CHAPTER 5

Monitoring Predefined Cisco Unified Communications Manager Objects

RTMT provides a set of default monitoring objects that assist you in monitoring the health of the Cisco Unified Communications Manager application. Default objects include performance counters for call processing activity and other supported services.

The system logs data every 5 minutes for predefined Cisco Unified Communications Manager counters.

This chapter contains information on the following topics:

Predefined Cisco Unified Communications Manager Objects Overview

RTMT displays information on predefined Cisco Unified Communications Manager objects in the monitoring pane when you select Communications Manager in the quick launch channel. The tool monitors the predefined objects on all servers in an cluster, if applicable.

Tip 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 *Cisco Unified Communications Manager Administration Guide* or *Cisco Unity Connection System Administration Guide*.

Table 5-1 provides information on the predefined object that RTMT monitors.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart in which you are interested. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the "**R**" key.

Table 5-1 Cisco Unified Communications Manager Categories

Category	Description
CallManager Summary	Displays registered phones, calls in progress, and active gateway ports and channels. To display information on predefined Cisco Unified Communications Manager objects, choose **CallManager > CallManager Summary**.
Call Process	• Call Activity—Displays the call activity on Cisco Unified Communications Manager, including calls completed, calls attempted, calls in progress, and logical partition total failures. This includes all servers in the cluster, if applicable. To display information on call activities, choose **CallManager > Call Process > Call Activity**. • Gateway Activity—Displays gateway activity on Cisco Unified Communications Manager, including active ports, ports in service, and calls completed. This includes all servers in the cluster, if applicable. To display information on gateway activities, choose **CallManager > Call Process > Gateway Activity**. Select the type of gateway interface from the **Gateway Type** drop-down box. • Trunk Activity—Displays the trunk activity on Cisco Unified Communications Manager, including calls in progress and calls completed. This includes all servers in the cluster, if applicable. To display information on trunk activities, choose **CallManager > Call Process > Trunk Activity**. Select the trunk type in the **Trunk Type** drop-down box. • SDL Queue—Displays SDL queue information, including number of signals in queue and number of processed signals. To display information on the SDL Queue, choose **CallManager > Call Process > SDL Queue**. Select the type from the **SDL Queue Type** drop-down list box. • SIP Activity—Displays SIP activity on Cisco Unified Communications Manager, including summary requests, summary responses, summary of failure responses in, summary of failure responses out, retry requests out, and retry responses out. This includes all servers in the cluster, if applicable. To display information on SIP activities, choose **CallManager > Call Process > SIP Activity**. • Session Trace—Displays all SIP message activity: specifically, the incoming and outgoing calls and sessions that pass through the Cisco Unified Communications Manager. Provides associated call flow diagram for each SIP transaction. To display information on Session Trace, choose **CallManager > Call Process > Session Trace**. For more information, see "Understanding Session Trace" section on page 5-8.

Table 5-1 Cisco Unified Communications Manager Categories (continued)

Category	Description
Device	Device Summary displays information on the Cisco Unified Communications Manager server, including the number of registered phone devices, registered gateway devices, and registered media resource devices. This includes all servers in the cluster, if applicable. Device Search displays cluster name and device types in a tree hierarchy and allows you to query for information on phones and devices. Phone Summary displays information on the Cisco Unified Communications Manager server, including the number of registered phones, registered SIP phones, registered SCCP phones, partially registered phones, and the number of failed registration attempts. This includes all servers in the cluster, if applicable. To display information on the number of registered phones, gateways, and media resource devices on Cisco Unified Communications Manager, choose **CallManager > Device > Device Summary**. **Tip** To monitor other devices, you must perform additional configuration steps, as described in the "Finding Specific Devices to Monitor" section on page 5-17.
Service	• Cisco TFTP—Displays Cisco TFTP status on the Cisco Unified Communications Manager server, including total TFTP requests, total TFTP requests found, and total TFTP requests aborted. This includes all servers in the cluster, if applicable. To display information on the Cisco TFTP service, choose **CallManager > Service > Cisco TFTP**. • Heartbeat—Displays heartbeat information for the Cisco Unified Communications Manager, Cisco TFTP service. To display the heartbeat status of Cisco Unified Communications Manager servers, Cisco TFTP servers, choose **CallManager > Service > Heartbeat**. • Database Summary—Provides connection information for the server, such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, the number of replicates that have been created, and the status of the replication. To display information on the database, choose **CallManager > Service > Database Summary.**

Table 5-1 Cisco Unified Communications Manager Categories (continued)

Category	Description
CTI Manager	Displays information on the devices and applications that interfaces with the CTI Manager. To display information on CTI Applications, choose **CallManager > CTI > CTI Manager**. To monitor specific CTI types, you must perform additional configuration steps, as described in the following sections: • Finding CTI Applications to Monitor, page 5-21 • Finding CTI Devices to Monitor, page 5-22 • Finding CTI Lines to Monitor, page 5-23 You cannot choose CTI Manager by using the menu bar. To monitor the number of open devices, lines, and CTI connections in a single window on Cisco Unified Communications Manager, see the "Working with Devices" section on page 5-17.
Intercompany Media Services	• Routing—Displays the total number of Cisco Intercompany Media Engine routes maintained by Cisco Unified Communications Manager. To display information on call activities, choose **CallManager > Intercompany Media Services > Routing**. • Call Activities—Displays the Cisco Intercompany Media Engine call activity, including the number of calls that were accepted, busy, no answer, and failed. To display information on call activities, choose **CallManager > Intercompany Media Services > Call Activities**. For more information, see the "Monitoring Intercompany Media Services" section on page 5-27.

Additional Information

See the Related Topics, page 5-28.

Viewing the Cisco Unified Communications Manager Summary

In a single monitoring pane, RTMT allows you to monitor information about a Cisco Unified Communications Manager server or about all servers in a cluster (if applicable). In the callmanager summary window, you can view information on the following predefined object:

- Registered Phones
- Calls in Progress
- Active Gateway, Ports & Channels

Additional Information

See the "Related Topics" section on page 5-28.

Monitoring Call-Processing Activity

The Call Process monitoring category monitors the following items:

- Call Activity—You can monitor the number of calls that were attempted, calls that were completed, calls in progress, and logical partition total failures for a particular server or for an entire cluster (if applicable).
- Gateway Activity—You can monitor gateway activity for each gateway type. Gateway activity monitoring includes the number of active ports, the number of ports in service, and the number of calls that were completed for each gateway type for a particular server or for an entire cluster (if applicable).
- Trunk Activity—The system monitors trunk activity by trunk type for a particular server or for an entire cluster (if applicable). Trunk activity monitoring includes the number of calls in progress and the number of calls that were completed for a particular trunk type.
- SDL Queue—SDL queue monitoring monitors the number of signals in the SDL queue and the number of signals that were processed for a particular signal distribution layer (SDL) queue type. The SDL queue types comprise high, normal, low, and lowest queue. You can monitor the SDL queue for a particular server or for an entire cluster (if applicable).
- SIP Activity—The system displays a summary of SIP requests, SIP responses, total number of failed incoming responses (4xx, 5xx, and 6xx), total number of failed outgoing responses (4xx, 5xx, and 6xx), number of retry requests, and number of retry responses.
- Session Trace—You can search or trace the calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. RTMT downloads the Call Log file that includes the Start Time and Duration, searches for the matching calls, lists the matching call records, and provides the Call Flow Diagram.

Table 5-2 provides information about the call processing objects that RTMT monitors, the alert, thresholds, and defaults. For information on Cisco Unified Communications Manager call activity daily reports, refer to *Cisco Unified Serviceability Administration Guide*.

Table 5-2 Call Processing Category

Monitored Objects (displayed)	Alert/Threshold/Default
CallsAttempted, CallsCompleted, CallsInProgress, and Logical Partition Failures Total for each server and cluster (if applicable).	N/A
CallsAttempted, CallsCompleted, and CallsInProgress of each type of MGCP FXS/FXO/PRI/T1CAS/H.323 gateway, as well as SIP and H.323 Trunks for each server and cluster (if applicable).	N/A
Channel/Port Status of each MGCP FXS/FXO/PRI/T1CAS gateway.	N/A
SDL Queue activity on each server.	N/A
MGCP FXS Gateway—Number of In-Service and Active ports for each server and cluster (if applicable).	Route-List exhausted

Table 5-2 Call Processing Category (continued)

Monitored Objects (displayed)	Alert/Threshold/Default
MGCP FXO Gateway—Number of In-Service and Active ports for each server and cluster (if applicable).	Route-List exhausted
MGCP PRI Gateway—Number of In-Service and Active channels for each server and cluster (if applicable).	• D-Channel out of service • Route List exhausted
MGCP T1CAS Gateway—Number of In-Service and Active ports for each server and cluster (if applicable).	Route List exhausted

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Call-Processing Logs

The system accumulates call-processing data in the memory whenever RTMT calls the LogCall API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters on the basis of the following calculation:

- cmCallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- cmCallsInProgress—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXO_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_PRI_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_T1_CAS_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwH323_CallsInProgress—Average of all the values that were collected in last 5 minutes
- gwH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkH323_CallsInProgress—Average of all the values collected in last 5 minutes
- trunkH323_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

- trunkSIP_CallsAttempted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- trunkSIP_CallsInProgress—Average of all the values that were collected in last 5 minutes
- trunkSIP_CallsCompleted—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- gwMGCP_FXS_PortsInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_PortsInService—Average of all the values that were collected in lasts 5 minutes
- gwMGCP_PRI_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_SpansInService—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXS_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_FXO_ActivePorts—Average of all the values that were collected in last 5 minutes
- gwMGCP_PRI_ActiveChannels—Average of all the values that were collected in last 5 minutes
- gwMGCP_T1_CAS_ActiveChannels—Average of all the values that were collected in last 5 minutes

The AMC service logs the call data in windows Performance tool-compatible csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for the server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the Call Log applies: CallLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Session Trace

The Cisco Unified Communications Manager captures and logs all SIP message activities, which comprise the incoming and outgoing calls or sessions that pass through the Cisco Unified Communications Manager. The Cisco Unified Communications Manager stores the messages on a per-transaction basis in a new Call Log file, which can be downloaded through RTMT for post-processing activity.

RTMT users can search or trace the calls based on the following criteria:

- Calling Number/URI
- Called Number/URI
- Start Time
- Duration

RTMT downloads the Call Log file that includes the Start Time and Duration. The tool searches for the matching calls, lists the matching call records, and provides the SIP message Call Flow Diagram.

Before you Begin

Perform the following task:

- Use the enterprise parameter, Enable Call Trace Log, to enable or disable Call Tracing. For more information on configuring enterprise parameters, refer to the *Cisco Unified Communications Manager Administration Guide*.
- The default value for maximum number of Call Trace log files specifies 2000 and the default value for maximum Call Trace log file size specifies 2 MB.

Procedure

Step 1 To display information on Session Trace, from the RTMT menus, choose **CallManager > Call Process > Session Trace**.

The Session Trace screen displays.

Step 2 Enter the search criteria and Click **Run**.

Note You can search calls based on the following criteria: Calling Number/URI, Called Number/URI, Start Time, and Duration. The search applies to the entire Unified CM cluster, not just the local node. If any node fails to collect the trace files, the system displays an error message in the bottom panel and pops up the message prompt to the user.

Click **Yes** to ignore the error and generate the table, based on the input.

Note In Calling Number/URI, Called Number/URI, you can use wild character "*" to match any number of characters. For example, a search for 123* fetches numbers like "123", "123456", "123*", "1234", etc.
If you want to search for numbers with a "*" in them, use "*". For example, to search for a Called Number like 12*45, enter 12*45 in the search box.

If matching calls are found, the Matching Call pane displays Start Time, Calling DN, Original Called DN, Final Called DN, and Termination Cause Code. The Termination Cause Code helps to identify the failure calls, and provides the reason for the failure of the calls. The Termination Cause Code is displayed in parenthesis followed by description.

Consider the following scenario:

- If the call is in progress or if the call trace logging is turned off after the call, the Termination Cause Code column remains blank.

Note If cause code description is missing or if you want more information on the Termination Cause Codes, refer the CDR cause codes in *Cisco Unified Call Details Records Administration Guide*.

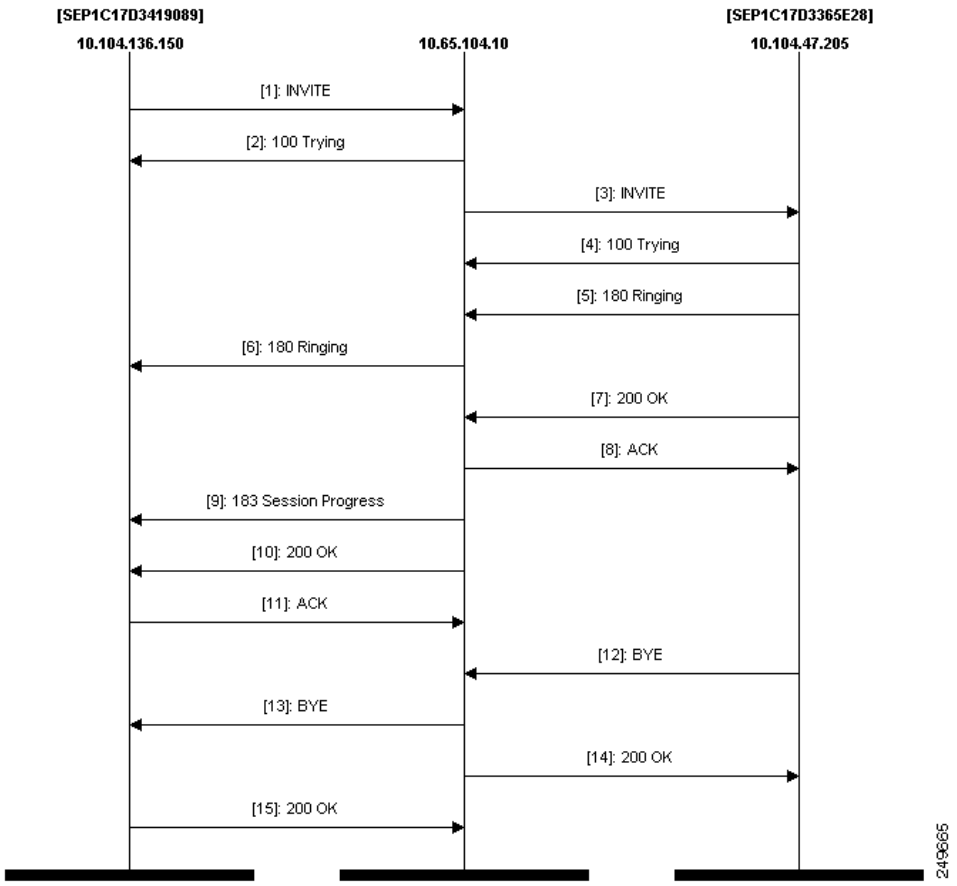
Step 3 Select a call (a row) to trace.

By default, **Include SIP Message** check box is selected to view the associated SIP protocol messages or call transactions.

Step 4 To generate the SIP Message Call Flow Diagram, click **Trace Call**. If you want to stop the generation of the session information, click **Cancel** on the progress window.

The Analyze Call Diagram window displays the corresponding SIP messages in the Call Flow Diagram.

Figure 5-1 Call Flow Diagram for Simple Call Scenario



Step 5 Click the tabs that you want to view. The following tabs are available:

- Call Flow Diagram—Displays the corresponding SIP messages in the Call Flow Diagram.
- Log File—Displays the entire log file.
- SIP Message—Appears only when the **Include SIP Message** check box is checked. Displays the actual SIP message that gets logged into the SDI log file.

Step 6 The following table lists the messages that display when you move your mouse on each SIP message in the Call Flow Diagram:

Displayed Messages	Description
Sender	Displays the IP address of the originating call.
SIP Call ID	Displays the SIP call ID.
Message Label	Displays the message type for the corresponding SIP message onto which you move your mouse; for example, 200 OK, or180 Ringing.

Displayed Messages	Description
Receiver	Displays the IP address of the destination call.
Device Name	Displays the name of the device.
Message Tag	Displays the sequence number to match the actual messages in the SDI Trace file.
Correlation ID	Displays the Correlation ID.
Timestamp	Displays the server time at which the call operation (call setup/split/join/release) happens.

- Click the **See message in log file** link to view the subset of call logs that can be downloaded and analyzed.
- Click the **See SIP Message** link. A new **SIP Message** tab displays adjacent to the **Log File** tab. Click the **SIP message** tab to display the actual SIP message that gets logged into the SDI log file.

  To view the SIP messages that get logged into the SDI log file, do the following:

  – check the **Enable SIP Call Processing Trace** check box in the Trace Configuration window of Cisco Unified Serviceability (**Trace > Configuration**). See *Cisco Unified Serviceability Administration Guide* for more information.

  – set the trace level to any one of the following—State Transition, Significant, Arbitrary or Detailed.

Note You can view the **See SIP Message** link only when the **Include SIP Message** check box is checked.

Step 7 Click **Save.**

The call flow diagram gets saved as index.html in the specified folder along with the SIP messages. You can email the files to the Technical Assistance Center (TAC).

Note If the files are zipped, extract the zipped files to a local folder and open them to view the images.

You can do the following:

a. To view the online help, click **Help**.

b. To exit the Analyze Call Diagram screen, click **Close**.

c. To navigate to the previous page, click **Previous Messages**.

d. To navigate to the next page, click **Next Messages**.

Note **Previous Messages** or **Next Messages** is enabled only when the message size exceeds a threshold.

Call Log files

The Session Manager logs the call data in new log files. These new log files are located in the following folder: /var/log/active/cm/trace/ccm/calllogs/.

The Call Log name has the following file name pattern: calllogs_dddddddd.txt.gz.

The Call Logs include the following message types:

- Call Control—Writes call information at call setup, split, join and release.

  ```
  Timestamp|MessageType (CC)|Operation (SETUP/SPLI/JOIN/RELEASE)|CI for one leg (aCI)|CI for other leg (bCI)|calling DN|Orig Called DN|Final Called DN
  ```

- Device Layer—Writes metadata information that relates to message from or to the device.

  ```
  Timestamp|MessageType (SIPL/SIPT)|My leg CI|Protocol(tcp/ucp)|Direction (IN/OUT)|local ip|local port|device name|device ip|device port|Correlation id|Message Tag|SIP Call ID|SIP method
  ```

Scenarios while Uninstalling RTMT

Consider the following scenarios, while uninstalling RTMT:

1. User saves the call flow diagram files in a folder (created by the user under **user.dir** directory)—All the files in **user.dir** are deleted except the newly created folder and the **user.dir** directory.
2. User saves the call flow diagram files in a folder (created during RTMT installation) under **user.dir** directory—All the files in **user.dir** are deleted including the **user.dir** directory.
3. User directly saves the call flow diagram files under **user.dir** directory—All the files in **user.dir** are deleted except the newly created files and the **user.dir** directory.
4. User saves the call flow diagram files in a folder which is outside **user.dir** directory—**user.dir** and its contents are removed. The folder created by the user is not deleted.

Limitations

The following limitations apply when the Call Flow Diagram gets generated:

- Search does not show incomplete calls.

  `Example:`

  When the user picks up the handset and hangs up without dialing the complete DN, it will not be listed in the search results.

- The Call Flow Diagram does not show some SIP messages in the following scenarios:
  - Conference calls involving more than three parties.
  - A call leg is used to invoke a feature alone.

  `Example:`

  Phone B and Phone C are in the same pickup group.

  1. User A calls Phone B.
  2. User C lifts up the Phone C handset.
  3. User C presses the PickUp softkey to pickup the call.

  SIP messages exchanged in Step 2 are not displayed in the Call Flow Diagram.

  In these cases, a RELEASE message is logged in the call logs without a corresponding SETUP message.

Monitoring Services

The Service monitoring category monitors the activities of Cisco TFTP requests, database activities, and heartbeat of the server or of different servers in a cluster (if applicable).

The Cisco TFTP service builds and serves files that are consistent with the trivial file transfer protocol, which is a simplified version of the File Transfer Protocol (FTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files. You can view the total Cisco TFTP requests, requests not found, and requests that were aborted.

The tool (RTMT) monitors the heartbeat of Cisco Unified Communications Manager and Cisco TFTP services for the server or for different servers in a cluster (if applicable). The heartbeat acts as an indicator of the life of whatever it is monitoring. When the heartbeat is lost, a blinking icon appears in the lower, right corner of the RTMT window. To find when the heartbeat loss was detected, click the blinking icon. An email can notify you of the heartbeat loss, if you configure the system to do so.

The database summary provides connection information for the server or for each server in a cluster (if applicable), such as the change notification requests that are queued in the database, change notification requests that are queued in memory, the total number of active client connections, the number of devices that are queued for a device reset, replicates created, and replication status.

Table 5-3 provides information about the service objects that RTMT monitors, the alert, thresholds, and defaults. For information on daily reports for CTI and Cisco TFTP usage statistics, refer to *Cisco Unified Serviceability Administration Guide*.

Table 5-3 Services Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of open devices, lines, CTI connections, and active Cisco Unified Communications Manager links for each CTI Manager.	N/A
TotalTftpRequests and TotalTftpRequestsAborted for each Cisco TFTP server.	N/A
Connection and replication status for each Directory server.	• Connection failed. • Replication failed.
Heartbeat rate for each Cisco CallManager, Cisco TFTP services.	• Cisco Unified Communications Manager heartbeat rate specifies <0.x. Default specifies 0.5. • Cisco TFTP heartbeat rate specifies <0.x. Default specifies 0.5.

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Service Logs

The service data accumulates in the memory whenever RTMT calls the LogService API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The system logs data every 5 minutes for the following counters, based on the following calculation:

- ctiOpenDevices—Average of all the values that were collected in last 5 minutes
- ctiLines—Average of all the values that were collected in last 5 minutes
- ctiConnections—Average of all the values that were collected in last 5 minutes
- ctiActiveCMLinks—Average of all the values that were collected in last 5 minutes
- tftpRequests—Cumulative (difference between last collected value and the first collected value in last 5 minutes)
- tftpAbortedRequests—Cumulative (difference between last collected value and the first collected value in last 5 minutes)

The AMC service logs the service data in csv format. The header of the log comprises the time zone information and a set of columns with the counters that were previously listed for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the Service Log applies: ServiceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log comprises the header.

Additional Information

See the "Related Topics" section on page 5-28.

Monitoring Devices

The Device monitoring category provides a summary of devices, device search capability, and a summary of phones.

Table 5-4 provides information about the device objects that RTMT monitors, the alert, thresholds, and defaults, and what kind of reports that RTMT generates for those devices. For information on daily reports on number of registered devices, refer to *Cisco Unified Serviceability Administration Guide*.

Table 5-4 Devices Category

Monitored Objects (displayed)	Alert/Threshold/Default
Number of registered phones for each server or for all servers in a cluster (if applicable).	Total number of registered phones drops by X% in consecutive polls. Default specifies 10%.

Table 5-4 Devices Category (continued)

Monitored Objects (displayed)	Alert/Threshold/Default
Number of registered gateways on each server or for all servers in a cluster (if applicable).	For Cisco Unified Communications Manager: • (Warning) Clusterwide total number of registered gateways decreased in consecutive polls. • (Informational) Clusterwide total number of registered gateways increased in consecutive polls. For Cisco Unified Communications Manager Business Edition 5000: • (Warning) Total number of registered gateways decreased in consecutive polls. • (Informational) Total number of registered gateways increased in consecutive polls.
Number of registered media devices on each server or for all servers in a cluster (if applicable).	For Cisco Unified Communications Manager: • (Warning) Clusterwide total number of registered media devices decreased in consecutive polls. • (Informational) Clusterwide total number of registered media devices increased in consecutive polls. • Media List exhausted. For Cisco Unified Communications Manager Business Edition 5000: • (Warning) Total number of registered media devices decreased in consecutive polls. • (Informational) Total number of registered media devices increased in consecutive polls. • Media List exhausted.

The Device Search menu comprises the following items on which you can search: phones, gateway devices, H.323 devices, CTI devices, voice-messaging devices, media resources, hunt lists, and SIP trunks.

You can search on any device in the Cisco Unified Communications Manager system and choose the status of the devices, including registered, unregistered, rejected, any status, and devices that are only configured in the database. You can also search by any model, or a specific device model, and set up criteria that include several different attributes. Within the phone search, you can also search on the basis of phone protocol.

RTMT queries RIS to find the matching device. Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

If you have Cisco Unified Communications Manager clusters and you search for a device by choosing the any status option, RTMT does not display a snapshot of the matched device type, but rather it displays data for that device type from the RIS database for all specified Cisco Unified Communications Manager servers for a period of time. As a result, you may see multiple entries of a device with multiple statuses (Registered, Unregistered, and so on) in RTMT.

When you see multiple entries of a device, the current status of the device reflects the entry that has the latest time stamp. By configuring the RIS Unused Cisco CallManager Device Store Period service parameter for the Cisco RIS Data Collector service in Cisco Unified Communications Manager Administration, you can configure the period of time that the RIS database keeps information on unregistered or rejected device. Refer to *Cisco Unified Communications Manager Administration Guide* for more information on configuring service parameter.

Tip To find the matching item, RTMT requires that you activate the Cisco RIS Data Collector service in the Service Activation window.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a time stamp of the device that has been opened/closed and the application that controls the device media.

The phone summary provides information on the number of registered phones, phones that are running SIP, phones that are running SCCP, partially registered phones, and the number of failed registration attempts.

Additional Information

See the "Related Topics" section on page 5-28.

Understanding Device Logs

The device data accumulates in the memory whenever RTMT calls the LogDevice API. Every 5 minutes, RTMT logs the data into the file as a single record and cleans the memory.

The data gets logged every 5 minutes for the following counters based on the following calculation:

- gatewayDevicesFXS—Average of all the values that were collected in last 5 minutes
- gatewayDevicesFXO—Average of all the values that were collected in last 5 minutes
- gatewayDevicesPRI—Average of all the values that were collected in last 5 minutes
- gatewayDevicesT1—Average of all the values that were collected in last 5 minutes
- gatewayDevicesH323—Average of all the values that were collected in last 5 minutes

The AMC service logs the device data in csv format. The header of the log comprises the time zone information and a set of columns with the previously listed counters for a server. These sets of columns repeat for every server in a cluster, if applicable.

The following file name format of the Device Log applies: DeviceLog_MM_DD_YYYY_hh_mm.csv.

The first line of each log file comprises the header.

Additional Information

See the "Related Topics" section on page 5-28.

Working with Devices

This section contains information on the following topics:

Finding Specific Devices to Monitor

By performing the following procedure, you can monitor data for the following device types:

- Phones
- Gateway Devices
- H.323 Devices
- CTI Devices
- Voice Mail Devices
- Media Resources
- Hunt List
- SIP Trunk

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click **CallManager.**
  - In the tree hierarchy, double-click **Device.**
  - Click the Device Search icon.
- Choose **CallManager > Device > Device Search > Open Device Search** > <device type; for example, Phone, Gateway, Hunt List, and so on>. A device selection window displays where you enter the search criteria. Go to Step 4.

The Device Search window displays the cluster names (if applicable) and tree hierarchy that lists all device types that you can monitor.

Tip After you display the Device Search or CTI Search panes, you can right-click a device type and choose **CCMAdmin** to go to Cisco Unified Communications Manager Administration.

Step 2 To find all devices or to view a complete list of device models from which you can choose, right-click the cluster name and choose **Monitor**.

Step 3 To monitor a specific device type, right-click or double-click the device type from the tree hierarchy.

Tip If you right-click the device type, you must choose **Monitor** for the device selection window to display.

Step 4 In the Select device with status window, click the radio button that applies.

Step 5 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specific Cisco Unified Communications Manager server for which you want the device information to display.

Tip In the remaining steps, you can choose the **< Back**, **Next >**, **Finish**, or **Cancel** buttons.

Step 6 Click the **Next >** button.

Step 7 In the Select Device with Download Status pane, click the radio button that applies, and click **Next**.

Step 8 In the Search by device model pane, click the radio button that applies.

Tip If you chose **Device Model**, choose the device type for which you want the device information to display.

Step 9 Click **Next**.

Step 10 In the Search with name pane, click the radio button that applies and enter the appropriate information in the corresponding fields, if required.

Tip If you enter the IPv6 address, the IP Subnet does not apply. Cisco Unified Communications Manager Business Edition 5000 does not support IPv6.

Step 11 Click **Next**.

Step 12 In the Monitor following attributes pane, check one or all of the search attributes.

Tip If you check the Ipv6Address check box, be aware that Cisco Unified Communications Manager Business Edition 5000 does not support IPv6.

Step 13 Click **Finish**.

Tip Some devices may not provide information for all search criteria. For example, if you select to monitor a phone for active load, inactive load, download status, or download reason, the download status results display Unknown for phone models that cannot provide this information.

Additional Information

See the Related Topics, page 5-28.

Viewing Phone Information

You can view information about phones that display in the RTMT device monitoring pane. This section describes how to view phone information.

Procedure

Step 1 To display the phone in the RTMT device monitoring pane, see the "Finding Specific Devices to Monitor" section on page 5-17.

Step 2 Perform one of the following tasks:

- Right-click the phone for which you want information to display and choose **Open**.
- Click the phone and choose **Device > Open**.

The Device Information Window displays.

Step 3 In the Select Device with Status pane, click the radio button that applies.

Step 4 In the drop-down list box next to the radio button that you clicked, choose **Any CallManager** or a specificCisco Unified Communications Manager server for which you want the device information to display.

Step 5 In the Search By Device Model pane, choose the phone protocol that you want to display.

Step 6 Click the **Any Model or Device Model** radio button. If you click the Device Model radio button, choose a particular phone model that you want to display.

Step 7 Click **Next**.

Step 8 In the Search With Name pane, click the radio button that applies and enter the appropriate information in the corresponding fields.

Step 9 In the Monitor following attributes pane, check one or all of the search attributes.

Step 10 Click **Finish**.

The Device Information window displays. For more information on the device, choose any field that displays in the left pane of the window.

Additional Information

See the Related Topics, page 5-28.

Viewing Device Properties

You can view the properties of devices that display in the RTMT device monitoring pane. This section describes how to view device properties.

Procedure

Step 1 Display the device in the RTMT device monitoring pane. See the "Finding Specific Devices to Monitor" section on page 5-17.

Step 2 Perform one of the following tasks:

- Right-click the device for which you want property information and choose **Properties**.

- Click the device for which you want property information and choose **Device > Properties**.

Step 3 To display the device description information, click the **Description** tab.

Step 4 To display other device information, click the **Other Info** tab.

Additional Information

See the Related Topics, page 5-28.

Configuring Polling Rate for Devices and Performance Monitoring Counters

Cisco Unified Communications Manager polls counters, devices, and gateway ports to gather status information. In the RTMT monitoring pane, you configure the polling intervals for the performance monitoring counters and devices.

Note High-frequency polling rate may adversely affect Cisco Unified Communications Manager performance. The minimum polling rate for monitoring a performance counter in chart view specifies 5 seconds; the minimum rate for monitoring a performance counter in table view specifies 1 second. The default value for both specifies 10 seconds.

The default value for devices specifies 10 minutes.

Perform the following procedure to update the polling rate:

Procedure

Step 1 Display the device or performance monitoring counter in the RTMT monitoring pane.

Step 2 Click the device and choose **Edit > Polling Rate**.

Step 3 In the Polling Interval pane, specify the time that you want to use.

Step 4 Click **OK**.

Additional Information

See the Related Topics, page 5-28.

Monitoring CTI Applications, Devices, and Lines

The CTI category monitors CTI Manager activities and provides CTI search capability. With CTI Manager, you can monitor the number of open devices, lines, and CTI connections.

You can specify criteria for the CTI applications, devices, and lines that include CTI status, device name, application pattern, and attributes.

Tip To find the matching item, RTMT requires that you activate the Cisco RIS Data Collector service in the Service Activation window inCisco Unified Serviceability.

Results display in a table with a row for each matched device, a column for each of the specified attributes, and a timestamp of the device that has been opened/closed and the application that controls the device media.

Working with CTI Applications, Devices, and Lines

This section contains information on the following topics:

Viewing CTI Manager Information

To display a chart of open devices, lines, and CTI connections for each server or for each server in a cluster (if applicable), click **CallManager** in the quick launch channel; double-click **CTI**, and then click the **CTI Manager** icon.

Additional Information

See the Related Topics, page 5-28.

Finding CTI Applications to Monitor

Perform the following procedure to find specific CTI applications to monitor:

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click CallManager.
  - In the tree hierarchy, double-click **CTI**.
  - Click the CTI Search icon.
- Choose **CallManager > CTI > CTI Search > CTI Applications**. The selection window displays where you can enter the search criteria.

Step 2 From the CTI Manager drop-down list box, choose the CTI Manager that you want to monitor.

Step 3 From the Applications Status drop-down list box, choose the application status.

Step 4 Click **Next**.

Step 5 In the Application Pattern pane, click the radio button that applies.

Step 6 Enter the information in the field for the radio button that you clicked; for example, if you clicked the IP Subnet radio button, enter the IP address and the subnet mask in the field.

Tip If you enter the IPv6 address, the IP Subnet does not apply. IPv6 support does not apply to Cisco Unified Communications Manager Business Edition 5000.

Step 7 Click **Next**.

Step 8 In the Monitor following attributes window, check one or all of the check boxes for the attributes that you want to monitor.

Step 9 Click **Finish**.

The applications monitoring pane displays the information that you chose.

Additional Information

See the Related Topics, page 5-28.

Finding CTI Devices to Monitor

Perform the following procedure to find specific CTI devices to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click CallManager.
  - In the tree hierarchy, double-click **CTI**.
  - Click the CTI Search icon.
- Choose **CallManager > CTI > CTI Search > CTI Devices**. The selection window displays where you can enter the search criteria. Go to Step 2.

Tip If you right-click the option, choose **Monitor**.

Step 2 From the CTI Manager drop-down list box, choose the CTI Manager that you want to monitor.

Step 3 From the Devices Status drop-down list box, choose the device status.

Step 4 In the Devices pane, click the radio button that applies.

Tip If you chose **Device Name**, enter the device name in the field.

Step 5 Click **Next**.

Step 6 In the Application Pattern window, click the radio button that applies.

Step 7 Enter the information in the field for the radio button that you clicked; for example, if you clicked IP Subnet, enter the IP address and subnet mask in the field.

Tip If you enter the IPv6 address, the IP Subnet does not apply. IPv6 support does not apply to Cisco Unified Communications Manager Business Edition 5000.

Step 8 Click **Next**.

Step 9 In the Monitor following attributes window, check one or all check boxes for the attributes that you want to monitor.

Step 10 Click **Finish**.

The devices monitoring pane displays the information that you chose.

Additional Information

See the Related Topics, page 5-28.

Finding CTI Lines to Monitor

Perform the following procedure to find specific CTI lines to monitor.

Procedure

Step 1 Perform one of the following tasks:

- On the Quick Launch Channel
  - Click CallManager.
  - In the tree hierarchy, double-click **CTI**.
  - Click the CTI Search icon.
- Choose **CallManager > CTI > CTI Search > CTI Lines**. The selection window displays where you can enter the search criteria. Go to Step 2.

Tip If you right-click the option, choose **Monitor**.

Step 2 From the CTI Manager & Status drop-down list box, choose the CTI manager that you want to monitor.

Step 3 From the Lines Status drop-down list box, choose the status.

Step 4 In the Devices pane, click the radio button that applies.

Tip If you chose **Device Name**, enter the device name in the field.

Step 5 In the Lines pane, click the radio button that applies:

Note If you chose **Directory Number**, enter the directory number in the field.

Step 6 Click **Next**.

Step 7 In the Application Pattern pane, click the radio buttons apply:

Step 8 Enter the information in the field for the radio button that you clicked; for example, if you clicked IP Subnet, enter the IP address and subnet mask in the field.

Tip If you enter the IPv6 address, the IP Subnet does not apply. IPv6 support does not apply to Cisco Unified Communications Manager Business Edition 5000.

Step 9 Click **Next**.

Step 10 In the Monitor following attributes window, check one or all check boxes for the attributes that you want to monitor.

Step 11 Click **Finish**.

The lines monitoring pane displays the information that you chose.

Additional Information

See the Related Topics, page 5-28.

Viewing Application Information

You can view the application information for selected devices such as the Cisco Unified IP Phone, CTI port, and CTI route point. This section describes how to view application information.

Procedure

Step 1 Display the devices in the RTMT monitoring pane, as described in the "Finding CTI Devices to Monitor" section on page 5-22.

Step 2 Perform one of the following tasks:

- Right-click the device for which you want application information; for example, CTI; then, choose **App Info**.
- Click the device for which you want application information and choose **Device > App Info**.

The Application Information window displays the CTI manager server name, application ID, user ID, application IP address, application status, app time stamp, device time stamp, device name, and CTI device open status.

Step 3 To view updated information, click **Refresh**. To close the window, click **OK**.

Additional Information

See the Related Topics, page 5-28.

Reporting on Learned Patterns and SAF Forwarders for the Call Control Discovery Feature

Learned pattern reports and SAF forwarder reports support the call control discovery feature. When you configure the call control discovery feature, Cisco Unified Communications Manager advertises itself and its hosted DN patterns to other remote call-control entities that use the SAF network. Likewise, these remote call-control entities advertise their hosted DN patterns, which Cisco Unified Communications Manager can learn and insert in digit analysis. For more information on the call control discovery feature, refer to the "Call Control Discovery" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

Learned Pattern reports include such information as learned pattern name, time stamp, reachability status for the pattern, remote call-control entity that hosts the pattern, the PSTN failover configuration, and the destination IP address and port. RTMT allows you to search based on different criteria; for example, if you specify a search for the remote call-control entity, all the learned patterns display for the remote call-control entity.

SAF Forwarder reports display information such as authentication status, registration status of SAF forwarders, and so on.

To access the Learned Patterns or SAF Forwarders reports in RTMT, perform the following procedure:

Procedure

Step 1 To access the report, perform one of the following tasks:

- For Learned Patterns—From the RTMT menus, choose **CallManager > Report > Learned Pattern**. Or, Click the **CallManager** tab; then, click **Learned Pattern**.
- For SAF Forwarders—From the RTMT menus, choose **CallManager > Report > SAF Forwarders**. Or, click the **CallManager** tab; then, click **SAF Forwarders**.

Step 2 Choose the node from the Select a Node drop-down list box.

For learned pattern reports, if the Cisco CallManager service is running but the CCD requesting service is not running on that node, a message displays that the CCD Report Service is not working after you choose the node. If the CCD requesting service is not active on the node that you choose, the report displays as empty.

Step 3 Review the data in the report, as described in Table 5-5 (for learned patterns) or Table 5-6 (for SAF forwarders).

Be aware that the learned pattern may be repeated in the report because the learned pattern may be coming from a different source; for example, it may be coming from a different IP address.

Table 5-5 Data from Learned Pattern Report

Column	Description
Pattern	Displays the name of the learned pattern from the remote call-control entity.
TimeStamp	Displays the date and time that the local Cisco Unified Communications Manager marked the pattern as a learned pattern.
Status	Indicates whether the learned pattern was reachable or unreachable

Table 5-5 Data from Learned Pattern Report (continued)

Column	Description
Protocol	Displays the protocol for the SAF-enabled trunk that was used for the outgoing call to the learned pattern; if the remote call-control entity has QSIG tunneling configured for the SAF-enabled trunk, the data indicates that QSIG tunneling was used; for example, EMCA is listed along with H.323 in this column.
AgentID	Displays the name of the remote call-control entity that advertised the learned pattern
IP Address	Displays the IP address for the call control entity that advertised the learned pattern; Displays the port number that the call-control entity uses to listen for the call.
ToDID	Displays the PSTN failover configuration for the learned pattern.
CUCMNodeId	Displays the ID from the local Cisco Unified Communications Manager node.

Table 5-6 Data from SAF Forwarder Report

Column	Description
Name	Displays the name of the SAF forwarder that you configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration.
Description	Displays the description for the SAF forwarder that you configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration. If None displays, you did not enter a description for the SAF forwarder.
IP Address	Displays the IP address for the SAF forwarder, as configured in the SAF Forwarder Configuration window in Cisco Unified Communications Manager Administration.
Port	Indicates the port number that Cisco Unified Communications Manager uses to connect to the SAF forwarder; by default, Cisco Unified Communications Manager uses 5050.
Type	Indicates whether the SAF forwarder is classified as the primary or backup SAF forwarder.
Connection Status	Indicates whether Cisco Unified Communications Manager can connect to the SAF forwarder.

Table 5-6 Data from SAF Forwarder Report (continued)

Column	Description
Authentication Type	Indicates that Cisco Unified Communications Manager used digest authentication to connect to the SAF forwarder.
Registration Status	Indicates whether the Cisco Unified Communications Manager is registered to the SAF forwarder.
Time Last Registered	Displays the date and time when the Cisco Unified Communications Manager last registered with the SAF forwarder.
No of Registered Applications	Displays the total number of CCD advertising and requesting services that are registered to the SAF forwarder.
No of Connection Re-Attempts	Displays the number of times that the call-control entity, in this case, the Cisco Unified Communications Manager, has attempted to connect to the SAF forwarder.

Step 4 After the data displays, if you want to filter the results based on specific criteria, click the **Filter** button; specific the criteria that you want to search, click **Apply** and then **OK**.

Step 5 To display the most current results, click **Refresh**.

Step 6 If you want to search on a specific string in the data, click the **Find** button, enter the string, then, click **Find Next**.

Step 7 If you want to save the results, click **Save**, and choose either **XML** or **Text**, depending on how you want to save the results. Browse to the location where you want to save the data, name the file that you want to save; then, click **Save**.

Monitoring Intercompany Media Services

Tip 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, not the backend server time, provides the basis for the time stamp in each chart.

Tip To zoom in on the monitor of a predefined object, click and drag the left mouse button over the area of the chart that interests you. Release the left mouse button when you have the selected area. RTMT updates the monitored view. To zoom out and reset the monitor to the initial default view, press the "**R**" key.

The Intercompany Media Services monitoring category monitors the following items:

- Routing—Displays the total number of Cisco Intercompany Media Engine routes that Cisco Unified Communications Manager maintains. This total includes the following routes:
  - Learned routes that represent the phone numbers that the Cisco Intercompany Media Engine client learned and that exist in the Cisco Unified Communications Manager routing tables
  - Unique domains of peer enterprises for which Cisco Intercompany Media Engine routes exist
  - Published routes that represent the number of direct inward dialing numbers (DIDs) that were published successfully to the IME distributed hash table across all Cisco Intercompany Media Engine services
  - Rejected routes that represent the number of learned routes that got rejected because the administrator blocked them.

  These charts represent the following performance counters for the Cisco IME Client performance object: RoutesLearned, DomainsUnique, RoutesPublished, and RoutesRejected.

  To display information on routing, choose **CallManager > Cisco IME Client > Routing**.
- Call Activities—Allows you to monitor the total number of Cisco Intercompany Media Engine calls. This total includes the following types of calls:
  - Calls that were attempted (including calls that were accepted, busy, no answer, and failed)
  - Calls that were received
  - Calls that were set up (that is, made by Cisco Unified Communications Manager and accepted by the remote party)
  - Calls that were accepted (that is, received by Cisco Unified Communications Manager and answered by the called party)
  - Calls that completed fallback to the PSTN
  - Calls that did not successfully fallback to the PSTN.

  These charts represent the following performance counters for the Cisco IME Client performance object: CallsAttempted, CallAccepted, CallsReceived, CallsSetup, IMESetupsFailed, and FallbackCallsFailed.

  To display information on call activities, choose **CallManager > Cisco IME Client > Call Activities**.

Additional Information

See the Related Topics, page 5-28.

Where to Find More Information

Related Topics

- Predefined Cisco Unified Communications Manager Objects Overview, page 5-2
- Viewing the Cisco Unified Communications Manager Summary, page 5-5
- Monitoring Call-Processing Activity, page 5-6
- Understanding Call-Processing Logs, page 5-7
- Monitoring Services, page 5-13
- Understanding Service Logs, page 5-13

- Monitoring Devices, page 5-14
- Understanding Device Logs, page 5-16
- Working with Devices, page 5-17
- Monitoring CTI Applications, Devices, and Lines, page 5-20
- Working with CTI Applications, Devices, and Lines, page 5-21
- Reporting on Learned Patterns and SAF Forwarders for the Call Control Discovery Feature, page 5-25
- Understanding Alerts, page 9-1
- Working with Alerts, page 10-1
- Understanding Performance Monitoring, page 3-1
- Working with Performance Queries, page 6-1
- Viewing Perfmon Log Files, page 7-1
- Working with Trace and Log Central, page 11-1