



Monitoring the Sensor

The IME lets you monitor all aspects of the sensor, including performance, statistics, and connections. You can monitor OS identifications and anomaly detection. This section describes how to monitor your sensor, and contains the following sections:

- [Monitoring Events, page 20-1](#)
- [Displaying Inspection Load Statistics, page 20-4](#)
- [Displaying Interface Statistics, page 20-5](#)
- [Monitoring Anomaly Detection KBs, page 20-7](#)
- [Configuring OS Identifications, page 20-17](#)
- [Monitoring LACP, page 20-18](#)
- [Clearing Flow States, page 20-22](#)
- [Resetting Network Security Health, page 20-23](#)
- [Generating a Diagnostics Report, page 20-24](#)
- [Viewing Statistics, page 20-25](#)
- [Viewing System Information, page 20-26](#)

Monitoring Events

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

- [Events Pane, page 20-1](#)
- [Events Pane Field Definitions, page 20-2](#)
- [Event Viewer Pane Field Definitions, page 20-3](#)
- [Configuring Event Display, page 20-3](#)
- [Clearing Event Store, page 20-4](#)

Events 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 IME 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 IME 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
 - High
- 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
- Show 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 IME 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.

For More Information

For a detailed explanation of threat rating, see [Understanding Threat Rating, page 11-4](#).


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.
- Sensor Local Time—Displays the local time of the sensor.
- Event ID—Displays 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.
- Performed Actions—Displays the actions the sensor has taken.

Configuring Event Display

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

-
- Step 1** Log in to the IME.
- Step 2** Choose **Configuration > sensor_name > 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 the Event Store.

To clear events from the Event Store, follow these steps:

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

Step 2 Clear the 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.

Displaying Inspection Load Statistics



Note You must be administrator to monitor inspection load statistics.

The Inspection Load Statistics pane displays the inspection load history across varying time periods. Historical peak and average values of the inspection load are displayed minute-by-minute (up to the last 60 minutes) or hour-by-hour (up to the last 72 hours).

The Inspection Load Statistics pane has two parts—a graphical chart on the top and a table on the bottom. The chart graphically displays the time versus the peak/average range. The table displays the raw peak/average values corresponding to the time value. You can hide each part of the pane by clicking the collapse toggle on the left side of the divider.

You can change the time scale of the statistics from the Type drop-down menu in the upper left corner. And you can export the statistics to a CSV or HTML file by clicking **Export**. Or you can right click on the graph to save and print the file.

Field Definitions

The following fields are found in the Inspection Load Statistics pane:

- **Type**—Lets you choose how to display inspection load statistics:
 - **Inspection Load Per Minute (Last 60 Minutes)**—Shows the statistics per minute over the last hour.
 - **Inspection Load Per Hour (Last 72 Hours)**—Shows the statistics per hour over the last three days.
- **Export**—Lets you export the data to one of the following file formats:
 - to CSV file
 - to HTML file

- Last Updated—Displays the date and time that the inspection load statistics were last updated.

Displaying Inspection Load Statistics

To configure how you want inspection load statistics to be displayed, follow these steps:

-
- Step 1** Log in to the IME.
- Step 2** Choose **Configuration > sensor_name > Sensor Monitoring > Inspection Load Statistics**.
- Step 3** From the Type drop-down list, select which view of the inspection load statistics you want to be displayed.
- Inspection Load Per Minute (Last 60 Minutes)—Shows the statistics per minute over the last hour.
 - Inspection Load Per Hour (Last 72 Hours)—Shows the statistics per hour over the last three days.
- Step 4** To collapse either the graph or the table, click the collapse toggle on the left side on the divider. To show the graph or table again, click the collapse toggle and then put your cursor on the divider and resize the pane.
- Step 5** To export data from the Inspection Load Statistics pane, click **Export** and choose one of the following file formats:
- to CSV file
 - to HTML file
- Step 6** A Save dialog box appears. Enter a filename and choose which folder you want to save the file in and click **Save**.
- Step 7** To refresh the view, click **Refresh**.
- Step 8** You can left click on the pane and from the popup menu you can save or print the statistics.
-

Displaying Interface Statistics

In the Interface Statistics pane you can view the historical interface statistics in chart or table format. All interfaces including the management interface are presented. You can view the data for all interfaces together and the various counters for the last 60 minutes or for the last 72 hours. And you can export the statistics to a CSV or HTML file by clicking **Export**. Or you can right click on the graph to save and print the file.

For each interface you can see the following statistics in either minutes or hours:

- Total packets received
- Total bytes received
- FIFO overruns
- Received errors
- Received Mbps
- Missed packets (in terms of percentage)
- Average load (in terms of percentage)
- Peak Load (in terms of percentage)

Field Definitions

The following fields are found in the Interface Statistics pane:

- Interface—Lets you choose the interface for which you want to display statistics.
- Parameter—Lets you sort the statistics by parameter.
- Interval—Lets you choose the last 60 minutes or 72 hours as the time interval in which to display the statistics.

Displaying Interface Statistics

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

-
- Step 1** Log in to the IME.
 - Step 2** Choose **Configuration > sensor_name > Sensor Monitoring > Interface Statistics**.
 - Step 3** From the Interface drop-down list, select the interface you want to display statistics for.
 - Step 4** From the Parameter drop-down list, select the way you want the statistics sorted:
 - Average load percentage
 - Peak load percentage
 - Missed packet percentage
 - Packets received
 - Bytes received
 - Bytes per second
 - Received errors
 - FIFO overruns
 - Step 5** From the Interval drop-down menu, select the time interval for which to display the statistics:
 - Last 60 minutes
 - Last 72 hours
 - Step 6** To collapse either the graph or the table, click the collapse toggle on the left side on the divider. To show the graph or table again, click the collapse toggle and then put your cursor on the divider and resize the pane.
 - Step 7** To export data from the Interface Statistics pane, click **Export** and choose one of the following file formats:
 - to CSV file
 - to HTML file
 - Step 8** A Save dialog box appears. Enter a filename and choose which folder you want to save the file in and click **Save**.
 - Step 9** To refresh the view, click **Refresh**.
 - Step 10** You can left click on the pane and from the popup menu you can save or print the statistics.
-

Monitoring Anomaly Detection KBs

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

- [Anomaly Detection Pane, page 20-7](#)
- [Understanding KBs, page 20-7](#)
- [Anomaly Detection Pane Field Definitions, page 20-9](#)
- [Showing Thresholds, page 20-9](#)
- [Comparing KBs, page 20-11](#)
- [Saving the Current KB, page 20-13](#)

Anomaly Detection Pane

**Note**

Anomaly detection is disabled by default. You must enable it to configure or apply an anomaly detection policy. Enabling anomaly detection results in a decrease in performance.

**Note**

You must be administrator to monitor anomaly detection KBs.

The Anomaly Detection 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 20-1](#) describes this example.

Table 20-1 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 20 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, 20, 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 (20).

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.

Triggering the High Category Histogram Before the Single-Scanner Threshold

Based on the default histogram (nonlearned knowledge base [KB]) values, histogram-based detection can occur before single-scanner detection.

Single scanner detection is based on the scanner threshold settings. The scanner threshold setting is a single number for that port or protocol and zone. Any single IP address scanning more than that number of hosts of that port or protocol in that zone is alerted as a scanner.

There is a histogram for that port or protocol and zone that tracks how many systems normally scan a smaller number of hosts (10 hosts, 20 hosts, or 100 hosts). When more than that normal number of scanners are seen, then a worm is declared and all IPs scanning more than the associated number of hosts are alerted on as being a worm scanner.

**Note**

An IP source address can be alerted on as being a worm scanner without ever reaching the scanner threshold. The scanner threshold is used to detect single systems scanning a large number of hosts and is tracked separately from the algorithms for detecting worms.

Anomaly Detection Pane Field Definitions

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

Field Definitions

- Virtual Sensor—Displays the virtual sensor to which the KB belongs.
- Knowledge Base Name—Displays 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—Indicates the size in KB of the KB. The range is usually less than 1 KB to 500-700 KB.
- Created—Displays 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.
- Delete All—Deletes all of the KBs.
- 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 20-10](#)
- [Thresholds for KB_Name Window Field Definitions, page 20-10](#)
- [Monitoring the KB Thresholds, page 20-10](#)

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—Specifies to filter to 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 IME using an account with administrator privileges.
 - Step 2** Choose **Configuration > sensor_name > 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 UDP, 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 20-11](#)
- [Differences between knowledge bases KB_Name and KB_Name Window, page 20-11](#)
- [Difference Thresholds between knowledge bases KB_Name and KB_Name Window, page 20-12](#)
- [Comparing KBs, page 20-12](#)

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 IME using an account with administrator privileges.
 - Step 2** Choose **Configuration > sensor_name > 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 save, load, or delete the current KB, and contains the following topics:

- [Save Knowledge Base Dialog Box, page 20-13](#)
- [Loading a KB, page 20-13](#)
- [Saving a KB, page 20-14](#)
- [Deleting a KB, page 20-14](#)
- [Renaming a KB, page 20-14](#)
- [Downloading a KB, page 20-15](#)
- [Uploading a KB, page 20-16](#)

Save Knowledge Base Dialog Box

You can save a KB under a different name. An error is generated if anomaly detection 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.



Note You cannot overwrite the initial KB.

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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > 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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > 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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > 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

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

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



Note You cannot rename the initial KB.

To rename a KB, follow these steps:

-
- Step 1** Log in to the IME using an account with administrator privileges.
 - Step 2** Choose **Configuration > sensor_name > 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—Specifies the IP address of the remote sensor from which you are downloading the KB.
- Directory—Specifies the path where the KB resides on the remote sensor.
- File Name—Specifies the filename of the KB.
- Username—Specifies the username corresponding to the user account on the remote sensor.
- Password—Specifies 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 IME using an account with administrator privileges.
 - Step 2** Choose **Configuration > sensor_name > 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—Specifies the IP address of the remote sensor to which you are uploading the KB.
- Directory—Specifies the path where the KB resides on the sensor.
- File Name—Specifies the filename of the KB.
- Virtual Sensor—Specifies the virtual sensor with which you want to associate this KB.
- Save As—Lets you save the KB as a new file name.
- Username—Specifies the username corresponding to the user account on the sensor.
- Password—Specifies 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 IME using an account with administrator privileges.
 - Step 2** Choose **Configuration > sensor_name > 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

This section describes how to display learned OS and imported OS maps for the sensor, and contains the following topics:

- [Configuring Learned Operating Systems, page 20-17](#)
- [Configuring Imported Operating Systems, page 20-18](#)

Configuring Learned Operating Systems

**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 maps 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 maps are immediately repopulated.

Field Definitions

The following fields are found in the Learned OS Pane:

- Virtual Sensor—Specifies the virtual sensor with which the OS value is associated.
- Host IP Address—Specifies the IP address to which the OS value is mapped.
- OS Type—Specifies 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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > 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.
-

For More Information

For detailed information on adding, editing, deleting, and moving configured OS maps, see [Adding, Editing, Deleting, and Moving Configured OS Maps, page 11-27](#).

Configuring Imported Operating Systems

**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 maps 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—Specifies the IP address to which the OS value is mapped.
- OS Type—Specifies 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 IME using an account with administrator privileges.
 - Step 2** Choose **Configuration > sensor_name > 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**.
-

For More Information

For detailed information about external product interfaces, see [Chapter 18, “Configuring External Product Interfaces.”](#)

Monitoring LACP

This section describes how to monitor LACP on your 4500 series sensor, and contains the following topics:

- [Displaying LACP Neighbors, page 20-19](#)
- [Displaying LACP Internals, page 20-20](#)

Displaying LACP Neighbors

The LACP Neighbor pane displays the list of the LACP neighbors with their system details. Click **Refresh** to update the list of LACP neighbors.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Field Definitions

The following fields are found in the LACP Neighbor pane:

- Interface—Displays the interface name.
- Flags—Displays the flags associated with this interface:
 - A—The device is in active mode.
 - F—The device is sending fast Link Aggregation Control Protocol Data Units (LACPDU).
 - S—The device is sending slow LACPDU.
 - P—The device is in passive mode.
- State—Displays the following states:
 - Independent—LACP is configured at the local end and LACP is not configured on a partner/other end, for example, no LACP partner PDU is received.
 - Bundled—LACP is configured on both ends and able to create a bundle successfully; this means the configuration is valid and able to create a bundle.
 - Suspended—LACP is configured on both ends, but the received partner information is invalid' this means there is an invalid configuration on the partner, such as half duplex on the link.
- Port Priority—Displays the port priority in interfaces that have LACP enabled. The range is 1 to 65535 with the higher number signifying a lower priority. The default is 32768. The port priority is only displayed with the port is in active or passive mode.
- Admin Key—Displays the administrative key, which is a 16-bit number used by LACP to manage aggregation. For the IPS, the channel ID is used as the administrative key. All members of the port channel have the same administrative key assigned by the system as the channel ID.
- Oper Key—Displays the operational key, which is a 16-bit number assigned to an interface signifying that it can aggregate with all of the other interfaces that are assigned the same operational key. The operational key matches the administrative key.
- Port Number—Displays the port number, which is a 16-bit number used as the port aggregation priority. The IPS generates a unique port number by concatenating the LACP node identification number with the port number.
- Port State—Displays the state variables of the local/partner port encoded as individual bits within a single octet:
 - LACP_Activity—Encoded in bit 0. This flag indicates the activity control value with regard to this link. Active LACP is encoded as a 1; passive LACP is encoded as a 0.
 - LACP_Timeout—Encoded in bit 1. This flag indicates the timeout control value with regard to this link. Short timeout is encoded as a 1; long timeout is encoded as a 0.

- Aggregation—Encoded in bit 2. If TRUE (encoded as a 1), this flag indicates that the system considers this link to be suitable for aggregation; this means, it is a potential candidate for aggregation. If FALSE (encoded as a 0), the link is considered to be Individual; this means, this link can be operated only as an individual link.
- Synchronization—Encoded in bit 3. If TRUE (encoded as a 1), the system considers this link to be IN_SYNC; this means, it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the system ID and operational key information transmitted. If FALSE (encoded as a 0), then this link is currently OUT_OF_SYNC; this means, it is not in the right aggregation.
- Collecting—Encoded in bit 4. TRUE (encoded as a 1) means collection of incoming frames on this link is definitely enabled; for example, collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. Its value is otherwise FALSE (encoded as a 0).
- Distributing—Encoded in bit 5. FALSE (encoded as a 0) means distribution of outgoing frames on this link is definitely disabled; for example, distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. Its value is otherwise TRUE (encoded as a 1).
- Defaulted—Encoded in bit 6. If TRUE (encoded as a 1), this flag indicates that the Actor's receive machine is using defaulted operational partner information, administratively configured for the partner. If FALSE (encoded as a 0), the operational partner information in use has been received in a LACPDU.
- Expired—Encoded in bit 7. If TRUE (encoded as a 1), this flag indicates that the actor's receive machine is in the EXPIRED state; if FALSE (encoded as a 0), this flag indicates that the actor's receive machine is not in the EXPIRED state.



Note The received values of defaulted and expired state are not used by LACP; however, knowing their values can be useful when diagnosing protocol problems.

- System Priority—Displays the system-wide priority setting that is assigned to this interface. It is a 16-bit value with a range of 1 to 65535 and a default of 32768. In most cases, we recommend that you use the default.
- System Mac—Displays the hard-coded System MAC address, which is used across the IPS interfaces to establish the port channel across the IPS.

For More Information

- For detailed information about LACP on the 4500 series sensors, see [Understanding ECLB Using LACP, page 7-15](#).
- For the procedure for enabling LACP on the 4500 series sensors, see [Configuring LACP, page 7-21](#).

Displaying LACP Internals

The LACP Internal pane displays the list of LACP internals and their details for the sensor interfaces. The output shows the channel listing, port, port state, channel group, mode, flags, and local information for each interface. Click **Refresh** to update the list of LACP internals.

Supported User Role

The following user roles are supported:

- Administrator
- Operator
- Viewer

Here is an example output of the LACP internal information:

```

Node Information
  Node Identification Information - 1
  System Priority - 32768

Interface Information
Interface - Gigabit Ethernet0/0
  Port State - indep
  Channel Id - 1
  Mode - LACP/Passive
  Local Information
    Flags - SP
    State - indep
    L A C P Port Priority - 32768
    Oper Key - 0x1
    Port Number - 0x105
    Port State - 0x7c
  Partner Information
    Flags - SP
    State - indep
    L A C P Port Priority - 0
    Oper Key - 0x0
    Port Number - 0x0
    Port State - 0x0
  State Machine
    Transmit S M - tx_p
    Receive S M - def
    Mux S M - col_dis
    P T X S M - no_p
  Rx States Events - INIT(begin)-> INIT(port_dis)-> PORT_DIS(lacp_en)->
  EXPIRED(ct_expired)-> INIT()-> INIT()-> INIT()-> INIT()-> INIT()-> INIT()
  Ptx States Events - NO_PERIODIC(no_periodic)-> NO_PERIODIC(short_timeout)->
  NO_PERIODIC(long_timeout)-> NO_PERIODIC()-> NO_PERIODIC()-> NO_PERIODIC()->
  NO_PERIODIC()-> NO_PERIODIC()-> NO_PERIODIC()-> NO_PERIODIC()
  Mux States Events - DETACHED(begin)-> DETACHED(outof_sync)-> DETACHED(outof_sync)->
  DETACHED(selected)-> WAITING(in_sync)-> WAITING(ready)-> ATTACHED(in_sync)->
  DETACHED()-> DETACHED()-> DETACHED()
  Tx States Events - TRANSMIT_PDU(ntl)-> TRANSMIT_PDU(ntl)-> TRANSMIT_PDU(ntl)->
  TRANSMIT_PDU(ntl)-> TRANSMIT_PDU()-> TRANSMIT_PDU()-> TRANSMIT_PDU()-> TRANSMIT_PDU()
  -> TRANSMIT_PDU()-> TRANSMIT_PDU()
  L A G

  State - no_partner
  Lag - 8000,02-49-50-53-04-05,0001,8000,0105), (0000,00-00-00-00-00-00,0000,0000,0000)

Counters
  Rx Cnt - 0
  Tx Cnt - 0
  Rx Marker Req Cnt - 0
  Tx Marker Req Cnt - 0
  Rx Marker Resp Cnt - 0
  Tx Marker Resp Cnt - 0
  Link Up Events Cnt - 1
  Link Down Events Cnt - 0

Internal Mem Stats
  Rx Alloc Buffer Cnt - 0

```

```
Rx Free Buffer Cnt - 0
Tx Alloc Buffer Cnt - 0
Tx Free Buffer Cnt - 0
```

```
Global Event Queue Information
No of Events - 0
```

Clearing Flow States

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

- [Clear Flow States Pane, page 20-22](#)
- [Clear Flow States Pane Field Definitions, page 20-22](#)
- [Clearing Flow States, page 20-23](#)

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.



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.

- 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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > *sensor_name* > 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.

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 Definition

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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > 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 are cleared.



Note To change the threat thresholds displayed in the Network Security gadget, choose **Configuration > sensor_name > 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 3-3](#).
- For the procedure for configuring sensor health, see [Configuring Sensor Health, page 19-16](#).
- For the procedure for configuring risk categories, see [Configuring Risk Category, page 11-31](#).

Generating a 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 IME 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 IME using an account with administrator privileges.
- Step 2** Choose **Configuration > sensor_name > 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.

Viewing Statistics

The Statistics pane shows statistics for the following categories:

- Analysis Engine
The Analysis Engine section also contains global correlation statistics.
- Anomaly Detection
- Event Store
- 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, 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 IME using an account with administrator or operator privileges.
- Step 2** Choose **Configuration** > *sensor_name* > **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 IME using an account with administrator or operator privileges.
 - Step 2** Choose **Configuration > *sensor_name* > 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.
-

