



## CHAPTER 2

# Configuring Dashboards

---

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

- [Understanding Dashboards, page 2-1](#)
- [Adding and Deleting Dashboards, page 2-1](#)
- [Understanding Gadgets, page 2-2](#)
- [Gadgets, page 2-2](#)

## 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:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | To add gadgets to a dashboard, choose <b>Home</b> and then click <b>Add Gadgets</b> . The seven gadget icons appear at the bottom of the Home pane.   |
| <b>Step 2</b> | Click the tab of the dashboard you want to customize, and then drag and drop the gadget you want in to the dashboard.   |
| <b>Step 3</b> | To customize the gadget, click the <b>Tool</b> 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. |
| <b>Step 4</b> | To add a dashboard, click <b>Add Dashboard</b> . A tab appears named <b>Untitled</b> .  |
| <b>Step 5</b> | Double-click <b>Untitled</b> and enter the dashboard name on the tab.   |
| <b>Step 6</b> | Click <b>Add Gadgets</b> and drag the desired gadget icons to the dashboard.  |
| <b>Step 7</b> | To collapse the gadget, click the <b>Double Arrow</b> icon in the upper right corner of the gadget.   |
| <b>Step 8</b> | To close the gadget, click the <b>X</b> 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 2-2](#).

## Understanding Gadgets

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

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.
- **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.

**For More Information**

For information on configuring the sensor health metrics that are displayed in gadgets, see [Configuring Sensor Health, page 15-16](#).

## Gadgets

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

- [Sensor Information Gadget, page 2-3](#)
- [Sensor Health Gadget, page 2-3](#)
- [Licensing Gadget, page 2-5](#)
- [Interface Status Gadget, page 2-5](#)
- [Network Security Gadget, page 2-6](#)

- [Top Applications Gadget, page 2-7](#)
- [CPU, Memory, & Load Gadget, page 2-8](#)

## 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 information on configuring the sensor health metrics that are displayed in gadgets, see [Configuring Sensor Health, page 15-16](#).
- For more information on bypass mode, see [Configuring Bypass Mode, page 5-25](#).
- For more information on interfaces, see [Chapter 5, “Configuring Interfaces.”](#)
- For a description of 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
- Active interface down

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:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Click the <b>Tool</b> icon in the upper right corner of the gadget.   |
| <b>Step 2</b> | In the Configure Settings window, you can change the following values: <ul style="list-style-type: none"><li>• Title of the gadget</li><li>• Device</li></ul> |
| <b>Step 3</b> | Click <b>Apply</b> to save your changes, or click <b>Cancel</b> 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 15-16](#).
- For the procedure for changing the threat thresholds, see [Configuring Risk Category, page 6-29](#).
- For more information on bypass mode, see [Configuring Bypass Mode, page 5-25](#).

## 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 15-13](#).
- For the procedure for obtaining IPS software, see [Obtaining Cisco IPS Software, page 19-1](#).
- For the procedure for configuring Automatic Update, see [Configuring Automatic Update, page 15-18](#).

## 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 5, “Configuring Interfaces.”](#)

## 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 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 6-29](#).
- For information on configuring the sensor health metrics that are displayed in gadgets, see [Configuring Sensor Health, page 15-16](#).
- 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 6-4](#).

## 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.

---

#### For More Information

For information on configuring the sensor health metrics that are displayed in gadgets, see [Configuring Sensor Health](#), page 15-16.

## 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.
- 

### For More Information

- For information on configuring the sensor health metrics that are displayed in gadgets, see [Configuring Sensor Health, page 15-16](#).
- For a description of Analysis Engine, see [Understanding Analysis Engine, page 6-2](#).

