CHAPTER 11

Configuring SNMP on the Cisco HCM-F Platform

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested). To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3.

This chapter, which describes how to configure SNMP v3 so the network management system can monitor Cisco HCM-F, contains the following topics:

SNMP Configuration Checklist

Table 11-1 provides an overview of the steps for configuring SNMP.

Table 11-1 SNMP Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS
Step 2	In the CLI, verify that the system started the SNMP services, including: • SNMP Master Agent • Native Agent • System Application Agent • Cisco Syslog Agent • MIB2 Agent • Host Resources Agent	In the command line interface, enter the following command: utils service list
Step 3	Configure the SNMP user.	SNMP Users, page 11-3
Step 4	Configure the notification destination for traps or informs.	• SNMP Trap Notification Destinations, page 11-4 • SNMP Inform Notification Destination, page 11-5

Table 11-1 SNMP Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Configure the system contact and location for the MIB2 system group.	MIB2 System Group, page 11-7
Step 6	Configure trap settings for CISCO-SYSLOG-MIB.	Use these guidelines to configure CISCO-SYSLOG-MIB trap settings on your system: • Set clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) to true by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID to true from the linux command line using: snmpset -c <*community string*> -v2c <*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 You can also use any other SNMP management application for the SNMP Set operation. • Set clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) value by using the SNMP Set operation; for example, use the net-snmp set utility to set this OID value from the linux command line using: snmpset -c public -v2c 1<*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <*value*> Enter a severity number for the <value> setting. Severity values increase as severity decreases. A value of 1 (Emergency) indicates highest severity, and a value of 8 (Debug) indicates lowest severity. Syslog agent ignores any messages greater than the value that you specify; for example, to trap all syslog messages, use a value of 8.
Step 7	Restart the SNMP Master Agent service. (Optional) **Tip** The system automatically restarts the SNMP Master Agent after you execute the utils snmp config commands.	At the command line, enter the following command: utils service start SNMP Master Agent
Step 8	On the NMS, configure the Cisco HCM-F trap parameters.	• SNMP Management Information Base (MIB), page 11-8 • SNMP product documentation that supports the NMS

Additional Information

See the "Related Topics" section on page 11-10.

SNMP Users

Table 11-2 shows the commands that you need to work with SNMP users on the Cisco HCM-F platform:

Table 11-2 Trace CLI Commands

Task	Command
List the SNMP users.	utils snmp config user 3 list
Add an SNMP user.	utils snmp config user 3 add The system prompts you for the parameters. See Table 11-3 for parameter names and descriptions.
Update an SNMP user.	utils snmp config user 3 update The system prompts you for the parameters. See Table 11-3 for parameter names and descriptions.
Delete an SNMP user.	utils snmp config user 3 delete The system prompts you for the parameters. See Table 11-3 for parameter names and descriptions.

SNMP User CLI Parameters

Table 11-3 describes the SNMP user parameter settings for V3.

Table 11-3 SNMP User Parameter Settings for V3

Field	Description
username	The name of the user for which you want to provide access. The name can contain up to 32 characters and can contain any combination of alphanumeric characters, hyphens (-), and underscore characters (_). **Tip** Enter users that you have already configured for the network management system (NMS).
authprotocol	Authentication protocol. To specify HMAC-SHA, enter SHA.
authpassphrase	Specifies the authentication protocol password. The password must contain at least 8 characters.
privprotocol	Specifies the privacy protocol, either AES128, AES192, or AES256
privpassphrase	Specifies the privacy protocol password. The password must contain at least 8 characters.

Table 11-3 SNMP User Parameter Settings for V3 (continued)

Field	Description
accessprivilege	Enter one of the following options for the access level: • **ReadOnly**—The user can only read the values of MIB objects. • **ReadWrite**—The user can read and write the values of MIB objects. • **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages. • **None**—The user cannot read, write, or send trap information. **Tip** To change the trap configuration parameters, you need to configure a user with NotifyOnly, ReadNotifyOnly, or ReadWriteNotify privileges.
ipaddress1	Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts.
ipaddress2	Specify an IP address from which to accept packets. The default specifies to accept packets from all hosts.

Additional Information

See the "Related Topics" section on page 11-10.

SNMP Trap Notification Destinations

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

The following section applies to SNMP V3 notification destination configuration.

Table 11-4 shows the commands that you need to work with SNMP trap notification destinations on the Cisco HCM-F platform:

Table 11-4 SNMP Trap Notification Destinations CLI Commands

Task	Command
List trap notification destinations.	utils snmp config trap 3 list
Add a v3 trap notification destination that is associated with a configured v3 username.	utils snmp config trap 3 add The system prompts you for the parameters. See Table 11-5 for parameter names and descriptions.

Table 11-4 SNMP Trap Notification Destinations CLI Commands (continued)

Task	Command
Update a trap notification destination.	utils snmp config trap 3 update The system prompts you for the parameters. See Table 11-5 for parameter names and descriptions.
Delete a trap notification destination.	utils snmp config trap 3 delete The system prompts you for the parameters. See Table 11-5 for parameter names and descriptions.

Trap Notification Destination Parameter Settings

Table 11-5 describes the trap notification destination parameter settings for V3.

Table 11-5 Trap Notification Destination Parameter Settings for V3

Field	Description
ipaddress	The host IP address of the notification destination.
portno	The notification-receiving port number on the destination server.
oldportno	The notification-receiving port number on the destination server that is currently configured.
newportno	The notification-receiving port number on the destination server that you want to use when updating the trap notification destination.
username	Specifies the SNMP user associated to the notification destination.

Additional Information

See the "Related Topics" section on page 11-10.

SNMP Inform Notification Destination

An SNMP agent sends notifications to NMS in the form of traps or informs to identify important system events. Traps do not receive acknowledgments from the destination whereas informs do receive acknowledgments.

Table 11-6 describes the inform notification destination configuration settings for V3.

Table 11-6 SNMP Inform Notification Destination CLI Commands

Task	Command
List inform notification destinations.	utils snmp config inform 3 list
Add a v3 inform notification destination.	utils snmp config inform 3 add The system prompts you for the parameters. See Table 11-7 for parameter names and descriptions.

Table 11-6 SNMP Inform Notification Destination CLI Commands (continued)

Task	Command
Update an inform notification destination.	utils snmp config inform 3 update The system prompts you for the parameters. See Table 11-7 for parameter names and descriptions.
Delete an inform notification destination.	utils snmp config inform 3 delete The system prompts you for the parameters. See Table 11-7 for parameter names and descriptions.

Inform Notification Destination Parameter Settings

Table 11-7 Inform Notification Destination Parameter Settings for V3

Field	Description
ipaddress	The host IP address of the notification destination.
portno	The notification-receiving port number on the destination server.
oldportno	The notification-receiving port number on the destination server that is currently configured.
newportno	The notification-receiving port number on the destination server that you want to use when updating the inform notification destination.
username	Specifies the SNMP user associated to the notification destination.
oldusername	Specifies the v3 username that is currently associated with the inform.
newusername	Specifies the v3 username that you want to associate with the inform.
deleteuserconf	Specifies confirmation for deleting the old user, either Y or N.
authprotocol	Authentication protocol. To specify HMAC-SHA, enter SHA.
authpassphrase	Specifies the authentication protocol password. The password must contain at least 8 characters.
privprotocol	Specifies the privacy protocol, either AES128, AES192, or AES256
privpassphrase	Specifies the privacy protocol password. The password must contain at least 8 characters.
accessprivilege	Enter one of the following options for the access level: • **ReadWriteNotify**—The user can read and write the values of MIB objects and send MIB object values for a trap and inform messages. • **NotifyOnly**—The user can only send MIB object values for trap and inform messages. • **ReadNotifyOnly**—The user can read values of MIB objects and also send the values for trap and inform messages.
engineId	Specifies the remote engine ID of the server to which to send inform messages.

Additional Information

See the "Related Topics" section on page 11-10.

MIB2 System Group

You can use the CLI to configure the system contact and system location objects for the MIB-II system group. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

Table 11-8 shows the commands that you need to work with MIB2 system groups on the Cisco IME server:

Table 11-8 MIB2 CLI Commands

Task	Command
List the MIB2 system group configuration.	utils snmp config mib2 list
Add a MIB2 system group.	utils snmp config mib2 add The system prompts you for the parameters. See Table 11-9 for parameter names and descriptions.
Update a MIB2 system group.	utils snmp config mib2 update The system prompts you for the parameters. See Table 11-9 for parameter names and descriptions.
Delete a MIB2 system group.	utils snmp config mib2 delete The system prompts you for the parameters. See Table 11-9 for parameter names and descriptions.

MIB2 System Group CLI Parameters

Table 11-9 describes the MIB2 System Group parameter settings.

Table 11-9 MIB2 System Group Parameter Settings

Field	Description
Server	The server for which you want to configure contacts.
SysContact	Specifies a person to notify when problems occur.
SysLocation	Specifies the location of the person that is identified as the system contact.

Additional Information

See the "Related Topics" section on page 11-10.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables).

The SNMP interface provides these Cisco Standard MIBs:

- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

The Simple Network Management Protocol (SNMP) extension agent resides in the server. The SNMP interface also provides these Industry Standard MIBs:

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

Cisco HCM-F SNMP Interface supports the following MIBs.

CISCO-CDP-MIB

Use the CDP subagent to read the Cisco Discovery Protocol MIB, CISCO-CDP-MIB. This MIB enables Cisco HCM-F to advertise itself to other Cisco devices on the network.

The CDP subagent implements the CDP-MIB. The CDP-MIB contains the following objects:

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

Use the System Application Agent to get information from the SYSAPPL-MIB, such as installed applications, application components, and processes that are running on the system.

System Application Agent supports the following object groups of SYSAPPL-MIB:

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

MIB-II

Use MIB2 agent to get information from MIB-II. The MIB2 agent provides access to variables that are defined in RFC 1213, such as interfaces, IP, and so on, and supports the following groups of objects:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

Use Host Resources Agent to get values from HOST-RESOURCES-MIB. The Host Resources Agent provides SNMP access to host information, such as storage resources, process tables, device information, and installed software base. The Host Resources Agent supports the following groups of objects:

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog tracks and logs all system messages, from informational through critical. With this MIB, network management applications can receive syslog messages as SNMP traps:

The Cisco Syslog Agent supports trap functionality with the following MIB objects:

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity

- clogMsgIgnores
- clogMsgDrops

Related Topics

- SNMP Configuration Checklist, page 11-1
- SNMP Users, page 11-3
- SNMP Trap Notification Destinations, page 11-4
- SNMP Inform Notification Destination, page 11-5
- MIB2 System Group, page 11-7
- SNMP Management Information Base (MIB), page 11-8