CHAPTER 17

Monitoring the Sensor

The IDM lets you monitor all aspects of the sensor, including performance, statistics, and connections. You can also view the list of denied attackers and events. You can configure IP logging, set up host and network blocks, and configure and manage rate limiting. You can monitor OS identifications and anomaly detection. This section describes how to monitor your sensor, and contains the following topics:

- Monitoring Events, page 17-1
- Configuring and Monitoring Denied Attackers, page 17-4
- Configuring Host Blocks, page 17-6
- Configuring Network Blocks, page 17-8
- Configuring Rate Limits, page 17-10
- Configuring IP Logging, page 17-12
- Monitoring Anomaly Detection KBs, page 17-15
- Configuring OS Identifications, page 17-25
- Clearing Flow States, page 17-26
- Resetting Network Security Health, page 17-28
- Generating the Diagnostics Report, page 17-29
- Displaying Statistics, page 17-30
- Viewing System Information, page 17-31

Monitoring Events

This section describes how to filter and view event data on your sensor, and contains the following topics:

- Event Pane, page 17-2
- Events Pane Field Definitions, page 17-2
- Event Viewer Pane Field Definitions, page 17-3
- Configuring Event Display, page 17-3
- Clearing Event Store, page 17-4

Event Pane

The Events pane lets you filter and view event data. You can filter events based on type, time, or both. By default all alert and error events are displayed for the past one hour. To access these events, click **View**.

When you click **View**, the IDM defines a time range for the events if you have not already configured one If you do not specify an end time of the range, it is defined as the moment you click **View**.

To prevent system errors when retrieving large numbers of events from the sensor, the IDM limits the number of events you can view at one time (the maximum number of rows per page is 500). Click **Back** and **Next** to view more events.

Events Pane Field Definitions

The following fields are found in the Events pane:

- Show Alert Events—Lets you configure the level of alert you want to view. The default is all levels enabled.
  - Informational
  - Low
  - Medium
  - Highì
- Threat Rating (0-100)—Lets you change the range (minimum and maximum levels) of the threat rating value.
- Show Error Events—Lets you configure the type of errors you want to view. The default is all levels enabled.
  - Warning
  - Error
  - Fatal
- Attack Response Controller events—Shows ARC (formerly known as Network Access Controller) events. The default is disabled.

  Note NAC is now known as ARC; however, in Cisco IPS, the name change has not been completed throughout the IDM and the CLI.

- Show status events—Shows status events. The default is disabled.
- Select the number of the rows per page—Lets you determine how many rows you want to view per page. The valid range is 100 to 500. The default is 100.
- Show all events currently stored on the sensor—Retrieves all events stored on the sensor.
- Show past events—Lets you go back a specified number of hours or minutes to view past events.
- Show events from the following time range—Retrieves events from the specified time range.

Event Viewer Pane Field Definitions

The following fields are found on the Event Viewer pane:

- #—Identifies the order number of the event in the results query.
- Type—Identifies the type of event as Error, NAC, Status, or Alert.
- Sensor UTC Time—Identifies when the event occurred.
- Event ID—The numerical identifier the sensor has assigned to the event.
- Events—Briefly describes the event.
- Sig ID—Identifies the signature that fired and caused the alert event.

Configuring Event Display

To configure how you want events to be displayed, follow these steps:

Step 1 Log in to the IDM.

Step 2 Choose **Monitoring > Sensor Monitoring > Events**.

Step 3 Under Show Alert Events, check the check boxes of the levels of alerts you want to be displayed.

Step 4 In the Threat Rating field, enter the minimum and maximum range of threat rating.

Step 5 Under Show Error Events, check the check boxes of the types of errors you want to be displayed.

Step 6 To display ARC (formerly known as Network Access Controller) events, check the **Show Attack Response Controller events** check box.

Step 7 To display status events, check the **Show status events** check box.

Step 8 In the Select the number of the rows per page field, enter the number of rows per page you want displayed. The default is 100. The values are 100, 200, 300, 400, or 500.

Step 9 To set a time for events to be displayed, click one of the following ratio buttons:

- **Show all events currently stored on the sensor**
- **Show past events**

  Enter the hours and minutes you want to go back to view past events.
- **Show events from the following time range**

  Enter a start and end time.

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

Step 10 Click **View** to display the events you configured.

Step 11 To sort up and down in a column, click the right-hand side to see the up and down arrow.

Step 12 Click **Next** or **Back** to page by one hundred.

Step 13 To view details of an event, select it, and click **Details**. The details for that event appear in another dialog box. The dialog box has the Event ID as its title.

Clearing Event Store

Note The Event Store has a fixed size of 30 MB for all platforms.

Use the **clear events** command to clear Event Store.

To clear events from Event Store, follow these steps:

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

Step 2 Clear Event Store.

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

Step 3 Enter **yes** to clear the events.

Configuring and Monitoring Denied Attackers

This section describes how to monitor the denied attackers list, and contains the following topics:

- Denied Attackers Pane, page 17-4
- Denied Attackers Pane Field Definitions, page 17-5
- Monitoring the Denied Attackers List and Adding Denied Attackers, page 17-5

Denied Attackers Pane

Note You must be administrator to monitor and clear the denied attackers list.

The Denied Attackers pane displays all IP addresses and the hit count for denied attackers. You can reset the hit count for all IP addresses or clear the list of denied attackers. You can also configure denied attackers to be monitored.

Denied Attackers Pane Field Definitions

The following fields are found in the Denied Attackers pane:

- Virtual Sensor—Virtual sensor that is denying the attacker.

  Note The AIM IPS and the NME IPS do not support virtualization.

- Attacker IP—IP address of the attacker the sensor is denying.
- Victim IP—IP address of the victim the sensor is denying.
- Port—Port of the host the sensor is denying.
- Protocol—Protocol that the attacker is using.
- Requested Percentage—Percentage of traffic that you configured to be denied by the sensor in inline mode.
- Actual Percentage—Percentage of traffic in inline mode that the sensor actually denies.

  Note The sensor tries to deny exactly what percentage you requested, but because of percentage fractions, the sensor is sometimes below the requested threshold.

- Hit Count—Displays the hit count for that denied attacker.

Monitoring the Denied Attackers List and Adding Denied Attackers

To view the list of denied attackers, their hit counts, and to add denied attackers, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Time-Based Actions > Denied Attackers**.

Step 3 To refresh the list, click **Refresh**.

Step 4 To clear the entire list of denied attackers, click **Clear List**.

Step 5 To have the hit count start over, click **Reset All Hit Counts**.

Step 6 To add a denied attacker to the list to be monitored, click **Add**.

Step 7 In the Attacker IP field, enter the attacker IP address.

Note You can enter IPv4 and IPv6 IP addresses.

Step 8 Click the **Specify Victim Address or Port** check box, and enter the IP address and port number.

Step 9 Click the **Specify Virtual Sensor** check box and choose the virtual sensor from the drop-down list.

Tip To discard your changes and return to the Denied Attackers pane, click **Cancel**.

Step 10 Click **OK** to save your changes. The denied attacker appears in the Denied Attacker list.

Configuring Host Blocks

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

- Host Blocks Pane, page 17-6
- Host Block Pane Field Definitions, page 17-6
- Add Active Host Block Dialog Box Field Definitions, page 17-7
- Configuring and Managing Host Blocks, page 17-7

Host Blocks Pane

Note Connection blocks and network blocks are not supported on security appliances. Security appliances only support host blocks with additional connection information.

Note You must be administrator or operator to configure active host blocks.

Use the Host Blocks pane to configure and manage blocking of hosts. A host block denies traffic from a specific host permanently (until you remove the block) or for a specified amount of time. You can base the block on a connection by specifying the destination IP address and the destination protocol and port.

A host block is defined by its source IP address. If you add a block with the same source IP address as an existing block, the new block overwrites the old block.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the host block remains in effect until the sensor is rebooted or the block is deleted.

Host Block Pane Field Definitions

The following fields are found in the Host Blocks pane:

- Source IP—Source IP address for the block.
- Destination IP—Destination IP address for the block.
- Destination Port—Destination port for the block.
- Protocol—Type of protocol (TCP, UDP, or ANY). The default is ANY.
- Minutes Remaining—Time remaining for the blocks in minutes.
- Timeout (minutes)—Original timeout value for the block in minutes. A valid value is between 1 to 70560 minutes (49 days).

- VLAN— Indicates the VLAN that carried the data that fired the signature.

Note Even though the VLAN ID is included in the block request, it is not passed to the security appliance. Sensors cannot block on FWSM 2.1 or greater when logged in to the admin context.

- Connection Block Enabled—Whether or not to block the connection for the host.

Add Active Host Block Dialog Box Field Definitions

The following fields are found in the Add Active Host Block dialog box:

- Source IP—Source IP address for the block.
- Enable connection blocking—Whether or not to block the connection for the host.
- Connection Blocking—Lets you configure parameters for connection blocking:
  - Destination IP—Destination IP address for the block.
  - Destination Port (optional)—Destination port for the block.
  - Protocol (optional)—Type of protocol (TCP, UDP, or ANY). The default is ANY.
- VLAN (optional)—Indicates the VLAN that carried the data that fired the signature.

Note Even though the VLAN ID is included in the block request, it is not passed to the security appliance. Sensors cannot block on FWSM 2.1 or later when logged in to the admin context.

- Enable Timeout—Lets you set a timeout value for the block in minutes.
- Timeout—Number of minutes for the block to last. A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Configuring and Managing Host Blocks

To configure and manage host blocks, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Time-Based Actions > Host Blocks**, and then click **Add** to add a host block.

Step 3 In the Source IP field, enter the source IP address of the host you want blocked.

Step 4 To make the block connection-based, check the **Enable Connection Blocking** check box.

Note A connection block blocks traffic from a given source IP address to a given destination IP address and destination port.

a. In the Destination IP field, enter the destination IP address.

b. (Optional) In the Destination Port field, enter the destination port.

c. (Optional) From the Protocol drop-down list, choose the protocol.

Step 5 (Optional) In the VLAN field, enter the VLAN for the connection block.

Step 6 Configure the timeout:

- To configure the block for a specified amount of time, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes.
- T o not configure the block for a specified amount of time, click the **No Timeout** radio button.

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

Step 7 Click **Apply**. The new host block appears in the list in the Host Blocks pane.

Step 8 Click **Refresh** to refresh the contents of the host blocks list.

Step 9 To delete a block, select a host block in the list, and click **Delete**. The Delete Host Block dialog box asks if you are sure you want to delete this block.

Tip To discard your changes and close the Delete Host Block dialog box, click **Cancel**.

Step 10 Click **Yes** to delete the block. The host block no longer appears in the list in the Host Blocks pane.

Configuring Network Blocks

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

- Network Blocks Pane, page 17-8
- Network Blocks Pane Field Definitions, page 17-9
- Add Network Block Dialog Box Field Definitions, page 17-9
- Configuring and Managing Network Blocks, page 17-9

Network Blocks Pane

Note Connection blocks and network blocks are not supported on security appliances. Security appliances only support host blocks with additional connection information.

Note You must be administrator or operator to configure network blocks.

Use the Network Blocks pane to configure and manage blocking of networks. A network block denies traffic from a specific network permanently (until you remove the block) or for a specified amount of time. A network block is defined by its source IP address and netmask. The netmask defines the blocked subnet. A host subnet mask is accepted also.

If you specify an amount of time for the block, the value must be in the range of 1 to 70560 minutes (49 days). If you do not specify a time, the block remains in effect until the sensor is rebooted or the block is deleted.

Network Blocks Pane Field Definitions

The following fields are found in the Network Blocks pane:

- IP Address—IP address for the block.
- Mask—Network mask for the block.
- Minutes Remaining—Time remaining for the blocks in minutes.
- Timeout (minutes)—Original timeout value for the block in minutes. A valid value is between 1 and 70560 minutes (49 days).

Add Network Block Dialog Box Field Definitions

The following fields are found in the Add Network Block dialog box:

- Source IP—IP address for the block.
- Netmask—Network mask for the block.
- Enable Timeout—Indicates a timeout value for the block in minutes.
- Timeout—Indicates the duration of the block in minutes. A valid value is between 1 and 70560 minutes (49 days).
- No Timeout—Lets you choose to have no timeout for the block.

Configuring and Managing Network Blocks

To configure and manage network blocks, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Time-Based Actions > Network Blocks**, and then click **Add** to add a network block.

Step 3 In the Source IP field, enter the source IP address of the network you want blocked.

Step 4 From the Netmask drop-down list, choose the netmask.

Step 5 Configure the timeout:

- To configure the block for a specified amount of time, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes.
- To not configure the block for a specified amount of time, click the **No Timeout** radio button.

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

Step 6 Click **Apply**. You receive an error message if a block has already been added.

The new network block appears in the list in the Network Blocks pane.

Step 7 Click **Refresh** to refresh the contents of the network blocks list.

Step 8 Select a network block in the list and click **Delete** to delete that block. The Delete Network Block dialog box asks if you are sure you want to delete this block.

Step 9 Click **Yes** to delete the block. The network block no longer appears in the list in the Network Blocks pane.

Configuring Rate Limits

This section describes how to configure and manage rate limits, and contains the following topics:

- Rate Limits Pane, page 17-10
- Rate Limits Pane Field Definitions, page 17-10
- Add Rate Limit Dialog Box Field Definitions, page 17-11
- Configuring and Managing Rate Limiting, page 17-11

Rate Limits Pane

Note You must be administrator to add rate limits.

Use the Rate Limits pane to configure and manage rate limiting.

A rate limit restricts the amount of a specified type of traffic that is allowed on a network device interface to a percentage of maximum bandwidth capacity. Traffic that exceeds this percentage is dropped by the network device. A rate limit can restrict traffic to a specified target host, or to all traffic that crosses the configured interface/directions. You can use rate limits permanently or for a specified amount of time. A rate limit is identified by a protocol, an optional destination address, and an optional data value.

Because the rate limit is specified as a percent, it may translate to different actual limits on interfaces with different bandwidth capacities. A rate limit percent value must be an integer between 1 and 100 inclusive.

Rate Limits Pane Field Definitions

The following fields are found in the Rate Limits pane:

- Protocol—Protocol of the traffic that is rate limited.
- Rate—Percent of maximum bandwidth that is allowed for the rate-limited traffic. Matching traffic that exceeds this rate will be dropped.
- Source IP—Source host IP address of the rate-limited traffic.
- Source Port—Source host port of the rate-limited traffic.
- Destination IP—Destination host IP address of the rate-limited traffic.
- Destination Port—Destination host port of the rate-limited traffic.

- Data—Additional identifying information needed to more precisely qualify traffic for a given protocol. For example, echo-request narrows the ICMP protocol traffic to rate-limit pings.
- Minutes Remaining—Remaining minutes that this rate limit is in effect.
- Timeout (minutes)—Total number of minutes for this rate limit.

Add Rate Limit Dialog Box Field Definitions

The following fields are found in the Add Rate Limit dialog box:

- Protocol—Protocol of the traffic that is rate-limited (ICMP, TCP, or UDP).
- Rate (1-100)—Percentage of the maximum bandwidth allowed for the rate-limited traffic.
- Source IP (optional)—Source host IP address of the rate-limited traffic.
- Source Port (optional)—Source host port of the rate-limited traffic.
- Destination IP (optional)—Destination host IP address of the rate-limited traffic.
- Destination Port (optional)—Destination host port of the rate-limited traffic.
- Use Additional Data—Lets you choose whether to specify more data, such as echo-reply, echo-request, or halfOpenSyn.
- Timeout—Lets you choose whether to enable timeout:
  - No Timeout—Timeout not enabled.
  - Enable Timeout—Lets you specify the timeout in minutes (1 to 70560).

Configuring and Managing Rate Limiting

To configure and manage rate limiting, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Time-Based Actions > Rate Limits**, and then click **Add** to add a rate limit.

Step 3 From the Protocol drop-down list, choose the protocol (ICMP, TCP, or UDP) of the traffic you want rate limited.

Step 4 In the Rate field, enter the rate limit (1 to 100) percent.

Step 5 (Optional) In the Source IP field, enter the source IP address.

Step 6 (Optional) In the Source Port field, enter the source port.

Step 7 (Optional) In the Destination IP field, enter the destination IP address.

Step 8 (Optional) In the Destination Port field, enter the destination port.

Step 9 (Optional) To configure the rate limit to use additional data, check the **Use Additional Data** check box.

Step 10 From the Select Data drop-down list, choose the additional data (echo-reply, echo-request, or halfOpenSyn).

Step 11 Configure the timeout:

- If you do not want to configure the rate limit for a specified amount of time, click the **No Timeout** radio button.

- If you want to configure a timeout in minutes, click the **Enable Timeout** radio button, and in the Timeout field, enter the amount of time in minutes (1 to 70560).

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

Step 12 Click **Apply**. The new rate limit appears in the list in the Rate Limits pane.

Step 13 Click **Refresh** to refresh the contents of the Rate Limits list.

Step 14 To delete a rate limit, select a rate limit from the list, and click **Delete**. The Delete Rate Limit dialog box asks if you are sure you want to delete this rate limit.

Tip To close the Delete Rate Limit dialog box, click **No**.

Step 15 Click **Yes** to delete the rate limit. The rate limit no longer appears in the rate limits list.

Configuring IP Logging

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

- Understanding IP Logging, page 17-12
- IP Logging Pane, page 17-13
- IP Logging Pane Field Definitions, page 17-13
- Add and Edit IP Logging Dialog Boxes Field Definitions, page 17-14
- Configuring IP Logging, page 17-14

Understanding IP Logging

Caution Turning on IP logging slows system performance.

The simplest IP logging consists of an IP address. You can configure the sensor to capture all IP traffic associated with a host you specify by IP address. The sensor begins collecting as soon as it sees the first IP packet with this IP address and continues collecting depending on the parameters that you have set. You can specify in minutes how long you want the IP traffic to be logged at the IP address, and/or how many packets you want logged, and/or how many bytes you want logged. The sensor stops logging IP traffic at the first parameter you specify.

Log files are in one of three states:

- Added—When IP logging is added
- Started—When the sensor sees the first packet, the log file is opened and placed into the Started state.
- Completed—When the IP logging limit is reached.

The number of files in all three states is limited to 20. The IP logs are stored in a circular buffer that is never filled because new IP logs overwrite the old ones. Once the limit of 20 is reached, you receive the following message in main.log: `Cid/W errWarnIpLogProcessor::addIpLog: Ran out of file descriptors.`

Note Logs remain on the sensor until the sensor reclaims them. You cannot manage IP log files on the sensor.

You can copy IP log files to an FTP or SCP server so that you can view them with a sniffing tool such as WireShark or TCPDUMP. The files are stored in PCAP binary form with the pcap file extension.

IP Logging Pane

Note You must be administrator or operator to configure IP logging.

The IP Logging pane displays all IP logs that are available for downloading on the system.

IP logs are generated in two ways:

- When you add IP logs in the Add IP Logging dialog box
- When you select one of the following as the event action for a signature:
  - Log Attacker Packets
  - Log Pair Packets
  - Log Victim Packets

  When the sensor detects an attack based on this signature, it creates an IP log. The event alert that triggered the IP log appears in the IP logging table.

IP Logging Pane Field Definitions

The following fields are found in the IP Logging pane:

- Log ID—ID of the IP log.
- Virtual Sensor—The virtual sensor with which the IP log is associated

  Note The AIM IPS and the NME IPS do not support virtualization.

- IP Address—IP address of the host for which the log is being captured.
- Status—Status of the IP log. Valid values are added, started, or completed.
- Start Time—Timestamp of the first captured packet.
- Current End Time—Timestamp of the last captured packet. There is no timestamp if the capture is not complete.
- Alert ID—ID of the event alert, if any, that triggered the IP log.
- Packets Captured—Current count of the packets captured.
- Bytes Captured—Current count of the bytes captured.

Add and Edit IP Logging Dialog Boxes Field Definitions

The following fields are found on the Add and Edit IP Logging dialog boxes:

- Virtual Sensor—Lets you choose the virtual sensor from which you want to capture IP logs.

  Note The AIM IPS and the NME IPS do not support virtualization.

- IP Address—IP address of the host for which the log is being captured.

  Note You can enter IPv4 and IPv6 IP addresses.

- Maximum Values—Lets you set the values for IP logging.
  - Duration—Maximum duration to capture packets. The range is 1 to 60 minutes. The default is 10 minutes.

    Note For the Edit IP Logging dialog box, the Duration field is the time that is extended once you apply the edit to IP logging.

  - Packets (optional)—Maximum number of packets to capture. The range is 0 to 4294967295 packets.
  - Bytes (optional)—Maximum number of bytes to capture. The range is 0 to 4294967295 bytes.

Configuring IP Logging

To log IP traffic for a particular host, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Time-Based Actions > IP Logging**, and then click **Add**.

Step 3 From the Virtual Sensor drop-down list, choose for which virtual sensor you want to turn on IP logging.

Step 4 In the IP Address field, enter the IP address of the host from which you want IP logs to be captured.

You receive an error message if a capture is being added that exists and is in the Added or Started state.

Note You can enter IPv4 and IPv6 IP addresses.

Step 5 In the Duration field, enter how many minutes you want IP logs to be captured. The range is 1 to 60 minutes. The default is 10 minutes.

Step 6 (Optional) In the Packets field, enter how many packets you want to be captured. The range is 0 to 4294967295 packets.

Step 7 (Optional) in the Bytes field, enter how many bytes you want to be captured. The range is 0 to 4294967295 packets.

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

Step 8 Click **Apply** to apply your changes and save the revised configuration. The IP log with a log ID appears in the list in the IP Logging pane.

Step 9 To edit an existing log entry in the list, select it, and click **Edit**.

Step 10 In the Duration field, edit the minutes you want packets to be captured.

Step 11 Click **Apply** to apply your changes and save the revised configuration. The edited IP log appears in the list in the IP Logging pane.

Step 12 To stop IP logging, select the log ID for the log you want to stop, and click **Stop**.

Step 13 Click **OK** to stop IP logging for that log.

Step 14 To download an IP log, select the log ID, and click **Download**.

Step 15 Save the log to your local machine. You can view it with WireShark.

Monitoring Anomaly Detection KBs

This section describes how to work with anomaly detection KBs, and contains the following topics:

- Anomaly Detection Pane, page 17-15
- Understanding KBs, page 17-16
- Anomaly Detection Pane Field Definitions, page 17-17
- Showing Thresholds, page 17-17
- Comparing KBs, page 17-19
- Saving the Current KB, page 17-21

Anomaly Detection Pane

Note You must be administrator to monitor anomaly detection KBs.

The anomaly detections pane displays the KBs for all virtual sensors. In the Anomaly Detection pane, you can perform the following actions:

- Show thresholds of specific KBs
- Compare KBs
- Load a KB
- Make the KB the current KB
- Rename a KB
- Download a KB

- Upload a KB
- Delete a KB or all KBs

Note The Anomaly Detection buttons are active if only one row in the list is selected, except for Compare KBs, which can have two rows selected. If any other number of rows is selected, none of the buttons is active.

Understanding KBs

The KB has a tree structure, and contains the following information:

- KB name
- Zone name
- Protocol
- Service

The KB holds a scanner threshold and a histogram for each service. If you have learning accept mode set to auto and the action set to rotate, a new KB is created every 24 hours and used in the next 24 hours. If you have learning accept mode set to auto and the action is set to save only, a new KB is created, but the current KB is used. If you do not have learning accept mode set to auto, no KB is created.

Note Learning accept mode uses the sensor local time.

The scanner threshold defines the maximum number of zone IP addresses that a single source IP address can scan. The histogram threshold defines the maximum number of source IP addresses that can scan more than the specified numbers of zone IP addresses.

Anomaly detection identifies a worm attack when there is a deviation from the histogram that it has learned when no attack was in progress (that is, when the number of source IP addresses that concurrently scan more than the defined zone destination IP address is exceeded). For example, if the scanning threshold is 300 and the histogram for port 445, if anomaly detection identifies a scanner that scans 350 zone destination IP addresses, it produces an action indicating that a mass scanner was detected. However, this scanner does not yet verify that a worm attack is in progress. Table 17-1 describes this example.

Table 17-1 Example Histogram

Number of source IP addresses	10	5	2
Number of destination IP addresses	5	20	100

When anomaly detection identifies six concurrent source IP addresses that scan more than 50 zone destination IP addresses on port 445, it produces an action with an unspecified source IP address that indicates anomaly detection has identified a worm attack on port 445. The dynamic filter threshold, 50, specifies the new internal scanning threshold and causes anomaly detection to lower the threshold definition of a scanner so that anomaly detection produces additional dynamic filters for each source IP address that scans more than the new scanning threshold (50).

You can override what the KB learned per anomaly detection policy and per zone. If you understand your network traffic, you may want to use overrides to limit false positives.

Anomaly Detection Pane Field Definitions

The following fields and buttons are found in the Anomaly Detection pane:

- Virtual Sensor—The virtual sensor that the KB belongs to.
- Knowledge Base Name—The name of the KB.

Note By default, the KB is named by its date. The default name is the date and time (year-month-day-hour_minutes_seconds). The initial KB is the first KB, the one that has the default thresholds.

- Current—Yes indicates the currently loaded KB.
- Size—The size in KB of the KB. The range is usually less than 1 KB to 500-700 KB.
- Created—The date the KB was created.

Button Functions

- Show Thresholds—Opens the Thresholds window for the selected KB. In this window, you can view the scanner thresholds and histograms for the selected KB.
- Compare KBs—Opens the Compare Knowledge Bases dialog box. In this dialog box, you can choose which KB you want to compare to the selected KB. It opens the Differences between knowledge bases *KB name* and *KB name* window.
- Load—Loads the selected KB, which makes it the currently used KB.
- Save Current—Opens the Save Knowledge Base dialog box. In this dialog box, you can save a copy of the selected KB.
- Rename—Opens the Rename Knowledge Base dialog box. In this dialog box, you can rename the selected KB.
- Download—Opens the Download Knowledge Base From Sensor dialog box. In this dialog box, you can download a KB from a remote sensor.
- Upload—Opens the Upload Knowledge Base to Sensor dialog box. In this dialog box, you can upload a KB to a remote sensor.
- Delete—Deletes the selected KB.
- Refresh—Refreshes the Anomaly Detection pane.

Showing Thresholds

This section describes how to display KB threshold information, and contains the following topics:

- Threshold for KB_Name Window, page 17-18
- Thresholds for KB_Name Window Field Definitions, page 17-18
- Monitoring the KB Thresholds, page 17-18

Threshold for KB_Name Window

In the Thresholds for *KB_Name* window, the following threshold information is displayed for the selected KB:

- Zone name
- Protocol
- Learned scanner threshold
- User scanner threshold
- Learned histogram
- User histogram

You can filter the threshold information by zone, protocols, and ports. For each combination of zone and protocol, two thresholds are displayed: the Scanner Threshold and the Histogram threshold either for the learned (default) mode or the user-configurable mode.

Thresholds for *KB_Name* Window Field Definitions

The following fields are found in the Thresholds for *KB_Name* window:

- Filters—Lets you filter the threshold information by zone or protocol:
  - Zones—Filter by all zones, external only, illegal only, or internal only.
  - Protocols—Filter by all protocols, TCP only, UDP only, or other only.

Note If you choose a specific protocol, you can also filter on all ports or a single port (TCP and UDP), all protocols, or a single protocol (other).

- Zone—Lists the zone name (external, internal, or illegal).
- Protocol—Lists the protocol (TCP, UDP, or Other)
- Scanner Threshold (Learned)—Lists the learned value for the scanner threshold.
- Scanner Threshold (User)—Lists the user-configured value for the scanner threshold.
- Histogram (Learned)—Lists the learned value for the histogram.
- Histogram (User)—Lists the user-configured value for the histogram.

Monitoring the KB Thresholds

To monitor KB thresholds, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To refresh the Anomaly Detection pane with the latest KB information, click **Refresh**.

Step 4 To display the thresholds for a KB, select the KB in the list and click **Show Thresholds**. The Thresholds for *KB_Name* window appears. The default display shows all zones and all protocols.

Step 5 To filter the display to show only one zone, choose the zone from the Zones drop-down list.

Step 6 To filter the display to show only one protocol, choose the protocol from the Protocols drop-down list. The default display shows all ports for the TCP or UDP protocol and all protocols for the Other protocol.

Step 7 To filter the display to show a single port for TCP or UPD, click the **Single Port** radio button and enter the port number in the Port field.

Step 8 To filter the display to show a single protocol for Other protocol, click the **Single Protocol** radio button and enter the protocol number in the Protocol field.

Step 9 To refresh the window with the latest threshold information, click **Refresh**.

Comparing KBs

This section describes how to compare KBs, and contains the following topics:

- Compare Knowledge Base Dialog Box, page 17-19
- Differences between knowledge bases KB_Name and KB_Name Window, page 17-19
- Difference Thresholds between knowledge bases KB_Name and KB_Name Window, page 17-20
- Comparing KBs, page 17-20

Compare Knowledge Base Dialog Box

You can compare two KBs and display the differences between them. You can also display services where the thresholds differ more than the specified percentage. The Details of Difference column shows in which KB certain ports or protocols appear, or how the threshold percentages differ.

Field Definitions

The following field is found in the Compare Knowledge Bases dialog box:

- Drop-down list containing all KBs

Differences between knowledge bases *KB_Name* and *KB_Name* Window

The Differences between knowledge base *KB_Name* and *KB_Name* window displays the following types of information:

- Zone
- Protocol
- Details of Difference

You can specify the percentage of the difference that you want to see. The default is 10%.

Field Definitions

The following fields are found in the Differences between knowledge bases *KB_Name* and *KB_Name* window:

- Specify Percentage of Difference—Lets you change the default from 10% to show different percentages of differences.
- Zone—Displays the zone for the KB differences (internal, illegal, or external).

- Protocol—Displays the protocol for the KB differences (TCP, UDP, or Other).
- Details of Difference—Displays the details of difference in the second KB.

Difference Thresholds between knowledge bases *KB_Name* and *KB_Name* Window

The Difference Thresholds between knowledge base *KB_Name* and *KB_Name* window displays the following types of information:

- Knowledge base name
- Zone name
- Protocol
- Scanner threshold (learned and user-configured)
- Histogram (learned and user-configured)

Field Definitions

The Difference Thresholds between knowledge base *KB_Name* and *KB_Name* window displays the following types of information:

- Knowledge Base—Displays the KB name.
- Zone—Displays the name of the zone (internal, illegal, or external).
- Protocol—Displays the protocol (TCP, UDP, or Other).
- Scanner Threshold (Learned)—Lists the learned value for the scanner threshold.
- Scanner Threshold (User)—Lists the user-configured value for the scanner threshold.
- Histogram (Learned)—Lists the learned value for the histogram.
- Histogram (User)—Lists the user-configured value for the histogram.

Comparing KBs

To compare two KBs, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To refresh the Anomaly Detection pane with the most recent KB information, click **Refresh**.

Step 4 Select one KB in the list that you want to compare and click **Compare KBs**.

Step 5 From the drop-down list, choose the other KB you want in the comparison.

Note Or you can choose KBs in the list by holding the **Ctrl** key and selecting two KBs.

Step 6 Click **OK**. The Differences between knowledge bases *KB_Name* and *KB_Name* window appears.

Note If there are no differences between the two KBs, the list is empty.

Step 7 To change the percentage of difference from the default of 10%, enter a new value in the Specify Percentage of Difference field.

Step 8 To view more details of the difference, select the row and then click **Details**. The Difference Thresholds between knowledge bases *KB_Name* and *KB_Name* window appears displaying the details.

Saving the Current KB

This section describes how to work with KBs, and contains the following topics:

- Save Knowledge Base Dialog Box, page 17-21
- Loading a KB, page 17-21
- Saving a KB, page 17-22
- Deleting a KB, page 17-22
- Renaming a KB, page 17-22
- To download a KB from a sensor, follow these steps:, page 17-23
- Uploading a KB, page 17-24

Save Knowledge Base Dialog Box

Note You cannot overwrite the initial KB.

You can save a KB under a different name. An error is generated if AD is not active when you try to save the KB. If the KB name already exists, whether you chose a new name or use the default, the old KB is overwritten. Also, the size of KB files is limited, so if a new KB is generated and the limit is reached, the oldest KB (as long as it is not the current or initial KB) is deleted.

Field Definitions

The following fields are found in the Save Knowledge Base dialog box:

- Virtual Sensor—Lets you choose the virtual sensor for the saved KB.
- Save As—Lets you accept the default name or enter a new name for the saved KB.

Loading a KB

Note Loading a KB sets it as the current KB.

To load a KB, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to load and click **Load**. The Load Knowledge Base dialog box appears asking if you are sure you want to load the knowledge base.

Step 4 Click **Yes**. The Current column now read Yes for this KB.

Saving a KB

To save a KB with a new KB and virtual sensor, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to save as a new KB and click **Save Current**.

Step 4 From the Virtual Sensor drop-down list, choose the virtual sensor to which you want this KB to apply.

Step 5 In the Save As field, either accept the default name, or enter a new name for the KB.

Tip To discard your changes and close the Save Knowledge Base dialog box, click **Cancel**.

Step 6 Click **Apply**. The KB with the new name appears in the list in the Anomaly Detection pane.

Deleting a KB

Note You cannot delete the KB that is loaded as the current KB, nor can you delete the initial KB.

To delete a KB, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to delete and click **Delete**. The Delete Knowledge Base dialog box appears asking if you are sure you want to delete the knowledge base.

Step 4 Click **Yes**. The KB no longer appears in the list in the Anomaly Detection pane.

Renaming a KB

Note You cannot rename the initial KB.

Field Definitions

The following field is found in the Rename Knowledge Base dialog box:

- New Name—Lets you enter a new name for the selected KB.

Renaming a KB

To rename a KB, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 Select the KB in the list that you want to rename and click **Rename**.

Step 4 In the New Name field, enter the new name for the KB.

Step 5 Click **Apply**. The newly named KB appears in the list in the Anomaly Detection pane.

Downloading a KB

You can download a KB to a remote location using FTP or SCP protocol. You must have the remote URL, username, and password.

Field Definitions

The following fields are found in the Download Knowledge Base From Sensor dialog box.

- File Transfer Protocol—Lets you choose SCP or FTP as the file transfer protocol.
- IP address—The IP address of the remote sensor from which you are downloading the KB.
- Directory—The path where the KB resides on the remote sensor.
- File Name—The filename of the KB.
- Username—The username corresponding to the user account on the remote sensor.
- Password—The password for the user account on the remote sensor.

Downloading a KB

To download a KB from a sensor, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To download a KB from a sensor, click **Download**.

Step 4 From the File Transfer Protocol drop-down list, choose the protocol you want to use (SCP or FTP).

Step 5 In the IP address field, enter the IP address of the sensor from which you are downloading the KB.

Step 6 In the Directory field, enter the path where the KB resides on the sensor.

Step 7 In the File Name field, enter the filename of the KB.

Step 8 In the Username field, enter the username corresponding to the user account on the sensor.

Step 9 In the Password field, enter the password for the user account on the sensor.

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

Step 10 Click **Apply**. The new KB appears in the list in the Anomaly Detection pane.

Uploading a KB

You can upload a KB from a remote location using FTP or SCP protocol. You must have the remote URL, username, and password.

Field Definitions

The following fields are found in the Upload Knowledge Base to Sensor dialog box:

- File Transfer Protocol—Lets you choose SCP or FTP as the file transfer protocol.
- IP address—The IP address of the remote sensor to which you are uploading the KB.
- Directory—The path where the KB resides on the sensor.
- File Name—The filename of the KB.
- Virtual Sensor—The virtual sensor with which you want to associate this KB.
- Save As—Lets you save the KB as a new file name.
- Username—The username corresponding to the user account on the sensor.
- Password—The password for the user account on the sensor.

Uploading a KB

To upload a KB to a sensor, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > Anomaly Detection**.

Step 3 To upload a KB to a sensor, click **Upload**.

Step 4 From the File Transfer Protocol drop-down list, choose the protocol you want to use (SCP or FTP).

Step 5 In the IP address field, enter the IP address of the sensor to which you are downloading the KB.

Step 6 In the Directory field, enter the path where the KB resides on the sensor.

Step 7 In the File Name field, enter the filename of the KB.

Step 8 From the Virtual Sensor drop-down list, choose the virtual sensor to which you want this KB to apply.

Step 9 In the Save As field, enter the name of the new KB.

Step 10 In the Username field, enter the username corresponding to the user account on the sensor.

Step 11 In the Password field, enter the password for the user account on the sensor.

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

Step 12 Click **Apply**. The new KB appears in the list in the Anomaly Detection pane.

Configuring OS Identifications

The Learned OS and Imported OS panes display the OS mappings for the sensor. This section describes how to display learned OS and imported OS mappings for the sensor, and contains the following topics:

- Learned OS Pane, page 17-25
- Imported OS Pane, page 17-26

Learned OS Pane

Note You must administrator or operator to clear the list or delete entries in the Learned OS pane.

The Learned OS pane displays the learned OS mappings that the sensor has learned from observing traffic on the network. The sensor inspects TCP session negotiations to determine the OS running on each host.

To clear the list or delete one entry, select the row and click **Delete**. Click **Refresh** to update the list. Click **Export** to export currently displayed learned OSes in the table to a comma-separated Excel file (using CSV) or HTML file. You can also use **Ctrl-C** to copy the contents in to a clipboard and later paste in to Notepad or Word using **Ctrl-V**.

Note If Passive OS fingerprinting is still enabled and hosts are still communicating on the network, the learned OS mappings are immediately repopulated.

Field Definitions

The following fields are found in the Learned OS pane:

- Virtual Sensor—The virtual sensor with which the OS value is associated.
- Host IP Address—The IP address to which the OS value is mapped.
- OS Type—The OS type associated with the IP address.

Deleting Values and Clearing the Learned OS List

To delete a learned OS value or to clear the entire list, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > OS Identifications > Learned OS**.

Step 3 To delete one entry in the list, select it, and click **Delete**. The learned OS value no longer appears in the list on the Learned OS pane.

Step 4 To get the most recent list of learned OS values, click **Refresh**. The learned OS list is refreshed.

Step 5 To clear all learned OS values, click **Clear List**. The learned OS list is now empty.

Step 6 To save the learned OS list to CSV and HTML formats, click **Export**. You can also use **Ctrl-C** to copy the contents of the Learned OS pane and then use **Ctrl-V** to copy the contents in a NotePad or Word

Imported OS Pane

Note You must administrator or operator to clear the list or delete entries in the Imported OS pane.

The Imported OS pane displays the OS mappings that the sensor has imported from CSA MC if you have CSA MC set up as an external interface product. Choose **Configuration > External Product Interfaces** to add an external product interface. To clear the list or delete one entry, select the row, and then click **Delete**.

Field Definitions

The following fields are found in the Imported OS pane:

- Host IP Address—The IP address to which the OS value is mapped.
- OS Type—The OS type associated with the IP address.

Deleting Values and Clearing the Imported OS List

To delete an imported OS value or to clear the entire list, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Dynamic Data > OS Identifications > Imported OS**.

Step 3 To delete one entry in the list, select it, and click **Delete**. The imported OS value no longer appears in the list on the Imported OS pane.

Step 4 To clear all imported OS values, click **Clear List**. The imported OS list is now empty.

Step 5 To update the pane with current imported OS values, click **Refresh**.

Clearing Flow States

This section describes how to clear sensor databases, and contains the following topics:

- Clear Flow States Pane, page 17-27
- Clear Flow States Pane Field Definitions, page 17-27
- Clearing Flow States, page 17-27

Clear Flow States Pane

Caution Clearing the alerts database deletes any summary alerts in progress, which prevents a final summary alert. We recommend that you only clear the alerts database for troubleshooting purposes.

The Clear Flow States pane lets you clear the database of some or all of its contents, for example, the nodes, alerts, or inspectors databases. If you do not provide the virtual sensor name, all virtual sensor databases are cleared.

Clearing the nodes in the database causes the sensor to start fresh as if from a restart. All open TCP stream information is deleted and new TCP stream nodes are created as new packets are received.

When you clear the inspectors database, the TCP and state information is retained, but all inspection records that might lead to a future alert are deleted. New inspection records are created as new packets are retrieved.

When you clear the alerts database, the alerts database is cleared entirely.

Clear Flow States Pane Field Definitions

The following fields are found in the Clear Flow States pane:

- Clear Nodes—Clears the overall packet database elements, including the packet nodes, TCP session information, and inspector lists.
- Clear Inspectors—Clears inspector lists contained within the nodes.

  Does not clear TCP session information or nodes. Inspector lists represent the packet work and observations collected during the sensor up time.
- Clear Alerts (not recommended)—Clears the alerts database, including the alerts nodes, Meta inspector information, summary state, and event count structures.

  Note Clearing the alerts database deletes any summary alerts in progress, which prevents a final summary alert. We recommend that you only clear the alerts database for troubleshooting purposes.
- Clear All—Clears all of the virtual sensor databases.
- Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)—Lets you clear the database of a specific virtual sensor.

Clearing Flow States

To clear flow states, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Properties > Clear Flow States**.

Step 3 Click the radio buttons of the values you want to clear:

- Clear Nodes
- Clear Inspectors
- Clear Alerts (not recommended)
- Clear All

Caution Clearing the alerts database deletes any summary alerts in progress, which prevents a final summary alert. We recommend that you only clear the alerts database for troubleshooting purposes.

Step 4 To clear the flow state of one virtual sensor, check the **Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)** check box. To clear the flow state for all virtual sensors, go to Step 6.

Step 5 From the drop-down list, select the virtual sensor for which you want to clear the flow state.

Step 6 Click **Clear Flow State Now**.

Resetting Network Security Health

Note You must be administrator to reset network security health.

Note The AIM IPS and the NME IPS do not support virtualization.

The Reset Network Security Health pane lets you reset the status and calculation of network security health. This clears the Network Security Health gadget on the Home page. If you do not provide the virtual sensor name, all virtual sensor network security health information is cleared.

Field Definitions

The following field is found in the Reset Network Security Health pane:

- Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)—Lets you clear the network security data for a specific virtual sensor.

Resetting Network Security Health Data

To reset network security health data, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Properties > Reset Network Security Health**.

Step 3 To reset the network security health of one virtual sensor, check the **Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)** check box. To reset the data for all virtual sensors, go to Step 5.

Step 4 From the drop-down list, select the virtual sensor for which you want to clear network security health data.

Step 5 Click **Reset Network Security Health Now**. The data in the Network Security Health gadget on the Home page is cleared.

Note To change the threat thresholds displayed in the Network Security gadget, choose **Configuration > Event Action Rules > rules0 > Risk Category**.

For More Information

- For more information on the Sensor Health gadget, which contains network security data, see Sensor Health Gadget, page 2-4.
- For the procedure for configuring sensor health, see Configuring Sensor Health, page 16-16.
- For the procedure for configuring risk categories, see Configuring Risk Category, page 9-32.

Generating the Diagnostics Report

Note You must be administrator to run diagnostics.

Note Generating a diagnostics report can take a few minutes.

You can obtain diagnostics information on your sensors for troubleshooting purposes. The diagnostics report contains internal system information, such as logs, status, configuration, and so forth, that is intended for TAC to use when troubleshooting the sensor. You can view the report in the Diagnostics Report pane or you can click **Save** and save it to the hard-disk drive.

Button Definitions

The following buttons are found in the Diagnostics Report pane:

- Save—Opens the Save As dialog box so you can save a copy of the diagnostics report to your hard-disk drive.
- Generate Report—Starts the diagnostics process.

  This process can take several minutes to complete. After the process is complete, a report is generated and the display is refreshed with the updated report.

Generating a Diagnostics Report

Caution After you start the diagnostics process, do not click any other options in the IDM or leave the Diagnostics pane. This process must be completed before you can perform any other tasks for the sensor.

To run diagnostics, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Support Information > Diagnostics Report**, and then click **Generate Report**.

Note The diagnostics process can take some time to complete. When the process has finished running, the display is refreshed with the updated results.

Step 3 To save this report as a file, click **Save**.

The **Save As** dialog box opens and you can save the report to your hard-disk drive.

Displaying Statistics

The Statistics pane shows statistics for the following categories:

- Analysis Engine

  The Analysis Engine section also contains global correlation statistics.
- Anomaly Detection
- External Product Interface
- Host
- Interface Configuration
- Logger
- Network Access (now known as Attack Response Controller)
- Notification
- OS Identification
- Transaction Server
- Virtual Sensor
- Web Server

Button Definitions

The following button is found in the Statistics pane

- Refresh—Displays the most recent information about the sensor applications, including the Web Server, Transaction Source, Transaction Server, Network Access Controller, Logger, Host, Event Store, Event Server, Analysis Engine, Interface Configuration, and Authentication.

Note Network Access Controller, now known as Attack Response Controller beginning with Cisco IPS 5.1, is still listed as Network Access Controller in the statistics output.

Viewing Statistics

To show statistics for your sensor, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Support Information > Statistics**.

Step 3 To update statistics as they change, click **Refresh**.

Viewing System Information

The System Information pane displays the following information:

- TAC contact information
- Platform information
- Booted partition
- Software version
- Status of applications (MainApp, Analysis Engine, and CollaborationApp)
- Upgrades installed
- PEP information
- Memory usage
- Disk usage

Button Definitions

The following button is found on the System Information pane:

- Refresh—Displays the most recent information about the sensor, including the software version and PEP information.

Viewing System Information

To view system information, follow these steps:

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

Step 2 Choose **Monitoring > Sensor Monitoring > Support Information > System Information**. The System Information pane displays information about the system.

Step 3 Click **Refresh**. The pane refreshes and displays new information.