IDS Device Manager Monitoring Tasks

This chapter describes how to set up monitoring from the Monitoring tab.

This chapter contains the following sections:
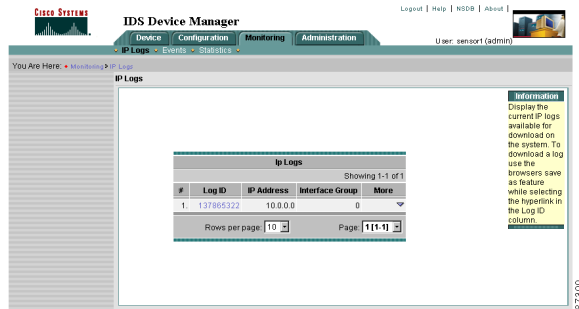
Downloading IP Logs

The Ip Logs page displays all IP logs that are available for downloading on the system. There is a hyperlink to each log file that is available for download. First, you have to turn on IP logging from Administration > IP Logging. The results of what you configure on that page show up in the list on the Ip Logs page. See Configuring IP Logging, page 5-5, for the procedure. You can also generate IP logs by setting a signature's EventAction to log. When the sensor detects an attack based on this signature, it automatically creates an IP log. See Configuring Signatures, page 3-1, for more information.

To download an IP log file, follow these steps:

Step 1   Select **Monitoring > IP Logs**.

The Ip Logs page appears.

Figure 4-1   Ip Logs Page

Step 2   Click the hyperlink for the log file that you want to download in the Log ID column.

Another page displays the IP log file.

Step 3   To save the file to a directory on your local hard disk drive, click **Save As** in your browser.

Configuring Event Display

Use the Events page to configure how you want events displayed. You can filter events based on event type, time, or both. By default, all events are displayed.

To configure the events display, follow these steps:

Step 1 Select **Monitoring > Events**.

The Events Display page appears.

Figure 4-2   Events Display Page

Step 2 To show alerts, select the Show Alerts check box.

Step 3 Select one or more check boxes next to the level of alerts you want to see:

- Informational
- Low
- Medium
- High

Step 4 To show all debug events, select the **Show Debug Events** check box.

Step 5 To show error events, select the **Show Error Events** check box.

Step 6 Select one or more check boxes next to the types of error events that you want to see:

- Warning
- Error
- Fatal

Step 7 To show log events, select the **Show Log Events** check box.

Step 8 To show network access controller (NAC) events, select the **Show Network Access Controller Events** check box.

Step 9   To show status events, select the **Show Status Events** check box.

Step 10   To view events within a specified time frame, follow these steps:

  a. Enter a time in the Start Time field (hh:mm:ss).

  b. Enter a date in the Start Date field (month:dd:yyyy).

  c. Enter a time in the End Time field (hh:mm:ss).

  d. Enter a date in the End Date field (month:dd:yyyy).

> ✎
>
> **Note**   You cannot leave the Time or Date fields blank.

Step 11   To specify events from a certain time range, enter a time range (1–65535) in the Past Hours field.

> ✎
>
> **Note**   To reset the form, click **Reset**.

Step 12   Click **Apply to Sensor** to save your changes.

The Events page lists the events you just selected.

Viewing Sensor Statistics

The Statistics page shows statistics for the following categories:

- WebServer
- TransactionSource
- TransactionServer
- NAC
- Logger
- Host
- EventStore
- EventServer

- AnalysisEngine
- Authorization

To show statistics for your sensor, follow these steps:

Step 1 Select **Monitoring > Statistics**.

The Statistics page appears.

Figure 4-3   Statistics Page

Step 2 To update the statistics as they change, click **Statistics** again or click **Reload** in your browser.