



CHAPTER 12

Monitoring the Sensor

This chapter describes how to monitor and clear the denied attackers list, how to monitor and configure active host blocks and network blocks, how to configure and manage rate limits, and how to configure and download IP logs. This chapter contains the following sections:

- [Configuring Denied Attackers, page 12-1](#)
- [Configuring and Managing Active Host Blocks, page 12-2](#)
- [Configuring and Managing Network Blocks, page 12-4](#)
- [Configuring and Managing Rate Limits, page 12-6](#)
- [Monitoring OS Identifications, page 12-10](#)
- [Monitoring Anomaly Detection, page 12-11](#)
- [Configuring IP Logging, page 12-19](#)

Configuring Denied Attackers



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.

Field Definitions

The following fields are found on the Denied Attackers pane:

- 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

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

-
- Step 1** Log in to IDM using an account with Administrator privileges.
- Step 2** Choose **Monitoring > 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**.
-

Configuring and Managing Active Host Blocks

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

- [Active Host Blocks Pane, page 12-2](#)
- [Active Host Blocks Pane Field Definitions, page 12-3](#)
- [Add Active Host Block Dialog Box Field Definitions, page 12-3](#)
- [Configuring and Managing Active Host Blocks, page 12-4](#)

Active Host Blocks Pane



Note You must be Administrator or Operator to configure active host blocks.



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

Use the Active Host Blocks pane to configure and manage blocking of hosts. An active 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. An active 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.

Active Host Blocks Pane Field Definitions

The following fields are found on the Active 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 Active Host Blocks

To configure and manage active host blocks, follow these steps:

-
- Step 1** Log in to IDM using an account with Administrator or Operator privileges.
 - Step 2** Choose **Monitoring > Active Host Blocks**, and then click **Add**.
 - 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.
- 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 Active Host Block dialog box, click **Cancel**.

Step 7 Click **Apply**.

The new active host block appears in the list in the Active Host Blocks pane.

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

Step 9 To delete a block, select an active host block in the list, and click **Delete**.

The Delete Active Host Block dialog box asks if you are sure you want to delete this block.



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

Step 10 Click **Yes** to delete the block.

The active host block no longer appears in the list in the Active Host Blocks pane.

Configuring and Managing Network Blocks

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

- [Network Blocks Pane, page 12-5](#)
- [Network Blocks Pane Field Definitions, page 12-5](#)

- [Add Network Block Dialog Box Field Definitions, page 12-5](#)
- [Configuring and Managing Network Blocks, page 12-6](#)

Network Blocks Pane

**Note**

You must be Administrator or Operator to configure network blocks.

**Note**

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

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 on 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 IDM using an account with Administrator or Operator privileges.
- Step 2** Choose **Monitoring > Network Blocks**, and then click **Add**.
- 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 and Managing Rate Limits

This section describes rate limiting and how to configure it. It contains the following sections:

- [Rate Limits Pane, page 12-7](#)
- [Rate Limits Pane Field Definitions, page 12-8](#)
- [Add Rate Limit Dialog Box Field Definitions, page 12-8](#)
- [Configuring and Managing Rate Limits, page 12-9](#)

Rate Limits Pane



Note

You must be Administrator or Operator to configure 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.

Understanding Rate Limiting

ARC is responsible for rate limiting traffic in protected networks. Rate limiting lets sensors restrict the rate of specified traffic classes on network devices. Rate limit responses are supported for the Host Flood and Net Flood engines, and the TCP half-open SYN signature. ARC can configure rate limits on network devices running Cisco IOS 12.3 or later. Master blocking sensors can also forward rate limit requests to blocking forwarding sensors.



Tip

To check the status of ARC, enter **show statistics network-access** at the `sensor#`. The output shows the devices you are managing, any active blocks and rate limits, and the status of all devices. Or in IDM, choose **Monitoring > Statistics** to see the status of ARC.

To add a rate limit, you specify the following:

- Source address and/or destination address for any rate limit.
- Source port and/or destination port for rate limits with TCP or UDP protocol.

You can also tune rate limiting signatures. You must also set the action to Request Rate Limit and set the percentage for these signatures.

Table 12-1 lists the supported rate limiting signatures and parameters.

Table 12-1 Rate Limiting Signatures

Signature ID	Signature Name	Protocol	Destination IP Address Allowed	Data
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	none
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	None
6910	Net Flood UDP	UDP	No	None

Table 12-1 Rate Limiting Signatures (continued)

Signature ID	Signature Name	Protocol	Destination IP Address Allowed	Data
6920	Net Flood TCP	TCP	No	None
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

For More Information

- For configuring rate limiting on routers, see [Configuring Router Blocking and Rate Limiting Device Interfaces, page 9-20](#).
- For more information on configuring a master blocking sensor to manage rate limits requests, see [Configuring the Master Blocking Sensor, page 9-27](#).
- For the procedure for adding a rate limit, see [Configuring and Managing Rate Limits, page 12-6](#).

Rate Limits Pane Field Definitions

The following fields are found on 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 Limits

To configure and manage rate limiting, follow these steps:

-
- Step 1** Log in to IDM using an account with Administrator or Operator privileges.
 - Step 2** Choose **Monitoring > Rate Limits**, and then click **Add**.
 - 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.
-

Monitoring OS Identifications

This section describes the Learned OS and Imported OS panes and how to monitor OS identifications. It contains the following topics:

- [Deleting and Clearing Values from the Learned OS Pane, page 12-10](#)
- [Deleting and Clearing Values from the Imported OS Pane, page 12-11](#)

Deleting and Clearing Values from the Learned OS Pane

**Note**

You must be Administrator to clear and delete learned OS mappings.

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**.

**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 that the OS value is associated with.
- Host IP Address—The IP address the OS value is mapped to.
- OS Type—The OS type associated with the IP address.
- Delete—Deletes the selected OS value from the list.
- Clear List—Removes all learned OS values from the list.
- Refresh—Refreshes the Learned OS pane.

Deleting and Clearing Learned OS Values

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

-
- Step 1** Log in to IDM using an account with Administrator privileges.
- Step 2** Choose **Monitoring > 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.
-

For More Information

For more information on passive OS fingerprinting and the sensor, see [Configuring OS Maps, page 6-25](#).

Deleting and Clearing Values from the Imported OS Pane

**Note**

You must be Administrator to clear and delete imported OS mappings.

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 on the Configuration > External Product Interfaces pane. To clear the list or delete one entry, select the row and click **Delete**.

Field Definitions

The following fields are found in the Imported OS pane:

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

Monitoring the Imported OS Values

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

-
- Step 1** Log in to IDM using an account with Administrator privileges.
 - Step 2** Choose **Monitoring > 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.
-

For More Information

For more information on external product interfaces, see [Chapter 10, “Configuring External Product Interfaces.”](#)

Monitoring Anomaly Detection

This section describes the Anomaly Detection pane, and contains the following topics:

- [Anomaly Detection Pane, page 12-12](#)
- [Anomaly Detection Pane Field Definitions, page 12-12](#)
- [Showing Thresholds, page 12-13](#)
- [Comparing KBs, page 12-14](#)
- [Saving the Current KB, page 12-15](#)
- [Renaming a KB, page 12-17](#)

- [Downloading a KB, page 12-17](#)
- [Uploading a KB, page 12-18](#)

Anomaly Detection Pane

**Note**

You must be Administrator to monitor anomaly detection KBs.

The Anomaly Detection pane displays the KBs for all virtual sensors. On 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

**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.

For More Information

For more information on KBs, see [The KB and Histograms, page 7-12](#)

Anomaly Detection Pane Field Definitions

The following fields 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.

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.

Showing Thresholds

**Note**

You must be Administrator to filter anomaly detection thresholds.

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.

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.
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 IDM using an account with Administrator privileges.
 - Step 2** Choose **Monitoring > 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



Note

You must be Administrator to compare KBs.

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.

Field Definitions

The following fields are found in the Differences between knowledge bases *KB_Name* and *KB_Name* dialog box.

- 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.

Field Definitions

The following fields are found in the Difference Thresholds between knowledge bases *KB_Name* and *KB_Name* window.

- 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 IDM using an account with Administrator privileges.
- Step 2** Choose **Monitoring > 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 click **Details**.
- The Difference Thresholds between knowledge bases *KB_Name* and *KB_Name* window appears displaying the details.
-

Saving the Current KB



Note You must be Administrator to save KBs.

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 IDM using an account with Administrator privileges.

Step 2 Choose **Monitoring > 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 IDM using an account with Administrator privileges.

Step 2 Choose **Monitoring > Anomaly Detection**.

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

The Save Knowledge Base dialog box appears.

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

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

To delete a KB, follow these steps:

**Note**

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

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

Step 2 Choose **Monitoring > 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 must be Administrator to rename KBs.

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



Note

You cannot rename the initial KB.

To rename a KB, follow these steps:

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

Step 2 Choose **Monitoring > 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



Note

You must be Administrator to download KBs.

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

Downloading a KB

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

-
- Step 1** Log in to IDM using an account with Administrator privileges.
- Step 2** Choose **Monitoring > 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 you are downloading the KB from.
- 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



Note You must be Administrator to upload KBs.

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 you are uploading the KB to.
- Directory—The path where the KB resides on the sensor.
- File Name—The filename of the KB.
- Virtual Sensor—The virtual sensor you want to associate this KB with.
- 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 IDM using an account with Administrator privileges.
 - Step 2** Choose **Monitoring > 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 you are downloading the KB to.
 - 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 that you want this KB to apply to.
 - 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 IP Logging

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

- [Understanding IP Logging, page 12-19](#)
- [IP Logging Pane, page 12-20](#)
- [IP Logging Pane Field Definitions, page 12-20](#)
- [Add and Edit IP Logging Dialog Boxes Field Definitions, page 12-21](#)
- [Configuring IP Logging, page 12-21](#)

Understanding IP Logging

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.



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.



Caution

Turning on IP logging slows system performance.

IP Logging Pane



Note

You must be Administrator 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 on the IP Logging pane:

- Log ID—ID of the IP log.
- Virtual Sensor—The virtual sensor the IP log is associated with.
- 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.
- Event Alert—Event alert, if any, that triggered the IP log.

- 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 in the Add and Edit IP Logging dialog boxes:

- Virtual Sensor—Lets you choose the virtual sensor from which you want to capture IP logs.
- IP Address—IP address of the host for which the log is being captured.
- Maximum Values—Lets you set the values for IP logging.
 - Duration—Maximum duration to capture packets.



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.

The range is 1 to 60 minutes. The default is 10 minutes.

- 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 IDM using an account with Administrator or Operator privileges.
 - Step 2** Choose **Monitoring > 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.
 - 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 undo 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**.
The Stop IP Logging dialog box appears.
- 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**.
The Save As dialog box appears.
- Step 15** Save the log to your local machine. You can view it with WireShark.
-