



CHAPTER 2

Configuring Device Lists

You can add devices to IME in the Device List pane and view important information about each device. This chapter describes the Device List pane and how to add devices. It contains the following sections:

- [Device List Pane, page 2-1](#)
- [Device List Pane Field Definitions, page 2-2](#)
- [Add and Edit Device List Dialog Boxes Field Definitions, page 2-3](#)
- [Adding, Editing, and Deleting Devices, page 2-3](#)
- [Starting, Stopping, and Displaying Device, Event, and Health Status, page 2-4](#)
- [Using Tools for Devices, page 2-5](#)

Device List Pane

IME manages up to five Cisco IPS devices. The upper half of the Device List pane displays pertinent information about each device.

You can customize which columns you want to view and which you want to hide by clicking the column button in the far-right corner of the pane to bring up the Choose Columns to Display dialog box.

From this pane, you can add, edit, or delete a sensor in the device list. You can start and stop the health and events connections for a sensor and you can view the status of a sensor. You can also obtain information about the sensor by using tools such as ping, trace route, whois, and DNS lookup.

You can use the **Add**, **Edit**, **Delete**, **Start**, **Stop**, **Status**, and **Tools** buttons in the Device List table, or you can select the sensor in the table and use the right-click menu.

In the lower half of the Device List pane, the IME health monitoring center displays the details about the sensor you have selected in the upper half of the pane. The data displayed here match the information in the customizable dashboard gadgets.

The Device Details pane contains the following details about the selected sensor:

- **Sensor Health**—Sensor health and network security health information shown in graph form.
You can click **Details** to obtain the specifics about the sensor health and network security health.
If you want to change the sensor health metrics, choose **Details > Configure Sensor Health Metrics**, and you are taken to **Configuration > sensor_name > Sensor Management > Sensor Health**, where you can reconfigure the health metrics.

If you want to change the threat thresholds, choose **Details > Configure thresholds**, and you are taken to **Configuration > sensor_name > Policies > IPS Policies**, where you can configure the threat thresholds.

If you want to reset the network security health, choose **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.

- **Sensor Information**—Displays the host name, IPS version, whether the sensor is using inline bypass, the total sensing interfaces, the sensor IP address, the device type, the total memory, and the total data storage.

Under Analysis Engine Status, you can view whether Analysis Engine is running or which state it is in.

- **CPU, Memory, and & Load**—Displays the CPU, memory, and sensor load in graph form.
- **Licensing**—Displays all of the pertinent license information.
- **Interface Status**—Displays the interface name, link status, whether it is enabled, the speed, the mode, and the received and transmitted packets.

For More Information

- For the procedure for configuring sensor and network security health, see [Configuring Sensor Health, page 17-14](#).
- For the procedure for changing threat thresholds, see [Configuring Risk Category, page 8-25](#).

Device List Pane Field Definitions

The following fields are found in the Device List pane:

- **Time**—If there is a problem with the synchronization between your local system and a sensor that you have added, an icon appears in the time field. If the local system and the sensor are synchronized, the field is empty.



Caution

If the time is not synchronized between the sensor and the local system, you do not receive accurate monitoring and reporting.

- **Device Type**—Displays the IPS model name.
- **Event Status**—Informs you that IME is connecting to the sensor to receive events.
- **Sensor Health**—Informs you whether the sensor health is normal or needs attention.
- **Version**—Displays the installed Cisco IPS software version.
- **License Expiration**—Informs you about how many days until the sensor license expires.
- **Load**—Displays the load percentage.
- **Memory**—Displays the memory percentage.
- **CPU**—Displays the percentage the CPU is using.
- **Signature Version**—Displays the current signature version.
- **Device Name**—Name that you gave this sensor.
- **IP Address**—IP address of this sensor.

Add and Edit Device List Dialog Boxes Field Definitions

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

- **Sensor Name**—Name of the sensor you are adding.
- **Sensor IP Address**—IP address of the sensor you are adding.
- **User Name**—Name of user account allowed to access this sensor.
- **Password**—Password of the user account allowed to access this sensor.
- **Web Server Port**—TCP port used by the web server.

The default is 443 for HTTP or HTTPS. You receive an error message if you enter a value out of the range of 1 to 65535.

- **Communication protocol**—Enables TLS and SSL in the web server.

The default is Use encrypted connection (https). We strongly recommend that you use an encrypted connection.

- **Event Start Time (UTC)**—Lets you choose to have the latest alerts retrieved or you can select the start date and time of alerts to retrieve.
- **Exclude alerts of the following severity level(s)**—Lets you choose to exclude security levels from retrieval. The default is for all security levels to be displayed.

Adding, Editing, and Deleting Devices

To add, edit, and delete devices, follow these steps:

Step 1 Choose **Home > Devices > Device List**, and then click **Add**.

Step 2 Fill in the required fields in the Add Device dialog box:

- Enter the sensor name and sensor IP address of the sensor you are adding.
- Enter the user name and password of the person who will have access to this sensor.
- To change the default web server port, enter a new port number.
- Choose the communication protocol.



Note We strongly recommend that you use an encrypted connection.

- Choose the event start time by either checking the **Latest Alerts** check box or entering a start date and time in the Start Date and Start Time fields.
- Under Exclude alerts of the following severity level(s), check the check boxes of any levels you want to exclude.
The default is to have all of the levels configured.
- Click **OK** to add the sensor to the IME system.

Step 3 Click **Yes** to accept the certificate and continue the HTTPS connection with the sensor.



Note If you click **No** you reject the certificate and IME cannot connect to the sensor.

IME checks the time setting between IME and the sensor to make sure it is correct. If it is not, you receive a warning message if the sensor time and the IME system are more than five minutes apart. Make sure you synchronize the sensor with your system.

**Caution**

Having the correct time is very important so that reports, historical events, and the top gadgets are accurate. If the time is not within the range of five minutes, an icon appears next to the device in the Device Lists pane.

Step 4 To edit a device, select it in the list, click **Edit**, make any changes needed, and then click **OK**.

**Note**

You cannot change the Sensor Name because it is a key for the IME database.

Step 5 To delete a device, select it in the list, and then click **Delete**.

The device no longer appears in the Device List pane.

Starting, Stopping, and Displaying Device, Event, and Health Status

IME queries the sensor every 10 seconds to obtain health status information as long as you choose **Start > Health Connection**. IME pulls alerts from the sensor as long as you choose **Start Events Connection**.

There are some situations in which you might want to stop the sensor from polling events. For example, you can stop polling events from a specific sensor if you do not want its real-time events interfering when you are analyzing the events of another sensor. Then you can resume after the polling is done. Or you can stop polling health and security if you want to look at a snapshot of the status without the 10-second update.

To start, stop, and display event and health status, follow these steps:

Step 1 Select the sensor in the device list for which you want to start or stop event and health status.

Step 2 Choose **Start** or **Stop > Health Connection** or **Events Connection**.

The column now reads Connected or Not Connected.

Step 3 To display the connection status of IME to the sensor, the sensor version, and statistics information, select the sensor in the list, and then click **Status**.

The following IPS component statistics are displayed:

- Analysis Engine
- Anomaly Detection
- Event Store
- External Product Interface
- Host
- Interface

- Network Access
- Notification
- OS Identification
- SDEE Server
- Transaction Server
- Virtual Sensor
- Web Server

Step 4 To display details about a sensor, select it in the list, and then view the information displayed in the Device Details section of the pane.

To change the metrics that you see in the Device Details pane, go to **Configuration > sensor_name > Sensor Management > Sensor Health**.

Using Tools for Devices

You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

To use tools for devices, follow these steps

Step 1 Choose **Home > Devices**.

Step 2 To obtain ping statistics for a sensor, select it in the device list table, and then click **Tools > Ping**.
The Executing command - ping dialog box appears displaying the ping statistics for that sensor.

Step 3 To find the route of the IP packet, select the sensor in the list, and then click **Tools > Traceroute**.
The Executing command - traceroute dialog box appears displaying the trace route statistics for that sensor.

Step 4 To find the whois information, select the sensor in the list, and then click **Tools > WhoIs**.
The Executing command - whois dialog box appears displaying the WHOIS statistics for that sensor.

Step 5 To find the DNS information, select the sensor in the list, and then click **Tools > DNS**.
The Executing command - nslookup dialog box appears displaying the DNS lookup statistics for that sensor.
