CHAPTER 3

Configuring Dashboards

This chapter describes dashboards, and how to add and delete them. It contains the following topics:

Understanding Dashboards

By default, the Health and Traffic dashboards with default gadgets are displayed. You can customize all dashboards. You can select from the available list of gadgets and drag and drop them into the default dashboards or you can create dashboards.

To add a dashboard, click **Add Dashboard**. To show the available gadgets you can add to a dashboard, click **Add Gadgets**.

Adding and Deleting Dashboards

You can display the available gadgets in the Dashboard pane and then drag and drop them into any dashboards that you have created.

IME has the following gadgets:

- Sensor Information—Displays the most important sensor information.
- Sensor Health—Displays two meters. The Sensor Health meter indicates overall sensor health status and the Network Security Health meter indicates overall network security status.

  The meters read Normal, Needs Attention, or Critical. Click **Details** to display the values or messages associated with the status.
- Licensing—Displays the licensing, signature version, and engine version of the sensor.

- Interface Status—Displays whether the interface is up or down, enabled or disabled, the speed and mode, and received and transmitted packet counts for each interface.
- Global Correlation Reports—Displays the alerts and the denied packets resulting from reputation data.
- Global Correlation Health—Displays the configuration status of global correlation and network participation.
- Network Security—Displays graphs of the alert counts (including Meta and Summary counts), the average threat rating and risk rating values and the maximum threat rating and risk rating values over a configured time period. The sensor aggregates these values every 10 seconds and puts them in one of three risk categories: red, yellow, or green.

  You can configure the risk value for each category in Event Action Rules as a threshold arrangement.
- Top Applications—Displays the top ten service ports that the sensor has observed over the past 10 seconds.
- CPU, Memory, & Load—Displays the current sensor CPU, memory, and disk usage. If the sensor has multiple CPUs, multiple meters are presented.

  Click the **i** icon to display the details about the usage.
- RSS Feed—A generic RSS feed gadget. By default, the data is fed from Cisco Security Advisories. You may customize the feed.
- Top Attackers—Displays the top number of attacker IP addresses that occurred in the last configured time interval.

  You can configure the top number of attacker IP addresses for 10, 20, or 30. You can configure the time interval to cover the last hour, last eight hours, or last 24 hours. And you can filter this information.
- Top Victims—Displays the top number of victim IP address that occurred in the last configured time interval.

  You can configure the top number of victim IP addresses for 10, 20, or 30. You can configure the time interval to cover the last hour, last eight hours, or last 24 hours. And you can filter this information.
- Top Signatures—Displays the top number of signatures that occurred in the last configured time interval. And you can filter this information.
- Attacks Over Time—Displays the attack counts in the last configured interval. Each set of data in the graph is the total alert counts that IME receives during each minute.

  You can configure the time interval to cover the last hour, last eight hours, or last 24 hours. And you can filter this information.

Note The top attackers, victims, signatures, and attacks over time come from the IME database. The RSS feed comes from the Cisco Security Advisories website. The Global Correlation Health and Reports gadgets get their data from the Cisco SensorBase Network.The other gadgets get their data from the get health and security status control transaction.

For More Information

- For information on customizing RSS feeds, see Configuring RSS Feeds, page 4-1.
- For the procedure for configuring filters, see Configuring Filters, page 3-16.

Understanding Gadgets

This section describes the IME gadgets, and contains the following topics:

Sensor Information Gadget

The Sensor Information gadget displays the following sensor information:

- Host name—Configured during initialization.
- IPS Version—Current installed IPS version.
- In Bypass—Whether interfaces are operating in bypass mode.
- Total Sensing Interfaces—Displays how many sensing interfaces your sensor platform has.
- Analysis Engine Status—Displays the running status of Analysis Engine. Unless Analysis Engine is initializing or being reconfigured, the status reads **Running Normally**.
- IP Address—Configured during initialization.
- Device Type—Displays your IPS sensor platform.
- Total Memory—Displays the total amount of memory available.
- Total Data Storage—Displays the total amount of data storage available.

Changing the Sensor Information Gadget Display

To change the title of the Sensor Information gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget

- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For a detailed description of Analysis Engine, see Understanding Analysis Engine, page 8-2.
- For a detailed description of bypass mode, see Configuring Bypass Mode, page 7-27.

Sensor Health Gadget

The Sensor Health gadget visually displays sensor health and network security information in two colored meters. The meters are labeled Normal, Needs Attention, or Critical according to an analysis of the specific metrics. The overall health status is set to the highest severity of all the metrics you configured. For example, if you configure eight metrics to determine the sensor health and seven of the eight are green while one is red, the overall sensor health is displayed as red.

Click the **i** icon by the Sensor Health graph to display the specific sensor health metrics, which are grouped according to yellow and red threshold levels.

To change the sensor health metrics, click **Details > Configure Sensor Health Metrics**, and you are taken to Configuration > *sensor_name* > Sensor Management > Sensor Health, where you can reconfigure the health metrics, and enable/disable the sensor health parameters.

The following sensor health metrics and their status are displayed:

- Inspection load
- Missed packet
- Signature update
- License time remaining
- Event retrieval
- Application failed
- In bypass mode
- Active interface down
- Global correlation
- Network participation

Click the **i** icon by the Network Security Health graph to display the specific network health metrics and their status. The colors reflect the risk and threat ratings gathered in the last five minutes, which are grouped in green, yellow, and red levels with red being the highest level of risk.

To change the threat thresholds, click **Details > Configure Thresholds**, and you are taken to Configuration > *sensor_name* > Policies > IPS Policies, > Risk Category where you can configure the threat thresholds.

To reset the network security health, click **Details > Reset Health Status**, and you are taken to Configuration > *sensor_name* > Sensor Monitoring > Properties > Reset Network Security Health, where you can reset the status and calculation of network security health.

Right-click in the meter to get a menu that lets you change the properties of the meters, print the information contained in the meters, and save the sensor and network health details.

Changing the Sensor Health Gadget Display

To change the title of the Sensor Health gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For the procedure for changing the threat thresholds, see Configuring Risk Category, page 8-31.
- For more information on bypass mode, see Configuring Bypass Mode, page 7-27.
- For the procedure for configuring sensor and network security health, see Configuring Sensor Health, page 18-17.
- For the procedure for resetting network security health, see Resetting Network Security Health, page 19-29.

Licensing Gadget

The Licensing gadget displays the following pertinent information about your license key and the status of other software updates:

- License Status—Tells you if you have a license key installed and when it expires.
- Signature Version—Displays the installed signature version.
  - Released On—Date this signature version was released.
  - Applied On—Date this signature version was applied.
  - Auto Update Status—Whether automatic update has checked for new versions.
- Engine version—Displays the installed signature engine version.
  - Released On—Date this signature engine was released.
  - Applied On—Date this signature engine was applied.
  - Auto Update Status—Last time automatic update checked for updates.

Changing the Licensing Gadget Display

To change the title of the Licensing gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

For the procedure for obtaining and installing the license key, see Configuring Licensing, page 18-12.

Interface Status Gadget

The Interface Status gadget displays the following information about each interface:

- Interface—The physical interface name (FastEthernet or GigabitEthernet).
- Link—Whether the interface is up or down.
- Enabled—Whether the interface is disabled or enabled.
- Speed—Whether the speed of the interface is Auto, 10 MB, 100 MB, or 1000 MB.
- Mode—Whether the interface is in promiscuous, inline interface, inline VLAN pair, or VLAN groups mode.
- Received packets—Total number of packets received on this interface.
- Transmitted packets—Total number of packets transmitted on this interface.

Changing the Interface Status Gadget Display

To change the title of the Interface Status gadget and the device whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

For more information about interfaces, see Chapter 7, “Configuring Interfaces.”

Global Correlation Reports Gadget

The Global Correlation Reports gadget displays the following information about reputation:

- Packets Denied Due to Global Correlation—Displays the percentage of malicious packets identified and whether any have been dropped due to global correlation.
- Total Packets Denied—Displays the total number of malicious packets that were identified and which ones were dropped because of global correlation criteria.

Changing the Global Correlation Reports Gadget Display

To change the title of the Global Correlation Reports gadget and the way information is displayed, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Method of display (pie chart, bar chart, or table)

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For a description of the reputation feature in global correlation, see Understanding Reputation, page 13-2.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 18-17.
- For more information on IME reporting, see Chapter 21, "Configuring and Generating Reports."

Global Correlation Health Gadget

The Global Correlation Health gadget displays the following information about global correlation:

- Global Correlation Health—Displays the status of global correlation.
  - Status of the Last Update Attempt—States whether global correlation is enabled or disabled and whether the last update was successful or failed. Click the **i** icon to view the description of the status.

    Note If the status reads `Disabled`, either global correlation is turned off or the sensor is unlicensed.

  - Time Since Last Successful Update—Indicates how long it has been since the last successful update.
  - Update Interval in Seconds—Indicates how many seconds between update intervals.
  - Update Server—Name of the global correlation server that performs the updates.
  - Update Server Address—IP address of the global correlation server that performs the updates.
- Counters—Displays the connection attempts.
  - Update Failures Since Last Success—How many failures have occurred since the last successful update.
  - Total Update Attempts—How many times the sensor has tried to update global correlation.
  - Total Update Failures—How many times the updates have failed.
- Current Versions—Displays the versions for the following components that the sensor checks for updates: drop, rule, ip, and config.
- Warnings—Number of warnings about global correlation.

- Network Participation—Displays the status of network participation.
  - Status—States whether connection status is good, has failed one to five times since the last successful connection, or has failed more than five times since the last successful connection. Click the **i** icon to view the description of the status.
- Counters—Displays the connection attempts.
  - Total connection attempts—How many times the connection has been attempted.
  - Total connection failures—How many times the connection has failed.
  - Connection failures since last success—How many connection failures have occurred since the last successful connection.
- Connection History—Displays all connection attempts and the results (successful or failure). Click the **i** icon to view the list of connection attempts.

Changing the Global Correlation Health Gadget Display

To change the title of the Global Correlation Health gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, change the title of the gadget.

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

For More Information

- For a description of the reputation feature in global correlation, see Understanding Reputation, page 13-2.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 18-17.
- For a description of Network Participation, see Understanding Network Participation, page 13-3.

Network Security Gadget

The Network Security gadget displays the following information about your network security:

- Alert counts including Meta and summary alerts.
- Average threat rating and risk rating values.
- Maximum threat rating and risk rating values over a designated time period.

These values are all aggregated by the sensor every 10 seconds and are categorized as green, yellow, or red with green being the most secure and red being the least. The overall network security value represents the least secure value from all virtual sensors.

The severity level for a given virtual sensor is calculated as follows:

- Red severity level if one or more red events have been detected on the sensor within the last *n* minutes, where *n* is a configured value that is defaulted to 5 minutes.
- Yellow severity level if one or more yellow events, but no red events, have been detected on the sensor within the last *n* minutes.

  Otherwise the severity level is green.

Choose **Configuration >** *sensor_name* **> Policies > Event Action Rules > rules0 > Risk Category** to configure risk categories and the risk values for green, yellow, and red as thresholds.

The top graph shows the number of events for each of the categories, such as total, red, yellow, and green events. It counts for alerts by severity or risk category. The lower graph shows the average risks versus the average threats, or the maximum risks versus the maximum threats. This information is categorized per virtual sensor.

Changing the Network Security Gadget Display

To change how the network security values are displayed in the Network Security gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- The device and virtual sensor
- Which graphs to display in the Number of Events graph (all, red, yellow, or green)
- Which graphs to display in the Risk vs. Threat graph (average risk vs. the average threat or the maximum risk vs. the maximum threat).

Step 3 Click **Apply**.

For More Information

For the procedure for changing the threat thresholds, see Configuring Risk Category, page 8-31.

Top Applications Gadget

The Top Applications gadget displays the top ten Layer 4 protocols that the sensor has discovered:

- TCP
- UDP
- ICMP
- IP

The Top Applications gadget gives you an on overall picture of the traffic mix on the sensor.

Changing the Top Applications Gadget Display

To change how the top applications are displayed in the Top Applications gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device whose information you want to display
- Method of display (pie chart, bar chart, or table)
- Virtual sensor whose information you want to display

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

CPU, Memory, & Load Gadget

The CPU, Memory, & Load gadget displays the sensor load, memory usage, and disk usage. If your sensor has multiple CPUs, multiple meters are displayed.

- Inspection Load—Indicates how much traffic inspection capacity the sensor is using.

  0 indicates that there is no traffic backup and 100 indicates that the buffers are completely backed up. Inspection load is affected by the following factors:

  - Rate of traffic that needs inspection
  - Type of traffic being inspected
  - Number of active connections being inspected
  - Rate of new connections per second
  - Rate of attacks being detected
  - Signatures active on the sensor
  - Custom signatures created on the sensor
- CPU Usage—Indicates how much of the CPU of the sensor is being used.
- Memory Usage
  - System—Amount of memory used for configuration and event storage.

    System memory is not used for traffic inspection. The number of configured virtual sensors affects system memory, but changes in traffic or attack rates do not affect system memory. System memory remains stable except when you are configuring the sensor.
  - Analysis Engine—A fixed amount of memory allocated to and used by Analysis Engine, which is part of SensorApp. The amount of memory that Analysis Engine is currently using is displayed here.
- Disk Usage
  - Boot—Contains the OS boot image and recovery image. This partitions is used when a system image is installed on the sensor.
  - Application Data—Contains the configuration data and IP log files.

Click the **i** icon to see the details of each usage.

Changing the Interface Status Gadget Display

To change the title of the CPU, Memory, & Load gadget and the sensor whose information it reflects, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner of the gadget.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Device

Step 3 Click **Apply** to save your changes, or click **Cancel** to discard your changes.

RSS Feed Gadget

By default, the RSS Feed gadget is directly fed from the Cisco Security Advisors site on Cisco.com. You can have the RSS Feed gadget display any RSS feed channel that you set up. You can make a gadget for each RSS feed that you want to monitor.

Changing the RSS Feed Gadget Display

To change how the RSS feeds are displayed in the RSS Feed gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Feed Channel URL

Step 3 Click **Apply**.

For More Information

For information on customizing RSS feeds, see Configuring RSS Feeds, page 4-1.

Top Attackers Gadget

The Top Attackers gadget displays the number of events for each top attacker IP address over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see. You can also choose to have DNS name resolution for each IP address.

Changing the Top Attackers Display

To change how the top attacker statistics are displayed in the Top Attackers gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Display form (bar chart, pie chart, or table)
- How many top attacker statistics to display at one time (10, 20, or 30)
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Check the **Resolve addresses** check box if you want to use DNS name resolution for each IP address.

Step 4 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Top Victims Gadget

The Top Victims gadget displays the number of events for each top victim IP address over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see. You can also choose to have DNS name resolution for each IP address.

Changing the Top Victims Display

To change how the top victim statistics are displayed in the Top Victims gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Display form (bar chart, pie chart, or table)
- How many top victim statistics to display at one time (10, 20, or 30)
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Check the **Resolve addresses** check box if you want to use DNS name resolution for each IP address.

Step 4 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Top Signatures Gadget

The Top Signatures gadget displays the top number of signatures over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see.

Changing the Top Signatures Display

To change how the top signatures statistics are displayed in the Top Signatures gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget

- Display form (bar chart, pie chart, or table)
- How many top signatures to display at one time (10, 20, or 30)
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Attacks Over Time Gadget

The Attacks Over Time gadget displays the number of attacks over a specified time. The graph is changed according to the time limit. You can also filter on various conditions to get only the information you want to see.

Changing the Attacks Over Time Display

To change how the attacks over time statistics are displayed in the Attacks Over Time gadget, follow these steps:

Step 1 Click the **Tool** icon in the upper right corner.

Step 2 In the Configure Settings window, you can change the following values:

- Title of the gadget
- Interval to gather the statistics (last one hour, last eight hours, last one day)
- Filter associated with this gadget

Step 3 Click **Apply**.

For More Information

For the procedure for configuring filters, see Configuring Filters, page 3-16.

Working with a Single Event for Individual Top Attacker and Victim IP Addresses

To work with a single event for a specific IP address for a top attacker or victim, follow these steps:

Step 1 Choose **Home > Dashboards > Dashboard**, and then click the tab of the dashboard for which you want to work with individual attacker or victim IP addresses.

Step 2 From the Events for drop-down list, choose an attacker or victim IP address, for example, **Attacker 51.66.166.10**.

Data are retrieved from the database and displayed. From this window, you can view the attacker or victim settings and change them, and you can view the event details.

Step 3 To work with a single event, select the event in the list, and then click **Event** on the toolbar.

From the Event drop-down list, you can view the following information (it also appears in the lower half of the window under Event Details displayed in tab form):

- Summary—Summarizes all information about that event.
- Explanation—Provides the description and related signature information about the signature associated with this event.
- Related Threats—Provides the related threats with a link to more detailed information in MySDN.
- Trigger Packet—Displays information about the packet that triggered the event.
- Context Data—Displays the packet context information.
- Actions Taken—Lists which event actions were deployed.
- Notes—Lets you take action on this event by assigning a designation for it (New, Assigned, Acknowledged, Closed, or Deleted). Add any notes in the Notes field and click **Save Note** to save it.

Step 4 To print the details of this event, click **Show All Details** to display the event details in a printer-friendly window.

Step 5 To add an attribute from a selected event, from the Filter drop-down menu, click **Add to Filter > Attacker IP/Victim IP/Signature ID**.

The Filter tabs appear in the upper half of the window.

Step 6 To create a filter from this event, from the Filter drop-down menu, click **Create a Filter**.

Step 7 To edit the signature associated with this event, click **Edit Signature**.

This takes you to Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures where you can edit the signature.

Step 8 To create an event action rules filter from this event, click **Create Rule**.

This takes you to Configuration > *sensor_name* > Policies > IPS Policies > Add Event Action Filter where you can add the event action rules filter.

Step 9 To stop the attacker, from the Stop Attacker drop-down menu, choose one of the following options:

- Using Inline Deny

  This takes you to Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Denied Attackers > Add Denied Attacker.

- Using Block on another device

  This takes you to Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks > Add Host Block.

Step 10 To use ping, traceroute, DNS, and whois on the IP addresses involved in this event, choose them from the Tools drop-down menu.

Step 11 To save, delete, or copy the event, from the Other drop-down list, choose the action you want to perform.

Step 12 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

For More Information

- For the procedure for adding filter rules, see Configuring Filters, page 3-16.
- For the procedure for adding an event action rules filter, see Configuring Event Action Filters, page 12-15.
- For the procedure for adding a denied attacker, see Configuring and Monitoring Denied Attackers, page 19-4.
- For the procedure for adding a host block, see Configuring Host Blocks, page 19-6.
- For more information on using tools, see Using Tools for Devices, page 2-6.

Working with a Single Event for a Top Signature

To work with a single event for a specific Signature ID, follow these steps:

Step 1 Choose **Home > Dashboards > Dashboard**, and then click the tab for the sensor for which you want to work with a specific event for a specific signature.

Step 2 From the Events for drop-down list, choose a signature ID, for example, **SigID 3142**.

Data are retrieved from the database and displayed. From this window, you can view the settings and change them, and you can view the event details.

Step 3 To work with a single event, select the event in the list, and then click **Event**.

From the Event drop-down list, you can view the following information (it appears in the bottom half of the window under Event Details, and the same menu items are displayed in tab form):

- Summary—Summarizes all information about that event.
- Explanation—Provides the description and related signature information about the signature associated with this event.
- Related Threats—Provides the related threats with a link to more detailed information in MySDN.
- Trigger Packet—Displays information about the packet that triggered the event.
- Context Data—Displays the packet context information.
- Actions Taken—Lists which event actions were deployed.
- Notes—Lets you take action on this event by assigning a designation for it (New, Assigned, Acknowledged, Closed, or Deleted). Add any notes in the Notes field and click **Save Note** to save it.

Step 4 To print the details of this event, click **Show All Details** to display the event details in a printer-friendly window.

Step 5 To add this event to a filter, from the Filter drop-down menu, click **Add to Filter > Attacker IP/Victim IP/Signature ID**.

The Filter tabs appear in the upper half of the window.

Step 6 To create a filter from this event, from the Filter drop-down menu, click **Create a Filter**.

Step 7 To edit the signature associated with this event, click **Edit Signature**.

This takes you to Configuration > *sensor_name* > Policies > Signature Definitions > sig0 > Active Signatures where you can edit the signature.

Step 8 To create an event action rule filter from this event, click **Create Rule**.

This takes you to Configuration > *sensor_name* > Policies > IPS Policies > Add Event Action Filter where you can add an event action rules filter.

Step 9 To stop the attacker, from the Stop Attacker drop-down menu, choose one of the following options:

- Using Inline Deny

  This takes you to Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Denied Attackers > Add Denied Attacker.

- Using Block on another device

  This takes you to Configuration > *sensor_name* > Sensor Monitoring > Time-Based Actions > Host Blocks > Add Host Block.

Step 10 To use Ping, Traceroute, DNS, and WHOIS on the IP addresses involved in this event, choose them from the Tools drop-down menu.

Step 11 To save, delete, or copy the event, from the Other drop-down list, choose the action you want to perform.

For More Information

- For the procedure for adding filter rules, see Configuring Filters, page 3-16.
- For the procedure for adding an event action rules filter, see Configuring Event Action Filters, page 12-15.
- For the procedure for adding a denied attacker, see Configuring and Monitoring Denied Attackers, page 19-4.
- For the procedure for adding a host block, see Configuring Host Blocks, page 19-6.
- For more information on using tools, see Using Tools for Devices, page 2-6.

Configuring Filters

To configure filters, follow these steps:

Step 1 Choose **Home > Dashboards**, and then click the tab of the dashboard for which you want to configure filter rules.

Step 2 Choose the gadget for which you want to apply filters, for example, the Top Attackers gadget.

You can apply filter rules to the Top Attackers, Top Victims, and Top Signatures gadgets.

Step 3 From the Events for drop-down menu, choose the IP address or signature ID to which you want to add a filter.

Step 4 Select the event(s) for which you want to apply filters.

Tip To select more than one item in the list, hold down the **Ctrl** key.

Step 5 Click **View Settings > Filter**.

Step 6 From the Filter Name drop-down menu, choose the filter name for this filter, or click the **Note** icon and then click **Add** to add a new filter:

Note The filtering fields now support IPv6 and IPv4 addresses.

a. In the Filter Name field, enter a name for this filter.

b. In the Attacker IP field, enter an attacker IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

c. In the Victim IP field, enter a victim IP address, or click the **Note** icon and add a unique IP address or a range of IP addresses, and then click **OK**.

d. In the Signature Name/ID field, enter a signature name or ID, or click the **Note** icon, and then choose a signature type, and click **OK**.

e. In the Victim Port field, enter a victim port, or click the **Note** icon and enter a victim port that meets the conditions you require, and then click **OK**.

f. Choose the severity levels you want for this filter.

g. In the Risk Rating field, enter the risk rating for this filter, or click the **Note** icon, and then enter the risk rating that meets the conditions you require, and click **OK**.

h. In the Reputation field, enter the reputation score for this filter, or click the **Note** icon, and then enter the reputation that meets the conditions you require, and click **OK**.

i. In the Threat Rating field, enter the threat rating for this filter, or click the **Note** icon, and then enter the threat rating that meets the conditions you require, and click **OK**.

j. In the Actions Taken field, enter the actions you want to trigger this filter, or click the **Note** icon, and then check the check boxes of the actions that you want to trigger this filter, and click **OK**.

k. In the Sensor Name(s) field, enter the names of the sensors that are affected by this filter, or click the **Note** icon, and check the check boxes of the sensor to which this filter applies and click **OK**.

l. In the Virtual Sensor field, enter the virtual sensor to which this filter applies.

m. From the Status drop-down menu, choose on which status you want to filter.

n. In the Victim Locality field, enter the name of any event action rules variable that you created on which you want to filter.

Step 7 To configure grouping, click the **Group By** tab:

o. Check the **Group events based on the following criteria** check box, and then set up the hierarchy of how you want to group the events by selecting the category from the drop-down menus.

p. Under Grouping Preferences, you can check the check boxes of the **Single Level**, **Show Group Columns**, or **Show Count Columns** check boxes.

You can only show count columns if you enable Show Group Columns.

Step 8 To add color rules, click the **Color Rules** tab, and then click **Add**.

a. In the Filter Name field, enter a name for this color rules filter.

b. Check the **Enable** check box.

Note If you do not check the **Enable** check box, your color rules filter do not go in to effect.

c. Under Packet Parameters, enter the IP addresses, signature names and/or victim ports for which you want this color rules filter to apply.

d. Under Rating and Action Parameters, enter the severity, risk rating, threat rating, and actions for which you want this color rules filter to apply.

e. Under Other Parameters, enter the sensor name, virtual sensor name, status, and/or victim locality for which you want this color rules filter to apply.

f. Under Color Parameters, choose the foreground and background colors, and the font type for this color rules filter, and then click **OK**.

Tip For aid in entering the correctly formatted values for these fields, click the **Note** icon.

Step 9 To event fields and their order, click the **Fields** tab, and then click **Add >>**, **<< Remove**, **Move Up**, and **Move Down** to chose which fields you want to display and to arrange the fields in the order in which you want to see them.

Step 10 Click the **General** tab, and then in the View Description field enter a description for your view.

Step 11 Click **Save As** to create the view, and then in the Name field, enter a name for your view.

The settings are copied to the new view.

Step 12 Click **Save** to save any changes to the view.

Your filter now appears in the Filter Name drop-down menu.

Step 13 To save any changes that you have made to the view, click **Apply**. To discard any changes, click **Reset**.

Manage Filter Rules Dialog Box Field Definitions

The following fields are found in the Manage Filter Rules dialog box:

- Basic Top Attacker Filter—Shows all severity levels (high, medium, low, and informational) for top attacker events.
- Action Denied-Attacker—Shows denied attacker actions, new alert status, and all severity levels (high, medium, low, and informational) for denied action events.
- Basic Over Time Attack Filter—Shows all severity levels (high, medium, low, and informational) for attacks over time events.
- Basic Top Signature Filter—Shows all severity levels (high, medium, low, and informational) for the top signature events.
- Basic Top Victim Filter—Shows all severity levels (high, medium, low, and informational) for top victims events.

- Related Events Filter—Shows all severity levels (high, medium, low, and informational) for related events.
- Critical Threat—Shows all threat ratings between 75 and 100, new alert status, and all severity levels (high, medium, low, and informational) for critical events.
- High Severity—Shows all alerts with a new alert status and high severity level for all events.
- Basic View Filter—Shows all severity levels (high, medium, low, and informational) for all events.
- Basic Filter—Shows new alert status and all severity levels (high, medium, low, and informational) for all events.

Add and Edit Filter Dialog Boxes Field Definitions

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

- Filter Name—Lets you name this filter or pick from the default filters.
- Attacker IP—Attacker IP address you want to include in this filter.

  The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.
- Victim IP—Victim IP address you want to include in this filter.

  The valid values are *ip_address*, *ip_address_range*, for example, 10.0.0.1, !10.0.0.1, !10.1.1.1.
- Signature Name/ID—Signature Name/ID you want to include in this filter.

  The valid values are *signature_name* or *signature_id* or *signature_id/subsig_id* or *signature_id_range*, for example:
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - 3300-400
- Victim Port—Victim port you want to include in this filter.

  The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Severity—Severity levels you want to include in this filter.
- Risk Rating—Risk rating you want to include in this filter.

  The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Reputation—Reputation score you want to include in this filter.

  The valid values are from -10.0 to 10.0.
- Threat Rating—Threat rating you want to include in this filter.

  The valid values are *number, number_range*, for example >=80, 70-100, <90, !100.
- Action(s) Taken—Lets you choose which actions the filter looks for in the alerts.

  The actions are a string that you can choose or you can enter free format strings.
- Sensor Name(s)—Lets you assign which sensors are included in this filter.
- Virtual Sensor—Lets you assign which virtual sensors are included in this filter.

- Status—Lets you assign a status to this filter (All, New Assigned, Closed, Detected, Acknowledged).

  The Status field is useful, for example, in a situation where you want to save analysis of certain events for later. You can add a note and change the status to 'Acknowledged,' and then later you can filter by status to see all cases that are acknowledged and then do further analysis.

- Victim Locality—An alert attribute in the participants/address alert on which you can filter. It is defined in the event action rules variables.