Configuring Dashboards

This chapter describes the sensor dashboards and gadgets, and contains the following topics:

Understanding Dashboards

By default, the Health dashboard with default gadgets is 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 new 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

To customize and add dashboards and gadgets, follow these steps:

Step 1 To add gadgets to a dashboard, choose **Home** and then click **Add Gadgets**. The nine gadget icons appear at the bottom of the Home pane.

Step 2 Click the tab of the dashboard you want to customize, and then drag and drop the gadget you want in to the dashboard.

Step 3 To customize the gadget, click the **Tool** icon in the upper-right corner. The Configure Settings pane appears. For the procedures for customizing the gadgets, see the individual sections on the gadgets.

Step 4 To add a dashboard, click **Add Dashboard**. A tab appears named **Untitled**.

Step 5 Double-click **Untitled** and enter the dashboard name on the tab.

Step 6 Click **Add Gadgets** and drag the desired gadget icons to the dashboard.

Step 7 To collapse the gadget, click the **Double Arrow** icon in the upper right corner of the gadget.

Step 8 To close the gadget, click the **X** icon in the upper right corner of the gadget.

For More Information

- For a general description of the gadgets, see Understanding Gadgets, page 2-2.
- For a detailed description of the individual gadgets, see Gadgets, page 2-3.

Understanding Gadgets

Note 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.

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

The IDM 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.
- Memory & Load—Displays the current sensor memory and disk usage. Click the **i** icon to display the details about the usage.

For More Information

- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.
- For more information on global correlation, see Chapter 11, “Configuring Global Correlation.”

Gadgets

This section describes the individual IDM gadgets, and contains the following topics:

Sensor Information Gadget

The Sensor Information gadget displays the following sensor information:

- Host Name—Displays the host name that was configured during initialization.
- IPS Version—Displays the current installed IPS version.
- In Bypass—Indicates whether the interfaces are operating in bypass mode.

Note The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

- Total Sensing Interfaces—Displays how many sensing interfaces your sensor platform has.
- Analysis Engine Status—Displays the running status of the Analysis Engine. If the Analysis Engine is initializing or being reconfigured, it reads **Processing Transaction**; otherwise the status reads **Running Normally**. Click the **i** icon to view a description of the Analysis Engine status. The following statuses are displayed:
  - Stage—Displays in a progress bar the stage of the Analysis Engine update.
  - Step—Displays in a progress bar any additional steps taken during an Analysis Engine update.
  - Activity—Lets you know when the Analysis Engine activity is complete.

Note The Stage, Step, and Activity bars disappear once the Analysis Engine update is complete.

- IP Address—Displays the IP address that was 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 information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.
- For more information on bypass mode, see Configuring Bypass Mode, page 5-31.
- For more information on interfaces, see Chapter 5, "Configuring Interfaces."
- For a description of the Analysis Engine, see Understanding Analysis Engine, page 6-2.

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 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

Note The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

- 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 > 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 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 information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.
- For the procedure for changing the threat thresholds, see Configuring Risk Category, page 6-37.
- For more information on bypass mode, see Configuring Bypass Mode, page 5-31.
- For more information on global correlation, see Chapter 11, “Configuring Global Correlation.”

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 and information about it. Click the **i** icon to view a description of the Signature Version:
  - Released On—Displays the date this signature version was released.
  - Applied On—Displays the date this signature version was applied.
  - Auto Update Status—Indicates whether automatic update has checked for new versions.
- Threat Profile Version—Displays the current threat profile version that is available to assign to the signature policy.
- Engine version—Displays the installed signature engine version and information about it. Click the **i** icon to view a description of Engine Version:
  - Released On—Displays the date this signature engine was released.
  - Applied On—Displays the date this signature engine was applied.
  - Auto Update Status—Displays the 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 17-11.
- For the procedure for obtaining IPS software, see Obtaining Cisco IPS Software, page 21-1.
- For the procedure for configuring automatic update, see Configuring Automatic Update, page 17-19.

Interface Status Gadget

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

- Interface—Displays the physical interface name (FastEthernet, GigabitEthernet, or PortChannel).
- Link—Indicates whether the interface is up or down.
- Enabled—Indicates whether the interface is disabled or enabled.

- Speed (Mbps)—Indicates whether the speed of the interface is Auto, 10 Mb, 100 Mb, 1000 Mb, or 10,000 Mb.
- Mode—Indicates whether the interface is in promiscuous, inline interface, inline VLAN pair, or VLAN groups mode.
- Received packets—Displays the total number of packets received on this interface.
- Transmitted packets—Displays the 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 5, "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 11-2.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.

Global Correlation Health Gadget

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

- Global Correlation Updates—Displays the status of global correlation:
  - Status of Last Update Attempt—Indicates 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—Displays the name of the global correlation server that performs the updates.
  - Update Server Address—Displays the IP address of the global correlation server that performs the updates.
- Counters—Displays the connection attempts:
  - Update Failures Since Last Success—Displays how many failures have occurred since the last successful update.
  - Total Update Attempts—Displays how many times the sensor has tried to update global correlation.
  - Total Update Failures—Displays 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—Displays the number of warnings about global correlation. Click the **i** icon to view the warnings.
- Network Participation—Displays the status of network participation:
  - Status—Indicates 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—Displays how many times the connection has been attempted.
  - Total Connection Failures—Displays how many times the connection has failed.
  - Connection Failures Since Last Success—Displays how many connection failures have occurred since the last successful connection.

- Connection History—Displays all of the connection attempts and the results (successful or failure).

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 11-2.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.
- For a description of network participation, see Understanding Network Participation, page 11-3.

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.

Chose **Configuration > Policies > Event Action Rules > rules0 > Risk Category** to configure risk categories and the risk values for green, yellow, and red 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 6-37.
- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.
- For a description of summary alerts, see Event Action Summarization, page 9-5 and Event Action Aggregation, page 9-5.
- For a detailed description of threat rating, see Understanding Threat Rating, page 9-4.
- For a detailed description of risk rating, see Calculating the Risk Rating, page 9-2.

Top Applications Gadget

The Top Applications gadget displays the top ten Layer 4 protocols that the sensor has discovered, which gives you an on overall picture of the traffic mix on the sensor:

- TCP
- UDP
- ICMP
- IP

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.

For More Information

For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.

Memory & Load Gadget

The Memory & Load gadget displays the sensor inspection load, memory usage, and disk usage.

- 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. Click the **i** icon to view the inspection load details. 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
- Memory Usage—Indicates how much memory the system and the Analysis Engine are using:
  - System—Displays the 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. Click the **i** icon to view a description of system memory.
  - Analysis Engine—Displays the fixed amount of memory allocated to and used by the Analysis Engine, which is part of the SensorApp. The amount of memory that the Analysis Engine is currently using is displayed here. Click the **i** icon to view a description of the Analysis Engine memory.
- Disk Usage—Indicates the amount of disk usage. Click the **i** icon to see the details of each usage.
  - Boot—Displays the amount of boot disk usage, which contains the OS boot image and recovery image. This partitions is used when a system image is installed on the sensor. Click the **i** icon to view a description of the boot partition.
  - System—Displays the amount system disk usage, which contains the system and application files loaded on the sensor. The amount changes after a software update. Click the **i** icon to view a description of the system partition.
  - Application Log—Displays the amount of application log used. Click the **i** icon to view the details.
  - Application Data—Displays the amount of application disk usage, which contains the configuration data and IP log files. The amount changes according to the number of configured virtual sensors and the number of IP logs stored on the device. Click the **i** icon to view the details of the application data partition.

Changing the Memory & Load Gadget Display

To change the title of the 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.

For More Information

- For information on configuring the sensor health metrics that are displayed in gadgets, see Configuring Sensor Health, page 17-16.
- For a description of the Analysis Engine, see Understanding Analysis Engine, page 6-2.