Configuring Device Lists

You can add devices to the 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

The IME manages up to ten 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 Device List 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** next to the Sensor Health and Network Security graphs 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, the total data storage, and the status of Analysis Engine.
- Memory and & Load—Displays the memory and sensor load usage in graph form.

  Click **Details** next to the Inspection Load graph to see a detailed description of how the inspection load is determined.
- Licensing—Displays all of the pertinent license, signature version, and signature engine version information.
- Interface Status—Displays the interface name, link status, whether it is enabled, the speed, the mode, and the received and transmitted packets.
- Global Correlation Health—Displays the configuration status of global correlation and network participation.

For More Information

- For the procedure for configuring sensor and network security health, see Configuring Sensor Health, page 19-16.
- For the procedure for changing threat thresholds, see Configuring Risk Category, page 11-31.
- For the procedure for resetting network security health, see Resetting Network Security Health, page 20-23.
- For more information about global correlation, see Chapter 13, "Configuring Global Correlation."

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.

  Note If the time in not synchronized between the sensor and the local system, you do not receive accurate monitoring and reporting.
- Device Name—Displays the name that you gave the sensor.
- IP Address—Displays the IP address of the sensor.
- Device Type—Displays the IPS model name.
- Event Status—Informs you that the IME is connecting to the sensor to receive events.
- Sensor Health—Informs you whether the sensor health is normal or needs attention.
- Global Correlation Status—Informs you of the global correlation status of the sensor.

- 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.

For More Information

- For information about time and the sensor, see Configuring Time, page 6-7.
- For more information about sensor health metrics, see Configuring Sensor Health, page 19-16.
- For more information about global correlation, see Chapter 13, “Configuring Global Correlation.”
- For more information about licensing the sensor, see Configuring Licensing, page 19-12.
- For the procedure for obtaining the latest IPS software, see Obtaining Cisco IPS Software, page 25-1.

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—Specifies the name of the sensor you are adding.
- Sensor IP Address—Specifies the IP address of the sensor you are adding.
- Web Server Port—Specifies the 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.
- Authentication—Lets you specify separate credentials for configuration and event subscription:
  - Configuration User Name—Specifies the name of user account allowed to configure this sensor.
  - Configuration Password—Specifies the password of the user account allowed to configure this sensor.
  - Use the Same Account for Configuration and Event Subscription (This is not recommended)—Lets you have the same account apply to users who can configure and monitor the sensor.

Caution Using the same credentials for both configuration and event retrieval is not as secure as maintaining separate user accounts. We recommend that you maintain separate accounts and that the configuration user name have an administrator user role and the event subscription user name have a viewer user role.

  - Event Subscription User Name—Specifies the name of user account allowed to view events on this sensor.
  - Event Subscription Password—Specifies the password of the user account allowed to view events on this sensor.

- 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.

For More Information

For the procedures for recovering sensor passwords, see Recovering the Password, page 19-4.

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:

a. Enter the sensor name and sensor IP address of the sensor you are adding.

b. To change the default web server port, enter a new port number.

c. Choose the communication protocol.

Note We strongly recommend that you use an encrypted connection.

d. Enter the user name and password of the account that will configure this sensor.

e. Enter the user name and password of the person who will monitor the event subscription for this sensor.

Caution Using the same credentials for both configuration and event retrieval is not as secure as maintaining separate user accounts. We recommend that you maintain separate accounts and that the configuration user name have an administrator user role and the event subscription user name have a viewer user role.

f. 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.

g. 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.

h. 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. The IME checks the time setting between the 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.

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

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.

For More Information

For more information about correcting time on the sensor, see Correcting Time on the Sensor, page 6-12.

Starting, Stopping, and Displaying Device, Event, Health, and Global Correlation Connection Status

The IME queries the sensor every 10 seconds to obtain health status information as long as you choose **Start > Health Connection**. The IME pulls alerts from the sensor as long as you choose **Start > Events Connection**. The IME sends and receives global correlation data as long as you choose **Start > Global Correlation 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, health, and global correlation connection status, follow these steps:

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

Step 2 Choose **Start** or **Stop > Health Connection** or **Events Connection** or **Global Correlation Connection**. The column now reads Connected or Not Connected.

Step 3 To display the connection status of the 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 in the Device Status dialog box:

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

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

Step 4 To update the contents of the Device Status dialog box, click **Refresh**.

Step 5 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 health metrics that you see in the Device Details pane, go to **Configuration >** *sensor_name* **> Sensor Management > Sensor Health**. To change the global correlation metrics that you see in the Device Details pane, go to **Configuration >** *sensor_name* **> Policies > Global Correlation**.

For More Information

- For more information about sensor health metrics, see Configuring Sensor Health, page 19-16.
- For more information about global correlation, see Chapter 13, "Configuring Global Correlation."

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 - dnslookup dialog box appears displaying the DNS lookup statistics for that sensor.