SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted

8.5(1)

December 2010

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: 408 527-0833

Table of Contents

Preface

Purpose

This document describes the Simple Network Management Protocol (SNMP) feature support found in Unified Intelligent Contact Manager/Contact Center Enterprise & Hosted (Unified ICM/CCE/CCH), 8.0(1).

Audience

This document is intended for System Installers, Unified ICM/CCE Administrators, and Network Administrators.

Organization

This document is organized as follows:

Chapter	Description
About Cisco SNMP	Contains information on SNMP Basics, Details the Agents and Management Information Bases (MIBs) used by the Cisco SNMP Service.
Cisco SNMP Installation and Basic Configuration	Preinstallation requirements and Configuration, starting and stopping the SNMP service.
Responding to Alarms	Details Notifications and Event Correlation. Provides configuration settings for Trap and Syslog destinations.
Cisco Discovery Protocol Driver	Contains general information and setup steps for the Cisco Discovery Protocol Driver.

Related Documentation

Related Documents include:

- *Installation and Setup Guide for Cisco Unified ICM/CCE*
- *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted, Release 8.0(1)*
- *Installation, Setup, and Configuration Guide for Cisco Unified CCE/CCH*
- *Administration Guide for Cisco Unified CCE/CCH*
- *Pre-installation Planning Guide for Cisco Unified ICM*
- *Installation, Setup, and Configuration Guide for Cisco Unified CCE/CCH*
- *Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following:

Convention	Description
	• Text as it appears in code or that the window displays. Example: **`<html><title>Cisco Systems,Inc. </title></html>`**
`< >`	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

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.

Documentation Feedback

You can provide comments about this document by sending email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Chapter 1

About Cisco SNMP

SNMP Basics

Network Management Systems use the Simple Network Management Protocol (SNMP), an industry-standard protocol, to exchange management information between network devices. SNMP enables administrators to remotely monitor network/application performance, find and solve network problems, and plan for network growth.

An SNMP-managed network contains: managed devices, agents, and Network Management Stations (NMS). Management Information Bases (MIBs) are used to structure the information that is passed between the components in the system.

- A managed device designates a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

  The following Release 8.0(1) Unified ICM/CCE components are valid managed devices:

  – Routers

  – Loggers

  – Peripheral Gateways (PGs)

  – Administration & Data Server

  – CTI Gateways (CGs)

  – CTI OS Servers

  – Outbound Option

- An agent resides on a managed device. An agent (or one of its subagents) retrieves local management information and translates it into the SNMP format to forward it to an SNMP Management Station. Subagents collect information for various components and then forwards that information to a master agent.

  Unified ICM/CCE supports the following agents:

  – SNMP Master Agent

  – Unified ICM/CCE Application(CISCO-CONTACT-CENTER-APPS-MIB) Subagent

  – Platform Subagent(s)[1]

  – System Applications Instrumentation (SYSAPPL-MIB) Subagent

  – Host Resources (HOST-RESOURCES-MIB) Subagent

  – Cisco Discovery Protocol (CISCO-CDP-MIB) Subagent[2]

- A Network Management Station (NMS) comprises an SNMP management application together with the computer on which it runs. An NMS executes applications that monitor and control managed devices. An NMS provides the bulk of the processing and memory resources that are required for network management. Cisco Unified ICM/CCE SNMP works with SNMP standards-compliant NMSs.

- A Management Information Base (MIB) designates a collection of information that is organized hierarchically. You can access instrumentation defined by a MIB using the SNMP protocol. MIBs are composed of managed objects, which are identified by object identifiers.

  A managed object (sometimes called a MIB object or an object) possesses one of any number of specific characteristics of a managed device. Managed objects comprise one or more object instances, which are essentially variables.

  Cisco Unified ICM/CCE supports the following MIBs:

  – CISCO-CONTACT-CENTER-APPS-MIB

  – CISCO-CDP-MIB (Cisco Discovery Protocol)

  – HOST-RESOURCES-MIB

  – SYSAPPL-MIB - (System-Level Managed Objects for Applications)

  See Detailed MIB Descriptions (page 7)

1) Provided by your hardware vendor

2) Only supported on Cisco MCS-78xx Hardware

SNMP Management Information Bases (MIBs)

Cisco Contact Center Application MIB

The Cisco Contact Center Application (CISCO-CONTACT-CENTER-APPS) MIB contains tables of objects and their corresponding values for the major components of an Unified ICM/CCE Enterprise/Hosted Edition installation.

Components include:

- Router (and a table of NICs)
- Logger
- Peripheral Gateway (PG) (and a table of PIMs)
- Distributor Administration and Data Server
- CTI Gateway (CG)
- CTI OS Server
- Outbound Option

The MIB definition can be viewed by opening the file: **`<INSTALL_DRIVE>\icm\snmp\CISCO-CONTACT-CENTER-APPS-MIB.my`** in a text editor or a MIB browser.

The MIB also provides a notification object which defines the format of SNMP notifications generated by Unified ICM/CCE components. The SNMP subagent on the Unified ICM/CCE Logger component sends alarms to the NMS.

The CISCO-CONTACT-CENTER-APPS-MIB is available at: **ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CONTACT-CENTER-APPS-MIB.my** .

See Also

Unified ICM/CCE Notifications on page 19

Cisco Discovery Protocol MIB (CDP)

The Cisco Discovery Protocol MIB (CISCO-CDP-MIB) provides information about device identifications, CDP running status, CDP transmitting frequency, and the time for the receiving device to hold CDP messages (time to live). For more information, see "Cisco Discovery Protocol Support."

The Cisco CDP MIB is available at **ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CDP-MIB.my**.

See Also

Cisco Discovery Protocol (CDP) Driver Installation/Uninstall on page 21

Host Resources MIB

The Host Resources MIB found in Cisco SNMP is an implementation of the Host Resources MIB document, proposed standard **RFC 1514** (http://www.ietf.org/rfc/rfc1514.txt). It is also compliant with Host Resources MIB, draft standard **RFC 2790** (http://www.ietf.org/rfc/rfc2790.txt?number=2790). This MIB defines objects that are useful for managing host systems and allows SNMP access to useful host information, such as the storage resources, process table, device information, and the installed software base.

System-level Managed Objects for Applications MIB

The System-level Managed Objects for Applications (SYSAPPL) MIB, **RFC 2287** (http://www.ietf.org/rfc/rfc2287.txt), supports configuration, fault detection, performance monitoring, and control of application software. It provides for tables that define an application as a series of processes and services. This includes objects for applications installed on the system, elements and processes that are included in an application, and current and previously run applications.

For more detailed information about monitoring and managing a Unified ICM/CCE deployment, see the *Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* available at **http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html**.

Chapter 2

Cisco SNMP Installation and Basic Configuration

Installation Prerequisites for SNMP Support

Unified ICM/CCE SNMP support is automatically installed during the course of normal setup. No extra steps need be taken *during* setup for SNMP support to be enabled. However, Microsoft Windows SNMP optional components must be installed on Unified ICM/CCE servers for any SNMP agents to function.

Install the appropriate Microsoft Windows SNMP component(s) before installing any Unified ICM CCE components that require SNMP monitoring. Following are the instructions to install the Microsoft Windows SNMP component are below.

Note: The Microsoft SNMP component(s) are required for Cisco SNMP support. The Microsoft Windows SNMP service is disabled as part of web setup and is replaced by the Cisco Contact Center SNMP Management service to process SNMP requests in its place. The Cisco Contact Center SNMP Management service provides for more sophisticated SNMP capabilities than the standard Microsoft SNMP Service.

How to install the Microsoft Windows SNMP Components on Windows 2003 Server

Complete the following steps to install the Windows SNMP components on Windows 2003 Server.

Note: You will need the Windows 2003 Server CD to complete this task.

Step 1 Click **Start** > **Settings** > **Control Panel** > **Add/Remove Program Files.**

Note: You might only need to click **Start** > **Control Panel** > **Add or Remove Programs**, depending on the Windows Theme you are using.

Step 2 Click **Add/Remove Windows Components**.

Step 3 In the **Windows Components Wizard** window, scroll down and highlight **Management and Monitoring Tools**.

Step 4 Click **Details**.

Step 5 Check the box next to **Simple Network Management Protocol**.

Step 6 Check the box next to **WMI Windows Installer Provider**.

Step 7 Click **OK** and follow the directions on screen. You might be asked to insert your Windows 2003 CD. Do so if prompted.

Cisco Contact Center SNMP Solution Configuration

The Cisco Contact Center SNMP solution is configurable from a Microsoft Management Console (MMC) Snap-in.

Basic Configuration

While all SNMP components are installed and enabled by default, the device is not manageable via an NMS until the solution is properly configured. For security reasons, certain parameters are not configured by default.

The system administrator must configure the following to grant access to the agents and enable the receipt of SNMP notifications:

1. Configure the Community Name or User Names:
   - If you are using SNMP version 1 or version 2c, at least one community string must be configured on each Unified ICM/CCE server to be managed (see below), OR
   - If using SNMP version 3, at least one user name must be configured on each Unified ICM/CCE server to be managed (see below).
2. Configure General Properties. See Configuring General Properties (page 13).
3. For trap forwarding, an SNMP trap destination must be configured on each Unified ICM/CCE Logger server. You can also optionally add a Syslog Destination. See Configuring Trap and Syslog Destinations (page 15).

All properties can be configured using the Cisco SNMP Agent Management MMC Snap-in.

Note: Some diagnostic tools may use SNMP locally to gather information about the system using one of the community strings configured for Windows SNMP. These community strings are not added to the Contact Center SNMP configuration, which will cause SNMP requests from these diagnostic tools to fail. All communities configured for Windows SNMP should be added to the Contact Center SNMP configuration. It is not necessary for the Windows SNMP

service to be started or enabled. The Windows SNMP communities can be found in the "Security" tab by selecting "properties" for the Windows SNMP service from the list of Windows services.

How to add the Cisco SNMP Agent Management Snap-in

You can configure Cisco SNMP Agent Management settings using a Windows Management Console Snap-in. To add the Snap-in and change Cisco SNMP Management settings:

Step 1 From the Start menu select **Run...**.

Step 2 In the Start box type in **`mmc`** and press ENTER.

Step 3 From the Console, select **`File > Add/Remove Snap-in`**

A new window appears.

Step 4 From the **Standalone** tab, verify **Console Root** is selected in the **Snap-ins added to:** field and click **`Add.`**

Step 5 In the Add Snap-in window scroll down and select **`Cisco SNMP Agent Management`**.

Step 6 In the Add Snap-in window click **`Add`**.

Step 7 In the Add Snap-in window click **`Close`**.

Step 8 Click **`OK`** in the Add/Remove Snap-in window.

The **`Cisco SNMP Agent Management`** Snap-in is now loaded in the console.

Saving the Snap-in View

Once you have loaded the Cisco SNMP Agent Management MMC Snap-in, you can save that console view to a file (with a .MSC file extension) that can be launched directly, instead of repeatedly adding the Snap-in to a new MMC console view. To do so, select the **Console > Save As** menu; a Save As dialog will appear.

Select a memorable file name such as **Cisco SNMP Agent Management.msc** (retain the .msc file extension) and save the file to the desired location. The Administrative Tools (start) menu is the default location, which makes it conveniently available for later access via the Start menu.

Configuring Community Names for SNMP V1 and V2c

If you are using SNMP v1 or v2c you must configure a Community Name so that Network Management Stations (NMSs) can access the data provided by your server. These names are left blank during installation for security reasons.

SNMP Community Names are used to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same Community Name.

To configure the Community Name for SNMP v1 and v2c:

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **Community Names (SNMP v1/v2c)** in the left pane under Cisco SNMP Agent Management.

Community Name, SNMP Version, and Restricted Access columns appear in the right pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.

A dialog box appears.

Step 5 Click **Add new Community**.

Step 6 In the dialog box, under **Community Information**, provide a community name.

Step 7 Select the **SNMP Version** by selecting the radio box for SNMP V1 or SNMP V2c.

Step 8 Optionally, enter one or more IP addresses in the IP Address entry field (containing "dots") and click **Insert** to enable the access solely for this community from the NMS with the IP Address provided.

Step 9 Click **Save**.

The community name appears in the **Configured Communities** section at the top of the dialog box.

Note: You can remove the community name by highlighting the name in the **Configured Communities** section and clicking **Remove Community**.

Changes become effective when you click **OK**.

Configuring User Names for SNMP v3

If you are using SNMP v3 you must configure a User Name so that Network Management Stations (NMSs) can access the data provided by your server. By default, these names are left blank for security reasons.

To configure a User Name for SNMP v3:

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **User Names (SNMP v3)** in the left pane under Cisco SNMP Agent Management.

User Name, Authentication, Privacy, and Restricted Access columns appear in the right pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.

A dialog box appears.

Step 5 Click **Add User**.

Step 6 In the **User Configuration** text box enter a user name.

Step 7 If you wish to use SNMP v3 authentication, check **Required?** under Authentication, choose an authentication protocol, then enter and confirm a password.

This setting encrypts the password information as it is sent over the network.

Note: These settings must also be used on your NMS to access SNMP data from this server.

Step 8 If you wish to use SNMP v3 privacy, check **Required?** under Privacy, choose an encryption type, and enter and confirm a password.

Note:

- This setting encrypts all SNMP information as it is sent over the network. If privacy is configured, authentication is required, but authentication can be configured without configuring privacy.
- These settings must also be used on your NMS to access SNMP data from this server.

Step 9 Optionally, enter one or more IP addresses in the IP Address entry field (containing "dots") and click **Insert** to enable access solely from the NMS with the IP Address provided.

Step 10 Click **Save**.

The User Name appears in the **Configured Users** section at the top of the dialog box.

Note: You can remove the User Name by highlighting the name in the **Configured Users** section and clicking **Remove User**.

Changes become effective when you click **OK**.

See Also

Configuring Trap and Syslog Destinations on page 15

Configuring General Properties

Use the Cisco SNMP Agent Management Snap-in (page 10) to access the configuration screens.

Configuring General Information Properties for Cisco SNMP Agent Management

You can configure general information properties for Cisco SNMP within the Cisco SNMP Agent Management Snap-in.

To configure general information properties:

Step 1 In the Cisco SNMP Agent Management Snap-in, expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 2 Highlight **General Information** in the left pane under Cisco SNMP Agent Management.

Attribute, Value, and Description columns appear in the right pane.

Step 3 Right click on the white space in the right pane and choose **Properties**.

A dialog box appears.

Step 4 You can change the following properties in the **SNMP System Information** section of the General Information Properties dialog box.

Table 1: SNMP System Information Properties

Property	Description
System name	The fully qualified domain name of the system. If empty this will be automatically filled in.
System Location	A text area to describe the location of the hardware. For example **`Building 5, Floor 3, Room 310`**.
System Contact	The name, email address and/or telephone number of the system contact. Enter anything that will aid an NMS user in contacting the system administrator.
System Description	A brief description of this system.
SNMP Port Number	The default port for SNMP applications is UDP 161. If your NMS uses a different port you can change that value here.
Enable Authentication Traps	Check if you wish to enable Authentication Traps. When a device receives an authentication that fails, a trap is sent to the NMS.

Step 5 You can change the Windows Execution Priority of the Cisco SNMP agents in the **Agent Performance** section under **Execution Priority**. The default is *Below Normal*. You can further lower it by setting it to *Low*. Keep the settings at the default levels unless you are seeing a significant performance impact.

Step 6 You can also further modify SNMP Agent Performance by changing the number of *Concurrent Requests*, *Subagent Wait Time* (in seconds), and *Subagents*. the default values are **5**, **25**, and **25** respectively. Keep the settings at the default levels unless you are seeing a significant performance impact.

Definitions:

- Concurrent requests: The maximum number of SNMP requests that can be concurrently processed by a subagent. Any pending requests above this value are queued.
- Subagent Wait Time: The maximum number of seconds that the master agent waits for a subagent response.
- Subagents: The maximum allowable subagents that the master agent loads.

Step 7 You can change the amount of information written to the SNMP logs by choosing Verbose (most information), Normal (Default), or Terse (least information). This value should only be changed under direction from Cisco Technical Assistance (TAC).

Note: Logs can be retrieved using Cisco Analysis Manager.

Step 8 Click **OK** to save any changes you have made.

Configuring Trap and Syslog Destinations

Use the Cisco SNMP Agent Management Snap-in (page 10) to access the configuration screens.

Note: Restarting the service does not clear conflicts between host address and SNMP destination. When there is a conflict between the host address list and the SNMP Trap Destination, if you delete the items from the host address list, and restart the service, the configuration is reset.

Configuring SNMP Trap Destinations

You can configure SNMP Trap Destinations for SNMP v1, SNMP v2c and SNMP v3. A Trap is a notification used by the SNMP agent to inform the NMS of a certain event.

Follow these steps to configure the trap destinations:

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **Trap Destinations** in the left pane under Cisco SNMP Agent Management.

Trap Entity Name and SNMP Version columns appear in the right pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.

A dialog box appears.

Step 5 Click **Add Trap Entity**.

Step 6 Under **Trap Entity Information** select the SNMP version radio box for the version of SNMP used by your NMS.

Step 7 Provide a name for the trap entity in the **Trap Entity Name** field.

Step 8 Select the SNMP Version Number.

Step 9 Select the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing users/community names that have already been configured.

Step 10 Enter one or more IP addresses in the IP Address entry field (containing "dots") and click **Insert** to define the destination(s) for the trap(s).

Step 11 Click **Save** to save the new trap destination.

The Trap Entity Name appears in the **Trap Entities** section at the top of the dialog box.

Note: You can remove the Trap Entity by highlighting the name in the **Trap Entities** section and clicking **Remove Trap Entity**.

Step 12 Changes become effective when you click **OK**

Configuring Syslog Destinations

You can configure Syslog destinations for SNMP from the Cisco SNMP Agent Management Snap-in. The syslog feed is only available on the Unified ICM/CCE Logger Node.

Follow these steps to configure Syslog destinations:

Step 1 Follow the steps in **How to install the Cisco SNMP Agent Management Snap-in** to access the Cisco SNMP Agent Management settings.

Step 2 Expand **Cisco SNMP Agent Management** in the left pane of the MMC plugin.

Step 3 Highlight **Syslog Destinations** in the left pane under Cisco SNMP Agent Management.

ICM Instance Name, Feed Enabled, Collector Address, Port, and Ping Disabled columns appear in the right pane.

Step 4 Right click on the white space in the right pane and choose **Properties**.

A dialog box appears.

Step 5 Select an Unified ICM/CCE Instance from the list box.

Step 6 Check the **Enable Feed?** checkbox.

Step 7 Enter an IP Address or Host Name in the **Collector Address** field.

Step 8 Optionally, enter the collector port number on which the Syslog collector is listening in the **Collector Port** field. The default port is 514.

Step 9 Optionally, check the **Disable Ping Tests?** checkbox.

Step 10 Click **Save**.

Step 11 Changes become effective when you click **OK** and restart the logger.

Starting, Stopping, and Confirming the SNMP Service

In general, the Cisco Contact Center SNMP Management Service is always running.

To confirm that the Cisco Contact Center SNMP Management Service is running or to restart or stop it, follow these steps:

Step 1 From the Windows desktop, choose **Start** > **Settings** > **Control Panel**

Step 2 Double-click **Administrative Tools**.

Step 3 Double-click **Services**.

The Services window appears.

Step 4 Look at the Status field in the **Cisco Contact Center SNMP Management service** row.

If this field displays "Started," the Cisco Contact Center SNMP Management Service is running. If this field is blank, the Cisco Contact Center SNMP Management Service is not running.

To start the Cisco Contact Center SNMP Management Service, right-click **Cisco Contact Center SNMP Management** and choose **Start**.

To stop the Cisco Contact Center SNMP Management Service, right-click SNMP Service and choose **Stop**.

To restart the Cisco Contact Center SNMP Management Service, right-click **Cisco Contact Center SNMP Management** and choose **Restart**.

SNMP Link to Support Tools

The Cisco Unified ICM/CCE SNMP implementation can detect the presence of a Cisco Support Tools 2.x server. Cisco Support Tools is no longer supported in Release 8.5(1) in lieu of the Cisco solution serviceability tool Analysis Manager. Although Support Tools is no longer supported, the SNMP link for the Support Tools server is deprecated in the 8.x CISCO-CONTACT-CENTER-APPS-MIB. This object will still be populated on servers that have been upgraded from Release 8.0(1) and have a Support Tools Node Agent installed.

Note: This is only applicable if Support Tools software is installed on the node being managed.

Finding the Support Tools URL from within your SNMP Monitoring Application

You can read the support tools URL from your SNMP Monitoring Application once the Support Tools URL has been configured on the server.

Follow these steps to find the Support Tools URL:

Step 1 From your SNMP Monitoring Application, select the server for which you want to determine the Support Tools URL.

Step 2 Use the Applications MIB Browser, and drill down through the following folders:

`MIBS > private > cisco > ciscoMgmt > ciscoCccaMIB`

Step 3 Highlight **`cccaSupportToolsURL`** and click the generic SNMP Monitoring Application's button for retrieving a field value.

Note: If the Support Tools URL has not been configured on the server, then the SNMP Monitoring Application will return the string **`cccaSupportToolsURL.0=`**.

Chapter 3

Responding to Alarms

Unified ICM/CCE Notifications

Notification Mechanism

SNMP notifications are error or warning events generated by component processes and are delivered to a network management station (NMS) via SNMP. The MIB componenet notification types describe objects which allow for correlating events and for easily identifying the component that generated the event.

SNMP notifications are derived from the event message stream continually being generated by the various Cisco Unified ICM/CCE processes throughout the system. These processes report events of interest to the central database as they occur. Just before being placed in the central database, the event stream is intercepted by a process called the Customer Support Forwarding Service (CSFS) that watches for events of significant interest which should be treated as SNMP notifications.

Most Unified ICM/CCE SNMP notifications are “stateful” in that the notification reports a “raise” or a “clear” state for a given error or warning event. Stateful notifications may or may not require system administrator intervention; often, the Unified ICM/CCE system’s fault tolerance features allow the system to recover automatically. Other notifications are “stateless” (e.g. “single-state raise”) whereby a “clear” event will not be forthcoming and resolution requires system administrator intervention.

The CSFS process running on the logger generates an event feed to a Cisco SNMP subagent which converts the event data into an SNMP notification in the format defined by a Cisco Unified ICM/CCE MIB. For Unified ICM/CCE 8.0(1), notifications are defined by the CISCO-CONTACT-CENTER-APPS-MIB.

Prior versions of Unified ICM/CCE (and IPCC) generate notifications defined by the CISCO-ICM-ALARMEX-MIB. CISCO-ICM-ALARMEX-MIB notifications were deprecated

in the 7.x release and are not supported in the 8.0(1) release. For 8.0(1) and subsequent releases, NMS rules must be altered to conform to the CISCO-CONTACT-CENTER-APPS-MIB format.

Event Correlation

Events are sent to the NMS as a series of **raises** and **clears**. A single **clear** can clear multiple **raises**. Events that relate to each other are given the same **correlation ID**.

The correlation ID is a combination of the event class name and the event component ID. The component ID (available in the MIB) is a combination of the class name and any substitution strings (arguments) that are passed into it.

To provide an organized view of events you need to create rules in your NMS to map events to a state-based object, using the correlation IDs to associate the events into like groups. When a clear event comes into the NMS you can cancel all previous raises that have the same correlation ID as the clear.

The raises and clears are defined in the file **`<INSTALL_DRIVE>/icm/snmp/ccca-Notifications.txt`**, which is found in the SNMP folder of your installation.

Note: Some raises have no automatic clears and must be manually cleared. You should set up an escalation path within your NMS for events that do not have a corresponding clear.

The ccca-Notifications.txt file contains a list of all alarms and each alarm contains an ccaEventState (Raise/Clear) and CorrelationID. Based on CorrelationID, you can determine if a Raise event has a corresponding Clear event or must be manually cleared.

This information is also available as part of the event; **`RAISE=9`** requires a manual Clear and **`RAISE=4`** is an event that has a corresponding Clear.

Enabling SNMP Notifications

Unified ICM/CCE 8.0(1) SNMP subagents are installed and enabled by default. To enable the flow of notifications to the management station, on the Unified ICM/CCE Logger node, the installer must first configure a community string (SNMP v1/v2c) or a user name (SNMP v3), and a trap destination. These properties specify security parameters to use for notification transport and the network management station that will receive the Unified ICM/CCE notifications.

Chapter 4

Cisco Discovery Protocol Driver

Cisco Discovery Protocol (CDP) Driver Installation/Uninstall

Supported Unified ICM/CCE systems use the Cisco Discovery Protocol (CDP) to periodically send out CDP messages to a designated multicast address. These messages contain information such as device identification, interface name, system capabilities, SNMP agent address, and time-to-live. Any Cisco device with CDP support can locate a Cisco Unified ICM/CCE server by monitoring these periodic messages.

You must install the CDP Driver if you want to use the Cisco CDP SNMP features available on Cisco MCS-78xx Series servers.

Note: The CDP Driver is automatically installed on Unified CCE Nodes. Unified ICM CCE/CCH must manually install the driver.

CDP Driver Installation.

Warning: DO NOT install the CDP Driver on any hardware other than Cisco MCS-78xx Series servers. Installation on other hardware can cause severe OS instability.

Follow these steps to install the CDP Driver:

Step 1 From the server on which you want to install the CDP Driver, use a **Command Prompt** and navigate to **`<INSTALL_DRIVE>\icm\snmp`**.

Step 2 Execute the application **`cdpinstall.bat`** and follow the on-screen instructions.

Note: If you execute this program by double-clicking it from Windows Explorer, you will not be able to see any messages that may appear, as Windows will close the command window when it completes execution.

Step 3 Reboot the system.

CDP Driver Uninstallation

To uninstall the CDP Driver:

Step 1 From the server on which you want to install the CDP Driver, use a **Command Prompt** and navigate to **`<INSTALL_DRIVE>\icm\snmp`**.

Step 2 Execute the application **`cdpUninstall.bat`** and follow the on-screen instructions.

Note: If you execute this program by double-clicking it from Windows Explorer you will not be able to see any messages that may appear, as Windows will close the command window when it completes execution.

Step 3 Reboot the system.

Default CDP Settings

The following table shows the default CDP settings:

Table 2: Default CDP Settings

Description	Default Value
Default Transmit Frequency	60 seconds
Default Time to Live	180 seconds
Default State	CDP advertisement enabled