CHAPTER 15

Configuring SNMP

This chapter describes how to configure the sensor to use SNMP and SNMP traps. It contains the following sections:

Understanding SNMP

Caution To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures.

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is a simple request/response protocol. The network-management system issues a request, and managed devices return responses. This behavior is implemented by using one of four protocol operations: Get, GetNext, Set, and Trap.

You can configure the sensor for monitoring by SNMP. SNMP defines a standard way for network management stations to monitor the health and status of many types of devices, including switches, routers, and sensors.

You can configure the sensor to send SNMP traps. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message.

Trap-directed notification has the following advantage—if a manager is responsible for a large number of devices, and each device has a large number of objects, it is impractical to poll or request information from every object on every device. The solution is for each agent on the managed device to notify the manager without solicitation. It does this by sending a message known as a trap of the event.

After receiving the event, the manager displays it and can take an action based on the event. For instance, the manager can poll the agent directly, or poll other associated device agents to get a better understanding of the event.

Note Trap-directed notification results in substantial savings of network and agent resources by eliminating frivolous SNMP requests. However, it is not possible to totally eliminate SNMP polling. SNMP requests are required for discovery and topology changes. In addition, a managed device agent cannot send a trap if the device has had a catastrophic outage.

For More Information

For the procedure for having the sensor send SNMP traps, see Assigning Actions to Signatures, page 9-17.

Configuring SNMP General Configuration

This section describes how to configure SNMP, and contains the following topics:

SNMP General Configuration Pane

Note You must be administrator to configure the sensor to use SNMP.

Use the SNMP General Configuration pane to configure the sensor to use SNMP.

SNMP General Configuration Pane Field Definitions

The following fields are found in the SNMP General Configuration pane:

- Enable SNMP Gets/Sets—If checked, allows SNMP gets and sets.
- SNMP Agent Parameters—Configures the parameters for SNMP agent.
  - Read-Only Community String—Identifies the community string for read-only access.
  - Read-Write Community String—Identifies the community string for read and write access.
  - Sensor Contact—Identifies the contact person, contact point, or both for the sensor.
  - Sensor Location—Identifies the location of the sensor.
  - Sensor Agent Port—Identifies the IP port of the sensor. The default is 161.
  - Sensor Agent Protocol—Identifies the IP protocol of the sensor.

    The default is UDP.

Configuring SNMP General Parameters

To set the general SNMP parameters, follow these steps:

Step 1 Log in to IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SNMP > General Configuration**.

Step 3 To enable SNMP so that the SNMP management workstation can issue requests to the sensor SNMP agent, check the **Enable SNMP Gets/Sets** check box.

Step 4 Configure the SNMP agent parameters:

These are the values that the SNMP management workstation can request from the sensor SNMP agent.

a. In the Read-Only Community String field, enter the read-only community string.

The read-only community string helps to identify the sensor SNMP agent.

b. In the Read-Write Community String field, enter the read-write community string.

The read-write community string helps to identify the sensor SNMP agent.

Note The management workstation sends SNMP requests to the sensor SNMP agent, which resides on the sensor. If the management workstation issues a request and the community string does not match what is on the senor, the sensor will reject it.

c. In the Sensor Contact field, enter the sensor contact user ID.

d. In the Sensor Location field, enter the location of the sensor.

e. In the Sensor Agent Port field, enter the port of the sensor SNMP agent.

The default SNMP port number is 161.

f. From the Sensor Agent Protocol drop-down list, choose the protocol the sensor SNMP agent will use.

The default protocol is UDP.

Tip To discard your changes, click **Reset**.

Step 5 Click **Apply** to apply your changes and save the revised configuration.

Configuring SNMP Traps

This section describes how to configure SNMP traps, and contains the following topics:

SNMP Traps Configuration Pane

Note You must be administrator to configure SNMP traps on the sensor.

Use the SNMP Traps Configuration pane to set up SNMP traps and trap destinations on the sensor. An SNMP trap is a notification. You configure the sensor to send traps based on whether the event is fatal, an error, or a warning.

Caution To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures.

For More Information

For the procedure for having the sensor send SNMP traps, see Assigning Actions to Signatures, page 9-17.

SNMP Traps Configuration Pane Field Definitions

The following fields are found in the SNMP Traps Configuration pane:

- Enable SNMP Traps—If chosen, indicates the remote server will use a pull update.
- Under SNMP Traps—Choose the error events to notify through SNMP:
  - Fatal—Generates traps for all fatal error events.
  - Error—Generates traps for all error error events.
  - Warning—Generates traps for all warning error events.
- Enable detailed traps for alerts—If checked, includes the full text of the alert in the trap. Otherwise, sparse mode is used. Sparse mode includes less than 484 bytes of text for the alert.
- Default Trap Community String—The community string used for the traps if no specific string has been set for the trap.
- Specify SNMP trap destinations—Identifies the destination for the trap. You must specify the following information about the destination:
  - IP Address—The IP address of the trap destination.
  - UDP Port—The UDP port of the trap destination.
  - Trap Community String—The trap community string.

Add and Edit SNMP Trap Destination Dialog Boxes Field Definitions

The following fields are found in the Add and Edit SNMP Trap Destination dialog boxes:

- IP Address—The IP address of the trap destination.
- UDP Port—The UDP port of the trap destination. The default is port 162.
- Trap Community String—The trap community string.

Configuring SNMP Traps

Caution To have the sensor send SNMP traps, you must also select **Request SNMP Trap** as the event action when you configure signatures.

To configure SNMP traps, follow these steps:

Step 1 Log in to IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Management > SNMP > Traps Configuration**.

Step 3 To enable SNMP traps, check the **Enable SNMP Traps** check box.

Step 4 Set the parameters for the SNMP trap:

a. Check the error events you want to be notified about through SNMP traps.

You can choose to have the sensor send an SNMP trap based on one or all of the following events: fatal, error, warning.

b. To receive detailed SNMP traps, check the **Enable detailed traps for alerts** check box.

c. In the Default Trap Community String field, enter the community string to be included in the detailed traps.

Step 5 Set the parameters for the SNMP trap destinations so the sensor knows which management workstations to send them to:

a. Click **Add**.

b. In the IP Address field, enter the IP address of the SNMP management station.

c. In the UDP Port field, enter the UDP port of the SNMP management station.

d. In the Trap Community String field, enter the trap Community string.

Note The community string appears in the trap and is useful if you are receiving multiple types of traps from multiple agents. For example, a router or sensor could be sending the traps, and if you put something that identifies the router or sensor specifically in your community string, you can filter the traps based on the community string.

Tip To discard your changes and close the Add SNMP Trap Destination dialog box, click **Cancel**.

Step 6 Click **OK**.

The new SNMP trap destination appears in the list in the Traps Configuration pane.

Step 7 To edit an SNMP trap destination, select it, and click **Edit**.

Step 8 Edit the **U**DP Port and Trap Community String fields, if needed.

Tip To discard your changes and close the Edit SNMP Trap Destination dialog box, click **Cancel**.

Step 9 Click **OK**.

The edited SNMP trap destination appears in the list in the Traps Configuration pane.

Step 10 To delete an SNMP trap destination, select it, and click **Delete**.

The SNMP trap destination no longer appears in the list in the Traps Configuration pane.

Tip To discard your changes, click **Reset**.

Step 11 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For the procedure for having the sensor send SNMP traps, see Assigning Actions to Signatures, page 9-17.

Supported MIBs

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

You can obtain these private Cisco MIBs under the heading SNMP v2 MIBs at this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note MIB II is available on the sensor, but we do not support it. We know that some elements are not correct (for example, the packet counts from the IF MIB on the sensing interfaces). While you can use elements from MIB II, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

Note CISCO-PROCESS-MIB is available on the sensor, but we do not support it. We know that some elements are not available. While you can use elements from CISCO-PROCESS-MIB, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.