Configuring SNMP

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

Understanding SNMP

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.

You can use SNMPv2 and SNMPv3 protocol concurrently. If the SNMP request contains version 3 user information, then you get a version 3 reply (provided the same user is configured as a version 3 user in the IPS). If the SNMP request is a version 2 request, the IPS returns the response (provided the correct version 2 community string is configured).

Note Encryption of the SNMPv3 payload uses AES-128 and authentication of the user password uses HMAC-SHA-96.

For More Information

For the procedure for having the sensor send SNMP traps, see Assigning Actions to Signatures, page 7-19.

Configuring SNMP General Configuration

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

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

Field Definitions

The following fields are found in the 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—Specifies the community string for read-only access.
  - Read-Write Community String—Specifies the community string for read and write access.
  - Sensor Contact—Specifies the contact person, contact point, or both for the sensor.
  - Sensor Location—Specifies the location of the sensor.
  - Sensor Agent Port—Specifies the IP port of the sensor. The default is 161.
  - Sensor Agent Protocol—Specifies the IP protocol of the sensor. The default is UDP.

Configuring SNMP General Parameters

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

To set the general SNMP parameters, follow these steps:

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

Step 2 Choose **Configuration > 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 SNMPv3 Users

This section describes how to configure SNMPv3 users, and contains the following topics:

SNMPv3 Users Pane

Note You must be administrator or operator to configure SNMPv3 users on the sensor.

Note Support for SNMPv3 is valid for IPS 7.3(2)E4 and later.

The SNMPv3 Users pane displays the username, access control, security level, authentication protocol, and privacy protocol of all SNMPv3 users configured on the system. In the SNMPv3 Users pane, you can add, edit, and delete SNMPv3 users. You can configure a maximum of 25 SNMPv3 users on the system.

Note You can also associate SNMPv3 users with SNMP trap destinations. If no SNMPv3 user is associated with a trap, then an SNMPv2 trap is sent.

SNMPv3 protocol introduces new security features, such as authentication and encryption that were missing from the previous versions. The security model supported by the sensor is USM (User-based Security Model). The U stands for User-based, because it contains a list of users and their attributes.

Note Encryption of the SNMPv3 payload uses AES-128 and authentication of the user password uses HMAC-SHA-96.

Note We recommend that you configure SNMPv3 users with security levels that require authentication, such as authPriv and authNoPriv, with authPriv being the most highly recommended. Configuring SNMPv3 users with the noAuthNoPriv security level is NOT recommended.

SNMPv3 Users Pane Field Definitions

The following fields are found in the SNMPv3 Users pane:

- Username—Displays the username on the host that belongs to the SNMP agent.
- Access Control—Displays the access control (rouser or rwuser) of the SNMPv3 user.
- Security Level—Displays one of the following security models for the SNMPv3 user:
  - noAuthNoPriv—No Authentication and No Privacy, which means that no security is applied to messages.
  - authNoPriv—Authentication but No Privacy, which means that messages are authenticated.
  - authPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.
- Authentication Protocol—Displays the authentication protocol (SHA or none) for the SNMPv3 user.
- Privacy Protocol—Displays the privacy or encryption algorithm used (AES or none) for the SNMPv3 user.

Add and Edit SNMPv3 User Dialog Boxes Field Definitions

The following fields are found in the Add and Edit SNMPv3 User dialog boxes:

- Username—Specifies a username for this SNMPv3 user. The maximum number of characters is 32; no spaces, double quotes, ‘(,’ ‘),’, or ‘[‘ symbols are allowed.
- Access Control—Specifies the access control for this SNMPv3 user:
  - rouser—Read-only user.
  - rwuser—Read-write user.

Note Both rouser and rwuser can do ‘get’ operations, but rwuser access control is mandatory to do ‘set’ operations.

- Security Level—Specifies the security level for this SNMPv3 user:
  - noAuthNoPriv—No Authentication and No Privacy, which means that no security is applied to messages.
  - authNoPriv—Authentication but No Privacy, which means that messages are authenticated.
  - authPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.
- Authentication Protocol—Specifies the authentication protocol (SHA or none) for this SNMPv3 user.
- Authentication Passphrase—Lets you assign an authentication passphrase for this SNMPv3 user. The valid range is 8 to 257 characters; no spaces or double quotes allowed.
- Confirm Authentication Passphrase—Lets you confirm the passphrase.
- Privacy Protocol—Specifies the privacy protocol (AES or none) for this SNMPv3 user.
- Privacy Passphrase—Lets you assign a privacy passphrase for this SNMPv3 user. The valid range is 8 to 257 characters; no spaces or double quotes allowed.
- Confirm Privacy Passphrase—Lets you confirm the passphrase

Caution The same passphrase value for both authentication and privacy is allowed, although it is not a recommended security practice.

Configuring SNMPv3 Users

To configure SNMPv3 users, follow these steps:

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

Step 2 Choose **Configuration > Sensor Management > SNMP > SNMPv3 Users**, and then click **Add**.

Step 3 In the Add SNMPv3 User dialog box, set the following user parameters:

a. In the Username field, enter the username of the SNMPv3 user. The maximum number of characters is 32; no spaces, double quotes, ‘(,’ ‘),’, or ‘[‘ symbols are allowed.

b. In the Access Control field, select rouser or rwuser, from the drop-down list.

c. In the Security Level field, select one of the following security levels from the drop-down list:

- noAuthNoPriv—No Authentication and No Privacy, which means that no security is applied to messages.
- authNoPriv—Authentication but No Privacy, which means that messages are authenticated.
- authPriv—Authentication and Privacy, which means that messages are authenticated and encrypted.

d. In the Authentication Protocol field, select SHA or None from the drop-down list.

e. In the Authentication Passphrase field, enter a passphrase and then confirm it in the Confirm Authentication Passphrase field.

f. In the Privacy Protocol field, select AES or None from the drop-down list.

g. In the Privacy Passphrase field, enter a passphrase and then confirm it in the Confirm Privacy Passphrase field.

Tip To discard your changes and close the Add SNMPv3 User dialog box, click **Cancel**.

Step 4 Click **OK**. The new SNMPv3 user appears in the list in the SNMPv3 Users pane.

Step 5 To edit an SNMPv3 user, select it, and click **Edit**.

Step 6 Edit the any of the fields, if needed.

Tip To discard your changes and close the Edit SNMPv3 User dialog box, click **Cancel**.

Step 7 Click **OK**. The edited SNMPv3 User appears in the list in the SNMPv3 Users pane.

Step 8 To delete an SNMPv3 user, select it, and click **Delete**. The SNMPv3 user no longer appears in the list in the SNMPv3 Users pane.

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

Step 9 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:

Traps Configuration Pane

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

Use the 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.

You can also associate SNMPv3 users with SNMP trap destinations. If no SNMPv3 user is associated with a trap, then an SNMPv2 trap is sent. For example, if a version 3 user is associated with a trap destination, all traps for that destination will be version 3 traps using the configured user. No version 2 trap is sent to that trap destination. If a version 3 user is not configured, then a version 2 trap is sent. Traps can be sent to one destination using version 3 and to another destination using version 2.

Traps Configuration Pane Field Definitions

The following fields are found in the Traps Configuration pane:

- Enable SNMP Traps—If checked, indicates the remote server will use a pull update.
- SNMP Traps—Let you 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.
- Send traps when health metrics change—If checked, sends SNMP traps containing information about the overall health of the sensor.

  Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration > Sensor Management > Sensor Health** to enable sensor health metrics.

- Default Trap Community String—Specifies the community string used for the traps if no specific string has been set for the trap.
- SNMP Trap Destinations—Specifies the destination for the trap. You must specify the following information about the destination:
  - IP Address—Specifies the IP address of the trap destination.
  - UDP Port—Specifies the UDP port of the trap destination.
  - Trap Community String—Specifies the trap community string.
  - SNMPv3 User—Specifies the SNMPv3 user of the trap destination.

    If no trap-v3user is specified, SNMPv2 is used.

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—Specifies the IP address of the trap destination.
- UDP Port—Specifies the UDP port of the trap destination. The default is port 162.
- Trap Community String—Specifies the trap community string.
- SNMPv3 User—Specifies the SNMPv3 user of the trap destination.

  If no trap-v3user is specified, SNMPv2 is used.

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 the IDM using an account with administrator privileges.

Step 2 Choose **Configuration > 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. To receive SNMP traps containing sensor health metrics, check the **Send traps when health metrics change** check box.

Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration > Sensor Management > Sensor Health** to enable sensor health metrics.

d. 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.

e. From the SNMPv3 User drop-down list, select the trap-v3user associated with this trap.

If no SNMPv3 user is specified, SNMPv2 is used.

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, and change the SNMPv3 user, 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.

Supported MIBs

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB

  The CISCO-CIDS-MIB has been updated to include SNMP health data
- 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.