Traces and Logs

Trace and Log Central

Note For Trace and Log Central to work, you must resolve DNS lookup for all nodes in the cluster on the client machine.

Preparation

Import Certificates

Follow this procedure to import the node certificates.

You can import the server authentication certificate that the certificate authority provides for the node or for each node in the cluster.

We recommend 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 nodes each time that you sign in to Unified RTMT and access the Trace and Log Central option. You cannot change any data that displays for the certificate.

Procedure

Step 1 To import the certificate, choose **Tools** > **Trace** > **Import Certificate**.

A messages appears that states that the system imported the node certificates.

Step 2 Click **OK**.

Types of trace support

This section describes the types of trace support.

Trace and Log Central disk IO and CPU throttling

Unified RTMT supports the throttling of critical Trace and Log Central operations and jobs, whether they are running on demand, scheduled, or automatic.

When you make a request for an on-demand operation when the node is running under high IO conditions, the system displays a warning that gives you the opportunity to cancel the operation. Be aware that the IO rate threshold values that control when the warning displays are configurable with the following service parameters (Cisco RIS Data Collector service):

- TLC Throttling CPU Goal
- TLC Throttling IOWait Goal

The values of these parameters are compared to the actual system CPU and IOWait values. If the goal (the value of the service parameter) is lower than the actual value, the system displays the warning.

View Trace and Log Central Options

Follow this procedure to view Trace and Log Central options in Unified RTMT.

Note From any option that displays in the tree hierarchy, you can specify the services and 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.

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

Before you begin

Before you begin, import the security certificates.

Procedure

Step 1 Perform one of the following actions to access Trace and Log Central:

a) Select **System** in the Quick Launch Channel**.**
b) Select **System** > **Tools** > **Trace** > **Trace & Log Central**.
c) Select the **Trace & Log Central** icon in the tree hierarchy.

Step 2 Perform one of the following tasks after you display the Trace and Log Central options in the Real-Time Monitoring Tool:

- Collect traces for services, applications, and system logs on one or more servers in the cluster.

- Collect and download trace files that contain search criteria that you specify as well as save trace collection criteria for later use.
- Collect a crash dump file for one or more servers on your network.
- View the trace files that you have collected.
- View all of the trace files on the server.
- 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.

Collect files

Collect Trace Files

Use the Collect Files option in Trace and Log Central to collect traces for services, applications, and system logs on one or more nodes in the cluster. You specify date and time range for which you want to collect traces, the directory in which to download the trace files and whether to delete the collected files from the node.

Follow this procedure to collect traces using the trace and log central feature.

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

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

Before you begin

Perform one or more of the following actions:

- 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, see 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 in Cisco Unified Serviceability. For more information, see the *Cisco Unified Serviceability Administration Guide*.
- Configure the throttling of critical Trace and Log Central operations and jobs by setting the values of the TLC Throttling CPU Goal and TLC Throttling IOWait Goal service parameters (Cisco RIS Data Collector service). For more information on configuring service parameters, see the *System Configuration Guide for Cisco Unified Communications Manager* .

Procedure

Step 1 Open the Trace and Log Central options.

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

The Trace Collection wizard appears. The services that you have not activated also appear, so you can collect traces for those services.

Note Unified Communications Manager and Cisco Unity Connection clusters: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Unified Communications Manager and Cisco Unity Connection clusters: You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the node on which you have activated the service/application.

Step 3 *Cisco Unity Connection* users go to Step 4. For Unified Communations Manager or Cisco Business Edition, perform one of the following actions in the **Select CCM Services/Application** tab:

a) To collect traces for all services and applications for all nodes in a cluster, check the **Select All Services on All Servers** check box and click **Next**.

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone node.

b) To collect traces for all services and applications on a particular node (or for particular system logs on the node for *Cisco Unity Connection*), check the check box next to the node and click **Next**.
c) To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
d) To go to the next tab without collecting traces for services or applications, click **Next**.

Go to Step 4 for Cisco Business Edition or go to Step 5 for Unified Communications Manager.

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

a) To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
b) To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.
c) To go to the next tab without collecting traces for system logs, click **Next**.

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

a) To collect all system logs for all nodes in a cluster, check the **Select All Services on all Servers** check box and click **Next**.

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for your standalone node.

b) To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
c) To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the trace collection wizard without collecting traces for system logs, click **Next**.

Step 6 In the Collection Time pane, specify the time range for which you want to collect traces. Choose one of the following options:

a) **Absolute Range**: Specify the node 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, appear 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. If you have nodes in a cluster in a different time zone, TLC will adjust for the time change and get files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second node (node x) that is in a time zone that is one hour ahead, TLC will download files from 10:00 a.m. to 11:00 a.m. from node x.

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.

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

Note Unified RTMT returns logs of a different time stamp, than that configured through the wizard. This occurs specifically, when the specified time stamp is lesser than that of the existing log files.

Log files exist on the node for a specific service from 11/24/09, and you have given the time range from 11/23/09 5:50 to 11/23/09 7:50; Unified RTMT still returns the existing log files.

Step 7 In the **Download File** option group box, specify the options that you want for downloading traces. 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.

This means that when you upgrade from one version of Unified Communications Manager, Cisco Business Edition 5000, or Cisco Unity Connection that is running on an appliance node to another version, and you restart the node with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log back in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified Communications Manager or Cisco Unity Connection versions that ran on the Windows platform.

Step 8 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_users_directory>\<server name or server IP address>\<download time>`.

Step 9 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 10 To delete collected log files from the node, check the **Delete Collected Log Files from the server** check box.

Step 11 Click **Finish** or, to abort the settings, click **Cancel**.

If you clicked Finish, the window shows the progress of the trace collection.

When the trace collection process is complete, the message “Completed downloading for node <Server name or IP address>” appears at the bottom of the window.

Step 12 To view the trace files that you collected, you can use the Local Browse option of the trace collection feature.

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

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 procedures to start a query and execute a query.

Before You Begin

- Configure the information that you want to include in the trace files for the various services from the **Trace Configuration** window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the **Alarm Configuration** window.

Start a Query

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Query Wizard** in the tree hierarchy.

Step 3 Perform one of the following actions:

If you want to:	Action	Result
Run a Saved Query	• Select **Saved Query**. • Select **Browse** to navigate to the query that you want to use. • Select the query and select **Open**.	• If you chose a single node generic query, the node to which RTMT is connected displays with a checkmark next to **Browse**. You can run the query on additional nodes by placing a checkmark next to those servers. • If you chose an all node generic query, all nodes display with a checkmark next to **Browse**. You can uncheck any server for which you do not want to run the query. • If you chose a regular query, all of the nodes that you selected when you saved the query display with a checkmark. You can check or uncheck any of the servers in the list. If you select new servers, you must use the wizard to select the services for that node
Create a query	Select **Create Query**.	
Run the query without any modification	• Select **Run Query**. • Complete the steps in "Execute a schedule."	
Modify the query	Go to Step 4.	

Step 4 Select **Next**.

Step 5 Perform one of the following actions:

- If you selected **Saved Query** and chose a query, the criteria that you specified for query appear. If necessary, modify the list of services and applications for which you want to collect traces.
- If you selected **Create Query**, you must select all services and applications for which you want to collect traces.

Step 6 Select **Next**.

Step 7 Perform one of the following actions:

If you want to:	Action
Collect traces for system logs or all system logs for all servers in the cluster	• Check the traces that apply. • Check **Select All Services on All Servers**. • Select **Next**.

If you want to:	Action
Collect traces for all services and applications for all servers in the cluster,	• Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all services and applications on a particular server,	• Check the name of the server. • Select **Next**.

Step 8 Perform one of the following actions to specify the time range for which you want to collect traces:

If you want to:	Action
Collect all the traces on the server for the services that you chose	Select **All Available Traces**.
Collect all the traces within an absolute date and time range	• Select **Absolute Range**. • Specify the server time zone and the time range (start and end date and time) for which you want to collect traces.
Collect all the traces within a relative date and time range	• Select **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 9 Enter the word or phrase in the Search String field to search by phrases or words that exist in the trace file. The tool searches for an exact match to the word or phrase that you enter.

What to do next

Execute a query.

Execute a Query

- If any node in the cluster is not available, a dialog box displays with a message that indicates which node is not available. The unavailable node does not display in the Trace & Log Central windows.
- You can install some listed services or applications only on a particular node in the cluster. To collect traces for those services or applications, make sure that you collect traces from the node on which you have activated the service or application.
- The services that you have not activated also display, so you can collect traces for those services.
- After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature.
- An error message displays if the service parameter values are exceeded or if the system is in code yellow.

Procedure

Step 1 Select **Run Query** to execute the query.

Step 2 Select **Save Query** to save the query and continue with the next step.

Step 3 Select **OK** when the dialog box displays that indicates that the query execution completed.

Step 4 Perform the following actions:

If you want to:	Action	Result
Create a query that you can run on nodes other than the one on which it was created	**a.** Select **Generic Query**. **b.** Select either the **Single Node Query** or **All Node Query**. **c.** Select **Finish**.	• You can only create a generic query if the services that you chose exist on a single node. If you chose services on more than one node, a message displays. You can either save the query as a regular query or select services on a single node. • If you select the Single Node Query, the trace collection tool by default selects the node on which you created the query when you execute the query. • If you select the All Node Query option, the trace collection tool by default selects all of the servers in the cluster when you execute the query.
Run the query on that node or cluster on which you created the query	**a.** Select **Regular Query**. **b.** Select **Finish**.	

Step 5 Browse to the location to store the query, enter a name for the query in the File Name field.

Step 6 Select **Save**.

Step 7 Perform one of the following actions:

If you want to:	Action
Run the query that you have just saved	• Select **Run Query**.
Exit the query wizard without running the query that you created	Select **Cancel**.

Step 8 Perform one of the following actions after the query execution completes:

If you want to:	Action
View a file that you collected	Follow these steps to navigate the file: **a.** Double-select **Query Results**. **b.** Double-select the <node> folder, where <node> equals the IP address or hostname for the node that you specified in the wizard. **c.** Double-select the folder that contains the file that you want to view. **d.** After you have located the file, double-select that file.
Download the trace files and the result file that contains a list of the trace files that your query collected	**a.** Select the files that you want to download. **b.** Select **Download**. **c.** Specify the criteria for the download. **d.** Select **Finish**.
Specify the directory in which you want to download the trace files and the results file	**a.** Select **Browse** next to the Download all files field. **b.** Navigate to the directory. **c.** Select **Open**.
Create a zip file of the trace files that you collected	Select **Zip File**.
Delete collected log files from the server	Check **Delete Collected Log Files from Server**.
Save the query	• Select **Save Query**.

Schedule Trace Collection in Cisco Unified Communications Manager

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.

Note You can schedule up ten 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

Note For large deployments, we recommend that you use a dedicated trace archive server and set up scheduled trace collections to this trace server.

Perform one or more of the following actions:

- 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, see 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, see the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Open the Trace and Log Central options.

Step 2 In the Trace and Log Central tree hierarchy, double-click **Schedule Collection**.

The Schedule Collection wizard appears.

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

Note If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note You can install some listed services and applications on a particular node in the cluster. To collect traces for those services and applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 Perform one of the following actions in the **Select CCM Services/Application** tab:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone node.

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for services or applications, click **Next**.

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

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for your standalone node.

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 5 Specify the node 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, appear in the **Select Time Zone** drop-down list box.

Step 6 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. In the **Date** tab, choose the appropriate date. In the **Time** tab, choose the appropriate time.

Step 7 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. In the **Date** tab, choose the appropriate date. In 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 8 From the **Scheduler Frequency** drop-down list box, choose how often you want to run the configured trace collection.

Step 9 From the **Collect Files that are 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 10 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 11 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 12 To delete collected log files from the node, check the **Delete Collected Log Files from the Server** check box.

Step 13 Choose one or more of the following actions:

- Download Files and go to Step 14.
- Run Another Query and go to Step 15.
- Generate Syslog. If you chose Generate Syslog, go to Step 16.

Step 14 In the SFTP/FTP Server Parameters group box, enter the node credentials for the node 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**.

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`.

You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Step 15 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 16 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 appears. Verify that you entered the correct IP address, username, and password.

Step 17 Click **OK**.

Step 18 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of the Quick Launch Channel.

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

Schedule Trace Collection in Cisco Unity Connection

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 ten 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 actions:

- 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, see 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, see the *Cisco Unified Serviceability Administration Guide*.

Procedure

Step 1 Open the Trace and Log Central options.

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

The Schedule Collection wizard appears.

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

Note Cisco Unity Connection: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Cisco Unity Connection: You can install some listed services and applications on a particular node in the cluster. To collect traces for those services and applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

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

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for your standalone node.

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the schedule collection wizard without collecting traces for system logs, click **Next**.

Step 5 Specify the node 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, appear in the **Select Time Zone** drop-down list box.

Step 6 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. In the **Date** tab, choose the appropriate date. In the **Time** tab, choose the appropriate time.

Step 7 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. In the **Date** tab, choose the appropriate date. In 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 8 From the **Scheduler Frequency** drop-down list box, choose how often you want to run the configured trace collection.

Step 9 From the **Collect Files that are 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 10 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 11 To create a zip file of the trace files that you collect, check the **Zip File** check box.

Step 12 To delete collected log files from the node, check the **Delete Collected Log Files from the Server** check box.

Step 13 Choose one or more of the following actions:

- Download Files. If you chose Download Files or Run Another Query, continue with Step 15.
- Run Another Query.
- Generate Syslog. If you chose Generate Syslog, go to Step 17.

Step 14 In the SFTP/FTP Server Parameters group box, enter the node credentials for the node 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**.

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`.

You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

Step 15 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 16 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 appears. Verify that you entered the correct IP address, username, and password.

Step 17 Click **OK**.

Step 18 To view a list of scheduled collections, click the **Job Status** icon in the Trace portion of the Quick Launch Channel.

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

Start a schedule

Before you begin

- Configure the information that you want to include in the trace files for the various services from the Trace Configuration window.
- If you want alarms to be sent to a trace file, select an SDI trace file as the alarm destination in the Alarm Configuration window.

Procedure

Step 1 Open Trace & Log Central.

Step 2 Double-select **Schedule Collection** in the tree hierarchy.

Step 3 Perform one of the following actions to collect trace on node logs:

If you want to:	Action
Collect traces for all services and applications for all nodes in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all services and applications on a particular node	• Check the name of the node. • Select **Next**.
Collect traces for particular services or applications on particular nodes	• Check the traces that apply. • Select **Next**.
Continue the trace collection wizard without collecting traces for services or applications	Select **Next**.

Step 4 Perform one of the following actions to collect traces on system logs:

If you want to:	Action
Collect all system logs for all nodes in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect traces for all system logs on a particular node	• Check the name of the node. • Select **Next**.
Collect traces for particular system logs on particular nodes	Check the traces that apply. For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users that are signing in and out, check **Security Logs**.
Continue the trace collection wizard without collecting traces for system logs	Select **Next**.

Step 5 Specify the node time zone and the time range for which you want to collect traces.

Step 6 Perform the following actions to specify the date and time that you want to start the trace collection:

a) Select the down arrow button next to the Schedule Start Date/Time field.
b) From the Date tab, select the appropriate date.
c) From the Time tab, select the appropriate time.

Step 7 To specify the date and time that you want to end the trace collection, perform the following actions:

a) Select the down arrow button next to the Schedule End Date/Time field.
b) From the Date tab, select the appropriate date.
c) From the Time tab, select the appropriate time.

Troubleshooting Tips

- The time zone of the client computer 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 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.

What to do next

Execute a schedule, on page 17

Execute a schedule

Procedure

Step 1 Select how often you want to run the configured trace collection from the Scheduler Frequency list box.

Step 2 Specify the time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect traces.

Step 3 Enter the word or phrase in the **Search String** field to search by phrases or words that exist in the trace file. The tool searches for an exact match to the word or phrase that you enter and only collects those files that match the search criteria.

Step 4 Check **Zip All Files** to create a zip file of the trace files that you collect.

Step 5 Check **Delete Collected Log Files from the Server** to delete collected log files from the server.

Step 6 Perform one or more of the following actions:

- To download files:
  a. Select **Download Files**.
  b. In the SFTP Server Parameters group box, enter the node credentials for the node where the trace and log central feature downloads the results.
  c. Select **Test Connection**.
  d. After the trace and log central feature verifies the connection to the SFTP server, select **OK**.
- To run another query:
  a. Select **Run Another Query**.
  b. Select **Browse** to locate the query that you want to run.
  c. Select **OK**.
- To generate a Syslog, select **Generate Syslog**.

Step 7 Select **Finish**.

Troubleshooting Tips

- If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node does not appear in the Trace & Log Central windows.
- If Unified RTMT cannot access the SFTP server, a message appears. Verify that you entered the correct IP address, username, and password.
- You can install some of the listed services/applications only on a particular node in the cluster. To collect traces for those services/applications, make sure that you collect traces from the node on which you have activated the service/application.
- The services that you have not activated also appear, so you can collect traces for those services.
- 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.
- 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 parameters fields: */home/<user>/Trace*.
- The trace and log central feature only executes the specified query if the first query generates results.

View Trace Collection Status

Follow this procedure to view the trace collection event status and to delete scheduled trace collections.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Job Status**.

The **Job Status** window appears.

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 appears.

Possible job types include the following:

- Scheduled Job
- OnDemand
- RealTimeFileMon
- RealTimeFileSearch

Possible statuses include the following:

- Pending
- Running
- Cancel

- Terminated

Step 4 To delete a scheduled collection, choose the event that you want to delete and click **Delete**.

Note You can cancel jobs with a status of "Pending" or "Running" and a job type of "Schedule Task" or job type of "RealTimeFileSearch."

Generate Problem Reporting Tool

The Problem Reporting Tool (PRT) on the Cisco IP Phone allows you to collect and send phone logs to your administrator. These logs are necessary for troubleshooting in case you run into issues with the phones.

Generate PRT for Endpoints

Use the Generate PRT option in Trace and Log Central to remotely trigger the log collection on the phone and upload it to the log server configured in the "Customer support upload URL" parameter.

Procedure

Step 1 Open the Trace and Log Central options.

Step 2 In the Trace & Log Central tree hierarchy, choose **Generate PRT**.
The Generate PRT wizard appears.

Step 3 Enter the Device name as configured in the Find and List Phones page in the Cisco Unified CM Administration user interface.

Step 4 Click **Generate PRT**.

The generated report is uploaded at the **Customer support upload URL**.

Note Configure the **Customer support upload URL** parameter in either the Enterprise, Profile, or Device level configuration page settings. Else, PRT generation fails.

Real-Time Trace

The real-time trace option of the Trace and Log Central feature allows you to view the current trace file that is being written on the server for each application. If the system has begun writing a trace file, the real-time trace starts reading the file from the point where you began monitoring rather than at the beginning of the trace file. You cannot read the previous content.

The real-time trace provides the option to view real-time data and monitor user events.

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 ten services, with a limit of three concurrent sessions on a single node. The log viewer refreshes every 5 seconds. As the traces are 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 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Real Time Trace**.

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not display in the Trace and Log Central windows.

Step 3 Double-click **View Real Time Data**.

The View Real Time Data wizard appears.

Step 4 From the **Nodes** drop-down list box, choose the node 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.

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

Note The following message appears at the bottom of this window: `If trace compression is enabled, the data seen in this window can be bursty due to buffering of data.`

Step 6 Click **Finish**. The real-time data for the chosen service displays in the generic log viewer.

Step 7 Perform one of the following actions:

- 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 8 Repeat this procedure to view data for additional services.

A message appears if you attempt to view data for too many services or too many services on a single node.

Step 9 After you finish with 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.

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 performs the action only once.

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.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Real Time Trace**.

Note Unified Communications Manager clusters and Cisco Unity Connection clusters only: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node does not display in the Trace and Log Central windows.

Step 3 Double-click **Monitor User Event**.

The Monitor User Event wizard appears.

Step 4 Perform one of the following actions:

If you want to:	Action
View the monitoring events that you have already set up	• Click **View Configured Events** • Select a node from the drop-down list box. • Click **Finish**. **Note** To delete an event, choose the event and click **Delete**.
Configure new monitoring events	• Select **Create Events.** • Select **Next**. • Continue with Step 5.

Step 5 Choose the node 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 appear, 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 node 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. If you have nodes in a cluster in a different time zone, TLC adjusts for the time change and get files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second node (node x) that is in a time zone that is one hour ahead, TLC downloads files from 10:00 a.m. to 11:00 a.m. from node x.

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:

If you want the system to:	Action
Generate an alarm when the system encounters the specified search string	Check **Alert**. **Note** For the system to generate the alarm, you must enable the enable the TraceCollectionToolEvent alert.
Log the errors in the application logs area in the SysLog Viewer	Check **Local Syslog**. **Note** The system provides a description of the alarm and a recommended action. You can access the SysLog Viewer from Unified RTMT.
Store the syslog messages on a syslog node	Check **Remote Syslog**. Enter the syslog node name in the **Server Name** field. **Note** By default, audit events are not sent to the remote syslog node, unless the severity is lowered to Warning, Notice, or Informational.
Download the trace files that contain the specified search string	Check **Download File**. Enter the node credentials for the node where you want to download the trace files in the SFTP Server Parameters group box. Select **Test Connection**. Select **OK** after the Trace and Log Central feature verifies the connection to the SFTP server. 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. You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers. If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command. **Note** FTP is not supported for Cisco Intercompany Media Engine.

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.

The following message appears: `If trace compression is enabled, there might be a delay in catching the event after it occurs, due to buffering of data.`

Step 10 Click **Finish**.

Collect Crash Dump in Cisco Unified Communications Manager

Follow this procedure to collect a core dump of trace files.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

The Collect Crash Dump wizard appears.

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

Note If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note You can install some of the listed services or applications on a particular node in the cluster. To collect traces for those services or applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 Perform one of the following actions in the **Select CCM Services/Application** tab:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone node.

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for services or applications, click **Next**.

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

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for your standalone node.

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.

- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 5 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 node 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, appear 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. If you have nodes in a cluster in a different time zone, TLC adjusts for the time change and gets files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m and you have a second node (node x) that is in a time zone that is one hour ahead, TLC downloads files from 10:00 a.m. to 11:00 a.m. from node x.

  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 length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect crash files.

Step 6 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.

When you upgrade from one version of your product that is running on the Linux platform to another version, and you restart the node with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection versions that ran on the Windows platform.

Step 7 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_users_directory>\<server name or server IP address>\<download time>`.

Step 8 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 9 To delete collected crash dump files from the node, check the **Delete Collected Log Files from Server** check box.

Step 10 Click **Finish**.

A message appears 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 that you chose. Choose the **Do Not Zip Files** radio button and try the collection again.

Collect Crash Dump in Cisco Unity Connection

Follow this procedure to collect a core dump of trace files.

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

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

The Collect Crash Dump wizard appears.

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

Note Cisco Unity Connection: If any node in the cluster is not available, a dialog box appears with a message that indicates which node is not available. The unavailable node will not appear in the Trace and Log Central windows.

Note Cisco Unity Connection: You can install some of the listed services or applications on a particular node in the cluster. To collect traces for those services or applications, make sure that you collect traces from the node on which you have activated the service or application.

Step 3 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

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

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for your standalone node.

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the collect crash dump wizard without collecting traces for system logs, click **Next**.

Step 5 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 node 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, appear 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. If you have nodes in a cluster in a different time zone, TLC adjusts for the time change and gets files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m and you have a second node (node x) that is in a time zone that is one hour ahead, TLC downloads files from 10:00 a.m. to 11:00 a.m. from node x.

  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 length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect crash files.

Step 6 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.

When you upgrade from one version of your product that is running on the Linux platform to another version, and you restart the node with the new version, Cisco Unified Serviceability moves the logs of the previous version to the inactive partition and stores logs for the newer version in the active partition. If you log in to the older version, Cisco Unified Serviceability moves the logs for the newer version to the inactive partition and stores the logs for the older version in the active directory.

Note Cisco Unified Serviceability does not retain logs from Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection versions that ran on the Windows platform.

Step 7 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_user_directory>\<server name or server IP address>\<download time>` where `<rtmt_user_directory>` specifies the directory where RTMT is installed.

Step 8 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 9 To delete collected crash dump files from the node, check the **Delete Collected Log Files from Server** check box.

Step 10 Click **Finish**.

A message appears 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 that you chose. Choose the **Do Not Zip Files** radio button and try the collection again.

Collect Installation Logs

Follow this procedure to collect installation and upgrade logs.

Procedure

Step 1 Choose **Tools** > **Trace** > **Trace & Log Central**.

The **Trace & Log Central** window appears.

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

The Collect Install Logs wizard appears.

Step 3 In the Select Servers Options box, specify from which server you would like to collect the install logs.

- To collect the install logs for a particular server, check the check box next to the server.
- To collect the install logs for all servers, check the Select All Servers check box.

Step 4 In the Download File Options, specify the directory where you want to download the log file. To specify the directory in which you want to download the log files, click **Browse** next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies `<rtmt_users_directory>`.

Step 5 Click **Finish**.

Collect audit logs

Browse Audit Logs

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard appears.

Step 3 Check the **Browse Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard appears.

Step 5 Perform one of the following actions in the **Action Options** window:

Note If you have a standalone server and check the **Select All Servers** check box, the system browses all audit logs for your standalone server.

a) To browse audit logs for all servers, check the **Select All Servers** check box.
b) To browse audit logs on a particular server, check the check box next to the server.

Step 6 Click **Finish**.

Step 7 The Remote Browse is Ready window appears. Click **Close**.

The Nodes pane appears.

Step 8 On the left side of the Nodes pane, double-click the **Nodes** folder. Navigate through the tree hierarchy until the Audit App folder appears.

Step 9 After the audit log file names display 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 want to use to view each file or double-click the selected file to display the file in the default viewer.

Step 10 Select an audit log file and perform one of the following actions:

- To create a zip file of the audit log files that you collect, click the **Zip File** radio button.

  Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

- To delete collected audit log files from the server, check the **Delete Files on Server** check box.
- To delete the selected audit log file, click **Delete**.
- To refresh the selected audit log file, click **Refresh**.
- To refresh all of the audit log files, click **Refresh All**.

Note Cisco Unified Serviceability does not retain audit logs from Unified Communications Manager or Unified Communications Manager IM and Presence Service versions that run on the Windows platform.

You have completed the steps for Browse Audit Logs.

Download Audit Logs

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard appears.

Step 3 Check the **Download Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard appears.

Step 5 Perform one of the following actions in the **Action Options** window:

Note If you have a standalone server and check the **Select All Servers** check box, the system downloads all audit logs for your standalone server.

a) To download audit logs for all servers, check the **Select All Servers** check box.
b) To download audit logs on a particular server, check the check box next to the server.

Step 6 Click **Finish**.

Step 7 To download audit logs, click **Next**.

The **Download Audit Logs** window appears.

Step 8 In the Nodes Selection Options pane, perform one of the following actions:

- Check the **Select All Servers** check box.
- Check a specific node check box.

Step 9 In the Collection Time pane, click one of the following radio buttons:

- **Absolute Range**: Specify the server time zone and the time range (start and end date and time) for which you want to audit logs.

  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, appear 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. If you have servers in a cluster in a different time zone, TLC adjusts for the time change and retrieves files for the same period of time. For example, if you specify files from 9:00 a.m. to 10:00 a.m. and you have a second server (server x) that is in a time zone that is one hour ahead, TLC downloads files from 10:00 a.m. to 11:00 a.m. from server x.

- **Relative Range**: Specify the length of time (in minutes, hours, days, weeks, or months) prior to the current time for which you want to collect audit logs based on the values from the following table:

Period of Time	Range
Minutes	5 - 60
Hours	2 - 24
Days	1 - 31
Weeks	1 - 4
Months	1 -12

Step 10 In the Download File Options pane, select one of the following options:

a) To specify the directory in which you want to download the audit log file, click the **Browse** button next to the Download File Directory field, navigate to the directory, and click **Open**. The default specifies `<\Program Files\Cisco\Unified RTMT\JRtmt>`.
b) To create a zip file of the audit log files that you collect, choose the **Zip File** radio button.

Note You cannot download a zipped audit log file that exceeds 2 gigabytes.

c) To delete collected audit log files from the server, check the **Delete Collected Log Files from Server** check box.

Step 11 Click **Finish**.

You have completed the steps for the download of audit logs.

Schedule Audit Log Download

Procedure

Step 1 Open the Trace & Log Central tree hierarchy.

Step 2 Double-click **Collect Audit Logs**.

The Collect Audit Logs Action Options wizard appears.

Step 3 Check the **Schedule Download of Audit Logs** check box.

Step 4 Click **Next**.

The Nodes Selection Options wizard appears.

Step 5 Perform one of the following actions in the **Action Options** window:

Note If you have a standalone node and check the **Select All Servers** check box, the system browses, downloads, or schedules a download of all audit logs for your standalone node.

a) To schedule a download of audit logs for all nodes, check the **Select All Servers** check box.
b) To schedule a download of audit logs on a particular node, check the check box next to the node.

Step 6 Click **Finish**.

The **Schedule Download of Audit Logs** window appears.

Step 7 In the Nodes Selection Options pane, perform one of the following actions:

- Check the **Select All Servers** check box.
- Check a specific node check box.

Step 8 In the Schedule Time pane, perform the following actions:

a) Highlight the **Select Reference Server Time Zone**.
b) Use the calendar and highlight a **Start Date/Time**.
c) Use the calendar and highlight an **End Date/Time**.
d) Select the Scheduler Frequency. You may choose Hourly, Daily, Weekly, or Monthly.
e) Check the **Zip All Files** check box to zip the audit log files.
f) Check the **Delete Collected Log Files From Server** check box to delete the collected audit log files from the node.

Step 9 In the Action Options pane, check the **Download Files** check box.
The **Trace Download Configuration Dialog** window appears.

Step 10 Enter the following information:

- Protocol: Select FTP (default) or SFTP.
- Host IP Address: Enter the IP address of the host node.
- User Name: Enter your username.

- Password: Enter your password.
- Port: Enter the FTP or SFTP port information.
- Download Directory Path: Enter the complete directory path where the files get downloaded.
- Click **Test Connection**. When the connection has been tested, the files are downloaded.

Note You can choose **Localhost** download option when downloading traces. This option is available only for Cisco Intercompany Media Engine servers.

If you download trace files to the local host directories on the Cisco Intercompany Media Engine server, you can offload the files to a remote SFTP server by using the **file get** CLI command.

Note FTP is not supported for Cisco Intercompany Media Engine.

You have completed the steps to schedule the download of audit logs.

Display Downloaded Trace Files Using Local Browse

After you collect trace files and download them to your PC, you can view them with a text editor that can handle UNIX variant line terminators such as WordPad on your PC, or you can view them by using the viewers within Unified RTMT.

Tip Do not use NotePad to view collected trace files.

Follow this procedure to display the log files that you collected with the Trace and Log Central feature. If you zipped the trace files when you downloaded them to your PC, you need to unzip the files to view them by using the viewers within Unified RTMT.

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

Before you begin

Collect the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection for instructions.

Procedure

Step 1 Open Trace and Log Central.

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.

If the file type has a viewer that is already associated with it, the file opens in that viewer. Otherwise, the Open With dialog box appears.

Step 5 Click the program that want to use to view the file. If your preferred program is not on the list, choose another program by clicking **Other**.

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

Unified RTMT displays the file in the appropriate viewer for the file type. If no other appropriate viewer applies, Unified RTMT opens files in the Generic Log Viewer.

Display and Download Trace Files in Cisco Unified Communications Manager

After the system generates trace files, you can view them on the node by using the viewers within Unified RTMT. You can also use the remote browse feature to download the traces to your PC.

Follow this procedure to display and download the log files on the node 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 the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection.

Procedure

Step 1 Open the Trace and Log Central options.

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 7.

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

Note If you choose Crash Dump, the wizard displays only the services that may cause a crash dump. If you do not see the service in which you are interested, click **Back** and choose Trace Files.

Note You can install some of the listed services/applications only on a particular node in the cluster. To choose traces for those services/applications, make sure that you choose traces from the node on which you have activated the service/application.

Step 4 Perform one of the following actions in the Select CCM Services/Application tab:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects traces for all service and applications for your standalone node.

- To collect traces for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
- To collect traces for all services and applications on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for services or applications, click **Next**.

Step 5 In the **Select System Services/Application** tab, perform one of the following actions:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects system logs for your standalone node.

a) To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
b) To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
c) To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.
e) Go to Step 10.

Step 6 Perform one of the following actions in the **Select CCM Services/Application** tab:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

a) To choose crash dump files for all services and applications for all nodes, check the **Select All Services on All Servers** check box and click **Next**.
b) To choose crash dump files for all services and applications on a particular node, check the check box next to the node and click **Next**.
c) To choose crash dump files for particular services or applications on particular nodes, check the check boxes that apply and click **Next**.
d) To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

Go to Step 8 for Cisco Business Edition or go to Step 9 for Unified Communications Manager.

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

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

a) To choose crash dump files for all nodes, check the **Select All Services on all Servers** check box.
b) To choose crash dump files for all system logs on a particular node, check the check box next to the node.
c) To choose crash dump files for particular system logs on particular nodes, check the check boxes that apply.
d) To continue the Remote Browse wizard without collecting crash dump files, go to the next step.

Step 8 Click **Finish**.

Step 9 After the traces become available, a message appears. Click **Close**.

Step 10 Perform one of the following actions:

- To display the results, navigate to the file through the tree hierarchy. After the log filename appears 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 appear 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.

- 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 **Browse** next to the Download all files field, navigate to the directory, and click **Open**. The default specifies `<rtmt_users_directory>\<server name or server IP address>\<download time>`.
  - 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 node, check the **Delete Files on server** check box.
- To delete trace files from the node, click the file that appears in the pane on the right side of the window; then, click **Delete**.
- To refresh a specific service or a specific node in a cluster, click the service or node name; then, click **Refresh**. After a message states that the remote browse is ready, click **Close**.
- To refresh all services or all nodes in a cluster that appear in the tree hierarchy, click **Refresh All**. After a message states that the remote browse is ready, click **Close**.

  Tip After you download the trace files, you can view them in Local Browse.

Display And Download Trace Files in Cisco Unity Connection

After the system generates trace files, you can view them on the node by using the viewers within Unified RTMT. You can also use the remote browse feature to download the traces to your PC.

Follow this procedure to display and download the log files on the node 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 the required traces files. See topics related to collecting trace files, downloading trace files using Query Wizard, and scheduling trace collection.

Procedure

Step 1 Open the Trace and Log Central options.

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

Step 3 Choose the appropriate radio button, and click **Next**.

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

Note If you choose Crash Dump, the wizard displays only the services that may cause a crash dump. If you do not see the service in which you are interested, click **Back** and choose Trace Files.

Note Cisco Unity Connection clusters: You can install some of the listed services on applications on a particular node in the cluster. To choose traces for those services or applications, make sure that you choose traces from the node on which you have activated the service or application.

Step 4 In the **Select CUC Services/Application** tab, perform one of the following actions:

- To collect all system logs for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To collect traces for particular system logs on the node, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.

Step 5 In the **Select System Services/Application** tab, perform one of the following actions:

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects system logs for your standalone node.

- To collect all system logs for all nodes, check the **Select All Services on all Servers** check box and click **Next**.
- To collect traces for all system logs on a particular node, check the check box next to the node and click **Next**.
- To collect traces for particular system logs on particular nodes, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting traces for system logs, click **Next**.

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

- To choose crash dump files for the node, check the **Select All Services on all Servers** check box or check the check box next to the node and click **Next**.
- To choose crash dump files for particular system logs on the node, check the check boxes that apply and click **Next**.
- To continue the Remote Browse wizard without collecting crash dump files, click **Next**.

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

Note If you have a standalone node and check the **Select All Services on All Servers** check box, the system collects crash dump files for your standalone node.

- To choose crash dump files for all nodes, check the **Select All Services on all Servers** check box.
- To choose crash dump files for all system logs on a particular node, check the check box next to the node.

- To choose crash dump files for particular system logs on particular nodes, check the check boxes that apply.
- To continue the Remote Browse wizard without collecting crash dump files, go to the next step.

Step 8 Click **Finish**.

Step 9 After the traces become available, a message appears. Click **Close**.

Step 10 Perform one of the following actions:

- To display the results, navigate to the file through the tree hierarchy. After the log filename appears 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 appear 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.

- 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 **Browse** next to the Download all files field, navigate to the directory, and click **Open**. The default specifies `<rtmt_user_directory>\<server name or server IP address>\<download time>` where `<rtmt_user_directory>` specifies the directory where Unified 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 node, check the **Delete Files on server** check box.
- To delete trace files from the node, click the file that appears in the pane on the right side of the window; then, click **Delete**.
- To refresh a specific service or a specific node in a cluster, click the service or node name; then, click **Refresh**. After a message states that the remote browse is ready, click **Close**.
- To refresh all services or all nodes in a cluster that appear in the tree hierarchy, click **Refresh All**. After a message states that the remote browse is ready, click **Close**.

  Tip After you download the trace files, you can view them in Local Browse.

Set Trace Collection Attributes

Before you begin

Collect traces files.

Procedure

Step 1 Open Trace & Log Central.

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

Step 3 Select the appropriate radio button, Trace Files or Crash Dump.

Step 4 Select **Next**.

Step 5 Perform one of the following actions:

a) If you select Trace Files, go to step 6.

b) If you select Crash Dump, go to step 8.

Step 6 Perform one of the following actions in the Voice/Video or IM and Presence Applications/Services tab:

If you want to:	Action
Collect traces for all services and applications for all servers in the cluster	• Select **All Services on All Servers** • Select **Next**.
Collect traces for all services and applications on a particular server	• Check the name of the server. • Select **Next**.
Collect traces for particular services or applications on particular servers	• Check the traces that apply. • Select **Next**.
Continue the trace collection wizard without collecting traces for services or applications	Select **Next**.

Step 7 Perform one of the following actions in the Select System Services/Application tab:

If you want to:	Action
Collect all system logs for all servers in the cluster	• Check **Select All Services on all Servers**. • Select **Next**
Collect traces for all system logs on a particular server	• Check the name of the server. • Select **Next**.
Collect traces for particular system logs on particular servers	• Check the traces that apply. **Note** For example, to collect CSA logs, check **Cisco Security Agent**. To access user logs that provide information about users that are signing in and out, check **Security Logs**. • Select **Next**.
Continue the remote browse wizard without collecting traces for system logs	Go to Select finish.

Step 8 Perform one of the following actions in the Voice/Video or IM and Presence Applications/Services tab:.

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.

If you want to:	Action
Collect crash dump files for all services and applications on a particular server	• Check the name of the server. • Select **Next**.
Collect crash dump files for particular services or applications on particular servers	• Check the traces that apply. • Select **Next.**

Step 9 Perform one of the following actions in the Select System Services/Application tab:.

If you want to:	Action
Collect crash dump files for all services and applications for all servers in the cluster	• Check **Select All Services on All Servers**. • Select **Next**.
Collect crash dump files for all services and applications on a particular server	• Check the name of the server. • Select **Next**.
Collect crash dump files for particular services or applications on particular servers.	• Check the traces that apply. • Select **Next.**
Continue the collect crash dump wizard without collecting crash dump files	Go to Step 10.

Step 10 Select **Finish**.

What to do next

View trace results.

View Trace Results

- You can install some listed services/applications only on a particular node in the cluster. To select traces for those services/applications, make sure that you select traces from the server on which you have activated the service/application.
- The services that you have not activated also display, so you can select traces for those services.
- After you have downloaded the trace files, you can view them by using the Local Browse option of the trace and log central feature.
- To sort the files that displays in the pane, select a column header; for example, to sort the files by name, select 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.
- The IM and Presence service does not support the Q931 Translator. IM and Presence does not support QRT report information.

Before you begin

Set your trace collection attributes.

Procedure

Step 1 Select **Close** when a message states that the trace results are available.

Step 2 Perform one of the following actions:

If you want to:	Action
To display the results	Perform one of the following actions to navigate to the file: Right-select the mouse to select the type of program that you would like to use to view the file.Double-select the file to display the file in the default viewer.
Download the trace files and the result file that contains a list of the trace files that your query collected	• Select the files that you want to download. • Select **Download**. • Specify the criteria for the download. • Select **Finish**.
Specify the directory in which you want to download the trace files and the results file	• Select **Browse** next to the Download all files field. • Navigate to the directory. • Select **Open**. The default specifies C:\Program Files\Cisco\Presence Serviceability\jrtmt\<server IP address>\<download time>
Create a zip file of the trace files that you collected	Check **Zip File**.
Delete collected log files from the server	Check **Delete Collected Log Files from Server**.
Delete trace files from the node	• Select the file that displays in the pane on the right side of the window. • Select **Delete**.
Refresh a specific service or node	• Select the server name or service. • Select **Refresh**. • Select **Close** when a message states that the remote browse is ready.
Refresh all services and nodes that display in the tree hierarchy	• Select **Refresh All**. • Select **Close** when a message states that the remote browse is ready.

Display Report Information

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

Note This section applies only to Unified Communications Manager.

You can view the IP phone problem reports that the Quality Report Tool 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 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 more information about how to configure and use QRT, see the *System Configuration Guide for Cisco Unified Communications Manager* .

Before you begin

Collect or view the Quality Report Tool (QRT) log files. See topics related to collecting trace files, scheduling trace collection, and downloading trace files using either Query Wizard or the Remote Browser.

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 appears.

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

Note The QRT viewer allows only the .xml files with a specific structure (having phone details), not the default one. If you open generic log files, you may see the following error message:

```
Fail to Open Cisco QRT Viewer, No Records Available!
```

Step 2 From the **Extension** drop-down list box, choose the extension or extensions that you want the report to include.

Step 3 From the **Device** drop-down list box, choose the device or devices 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**.

Log Compression

In Unified Communications Manager 8.0 onward, the log compression feature only compresses the following log files:

- `cm/trace/cti/sdl`
- `cm/trace/cti/sdi`
- `cm/trace/ccm/sdl`
- `cm/trace/ccm/sdi`

The other log files are not compressed and are written directly to the hard disk.

The compressed files have a .gz extension. The file that is being actively written to the disk will have a .gzo extension.

All the CLI commands used to view and tail the files will work on the compressed files and will automatically uncompress them for viewing or tailing. The only difference is in specifying file names with the .gz and .gzo extension.

The following option is available with the file tail command:

file tail activelog cm/trace/cti/sdl recent

The recent option, when used with a compressed directory, continually tails the most recent log file. You do not need to switch to a newer log file when the currently written-to log file is closed, so it is an infinite and ongoing tail. This option is only available with the compressed log files.

The log files are compressed in the gzip format. For uncompressing the log files, the open source program 7-Zip is available at `http://www.7-zip.org`, and works on all Windows platforms. You can use 7-Zip on any computer, including a computer in a commercial organization. You do not need to register or pay for 7-Zip. On a Linux platform, you can use the gzip or gunzip commands.

Edit Trace Settings

Follow this procedure to edit trace settings for Unified RTMT.

Note The Error radio button is the default setting.

Procedure

Step 1 Choose **Edit** > **Trace Setting**

Step 2 Click the radio button that applies.

The system stores the rtmt.log file in the Documents and Settings directory for the user; for example, on a Windows machine, the log is stored in `C:\Documents and Settings\<userid>\.jrtmt\log`.

Log Viewers

Messages in AuditLog Viewer

You can display the following messages in AuditLog Viewer:

- AuditApp Logs: These logs are related to Unified Communications Manager application audit logs.
- Vos Logs: These logs are related to platform (terminal, port or network address of the system) activities.

The following table describes the AuditLog Viewer buttons.

Table 1: AuditLog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the Auditlog Viewer. **Tip** You can enable the Auditlog Viewer to automatically update the current log file every 5 seconds by checking the **Auto Refresh** check box.
Clear	Clears the display of the current log.
Filter	For auditapp logs, limits the logs displayed based on the UserID you select. For vos logs, limits the logs displayed based on the set of options (Address, Terminal, and Type) that you select. **Tip** You can display logs other than the set of options you selected by checking the **Filter Inverse** check box.
Clear Filter	Removes the filter that limits the type of logs that appear.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC.

To make a column larger or smaller when viewing an auditlog message, drag the arrow that displays when your mouse hovers between two column headings.

You can order the displayed auditlog messages by clicking a column heading. The first time that you click a column heading, the logs display in ascending order. A small triangle pointing up indicates ascending order. If you click the column heading again, the logs display in descending order. A small triangle pointing down indicates descending order. If you click the column heading one more time, the logs display in the unsorted state.

Display AuditApp Logs

Procedure

Step 1 Choose **System** > **Tools** > **AuditLog Viewer**.

Step 2 From the Select a Node drop-down list, choose the server on which the logs that you want to view are stored.

Step 3 Double-click the **AuditApp Logs** folder.

Step 4 Click the **.log** file located outside the Archive folder to view the current logs. The AuditApp Logs for the selected node are displayed in a tabular form.

Note If you want see the old logs, double-click the **Archive** folder and click the corresponding file.

Step 5 Double-click the entry that you want to view. The auditlog message for that particular entry appears in a new window.

Tip You can filter the auditlog message display results by choosing an option in the Filter By drop-down list box. To remove the filter, click **Clear Filter**. All logs appear after you clear the filter.

Display Cisco Unified OS Logs

Procedure

Step 1 Choose **System** > **Tools** > **AuditLog Viewer**

Step 2 From the **Select a Node** drop-down list, choose the node where the logs that you want to view are stored.

Step 3 Double-click the **Cisco Unified OS Logs** folder.

Step 4 Click the **vos-audit.log** file located outside the Archive folder to view the current logs. The Cisco Unified OS Logs for the selected node appear in a tabular form.

Note If you want see the old logs, double-click the **Archive** folder and click the corresponding file.

Step 5 Double-click the entry that you want to view. The Cisco Unified OS log message for that particular entry is displayed in a new window.

Tip You can filter the Cisco Unified OS log message display results by choosing the set of options in a pop up window that appears after you click **Filter**. To remove the filter, click **Clear Filter**. All logs appear after you clear the filter.

Display Messages in SysLog Viewer

You can display messages in SysLog Viewer.

Tip CiscoSyslog messages also display the syslog definition, which includes recommended actions, in an adjacent pane when you double-click the syslog message. You do not have to access the Alarm Definitions in Cisco Unified Serviceability for this information.

The following table describes the SysLog Viewer buttons.

Table 2: Syslog Viewer Buttons

Button	Function
Refresh	Updates the contents of the current log on the syslog viewer. **Tip** You can enable the syslog viewer to automatically update the syslog messages every 5 seconds by checking the Auto Refresh check box.
Clear	Clears the display of the current log.
Filter	Limits the messages that appear based on the set of options that you select.
Clear Filter	Removes the filter that limits the type of messages that appear.
Find	Allows you to search for a particular string in the current log.
Save	Saves the currently selected log on your PC.

When you view the syslog message, drag the arrow that appears when your mouse hovers between two column headings to make the column larger or smaller.

You can order the displayed syslog messages by clicking a column heading. The first time that you click a column heading, the records display in ascending order. A small triangle pointing up indicates ascending order. If you click the column heading again, the records display in descending order. A small triangle pointing down indicates descending order. If you click the column heading one more time, the records display in the unsorted state.

Procedure

Step 1 Choose **System** > **Tools** > **SysLog Viewer** > **Open SysLog Viewer**.

Step 2 From the **Select a Node** drop-down list box, choose the server where the logs that you want to view are stored.

Step 3 Click the tab for the logs that you want to view.

Step 4 After the log appears, double-click the log icon to list the filenames in the same window.

Tip If some syslog messages do not appear in the window, scrolling the mouse pointer over the missing syslog messages refreshes the display.

Step 5 To view the contents of the file at the bottom of the window, click the filename.

Step 6 Click the entry that you want to view.

To view the complete syslog message, double-click the syslog message. You can also use the buttons described in the SysLog Viewer Buttons table to view the syslog messages.

Tip You can filter the syslog message display results by choosing an option in the Filter By drop-down list box. To remove the filter, click **Clear Filter**. All logs appear after you clear the filter.

Plugins

Download and Install Application Plug-Ins

You can expand the functionality of Unified RTMT by installing application plug-ins, such as the Voice Log Translator (VLT) application. You can download the latest plug-ins for Unified RTMT from Cisco.com. After installing the plug-in, you can access the application in Unifed RTMT.

To download and install the plug-in, perform the following procedure:

Procedure

Step 1 Choose **Application** > **CCO Voice Tools Download**.

The Login Prompt appears.

Step 2 Enter your Cisco.com username and password and click **OK**.

Step 3 Download the file to your PC.

Step 4 To begin the installation, double-click the download file.

Step 5 Follow the installation instructions.

Launch Application Plug-Ins

After downloading and installing the plug-in, you can access the application in the RTMT viewer.

Procedure

Under **System** > **Tools** > **Plugin**, choose the plug-in that you want to launch.

The application appears in the plugin window. See the application document for usage information.