



CHAPTER 9

Configuring Trace and Log Central in RTMT

The trace and log central feature in the Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT) allows you to configure on-demand trace collection for a specific date range or an absolute time. You can collect trace files that contain search criteria that you specify and save the trace collection criteria for later use, schedule one recurring trace collection and download the trace files to a SFTP or FTP server on your network, or collect a crash dump file. After you collect the files, you can view them in the appropriate viewer within the real-time monitoring tool. You can also view traces on the server without downloading the trace files by using the remote browse feature. You can open the trace files by either selecting the internal viewer that is provided with RTMT or choosing an appropriate program as an external viewer.



Note

From RTMT, you can also edit the trace setting for the traces on the server that you have specified. Enabling trace settings decreases system performance; therefore, enable Trace only for troubleshooting purposes.



Note

To use the trace and log central feature in the RTMT, make sure that RTMT can access the server directly without Network Access Translation (NAT). If you have set up a NAT to access devices, configure the Cisco Unified Communications Manager with a hostname instead of an IP address and make sure that the host names and their routable IP address are in the DNS server or host file.



Note

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

This chapter contains information on the following topics:

- [Importing Certificates, page 9-2](#)
- [Displaying Trace and Log Central Options in RTMT, page 9-2](#)
- [Collecting Trace Files, page 9-3](#)
- [Using the Query Wizard, page 9-5](#)
- [Scheduling Trace Collection, page 9-8](#)
- [Viewing Trace Collection Status and Deleting Scheduled Collections, page 9-11](#)
- [Collecting a Crash Dump, page 9-11](#)
- [Using Local Browse, page 9-13](#)
- [Using Remote Browse, page 9-14](#)

- [Using Q931 Translator, page 9-17](#)
- [Displaying QRT Report Information, page 9-18](#)
- [Using Real-Time Trace, page 9-19](#)
- [Updating the Trace Configuration Setting for RTMT, page 9-22](#)

Importing Certificates

You can import the server authentication certificate that the certificate authority provides for the server. Cisco recommends that you import the certificates before using 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 into RTMT and access the trace and log central option. You cannot change any data that displays for the certificate.

To import the certificate, choose **System > Tools > Trace > Import Certificate**.

A messages displays that states that the system completed the importing of server certificates. Click **OK**.

Additional Information

See the [Related Topics, page 9-22](#).

Displaying Trace and Log Central Options in RTMT

Before you begin, make sure that you have imported the security certificates as described in the [“Importing Certificates” section on page 9-2](#).

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

- In the Quick Launch Channel, click **System**; in the tree hierarchy, double-click **Tools**; then, click the **Trace & Log Central** icon.
- Choose **System > Tools > Trace > Trace & Log Central**.



Tip

From any option that displays in the tree hierarchy, you can specify the services/applications for which you want traces, specify the logs and servers that you want to use, schedule a collection time and date, configure the ability to download the files, configure zip files, and delete collected trace files.

After you display the Trace and Log Central options in the real-time monitoring tool, perform one of the following tasks:

- Collect traces for services, applications, and system logs on the server. See [“Collecting Trace Files” section on page 9-3](#)
- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use. See [“Using the Query Wizard” section on page 9-5](#)
- Schedule a recurring trace collection and download the trace files to a SFTP or FTP server on your network. See [“Scheduling Trace Collection” section on page 9-8](#)
- Collect a crash dump file for one or more servers on your network. See [“Collecting a Crash Dump” section on page 9-11](#).
- View the trace files that you have collected. See the [“Using Local Browse” section on page 9-13](#).

- View all of the trace files on the server. See the [“Using Remote Browse” section on page 9-14](#).
- View the current trace file being written on the server for each application. You can perform a specified action when a search string appears in the trace file. See [“Using Real-Time Trace” section on page 9-19](#).

Additional Information

See the [Related Topics, page 9-22](#).

Collecting Trace Files

Use the Collect Files option in Trace and Log Central to collect traces for services, applications, and system logs on the server. You specify date/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 collect traces by using the trace and log central feature.



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

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, see the [“Using the Query Wizard” section on page 9-5](#).

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window in Cisco Unified Serviceability. For more information, refer to *Cisco Unified Serviceability Administration Guide*.
- 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 in Cisco Unified Serviceability. For more information, refer to *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Display the Trace and Log Central options, as described in the [“Displaying Trace and Log Central Options in RTMT” section on page 9-2](#).

Step 2 In the Trace & Log Central tree hierarchy, double-click **Collect Files**.

The Trace Collection wizard displays.



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

Step 3 In the Select CCM Services/Applications tab, perform one of the following tasks:

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.

- To continue the trace collection wizard without collecting traces for services or applications, go to [Step 4](#).

Step 4 Click **Next**.

Step 5 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the trace collection wizard without collecting traces for system logs, go to [Step 6](#).

Step 6 Click **Next**.

Step 7 In the Select System Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the trace collection wizard without collecting traces for system logs, go to [Step 8](#).

Step 8 Click **Next**.

Step 9 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Trace and Log Central downloads the file with a time range that is based on your Selected Reference Server Time Zone field.

To set the date range for which you want to collect traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.

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

In the Download File option group box, specify the options you want for downloading traces.

Step 10 From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

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.

So, when you upgrade from one version of Cisco Unified Communications Manager Business Edition that is running on the Linux platform to another version and you restart the server with the new version Cisco Unified Communications Manager Business Edition, Cisco Unified Serviceability moves the logs from 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 of Cisco Unified Communications Manager Business Edition, Cisco Unified Serviceability moves the logs for the newer version of Cisco Unified Communications Manager Business Edition to the inactive partition and stores the logs for the older version in the active directory.

- Step 11** To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
- Step 12** To create a zip file of the trace files that you collect, choose the **Zip File** radio button. To download the trace files without zipping the files, choose the **Do Not Zip Files** radio button.
- Step 13** To delete collected log files from the server, check the **Delete Collected Log Files from the server** check box.
- Step 14** Click **Finish**.
- The window shows the progress of the trace collection. If you want to stop the trace collection, click **Cancel**.
- When the trace collection process is complete, the message “Completed downloading for node <Server name or IP address>” displays at the bottom of the window.
- Step 15** To view the trace files that you collected, you can use the Local Browse option of the trace collection feature. For more information, see the [“Using Local Browse” section on page 9-13](#).

Additional Information

See the [Related Topics, page 9-22](#).

Using the Query Wizard

The Trace Collection Query Wizard allows you to collect and download trace files that contain search criteria that you specify as well as to save 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 and Log Central. This includes using the Query Wizard, Local Browse, and Remote Browse features.

Before You Begin

Perform one or more of the following tasks:

- From the Trace Configuration window in Cisco Unified Serviceability, configure the information that you want to include in the trace files for the various services. For more information, refer to *Cisco Unified Serviceability Administration Guide*.
- 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. For more information, refer to *Cisco Unified Serviceability Administration Guide*.

Procedure

- Step 1** Display the Trace and Log Central options, as described in the [“Displaying Trace and Log Central Options in RTMT” section on page 9-2](#).
- Step 2** In the Trace & Log Central tree hierarchy, double-click **Query Wizard**.
- The Query wizard displays.

Step 3 In the Query Wizard Options window, click one of the following radio buttons:

- Saved Query

Click the **Browse** button to navigate to the query that you want to use. Choose the query and click **Open**.

To run the query without any modifications, click **Run Query** and go to [Step 20](#). To modify the query, go to [Step 4](#).

- Create Query

Step 4 Click **Next**.

Step 5 If you clicked the Saved Query radio button and chose a query, the criteria that you specified for query display. If necessary, modify the list of services/applications for which you want to collect traces. If you clicked the Create Query radio button, you must choose all services/applications for which you want to collect traces.



Tip

To collect traces for all services and applications on a particular server, check the check box next to the server name or server IP address.



Note

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

Step 6 In the Select CCM Services/Applications tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 7 Click **Next**.

Step 8 In the Select CUC Services/Application tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 9 Click **Next**.

Step 10 In the Select System Services/Application tab, choose the services and application logs in which you are interested by checking all check boxes that apply.

Step 11 Click **Next**.

Step 12 In the Query Time Options box, 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 service(s) that you chose.
- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field.

To set the date range for which you want to collect traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.

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

- Step 13** To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box.
- Step 14** In the Call Procession Impact Options box, specify From the level of impact you want the string search activity to have on call processing. From the Select Impact Level drop down box, select Low, Medium, or High. Low impact causes the least impact on call processing but yields slower results. High impact causes the most impact on call processing but yields faster results.

- Step 15** Choose one of the following options:

- To execute the query, click **Run Query**.

The Query Results folder displays. When the query completes, a dialog box that indicates that the query execution completed displays. Click **OK** and continue with [Step 20](#).

- To save the query, click the **Save Query** button and continue with [Step 16](#).

- Step 16** Check the check box next to the type of query that you want to create.

- **Generic Query**—Choose this option if you want to create a query that you can run on servers other than the one on which it was created. You can only create a generic query if the services that you chose exist on that server.

Then, choose either the Single Node Query or All Node Query option. If you choose the Single Node Query, the trace collection tool by default chooses the server on which you created the query when you execute the query. If you choose the All Node Query option, the trace collection tool chooses the server on which you created the query when you executed the query.



Note You can choose servers other than the default before running the query.

- **Regular Query**—Choose this option if you only want to run the query on the server on which you created the query.

- Step 17** Click **Finish**.

- Step 18** Browse to the location to store the query, enter a name for the query in the File Name field, and click **Save**.

- Step 19** Do one of the following tasks:

- To run the query that you have just saved, click **Run Query** and continue with [Step 20](#).
- To exit the query wizard without running the query that you created, click **Cancel**.

- Step 20** After the query execution completes, perform one or more of the following tasks:

- To view a file that you collected, navigate to the file by double-clicking Query Results, double-clicking the <node> folder, where <node> equals the IP address or host name for the server that you specified in the wizard, and double-clicking the folder that contains the file that you want to view.

After you have located the file, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer. The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer.

**Note**

If your file contains Q931 messages, go to [“Using Q931 Translator” section on page 9-17](#) to view the Q931 messages. To view reports that the QRT Quality Report Tool (QRT) generates, see the [“Displaying QRT Report Information” section on page 9-18](#).

- Download the trace files and the result file that contains a list of the trace files that your query collected by choosing the files that you want to download, clicking the **Download** button, specifying the criteria for the download, and clicking **Finish**.
 - To specify the directory in which you want to download the trace files and the results file, click the **Browse** button next to the Download all files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
 - To create a zip file of the trace files that you collect, check the **Zip File** check box.
 - To delete collected log files from the server, check the **Delete Collected Log Files from Server** check box.

**Tip**

After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the [“Using Local Browse” section on page 9-13](#).

- To save the query, click **Save Query** button and complete [Step 16](#) through [Step 18](#).

Additional Information

See the [Related Topics, page 9-22](#).

Scheduling Trace Collection

You can use the Schedule Collection option of the trace and log central feature to schedule up to six concurrent trace collections and to download the trace files to a 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 10 trace collection jobs, but only six trace collection can be concurrent. That is, only six jobs can be in a running state at the same time.

Before You Begin

Perform one or more of the following tasks:

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window of Cisco Unified Serviceability. For more information, refer to the *Cisco Unified Serviceability Administration Guide*.
- 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. For more information, refer to the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Display the Trace and Log Central options, as described in the [“Displaying Trace and Log Central Options in RTMT”](#) section on page 9-2.

Step 2 In the Trace & Log Central tree hierarchy, double-click **Schedule Collection**.
The Schedule Collection wizard displays.



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

Step 3 In the Select CCM Services/Applications tab, perform one of the following tasks:

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the schedule collection wizard without collecting traces for services or applications, go to [Step 4](#).

Step 4 Click **Next**.

Step 5 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the schedule collection wizard without collecting traces for system logs, go to [Step 6](#).

Step 6 Click **Next**.

Step 7 In the Select System Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the schedule collection wizard without collecting traces for system logs, go to [Step 8](#).

Step 8 Click **Next**.

Step 9 Specify the server time zone and the time range for which you want to collect traces.
The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Step 10 To specify the date and time that you want to start the trace collection, click the down arrow button next to the Schedule Start Date/Time field. From the Date tab, choose the appropriate date. From the Time tab, choose the appropriate time.

Step 11 To specify the date and time that you want to end the trace collection, click the down arrow button next to the Schedule End Date/Time field. From the Date tab, choose the appropriate date. From the Time tab, choose the appropriate time.

**Note**

The trace collection completes, even if the collection goes beyond the configured end time; however, the trace and log central feature deletes this collection from the schedule.

- Step 12** From the Scheduler Frequency drop-down list box, choose how often you want to run the configured trace collection.
- Step 13** From the Collect Files generated in the last drop-down list boxes, specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.
- Step 14** To search by phrases or words that exist in the trace file, enter the word or phrase in the Search String field. The tool searches for a match to the word or phrase that you enter and collects those files that match the search criteria. If you want to search for an exact match to the word or phrase that you entered, check the Case Sensitive check box
- Step 15** To create a zip file of the trace files that you collect, check the **Zip File** check box.
- Step 16** To delete collected log files from the server, check the **Delete Collected Log Files from the Server** check box.
- Step 17** Choose one or more of the following actions:
- Download Files. If you chose Download Files or Run Another Query, continue with [Step 18](#).
 - Run Another Query
 - Generate Syslog. If you chose Generate Syslog, go to [Step 20](#).
- Step 18** In the SFTP/FTP Server Parameters group box, enter the server credentials for the server where the trace and log central feature downloads the results and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP or FTP server, click **OK**.

**Note**

The **Download Directory Path** field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP or FTP parameters fields:
/home/<user>/Trace.

- Step 19** If you chose the Run Another Query Option, click the **Browse** button to locate the query that you want to run, and click **OK**.

**Note**

The trace and log central feature only executes the specified query if the first query generates results.

- Step 20** Click **Finish**.
A message indicates that the system added the scheduled trace successfully.

**Note**

If the real-time monitoring tool cannot access the SFTP or FTP server, a message displays. Verify that you entered the correct IP address, user name, and password

- Step 21** Click **OK**.
- Step 22** To view a list of scheduled collections, click the Job Status icon in the Trace & Log Central tree hierarchy in the Quick Launch Channel.

**Tip**

To delete a scheduled collection, choose the collection event and click **Delete**. A confirmation message displays. Click **OK**.

Additional Information

See the [Related Topics, page 9-22](#).

Viewing Trace Collection Status and Deleting Scheduled Collections

To view trace collection event status and to delete scheduled trace collections, use the following procedure:

Procedure

- Step 1** Display the Trace & Log Central tree hierarchy, as described in [“Displaying Trace and Log Central Options in RTMT” section on page 9-2](#).
- Step 2** Double-click **Job Status**.
The Job Status Window displays.
- Step 3** From the Select a Node drop-down list box, choose the server for which you want to view or delete trace collection events.

This list of scheduled trace collections displays.

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 jobs with a status of “Pending” or “Running” and a job type of “Schedule Task” or job type of “RealTimeFileSearch.”

Additional Information

See the [Related Topics, page 9-22](#).

Collecting a Crash Dump

Perform the following procedure to collect a core dump of trace files:

Procedure

Step 1 Display the Trace & Log Central tree hierarchy, as described in [“Displaying Trace and Log Central Options in RTMT” section on page 9-2](#).

Step 2 Double-click **Collect Crash Dump**.

The Collect Crash Dump wizard displays.



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

Step 3 In the Select CCM Services/Applications tab, perform one of the following tasks:

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the collect crash dump wizard without collecting traces for services or applications, go to [Step 4](#).

Step 4 Click **Next**.

Step 5 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the collect crash dump wizard without collecting traces for system logs, go to [Step 6](#).

Step 6 Click **Next**.

Step 7 In the Select System Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the collect crash dump wizard without collecting traces for system logs, go to [Step 8](#).

Step 8 Click **Next**.

Step 9 In the Collection Time group box, specify the time range for which you want to collect traces. Choose one of the following options:

- **Absolute Range**—Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Trace Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field.

To set the date range for which you want to collect crash files, choose the drop-down list box in the From Date/Time and To Date/Time fields.

- **Relative Range**—Specify the amount of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect crash files.

Step 10 From the Select Partition drop-down list box, choose the partition that contains the logs for which you want to collect traces.

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.

So, when you upgrade from one version of Cisco Unified Communications Manager Business Edition 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 from 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 of Cisco Unified Communications Manager Business Edition, Cisco Unified Serviceability moves the logs for the newer version of Cisco Unified Communications Manager Business Edition to the inactive partition and stores the logs for the older version in the active directory.

Step 11 To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.

Step 12 To create a zip file of the crash dump files that you collect, choose the **Zip File** radio button. To download the crash dump files without zipping the files, choose the **Do Not Zip Files** radio button.



Note You cannot download a zipped crash dump file that exceeds 2 gigabytes.

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

Step 14 Click **Finish**.

A message displays that states that you want to collect core dumps. To continue, click **Yes**.



Note If you chose the **Zip File** 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 with the **Zip File** radio button selected. Choose the **Do Not Zip Files** radio button, and try the collection again.

Additional Information

See the [Related Topics](#), page 9-22.

Using Local Browse

After you have collected trace files and downloaded 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 the real-time monitoring tool.

**Note**

Do not use NotePad to view collected trace files.

Perform the following procedure to display the log files that you have collected with the trace and log central feature. If you zipped the trace files when you downloaded them to your PC, you will need to unzip them to view them by using the viewers within the real-time monitoring tool.

**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 traces files as described in one of the following sections:

- “Collecting Trace Files” section on page 9-3
- “Using the Query Wizard” section on page 9-5
- “Scheduling Trace Collection” section on page 9-8

Procedure

- Step 1** Display the Trace and Log Central options, as described in the “[Displaying Trace and Log Central Options in RTMT](#)” section on page 9-2.
- Step 2** Double-click **Local Browse**.
- Step 3** Browse to the directory where you stored the log file and choose the file that you want to view.
- Step 4** To display the results, double-click the file.
- Step 5** Click the program (viewer) that you would like to use to view the file. If the program is not on the list, choose another program by clicking the **Other** button.

If you want to use this program as your default viewer, click the **Always use this program to open these files** check box

The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer. For more information on using the QRT Viewer, see the “[Displaying QRT Report Information](#)” section on page 9-18. For more information on the QRT Translator, see the “[Using Q931 Translator](#)” section on page 9-17.

Additional Information

See the [Related Topics](#), page 9-22.

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 the trace and log central feature.

**Note**

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

Before You Begin

Collect traces files as described in one of the following sections:

- “Collecting Trace Files” section on page 9-3
- “Using the Query Wizard” section on page 9-5
- “Scheduling Trace Collection” section on page 9-8

Procedure

Step 1 Display the Trace and Log Central options, as described in the “[Displaying Trace and Log Central Options in RTMT](#)” section on page 9-2.

Step 2 Double-click **Remote Browse**.

Step 3 Choose the appropriate radio button, and click **Next**. If you choose Trace Files, go to [Step 4](#). If you choose Crash Dump, go to [Step 14](#).

**Note**

The services that you have not activated also display, so you can choose traces for those services.

**Note**

If you choose Crash Dump, the wizard only displays 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 In the Select CCM Services/Applications tab, perform one of the following tasks:

- To collect traces for all services and applications for all servers, check the **Select All Services on All Servers** check box.
- To collect traces for all services and applications on a particular server, check the check box next to the server.
- To collect traces for particular services or applications on particular servers, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting traces for services or applications, go to [Step 5](#).

Step 5 Click **Next**.

Step 6 In the Select CUC Services/Application tab, perform one of the following tasks:

- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
- To collect traces for all system logs on a particular server, check the check box next to the server.
- To collect traces for particular system logs on particular servers, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting traces for system logs, go to [Step 7](#).

Step 7 Click **Next**.

- Step 8** In the Select System Services/Application tab, perform one of the following tasks:
- To collect all system logs for all servers, check the **Select All Services on all Servers** check box.
 - To collect traces for all system logs on a particular server, check the check box next to the server.
 - To collect traces for particular system logs on particular servers, check the check boxes that apply.
 - To continue the Remote Browse wizard without collecting traces for system logs, go to [Step 14](#).
- Step 9** In the Select CCM Services/Applications tab, perform one of the following tasks:
- To choose crash dump files for all services and applications for all servers, check the **Select All Services on All Servers** check box.
 - To choose crash dump files for all services and applications on a particular server, check the check box next to the server.
 - To choose crash dump files for particular services or applications on particular servers, check the check boxes that apply.
 - To continue the Remote Browse wizard without collecting crash dump files, go to [Step 10](#).
- Step 10** Click **Next**.
- Step 11** In the Select CUC Services/Application tab, perform one of the following tasks:
- To choose crash dump files for all servers, check the **Select All Services on all Servers** check box.
 - To choose crash dump files on a particular server, check the check box next to the server.
 - To choose crash dump files for particular system logs on particular servers, check the check boxes that apply.
 - To continue the Remote Browse wizard without collecting crash dump files, go to [Step 12](#).
- Step 12** Click **Next**.
- Step 13** In the Select System Services/Application tab, perform one of the following tasks:
- To choose crash dump files for all servers, check the **Select All Services on all Servers** check box.
 - To choose crash dump files for all system logs on a particular server, check the check box next to the server.
 - To choose crash dump files for particular system logs on particular servers, check the check boxes that apply.
 - To continue the Remote Browse wizard without collecting crash dump files, go to [Step 14](#).
- Step 14** Click **Finish**.
- Step 15** After the traces become available, a message displays. Click **Close**.
- Step 16** Perform one of the following tasks:
- To display the results, navigate to the file through the tree hierarchy. After the log file name displays in the pane on the right side of the window, you can either right-click the mouse to select the type of program that you would like to use to view the file or double-click the file to display the file in the default viewer.

**Tip**

To sort the files that displays in the pane, click a column header; for example, to sort the files by name, click the Name column header.

The real-time monitoring tool displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, the real-time monitoring tool opens files in the Generic Log Viewer. For more information on using the QRT Viewer, see the [“Displaying QRT Report Information” section on page 9-18](#). For more information on the QRT Translator, see the [“Using Q931 Translator” section on page 9-17](#).

- To download the trace files, choose the files that you want to download, click **Download**, specify the criteria for the download, and click **Finish**.
 - To specify the directory in which you want to download the trace files, click the **Browse** button next to the Download all files field, navigate to the directory, and click **Open**. The default specifies <rtmt_install_directory>\<server name or server IP address>\<download time> where <rtmt_install_directory> specifies the directory where RTMT is installed.
 - To create a zip file of the trace files that you collect, check the **Zip File** check box.
 - To delete collected log files from the server, check the **Delete Files on server** check box.
- To delete trace files from the server, click the file that displays in the pane on the right side of the window; then, click the **Delete** button.
- To refresh a specific service, click the server name or service; then, click the **Refresh** button. After a message states that the remote browse is ready, click **Close**.
- To refresh all services and nodes that display in the tree hierarchy, click the **Refresh All** button. After a message states that the remote browse is ready, click **Close**.

**Tip**

After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature. For more information, see the [“Using Local Browse” section on page 9-13](#).

Additional Information

See the [Related Topics, page 9-22](#).

Using Q931 Translator

Cisco Unified Communications Manager generates ISDN trace files, which can help you diagnose and troubleshoot connectivity problems in Cisco Unified Communications Manager installations. The log files contain Q.931 type messages (ISDN Layer 3 protocol).

The message translation feature works by filtering incoming data from Cisco Unified Communications Manager system diagnostic interface (SDI) log files, then parsing and translating them into Cisco IOS-equivalent messages. Message translator supports XML and text files.

Using the message translator tool, Cisco Support Engineers translate your incoming debugging information into familiar Cisco IOS-equivalent messages.

Before You Begin

Collect traces files as described in one of the following sections:

- [“Collecting Trace Files” section on page 9-3](#)
- [“Using the Query Wizard” section on page 9-5](#)

- [“Scheduling Trace Collection” section on page 9-8](#)

Procedure

- Step 1** Display the log file entries by using the Query Wizard as described in the [“Using the Query Wizard” section on page 9-5](#) or by using the Local Browse option in the trace and log central feature as described in the [“Using Local Browse” section on page 9-13](#).



Note CTIManager and Cisco Unified Communications Manager SDI trace files may contain Q931 messages.

- Step 2** Click the log entry for which you want the Q931 message translation.

- Step 3** Click **Translate Q931 Messages**.

If the trace file that you chose does not have any ISDN messages in it, the message, No ISDN Messages in the File, displays.

If the trace file that you chose does have ISDN messages in it, the Q931 Translator dialog box contains a list of the messages.

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

- To view the details of a particular message, choose that message from the list. The details display in the Detailed Message group box.
- To filter the results, choose a Q931 message from the list, choose an option from the drop-down list box (such as filter by gateway), and/or enter text in the Filter by Search String field. To remove the filters, click Clear Filter. All logs display after you clear the filter.
- To close the Q931 Translator dialog box, click the **Close** button.

Additional Information

See the [Related Topics, page 9-22](#).

Displaying QRT Report Information

You can view the IP phone problem reports that the Quality Report Tool (QRT) generates by using the QRT viewer. QRT serves as a voice-quality and general problem-reporting tool for Cisco Unified IP Phones. After you collect the QRT log files, you can use the following procedure to list and view Cisco Unified Communications Manager IP Phone problem reports by using the QRT viewer. The QRT viewer allows you to filter, format, and view phone problem reports that are generated. For detailed information about how to configure and use QRT, refer to the *Cisco Unified Communications Manager Features and Services Guide*.

Before You Begin

You can view the QRT log files by either viewing the files on the server or by downloading the files onto your computer.

Collect or View the QRT log files as described in one of the following sections:

- [“Collecting Trace Files” section on page 9-3](#)

- [“Using the Query Wizard” section on page 9-5](#)
- [“Scheduling Trace Collection” section on page 9-8](#)
- [“Using Remote Browse” section on page 9-14](#)

After you download the files onto your computer, you can use the Local Browse option in the trace and log central feature as described in the [“Using Local Browse” section on page 9-13](#).

Procedure

Step 1 Display the log file entries by using the Query Wizard, the Remote Browse or the Local Browse option in trace and log central.

The QRT Viewer window displays.



Note Only log files from the Cisco Extended Functions service contain QRT information. The following format for the log file name that contains QRT data applies: qrtXXX.xml.

Step 2 From the Extension drop-down list box, choose the extension(s) that you want the report to include.

Step 3 From the Device drop-down list box, choose the device(s) that you want the report to include.

Step 4 From the Category drop-down list box, choose the problem category that you want the report to include.

Step 5 From the Select Fields drop-down list box, choose the fields that you want the report to include.



Note The order in which you choose the fields determines the order in which they appear in the QRT Report Result pane.

Step 6 To view the report in the QRT Report Result pane, click **Display Records**.

Using Real-Time Trace

The real-time trace option of the trace and log central feature in the RTMT 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 following options:

- [View Real-Time Data, page 9-19](#)
- [Monitor User Event, page 9-20](#)

View Real-Time Data

The view real-time data option of the trace and log central feature allows you to view a trace file as the system writes data to that file. You can view real-time trace data in the generic log viewer for up to 10 services, with a limit of 3 concurrent sessions on a single server. The log viewer refreshes every 5 seconds. As the traces get rolled into a new file, the generic log viewer appends the content in the viewer.

**Note**

Depending on the frequency of the traces that a service writes, the View Real Time Data option may experience a delay before being able to display the data in the generic log viewer.

Procedure

- Step 1** Display the Trace & Log Central tree hierarchy, as described in [“Displaying Trace and Log Central Options in RTMT” section on page 9-2](#).
- Step 2** Double-click **Real Time Trace**.
- Step 3** Double-click **View Real Time Data**.
The View Real Time Data wizard displays.
- Step 4** From the **Nodes** drop-down list box, choose the server for which you want to view real-time data and click **Next**.
- Step 5** Choose the product, service, and the trace file type for which you want to view real-time data and click **Finish**.

**Note**

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

The real-time data for the chosen service displays in the generic log viewer.

- Step 6** Check the **Show New Data** check box to keep the cursor at the end of the window to display new traces as they appear. Uncheck the **Show New Data** check box if you do not want the cursor to move to the bottom of the window as new traces display.
- Step 7** Repeat this procedure to view data for additional services. You can view data for 5 services. A message displays if you attempt to view data for too many services or too many services on a single node.
- Step 8** When you are done viewing the real-time data, click **Close** on the generic log viewer.

**Tip**

To search by phrases or words in the Log Viewer, enter the word or phrase in the Search String field. If you want to do a case sensitive search for a word or phrase, check the Match Case check box.

Additional Information

See the [Related Topics, page 9-22](#).



Monitor User Event

The monitor user event option of the trace and log central feature monitors real-time trace files and performs a specified action when a search string appears in the trace file. The system polls the trace file every 5 seconds. If the search string occurs more than once in one polling interval, the system only performs the action once. You can monitor one service for each event.

Before you Begin

If you want to generate an alarm when the specified search string exists in a monitored trace file, enable the LogFileSearchStringFound alert. For more information on enabling alerts, see the [“Setting Alert Properties” section on page 7-2](#).

Procedure

-
- Step 1** Display the Trace & Log Central tree hierarchy, as described in [“Displaying Trace and Log Central Options in RTMT” section on page 9-2](#).
- Step 2** Double-click **Real Time Trace**.
- Step 3** Double-click **Monitor User Event**.
The Monitor User Event wizard displays.
- Step 4** Perform one of the following tasks:
- To view the monitoring events that you have already set up, choose the **View Configured Events** radio button, choose a server from the drop-down list box, and click **Finish**.
The events configured for the server that you choose display.
-  **Note** To delete an event, choose the event and click **Delete**.
-
- To configure new monitoring events, choose the **Create Events** radio button, click **Next**, and continue with [Step 5](#).
- Step 5** Choose the server that you want the system to monitor from the **Nodes** drop-down list box and click **Next**.
- Step 6** Choose the product, service, and the trace file type that you want the system to monitor and click **Next**.
-  **Note** The services that you have not activated also display, so you can collect traces for those services.
-
- Step 7** In the **Search String** field, specify the phrases or words that you want the system to locate in the trace files. The tool searches for an exact match to the word or phrase that you enter.
- Step 8** Specify the server time zone and the time range (start and end date and time) for which you want the system to monitor trace files.

The time zone of the client machine provides the default setting for the Select Reference Server Time Zone field. All the standard time zones, along with a separate set of entries for all time zones that have Daylight Saving settings, display in the Select Time Zone drop-down list box.

Trace and Log Central downloads the files with a time range that is based on your Selected Reference Server Time Zone field.

To set the date range for which you want to monitor traces, choose the drop-down list box in the From Date/Time and To Date/Time fields.
- Step 9** Choose one or more of the following actions that you want the system to perform when it encounters the search string that you specified in the Search String field:
- Alert—Choose this option to generate an alarm when the system encounters the specified search string. For the system to generate the alarm, you must enable the enable the LogFileSearchStringFound alert. For more information on enabling alerts, see the [“Setting Alert Properties” section on page 7-2](#).

- **Local Syslog**—Choose this option if you want the system to log the errors in the application logs area in the SysLog Viewer. The system provides a description of the alarm and a recommended action. You can access the SysLog Viewer from RTMT.
- **Remote Syslog**—Choose this option to enable the system to store the syslog messages on a syslog server. In the **Server Name** field, specify the syslog server name.
- **Download File**—Choose this option to download the trace files that contain the specified search string. In the SFTP/FTP Server Parameters group box, choose either FTP or SFTP, enter the server credentials for the server where you want to download the trace files, and click **Test Connection**. After the trace and log central feature verifies the connection to the SFTP or FTP server, click **OK**.

**Note**

The Download Directory Path field specifies the directory in which the trace and log central feature stores collected files. By default, the trace collection stores the files in the home directory of the user whose user ID you specify in the SFTP/FTP parameters fields: /home/<user>/Trace.

**Note**

The system polls the trace files every 5 seconds and performs the specified actions when it encounters the search string. If more than one occurrence of the search string occurs in a polling interval, the system performs the action only once.

Step 10 Click **Finish**.

Additional Information

See the [Related Topics](#), page 9-22.

Updating the Trace Configuration Setting for RTMT

To edit trace settings for the Real-Time Monitoring plug-in, choose **Edit > Trace Settings**; then, click the radio button that applies. The system stores the rtmt.log file in the logs directory where you installed the RTMT plug-in; for example, C:\Program Files\Cisco\Unified Serviceability\jrtmt\log.

**Tip**

The Error radio button equals the default setting.

Additional Information

See the [Related Topics](#), page 9-22.

Related Topics

- [Using the Query Wizard](#), page 9-5
- [Using Local Browse](#), page 9-13
- [Collecting Trace Files](#), page 9-3
- [Scheduling Trace Collection](#), page 9-8
- [Displaying Trace and Log Central Options in RTMT](#), page 9-2

- [Collecting a Crash Dump, page 9-11](#)
- [Using Local Browse, page 9-13](#)
- *Cisco Unified Serviceability Administration Guide*

