SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions

7.0(0)

February 2007

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright Â© 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

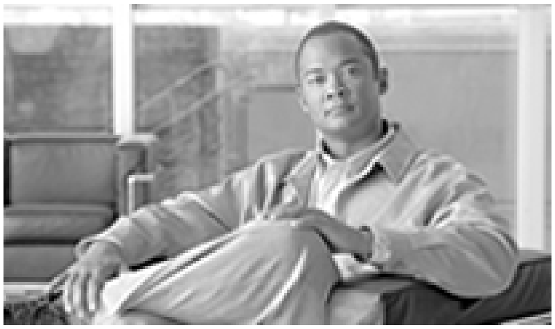
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Table of Contents



Preface

Purpose

This document describes the new SNMP feature support found in ICM/IPCC 7.0(0).

Audience

This document is intended for System Installers, ICM/IPCC 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:

- *ICM Installation Guide for Cisco ICM Enterprise Edition*
- *Staging and Active Directory Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*
- *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*
- *IPCC Administration Guide for Cisco IPCC Enterprise Edition*
- *ICM/IPCC Pre-Installation Planning Guide*
- *Installation Guide for System IPCC*

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*.

Convention	Description
`window font`	Window font, such as Courier, is used for the following: • 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL::

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at **tech-doc-store-mkpl@external.cisco.com** or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems Attn: Customer Document Ordering 170 West Tasman Drive San Jose, CA 95134-9883

We appreciate your comments.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can register to receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information. Access the tool at this URL: **http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en**.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only: security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies: psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Note: We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note: Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting**show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly

To open a service request by telephone, use one of the following numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) - Your network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) - Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) - Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) - You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

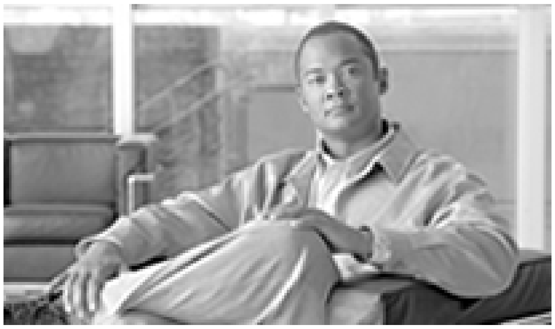
  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html



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 7.0(0) ICM/IPCC components are valid managed devices:

  - Routers
  - Loggers
  - Peripheral Gateways (PGs)
  - Distributor Admin Workstation (AWs)[1]
  - CTI Gateways (CGs)

[1] SNMP support is available for Distributor AWs only. Client AWs are not supported.

  - CTI OS Servers

- 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 for forwarding to an SNMP Management Station. Subagents collect information for various components and then forwards that information to a master agent.

  Release 7.0(0) ICM/IPCC supports the following agents:

  - SNMP Master Agent
  - ICM/IPCC Application(CISCO-CONTACT-CENTER-APPS-MIB) Subagent
  - Cisco ICM/IPCC Alarm (CISCO-ICM-ALARMEX-MIB) Subagent[2]
  - Platform Subagent(s)[3]
  - System Applications Instrumentation (SYSAPPL-MIB) Subagent
  - Host Resources (HOST-RESOURCES-MIB) Subagent
  - Cisco Discovery Protocol (CISCO-CDP-MIB) Subagent[4]

- 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 ICM/IPCC SNMP works with SNMP standards-compliant NMSs.

- A Management Information Base (MIB) designates a collection of information that is organized hierarchically. You access MIBs using the Simple Network Management Protocol, SNMP. 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 ICM/IPCC 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)

[2] For ICM/IPCC Logger Servers only. Deprecated, for backward compatibility only.

[3] Provided by your hardware vendor

[4] Only supported on Cisco MCS-78xx Hardware

See Detailed MIB Descriptions (page 11)

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 ICM/IPCC Enterprise/Hosted Edition installation.

Components include:

- Router (and a table of NICs)
- Logger
- Peripheral Gateway (PG) (and a table of PIMs)
- Distributor Admin Workstation
- CTI Gateway (CG)
- CTI OS Server

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.

Cisco ICM/IPCC Alarm MIB

The ICM/IPCC Alarm MIB (CISCO-ICM-ALARMEX-MIB) is installed when you install the Logger component.

The ICM/IPCC Alarm capability is made up of a set of alarm-able objects within a Cisco ICM/IPCC system. The ICM/IPCC Alarm MIB Subagent can send these messages to an NMS.

See Also

ICM/IPCC Notifications on page 23

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

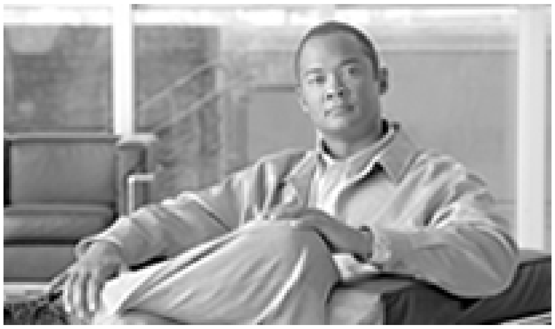
Cisco Discovery Protocol (CDP) Driver Installation/Uninstall on page 27

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.

SYSAPPL 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.



Chapter 2

Cisco SNMP Installation and Basic Configuration

Installation Prerequisites for SNMP Support

ICM/IPCC 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 ICM/IPCC servers for any SNMP agents to function.

Install the appropriate Microsoft Windows SNMP component(s) before installing any ICM or IPCC Enterprise components that require SNMP monitoring. Instructions for installing 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 ICM 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 Component on Windows 2000 Server

Complete the steps below to install the Windows SNMP component on Windows 2000 Server.

Note: You will need to have the Windows 2000 Server CD available to complete this task.

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

Step 2 Click **Add/Remove Windows Components** on the left-hand side of the window.

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 Click **OK** and follow the directions on screen. You might be asked to insert your Windows 2000 Server CD. Do so if prompted.

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

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

Note: You will need to have the Windows 2003 Server CD available 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 which Windows Theme that you are using.

Step 2 Click **Add/Remove Windows Components** on the left-hand side of the window.

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 using SNMP version 1 or version 2c, at least one community string must be configured on each ICM/IPCC server to be managed (see below), OR
   - If using SNMP version 3, at least one user name must be configured on each ICM/IPCC server to be managed (see below).
2. Configure General Properties. See Configuring General Properties (page 18).
3. Fo trap forwarding, an SNMP trap destination must be configured on each ICM/IPCC Logger server. You can also optionally add a Syslog Destination. See Configuring Trap and Syslog Destinations (page 20).

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 20

Configuring General Properties

Use the Cisco SNMP Agent Management Snap-in (page 14) 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.

Property	**Description**
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 Check **Send CISCO-ICM-ALARMEX-MIB Traps** if you wish to send the deprecated notifications defined by this MIB. Otherwise, the notifications found in CISCO-CONTACT-CENTER-APPS-MIB.my are used.

The notifications are explained in **`<INSTALL_DRIVE>/icm/snmp/ccca-Notifications.txt`**.

Step 6 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 7 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 8 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 Support Tools.

Step 9 Click **OK** to save any changes you have made.

Configuring Trap and Syslog Destinations

Use the Cisco SNMP Agent Management Snap-in (page 14) to access the configuration screens.

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.

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 ICM/IPCC Logger Node.

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 ICM/IPCC 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 ICM/IPCC SNMP implementation can detect the presence of a Cisco Support Tools 2.0(0) server. This features enables you to easily see which Cisco Support Tools server is associated with an ICM/IPCC component right from your SNMP monitoring tool.

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.

To find the Support Tools URL:

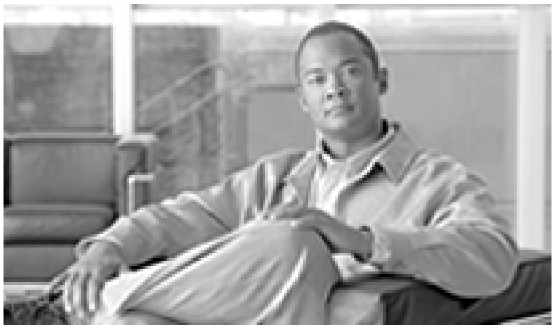
Step 1 From your SNMP Monitoring Application, select the server for which you want to determine the Support Tools URL.

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

ICM/IPCC 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. MIB 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 ICM/IPCC 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 ICM/IPCC 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 ICM/IPCC 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 ICM/IPCC MIB. For ICM/IPCC 7.0(0), notifications are defined by the CISCO-CONTACT-CENTER-APPS-MIB.

Prior versions of ICM/IPCC generate notifications defined by the CISCO-ICM-ALARMEX-MIB. CISCO-ICM-ALARMEX-MIB notifications have been deprecated in the 7.0(0) version for backward compatibility, however, NMS rules should be altered in due time 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

ICM/IPCC 7.0(0) SNMP subagents are installed and enabled by default. To enable the flow of notifications to the management station, on the ICM/IPCC 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 ICM/IPCC notifications.

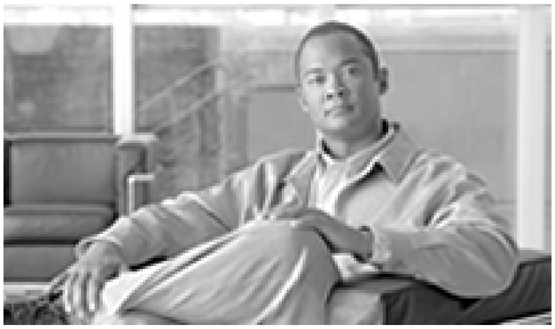
Support for CISCO-ICM-ALARMEX-MIB Notification

To support backwards compatibility, notifications that conform to the CISCO-ICM-ALARMEX-MIB are supported but deprecated for the ICM/IPCC 7.0(0) release. This support allows customers to upgrade from previous releases of ICM/IPCC without requiring immediate changes to rules on the NMS. Support for this deprecated MIB also retains integration support for the Cisco Internet Service Node (ISN) or Customer Voice Portal (CVP) product.

Note: ISN/CVP uses the SDDSN service to transport events. These traps are defined by the CISCO-ISN-ALARM-MIB.

The CISCO-ICM-ALARMEX-MIB and the CISCO-ISN-ALARM-MIB define traps that are not within the Cisco Systems, Inc. “enterprises” object identifier (OID). These traps are within the “enterprises.1539” (GeoTel Communications) OID and are processed by the AlarmEx subagent. The AlarmEx subagent is a dynamic link library (DLL) installed on the ICM/IPCC Logger and/or the SDDSN server.

Note: In order to correctly interpret the Cisco generated notifications, the appropriate ICM/IPCC SNMP MIB must be loaded by the NMS. Additionally, if another product (such as ISN/CVP) is being monitored, then the appropriate MIB for that product must also be loaded.



Chapter 4

Cisco Discovery Protocol Driver

Cisco Discovery Protocol (CDP) Driver Installation/Uninstall

Supported ICM/IPCC 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 ICM/IPCC 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 System IPCC Nodes. Enterprise and Hosted ICM and IPCC systems 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.

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