Cisco Unified Communications Analysis Manager User Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-21440-01

CONTENTS

Preface

This chapter describes the purpose, audience, and organization of this document and describes the conventions that convey instructions and other information. It contains the following sections:

Purpose

This document provides information for installing and using the Analysis Manager. The Analysis Manager application is installed as an option when you install the RTMT software. The Analysis Manager interface is accessed from a drawer on the RTMT main menu.

Once it is installed, the application can identify the supported UC products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files.

Audience

The Cisco Unified Analysis Manager User Guide provides information for network administrators who are responsible for managing and supporting Cisco Unified Communications Manager, Cisco Unified Communications Manager Business Edition, and Cisco Unity Connection. Network engineers, system administrators, or telecom engineers use this guide to learn about, and administer, remote serviceability features. This guide requires knowledge of telephony and IP networking technology.

Organization

The following table provides an outline of the chapters in this document.

Chapter	Description
Chapter 1, "Overview"	Describes an overview of the Analysis Manager Tool.
Chapter 2, "Installing and Configuring Cisco Unified Analysis Manager "	Describes the steps for installing and configuring the Analysis Manager
Chapter 3, "Identifying and Adding Nodes to Cisco Unified Analysis Manager"	Describes how to add nodes, groups and manage templates with Analysis Manager.
Chapter 4, "Using the Cisco Unified Analysis Manager Tools"	Describes the tools available for managing servers and call tracking with Analysis Manager.

Related Documentation.

For additional documentation on Cisco Unified Communications products supported by the Unified Analysis Manger, refer to the following:

- Cisco Unified CM Release 8.0
- Unified CCE Release 8.0(1)
- Unified CCX Release 8.0
- Unity Connection Release 8.0
- Unified Presence Release 8.0(2)

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.

Convention	Description
italic screen font	Arguments for which you supply values are in *italic screen* font.
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

Tip Means *the following are useful tips.*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco Product Security Overview

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

A summary of U.S. laws governing Cisco cryptographic products may be found at—http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.

If you require further assistance please contact us by sending email to export@cisco.com.

CHAPTER 1

Understanding Cisco Unified Analysis Manager

The Cisco Unified Analysis Manager (Unified Analysis Manager), a tool included with the Cisco Unified Real-Time Monitoring Tool (RTMT), is used to perform troubleshooting operations. When the Unified Analysis Manager is launched, it collects troubleshooting information from your system and provides an analysis of that information. You can use this information to perform your own troubleshooting operation or to send the information to Cisco Technical Assistance for analysis.

The Analysis Manager application is installed as an option when you install the RTMT software. The Analysis Manager interface is accessed from the RTMT main menu and quick launch channel.

Once it is installed, the application can identify the supported UC products and applications that you have in your system and troubleshoot call failures across these UC applications, collecting trace and log files.

The Unified Analysis Manager will support the following products:

- Cisco Unified Communications Manager (Unified Communications Manager) Release 8.0 (1)
- Cisco Unified Contact Center Enterprise (Unified CCE) Release 8.0(1)
- Cisco Unified Contact Center Express (Unified CCX) Release 8.0(1)
- Cisco IOS Voice Gateways (37xx, 28xx, 38xx, 5350XM, 5400XM) IOS Release PI 11
- Cisco Unity Connection (Unity Connection) Release 8.0(1)
- Cisco Unified Presence (Unified Presence) Release 8.0(2)

The three primary components of the Unified Analysis Manager interface are

- Administration—The system component lets you import device and group configuration from an external file and provide a status of jobs run by the Unified Analysis Manager.
- Inventory —The inventory component is used to identify all of the devices in your system that can be accessed and analyzed by the Unified Analysis Manager.
- Tools —The tools component contains all of the functions that Unified Analysis Manager supports. This includes configuring traces settings, collecting logs and viewing configurations.

How the Unified Analysis Manager Works

The Unified Analysis Manager application is installed as part of the RTMT installation. So once you complete the RTMT installation, you have access to the Unified Analysis Manager features.

The Unified Analysis Manager application is not displayed when RTMT is connected to a Cisco Unity Connection or Cisco Unified Presence server.

When you use RTMT to connect to a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Business Edition server, you can add nodes to include Cisco Unity Connection and Cisco Unified Presence servers in Unified Analysis Manager.

Where to Find More Information

For more information about RTMT and Cisco Unified Communications Manager, refer to:

- Cisco Unified Communications Manager Release 8.0(1)
- Cisco Unified Communications Manager Business Edition Release 8.0(1)

For more information about products that can be managed with Unified Analysis Manager, refer to:

- Cisco Unified Contact Center Enterprise Release 8.0(1)
- Cisco Unified Contact Center Express Release 8.0(1)
- Cisco Unity Connection Release 8.0(1)
- Cisco Unified Presence Release 8.0(2)

CHAPTER 2

Installing and Configuring Cisco Unified Analysis Manager

You can install Cisco Unified Real-Time Monitoring Tool (RTMT), which works for resolutions 800*600 and above, on a computer that is running Windows 98, Windows XP, Windows 2000, Windows Vista, or Linux with KDE and/or Gnome client.

Note RTMT requires at least 128 MB in memory to run on a Windows operating system platform.

This chapter contains information on the following topics:

Installing Cisco Unified Real-Time Monitoring Tool

To install the tool, perform the following procedure:

Note While installing Cisco Unified Real-Time Monitoring Tool on a Windows Vista platform, you will see a User Account Control pop-up message that says, “An unidentified program wants to access your computer.” Click **Allow** to continue working with Cisco Unified Real-Time Monitoring Tool.

Procedure

Step 1 Go to the **Plug-ins** window of the administration interface for your configuration:

Cisco Unified Communications Manager	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
Cisco Unified Communications Manager Business Edition	From Cisco Unified Communications Manager Administration, choose **Application > Plugins**.
Cisco Unity Connection	From Cisco Unity Connection Administration, choose **System Settings > Plugins**.

Step 2 Click the **Find** button.

Step 3 To install the Cisco Unified Real-Time Monitoring Tool on a client that is running the Microsoft Windows operating system, click the **Download** link for the Cisco Unified Communications Manager Real-Time Monitoring Tool-Windows.

Step 4 To install the Cisco Unified Real-Time Monitoring Tool on a client that is running the Linux operating system, click the **Download** link for the Cisco Unified Communications Manager Real-Time Monitoring Tool-Linux.

Step 5 Download the executable to the preferred location on your client.

Step 6 To install the Windows version, double-click the Cisco Unified Real-Time Monitoring Tool icon that displays on the desktop or locate the directory where you downloaded the file and run the Cisco Unified Real-Time Monitoring Tool installation file.

Step 7 The extraction process begins.

Step 8 To install the Linux version, ensure that the file has execute privileges; for example, enter the following command, which is case sensitive: chmod +x CcmServRtmtPlugin.bin

Step 9 After the Unified Real-Time Monitoring Tool welcome window displays, click **Next**.

To accept the license agreement, click **I accept the terms of the license agreement**; then, click **Next**.

Step 10 Choose the location where you want to install Cisco Unified Real-Time Monitoring Tool. If you do not want to use the default location, click **Browse** and navigate to a different location. Click **Next**.

Step 11 To begin the installation, click **Next**.

Step 12 The Setup Status window displays. Do not click **Cancel**.

Step 13 To complete the installation, click **Finish**.

Uninstalling Cisco Unified Real-Time Monitoring Tool and Cisco Unified Analysis Manager

On a Windows client, use Add/Remove Programs under the Control Panel to uninstall Unified Real-Time Monitoring Tool and Cisco Unified Analysis Manager (Unified Analysis Manager).

Launching Cisco Unified Analysis Manager

Caution *Unified Communications Manager clusters only.* You must configure a second server as the failover collector in Cisco Unified Communications Manager Administration, so Cisco Unified Real-Time Monitoring Tool can continue to retrieve information if the primary collector fails.

Note While using Cisco Unified Real-Time Monitoring Tool on a Windows Vista machine, you will see a User Account Control pop-up message that says "An unidentified program wants to access your computer." Click **Allow** to continue working with Cisco Unified Real-Time Monitoring Tool.

The Unified Analysis Manager application is not displayed when Cisco Unified Real-Time Monitoring Tool is connected to a Cisco Unity Connection or Cisco Unified Presence server because these products do not have a Call Record database.

When you use Cisco Unified Real-Time Monitoring Tool to connect to a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Business Edition server, you can add nodes to include Cisco Unity Connection and Cisco Unified Presence servers in the Unified Analysis Manager.

To launch Unified Analysis Manager, do the following procedure:

Procedure

Step 1 After you install the plug-in, perform one of the following tasks:

- From your Windows desktop, double-click the **Real Time Monitoring Tool 8.5** icon.
- Choose **Start > Programs > Cisco Unified Serviceability > Real-Time Monitoring Tool**.

The Unified Real-Time Monitoring Tool Login window displays.

Step 2 In the IP Host Address field, enter either the IP address or host name of the server, or (if applicable), first server in a cluster.

Step 3 In the User Name field, enter the Administrator username for the application.

Step 4 in the Password field, enter the Administrator user password that you established for the username.

Step 5 Enter the port that the application will use to listen to the server. The default port number is 8443.

Step 6 Check the **Secure Connection** check box.

Step 7 Click **OK**.

Step 8 When prompted, add the certificate store by clicking **Yes**.

The Cisco Unified Real-Time Monitoring Tool starts.

Configuring Cisco Unified Analysis Manager

The **Administration** option on the Unified Analysis Manager menu allows you to import device and group configurations from a .csv file to the Unified Analysis Manager tool.

Importing Configurations

This option allows you to import device and group configuration from a .csv file into the Unified Analysis Manager.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Administration > Import**.

Step 2 Use the Import window to select the .csv configuration file that you want to import.

Step 3 Click the **Import** button. The selected file will display.

Displaying Job Status

This function allows you to display status of scheduled trace setting and log collection jobs. Jobs can be scheduled using the Unified Analysis Manager Tools. Once a device is added to a group, you can schedule trace setting and log collections jobs on the device.

A scheduled job is linked to the machine it is configured on, and the job cannot be run on a different machine. If the machine on which a job was scheduled is not usable for any reason, the old job can be cloned and saved as a new job with new parameters to be run on the new machine.

Jobs running on a device can have one of the following states:

- Scheduled—A job is scheduled within Unified Analysis Manager; however it has not started
- Running—A job that is currently either setting traces or collecting logs
- Completed—A job that is done
- Pending—A job that has completed one run of collecting logs and is waiting to start the next run.
- Aborted—A job that has stopped abnormally due to an unexpected error
- Canceled—A job that has stopped due to a cancel operation by the user.

The Job Status screen gives a system view of all the jobs in Unified Analysis Manager. For jobs that have multiple runs, the status and time of the last run is also shown in this page.

The following operations can be performed on a job:

- View Details—Use this option to get more detailed view of the job.
- Cancel—Use this option to cancel a job. The Cancel operation can only be done on the machine that the job is running or scheduled on. This option cannot be used for jobs that are in the Completed/Aborted/Canceled state.
- Clone—Use this option to select any job and save it as a new job. The job being cloned from can be in any state. This option allows you to change any attribute of the job before saving. Cloning a job does not impact the attributes of the job being cloned.

Uploading Configuration Files

This option allows you to transfer files to a configured FTP server and send an email to interested parties. You can use this option to transfer some files to another machine so they can be viewed by others.

This screen allows you to specify the files and folders to be transferred as well as any annotations to accompany those files.

The following procedure explains how to transfer files to an FTP server:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Administration > Upload Files**.

Step 2 The **Upload Files** screen displays.

Step 3 In the **Case ID** field, enter the number that Cisco TAC has assigned to the case.

Step 4 Use the drop-down list box in the **Send to Server** field to select the FTP server you are sending the file to.

Step 5 Use the **Notes** box to provide any additional information about the file.

Step 6 Use the **Send Email Notifications** checkbox if you want to add the email addresses to send a notification that the file is uploaded. To add multiple email addresses, add the mail ids separated by comma. The mail addresses can be only the <username> or it can be of the format username@domain.com.

Step 7 In the bottom section of the screen, in the **Files to upload** box, select the files you want to transfer. Use the **Add** or **Remove** buttons to select or deselect files from the system. The files selected will be zipped by default and then uploaded. The name of the zipped file will be of the format <case id>_uploadedfile.zip.

Step 8 Click the **OK** button to transfer the file.

Cisco Unified Analysis Manager Preferences

Use the Unified Analysis Manger dropdown menu to set preferences for:

- FTP Server
- Mail Server
- Trace Collection directory

Setting these preferences is described in the following sections:

- Accessing FTP Server Options, page 2-6
- Adding or Editing an FTP Server, page 2-6
- Configuring a Mail Server , page 2-7
- Adding or Editing a Mail Server and Recipients, page 2-7
- Trace Collection Directory, page 2-8

Configuring an FTP Server

This function allows you to configure a FTP Server which you can then use to export information to. These servers can be Cisco TAC FTP servers. This information can include things such as Logs/trace files, system call trace information, etc.

By default, Cisco's TAC FTP server will be pre-populated. You can modify this configuration for this default FTP server.

The FTP Sever option allows you to manage the configured servers. This includes the following operations:

- Adding a new FTP server
- Editing an existing FTP server
- Deleting FTP servers
- Testing the connection of an FTP server

Cisco TAC has two FTP servers you can configure for exporting files:

- ftp-rtp.cisco.com
- ftp-sj.cisco.com

On both servers, files should be uploaded to the **/incoming** directory.

Accessing FTP Server Options

The following procedure explains how to access the FTP Server Options:

Procedure

Step 1 From the Unified Analysis Manager dropdown menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **FTP Server**.

Step 2 The **FTP Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server.

Step 3 Use the buttons to select the option you want.

Adding or Editing an FTP Server

The following procedure explains how to add an FTP Server or edit and exiting configuration:

Procedure

Step 1 From the Unified Analysis Manager dropdown menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **FTP Server**.

Step 2 The **FTP Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server.

Step 3 Click the **Add** button to add a server or the **Edit** button to edit an existing configuration. The **Add FTP Server** screen displays.

Step 4 In the **Name/IP Address** field, enter the name or the IP address of the FTP server you are adding.

Step 5 In the **Protocol** field, select either the FTP or SFTP protocol, depending on the type of server you are connecting to. Use SFTP if you are connecting to a Cisco TAC server.

Step 6 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the server.

Step 7 In the **Port** field, enter the port number on the server that you will be using.

Step 8 In the **Destination Directory** field, enter the path for the directory to which you will be exporting files. If you are adding a Cisco TAC server, use the **/incoming** directory.

Step 9 Click the **OK** button to add the server. You can use the **Cancel** button to end the operation without adding the FTP server.

Configuring a Mail Server

This option allows you to configure a mail server for the purpose of notifying a set of user configured recipients on the status of Unified Analysis Manager operations such as trace and log collections and file transfers.

You must configure at least one mail server in order to be able to send a notification.

Note You can only use mail servers configured with this option for Unified Analysis Manager notifications. For Cisco Unified Real-Time Monitoring Tool notifications, you must configure a separate mail server.

Adding or Editing a Mail Server and Recipients

The following procedure explains how to add a Mail Server and recipient or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager dropdown menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **Mail Server**.

Step 2 The **Mail Servers** screen displays with a list of configured servers and buttons to **Add**, **Edit**, or **Delete** a server. The **Test Connection** button allows you to test connectivity to a server. The bottom part of the screen shows the recipients listed for each server and buttons to **Add**, **Edit**, or **Delete** a recipient.

Step 3 Click the **Add** button to add a server or the **Edit** button to edit an existing configuration. The **Add Mail Server** screen displays.

Step 4 In the **Name/IP Address** field, enter the name or the IP address of the Mail server you are adding.

Step 5 In the **Port** field, enter the port number on the server that you will be using.

Step 6 Click the **OK** button to add the server. You can use the **Clear** button to clear the field, or the **Cancel** button to end the operation without adding the Mail server.

Step 7 To add or edit a recipient, go back to the Mail Server screen and Click the **Add** button to add a recipient or the **Edit** button to edit an existing configuration. The **Add Mail Server** screen displays.

Step 8 In the **Email address** field, enter the name or the email address of the recipient you are adding.

Step 9 Click the **OK** button to add the recipient. You can use the **Cancel** button to end the operation without adding the recipient.

Trace Collection Directory

The following procedure explains how to use the Trace Collection option under Preferences to set a directory for trace logs:

Step 1 From the Unified Analysis Manager drop-down menu, select **AnalysisManager > Preferences**. The Preferences window displays. Click on **Trace Collection**.

Step 2 The **Trace Collection** screen displays. Enter the directory you want to use for traces logs in the **Download Directory** box, or use the **Browse** button to locate the directory. Optionally, you can click the **Default** button to select the default dirctory.

Step 3 Click the **Save** button.

CHAPTER 3

Identifying and Adding Nodes to Cisco Unified Analysis Manager

This chapter covers the operations involved with identifying which nodes the Unified Analysis Manager can diagnose. This chapter contains the following sections:

Managing Nodes

Once configured, a supported node is added to the Unified Analysis Manager database and will appear on the supported Unified Analysis Manager node list. You can identify a Unified Analysis Manager node in one of three ways:

- Importing node and group configuration from a configuration file.
- Manually entering node and group information with the Unified Analysis Manager screens.
- Discovering Unified Analysis Manager nodes from a seed node. A seed node is one that can return information about all the nodes within a deployment. Once discovered, the nodes can then be added to the node inventory. This option saves you from manually entering details of these nodes.

For Cisco Unified Communications Manager, the first node (publisher) is the seed node. For Cisco Unified Customer Voice Portal (Unified CVP), the Cisco Unified CVP OAMP server is the seed node.

This option allows you to perform Add/Edit/Delete and Discover operations on nodes. All configured Unified Analysis Manager nodes (manually entered, imported from a file, or discovered) will be displayed in the list of nodes.

You can use the Nodes option to perform the following functions:

- Add—The Add button allows you to manually enter a new node.
- Edit—The Edit button allows you to edit a node that has already been configured.
- Delete—The Delete button allows you to delete one or more nodes.

- Discover—You can use the Discover option, which applies only to a seed node. Use the Discover button to send a query to the seed node, which then returns information about all the nodes within that deployment that the seed node is aware of. Once discovered, the nodes are automatically added to the node inventory.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to the node using the configured access information.

Node Summary

The Node summary screen displays all of the nodes currently configured with the Unified Analysis Manager application. Use the following procedure to access the Node summary screen.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Nodes.**

Step 2 The **Node** summary screen displays with a list of configured nodes and buttons to **Add**, **Edit**, **Delete, Discover**. The **Test Connection** button allows you to test connectivity to a node. Nodes are listed by **Name** and **Product Type**.

Adding or Editing a Node

The following procedure explains how to add a node or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Node**. The Node window displays.

Step 2 Click the **Add** button to add a node or select a node from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Node** screen displays.

Note Fields on this screen that are marked with an asterisk (*) are required fields.

Step 3 Use the **Product Type** drop-down list box to select a product.

Step 4 In the **IP/Host Name** field, enter the host name or the IP address of the node you are adding or editing.

Step 5 In the **Transport Protocol** field, select the protocol you want to use. Options for this field depend on the **Product Type** you selected.

Step 6 In the **Port Number** field, enter the port number on the node that you will be using.

Step 7 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the node. Reenter the password in the **Confirm Password** field.

Step 8 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 9 In the **Associated Call Record Server** and **Associated Trace File Server** fields, use the drop down list to select the respective servers you want to use for the node.

Step 10 Use the **Associated Group** checkboxes if you want to add the node to an existing group.

Step 11 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Node-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 12 Click the **Save** button to add the node. You can use the **Cancel** button to end the operation without adding the node.

Managing Groups

Within Unified Analysis Manager, you can create groups and add nodes to these groups. Once the nodes are added to a group, the user can perform a set of functions (for example, Trace Collection and Trace Setting) at a group level. A single node can belong to multiple groups. Nested groups will not be supported. Copying a group will not be supported.

Note The **AllNodes** group is added by default when a node is added in Unified Analysis Manager. Any nodes added to Unified Analysis Manager are part of the AllNodes group by default. The AllNodes group cannot be edited or deleted.

Note The number of groups you can have is limited to 20 and the number of nodes in a group (with the exception of the AllNodes group) is 20.

You can use the Group option to perform the following functions:

- Add—Use the Add button to create a group. Once a Group is created, you can add nodes to the group.
- Edit—Use the Edit button to select and edit group information. The Edit function also allows you add or delete the node members of the group. You can change which nodes belong to a group by adding or deleting nodes from that group.
- Delete—Use the Delete button to delete a Group. This function deletes that group from the Unified Analysis Manager. However, this function does not delete the individual nodes in the group from the Unified Analysis Manager. Nodes must be deleted individually using the Edit button.

For more information, see the "Adding or Editing a Node" section on page 3-2.

Adding or Editing a Group

The following procedure explains how to add a group or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Node Groups**.

Step 2 The **Groups** window displays. Click the **Add** button to add a group or select a group from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Group** screen displays.

Step 3 Use the **Group Name** field to enter the name of the group.

Step 4 Use the **Group Description** field to enter a brief description of the group.

Step 5 The **Select Nodes** section contains a list of each configured node. To add a node to the group, highlight the node in the list and click the **Add** button.

Step 6 When you have finished selecting nodes for the group, click the **Add** button to add the group or the **Update** button if you are editing the group content. You can use the **Cancel** button to end the operation without adding or editing the group.

Managing the Trace File Repositories

This option allows you to perform Add/Edit/Delete operations on trace file servers for the Unified Analysis Manager. Managed nodes typically use the trace file server to off load its trace and log files. The Unified Analysis Manager can then connect to the trace file server to collect logs and traces.

You can use the Trace File Server option to perform the following functions:

- Add—The Add button allows you to manually enter a new server.
- Edit —The Edit button allows you to edit a server that has already been configured.
- Delete—The Delete button allows you to delete one or more servers.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to a server using the configured access information.

For more information, see the "Adding or Editing a Trace File Repository" section on page 3-4.

Adding or Editing a Trace File Repository

The following procedure explains how to add a Trace File Server or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory> Trace File Repositories**.

Step 2 The **Trace File Repository** window displays with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list and click the **Edit** button to edit an existing configuration.

Step 3 In the **IP/Hostname** field, enter the name or the IP address of the server you are adding.

Step 4 In the **Transport Protocol** field, use the drop-down list box to select the protocol you want to use, either SFTP or FTP.

Step 5 In the **Port Number** field, enter the port number on the server that you will be using.

Step 6 In the **User Name** and **Password** fields, enter the user name and password that gives you access to the server. Reenter the password in the **Confirm Password** field.

Step 7 In the **Description** field, you can optionally provide a brief description of the server you are adding.

Step 8 In the **Associated Nodes** field, use the check boxes to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Trace File Server-Advanced** screen. Enter the appropriate information in the **Alternate IP/Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Managing the Call Record Repositories

This option allows you to perform Add/Edit/Delete operations on call record servers for the Unified Analysis Manager. Managed nodes typically see the Call Record Server to store the call data in a database. The Unified Analysis Manager can then connect to the Call Record Server to get detailed call data.

You can use the Call Record Server option to perform the following functions:

- Add—The Add button allows you to manually enter a new server.
- Edit—The Edit button allows you to edit a server that has already been configured.
- Delete—The Delete button allows you to delete one or more servers.
- Test Connectivity—The Test Connectivity button allows you to test connectivity to a server using the configured access information.

For more information, see the "Adding or Editing a Call Record Repository" section on page 3-5.

Adding or Editing a Call Record Repository

The following procedure explains how to add a call record server or edit an existing configuration:

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory > Call Record Repositories**.

Step 2 The **Call Record Repository** window displays with a list of configured servers. Click the **Add** button to add a new server or highlight a server on the list and click the **Edit** button to edit an existing configuration.

Step 3 Use the **Repository Type** drop down list to select the product type for the node that will be accessing the server.

Step 4 In the **Hostname** field, enter the name of the server you are adding.

Step 5 In the **JDBC Port** field, enter the port number on the server that you will be using.

Step 6 In the **JDBC User Name** and **JDBC Password** fields, enter the user name and password that gives you access to the server. Re-enter the password in the **Confirm Password** field.

Step 7 In the **Description** field, you can optionally provide a brief description of the node you are adding.

Step 8 Use the **Nodes Available for Association** to select the nodes that will have access to the server.

Step 9 If you have a NAT or Terminal Server configuration, use the **Advanced** button to display the **Add Call Record Server-Advanced** screen. Enter the appropriate information in the **Alternate Hostname** and **Alternate Port** fields.

Step 10 Click the **Add** button to add the server or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

Defining Trace Templates

If you have large number of nodes in a group, the Unified Analysis Manager provides templates as a shortcut for selecting components to change trace levels. You can also use templates to establish the new trace levels for nodes. You can also use template for collecting logs and trace files.

You can use the Templates option to perform the following functions:

- Add—The Add button allows you to create a new template. When adding a template you should note that you are doing so for node types and not actual nodes. For a given node type, there is a known fixed set of components and services.
- Edit—The Edit button allows you to edit an existing template.
- Clone—The Clone button allows you to save an existing template as a new template without replacing the original one.
- Delete—The Delete button allows you to delete a template.
- Import—Use the Import button to import predefined templates from a flat file.
- Export—Use the Export button to export a template to a flat file.

For more information, see the "Adding or Editing a Template" section on page 3-6.

Adding or Editing a Template

The following procedure explains how to add a template or edit an existing configuration:

Note Unified Analysis Manager has default templates which cannot be edited or deleted.

Procedure

Step 1 From the Unified Analysis Manager menu, select **Inventory> Templates**.

Step 2 The **Templates** window displays. Click the **Add** button to add a template or select a template from the list and click the **Edit** button to edit an existing configuration. The **Add** or **Edit Template** screen displays.

Step 3 Use the **Name** field to enter the name of the template.

Step 4 Use the **Description** field to enter a brief description of the group.

Step 5 The **Product Types** section contains a list of products supported by the Unified Analysis Manager. When you select a product from this list, the associated components display in the **Component Name** field.

Step 6 For each component displayed, you can apply a trace level by using the drop down list in the **Trace Level** field.

Note Not all components are available for setting trace levels with this screen.

Step 7 You can indicate if you want to collect trace logs for the component by checking the box in the **Collect** field.

Step 8 Click the **Add** button to add the template or **Edit** to update the configuration. You can use the **Cancel** button to end the operation without adding the server.

CHAPTER 4

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

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 4-1 defines the types of call termination.

Table 4-1 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 4-2 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 4-8
- Schedule Trace Collection, page 4-8
- Schedule Trace Settings and Collection, page 4-9

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 4-3 describes the general trace level settings for the Cisco Unified Communications components that are managed by Unified Analysis Manager.

Table 4-3 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.

CHAPTER 5

Cisco Unified Analysis Manager Troubleshooting and Limitations

This chapter contains the following sections:

Cisco Unified Analysis Manager Limitations

The following are the limitations you should consider when implementing and using the Unified Analysis Manager.

- The maximum number of call records that the Call Search Report can display is 500.
- The maximum number of call records that the Call Track Report can display is 100.
- Since there is no globally unique callID to use, Unified Analysis Manager uses link-by-link approach to trace the call. If any record for a call is missing in one of the products in the call path, the link will be broken for the rest of the chain and the tracking will not be complete.
- Call records are not stored in the database orderly based on any particular column. When running Call Search Report, the number of returned records is limited to 500. The 500 records that are retrieved may not be the earliest (based on originating time, connection time, or disconnect time) in the specified time range. To make sure all of the call records within the specified time range are retrieved, you need to shorten the time range until the returned number of records is less than 500.
- The Unified Analysis Manager option is not displayed when the Cisco Unified Real Time Monitoring Tool is connected to a Cisco Unity Connection or Cisco Unified Presence server, because these products do not have a Call Record database.

  When you use the Cisco Unified Real Time Monitoring Tool to connect to a Cisco Unified Communications Manager or a Cisco Unified Communications Manager Business Edition server, you can add nodes to include Cisco Unity Connection and Cisco Unified Presence servers in the Unified Analysis Manager.
- Call Tracking does not support tracking of SIP Unified Outbound Option calls from Unified CCE and Unified IME to Cisco IOS gateways.
- Call Tracking does not support direct call tracking of call paths using a GED-125 protocol from Unified CCE to Unified CVP.
- Cisco Unified Communications Manager needs to be in the call path for tracking calls from Cisco Unified Communications Manager.

- Call tracking only supports single branch tracking from Cisco Unified Communications Manager.
- No Call Detail Records (CDR) are generated for calls on the MGCP gateway, as the gateway does not implement call control and Q.931 is backhauled/tunneled to the Cisco Unified Communications Manager for signalling. The CDR is available only on the Cisco Unified Communications Manager.
- With ACS servers, Unified Analysis Manager is used only for call tracing, and then used only if you want to include gateway records and information in the tracing data. If you do not have an ACS server or a supported hardware/software version of the ACS server, most of Unified Analysis Manager functions in your deployment will continue to work; however, your gateway information will not be included in your call traces.

Cisco Unified Analysis Manager Troubleshooting

Table 5-1 provides a list of errors that you may see when testing Unified Analysis Manager connectivity to a node and the suggested action for correcting the errors.

Table 5-1 Test Connectivity Errors and Corrective Actions

No.	Error Code	Message	Corrective Action
1	*NOT_AUTHORIZED_CODE*	Username or password is not correct	Enter the correct username and password.
2	*MISSING_SERVICE_CODE*	Missing Service	The requested web service was not found. Check to see if the web service is down on the target application.
3	*SERVER_BUSY_CODE*	Server is busy	Check to see if there are any other ongoing jobs running on the server. If so, wait until the job is done. If not, wait a few minutes and try again.
4	*INVALID_PORT_CODE*	Invalid Port	The specified port may be syntactically incorrect or may be out of range.
5	*CONNECTION_FAILED_CODE*	Not connected to the specified node	Verify that you have entered the correct address for this node. If the address is correct, then verify that the node is up and that it is reachable.
6	*NOT_SUPPORTED_CODE*	Not supported	This version of the specified product is not supported for this release. Upgrade this product to a supported version.

Table 5-1 Test Connectivity Errors and Corrective Actions (continued)

7	*CERTIFICATE_HANDLING_ERROR_CODE*	SSL handshake failed. The client and server could not negotiate desired level of security	Verify that you have accepted the certificate that was sent to the client from the server.
8	*GENERAL_CONNECTION_ERROR_CODE*	An internal error has occurred	Save the recent Unified Analysis Manager log files and contact Unified Analysis Manager support for help.