane.

**Step 17** **To schedule a download of audit logs:** In the Audit Logs dialog box, check the **Schedule Download of Audit Logs** check box and click **Next**.

**Step 18** In the Nodes Selection Options section of the Audit Logs dialog box, perform one of the following actions:

- To download the audit logs for all servers, check the **Select All Servers** check box.
  If you have a standalone server and check the **Select All Servers** check box, the system will download all audit logs for your standalone server.

- To download the audit logs on a particular server, check the check box beside the server name.

**Step 19** In the Schedule Time section of the Audit Logs dialog box, perform one of the following tasks:

- **Select Reference Server Time Zone:** Select the time zone and the start and end dates and time for which you want to collect the audit logs.
  By default, the default selection in the Select Reference Server Time Zone list box is the time zone on the RTMT client computer. Your alternate choice is the server time zone.

  Trace & Log Central downloads the files with a time range that is based on the selected time zone. If you have servers in different time zones, Trace & Log Central adjusts for the time change and collects the files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second server (server x) that is in a time zone that is one hour ahead, Trace & Log Central downloads the files from 10:00 a.m. to 11:00 a.m. from server x.

  To set the date range for the audit logs collection, choose the dates in the Schedule From Date/Time and Schedule End Date/Time fields.
- **Scheduler Frequency:** Specify how often you want to collect audit logs.

**Step 20** Check the following check boxes, as required:

- **Zip all Files**
- **Delete Collected Log Files from Server**

**Step 21** In the Action Options section, check the **Download Files** check box.
The Trace Download Configuration dialog box appears.

**Step 22** In the Trace Download Configuration dialog box, perform the following tasks:

a) Configure the FTP/SFTP parameters.

- Protocol: Select FTP (default) or SFTP.
- Host IP Address: Enter the IP address of the host server.
- User Name: Enter your username.
- Password: Enter your password.
- Port: Enter the FTP or SFTP port information.
- Download Directory Path: Enter the complete directory path where the files get downloaded.
- Click **Test Connection**. When the connection has been tested, the files are downloaded.

b) Click **Test Connection** to verify that the connection is good.

c) When you are finished, click **OK** to close the Trace Download Configuration dialog box.

**Note** HCM-F RTMT does not support the **Localhost** option.

**Localhost** is available for Cisco Intercompany Media Engine servers only. If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command. FTP is not supported for Cisco Intercompany Media Engine.

**Step 23** Click **Finish**.

A confirmation dialog box appears to indicate successful configuration for schedule audit log collection.

## Display Downloaded Trace Files using Local Browse

After you collect trace files and download them to your PC, you can view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within RTMT.

**Note** Do not use Notepad to view collected trace files.

Perform the following procedure to display the log files that you collect with Trace & Log Central. If you zip the trace files for the download, you must unzip them to view them using the viewers within RTMT.

**Note** You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

### Before You Begin

Collect the required trace files. For information, see the following topics:

- Collect Trace Files, on page 84
- Collect and Download Trace Files Using Query Wizard, on page 87
- Schedule Trace Collection, on page 91

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** Double-click **Local Browse**.

**Step 3** Navigate to the directory where you stored the log file and choose the file that you want to view.

**Step 4** Double-click the file (or click **Finish**).
If the file type has a viewer that is already associated with it, the file opens in that viewer. Otherwise, the Open With dialog box appears.

**Step 5** Click the program (viewer) that you want to use to view the file.
If your preferred program is not on the list, choose another program by clicking **Other**.

If you want to use the selected program as your default viewer, check the **Always use this program to open these files** check box.

RTMT displays the file in the chosen viewer. If no other appropriate viewer applies, RTMT opens files in the Generic Log Viewer.

## Display and Download Trace Files using Remote Browse

After the system has generated trace files, you can view them on the server by using the viewers within the Real-Time Monitoring Tool. You can also use the Remote Browse feature to download the traces to your PC.

Perform the following procedure to display and/or download the log files on the server with Trace & Log Central.

**Note** You can open a maximum of five concurrent files for viewing within Trace & Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

### Before You Begin

Collect the required trace files. For information, see the following topics:

- Collect Trace Files, on page 84
- Collect and Download Trace Files Using Query Wizard, on page 87
- Schedule Trace Collection, on page 91

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **Trace & Log Central**.
- On the menu bar, choose **System** > **Tools** > **Trace** > **Trace & Log Central**.

**Step 2** Double-click **Remote Browse**.

**Step 3** Select one of the following radio buttons, and then click **Next**.

- **Trace Files:** Go to **Step 4**.
- **Crash Dumps:** Go to **Step 7**.

**Note** The services that you have not activated also appear, so you can choose traces for those services.

**Note** If you choose Crash Dumps, the wizard displays only the services that may cause a crash dump. If you do not see the service in which you are interested, click **Back** and choose **Trace Files**.

**Step 4** **To display trace files:** Perform one of the following actions on the Select HCS Services/Application tab.

**Note** If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone server.

- To display trace files for all HCS services and applications on the server, check the **Select All Services on All Servers** check box and click **Next**.

- To display trace files for all services and applications on a specific server, check the check box beside the server name and click **Next**.
- To display trace files for services and applications on specific servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without choosing HCS services and applications, click **Next**.

**Step 5** On the Select System Services/Application tab, perform one of the following tasks:

- To display trace files for all system services and applications on the server, check the **Select All Services on All Servers** check box and click **Next**.
- To display trace files for all services and applications on a specific server, check the check box beside the server name and click **Next**.
- To display trace files for services and applications on specific servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without choosing system services and applications, click **Next**.

**Step 6** Click **Finish**.
A new tab appears in the Trace & Log Central pane, and the Result dialog box appears to indicate that the data is ready for browsing. The tab contains the Nodes folder list in the left pane, and a list of the trace files in the right pane. To view the files, go to **Step 10**.

**Step 7** **To display crash dumps:** Perform one of the following actions on the Select HCS Services/Application tab:

**Note** If you have a standalone server and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone server.

- To display crash dump files for all HCS services and applications on the server, check the **Select All Services on All Servers** check box and click **Next**.
- To display crash dump files for all HCS services and applications on a specific server, check the check box beside the server name and click **Next**.
- To display crash dump files for HCS services and applications on specific servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without choosing HCS services and applications, click **Next**.

**Step 8** On the Select System Services/Application tab, perform one of the following tasks:

- To display crash dump files for all system services and applications on the server, check the **Select All Services on All Servers** check box and click **Next**.
- To display crash dump files for all system services and applications on a specific server, check the check box beside the server name and click **Next**.
- To display crash dump files for system services and applications on specific servers, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without choosing system services and applications, click **Next**.

**Step 9** Click **Finish**.

A new tab appears in the Trace & Log Central pane, and the Result dialog box appears to indicate that the data is ready for browsing. The tab contains the Nodes folder list in the left pane, and a list of the crash dump files in the right pane. To view the files, go to **Step 10**.

**Step 10** In the Result dialog box, click **Close**.

**Step 11** In the Nodes list, perform the following actions:

a) Double-click the **Nodes** folder.
b) Double-click the <node> folder (where <node> is the IP address or hostname for the server that you specified).
c) Double-click each folder in the list until one or more files appear in the right pane.

**Step 12** To open the file in a viewer, perform the following tasks:

a) Double-click the file.
The Open With dialog box appears.
b) Select the viewer to use.
c) If desired, check the **Always use this program to open these files** check box.
d) Click **OK**.
The viewer opens to show the contents of the selected file. When you are finished reviewing the file, click **Close** to close the viewer.

## Real-time Trace

The Real Time Trace option in Trace & Log Central allows you to view the current trace file that is being written on the server for each application. If the system has begun writing a trace file, the real-time trace starts reading the file from the point where you began monitoring rather than at the beginning of the trace file. You cannot read the previous content.

The real-time trace provides the option to view real-time data and monitor user events.

## Edit RTMT Trace Settings

To edit trace settings for RTMT, choose **Edit** > **Trace Setting**; then, click the radio button that applies. The system stores the rtmt.log file in the Documents and Settings directory for the user; for example, on a Windows machine, the log is stored in `C:\Documents and Settings\<userid>\.jrtmt\log`.

**Tip** The default Trace Setting is Error.

## Display Messages in SysLog Viewer

You can display messages in SysLog Viewer.

**Note** CiscoSyslog messages (in the Application Logs folder) also display the syslog definition, which includes recommended actions, in an adjacent pane when you double-click the syslog message. You do not have to access the Alarm Definitions in Cisco Unified Serviceability for this information.

The following table describes the SysLog Viewer buttons.

***Table 49: SysLog Viewer Buttons***

| Button | Function |
|---|---|
| **Refresh** | Updates the contents of the current log in SysLog Viewer.<br>**Note** You can enable SysLog Viewer to automatically update the syslog messages every 5 seconds by checking the **Auto Refresh** check box. |
| **Clear** | Clears the display of the current log. |
| **Filter** | Limits the messages that displayed base on the set of options that you select. |
| **Clear Filter** | Removes the filter that limits the type of messages that display. |
| **Find** | Allows you to search for a particular string in the current log. |
| **Save** | Saves the currently selected log on your PC. |

When viewing the syslog message, drag the arrow that appears when your mouse hovers between two column headings to make the column wider or narrower.

You can sort the displayed syslog messages by clicking a column heading. The first time that you click a column heading, the records sort into ascending order. An up arrow indicates ascending order. If you click the column heading again, the records sort into descending order. A down arrow indicates descending order. If you click the column heading one more time, the records revert to unsorted state.

### Procedure

**Step 1** Perform one of the following tasks:

- In the QuickLaunch Channel pane, choose **Tools** > **SysLog Viewer**.

- On the menu bar, choose **System** > **Tools** > **SysLog Viewer** > **Open SysLog Viewer**.

**Step 2** In the Select a Node list box, choose the server where the logs that you want to view are stored.

**Step 3** Click the tab for the logs that you want to view.

**Step 4** Double-click each item in the folder hierarchy until the logs appear in the bottom section of SysLog Viewer.

**Note** If some syslog messages do not appear properly, scroll the mouse pointer over the missing syslog messages to refresh the display.

**Step 5** To filter the syslog message display results, select an option in the **Filter By** list box.
To remove the filter, click **Clear Filter**. All logs reappear after you clear the filter.

**Step 6** To view more information for a syslog message, double-click the syslog message.
The Show Detail dialog box appears for the selected syslog message.

CHAPTER 3

# Backup and Restore



## Overview

The Disaster Recovery System backs up and restores all configuration for Cisco HCM-F and all data that is stored in the Shared Data Repository. In addition, DRS restores its own settings (backup device settings and schedule settings) as part of the backup/restore process. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure the DRS backup device and schedule.

For more detailed information about the backup and restore relationships between Cisco Hosted Collaboration Mediation Fulfillment, Cisco Unified Communications Domain Manager(s) and Cisco Unified Communications Applications, refer to the *Cisco Hosted Collaboration Solution, Release 10.6(1) Maintain and Operate Guide*.

### System Requirements

**Tip** Schedule backups during periods when you expect less network traffic.

**Note** While a backup or restore is running, the command line interface may block you from running some commands, including commands that support upgrades.

Archive backups to a local drive or remote SFTP server. The Disaster Recovery System does not support tape drives for backup and restore on the Cisco Hosted Collaboration Mediation Fulfillment platform. You must choose a local device if you do not have outgoing SFTP access to the Cisco Hosted Collaboration Mediation Fulfillment platform. If you store backup files to a local device, DRS stores the backup files in the /common/adminsftp/backup directory. You must manually move local backup files from the Cisco Hosted Collaboration Mediation Fulfillment platform by opening an SFTP client and connecting to the Cisco Hosted

Collaboration Mediation Fulfillment platform by using the adminsftp user and the administrator password that you set up during installation.

To back up data to a remote device on the network or to move a local backup to another location, you must have an SFTP server that is configured. Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified versions. For information on which vendors have certified their products with your version, refer to the following URL:

http://solutionpartner.cisco.com/web/join-the-network/partner/isv

For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to the following URL:

http://www.globalscape.com/gsftps/cisco.aspx

You may use one of the following third-party servers, but Cisco recommends that you must contact the vendor for support:

- Open SSH (refer to http://sshwindows.sourceforge.net/)
- Cygwin (refer to http://www.cygwin.com/)
- Titan (refer to http://www.titanftp.com/)

**Note** For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

# Disaster Recovery System Access

To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform. To log in to the CLI, you must enter the administrator username and password (from the Cisco HCM-F installation, unless you changed it after installation).

# Master Agent Duties and Activation

The system automatically activates the Master Agent on the Cisco HCM-F platform. The Master Agent performs the following duties:

- The Master Agent stores systemwide component registration information.
- The Master Agent maintains a complete set of scheduled tasks in an XML file. The Master Agent updates this file when it receives updates of schedules from the user interface. The Master Agent sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)
- You access the Master Agent through Disaster Recovery System to perform activities such as configuring backup devices, scheduling backups by adding new backup schedules, viewing or updating an existing schedule, displaying status of executed schedules, and performing system restoration.
- The Master Agent stores backup data on a local directory or a remote network location.

# Local Agents

The server has a Local Agent to perform backup and restore functions. The Local Agent runs backup and restore scripts on the server.

# Backup and Restore Tasks

## Quick-Reference Tables for Backup and Restore Procedures

The following tables provide a quick reference for the backup and restore procedures.

**Note** DRS backs up and restores the drfDevice.xml and drfSchedule.xml files. These backup device settings and schedule settings get restored as a part of the restore process. After the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

### Backup Quick Reference

The following table provides a quick, high-level reference to the major steps, in chronological order, for backups through the Disaster Recovery System.
Note that certain backup rules must be followed:

- No more than two simultaneous application backups per blade; specifically, when creating the scheduled backup list, careful attention is required such that no more than two applications are being backed up at the same time on the same blade.
- The backup schedule list that is created must be created in such a way as not to overload IOPS on a given RAID pool.

For more detailed information on rules to follow when performing a backup, refer to the *Cisco Hosted Collaboration Solution, Release 10.6(1) Maintain and Operate Guide*.

***Table 50: Major Steps for Performing a Backup Procedure***

| Action | Reference |
|---|---|
| Create backup devices on which to back up data. | Manage Backup Devices, on page 110 |
| Create backup schedules to back up data on a schedule. | Create Backup Schedules, on page 111 |
| Enable and disable backup schedules to back up data. | Enable, Disable, and Delete Schedules, on page 112 |

| Action | Reference |
|---|---|
| Optionally, run a manual backup.<br>**Note** If you run a manual backup, make sure that the engineering rules for a backup are followed. | Start Manual Backup, on page 113 |
| Check the Status of the Backup—While a backup is running, you can check the status of the current backup job. | Check Backup Status, on page 113 |

## Restore Quick Reference

The following table provides a quick, high-level reference to the major steps, in chronological order, for restores through the Disaster Recovery System.

***Table 51: Major Steps for Performing a Restore Procedure***

| Action | Reference |
|---|---|
| Restore a backup file from a local or network directory. | Restore Cisco HCM-F, on page 114 |
| Check the Status of the Restore—While the restore process is running, you can check the status of the current restore job. | View Restore Status, on page 116 |

# Manage Backup Devices

Before using the Disaster Recovery System, you must configure the locations where you want the backup files to be stored. You can create local or network backup devices. If you create a local backup device, Disaster Recovery System stores the backup files in the a preconfigured directory on the Cisco HCM-F platform. You must manually move local backup files from the Cisco HCM-F platform by opening an SFTP client and connecting to the Cisco HCM-F platform by using the adminsftp user and the administrator password that you set up during Cisco HCM-F installation.

**Note** You can estimate the size of the .tar file that the backup creates by entering **utils disaster_recovery estimate_tar_size HCS**.

You can configure up to 10 backup devices. Perform the following steps to configure backup devices.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** To create a local device, enter **utils disaster_recovery add local** *device_name number of backups*
where

*device_name* equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), hyphens (-) and underscores (_). Do not use any other characters. By default, DRS stores backup files for local devices in the /common/adminsftp/backup directory.

*number of backups* equals the number of backups that are retained for the backup server. When the backup reaches the limit, the oldest backup files on the backup server are deleted and the new backup files are added.

**Step 3** To create a network device so that you can store backup files on a network drive that is accessed through an SFTP connection, enter **utils disaster_recovery device add network** *device_name path server_name username number_of_backups*
where

*device_name* equals the name of the backup device. The backup device name may contain only alphanumeric characters, spaces ( ), hyphens (-) and underscores (_). Do not use any other characters.

*path* equals the path name for the directory where you want to store the backup file

*server_name* equals the name or IP address of the network server

*username* equals a valid username for an account on the remote system

*number of backups* equals the number of backups allowed for this device

**Note** You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. The account that is used to access the SFTP server must have write permission for the selected path.

**Note** The DRS Master Agent validates the selected backup device. If the username, password, server name, or directory path is invalid, the command fails.

**Step 4** To display a list of backup devices, enter **utils disaster_recovery** *device list*.
The device name, device type, and device path for each backup device displays.

**Step 5** To delete a backup device, enter **utils disaster_recovery device delete** *device_name*, where *device_name* equals the name of the device that you want to delete.

**Note** You cannot delete a backup device that is configured as the backup device in a backup schedule. You must first delete the schedule which uses this device name, and then delete this device.

# Create Backup Schedules

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.

**Caution** Schedule backups during off-peak hours to avoid call-processing interruptions and impact to service.

**Note** To view a history of backups, enter **utils disaster_recovery history Backup**. The results of all backups display.

Perform the following steps to create backup schedules:

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** Enter **utils disaster_recovery schedule add** *schedulename devicename featurelist datetime frequency* where

*schedulename* equals the name of the schedule

*devicename* equals the location where Disaster Recovery System stores the backup files

*featurelist* equals HCS

*datetime* specifies the time and date when Disaster Recovery System performs the backup. The format is yyyy/mm/dd-hh:mm. Enter the time based on a 24-hour clock.

*frequency* equals how often Disaster Recovery System performs the backup. Options are once, daily, weekly, and monthly.

**Step 3** To enable a schedule, enter **utils disaster_recovery schedule enable** *schedulename.*
The next backup occurs automatically at the time that you set.

**Note** To disable or delete schedules, see the Enable, Disable, and Delete Schedules, on page 112.

## Enable, Disable, and Delete Schedules

Follow this procedure to enable, disable, or delete backup schedules.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** To view the list of backup schedules, enter **utils disaster_recovery schedule list**.
The CLI displays the device name and status for each schedule. The device name specifies where Disaster Recovery System stores the backup files.

**Step 3** Perform one of the following tasks:

a) To enable a schedule, enter **utils disaster_recovery schedule enable** schedulename.

b) To disable a schedule, enter **utils disaster_recovery schedule disable** schedulename.

c) To delete a schedule, enter **utils disaster_recovery schedule delete** schedulename.
The schedules can be enabled, disabled, or deleted only one at a time.

# Start Manual Backup

Follow this procedure to start a manual backup.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** Enter **utils disaster_recovery backup** *type featurelist device_name*
where

type equals the location of the backup, either local or network

*featurelist* equals HCS

*device_name* equals the name of the backup device

**Step 3** To view the status of the current backup, enter **utils disaster_recovery status backup**.

**Step 4** To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.

# Check Backup Status

You can check the status of the current backup job and cancel the current backup job. 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. You will then need to begin a fresh backup.

**Note** Successful backups display a status of successful. To view a history of backups, enter **utils disaster_recovery history backup**. The results of all backups display.

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** To view the status of the current backup, enter **utils disaster_recovery status backup**.

**Step 3** To cancel the current backup, enter **utils disaster_recovery cancel_backup yes**.
**Note** The backup cancels after the current component completes its backup operation.

# Display Backup Files

Using the following procedures, you can see the list of backup files that are stored to the local or network drives:

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** To view backup files, do one of the following:

- To view the list of backup files in the local directory (/common/adminsftp/backup), enter **utils disaster_recovery show_backupfiles local backup**.
- To view the list of backup files in the local restore directory (/common/adminsftp/restore), enter **utils disaster_recovery show_backupfiles local restore**.
- To view the list of backup files on a network drive, enter **utils disaster_recovery show_backupfiles network** *path servername userid.*

where

*path* equals the path name for the directory where the backup file is stored

*servername* equals the name or IP address of the network server

*userid* equals a valid user ID for an account on the remote system

# Restore Cisco HCM-F

You can restore the data for Cisco HCM-F from a backup file in a network directory or in a local directory. Use one of the following procedures to restore the data for Cisco HCM-F:

**Caution** Before you restore Cisco HCM-F platform, ensure that the Cisco HCM-F version that is installed on the platform matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Cisco HCM-F for restore. For example, the Disaster Recovery System does not allow a restore from Version 8.6(**2**)ES1.1000-1 to Version 8.6(**2**)ES1.1000-2. Essentially, the product version needs to match, end-to-end, for the Disaster Recovery System to run a successful restore. Disaster Recovery System adheres to strict version checking and allows restore only between matching versions of Cisco HCM-F.

**Note** After you choose the server to which you want the data restored, any existing data on that server gets overwritten.

**Important** In multi-node systems, restore the App node first, then restore any WS nodes.

### Procedure

**Step 1** Copy the backup file to the Cisco HCM-F platform by opening an SFTP client, and connecting to the Cisco HCM-F platform by using the adminsftp user and the administrator password that you set up during installation. To do that, navigate to the backup directory by entering **cd backup**, and copy the backup file to the /common/adminsftp/restore directory.

**Step 2** Access the Disaster Recovery System by starting an SSH session and logging in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 3** Enter **utils disaster_recovery restore local** *restore_server tarfilename device_name*
where

*restore_server* equals the hostname of the server to be restored

*tarfilename* equals the name of the backup file to be restored without extension; for example, 2008-01-21-18-25-03

device_name equals the name of the backup device

**Step 4** Your data gets restored on the server that you chose. To view the status of the restore, enter **utils disaster_recovery status restore**.

**Step 5** Restart the Cisco HCM-F platform.

### What to Do Next

**Important** In a multi-node system, after restoring the App node and all WS nodes, run the **set hcs sdrconfig** command on each WS node to fetch the new SDR credentials.

# View Restore Status

To check the status of the current restore job, perform the following steps:

### Procedure

**Step 1** To access the Disaster Recovery System, start an SSH session and log in to the CLI on the Cisco HCM-F platform.
The CLI admin prompt displays.

**Step 2** To view information about the current restore job, enter **utils disaster_recovery status restore**. The status shows the restore percentage, log file location, timestamp, feature name, platform name, component name, and component status.

# Error messages

The Disaster Recovery System (DRS) issues alarms for various errors that can occur during a backup or restore procedure. The following table provides a list of Cisco DRS alarms:

***Table 52: Disaster Recovery System Alarms***

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFBackupDeviceError | DRF backup process has problems accessing device. | DRS backup process encountered errors while it was accessing device. |
| DRFBackupFailure | Cisco DRF Backup process failed. | DRS backup process encountered errors. |
| DRFBackupInProgress | New backup cannot start while another backup is still running. | DRS cannot start new backup while another backup is still running. |
| DRFInternalProcessFailure | DRF internal process encountered an error. | DRS internal process encountered an error. |
| DRFLA2MAFailure | DRF Local Agent cannot connect to Master Agent. | DRS Local Agent cannot connect to Master Agent. |
| DRFLocalAgentStartFailure | DRF Local Agent does not start. | DRS Local Agent may be down. |
| DRFLocalDeviceError | DRF has problems accessing local device. | DRS encountered errors while it was accessing local device. |
| DRFMA2LAFailure | DRF Master Agent does not connect to Local Agent. | DRS Master Agent cannot connect to Local Agent. |

| Alarm Name | Description | Explanation |
|---|---|---|
| DRFMABackupComponentFailure | DRF cannot back up at least one component. | DRS requested a component to back up its data; however, an error occurred during the backup process, and the component did not 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 Agent was running a backup operation, the Cisco HCM-F platform disconnected before the backup operation completed. |
| DRFMARestoreComponentFailure | DRF cannot restore at least one component. | DRS requested a component to restore its data; however, an error occurred during the restore process, and the component did not get restored. |
| DRFMARestoreNodeDisconnect | The node that is being restored disconnected from the Master Agent prior to being fully restored. | While the DRS Master Agent was running a restore operation on the Cisco HCM-F platform, the platform disconnected before the restore operation completed. |
| DRFMasterAgentStartFailure | DRF Master Agent did not start. | DRS Master Agent may be down. |
| DRFNoRegisteredComponent | No registered components are available, so backup failed. | DRS backup failed because no registered components are available. |
| DRFNoRegisteredFeature | No feature got selected for backup. | No feature got selected for backup. |
| DRFRestoreDeviceError | DRF restore process has problems accessing device. | DRS restore process cannot read from device. |
| DRFRestoreFailure | DRF restore process failed. | DRS restore process encountered errors. |
| DRFSftpFailure | DRF SFTP operation has errors. | Errors exist in DRS SFTP operation. |
| DRFSecurityViolation | DRF system detected a malicious pattern that can result in a security violation. | The DRF Network Message contains a malicious pattern that can result in a security violation like code injection or directory traversal. DRF Network Message has been blocked. |
| DRFTruststoreMissing | The IPsec trust store is missing on the node. | The IPsec trust store is missing on the node. DRF Local Agent cannot connect to Master Agent. |
| DRFUnknownClient | DRF Master Agent on the platform received a client connection request from an unknown server. The request has been rejected. | The DRF Master Agent on the platform received a client connection request from an unknown server. The request has been rejected. |

CHAPTER 4

# Service Inventory Common Report Format



## Service Inventory Data

This section provides an outline of the types of data that are collected during the Service Inventory process. The purpose of the format specification is to represent the information in a common format that is not specifically tied to any single customer's format requirements. The data points listed comprise elements required by current customers, elements required by Cisco, and additional fields that are reserved for future use. This section is a summary of the types of data that are collected and is not a complete list. See the format definitions and example files in Filename Specifications, on page 124 for a complete listing of fields and data.

### Data Points

**Note** This listing does not specify the order or arrangement of data in the files. This section provides a summary of the types of data that are presented.

## Report Summary Information

The following data points are included in the Report Summary Information:

- Filename
- Domain Manager Hostname
- Domain Manager IP Address
- Reporting Period Start Date/Time (reporting period)
- Reporting Period End Date/Time (reporting period)

## Report Statistical Information

The following data points are included in the Report Statistical Information:

- Total Provider Count
- Total Reseller Count
- Total Customer Count
- Total Site Count
- Total Subscriber Count
- Total Unassigned Device Count
- Total MACD Row Count

## Service Inventory Report Data

The following data points are found in the Service Inventory Report Data:

- Report Summary information
  - Report format version
  - Filename
  - Domain Manager details
  - Start date/time and End date/time
- Provider information
  - Provider Name
  - Provider ID
- Reseller information
  - Provider ID
  - Reseller Name

  - Reseller ID

- Customer Information
  - Provider and Reseller ID
  - Customer ID and Name
  - Address
  - Contact Information
  - Additional Details

- Customer Device Details
  - Customer Device Information
  - Device Make
  - Device Model

- Site Information
  - Customer ID
  - Site ID
  - Site Name
  - Site Address
  - Additional Details

- Subscriber Information
  - Customer Name
  - Site Name
  - Subscriber Username
  - License type consumed and number of licenses
  - Entitlement information, including Entitlement Profile and Entitlement Catalog
  - EM Enabled and SNR Enabled

- Subscriber Feature Information
  - Customer Name
  - Feature Name/Identifier
  - Feature State Details

- Device/Line Information
  - Device identifiers, Device MAC addresses
  - Device License details

    - Device Line Associations

- Move/Add/Change/Delete (MACD) Information
    - Provider MACD Events
    - Reseller MACD Events
    - Customer MACD Events
    - Site MACD Events
    - Subscriber MACD Events
    - Feature MACD Events
    - Device MACD Events
    - Line MACD Events

- Statistical Information
    - Total number of Providers, Resellers, Customers, Sites, and Subscribers
    - Total number of Devices assigned and unassigned
    - Total number of MACD rows
    - Timestamps indicating when SI files were requested, proceessed and completed, for performance and debugging information

- Summary Information
    - Prime License Manager server usage summary
    - Customer license usage summary
    - Site level license usage summary

# Viewing Layout and Format

This section outlines the layout and format of data points in the Cisco Service Inventory output file. In general, the data stored in the files is displayed by the customer with some additional processing information included where necessary. The following section gives an overview of the format, a description of the file layout, a listing of the various row formats and data types that are in the output files, and finally, examples of Cisco Service Inventory output files.

Service Inventory can produce three different types of reports:

- Unified Communications Domain Manager Service Inventory Common Format (.si)
- UC Application Service Inventory Common Format (.ucsi)
- UC Application MACD Format (.simacd)

# File Extensions and Output

The Cisco Unified Communications Domain Manager Service Inventory Common Format presents all necessary data in a human-readable format while keeping output file size to a minimum. The format is an ASCII-based file with the ".si" file extension. Files that are delivered by the Cisco Unified Communications Domain Manager server (or any other Domain Manager) before final output are identified by the ".dsi" file extension ("Domain Manager Service Inventory"). The Domain Manager server delivers files in a single-file output. The file extension for the UC Application Service Inventory Common Format is ".ucsi". The Service Inventory application also maintains additional intermediate file formats that follow a similar naming convention; however, these file formats are for internal use only and are not the focus of this document.

The output is arranged into the following sections:

- Report Summary Information
- Report Definition Information
- Service Inventory Data
  - **Provider Data** > **Reseller Data** > **Customer Data** > **Site Data** > **Subscriber Data (+Subscriber Feature Data, +Subscriber License Data, + Subscriber Device Data, +Subscriber Entitlement Data)**
- MACD Data
  - Reseller, Customer, Site, Subscriber, Device, Line, and Feature Group MACD Data
- Report Statistical Information

# MACD Data

MACD data in the file is represented as a row indicating the updated state of whatever entity is currently being added, changed, or deleted. Unlike a change notification, which shows a "before" and "after" state of the entity, the MACD representation shows only the "after" state. For a delete operation, the "before" state is shown fully, and in most cases, it shows precisely the information that is being deleted. This information may differ depending on the Unified Communications Domain Manager and the case. Where necessary, the parsing applications must interpret intermediate states based on the combination of static service inventory data and MACD data.

You can also run a report for the UC Applications that is slightly different from the MACD for the Unified Communications Domain Manager report. See MACD Format for UC Applications, on page 164.

# UC Application Service Inventory Common Format

The Unified Communications Application Service Inventory Common Format generates a report with information that is specific to the UC Application. It contains similar information to the Unified Communications Domain Manager report but with data from your UC Application. You can also generate a specific report for MACD information on your UC Application. See MACD Format for UC Applications, on page 164.

# Filename Specifications

The format of the service inventory filenames are critical to the proper operation of the SI applications. The following parameters apply to filenames in this format:

- The filename follows this format:

```
<date><time><timezone>+<domainManagerSequenceID>+<domainManagerType>+<fileNumber>+
<fileCount>.<extension>
```

| Formats | Example |
|---|---|
| **File:** | **20110528032327GMT+1+CUCDM+1+1.dsi** |
| 1 File for Cisco Unified Communications Domain Manager 8.x: | 110528032329GMT+1+CUCDM+1+1.csi |
| 1 File for Cisco Unified Communications Domain Manager 10.x: | 20110528032329GMT+1+CUCDM2+1+1.si |
| 3 Split Files (Cisco Unified Communications Domain Manager 8.x): | `20110528032329GMT+1+CUCDM+1+3.si`<br>`20110528032329GMT+Chicago45+CUCDM+2+3.si`<br>`20110528032329GMT+1+CUCDM+2+3.si` |

- The standard field delimiter in the filename is “+”. This avoids UNIX/Linux escape character issues and minimizes character escape when writing Java applications against the format.
- The <**domainManagerSequenceID**> field is mandatory and identifies the specific Domain Manager that is used to generate the output file. This field must be unique across Domain Managers within a data center.

If it becomes necessary to compress the service inventory file for any reason, prior to transmission across a network, for instance, then the transmitting entity "ZIPs" up the file in an appropriate format. We recommend a ".gz" file format. Domain managers add the .gz extension to the existing filename+extension. In this case, the transmitted file is “<filename>.<extension>.gz”.

Additionally, you should assign compressed files the appropriate permissions to allow proper reading and writing upon being extracted into their uncompressed form. We recommend an “a+rw” permission. File ownership should be treated similarly.

# General Format Specifications

Additional general format specifications include:

- Data elements in the file are stored in text, integer, and standard date/time formats where appropriate.

- The standard end-of-line character "\n", while not typically visible in common text-editing applications, is used and available for parsing applications to use for line tokenization.
- The data element delimiter is the pipe symbol (|). Each line starts and ends with a pipe symbol, with a pipe symbol between each data point on the line.
- The pipe symbol "|" is not a valid character within fields in the format.
- An empty (null) field is represented by a tilde symbol (~). Empty fields/columns are not skipped.
- Data rows that are entirely or partially inaccurate are appended with an asterisk (*). This notation is *not* applied to Report Summary or Report Definition rows. For more information see Data Accuracy Handling, on page 125.
- All MACD rows in the file are listed in the MACD section defined by the starting tag |**MACDSTART**| and by the closing tag |**MACDEND**|. (For more information see MACD Row Format, on page 143 .) MACD rows are ordered TOP to BOTTOM in the file by timestamp, NEWEST to OLDEST.

# Data Accuracy Handling

Certain scenarios exist in which the data provided is not entirely accurate or does not even exist while Service Inventory data is processed. To effectively handle such scenarios while still preserving the overall integrity of a service inventory file, the format provides the asterisk (*) symbol for proper notation.

**Note** You cannot apply this notation to Report Summary rows. Use caution with parsing applications that handle and process data in the report.

## Usage Conventions and Scenarios

If a single data element is known to be invalid, an asterisk is placed at the end of the field itself.

### Use of asterisk at the end of a field

```
|CUST|1|31|1|XYZ, Inc.|~| ~*|~*|~*|~*|~*|~*|~*|
```

**Note** The * after the ~ in the preceding example indicates that the fields are not empty but are shown as empty because the actual values for the data field in question cannot be provided for some reason. For more information see Customer Data Row, on page 137.

If an entire row is known to be inaccurate, the asterisk is placed at the end of the row outside the final pipe symbol.

### Use of asterisk at the end of a row

```
|DEF|FGROUP|CompanyXYZ|1|Basic Feature Group|10|11|19|17|*
```

**Note** The * in the preceding example indicates here that the list of features in this feature group are not guaranteed to be accurate at report generation time. For more information the feature group definition row field see Report Definition Row, on page 129.

# Global Data Formats

This section outlines the data formats that are used throughout the row formats. Deviation from these global formats is not permitted in the scope of this SI Common Format definition.

## Telephone Number (Internal TN)

This format describes the representation of an internal telephone number (TN) or line (terms used interchangeably) throughout the specification.

| Format | Example |
|---|---|
| \|<internalTN>\| | `\|810100001\|` |

**Note** Anywhere internal TNs are reported, the format is changed to report the IPPBX-configured full internal number.

## Telephone Number (External TN)

This format describes the representation of an external E.164-compliant telephone number (TN) or line (terms used interchangeably) throughout the specification.

| Format | Example |
|---|---|
| \|+<countryCode><areaCode><localNumber>\| | `\|+19195552600\|` |

**Note** External TNs that are listed in the report must adhere to the standard E.164 format specification. Typically, a list of external E.164 telephone numbers is associated with an internal TN. The first E.164 number listed (if there is more than one) is the primary E.164 number.

# Device Identifier Fields

This format describes the representation of a device name and, where applicable, the device type, the Media Access Control (MAC) address number throughout the specification.

| Format | Examples |
|---|---|
| |<deviceName>| <16DigitHexMACAddress>| | `\|SEP044553abf49C\|044553abf49C\| \|TCPNAME\|~\|` |

**Note** No colon (:) is needed between the HEX digits in the MAC address element.

# Date/Time Element

This format definition describes the way in which Date/Time elements are represented in information rows. All dates/times are represented in Greenwich Mean Time. All times are represented in 24-hour format. No separate definition row is required in the file to describe the date elements.

The following describes the characters that are used to construct the format:

- **yyyy** = Year
- **MM** = Month
- **dd** = Day
- **HH** = Hours
- **mm** = Minutes
- **ss** = Seconds
- **z** = Time Zone

| Format | Example |
|---|---|
| |<yyyyMMddHHmmssz>| | `\|20110423163455GMT\|` |

# Time Zone Element

This format describes the representation of a Time Zone throughout the report. The Time Zone format is <"Region/City">.

| Format | Examples |
|---|---|
| \|<timeZone>\| | `\|Africa/Pretoria\|`<br>`\|Europe/London\|`<br>`\|Pacific/Fiji\|`<br>`\|Indian/Maldives\|` |

# Row Format Specifications

This section outlines the various secondary row formats that are used in the Cisco SI Common Format. Each type specification provides a format definition and an example usage.

## File Header

File Header is the first line of each output file.

| Format | Example |
|---|---|
| \|FSTART\| | `\|FSTART\|` |

**Note** This row is *required*.

## File Footer

File Footer is the last line of each output file.

| Format | Example |
|---|---|
| \|FEND\| | `\|FEND\|` |

**Note** This row is *required*.

# Report Definition Header

| Format | Example |
|---|---|
| \|DEFSTART\| | `\|DEFSTART\|` |

**Note** This row is *required*.

# Report Definition Row

These row definitions specify which interpreted fields later on in the format are defined specific to the file. For instance, you need to define the list of features that are available on the system before specifying feature inclusion in a feature group. By encapsulating these definitions in the output, a parsing application can programmatically, at runtime, determine how to interpret information that is presented later in the output file.

| Format |
|---|
| \|DEF\|<definitionName>\|{additional column definitions here}\| |

## Country Code Definition

| Format | Example |
|---|---|
| \|DEF\|COUNTRY\|<country[1] ID>\|<country[1] Name>\|<country[1] Code>\|…\|<country[N]ID>\| <country[N]Name>\|<country[N] Code>\| | `\|DEF\|COUNTRY\|15\|United States\|USA\|16\|United Kingdom\|UK\|` |

- This definition format permits the country code data to appear in either a two-character representation or a three-character representation. Parsing applications may use the definition row to map “country_X_id” to the appropriate names and abbreviations.
- All fields are *required* in this row.

## Domain Manager Global Feature List Definition

| Format | Example |
|---|---|
| \|DEF\|FEATURES\|<br><feature_1_ID>\|<br><feature_1_Name>\|…\|<br><feature_N_ID>\|<br><feature_N_Name>\| | `\|DEF\|FEATURES\|10\|Voice\|11\|Voicemail\|19\|Mobility\|` |

- This row defines all possible features that are available on the current version of the Domain Manager server. Both **<featureID>** and **<featureName>** are required to properly map these features to subscribers and devices through the Feature Group Definition Row later in the file format.
- The Cisco Unified Communications Domain Manager server provides a list of more than 50 features. In this case, the definition row for a report from that Domain Manager define the same number of **<featureID>-<featureName>** pairs.
- The **<featureID>** values in this row are merely integers used for cross-reference within the current file. There is no guarantee of consistency for these IDs between different physical files. The integers are generated at runtime.
- The actual list of <**feature**> values corresponds to the supported features on the current version of the Unified Communications Domain Manager server, regardless of the report format version being generated. For example, you can generate an 8.6(2) SI report version using an 8.1 Unified Communications Domain Manager application. In this case, the 8.6.2.1 report may contain features that did not exist on a 8.0 Unified Communications Domain Manager application serving as the source of data for the same report version. Parsing applications import the features list at runtime to ensure data integrity and not simply validate features or feature groups based on <**featureID**> values. Each <**featureID**> value is still guaranteed to be a unique integer within the space of all <**featureID**> values.
- All fields are *required* in this row.

## Customer Feature Group Definition

| Format | Examples |
|---|---|
| \|DEF\|FGROUP\|<br><customerName>\|<br><featureGroupID>\|<br><featureGroupName>\|<feature[1]ID>\|<feature[2]ID>\|…\|<feature[N]ID>\| | `\|DEF\|FGROUP\|CompanyXYZ\|-1\|Basic Feature Group\|10\|11\|19\|17\|`<br><br>`\|DEF\|FGROUP\|CompanyXYZ\|-1\|Advanced Feature Group\|10\|11\|19\|17\|22\|34\|35\|36\|53\|` |

| Format | Examples |
|---|---|
| • This row defines all features that are assigned as part of a feature group.<br>• Features listed in the feature group definition row are “assigned” and available to those subscribers who were placed in this group. A subscriber does not necessarily use these features.<br>• *All fields are **required** in this row.*<br>• The usage of the <ID> fields in the service inventory section of the report is deprecated. The value of the <featureGroupID> is replaced with “-1” , during data translation or correction, since its original value accuracy is no longer guaranteed. | |

## Customer Device Definition Row

| Format | Example |
|---|---|
| | `\|DEF\|DEV\|CompanyXYZ\|1\|Cisco\|7960\|2\|Cisco\|7965\|3\|Cisco\|Cius_V1 \|4\|Avaya\|Phone1000\|5\|Apple\|iPhone 3GS\|11\|Cisco\|CUPC8\|`<br>Example - Entitlement Feature Group<br>`\|DEF\|EFGROUP\|EntitlementFeatureGroup_1\|1\|51\|`<br>Example - Entitlement Device Group<br>`\|DEF\|DGROUP\|devicegroup2\|3\|~\|Cisco DX80\|2\|~\|Cisco 7961\|1\|~\|Cisco 7961G-GE\|`<br>Example - Entitlement Catalog<br>`\|DEF\|ECATALOG\|Provider1\|Reseller 1\|~\|EntitlementFeatureGroup_1\|10\|devicegrp1\| 9\|devicegroup2\|1\|`<br>Example - Entitlement Profile<br>`\|DEF\|EPROFILE\|Provider1\|Reseller1\|Customer1\|ent_profile\|EntitlementFeatureGroup_3 \|1\|devicegroup2\|1\|` |

| Format | Example |
|---|---|
| \|DEF\|DEV\| <customerName>\|<device [1]ID>\|<device[1]Make>\| <device[1]Model>\|…\| <device[N]ID>\|<device[N] Make>\|<device[N]Model>\|<br>**Format for Entitlement Feature Group:**<br>\|DEF\|EFGROUP\|<Entitlement Feature Group Name>\| feature [1] ID\|>\|<feature [2] ID>\|…\|<feature [N] ID>\|<br>**Format for Entitlement Device Group:**<br>\|DEF\|DGROUP\|<Entitlement Device Group Name>\|>\|<device [1] ID>\|<device [1] Make>\|<device [1] Model>\|…\|<device [N] ID>\|<device [N] Make>\|<device [N] Model>\|<br>**Format for Entitlement Catalog:**<br>\|DEF\|ECATALOG\|<Provider Name>\|<Reseller Name>\|<Customer Name>\|<Entitlement Feature Group Name>\|<maximum allowed number of total devices irrespective of the device groupings>\|<Device Group [1] Name>\|<maximum allowed number of devices in the group >\|… \|< Device Group [n] Name >\|< | |

| Format | Example |
|---|---|
| maximum allowed number of devices in the group >\|<br>**Format for Entitlement Profile:**<br>\|DEF\| EPROFILE \|<Provider Name>\|<Reseller Name>\|<Customer Name>\|<Entitlement Profile Name>\|<Entitlement Feature Group Name>\|< maximum allowed number of total devices irrespective of the device groupings>\|<Device Group [1] Name>\|< maximum allowed number of devices in the group >\|… \|< Device Group [n] Name >\|< maximum allowed number of devices in the group >\| | |

- The **<deviceID>** field is used to cross-reference the device make and model information in the Device Data Row, on page 141 for a particular device assigned to a subscriber.
- The device ID is a value provided by the CUCDM server that stores the device make and model information.
- Soft clients and mobile devices are reported in this row.
- All fields are *required*.

**Note** The Feature Definition, |DEF|FEATURES| in the Service Inventory report for Cisco Unified Communications Domain Manager 10.x are derived from features assigned to each subscriber, phone.

**Note** Cisco Unified Communications Domain Manager 10.x does not have the concept Feature Groups (FGROUP). For backward compatibility reasons, Service inventory reports notional feature group (FGROUP) definitions for reports generated from Cisco Unified Communications Domain Manager 10.x. This notional Feature Group is based on the actual feature assigned to each subscriber.

**Note** The Customer *Device Definition* rows |DEF|DEV| in the SI report for Cisco Unified Communications Domain Manager 10.x are derived from the actual devices configured for subscriber or devices provisioned under a site.

# Report Definition Footer

| Format | Example |
|---|---|
| \|DEFEND\| | `\|DEFEND\|` |

**Note** This row is *required*.

# SI Report Header

| Format | Example |
|---|---|
| \|SISTART\| | `\|SISTART\|` |

**Note** This row is *required*.

# Provider Data Row

| Format | Example |
|---|---|
| \|PROV\|<providerID>\| <providerName>\| | `\|PROV\|-1\|PartnerXYZ\|` |

**Note** All fields are *required* in this row.

**Note** The **<providerID>** field value is always “-1” because its original value accuracy is not guaranteed.

# Provider Footer Row

| Format | Example |
|---|---|
| \|PEND\| | `\|PEND\|` |

**Note** This row is *required* if a |PROV| data row exists.

# Reseller Data Row

| Format | Example |
|---|---|
| \|RESELL\|<providerID>\|<resellerID>\|<resellerName>\| | `\|RESELL\|-1\|-1\|ResellerXYZ\|` |

**Note** All fields are *required* in this row.

**Note** The **<providerID>** and **<resellerID>** field values are always “-1” because their original value accuracy is not guaranteed.

# Reseller Footer Row

| Format | Example |
|---|---|
| \|REND\| | `\|REND\|` |

**Note** This row is *required* if a |RESELL| data row exists.

# Customer Data Row

The **<customerCountry>** within this field is represented by an ID that maps to the country definition row in this example.

| Format | Example |
|---|---|
| \|CUST\|<providerID>\|<br><resellerID>\|<customerID>\|<br><customerName>\|<br><externalCustomerID>\|<br><customerAddress1>\|<br><customerAddress2>\|<br><customerAddress3>\|<br><customerCity>\|<customerState>\|<br><customerCountry>\|<br><customerPostalCode>\| | `\|CUST\|-1\|-1\|-1\|XYZ, Inc.\|~\|7600 RTP Road\|~\|~\|Cary\|NC\|15\|27513\|` |

**Note** All fields are *required* in this row.

**Note** The **<provider_id>**, **<reseller_id>** and **<customer_id>** **<providerID>** field values are always "-1" because its original value accuracy is not guaranteed.

# Customer Footer Row

| Format | Example |
|---|---|
| \|CEND\| | `\|CEND\|` |

**Note** This row is *required* row if a **|CUST|** data row exists.

# Site Data Row

| Format | Example |
|---|---|
| \|SITE\|<customerID>\|<siteID>\|<siteName>\|<externalSiteID>\|<siteAddress1>\|<siteAddress2>\|<siteAddress3>\|<siteCity>\|<siteState>\|<siteCountry>\|<sitePostalCode>\|<cityTimezone>\| | `\|SITE\|-1\|-1\|RTP\|~\|7600 RTP Road\|~\|~\|Cary\|NC\|15\|27513\|EST\|`<br><br>`\|SITE\|-1\|-1\|New York\|~\|100 Broadway Ave\|~\|~\|New York\|NY\|15\|10101\|EST\|` |

- For more information about the proper representation of the <cityTimezone> field for the site/location, see Time Zone Element, on page 127.
- All fields are*required* in this row.

**Note** All fields are *required* in this row.

**Note** The field values for**<customer_id>** and **<site_id>** are replaced with “-1” because their original value accuracy is not guaranteed.

# Site Footer Row

| Format | Example |
|---|---|
| \|SEND\| | `\|SEND\|` |

**Note** This is a *required* row if a |SITE| data row exists.

# Subscriber Data Row

This section describes the format of the Subscriber Data Row.

| Format | Example |
|---|---|
| |SUB|<customerID>|<siteID>|<subID>|<subUsername>|<subEmail>|<subNameFirst>|<subNameMiddle>|<subNameLast>|<subTitle>|<subDepartment>|<subDepartmentCode>|<subContactTelephone>|<featureGroupName>|EntitlementProfile|<EM Enabled>|<SNR Enabled>|<HCS License type>| <License Count>|…|<HCS License type>|<License Count>| | `\|SUB\|-1\|-1\|-1\|jsmith\|jsmith@xyz.com\|John\|Thomas\|Smith\|Manager\|Finance\|99\|+19198548001\|Basic Services\|BasicProfile\|0\|0\|~\|0\|`<br><br>`\|SUB\|-1\|-1\|-1\|jdoe\|jdoe@xyz.com\|Jane\|Mary\|Doe\|SeniorAccountant\|Finance\|99\|+19198548005\|Basic Services\|~\|0\|0\|~\|0\|`<br><br>In the above examples, both John Smith and Jane Doe are a part of feature group “Basic Services”. The assignment determines the features available to John and Jane as defined in the feature group definition row with the corresponding **<customerName>** and **<featureGroupName>**.<br><br>`\|SUB\|-1\|-1\|-1\|larryj\|larryj@cisco.com\|Larry\|~\|Jones\|~\|~\|~\|~\|Group1\|StandardProfile\|0\|0\|HCS Foundation\|1\|`<br><br>In the above example, Larry Jones is part of Feature Group “Group1”. “Group1” is not a feature group defined in Cisco Unified Communications Domain Manager. It is a Service Inventory derived feature group (derived from Features assigned to subscribers when the SI report is generated). Also <EM Enabled>/<SNR Enabled> is indicated by a 1 or 0 value, where 1 is Enabled. If a subscriber activates a license then the <HCS License Type> indicates the type of license activated and <License Count> indicates the number of license units of license activated. If a subscriber activates more than one type of license, then each type of license, along with the number of license units activated is reported in the Subscriber data row.<br><br>`\|SUB\|-1\|-1\|-1\|staufel\|staufel@cisco.com\|Simon\|~\|Tuafel\|~\|~\|~\|~\|Group1\|Advanced Profile\|0\|0\|HCS Foundation\|1\|Telepresence Room\|1\|`<br><br>**Note** The <EntitlementProfile> indicates the type of entitlement profile a Subscriber is associated with. This should correspond to the one defined in the |DEF|EPROFILE| section. If no Entitlement profile is associated with the subscriber, this field appears as “~”.<br><br>`\|SUB\|-1\|-1\|-1\|STBSub7\|~\|~\|~\|STBSub7L\|~\|~\|~\|~\|FeatureGroup_3\|~\|0\|1\|HCS Basic\|1\|HCUC_BasicMessaging\|1\|`<br><br>The above example shows the multiple licenses. Here, multiple licenses are HCS Basic and another is unity connection license that is HCUC_BasicMessaging. |

| Format | Example |
|---|---|
| **Note** All fields are *required* in this row.<br>**Note** The values for the following fields: **customer_id**, **site_id** and **sub_id** have been replaced with "-1" during data translation or correction, since its original value accuracy is no longer guaranteed. The usage of the <ID> fields in the service inventory section of the report is deprecated. | |

# Subscriber Footer Row

| Format | Example |
|---|---|
| \|SUBEND\| | `\|SUBEND\|` |

**Note** This row is *required* if a |SUB| data row exists.

# Eprofile Definition Row

| Format | Example |
|---|---|
| \|DEV\|<profilename>\|<profileID>\|<customerID>\|<customerprofile>\|<deviceIDs>\|<devicegroup>\| <numberofdevices>\|<numberofdevicesingroup>\| | `\|DEF\|EPROFILE\|p1\|~\|cust02\|cust02EntProfile\|51\|53\|1\|46\|p1devicegroup02\|10\|10\|` |

# Ecatalog Definition Row

| Format | Example |
|---|---|
| \|DEV\|<profilename>\|<profileID>\|<customerID>\|<customerprofile>\|<deviceIDs>\|<devicegroup>\|<numberofdevices>\|<numberofdevicesingroup>\| | `\|DEF\|ECATALOG\|p1\|~\|cust01\|51\|53\|1\|46\|p1devicefroup01\|10\|10\|` |

# Devicegroup Definition Row

| Format | Example |
|---|---|
| \|DEV\|<groupname>\|<devicegroup>\| <numberofdevices>\| | `\|DEF\|DGROUP\|p1devicegroup02\|25\|` |

# Device Data Row

This format defines how a single device is represented in the report. The device is registered and assigned to the subscriber when represented within a **|SUB|/|SUBEND|** pair. The device is registered to and functional at a site but is not assigned to a user when a device is placed outside a **|SUB|/|SUBEND|** pair in the report. Device examples include conference room phones, lobby phones, or Cisco Extension Mobility-enabled "empty" devices.

In these scenarios, the **|DEV|** row exists immediately following the **|SITE|** row and before **|SUB|** rows for that site. Device Data Rows cannot exist anywhere else in the report. Cisco Extension Mobility profiles are reported in the same way as traditional devices.

| Format | Examples |
|---|---|
| \|DEV\|<customerID>\| <siteID>\|<subID>\|<deviceName>\| <deviceMAC>\| <phoneOrExtMobility>\| <deviceTypeID> or <device Type>\|<lineCount>\| <HCS License Type>\| | `\|DEV\|-1\|-1\|-1\|SEP0445687B8AAF\|0445687B8AAF\|\|0\|3\|1\|~\|`<br>In the example above, the **<deviceMAC>** field follows the preceding MAC Address format definition. The **<deviceTypeID>** field references the device type as defined in the Device Definition Row. The device type is "3" in this example. It shows a device assigned to a subscriber with an ID "9865." The **<phoneOrExtMobility>** parameter is set to 0 to indicate that it is a physical phone.<br>`\|DEV\|-1\|-1\|~\|SEP1143ADFE23FF\|1143ADFE23FF\|0\|3\|1\| HCS Standard\|`<br>The example above shows a similar device, but in this case, the device is registered to a site/location but not assigned to an individual subscriber. The tilde (~) shows that there is no **<subID>** associated with this device. The **<phoneOrExtMobility>** parameter is set to 0 to indicate that it is a physical phone.<br>`\|DEV\|-1\|-1\|-1\|jsmith\|~\|1\|3\|1\|~\|`<br>The example above shows an Extension Mobility profile assigned with profile name "jsmith," **<deviceTypeID>** = "3", and no **<deviceMAC**> field. The **<phoneOrExtMobility>** parameter is set to 1 to indicate that it is a Cisco Extension Mobility profile.<br>`\|DEV\|-1\|-1\|-1\|sep098765432108\|098765432108\|0\|8\|0\|HCS Foundation\|`<br>The example above shows how a typical \|DEV\| data row appears in the 10.6.1 report format. This format provides the HCS License Type to report the type of HCS license activated by the device. For devices owned or controlled by subscribers, the value appears as "~". |

| Format | Examples |
|---|---|
| **Note** | • The **<phoneOrExtMobility>** field indicates whether it is a physical device (value of 0) or an Extension Mobility profile (value of 1).<br>• The **<lineCount>** field gives the number of lines, specifically Internal TNs, assigned to the device. External TNs are mapped to individual internal lines. The number of Line Data Rows that follows MUST match this **<lineCount>** value.<br>• If a single device is being shared by more than one user or device, you can list that device in more than one subscriber record. If a single device is shared or assigned to more than one user, the TOTAL device count is not affected in the Report Statistical section.<br>• All fields are *required* in this row. The following fields cannot be empty:<br>◦ **<deviceName>** (if an EM Profile)<br>◦ **<deviceMAC>** (if a physical device or soft client). |

**Note** All fields are *required* on this row. The following fields may not be empty: **<device Name>** (if an EM Profile) -or- **<deviceMAC>** (if a physical device or soft client).

**Note** The values for the following fields:**<customer_id>** , **<site_id>**, and **<subscriber_ID>** are replaced with "-1" because their original value accuracy is not guaranteed.

# Device Line Data Row

This format definition describes how device lines are represented in the report. This format definition depends on the previous definitions of Telephone Number (Internal TN) and Telephone Number (External TN), on page 126.

| Format | Examples |
|---|---|
| \|LINE\|<internalTN>\|<br><contactCenterAgentLineService>\|<br><externalTNe164[1]>\|…\|<externalTNe164[N]>\| | `\|LINE\|4761000\|0\|`<br>The example above describes a single internal TN only.<br>`\|LINE\|4761001\|1\|+19194761001\|`<br>The example above describes a single internal TN with a mapped external TN (E.164 compliant) and the extension enabled as a contact center agent line.<br>`\|LINE\|4761001\|0\|+19194761001\|+19194761002\|`<br>The example above describes two external TNs associated with a single line. |

| Format | Examples |
|---|---|
| The <**contactCenterAgentLineService**> field in all the examples above is a Boolean field indicating whether this particular device LINE is activated for contact center agent usage. Availability of contact center features is described by the appropriate feature in the subscriber's assigned feature group. The <**contactCenterAgentLineService**> field indicates actual activation of the feature, rather than simply indicating availability of this feature.<br>**Note** • If a single line is being shared by more than one user or device, the line number can be listed in more than one device record.<br>• All fields are *required* in this row. The following fields cannot be empty: **<internalTN>**, **<contactCenterAgentLineService>**. | |

# SI Report Footer

| Format | Example |
|---|---|
| \|SIEND\| | `\|SIEND\|` |

**Note** This row is *required*.

# MACD Report Header

| Format | Example |
|---|---|
| \|MACDSTART\| | `\|MACDSTART\|` |

**Note** This row is *required*.

# MACD Row Format

This format definition describes the general layout of all MACD rows in the report. Certain fields described are required of each MACD row, regardless of type, while individual differences are highlighted in the definition for each type later.

| Format | Examples |
|---|---|
| \|MACD\|<macdEffectiveDT>\|<br><macdCategory>\|<macdCode…<br><additional fields>…\| | `\|MACD\|20110811983040511GMT\|FGROUP\|A\|...\|`<br>`\|MACD\|20110811983040511GMT\|RESELL\|A\|...\|`<br>`\|MACD\|20110811983040511GMT\|CUST\|A\|...\|`<br>`\|MACD\|20110811983040511GMT\|SUB\|A\|...\|`<br>`\|MACD\|20110811983040511GMT\|SITE\|A\|...\|`<br>`\|MACD\|20110811983040511GMT\|DEV\|A\|...\|`<br>`\|MACD\|20110811983040511GMT\|LINE\|A\|...\|` |

- The fields are *required* for ALL MACD rows, regardless of type.
- In the format and examples, the **<macdCategory>** field always matches the row type name of the corresponding type to the change.
- The **<macdEffectiveDT>** field represents the effective date/time of the MACD event. The format of this element should follow the Date/Time Element, on page 127 format.

# MACD Code Element (General)

This format definition describes how MACD Code elements are represented in all MACD rows. No separate definition row is required in the file to describe the MACD Code elements.

The following list describes the characters used to construct the format:

- **M** = Moved
- **A** = Entity is Added
- **D** = Entity is Deleted
- **C** = Entity is Changed
- **N** = No Change / Active

| Format | Examples |
|---|---|
| \|<macdCode>\| | `\|M\|\|A\|`<br>`\|D\|`<br>`\|C\|` |
| This field applies to all row types that have corresponding MACD rows, except devices. Devices have additional states for registration and assignment that require a separate representation. See MACD Code Element (Devices Only), on page 145. | |

# MACD Code Element (Devices Only)

This format definition describes how MACD Code elements are represented in all MACD rows for devices. No separate definition row is required in the file to describe the MACD Code Elements for devices.

The following list describes the characters used to construct the format:

- **A** = Device is Registered
- **D** = Device is Unregistered
- **S** = Device is Associated to a user/Cisco Extension Mobility profile is added to a user
- **U** = Device is Disassociated from a user/Cisco Extension Mobility profile is removed from a user
- **C** = Device is Modified/Cisco Extension Mobility profile is Modified

| Format | Examples |
|---|---|
| \|<macdCode>\| | `\|A\|\|D\|`<br>`\|S\|`<br>`\|U\|`<br>`\|C\|` |

# MACD Data Row (Feature Group)

This format definition describes how the function “add, change, or delete” a feature group can appear in the MACD section of the SI report.

| Format | Examples |
|---|---|
| \|MACD\|<br><macdEffectiveDT>\|<br>FGROUP\|<macdCode>\|<br><customerName>\|<br><featureGroupName>\|<br><feature[1]ID>\|<feature[2]ID>\|<br>…\|<feature[N]ID>\| | `\|MACD\|20110423163455GMT\|FGROUP\|A\|CompanyXYZ\|Advanced Feature Group\|10\|11\|19\|33\|99\|`<br>In the example above, a feature group is added to the system, assigned to customer “CompanyXYZ” and contains features 10, 11, 19, 33, and 99 (mapped to the **\|FEATURES\|** definition row previously).<br>`\|MACD\|20110423163455GMT\|FGROUP\|C\|CompanyXYZ\|Advanced Feature Group\|10\|11\|19\|99\|`<br>In the example above, the same feature group is modified, and feature 33 is removed.<br>`\|MACD\|20110423163455GMT\|FGROUP\|D\|CompanyXYZ\|Advanced Feature Group\|10\|11\|19\|99\|`<br>In the example above, the entire feature group is deleted. In the next day’s report, this feature group would no longer exist unless it was re-added. |

# MACD Data Row (Provider)

There is no “Provider” MACD information supported or needed in this version of the report format.

# MACD Data Row (Reseller)

This format definition describes how reseller MACD information is presented within the SI report file.

| Format | Examples |
|---|---|
| \|MACD\|<macdEffectiveDT>\| RESELL\|<macdCode>\| <resellerName>\| | `\|MACD\|20110423163455GMT\|RESELL\|A\|ResellerXYZ\|`<br>In the example above, a reseller named “ResellerXYZ” is added to the Domain Manager on April 23, 2011 at 04:34:55 PM GMT.<br>`\|MACD\|20110423163455GMT\|RESELL\|D\|ResellerXYZ\|`<br>The example above shows that the reseller is deleted from the Cisco Unified Communications Domain Manager.<br>`\|MACD\|20110423163455GMT\|RESELL\|C\|ResellerXYZ\|`<br>The example above shows a change to the reseller in the example. |
| **Note** | • Reseller metadata changes are supported on Cisco Unified Communications Domain Manager and result in the generation of a MACD row; however, Cisco Unified Communications Domain Manager does not currently support indicating the nature of such changes in the MACD row. This may be updated in future releases with more detail.<br>• Only the new state of the entity is reported in the MACD row. |

# MACD Data Row (Customer)

This format definition describes how customer MACD information is presented within the SI report file.

| Format | Examples |
|---|---|
| \|MACD\| <macdEffectiveDT>\|CUST\| <macdCode>\| <customerName>\| <resellerName>\| <externalCustomerID>\| | `\|MACD\|20110423163455GMT\|CUST\|A\|CompanyXYZ\|ResellerXYZ\|~\|`<br>In the example above, “CompanyXYZ” is added on April 23, 2011 at 4:34:55 PM GMT to the Cisco Unified Communications Domain Manager.<br>`\|MACD\|20110423163455GMT\|CUST\|D\|CompanyXYZ\|ResellerXYZ\|~\|`<br>The example above describes deleting the customer.<br>`\|MACD\|20110423163455GMT\|CUST\|C\|CompanyXYZ\|ResellerXYZ\|34587573\|`<br>The above example describes the change of the customer where the **<externalCustomerID>** field was updated. |
| **Note** | • The only changes that are currently supported are changes to the **<externalCustomerID>** field. Other customer metadata changes are supported on Cisco Unified Communications Domain Manager and result in generation of a MACD row; however, Cisco Unified Communications Domain Manager does not support indicating the nature of such changes in the MACD row.<br>• Only the new state of the entity is reported in the MACD row. |

# MACD Data Row (Division)

No “Division” MACD information is supported or needed in this version of the report format.

# MACD Data Row (Site)

This format definition describes how site MACD information is presented within the SI report file.

| Format | Examples |
|---|---|
| \|MACD\| <macdEffectiveDT>\|SITE\| <macdCode>\| <customerName>\| <siteName>\|<externalSiteID>\| | `\|MACD\|20110423163455GMT\|SITE\|A\|CompanyXYZ\|New York\|~\|`<br>In the example above, a site with the name “New York” is added on April 23, 2011 at 4:34:55 PM GMT to the Domain Manager.<br>`\|MACD\|20110423163455GMT\|SITE\|D\|CompanyXYZ\|New York\|~\|`<br>In the example above, a site was deleted from customer “CompanyXYZ”.<br>`\|MACD\|20110423163455GMT\|SITE\|C\|CompanyXYZ\|New York\|74536577456\|`<br>In the example above, the **<externalSiteID>** field was updated. |

| Format | Examples |
|---|---|
| **Note** | • The only changes that are currently supported and meaningful are changes to the **<externalSiteID>** field. Other site metadata changes are supported on Cisco Unified Communications Domain Manager and result in the generation of a MACD row; however, Cisco Unified Communications Domain Manager does not support indicating the nature of such changes in the MACD row.<br>• Only the new state of the entity is reported in the MACD row. |

[1]

# MACD Data Row (Subscriber)

This format definition describes how subscriber MACD information is presented within the SI report file.

1

| Format | Examples |
|---|---|
| |MACD|<macdEffectiveDT>|SUB|<br><macdCode>|<customerName>|<br><siteName>|<subUsername>|<br><subEmail>|<subNameFirst>|<br><subNameMiddle>|<subNameLast>|<br><subTitle>|<subDepartment>|<br><subDepartmentCode>|<br><subContactTelephone>|<br><featureGroupName>| | `\|MACD\|20110423163455GMT\|SUB\|A\|CompanyXYZ\|NewYork\|jsmith\|jsmith@xyz.com\|John\|Thomas\|Smith\|Manager\|Finance\|99\|+19198548001\|Basic Features\|`<br><br>In the example above, subscriber John Smith is added on April 23, 2011 at 4:34:55 PM GMT to the customer “CompanyXYZ” at site “New York”. John Smith’s full details are provided on the MACD line to show all the data that was added.<br><br>`\|MACD\|20110423163455GMT\|SUB\|D\|CompanyXYZ\|NewYork\|jsmith\|jsmith@xyz.com\|John\|Thomas\|Smith\|Manager\|Finance\|99\|+19198548001\|Basic Features\|`<br><br>The example above shows the deletion of user John Smith.<br><br>`\|MACD\|20110423163455GMT\|SUB\|C\|CompanyXYZ\|NewYork\|jsmith\|jsmith@xyz.com\|John\|Thomas\|Smith\|Manager\|Finance\|99\|~\|Basic Features\|`<br><br>Various types of changes are possible where a subscriber is concerned. The first type is metadata changes including modifications to email, name (first, middle, last), title, department, and department code. The second type of change are modifications to, additions, or deletions of the **<subContactTelephone>** and **<featureGroupID>** fields. A deletion of the external TN from the user, therefore, appears as a MACD change type.<br><br>`\|MACD\|20110423163455GMT\|SUB\|C\|CompanyXYZ\|NewYork\|jsmith\|jsmith@xyz.com\|John\|Thomas\|Smith\|Manager\|Finance\|99\|+19198548001\|~\|`<br><br>Adding or removing a user to or from a feature group also appears as a MACD change type. The example above shows the removal of user John Smith from the feature group.<br><br>`110423163455GMT\|SUB\|A\|CompanyXYZ\|NewYork\|jsmith\|jsmith@xyz.com\|John\|Thomas\|Smith\|Manager\|Finance\|99\|+19198548001\|Basic Features\|`<br><br>The example above shows the addition of user John Smith back into the feature group. |

Only the new state of the entity is reported in the MACD row. Entitlement/SNR enabled/EM enabled/Licensing delta are not reported in MACD section.

# MACD Data Row (Device Line and Service)

This format definition describes how device and line MACD information is presented within the SI report file. Reporting MACD data for devices includes registration, assignment, and change operations for devices listed as part of sites and subscribers only. It also includes the addition, deletion, and modification of lines for those devices. In almost all cases, the device and line MACD rows are presented together. In some cases, the line MACD rows can be omitted. Line MACD rows can never be presented in standalone fashion. Service Inventory and MACD data for devices listed in Provider, Reseller, and Division, Customer, and Site inventories are not reported. Only data for registered devices under Site and Subscriber entities are reported.

| Format |
| --- |
| \|MACD\|<macdEffectiveDT>\|DEV\|<macdCode>\|<customerName>\|<siteName>\|<subUsername>\| |
| <deviceName>\|<deviceMAC>\|<phoneOrExtMobility>\|<deviceTypeID>\|<lineCount>\| |
| \|MACD\|<macdEffectiveDT>\|LINE\|<macdCode>\|<internalTN>\|<contactCenterAgentLineService>\|… |
| \|MACD\|<macdEffectiveDT>\|LINE\|<macdCode>\|<internalTN>\|<contactCenterAgentLineService>\| |

The following are examples of different scenarios for the MACD Data Row:



## A device with two internal TNs is registered to a site.

### Example 13-26

```
|MACD|20110423171235GMT|DEV|A|CompanyXYZ|NewYork|~|SEP0445687B8A11|0445687B8A11|0|3|2|
| MACD|20110423171235GMT|LINE|A|4761000|0|
| MACD|20110423171235GMT|LINE|A|4761001|0|
```

## Assignment of the device to a subscriber described in A device with two internal TNs is registered to a site.

| Example |
|---|
| **Example 13-27**<br>`\|MACD\|20110423171235GMT\|DEV\|S\|CompanyXYZ\|NewYork\|~\|SEP0445687B8A11\|0445687B8A11\|0\|3\|0\|` |
| **Note** Line information is omitted in this scenario if it has not changed. |

## Unassignment of device from a subscriber described in A device with two internal TNs is registered to a site.

| Example |
|---|
| **Example 13-27**<br>`\|MACD\|20110423171235GMT\|DEV\|U\|CompanyXYZ\|NewYork\|jsmith\|SEP0445687B8A11\|0445687B8A11\|0\|3\|~\|` |
| **Note** Line information is omitted in this scenario if it has not changed. |

## A device with two lines is unregistered from a site.

| Example |
|---|
| **Example 13-29**<br>`\|MACD\|20110423171235GMT\|DEV\|D\|333\|1\|~\|SEP0445687B8A11\|0445687B8A11\|0\|3\|~\|` |
| **Note** Line information is omitted in this scenario. |

## A device with two lines is registered and assigned to a subscriber.

```
|MACD|20110423171235GMT|DEV|S|CompanyXYZ|NewYork|jsmith|
SEP0445687B8A11|0445687B8A11|0|3|~|
|MACD|20110423171235GMT|DEV|A|CompanyXYZ|NewYork|~|SEP0445687B8A11|0445687B8A11|0|3|2|
|MACD|20110423171235GMT|LINE|A|4761000|0|
|MACD|20110423171235GMT|LINE|A|4761001|0|
```

## A device with two lines is unassigned and unregistered from a subscriber.

```
|MACD|20110423171235GMT|DEV|D|CompanyXYZ|NewYork|~|SEP0445687B8A11|0445687B8A11|0|3|~|
|MACD|20110423171235GMT|DEV|U|CompanyXYZ|NewYork|jsmith|
SEP0445687B8A11|0445687B8A11|0|3|~|
```

**Note** Line information may be omitted in this scenario.

## A device with two lines has a setting modified on either the device itself, one of its lines, or both of its lines. Modification does not affect the service inventory record but a MACD row appears.

**Example 13-32**

```
|MACD|20110423171235GMT|DEV|C|CompanyA|NewYork|jsmith|
SEP0445687B8A11|0445687B8A11|0|3|2|
| MACD|20110423171235GMT|LINE|C|4761000|0|
| MACD|20110423171235GMT|LINE|C|4761001|0|
```

## A device with two lines. Contact Center service is enabled on line 1 but is already enabled on the second line.

**Example 13-33**

```
|MACD|20110423171235GMT|DEV|C|CustomerXYZ|NewYork|jsmith|
SEP0445687B8A11|0445687B8A11|0|3|2|
|MACD|20110423171235GMT|LINE|C|4761000|1|
|MACD|20110423171235GMT|LINE|C|4761001|1|
```

**Note** In this example, the second line already has Contact Center service enabled. However, due to the nature of reporting MACD operations, the new state of the entire device (and lines) is reported, which, in this example, now includes Contact Center service on both lines for the device.

## A device with two lines. Contact Center service is enabled on line 2.

**Example 13-34**

```
|MACD|20110423171235GMT|DEV|C|CustomerXYZ|NewYork|jsmith|
SEP0445687B8A11|0445687B8A11|0|3|2|
|MACD|20110423171235GMT|LINE|C|4761000|0|
|MACD|20110423171235GMT|LINE|C|4761001|1|
```

## A device with two lines. Contact Center service is disabled on line 1 and enabled on line 2.

**Example 13-35**

```
|MACD|20110423171235GMT|DEV|C|CustomerXYZ|NewYork|jsmith|
SEP0445687B8A11|0445687B8A11|0|3|2|
| MACD|20110423171235GMT|LINE|C|4761000|0|
| MACD|20110423171235GMT|LINE|C|4761001|1|
```

**Note** A device with two lines. Contact Center service is enabled on line 1 but is already enabled on the second line., on page 152 and A device with two lines. Contact Center service is enabled on line 2., on page 152 represent different scenarios resulting in the generation of identical MACD rows for this device. In both cases, the new state of the device (and lines) is reported, regardless of the operation leading to that state.

## A device with 0 lines is registered and assigned to a subscriber.

| Example |
|---|
| **Example 13-36**<br>`\|MACD\|20110423171235GMT\|DEV\|S\|CustomerXYZ\|NewYork\|jsmith\|`<br>`SEP0445687B8A11\|0445687B8A11\|0\|3\|~\|`<br>`\|MACD\|20110423171235GMT\|DEV\|A\|CustomerXYZ\|NewYork\|~\|`<br>`SEP0445687B8A11\|0445687B8A11\|0\|3\|~\|` |
| **Note** Line information is omitted in this scenario because it does not exist. |

## A device with two lines is modified. A third line is added.

**Example 13-37**

```
|MACD|20110423171235GMT|DEV|C|CompanyXYZ|NewYork|jsmith|
SEPMyNewPhoneName|0445687B8A11|0|3|1|
|MACD|20110423171235GMT|LINE|A|4761002|0|
```

## A device with three lines is modified. The second line is deleted.

**Example 13-38**

```
|MACD|20110423171235GMT|DEV|C|CompanyXYZ|NewYork|jsmith|
SEPMyNewPhoneName|0445687B8A11|0|3|1|
|MACD|20110423171235GMT|LINE|D|4761001|0|
```

**Note**

- The examples describe several scenarios that may occur in the registration and assignment of devices to both sites and subscribers. If a device is registered with lines, the line MACD row is reported with the device MACD row. If a device is already registered and later assigned, the line MACD rows are not reported because those have not changed.
- The only supported change to a device for Service Inventory purposes is the modification of the **<lineCount>** field. Modifications to the **<lineCount>** field, however, are the result of additions or deletions of lines, and those corresponding line MACD rows must immediately follow this device MACD row.
- Modify various device and line settings on the CUCDM application for a device that does not affect the billing record. Such changes, however, still result in the generation of a MACD row for the device (with optional line MACD rows). You cannot capture the nature of the change and indicate whether the MACD row in question has or has not affected the billing record. Similar to MACD rows for other entities, the Device (and Line) MACD rows simply report the state of the device (and lines) following the change operation in question.
- To modify user assignment of a device, the device must be unassociated with a user, then associated with another user.
- You can also modify the site assignment. If the device is associated with a user it must be unassociated with that user. Then it must be unregistered from the site, then reregistered under another site.
- If multiple devices are added, changed, or deleted at the same time, these are reported on a separate MACD row.
- Soft client and mobile device MACDs are reported the same way as traditional devices.
- Device MACD rows use the **<lineCount>** field to identify the number of **|LINE|** MACD records that immediately follow the **|DEV|** MACD record in the report. This number is *not* the total count of lines that are assigned to the device at the time of the MACD operation. Be aware of this notation when you use parsing applications. For device changes that result in zero line changes, the <**lineCount**> field is a tilde (~).
- Licensing (Licensing Type) is not included as part of a MACD report.

# MACD Report Footer

| Format | Examples |
|---|---|
| \|MACDEND\| | `\|MACDEND\|` |
| **Note** This row is *required*. | |

# Report Statistical Header

| Format | Examples |
|---|---|
| \|STATSTART\| | `\|STATSTART\|` |
| **Note** This row is *required*. | |

# Report Statistical Row

| Format | Examples |
|---|---|
| \|STAT\|<fieldName>\|<fieldValue>\|<fieldUnits>\| | `\|STAT\|providerCount\|1\|~\|`<br>`\|STAT\|resellerCount\|1\|~\|`<br>`\|STAT\|customerCount\|3\|~\|`<br>`\|STAT\|siteCount\|6\|~\|`<br>`\|STAT\|subscriberCount\|12\|~\|`<br>`\|STAT\|devRegAssigned\|20\|~\|`<br>`\|STAT\|devRegUnassigned\|20\|~\|`<br>`\|STAT\|macdCount\|126\|~\|`<br>`\|STAT\|siRequestDT\|06013011030000GMT\|~\|`<br>`\|STAT\|siStartDT\|06013011030800GMT\|~\|`<br>`\|STAT\|siEndDT\|06013011032314GMT\|~\|` |
| **Note** Each Domain Manager must properly write out the preceding time stamps because of how the SI files are received from the Domain Manager servers. This information is used for performance tracking and debugging information. The preceding column <**fieldUnits**> is currently unused and left empty. | |

The following lists the meaning of each requested statistic:

| Field Name | Description |
|---|---|
| **providerCount** | The total number of unique providers (and thus, \|**PROV**\| rows) listed in the report. |
| **resellerCount** | The total number of unique resellers (and thus, \|**RESELL**\| rows) listed in the report. |
| **customerCount** | The total number of unique customers (and thus, \|**CUST**\| rows) listed in the report. |
| **siteCount** | The total number of unique sites (and thus, \|**SITE**\| rows) listed in the report. |
| **subscriberCount** | The total number of unique subscribers (and thus, \|**SUB**\| rows) listed in the report. |

| Field Name | Description |
|---|---|
| **devRegAssigned** | The total number of unique devices that are both registered and assigned to a subscriber listed in the report. If devices are shared, this count does not accurately reflect the number of **\|DEV\|** rows present in the report. Uniqueness is required. |
| **devRegUnassigned** | The total number of unique devices that are registered but not assigned to a subscriber, listed in the report. This is the count of devices that are assigned to sites, such as conference room phones, lobby phones, and "empty" Cisco Extension Mobility phones. If devices are shared, this count does not accurately reflect the number of **\|DEV\|** rows that are present. Uniqueness is required. |
| **macdCount** | The total number of MACD rows reported in the MACD section of the file. |

The following lists the meaning of each requested Date/Time (DT) field:

| Field Name | Description |
|---|---|
| **siRequestDT** | The time when the SI request is received or activated by the Domain Manager. |
| **siStartDT** | The time when the Domain Manager begins the SI process (after delays, for example). |
| **siEndDT** | The time when the Domain Manager ends the SI process. This field should not include any file transfer times or the like. |

## Report Statistical Footer

| Format | Examples |
|---|---|
| \|STATEND\| | `\|STATEND\|` |
| **Note** This row is *required*. | |

# Summary

## License Summary

The Summary Licensing Sections are added with the following licenses in the Service Inventory Report.

- **PLM License:** It contains the information about PLM server details, cluster applications which are assigned to the PLM host, license usages such as License type, Installed licenses, Required licenses, Status of the licenses from the specific clusters.
- **Customer License:** It contains the information about PLM server details with hierarchy of customer level, including the cluster applications which are assigned to the customers with IP Address of the cluster, Licenses type and Number of licenses used by the customer from the cluster Apps.
- **Site License:** It contains the information about Site level licensing which includes the information of Lobby Device licenses, Subscriber licenses and license usages such as License type and License count with each hierarchy of sites.

**Note** The PLM customer summary section shows only those customers who are available in the service inventory report.

# Report Summary Header

| Format | Example |
|---|---|
| \|INFOSTART\| | `\|INFOSTART\|` |

**Note** This row is *required*.

# Licence Summary Header

| Format | Example |
|---|---|
| \|LICENSESUMMARYSTART\| | `\|LICENSESUMMARYSTART\|` |

**Note** This row is *required*.

# Report Summary Row

This format definition describes how summary information is presented in the output files. An example of each data element is described.

| Format | Examples |
|---|---|
| \|INFO\|<fieldName>\| <fieldValue>\| | Cisco Unified Communications Domain Manager 8.1(x) format:<br>`\|INFO\|formatVersion\|9.0.1.1\|`<br>`\|INFO\|filename\|20110528032329GMT+12345+CUCDM+1+1.si\|`<br>`\|INFO\|dmVerPlatform\|4.1.6+0.4.47\|`<br>`\|INFO\|dmVerSoftware\|7.3.0+er15\|`<br>`\|INFO\|dmHostname\|nelco-cucdm4\|`<br>`\|INFO\|dmDomain\|cisco.com\|`<br>`\|INFO\|dmIP\|172.18.200.200\|`<br>`\|INFO\|reportStartDT\|06012011000000GMT\|`<br>`\|INFO\|reportEndDT\|06012011235959GMT\|`<br>Cisco Unified Communications Domain Manager 10.6(1) format:<br>`\|INFO\|formatVersion\|10.6.1\|`<br>`\|INFO\|filename\|20141126132645GMT+1+CUCDM2+1+1.si\|`<br>`\|INFO\|dmVerPlatform\|1.2.0-1415027768\|`<br>`\|INFO\|dmVerSoftware\|1.2.0+65\|`<br>`\|INFO\|dmHostname\|10.106.215.12\|`<br>`\|INFO\|dmDomain\|~\|`<br>`\|INFO\|dmIP\|10.106.215.12\|`<br>`\|INFO\|reportStartDT\|20141126132645GMT\|`<br>`\|INFO\|reportEndDT\|20141126132645GMT` |
| [2]<br>**Note** • The "reportStartDT" and "reportEndDT" fields are used to describe the reporting period covered by a report. These values do not indicate the time when the report is generated, nor the amount of time taken to generate the report.<br>• These rows are *required*. All fields are *required* in all rows. | |

[2] These fields can appear in any order, except the "formatVersion" row, which must be the first row and the "filename" row , which must be the second row in the Report Summary section.

# Licence Summary Footer

| Format | Example |
|---|---|
| \|LICENSESUMMARYEND\| | `\|LICENSESUMMARYEND\|` |

**Note** This row is *required*.

## Report Summary Footer

| Format | Example |
|---|---|
| \|INFOEND\| | `\|INFOEND\|` |

**Note** This row is *required*.

# Create Microsoft Excel-Based Service Inventory Report

**Procedure**

**Step 1** Generate a Microsoft Excel-Based Service Inventory Report by selecting the **Generate XLS report** checkbox.

**Step 2** Download the generated report.

**Step 3** To perform an audit of the Entitlement violations, perform the following:

a) Open the MetaData tab in the report.

b) Click **Audit**.

A popup box appears when the audit is complete. The Audit tab is added as the last sheet of the Microsoft Excel-Based Service Inventory Report. If the Audit sheet is blank, there are no entitlement violations.

# Microsoft Excel-based Service Inventory Report

Service Inventory information can also be provided in a Microsoft Excel-based report. It is a additional provision to a text based SI report. User has a choice to select for Microsoft Excel-based report format. The Excel-based report contains the following information:

**Note** Fields are left blank if they do not apply to the specific Cisco Unified Communications Domain Manager used to generate the report.

*Table 53: Microsoft Excel-Based Service Inventory Report Format*

| Tab | Description | Correlation to regular SI Report |
|---|---|---|
| MetaData | Provides general information such as:<br>• Format Version such as 10.6.1<br>• Filename; for example, 20150406093636GMT+1+CUCDM2+1+1.si<br>20150406093636GMT+1+CUCDM2+1+1.xlsx<br>• Domain Manager Platform Version<br>• Domain Manager Software<br>• Domain Manager domain<br>• Domain Manager IP Address<br>• Report Start Time Stamp<br>• Report End Time Stamp<br>• Country ID<br>• Country Name<br>• Country Code. The ISO country code abbreviation in either 2-character or 3-character format. See http://www.nationsonline.org/oneworld/country_code_list.htm.<br><br>Click **Audit** on this tab to perform an audit for Entitlement violations. Audit results appear in an Audit tab. | Information between \|INFOSTART\| and \|INFOEND\| |
| Features | A list of all possible features that are currently on the domain manager and their feature numbers. The feature numbers are generated at runtime, and are merely integers used for cross-referencing in the current file. There is no guarantee that feature IDs are consistent between files. | \|DEF\|FEATURES\| |
| FeatureGroups | A list of feature IDs by Feature Group Name and Customer Name. Features listed in the feature group are “assigned” and available to those subscribers who were placed in this group. A subscriber does not necessarily use these features. | \|DEF\|FGROUP\| |
| DeviceDefs | A list of devices configured for each customer. Each row includes the Customer Name, as well as the Device ID, Make, and Model. The Device ID is a value provided by the Cisco Unified Communications Domain Manager server that stores the device make and model information. | \|DEF\|DEV\| |
| DeviceGroup | A list of the configured device groups, each on a separate row. Includes the Device Group Name, ID, Make, and Model. The Device ID is a value provided by the Cisco Unified Communications Domain Manager server that stores the device make and model information. | \|DEF\|DGROUP\| |

| Tab | Description | Correlation to regular SI Report |
|---|---|---|
| EntitlementFeatureGroup | Provides a row for each Entitlement Feature Group, with a list of the feature IDs that are available to the Entitlement Group. Features listed in this tab are “assigned” and available to those subscribers who were placed in this group. A subscriber does not necessarily use these features. | \|DEF\|EFGROUP\| |
| EntitlementCatalog | A list of Entitlement Feature Groups by Provider, Reseller, and Customer. Includes the maximum number of allowable devices for each Entitlement Feature Group. | \|DEF\|ECATALOG\| |
| EntitlementProfile | A list of Entitlement Profiles by Provider, Reseller, Customer, and Entitlement Catalog. Includes the maximum number of allowable devices for each Entitlement Feature Group. The maximum number of devices are limitations for an individual user, not for all users in the system. | \|DEF\|EPROFILE\| |
| Providers | A list of Providers by name | \|PROV\| to \|PEND\| |
| Resellers | A list of Resellers by name, for each Provider | \|RESELL\| to \|REND\| |
| Customers | A list of Customers by Reseller and Provider. Customer information includes Name, External Customer ID, Address, City, State, Country, and Postal Code. | \|CUST\| to \|CEND\| |
| Sites | A list of Sites by Customer. Site information includes Name, External Site ID, Address, City, State, Country, Postal Code, and Time Zone. | \|SITE\| to \|SEND\| |

| Tab | Description | Correlation to regular SI Report |
|---|---|---|
| Subscribers | A list of Subscribers by Name. Includes the following information about the subscriber (if available):<br>• Customer the subscriber belongs to<br>• Site the subscriber belongs to<br>• Email address<br>• First Name<br>• Middle Name<br>• Last Name<br>• Title<br>• Department<br>• Department Code<br>• Primary Extension<br>• Feature Group the subscriber belongs to<br>• Entitlement Profile to which the subscriber is associated with. This corresponds with the profile on the Entitlement Profile tab.<br>• Extension Mobility (EM) License status (1 or 0, where 1 is Enabled)<br>• SNR License status (1 or 0, where 1 is Enabled)<br>• License Type shows the value, if a phone assigned to a subscriber and EM or SNR license is activated by the subscriber<br>• License Count<br>• VM License Type or Telepresence license type, if the VM license is activated by the subscriber<br>• VM License Count | \|SUB\| to \|SUBEND\| |

| Tab | Description | Correlation to regular SI Report |
|---|---|---|
| Devices | A list of devices, including the following information about each device:<br>• Device MAC address<br>• Phone or Extension Mobility—Set to 0 if device is a physical phone, or set to 1 if device is a Cisco Extension Mobility profile<br>• Device Type ID—Device type defined in the DeviceDefs tab<br>• Line Count—The number of lines, specifically Internal TNs assigned to the device. External TNs are mapped to individual internal lines.<br>• Subscriber where device is registered. If the device is registered to a site or location, but is not assigned to an individual subscriber, a tilde (~) shows that there is no subscriber associated with this device.<br>• Site where device is registered<br>• Customer where device is registered<br>• License Type—The type of Cisco HCS license activated by the device. For devices owned or controlled by subscribers, the type appears as "~". | \|DEV\| |
| DeviceLines | A list of device lines, including the following information about each device line:<br>• Full Line Internal Number<br>• Contact Center Line Service—Indicates whether this particular device LINE is activated for contact center agent usage (0 is Not Activated, 1 is Activated). Availability of contact center features is described by the appropriate feature in the subscriber's assigned feature group. This field indicates actual activation of the feature, rather than simply indicating availability of the feature.<br>• Line E164 Number(s)<br>• Device<br>**Note** If a single line is being shared by more than one user or device, the line number can be listed in more than one device record. | \|LINE\| |
| MACD | Provides all MACD details | Information between \|MACDSTART\| and \|MACDEND\| |

| Tab | Description | Correlation to regular SI Report |
|---|---|---|
| PLMLicense | Provides PLM server details, as well as information about the cluster applications (for example, Cisco Emergency Responder (CER) or HCS Cisco Unity Connection (HCUC)) which are assigned to the PLM host. License Type, number of Installed licenses, number of Required and Available Licenses, and the Status of the licenses from the specific clusters is provided. | \|SUMMARY\|PLMINFO\| |
| CustomerLicense | Provides PLM server details for the Customer hierarchy node level, including the cluster applications which are assigned to the customers. IP Address of the cluster, License Type, and number of licenses used by the customer from the clusterApps is provided. | \|SUMMARY\|CUSTLICENSEINFO\| |
| SiteLicense | Provides details about site level licensing, including lobby device licenses, subscriber licenses, and license usage. The License Type is provided as well as a count of the number of licenses for each hierarchy of sites. | \|SUMMARY\|SITELICENSEINFO\| |
| Audit | When the **Audit** button is clicked on the MetaData tab, an audit for entitlement violations is completed. The system checks for mismatches between the following:<br>• Entitlement Feature Group and Subscriber Feature Group<br>• Device Group and Device List +count<br>A pop-up message indicates when the audit is finished, and the results are displayed in the Audit tab.<br>If there are no violations, the Audit tab is created, but it is left blank. | Not Applicable |

# Service Inventory Report Examples

The service inventory reports are located at the links provided below:

- ".si", ".ucsi", ".simacd" reports in text format: http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/hcs/10_6_1/HCMF_Product/Maintain_and_Operate_Guide/Examples/20150324124047GMT.zip
- Location report in Excel format: http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/hcs/10_6_1/HCMF_Product/Maintain_and_Operate_Guide/Examples/20150601161733GMT_Loc.csv
- .si report in Excel format: http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/hcs/10_6_1/HCMF_Product/Maintain_and_Operate_Guide/Examples/20150602213320GMT_1_CUCDM_1_1.xlsx

# MACD Format for UC Applications

As of 9.1(1), Service Inventory can generate reports directly from Cisco Unified Communications Manager and Cisco Unity Connection application servers for customers that are provisioned in Cisco Hosted

Collaboration Mediation-Fulfillment that do not have a Unified Communications Domain Manager configured. Most of the formats in the generated report are the same as the Unified Communications Domain Manager report results. However, a new MACD format report is also available specifically for a supported UC Application.

The following section shows the formats for the MACD Service Inventory Report for supported UC Applications.

**Note** The **<LOCATION>** field is configured differently for UC Applications. Make sure you have configured the **<LOCATION>** correctly in your Cisco Unified Communications Manager under **System** > **Location**. This field is required for Service Inventory to generate UC Application-based reports.

# UC Applications MACD Format

HCM-F provides a Service Inventory (SI) application that periodically queries Unified Communications Application Servers and reports their current operating state. This report provides information about modifications to Subscribers, Devices and Lines provisioned on the UC Applications Servers of the HCS system. This data is ultimately used by the service provider (SP) customer to generate or facilitate the correct generation of appropriate billing records for their end customers as part of their regular business processes.

This section outlines the layout and format of data points in the Cisco Service Inventory MACD output file. The MACD file is organized by Customer with some additional processing information included where necessary. The following sections give an overview of the format, a description of the file layout, a listing of the various row formats and data types contained in the output file, and finally, examples of Cisco Service Inventory MACD output file.

The Cisco SI Common MACD Format is designed to present all Subscriber MACD data in a human-readable format while keeping output file size to a minimum. The format is an ASCII-based file, with the ".simacd" file extension.

The output is arranged into the following sections:

Report Information

- Report Start Time
- Report Version

Customer Data

- UC Application Type
- Version
- Hostname/IP

- Subscriber MACD Data
- Subscriber Total Count
- UC Application, Subscriber, Device, Line, and Feature MACD data

Subscriber MACD data will be represented as a row indicating the new state of whatever entity is currently being added, changed, or deleted. Unlike a change notification, which would show a “before” and “after” state of the entity, the MACD representation only shows the “after” state.

# UC Applications File Layout

***Table 54: Report Format for the UC Applications MACD***

| Report Formats |
|---|
| |FILESTART| |
| |INFOSTART| |
| |<FORMAT-VERSION>|<REPORT_CREATION_TIME>| |
| |INFOEND| |
| |CUST| |
| |<CUSTOMER_NAME>|<APP1_TYPE>|<APP1_VERSION>|<APP_1HOSTNAME>|<APP2_TYPE>| |
| <APP2_VERSION>|<APP2_HOSTNAME> |
| |...| |
| <APP(N)_TYPE>|<APP(N)_VERSION>|<APP(N)_HOSTNAME>| |
| |MACDSTART| |
| |SUB-TOT|<COUNT>| |
| |SUB|<MACDCODE>|<CUCM_IP>|<CUC_IP>|<SUB_USERNAME>| |
| <SUB_UUID>|<SUB_FIRSTNAME>|<SUB_LASTNAME>|<SUB_EMAIL>| |
| <PRIMARY_TN>|<PRIMARY_EXTENSION>|<CUC_VM_EXTENSION>|<CUC_BILLING_ID>| |
| <VOICE_FEATURE>|<VM_FEATURE>| |
| <PRESENCE_FEATURE>|<CUEAC_FEATURE>|DEV|<DEVICE_NAME>|<DEVICE_TYPE>| |
| <DEVICE_MODEL>|<LOCATION> |
| |<EXT_MOBILITY>|LINE|<DIRECTORY_NUMBER>|<EXTERNAL_NUM_MASK>|LINE(N) |
| |…| |
| LINE_END(N)|DEV_END|DEV(N) |
| |…| |
| DEV_END(N)|SUB_END| |
| |MACDEND| |
| |CUSTEND| |
| |CUST(N)| |
| |CUSTEND(N)| |
| |FILEEND| |

# UC Applications Filename Specifications

The format of the Service Inventory MACD filename is critical to the proper operation of the SI applications. The following parameters apply to filenames in this format:

The filename follows this format:

```
<date><time><timezone> .<extension>
```

SI MACD File

```
20130111015000GMT.simacd
```

This MACD file naming convention is for a single file output that contains all Customers and their respective Subscriber MACD data.

# UC Application General Format Specification

Some additional general format specifications include the following:

- Data elements in the file will be stored in text, integer, and standard date/time formats where appropriate.
- The standard end-of-line character "\n," while typically not visible in common text-editing applications, will be used and is available for parsing programs to use for line tokenization.
- The data element delimiter will be the PIPE symbol "|". Each line will start and end with a PIPE symbol, with a PIPE symbol between each data point on the line as well.
- The PIPE symbol "|" is not a valid character within fields in the format.
- An empty (null) field will be represented by a TILDE symbol "~". Empty fields/columns will not be skipped.
- Report Data Collection Failures will be noted in the Customer Data Row. At a minimum the failed Customer Name will be appended with an asterisk "*" and if available the failed UC Application(s) will also will be appended with an asterisk "*". See the Customer Data Row Definition Section for example.

# Global Data Formats

This section outlines the data formats that are used throughout the row formats. Deviation from these global formats is not permitted in the scope of this SI Common Format definition.

## Date/Time Element

This format definition describes the way in which Date/Time elements are represented in information rows. All dates/times are represented in Greenwich Mean Time. All times are represented in 24-hour format. No separate definition row is required in the file to describe the date elements.

The following describes the characters that are used to construct the format:

- **yyyy** = Year
- **MM** = Month

- **dd** = Day
- **HH** = Hours
- **mm** = Minutes
- **ss** = Seconds
- **z** = Time Zone

| Format | Example |
|---|---|
| |<yyyyMMddHHmmssz>| | `\|20110423163455GMT\|` |

# UC Applications Row Format Specifications

This section outlines the various row formats used in the Cisco SI Common MACD Format. Each type specification provides a format definition and an example usage.

## File Header

File Header is the first line of each output file.

| Format | Example |
|---|---|
| |FSTART| | `\|FSTART\|` |

**Note** This row is *required*.

## File Footer

File Footer is the last line of each output file.

| Format | Example |
|---|---|
| |FEND| | `\|FEND\|` |

**Note** This row is *required*.

## Report Summary Header

| Format | Example |
|---|---|
| \|INFOSTART\| | `\|INFOSTART\|` |

**Note** This row is *required*.

## UC Applications Report Summary Row

This format definition describes the manner in which summary information is presented in the output files. An example of each data element is described below.

| Format | Examples |
|---|---|
| \|<format_version>\|<report_creation_time>\| | `\|9.1.1.1\|20130108225300GMT\|` |
| **Note** | • The "report_creation_time" field in the above example is used to describe scheduled report start time. These values in no way indicate the final report generation time, nor the amount of time taken to generate the report itself.<br>• All fields are *required* in all rows. |

## Report Summary Footer

| Format | Example |
|---|---|
| \|INFOEND\| | `\|INFOEND\|` |

**Note** This row is *required*.

## Customer Data Header

| Format | Example |
|---|---|
| \|ICUST\| | `\|CUST\|` |

**Note** This row is *required*.

## UC Applications Customer Data Row

| Format | Examples |
|---|---|
| \|<customer_name>\|<app_type>\|<app_version>\|<br><app_hostname>\|<br><app2_type>\|<app2_version>\|<br><app2_hostname>\|...<br>\|<app(N)_type>\|<app(N)_version>\|<br><app(N)_hostname>\| | `\|Customer2\|CUCM\|VERSION_8_6\|10.81.120.27\|`<br>`\|Customer5\|CUCM\|VERSION_8_6\|CUCM-5\|`<br>`\|Customer4*\|CUCM\|VERSION_8_6\|10.81.120.29\|CUC\|VERSION_8_6\|si911cxnpub-1\|`<br>**Note** This example shows that "Customer4" has failed report data collection and as a result no Subscriber MACD data rows will be displayed. In this case, SI was unable to indicate which UC Application had failed and so only the "customer_name" field is appended with the asterisk '*'.<br>`\|Customer6*\|CUCM\|VERSION_8_6\|~*\|`<br>**Note** This example shows that Customer6 has failed report data collection. The failed UC App ('~') has also been marked with the asterisk. In the case the "app_hostname" field has been populated with the tilde ('~') to indicate that "app_hostname" data was not available. This example was obtained by provisioning a Customer in SDR with an empty Unified Communications Manager cluster (no Unified Communications Manager application servers were provisioned). |

- The "app_hostname" field in the above example may be populated with either a hostname or IP Address. The "app_type" field indicates the version of the UC Application as it is provisioned in HCM-F SDR. The "app_type" field indicates the type of UC Application. As of HCM-F 9.1(1), SI only supports report collection from 8.6 Version UC Applications.

## Customer Footer Row

| Format | Example |
|---|---|
| \|CEND\| | `\|CEND\|` |

**Note** This row is *required* row if a **|CUST|** data row exists.

## MACD Report Header

| Format | Example |
|---|---|
| \|MACDSTART\| | `\|MACDSTART\|` |

**Note** This row is *required*.

## UC Applications Subscriber Summary Row

| Format | Examples |
|---|---|
| \|SUB-TOT\|<count>\| | `\| SUB-TOT \|6\|` |
| **Note** | • The SUB-TOT is a count of all Subscribers for a Customer included in the MACD report.<br>• The Lobby Phone User is included in this total count. |

## UC Applications Subscriber MACD Code Element

This format definition describes the way in which MACD Code elements will be represented in all Subscriber MACD rows. There is no separate definition row required in the file to describe the MACD Code elements.

MACD operations are reported at the Subscriber level only. Changes to Devices and Lines, including adding and deleting Devices and Lines are reported as a Change (‘C’) in the Subscriber MACD Row.

The following list describes the characters used to construct the format:

- A = Subscriber Entity is Added
- D = Subscriber Entity is Deleted
- C = Subscriber Entity is Changed

| Format | Examples |
|---|---|
| \|<macdcode>\| | `\|A\|`<br>`\|D\|`<br>`\|C\|` |
| **Note** | • Service Inventory reports the difference between the last successful data snapshot and the current data snapshot daily. Intermediate changes to Subscribers, Devices and Lines are not captured.<br>• " Last successful data snapshot", refers to the data snapshot that was taken during the most recent and successful scheduled report run. "Current data snapshot", refers to the data snapshot that is taken when current daily scheduled report is started.<br>• Typically, Service Inventory runs and generates a report every 24 hours. Scheduled report time changes, disabling the scheduled report or report generation errors affect this behavior. |

## UC Applications Subscriber MACD Row Format

This format definition describes the general layout of all MACD rows in the report. Certain fields described below are required of each MACD row, regardless of type, while individual differences are highlighted in the definition for each type later.

**Format**

|SUB|<MACDCODE>|<CUCM_IP>|<CUC_IP>|<SUB_USERNAME>|<SUB_UUID>|<SUB_FIRSTNAME>|<SUB_LASTNAME>|<SUB_EMAIL>|

<PRIMARY_TN>|<PRIMARY_EXTENSION>|<CUC_VM_EXTENSION>|<CUC_BILLING_ID>|<VOICE_FEATURE>|<VM_FEATURE>|

<PRESENCE_FEATURE>|<CUEAC_FEATURE>|DEV|<DEVICE_NAME>|<DEVICE_TYPE>|<DEVICE_MODEL>|<LOCATION>|

<EXT_MOBILITY>|LINE|<DIRECTORY_NUMBER>|<EXTERNAL_NUM_MASK>|LINE(N)|…|LINE_END(N)|DEV_END|DEV(N)|

…

|DEV_END(N)|SUB_END|

- The above fields are populated with the value retrieved from the provisioned Unified Communications Manager and Cisco Unity Connection UC Application servers. If a value for a field is not provisioned on the UC Application Servers or is not available for the type of Subscriber, then a '~' appears in the field of the SUB MACD row. In this case, where a field value is available on both the Unified Communications Manager and Cisco Unity Connection, the Unified Communications Manager value is always be used. The Cisco Unity Connection value is only be used if Unified Communications Manager value are not available for that subscriber, for example voice mail only user.
- The <CUCM_IP> and <CUC_IP> fields are populated with the UC Application Server's HCM-F provisioned IP address or the Hostname where Subscriber data is retrieved.
- The <SUB_UUID> field for a Voice Mail Only user is the equivalent Cisco Unity Connection Object ID field that is defined in the Cisco Unity Connection Rest API. If the user has both Unified

Communications Manager and Cisco Unity Connection features enabled, then this SUB_UUID field is populated with the Unified Communications Manager UUID and the Cisco Unity Connection Object ID is ignored.

- The <SUB_USERNAME>, <SUB_FIRSTNAME> and <SUB_LASTNAME> fields are populated with the Unified Communications Manager End User's "User ID", "First name" and "Last name" unless the Subscriber is a Voice Mail Only User. In that case, the fields are populated with the Cisco Unity Connection User's "Alias", "First Name" and "Last Name" fields.
- The <SUB_EMAIL> is populated with Unified Communications Manager "Email ID" field. For a Voice Mail Only User, the <SUB_EMAIL> field is populated with the Cisco Unity Connection "Corporate Email Address" field.
- The <PRIMARY_TN> field is populated from the Unified Communications Manager End User "Telephone Number" field. If the Subscriber is a Voice Mail Only User, then the "Extension" field of the Cisco Unity Connection User is used.
- The <PRIMARY_EXTENSION> field is populated from the "Directory Number" of the Unified Communications Manager End User's first LINE of the first DEVICE.
- The <VOICE_FEATURE> field is populated with a '1' is the Subscriber is provisioned on a Unified Communications Manager
- The <PRESENCE_FEATURE> field is populated with the Unified Communications Manager End User's provisioned "Primary Extension" field and typically populated with 0/1.
- The <VM_FEATURE> field is populated from the Cisco Unity Connection User's provisioned "Class of Service". If the COS indicates that the User is enrolled in Voice Mail, then the field is set with 1. Otherwise, this field is set to '~'.
- The Subscriber <CUC_BILLING_ID> and <CUC_VM_EXTENSION> Fields are only be populated if the <VM_FEATURE> field is 1, and is filled with a ~ in the event that the <VM_FEATURE> is set to '0' or '~'.
- The Subscriber field <CUEAC_FEATURE> is always filled with a ' ~' as the field is unobtainable with the current UC Application API's available.
- All <DEVICE> and <LINE> field data is only available from Unified Communications Manager.
- The <DEVICE_NAME> and <DEVICE_MODEL> fields are populated from the "MAC Address" and the "Product Type" of the Unified Communications Manager Device. The <DEVICE_TYPE> field is populated from the Unified Communications Manager API and is set to "Phone" for all Phone Device Types.
- The <LOCATION> field is populated with the device's provisioned location name. The device's location name is set using the Unified Communications Manager "System->Location" configuration page
- The Device's < EXT_MOBILITY> field is set using the Unified Communications Manager's "Enable Extension Mobility" check box of the Unified Communications Manager device.
- The < EXTERNAL_NUM_MASK > field is populated using the "External Phone Number Mask" of the Line of the Unified Communications Manager Device.

## UC Applications Subscriber MACD Add Records - Examples

Below are examples of a Subscriber MACD Add records.

An Add record is seen when a new End User is provisioned on CUCM or CUCxN since the last success report or if this is a Day Zero Report.

### CUCM Subscriber MACD Add

**Example 13-46**

```
|SUB|A|10.81.120.27|~|userA|{4BFD972A-F280-B694-E616-E4FBD7060711}|sitest|userA|userA|
~|v1501merpart1|~|~|1|~|1|~|DEV|SEP111111A01016|Phone|Cisco|7970|Hub_None|1|LINE|801016|~|LINE_END|
DEV_END|SUB_END|
```

### CUCxN Subscriber MACD Add

**Example 13-40**

```
|SUB|A|~|108.2.5.25|user09000|3722c735-a696-4efb-9c7d-91b0e9ae5e07|
09000_first_changed0110|09000_last_changed0110|9000@yutu.com.changed0110|809000|~|809000|user09000billing
|~|1|~|~|DEV|LINE|LINE_END|DEV_END|SUB_END|
```

## UC Applications Lobby Phone Subscriber MACD - Examples

A lobby phone has more than 0 lines and is not associated to any end user. The Change indicates that a DEVICE or LINE or some other Device or Line field was Added, Deleted or Changed. The Lobby Phone Subscriber has a list of Devices Per Customer. The Lobby Phone Subscriber is Add when the “Day Zero Report” is generated.

### Lobby Phone Subscriber MACD Add

**Example 13-41**

```
|SUB|A|~|~|~|~|~|~|~|~|~|~|~|~|~|~|~|DEV|SEP111111A09006|Phone|Cisco
7970|Hub_None|0|LINE|809006|~|LINE_END|
LINE|29006|~|LINE_END|DEV_END|DEV|SEP111111A09008|Phone|Cisco
7970|Hub_None|0|LINE|809008|~|LINE_END|LINE|29008|~|
LINE_END|LINE|39008|~|LINE_END|DEV_END|DEV|SEP111111A09013|Phone|Cisco
7970|Hub_None|0|LINE|809013|~|LINE_END|DEV_END|
DEV|SEP999999999999|Phone|Cisco
E20|Hub_None|0|LINE|999999999|~|LINE_END|DEV_END|DEV|SEP111111A08001|Phone|Cisco
 7970|
Hub_None|0|LINE|808001|~|LINE_END|LINE|7777|~|LINE_END|LINE|28001|~|LINE_END|DEV_END|DEV|SEP111111A08002
|Phone|Cisco
7970|Hub_None|0|LINE|808002|~|LINE_END|DEV_END|DEV|SEP111111A08003|Phone|Cisco
 7970|Hub_None|0|LINE|
808003|~|LINE_END|DEV_END|DEV|SEP111111A08011|Phone|Cisco
7970|Hub_None|0|LINE|808011|~|LINE_END|DEV_END|DEV|
SEP111111A08012|Phone|Cisco
7970|Hub_None|0|LINE|808012|~|LINE_END|DEV_END|DEV|SEP111111A08013|Phone|Cisco
 7970|
Hub_None|0|LINE|808013|~|LINE_END|DEV_END|DEV|SEP123412341234|Phone|Cisco
 TelePresence|v1501mer_loc1_50k|0|LINE|1234
```

```
|~|LINE_END|LINE|8888|~|LINE_END|DEV_END|DEV|SEP444444444444|Phone|Cisco
 Cius|v1501mer_loc3_160k|0|LINE|4444
|~|LINE_END|DEV_END|DEV|SEP555555555555|Phone|Cisco
7975|Hub_None|0|LINE|5555|~|LINE_END|DEV_END|DEV|
SEP999999999999|Phone|Cisco
E20|Hub_None|0|LINE|999999999|~|LINE_END|DEV_END|SUB_END|
```

### Lobby Phone Subscriber MACD Change

#### Example 13-42

```
|SUB|C|~|~|~|~|~|~|~|~|~|~|~|~|~|~|DEV|SEP5679650A2502|Phone|Cisco
7970|Hub_None|0|LINE|2502|~|
LINE_END|DEV_END|DEV|SEP5679650A2503|Phone|Cisco
7970|Hub_None|0|LINE|2503|~|LINE_END|DEV_END|DEV
|SEP111111A01000|Phone|Cisco
7970|Hub_None|0|LINE|801000|~|LINE_END|DEV_END|DEV|
SEP5679650A2201|Phone|Cisco
7970|Hub_None|0|LINE|23423510101|~|LINE_END|DEV_END|SUB_END|
```

## UC Applications Subscriber MACD Delete - Examples

Below are examples of a Subscriber MACD Delete records.

### CUCM Subscriber MACD Delete

#### Example 13-43

```
|SUB|D|108.2.5.23|~|test111|{1297144E-C445-ED64-3679-A1F103F949B1}
|cucm111|cucm111_changed|cucm111@cisco.com|cucm_TN_111|~|~|~|1|~|1|~|DEV|LINE|LINE_END|DEV_END|SUB_END|
```

### CUCxN Subscriber MACD Delete

#### Example 13-44

```
|SUB|D|~|108.2.6.13|user08013|538cb999-d224-4432-bfad-ddfe4e39e94f|sitest|user08013
|~|808013|~|808013|~|~|1|~|~|DEV|LINE|LINE_END|DEV_END|SUB_END|
```

## UC Applications Subscriber MACD Change - Examples

Below are examples of a Subscriber MACD Change records.

### CUCM and CUCxN Subscriber MACD Change

#### Example 13-45

```
|SUB|C|108.2.6.11|108.2.6.13|user08005|{0AE9953B-37EF-54AE-B930-454E6553DFD0}|
sitest|user08005_chanagedforES|~|808005|v1501mer-part1|808005|~|1|1|1|~|DEV|SEP111111A08005
|Phone|Cisco 7970|Hub_None|0|LINE|808005|~|LINE_END|DEV_END|SUB_END|
```

### CUCM Subscriber MACD Add

#### Example 13-46

```
|SUB|A|10.81.120.27|~|userA|{4BFD972A-F280-B694-E616-E4FBD7060711}|sitest|userA|userA|
~|v1501merpart1|~|~|1|~|1|~|DEV|SEP111111A01016|Phone|Cisco|7970|Hub_None|1|LINE|801016|~|LINE_END|
DEV_END|SUB_END|
```

## MACD Report Footer

| Format | Examples |
|---|---|
| \|MACDEND\| | `\|MACDEND\|` |
| **Note** This row is *required*. | |