CHAPTER 17

Using the Cisco Unified Analysis Manager Tools

The Unified Analysis Manager provides a set of tools that allow you to perform management tasks for specific devices and groups of devices. The following sections describe the tasks you can perform with the Unified Analysis Manager tools:

Analyze Call Path

The Analyze Call Path tool allows you to trace a call between multiple Cisco Unified Communications products. In order to trace a call using the Analyze Call Path tool, a node must be defined in Unified Analysis Manager and the node must belong to a group. See Identifying and Adding Nodes to Cisco Unified Analysis Manager for more information about adding nodes and assigning them to groups.

Note All nodes that you define are assigned to the AllNodes group by default. Use the Node Groups function if you want to assign the node to a different group. See Configuration Considerations for Analyze Call Path for more information on configuring a Call Record Repository before using the Analyze Call Path function.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Analyze Call Path**. The Analyze Call Path Information window displays.

Step 2 Click the **Continue** button. The **Search Criteria** window displays

Step 3 Enter the number where the call originated in the **Calling Number** field. The default is an asterisk (*) which is a wildcard that will trace all numbers for the node.

Step 4 Enter the number where the call terminated in the **Called Number** field. The default is an asterisk (*) which is a wildcard that will trace all numbers for the node.

Step 5 Use the **Termination Cause** drop-down list box to select the reason for the call termination; either Abandoned, Dropped, Failed or all three.

Step 6 Use the **Start Time** field to enter the start time for the trace.

Step 7 Use the **Duration** field to indicate the length of the time period you want to trace.

Step 8 Use the **Time Zone** drop-down list box to select the time zone where you are tracing calls.

Step 9 Use the **Filter Nodes by Group** drop-down list box to select the group of nodes that you want to trace.

Step 10 Use the **and Node Type** drop-down list box to select specific types of nodes that you want to trace. When you have selected the Group and Node, information displays for each node. You can then use the checkbox for each node listed to select or deselect the node.

Note The limit for the number of nodes that you can select at a time is 20.

Step 11 Click the **Run** button to begin the trace. The trace results display on the bottom of the window. If you selected multiple nodes, a tab is displayed for each node. Click on the tab to display information for that node.

Step 12 When the call record information displays, you can click the **View Full Path** button to see the complete call path. You can click the **View Record Details** button to see the information about the call. Use the **Save Results** button to save the reports.

Configuration Considerations for Analyze Call Path

When using the Analyze Call Path tool, there are configuration considerations for each product that the Unified Analysis Manager manages. Refer to the following sections for configuration information for these products.

- Cisco Unified Communications Manager/Cisco Unified Communications Manager Business Edition, page 17-2
- Cisco Unified Contact Center Express, page 17-4
- Cisco Unified Intelligent Contact Management Enterprise/Cisco Unified Contact Center Enterprise, page 17-4
- Cisco Unified Customer Voice Portal, page 17-5
- Cisco Access Control Server and Cisco IOS Gateway, page 17-6

The Analyze Call Path tool does not include information for Cisco Unity Connection and Cisco Unified Presence servers.

Cisco Unified Communications Manager/Cisco Unified Communications Manager Business Edition

The following information applies when configuring the Analyze Call Path for Cisco Unified Communications Manager and Cisco Unified Communications Manager Business Edition:

- Version Support—Unified Analysis Manager supports Release 8.0(1) and above for Cisco Unified Communications Manager and Release 8.0(1) and above for Cisco Unified Communications Manager Business Edition.
- Call Record Server—For Cisco Unified Communications Manager, use the first node (publisher) as the Call Record Server with the HTTPS protocol and the default port 8443.
- User Group and Access Permissions— Users should belong to a user group whose role contains read and update permissions required to access Call Records for the following resources:

  - SOAP Call Record APIs
  - SOAP Control Center APIs
  - SOAP Diagnostic Portal Database Service
  - SOAP Log Collection API
  - SOAP Performance Informations APIs
  - SOAP Realtime Informations and Control Center APIs

Note New resources "SOAP Diagnostic Portal Database Service" and "SOAP Call Record APIs" added on an upgrade should not have the read and update permissions by default due to security reasons for existing users. Users need to create or copy the role to custom resources and update the required permissions for above mentioned resources as needed. Refer to *Cisco Unified Communications Manager Administration Guide* for additional details.

- Configuring NTP—Each product installed in the solution should be configured to point to same set of external NTP clock sources. NTP is required to be configured on all nodes that involve calls for SCT features. For Cisco Unified Communications Manager, use the **utils ntp config** CLI command to configure NTP.
- Enable Call Record Logging—In Cisco Unified Communications Manager Administration, go to the Service Parameter Configuration window, and choose the **Cisco CallManager Service**. Enable the **CDR Enabled Flag** and the **CDR Log Calls with Zero Duration Flag** parameters. Restart the **Cisco CallManager** service for change-notification to take effect immediately. Repeat this procedure for all nodes in the Cisco Unified Communications Manager cluster.

Note You can verify that flags are set as desired at https://<HOSTNAME:PORT>/ccmadmin/vendorConfigHelp.do

- CDR CAR Loader—Ensure your CDR Analysis and Reporting (CAR) Loader is set to **Continuous Loading 24/7**. To verify this:
  - Go to the Cisco Unified Serviceability and select **Tools > CDR Analysis and Reporting** (CAR) page. The CAR page opens in a new browser.
  - Go to **System > Scheduler > CDR Load** page.
  - Verify if Loader is not disabled and that **Continuous Loading 24/7** is enabled. This allows CDR records that are generated from Cisco Unified Communications Manager nodes to be loaded into the CAR database as soon as they arrive to Cisco Unified Communications Manager first node (publisher).

  If call records are not found on the Cisco Unified Communications Manager, it is possible that the CAR Loader failed or is having a delay loading the latest CDR records. If this occurs, go to the CAR **System > Database > Manual Purge** page and click the **Table Information** button. Check for the oldest and latest CDR records that are available in the CAR database. If records are not set to the latest date, go to **System > Log Screens > Event Log** and select **CDR Load** to check its recent run status to see if there were any Unsuccessful runs. If CDR Load failure is found, collect CAR Scheduler traces to provide to Cisco Support for troubleshooting.
- Raw Call Record Details—For information on Raw Call Record details help for the Cisco Unified Communications Manager, refer to *Cisco Unified Communications Manager Call Detail Records Administration Guide* for 8.0(1).

Cisco Unified Contact Center Express

The following information applies when configuring the Analyze Call Path for Unified CCX:

- Version Support—Unified Analysis Manager supports Unified CCX version 8.0(1) and later.
- Call Record Server—The Call Record Server used for Unified CCX is either (or both in the case of a High Availability system) of the Unified CCX nodes. The database is active on both nodes and the data is replicated. The JDBC user is **uccxsct** and the password is the encrypted version of the TFTP password. The password is typically set by the Unified CCX administrator.
- Default user for adding Unified CCX Call Record Server—The Informix user for adding (and connecting to) Unified CCX Call Record Server is**: uccxsct.** You can reset the default install time password for above user in the Unified CCX Application **Administration > Tools > Password Management** page. Typically, the Unified CCX administrator will reset to the desired password and pass it on to the Unified Analysis Manager administrator.
- User Group and Access Permissions—Unified CCX does not require any additional user group and access permission to access Call Records. The access permissions of the uccxsct user is set by Unified CCX install for read access to specific tables. No external settings are required.
- Configuring NTP—To configure NTP for Unified CCX, go to **OS Administration > Settings > NTP Server**.
- Enable Call Record Logging—Unified CCX always generates Call Records by default, so no configuration is required to enable logging of Call Records.

Cisco Unified Intelligent Contact Management Enterprise/Cisco Unified Contact Center Enterprise

The following information applies when configuring the Analyze Call Path for Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Unified CCE:

- Version Support—Unified Analysis Manager supports Release 8.0(1) and above for Unified ICME and Unified CCE.
- Call Record Server—The Call Record Server used for Unified ICME is either AW-HDS-DDS or HDS-DDS. The server used for Unified CCE is HDS/AW Database (port 1433).
- User Group and Access Permissions—For Release 8.0(1), the recommended user group and access permissions that are required to access Call records are the Windows only Authentication for SQL Server. This is done by using the **User List** tool from the Configuration Manager and creating a user with the right access privileges.
- Configuring NTP—Configuration for Time Synchronization of Unified CCE servers is based on Microsoft Windows Time Services. When setting up the Unified CCE router component, retain the default settings of the “Disable ICM Time Synchronization” box as checked. With the recommended default setting, the time synchronization for Unified CCE servers is provided by the Windows Time Service, which automatically synchronizes the computer's internal clock across the network. The time source for this synchronization varies, depending on whether the computer is in an Active Directory domain or a workgroup. For additional information on setting up Windows Time Service, refer to the Microsoft Windows Time Service Technical Reference documentation at: http://technet.microsoft.com/en-us/library/cc773061(WS.10).aspx
- Enable Call Record Logging—To check that Call Record logging is enabled, first be sure that the Unified Analysis Manager service on Unified CCE is enabled. Using the web setup, you need to install the AW-HDS-DDS or HDS-DDS servers with Administration and Data Server roles. Once you install these roles using the web setup, the call records are available by default.

- Raw Call Record Details—To find help for the Raw Call Record details, refer to the Schema Help which you can access from the Unified CCE Administration Tool group on either the AW-HDS-DDS or HDS-DDS server. You can also refer to the United CCE Database Schema Handbook for a specific release.

Cisco Unified Customer Voice Portal

The following information applies when configuring the Analyze Call Path for to Unified CVP:

- Version Support—United Analysis Manager supports Unified CVP Release 8.0(1) and above.
- Call Record Server—Unified CVP uses the Unified CVP Reporting Server for the Call Record Server.
- User Group and Access Permissions—Unified CVP uses Unified CVP OAMP to set user group and access permissions required to access Call Records:
  - All users trying to access Unified CVP records from the Unified CVP database need to be created via Unified CVP OAMP.
  - Unified CVP Reporting users need to be granted the Unified CVP Reporting role in Unified CVP OAMP.
  - User passwords may expire if security hardening is installed on the Unified CVP Reporting Server. SNMP monitor displays alerts when this happens.
- Configuring NTP—Configuration for Time Synchronization of the Unified CVP servers is based on Microsoft Windows Time Services. For additional information on setting up Windows Time Service, refer to the Microsoft Windows Time Service Technical Reference documentation at http://technet.microsoft.com/en-us/library/cc773061(WS.10).aspx.
- Enable Call Record Logging—To ensure that Call Record logging is enabled, do the following:
  - Unified CVP Reporting Server is not installed nor configured by default. Customers and Partners will have to install a Unified CVP Reporting Server to use the Analyze Call Path tool with Unified CVP.
  - Unified CVP Database schema needs to be laid down by the Unified CVP_database_config.bat file. This file needs to be run by the user after Unified CVP Reporting Server installation is completed.
  - Once a Unified CVP Reporting Server is installed, it needs to be configured via Unified CVP OAMP and a Unified CVP Call Server needs to be associated with the Unified CVP Reporting Server.
  - Follow the Unified CVP CAG and RPT guidelines for configuring the Unified CVP Reporting Server, Unified CVP VXML Server, and Unified CVP Call Servers.
  - Unified CVP data retention is 30 days, by default. You can customize this value via Unified CVP OAMP. Unless you back up the database, data will be purged at the end of data retention day. Backed up Unified CVP data is not accessible unless it is imported back into the database.
  - Unified CVP VXML Server filters need to be configured on Unified CVP OAMP. Refer to the Unified CVP OAMP guide for configuring these filters.
- Raw Call Record Details—For information relating to Raw Call Record details, refer to the Unified CVP Reporting Guide for version 7.0(2).

Cisco Access Control Server and Cisco IOS Gateway

The following information applies when configuring the Analyze Call Path for Cisco Access Control (ACS) Servers and Cisco IOS Gateways:

- Version Support—Unified Analysis Manager supports ACS Release 5.1.
- Call Record Server—To assign a Call Record Server One of the acs servers can be configured as a "collector" node.
- User Group and Access Permissions—To set user group and access permissions, after the ACS server is installed, in ssh/telnet access, enter **acsadmin** as the username and **default** as the password, You will be prompted to change the password.
- Configuring NTP—To configure an NTP server on an ACS server, use cli: **ntp server <NTP server IP/host>**.
- Enable Web View—Execute the CLI command acs **config-web-interface view enable** to enable web view. It is disabled by default.
- Cisco IOS gateways as ACS network devices or AAA clients—You need to configure ACS network device to have the correct Radius secret, which is the same secret as the one on the IOS gateway.
  - From acsadmin, access **Network Devices Group > Network Devices and AAA clients** to add the Cisco IOS gateway as the ACS network device or AAA client.
- For IOS configurations:
  - Use the CLI to configure NTP server: ntp server <<NTP server IP/host>
  - Configure Cisco IOS gateway as a Radius client of the ACS server. Sample CLIs are below:

```
aaa new-model
!
!
aaa group server radius acs
server 172.27.25.110 auth-port 1812 acct-port 1813
!
aaa authentication login h323 group acs
aaa authorization exec h323 group acs
aaa accounting connection h323 start-stop group acs
aaa session-id common
gw-accounting aaa
radius-server host 172.27.25.110 auth-port 1812 acct-port 1813
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

- Be sure you have local login access to your Cisco IOS gateways.
- Enable Call Record Logging—To check that Call Records logging is enabled:
  - aaa accounting connection h323 start-stop group acs
    aaa session-id common
    gw-accounting aaa
    radius-server host 172.27.25.110 auth-port 1812 acct-port 1813
    radius-server key cisco
    radius-server vsa send accounting

Call Definitions

Table 17-1 defines the types of call termination.

Table 17-1 Call Definitions

Call Type	Call Termination Explanation
Failed call	The call is not connected for any reason other than user hang-up before the connection is completed.
Abandoned call	The call is not connected because the user hangs up after initiating the call.
Dropped call	The call is disconnected after connection for any reason other than user hanging up.

Table 17-2 Product Support for Call Types

Call Type	Unified CM/ Unified CMBE	Unified CCE	Unified CVP	Unified CCX
Failed Call	Supported	Supported	Supported	Supported
Abandoned call	Supported	Supported	Not Supported	Supported
Dropped Called	Supported	Supported	Not Supported	Supported

Collecting Traces

Unified Analysis Manager allows you to collect log and trace files from services of supported devices. There are three ways you can collect logs and trace files:

- Collect Traces Now— Collect Traces Now option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time that has occurred in the past.
- Schedule Trace Collection— Schedule Trace Collection option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time in the future.
- Schedule Trace Settings and Collections—Schedule Trace Settings and Collection option allows you to collect trace files from the present into the future and also specify the trace levels to be used during the scheduled time.

The following sections describe each of the above option:

- Collect Traces Now, page 17-8
- Schedule Trace Collection, page 17-8
- Schedule Trace Settings and Collection, page 17-9

Collect Traces Now

The Collect Traces Now option allows you to collect trace files based on a selection of services on a device or group of devices for any period of time that has occurred in the past.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Collect Traces Now**. The Collect Trace on Demand window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize new trace levels for the group or device.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 You can optionally click the **View Summary** button to view the Collection Summary window. This window contain a list of the components associated with the node.

Step 7 Click the **OK** button to start the trace. When the trace is completed, the window displays a Status Summary and Status Details for the trace. The Status Details provide the path to the directory to which the log was sent.

Schedule Trace Collection

Use the Schedule Trace Collection option if you want to collect trace files for any period of time from the present into the future.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Schedule Trace Collection. The Schedule Trace Collection** window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to collect traces for specific components.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 Use the **Collect Traces Every** dropdown field to indicate the frequency of the collection.

Step 7 Optionally, you can choose to have an email notification sent regarding the trace collection. To do that, click the **Send Email Notification to** checkbox and enter the email address in the text box.

Step 8 You can optionally click the **View Summary** button to view the Collection Summary window. This window contains a list of the components associated with the node.

Step 9 Click the **OK** button to start the trace. When the trace is scheduled, the window displays a Status Summary and Status Details for the trace. When the trace is completed, a report is written to your log file and, if email information was provided, a system-generated email is sent.

Schedule Trace Settings and Collection

Use the Schedule Trace Settings and Collection option if you want to collect trace files for any period of time from the present into the future and, in addition, also specify the trace levels to be used during the scheduled time. If you change trace settings with this option, trace levels are restored to their default settings after the collection period is over.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Schedule Trace Collection. The Schedule Trace Collection** window displays.

Step 2 Select either the Group to display a list of supported groups or Node, for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize new trace levels for the group or device. This option also allows you to collect traces for specific components.

Step 4 Use the **Start Time** and **End Time** fields to select the collection time period.

Step 5 Use the **Referenced Time Zone** field to select the time zone for the collection time period.

Step 6 Use the **Collect Traces Every** dropdown field to indicate the frequency of the collection.

Step 7 Optionally, you can choose to have an email notification sent regarding the trace collection. To do that, click the Send **Email Notification to** checkbox and enter the email address in the text box.

Step 8 You can optionally click the **View Summary** button to view the Collection Summary window. This window contains a list of the components associated with the node.

Step 9 Click the **OK** button to start the trace. When the trace is scheduled, the window displays a Status Summary and Status Details for the trace. When the trace is completed, a report is written to your log file and, if email information was provided, a system-generated email is sent.

Setting Trace Levels

Use the Set Trace Level option to assign trace levels for a group of devices or individual devices. You can assign trace levels using a template or you can customize trace levels. Trace levels can be set for the following Cisco Unified Communications components:

- Cisco Unified Communications Manager—Allows setting trace levels for Cisco Unified Communications Manager and Common Trace Components.
- Cisco Unified Presence—Allows setting trace levels for Unified Presence and Common Trace Components.
- Cisco Unity Connection—Allows setting trace level for Cisco Unity Connection and Common Trace Components.

- Cisco Unified Contact Center Express—Allows setting trace level only for Common Trace Components.

Table 17-3 describes the general trace level settings for the Cisco Unified Communications components that are managed by Unified Analysis Manager.

Table 17-3 Unified Analysis Manager Trace Level Settings

Trace Level	Guidelines	Expected Volume of Traces
Default	This level should include all traces generated in abnormal paths. This level is intended for coding error traces and error s traces that normally should not occur.	Minimum Traces expected
Warning	This level should include traces for system-level operations. This should include all traces generated by "State Transitions" within components.	Medium Volume of Traces Expected when component is used
Informational	This should include traces that can be used in the lab for debugging difficult problems of the component.	High Volume of Traces Expected when component is used
Debug	This level should include detailed debug information or high volume of messages which are primarily used for debugging.	Very High Volume of Traces Expected when component is used

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > Set Trace Level. The Set Trace Level** window displays.

Step 2 Select either the Group to display a list of supported groups or the Node for a list of supported devices. Select the groups or devices that you want to collect traces for.

Step 3 Use the **Select the template to** dropdown list to select the template containing the trace levels you want to use. Alternately, you can click the **Customize** button if you want to customize trace levels for the group or device. If you choose the **Customize** option, the Design Preview dialog displays with a list of supported devices. Choose the device you want and use the **Selected Components** fields to set the trace levels.

Step 4 You can click the **View Changes** button to see any changes made to traces levels for the node. Click **OK** to set the level and exit the screen.

Viewing a Configuration

Use the View Configuration option to view configuration information related to a node. You can collect the version and configuration information and view it in a browser or save the results.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Tools > View Configuration**. The **View Configuration** window displays.

Step 2 The window displays a list of nodes. Select a node and click the **Next** button to display the **Selected Components** screen. This screen lists the Version, Platform, License and other category configuration information for the product.

Step 3 Click the **Finish** button to collect the configuration information. The summary window displays. The window has a **View** and a **Save As** button. User can view the collected information in a browser or save the collected configuration information using the **Save As** button.