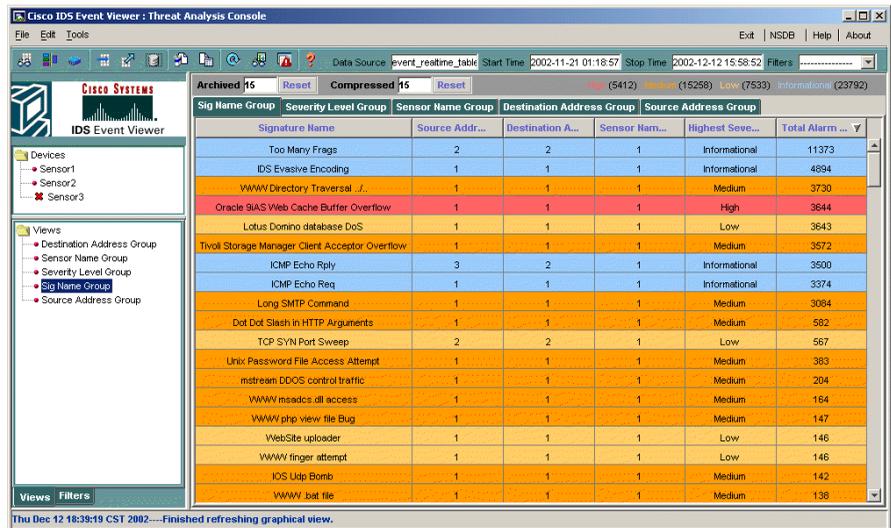




IDS Event Viewer Introduction

IDS Event Viewer is a Java-based application that enables you to view and manage alarms for up to five sensors. With IDS Event Viewer you can connect to and view alarms in real time or in imported log files. You can configure filters and views to help you manage the alarms. You can also import and export event data for further analysis. IDS Event Viewer also provides access to the Network Security Database (NSDB) for signature descriptions.

Figure 6-1 *IDS Event Viewer*



83732

System Requirements

IDS Event Viewer can be installed on the following platforms (English version only):

- Windows NT 4 Service Pack 6.
- Windows 2000 Service Pack 2.

IDS Event Viewer installs and uses the following support applications:

- Java 2 Runtime Environment Version 1.3.1.
- MySQL server Version 3.23.

IDS Event Viewer can be installed on a system that meets or exceeds the following minimum hardware requirements:

- Pentium III 800 Mhz or greater.
- 256 MB Ram.
- 500 MB free disk space.

Working with IDS Event Viewer

IDS Event Viewer enables you to view and manage alarm feeds from up to five sensors. The following task flow outlines the high-level tasks for configuring and working with IDS Event Viewer.

Step 1 Install and start IDS Event Viewer.



Warning

You cannot upgrade from version 3.1 to version 4.0. If you have IDS Event Viewer 3.1, you must uninstall that version before installing version 4.0.

For more information, see the following references:

1. [Installing IDS Event Viewer, page 6-4](#)
2. [Uninstalling IDS Event Viewer, page 6-5](#)
3. [Starting IDS Event Viewer, page 6-6](#)

- Step 2** Specify the devices you will monitor with IDS Event Viewer.
For more information, see the following references:
1. [Adding a Device, page 6-7](#)
 2. [Reviewing Device Status, page 6-10](#)
 3. [Accessing the IDS Device Manager, page 6-12](#)
- Step 3** Configure filters and views to specify the alarms you want to view.
For more information, see the following references:
1. [Creating a Filter, page 6-13](#)
 2. [Creating a View, page 6-18](#)
- Step 4** Configure refresh cycle settings and database archival settings and verify application settings.
For more information, see the following references:
1. [Configuring Refresh Cycle Settings, page 6-21](#)
 2. [Configuring Data Archival Settings, page 6-23](#)
 3. [Specifying Web Browser Application Location, page 6-25](#)
 4. [Specifying Ethereal Application Location, page 6-27](#)
 5. [Specifying NSDB Folder Location, page 6-28](#)
 6. [Changing the Auto Refresh View Setting, page 6-29](#)
- Step 5** View the events and individual alarms.
For more information, see the following references:
1. [Viewing Event Data, page 6-30](#)
 2. [Working with Alarms, page 6-41](#)
- Step 6** Maintain the database by importing, exporting, and deleting event data.
For more information, see [Database Administration, page 6-44](#)
-

Installing IDS Event Viewer

The following procedure assumes that you have downloaded the IDS Event Viewer executable file to the appropriate host.



Warning

You cannot upgrade from version 3.1 to version 4.0. If you have IDS Event Viewer 3.1, you must uninstall that version before installing version 4.0. Refer to [Uninstalling IDS Event Viewer, page 6-5](#), for more information.

Before You Begin

You must be logged in to the host as a user with administrative privileges to install IDS Event Viewer.

To install IDS Event Viewer, follow these steps:

-
- Step 1** Locate and double-click the IDS Event Viewer executable to start the setup program.
The Welcome panel of the IDS Event Viewer setup program appears.
 - Step 2** Click **Next** to proceed with the setup program.
The Select Destination Location panel appears.
 - Step 3** To accept the default location for the IDS Event Viewer files, click **Next**. Otherwise, click **Browse** to locate a different folder, and then click **Next**.
The Select Program Manager Group panel appears.
 - Step 4** Click **Next** to proceed with the setup program.
The Start Installation panel appears.
 - Step 5** Click **Next** to proceed with the setup program.
The Installing panel appears.
 - Step 6** Click **Next** to proceed with the setup program.
The Installation Complete panel appears.

- Step 7** Click **Finish** to complete the IDS Event Viewer setup program.
The Install popup window appears.
- Step 8** You must reboot this host to complete the IDS Event Viewer installation. Click **OK** to reboot the host.
-

Uninstalling IDS Event Viewer

You cannot upgrade from version 3.1 to version 4.0. Instead, you must uninstall 3.1 before installing version 4.0.

To uninstall IDS Event Viewer, follow these steps:

-
- Step 1** Choose **Start > Programs > Cisco Systems > Cisco IDS Event Viewer > Uninstall Cisco IDS Event Viewer**.

The Select Uninstall Method panel appears.

- Step 2** Select **Automatic**, and then click **Next**.

The Perform Uninstall panel appears.

- Step 3** Click **Finish** to continue with the uninstallation.

If you are uninstalling 3.1, the uninstallation program does not remove the paths that were created when 3.1 was installed. To complete the uninstallation of 3.1, you must manually remove the following paths from the Windows system PATH variable:

- [drive letter:\...]Cisco IDS Event Viewer\MySQL\bin
- [drive letter:\...]Cisco IDS Event Viewer\JRE\bin
- [drive letter:\...]Cisco IDS Event Viewer\DataFeed\bin
- [drive letter:\...]Cisco IDS Event Viewer\IEV\bin
- [drive letter:\...]Cisco IDS Event Viewer\MySQL\lib\opt

The Cisco IDS Event Viewer and MySQL services are stopped and removed along with the entire Cisco IDS Event Viewer directory.

Starting IDS Event Viewer

**Tip**

Ensure the Windows NT services for IDS Event Viewer are running. You can review the status of the Cisco IDS Event Viewer and MySQL services by selecting Start > Settings > Control Panel > Services.

To start IDS Event Viewer, follow these steps:

-
- Step 1** Double-click the Cisco IDS Event Viewer shortcut on your desktop, or
- Step 2** From the Windows Start menu, select **Programs > Cisco Systems > Cisco IDS Event Viewer > Cisco IDS Event Viewer**.
-

Specifying Devices to Monitor

IDS Event Viewer enables you to view alarms for up to five sensors at a time. To specify which five sensors IDS Event Viewer should monitor, you have to add each sensor to the Devices folder. You can later change the properties associated with a device or delete a device from IDS Event Viewer. This section includes the following procedures:

- [Adding a Device, page 6-7](#)
- [Editing Device Properties, page 6-10](#)
- [Deleting a Device, page 6-10](#)
- [Reviewing Device Status, page 6-10](#)

Adding a Device

To add a sensor to the IDS Event Viewer Devices folder, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **File > New > Device**.
The Device Properties panel appears.

Figure 6-2 Device Properties

The screenshot shows the 'Device Properties' dialog box with the following fields and options:

- New Sensor Information:**
 - Sensor IP Address: [Text Box]
 - Sensor Name: [Text Box]
 - User Name: [Text Box]
 - Password: [Text Box]
 - Web Server Port: 443 [Text Box]
- Choose the communication protocol:**
 - Use encrypted connection (https)
 - Use non-encrypted connection (http)
- Event Start Time (UTC):**
 - Latest Alerts
 - Start Date(YYYY:MM:DD): [Picker] : [Picker] : [Picker]
 - Start Time(HH:MM:SS): [Picker] : [Picker] : [Picker]
- Exclude alerts of the following severity level(s):**
 - Informational
 - Low
 - Medium
 - High

Buttons: OK, Cancel

- Step 2** Complete the following fields in the Device Properties panel:
- Sensor IP Address
 - Sensor Name
 - User Name

- Password
- Web Server Port



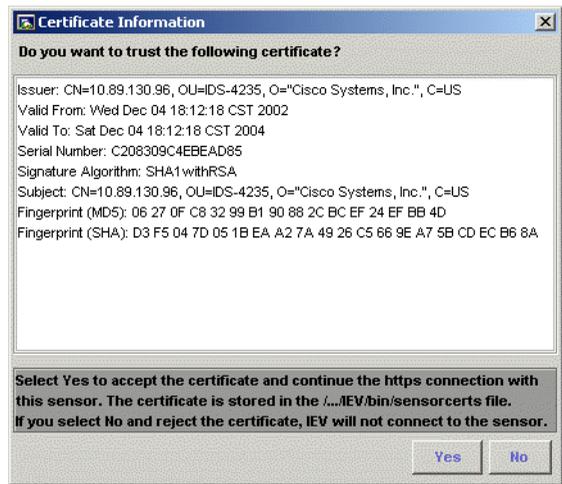
Note The information you provide in the Device Properties panel should match the settings you entered during initial configuration of the sensor. If you have set up a user account with Viewer access for IDS Event Viewer, specify the username and password for that account.

- Step 3** To specify the communication protocol IDS Event Viewer should use when connecting to the sensor, select the **Use encrypted connection (https)** or **Use non-encrypted connection** radio button.
- Step 4** To specify what alerts to pull from the sensor, follow these steps:
- To pull the latest alerts from the sensor, select the **Latest Alerts** check box.
IDS Event Viewer will receive alerts from the sensor, beginning with the first alert the sensor receives after connecting with IDS Event Viewer.
 - To pull alerts from the sensor eventStore, deselect the **Latest Alerts** check box and specify the following:
 - Start Date
 - Start Time
 IDS Event Viewer will receive alerts from the sensor, beginning with the first alert that matches the criteria you specified.
- Step 5** To exclude alarms of a certain severity level, select one or more of the following:
- Informational
 - Low
 - Medium
 - High
- Alarms that match the severity level(s) you selected are not pulled from the sensor event store and will not appear in the Statistical Graph.
- Step 6** Click **OK** to close the Device Properties panel.
- IDS Event Viewer sends a subscription request to the sensor. This request remains open until you modify the device properties or delete the device.

**Note**

If you specified https as the communication protocol, IDS Event Viewer retrieves the certificate information from the sensor and displays the Certificate Information dialog box. You must click Yes to accept the certificate and continue the https connection between IDS Event Viewer and the sensor.

Figure 6-3 Certificate Information



Step 7 Repeat Steps 1 through 3 for any additional sensors you want to monitor (up to 5).

**Note**

If IDS Event Viewer cannot connect to the sensor, a red X appears next to the device name to indicate that no connection is present. IDS Event Viewer continues trying to connect to the sensor every 20 seconds until a connection is established or you delete the device from IDS Event Viewer.

Editing Device Properties

To edit properties for an existing device in the Devices folder, follow these steps:

-
- Step 1** Expand the **Devices** folder to view the list of devices.
 - Step 2** Right-click the device you want to edit, and then click **Properties**.
The Device Properties panel appears.
 - Step 3** Select and edit the properties you want change, and then click **Update** to save your changes.
-

Deleting a Device

To delete a device from the Devices folder, follow these steps:

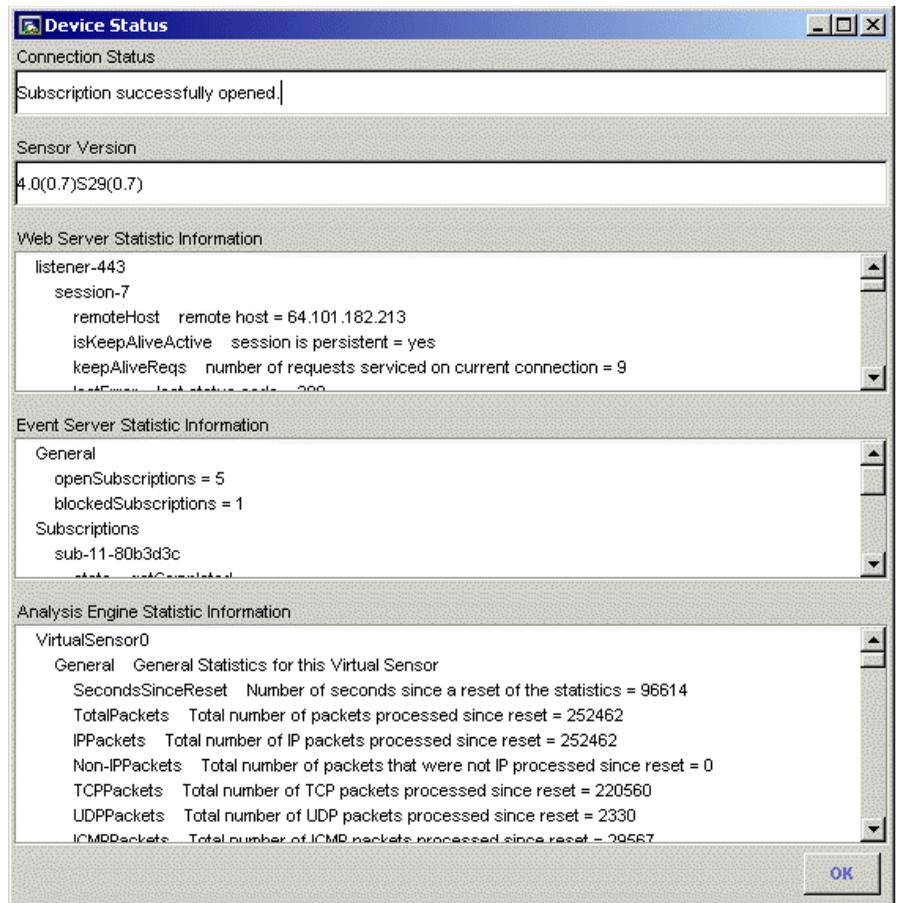
-
- Step 1** Expand the **Devices** folder to view the list of devices.
 - Step 2** Right-click the device you want to delete, and then click **Delete Device**.
The Device Deletion Confirmation dialog box appears.
 - Step 3** Click **Yes** to delete the device from the Devices folder.
-

Reviewing Device Status

To review the version information and connection status for a device, follow these steps:

-
- Step 1** Expand the **Devices** folder to view the list of sensors.
 - Step 2** Right-click the sensor for which you want to review status information, and then click **Device Status**.
The Device Status dialog box displays the Sensor Version, Device Status, Web Server Statistic Information, Event Server Statistic Information, and Analysis Engine Statistic Information.

Figure 6-4 Device Status



IDS Event Viewer will return one of the following connection status responses:

- Subscription not open yet.
- Subscription successfully opened.

- Failed to open subscription. Check communication parameters.
- Network connection error. Is the web server running?
- Status unknown. IEV server program may not be running.

Step 3 To close the Device Status dialog box, click **OK**.

Accessing the IDS Device Manager

You can access IDS Device Manager for a particular sensor from IDS Event Viewer.

To access IDS Device Manager, follow these steps:

Step 1 Expand the **Devices** folder to view the list of sensors.

Step 2 Double-click the sensor you want to manage.

The browser application opens and connects to the IP address for this sensor, using the port number and encryption specified in the Device Properties panel.

Configuring Filters

Filters enable you to customize and refine your view of event data by specifying alarms to exclude from your view. IDS Event Viewer ships with a default filter; however, you can create and store user-defined filters in the Filters folder. These filters can later be applied to any default or user-defined view. This section includes the following procedures:

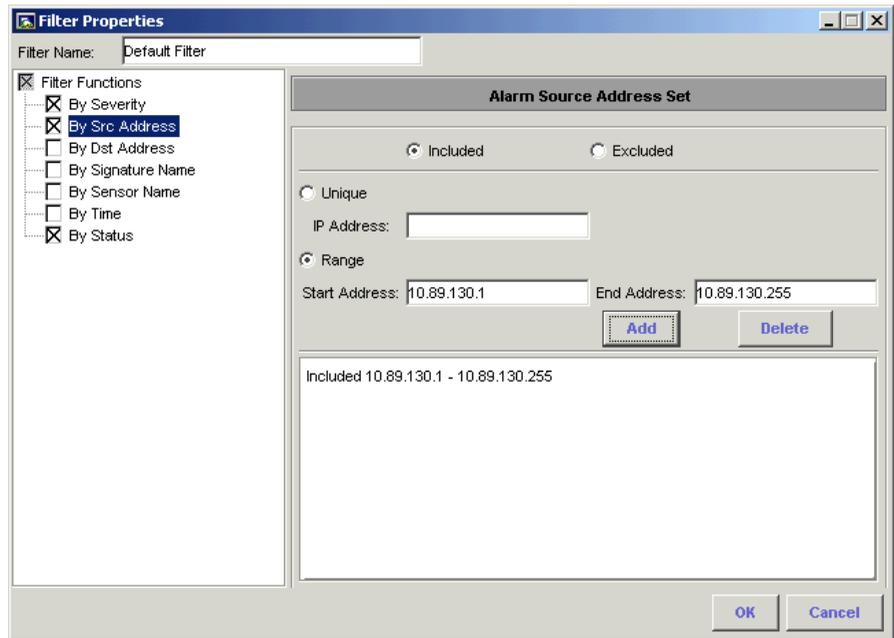
- [Creating a Filter, page 6-13](#)
- [Editing Filter Properties, page 6-16](#)
- [Deleting a Filter, page 6-17](#)

Creating a Filter

To create a filter, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **File > New > Filter**.
The Filter Properties panel appears.

Figure 6-5 Filter Properties



- Step 2** To name the filter, type an alpha or numeric text string (up to 64 characters) in the Filter Name field.
- Step 3** To filter alarms by severity, select the **By Severity** check box under Filter Functions and select one or more of the following severity level check boxes: **Informational**, **Low**, **Medium**, or **High**.

Step 4 To filter alarms by source address or destination address, select the **By Src Address** or **By Dst Address** check box, respectively, under Filter Functions and perform the following steps:

- a. To include an IP address or range, select the **Included** radio button. To exclude an IP address or range, select the **Excluded** radio button.
- b. To specify a single IP address, select the **Unique** radio button, enter a valid IP address in the IP Address field, and then click **Add**.

The IP address is added to the group of addresses excluded or included (depending on what you selected) by this filter.

- c. To specify a range of IP addresses, select the **Range** radio button, enter a valid starting IP address in the Start Address field and a valid ending IP address in the End Address field, and then click **Add**.

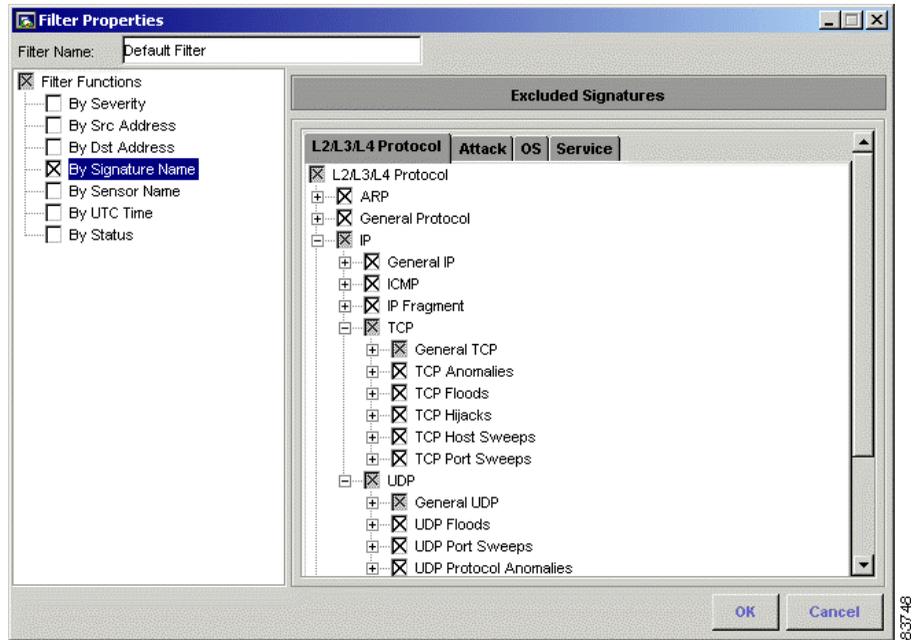
The IP address range is added to the group of addresses excluded or included (depending on what you selected) by this filter.

- d. Repeat Step 4 to continue adding IP addresses or ranges of IP addresses.

Step 5 To filter alarms by signature name, select the **By Signature Name** check box under Filter Functions and follow these steps:

- a. To locate a signature, click one of the following tabs:
 - **Attack**—Identifies the attack classification categories. You can select an attack category, such as Denial of Service, to exclude all signatures contained in that category.
 - **L2/L3/L4 Protocol**—Identifies the Layer 2, 3, and 4 protocol categories. You can expand each protocol category to view the individual signatures contained in that category. You can select an entire protocol category, such as UDP signatures, to exclude all signatures contained in that category.
 - **OS**—Identifies the operating system categories. You can expand each operating system category to view the individual signatures contained in that category. You can select an entire operating system category, such as Windows NT, to exclude all signatures contained in that category.
 - **Service**—Identifies the service categories. You can expand each service category to view the individual signatures contained in that category. You can select an entire service category, such as DNS, to exclude all signatures contained in that category.

Figure 6-6 Filter Properties



- b. To exclude individual signatures, expand the appropriate signature category and select the desired signatures.

The signatures you select are excluded by this filter.

Step 6 To exclude alarms by sensor, select the **By Sensor Name** check box under Filter Functions and choose a sensor from the Devices folder.

Step 7 To exclude alarms by time and date, select the **By UTC Time** check box under Filter Functions and follow these steps:

- a. Enter a valid numerical start date, beginning with the 4-digit year, and then the 2-digit month and day in the Start Date field.
- b. Enter a valid start time, beginning with the 2-digit hour, and then minute and seconds in the Start Time field.



Tip 16:00:00 is the equivalent to 4:00 p.m.

- c. Enter a valid numerical end date, beginning with the 4-digit year, and then the 2-digit month and day in the End Date field.
- d. Enter a valid end time, beginning with the 2-digit hour, and then minute and seconds in the End Time field.



Tip 22:30:00 is the equivalent to 10:30 p.m.

- e. Repeat Step 7 to add additional time periods.

Step 8 To exclude alarms by status, select the **By Status** check box under Filter Functions and select one or more of the following status level check boxes:

- New
- Acknowledged
- Assigned
- Closed
- Deleted

Step 9 To save the filter, click **OK**.

The filter is added to the Filters folder and can now be used in a view.

Editing Filter Properties

To edit the properties for an existing filter in the Filters folder, follow these steps:

Step 1 Expand the **Filters** folder to view the list of defined filters.

The Filter Properties panel appears.

Step 2 Right-click the filter you want to edit, and then click **Properties**.

- Step 3** Select and edit the properties, as appropriate, listed under Filter Functions, and then click **OK**.
- A dialog box appears and warns you that you are about to overwrite the existing filter with the edited filter.
- Step 4** Click **Yes** to overwrite the existing filter and save your changes.
-

Deleting a Filter

To delete a filter from the Filters folder, follow these steps:

-
- Step 1** Expand the **Filters** folder to view the list of defined filters.
- The Filter Deletion Confirmation dialog box appears.
- Step 2** Right-click the filter you want to delete, and then click **Delete Filter**.
- Step 3** Click **Yes** to delete the filter from the Filters folder.
-

Configuring Views

Views enable you to analyze filtered event data from a specified source. IDS Event Viewer ships with five default views; however, you can use the View Wizard to create and store user-defined views in the Views folder. This section includes the following procedures:

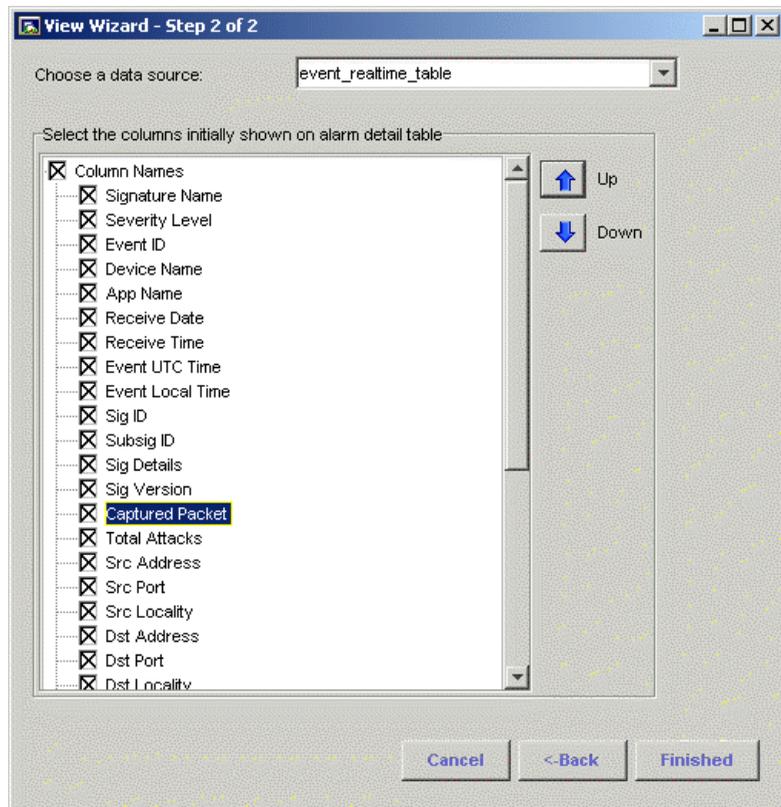
- [Creating a View, page 6-18](#)
- [Editing View Properties, page 6-20](#)
- [Deleting a View, page 6-21](#)

Creating a View

To create a view, follow these steps:

-
- Step 1** From the IDS Event Viewer main menu, select **File > New > View**.
The View Wizard appears.
 - Step 2** To name the view, enter an alpha or numeric text string (up to 64 characters) in the View Name field.
 - Step 3** To specify a filter, select the **Use Filter** check box and choose a filter from the list.
 - Step 4** To specify how alarms are grouped in the table, select a grouping style under Select the grouping style on alarm aggregation table.
 - Step 5** To specify the columns that should appear in the table, select one or more check boxes under Select the columns initially shown on alarm aggregation table.
 - Step 6** To specify sort order for the columns, select an option from the Column Secondary Sort Order list.
 - Step 7** Click **Next** to advance to the final panel of the View Wizard.
The final panel of the View Wizard appears.

Figure 6-7 View Wizard



- Step 8** To specify the alarms that should populate this view, select a source from the Choose a data source list box.



Note To view alarms in real time, select **event_realtime_table**. IDS Event Viewer also comes with a demo table. If the data source you want to use has not yet been established, you can select the default source (event_realtime_table) and later edit the view to associate a different data source.

- Step 9** To specify the columns that should appear in the alarm detail, select one or more columns from the Select the columns initially shown on alarm detail table list. You can rearrange the order of these columns by using the Up or Down buttons.
- Step 10** To save your changes and create the view, click **Finish**.
The view is added to the Views folder.
-

Editing View Properties

**Tip**

If you only need to change the data source associated with this view, right-click the view and select Data Source. From the Change Data Source panel you can select a new source for the current view. For more information, see [Specifying a Data Source, page 6-31](#).

To edit the properties for an existing view in the Views folder, follow these steps:

- Step 1** Expand the **Views** folder to view the list of defined views.
The View Wizard appears.
- Step 2** Right-click the view you want to edit, and then click **Properties**.
- Step 3** Select and edit the view name, associated filter, grouping style, columns, or sort order. Or, click **Next** to advance to the final panel from which you can edit the data source and columns for the alarm detail.
- Step 4** Click **Finish** to accept your changes.
A dialog box appears and warns you that you are about to overwrite the existing view with the edited view.
- Step 5** Click **Yes** to overwrite the existing view and save your changes.
-

Deleting a View

To delete a view from the Views folder, follow these steps:

-
- Step 1** Expand the **Views** folder to view the list of defined views.
The View Deletion Confirmation dialog box appears.
- Step 2** Right-click the view you want to delete, and then click **Delete View**.
- Step 3** Click **Yes** to delete the view from the Views folder.
-

Configuring Preferences

From the Edit menu, you can specify how often contents in a graph or table view are refreshed. You can also configure archival settings to optimize performance. This section includes the following procedures:

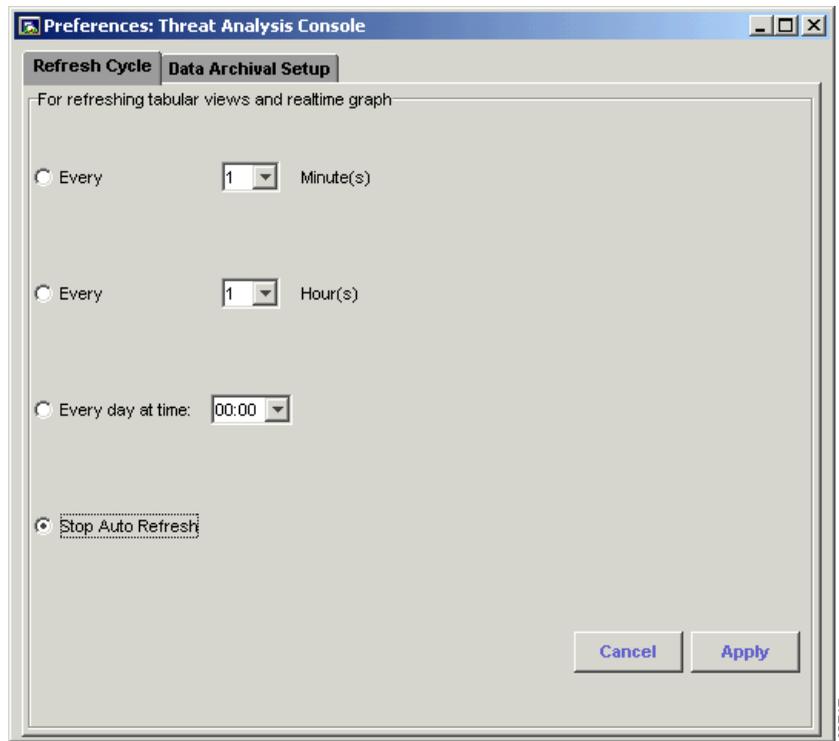
- [Configuring Refresh Cycle Settings, page 6-21](#)
- [Configuring Data Archival Settings, page 6-23](#)

Configuring Refresh Cycle Settings

To configure the Refresh Cycle settings, follow these steps:

-
- Step 1** From the IDS Event Viewer main menu, select **Edit > Preferences > Refresh Cycle**.
The Refresh Cycle tab of the Preferences panel appears.

Figure 6-8 Refresh Cycle



- Step 2** To set the automatic refresh, perform one of the following steps:
- a. To set the automatic refresh to occur every 1 to 59 minutes, select the **Every_ Minute(s)** radio button, select a time interval from the list, and then click **Apply**.
 - b. To set the automatic refresh to occur every 1 to 23 hours, select the **Every_ Hour(s)** radio button, select a time interval from the list, and then click **Apply**.

- c. To set the automatic refresh to occur once a day, select the **Every day at time** radio button, select a specific time from the list, and then click **Apply**.
- d. To stop the automatic refresh, select the **Stop Auto Refresh** radio button, and then click **Apply**.

Step 3 To close the Preferences panel, click the **Close** button.

Configuring Data Archival Settings

IDS Event Viewer includes a database archival feature that enables you to archive real-time events and ensure available disk space for incoming events. Two thresholds control the archival process. The first is a time interval and the second is a maximum number of records. Crossing either threshold triggers the archival processes.

If the time interval threshold is crossed, all records with a status matching the archival settings are moved from `event_realtime_table` to `archive_table.timestamp`. Any alarms with a status set to Deleted are deleted.

If the maximum records threshold is crossed, any alarms with a status set to Deleted are deleted from the `event_realtime_table`. Then, all records with a status matching the archival settings are moved from `event_realtime_table` to `archive_table.timestamp`. If, after the initial archival process, the `event_realtime_table` still contains more than half of the maximum number of records allowed, the archival process continues to archive and remove records (except those with a status set to New). If the number of records remaining exceeds the maximum number of records allowed, all remaining records are archived, including those with a status set to New.

To configure data archival settings, follow these steps:

Step 1 From the IDS Event Viewer main menu, select **Edit > Preferences > Data Archival Setup**.

The Data Archival Setup tab of the Preferences panel appears.

Step 2 To specify the alarms that you want to archive, select one or more of the following alarm status check boxes:

- New
- Acknowledged

- Assigned
- Closed

- Step 3** To enable a time interval threshold, select **Enable time schedule for archiving events** and follow these steps:
- To set the archival to occur every 1 to 59 minutes, select the **Every _ Minute(s)** radio button and select a time interval from the list.
 - To set the archival to occur every 1 to 23 hours, select the **Every _ Hour(s)** radio button and select a time interval from the list.
 - To set the archival to occur once a day, select the **Every day at time** radio button and select a specific time from the list.
- Step 4** To specify the maximum number of real-time events to allow in the event_realtime_table, enter a numerical value (from 1000 to 1,000,000) in the **Maximum number of events in 'event_realtime_table'** field. When this threshold is met, IDS Event Viewer begins to archive events to make room for new events in the event_realtime_table.
- Step 5** To specify the maximum number of archived files, enter a numerical value (from 10 to 400) in the **Maximum number of archived files** field. When this threshold is met, IDS Event Viewer begins to compress half of the oldest archived files and moves them to the compressed directory.
- Step 6** To specify the maximum number of compressed archived files, enter a numerical value (from 10 to 400) in the **Maximum number of compressed archived files** field. When this threshold is met, IDS Event Viewer begins to purge half of the oldest compressed archived files.



Note To maintain available disk space for a full event_realtime_table, IDS Event Viewer purges compressed and archived files on a first-in, first-out basis until the available disk space is greater than three times the space needed.

- Step 7** To save your changes, click **Apply**.
- Step 8** To close the Preferences panel, click the **Close** button.
-

Configuring Application Settings

IDS Event Viewer relies on supporting applications to carry out database, retrieval, and communication functions. From the Edit menu, you can specify the location of these supporting applications. This section includes the following procedures:

- [Specifying Web Browser Application Location, page 6-25](#)
- [Specifying Ethereal Application Location, page 6-27](#)
- [Specifying NSDB Folder Location, page 6-28](#)
- [Configuring Refresh Cycle Settings, page 6-21](#)

Specifying Web Browser Application Location

**Note**

IDS Event Viewer detects the location of your web browser when you install IDS Event Viewer. You only need to specify the location of the browser application if you later move the Internet Explorer or Netscape executable file to a different directory.

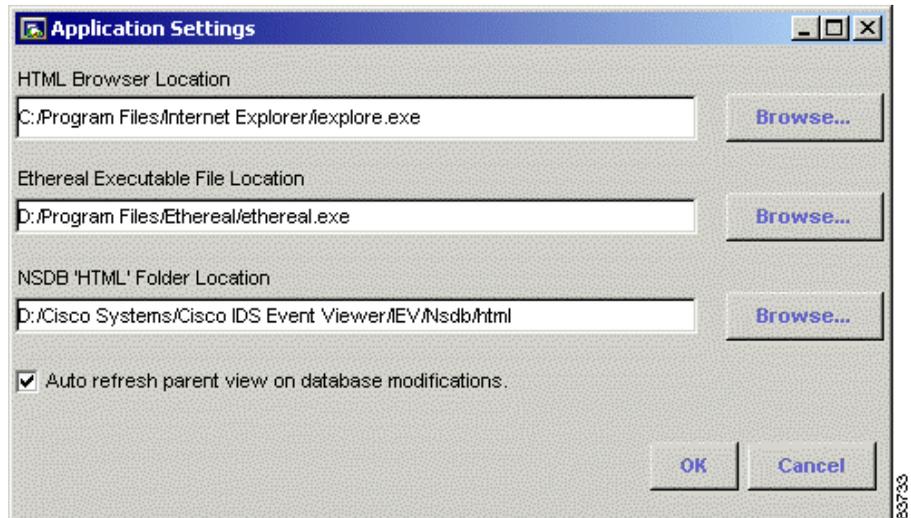
**Note**

IDS Event Viewer version 4.0 supports Internet Explorer versions 5.5 and later and Netscape versions 4.7 and later.

To specify the location of your browser, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **Edit > Applications Settings**. The Application Settings panel appears.

Figure 6-9 Application Settings



- Step 2** Enter the path, beginning with the drive letter, to the Internet Explorer or Netscape executable file in the HTML Browser Location field, or click **Browse** to locate the file.
- Step 3** Click **OK** to accept your changes and close the Application Settings panel.

Specifying Ethereal Application Location

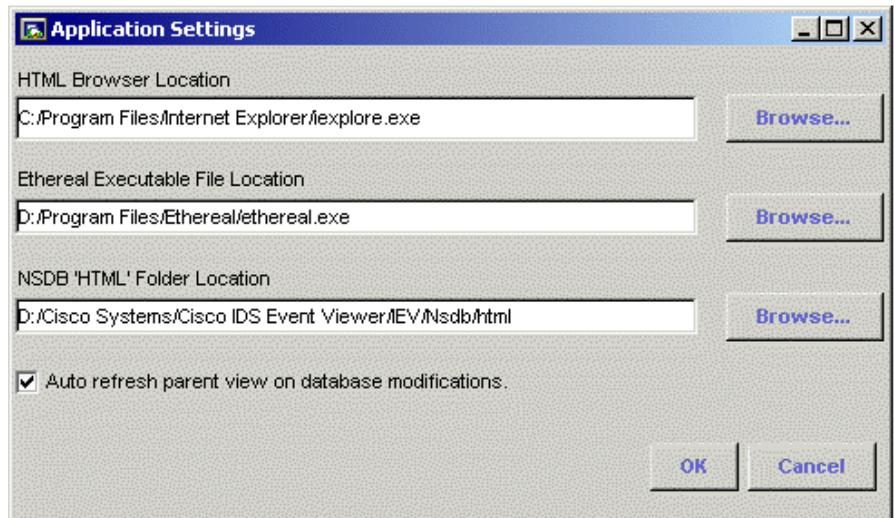
**Note**

If Ethereal is installed on your system when you install IDS Event Viewer, IDS Event Viewer detects the location. You only need to specify the location of Ethereal if you later move the Ethereal executable file to a different directory or if you decide to install Ethereal after installing IDS Event Viewer.

To specify the location of Ethereal, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **Edit > Applications Settings**. The Application Settings panel appears.

Figure 6-10 Application Settings



- Step 2** Enter the path, beginning with the drive letter, to the Ethereal executable file in the Ethereal Executable File Location field, or click **Browse** to locate the file.
- Step 3** Click **OK** to accept your changes and close the Application Settings panel.

Specifying NSDB Folder Location



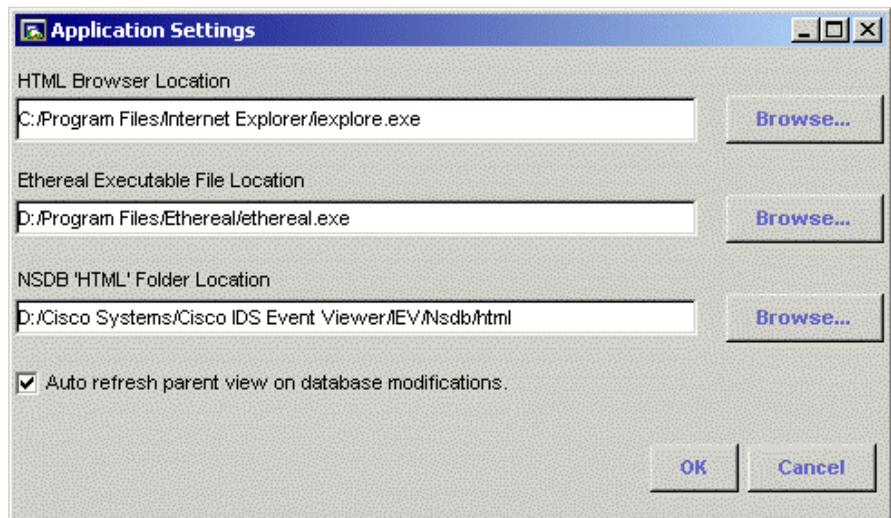
Note

The NSDB is installed during IDS Event Viewer installation. You only need to specify the location of the NSDB if you have moved the NSDB HTML folder to a different directory since installing IDS Event Viewer.

To specify the location of the NSDB, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **Edit > Applications Settings**. The Application Settings panel appears.

Figure 6-11 Application Settings



- Step 2** Enter the path, beginning with the drive letter, to the NSDB HTML folder in the NSDB HTML Folder Location field, or click **Browse** to locate the folder.
- Step 3** Click **OK** to accept your changes and close the Application Settings panel.

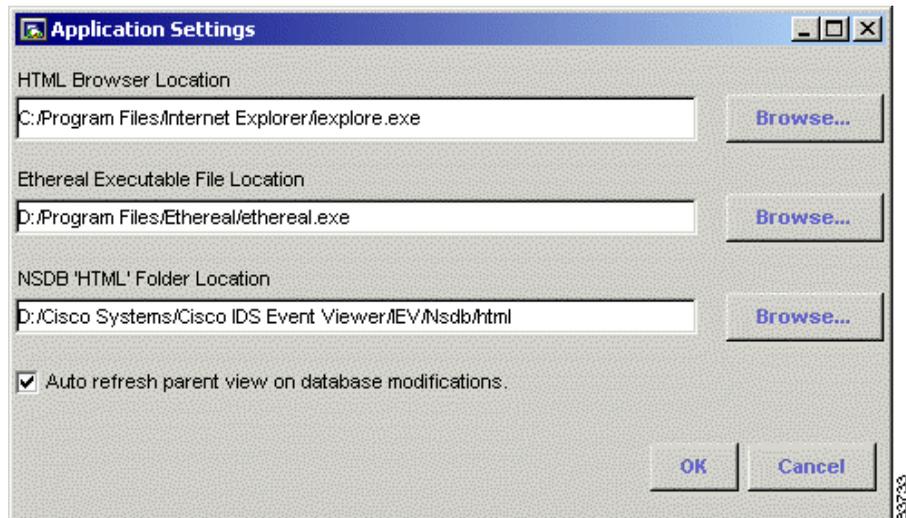
Changing the Auto Refresh View Setting

By default, if you delete a row in the Drill Down Dialog table or Expanded Details Dialog table, the aggregation table for that view is automatically refreshed to reflect the changes. However, you can change the default setting so that a change in a subordinate view is not reflected in the parent view until the next refresh cycle.

To change the auto refresh database setting, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **Edit > Applications Settings**. The Application Settings panel appears.

Figure 6-12 Application Settings



- Step 2** To change the default auto refresh view setting, deselect the **Auto refresh parent view on database modifications** check box.
- Step 3** Click **OK** to accept your changes and close the Application Settings panel.

Viewing Event Data

After you configure IDS Event Viewer, you can manipulate the views and tables to display event data from the sensors you are monitoring. This section includes the following introduction and procedures:

- [Introduction to Tables and Graphs, page 6-30](#)
- [Specifying a Data Source, page 6-31](#)
- [Viewing All Columns, page 6-32](#)
- [Sorting Data in Columns, page 6-33](#)
- [Displaying Multiple Views, page 6-33](#)
- [Viewing Events in a Graph, page 6-34](#)
- [Viewing Event Details, page 6-34](#)
- [Viewing Events in the Realtime Dashboard, page 6-37](#)
- [Using Ethereal, page 6-40](#)

Introduction to Tables and Graphs

IDS Event Viewer enables you to access various tables and graphs that provide specialized views into the event data you are analyzing. Before you create a view and begin working with the individual tables and graphs, you should review the following descriptions.

The following tables and graph organize the events for a view. The events shown in these tables and graph differ depending on the data source you select for the view. The data source can be the event_realtime_table, archived tables, or imported log files.

- **Alarm Aggregation table**—The first table displayed for any view. You access an alarm aggregation table by double-clicking the view name in the Views folder.
- **Expanded Details Dialog table**—Displays the details of a particular event listed in an alarm aggregation table. You access the Expanded Details Dialog table by right-clicking a row in the first column of an alarm aggregation table.

- Drill Down Dialog table—Displays the individual entries for a particular column in the alarm aggregation table, such as the individual source addresses associated with a UDP Bomb event. You access the Drill Down Dialog table by double-clicking a column (except first or Total Alarm Count) in an alarm aggregation table.
- Alarm Information Dialog table—Displays the individual alarms for a particular event. You access the Alarm Information Dialog table by double-clicking the Total Alarm Count column in the alarm aggregation table, or by right-clicking the first column of the Expanded Details Dialog table.
- Statistical Graph—Displays the average number of alarms received by IDS Event Viewer, based on the filter that is applied to the data source. Therefore, depending on the filter, the Statistical Graph may not reflect the true average number of alarms. The time stamp for these events reflects the time the sensor generated the alarm.

The following table and graph organize events from a continuously running thread in IDS Event Viewer. This thread continuously monitors and aggregates the total number of alarms IDS Event Viewer receives.

- Realtime Dashboard—Displays the events, in real time, as IDS Event Viewer receives these events from the sensor(s). The most recent events appear at the top of the table. By default, the Realtime Dashboard displays the most recent events received from every device configured in IDS Event Viewer. You can configure the Realtime Dashboard to display only events from a particular device or only events of a particular severity level. You can also configure how often IDS Event Viewer should retrieve events from the sensor(s) and the maximum number of events to display.
- Realtime Graph—Displays the average number of alarms received by IDS Event Viewer. The time stamp for these events reflects the time IDS Event Viewer received the alarm, not necessarily the time the sensor generated the alarm.

Specifying a Data Source

You must associate a data source with a view to indicate the events that view should display.

To specify or change the data source associated with a view, follow these steps:

-
- Step 1** Expand the **Views** folder to view the list of defined views.
- Step 2** Right-click the view for which you want to specify a data source, and then click **Data Source**.

The Change Data Source dialog box appears.

- Step 3** Select a data source from the Select the data source for current view(s) list, and then click **OK**.

If the view is open, the table automatically refreshes with events from the new data source. Otherwise, to reset the view with events from the new data source, double-click the view in the Views folder.

Viewing All Columns

You can right-click a column to hide it from the current view. You can later display all columns, including those hidden from view.

To view all columns, follow these steps:

-
- Step 1** To view all columns for the current view, right-click a column heading and select **Show All Columns**.

The columns configured for this view are displayed.

- Step 2** To hide a single column, right-click the column heading and select **Hide Column**.



Note You cannot hide the first or last column in an alarm aggregation table.

The column is hidden from the current view only. The next time you open this particular view, the column appears. If you want to permanently remove the column, edit the view properties.

- Step 3** For columns that display an ellipses (...) after the column heading, click and drag the split bar that separates the columns to expand the column.

Step 4 For all columns, except the first, double-click a cell in that column to drill down and view the contents of the column.

The Drill Down Dialog appears, unless you double-click the Total Alarm Count column, in which case the Alarm Information Dialog appears.

Step 5 For cells that display an arrow (—>) after the number of occurrences, double-click that cell to display the contents of the cell.

A second table appears in the Drill Down Dialog and displays the contents of the cell. Double-clicking a cell containing an arrow (—>) in this second table displays the Alarm Information Dialog.

Sorting Data in Columns

You can sort the table data in ascending or descending order by column.

To sort data in columns, follow these steps:

Step 1 To view all columns for the current view, right-click a column heading, and then select **Show All Columns**.

Step 2 Double-click the column heading to select the column containing the data you want to sort.

An Up Arrow or Down Arrow appears, indicating the possible sort order for the column data.

Step 3 Click the arrow to sort the data in the order indicated.



Note You can only sort the table by one column at a time. Therefore, when you double-click an additional column heading, the arrow is removed from the previous column and appears next to the selected column heading.

Displaying Multiple Views

You can display multiple views at the same time. IDS Event Viewer places one view behind the other and displays a tab for each view.

To display multiple views, follow these steps:

-
- Step 1** Expand the **Views** folder to view the list of defined views.
- Step 2** To open a view, double-click the view name.
The view appears in the right view pane and displays an alarm aggregation table.
- Step 3** Repeat Step 2 for each additional view that you want to open.
- Step 4** To close a single view, right-click the tab for that view and select **CloseX**, where **X** stands for the name of the view.
- Step 5** To close all views, right-click the tab for any view and select **Close All Views**.
All open views close.
-

Viewing Event Details

You can expand an event to view the details, such as signature name and severity level, associated with that event.

To view event details, follow these steps:

-
- Step 1** Right-click a cell in the first column in an alarm aggregation table associated with the event you want to expand, and then select **Expand Whole Details**.
The Expanded Details Dialog appears with the Whole Address panel displayed.
- Step 2** To view the events by address category, click the **Class A Level**, **Class B Level**, or **Class C Level** tab.
-

Viewing Events in a Graph

You can view events in a Realtime Graph or Statistical Graph. Each graph provides a view of the average number of alarms per minute, based on severity level. However, each graph represents a different data source and therefore a different view into the events.

The Realtime Graph is populated with events from a continuously running thread in IDS Event Viewer. This thread continuously monitors and aggregates the total number of alarms IDS Event Viewer receives. The events displayed in the Realtime Graph reflect the average number of alarms received by IDS Event Viewer. The time stamp for these events reflects the time IDS Event Viewer received the alarm, not necessarily the time the sensor generated the alarm.

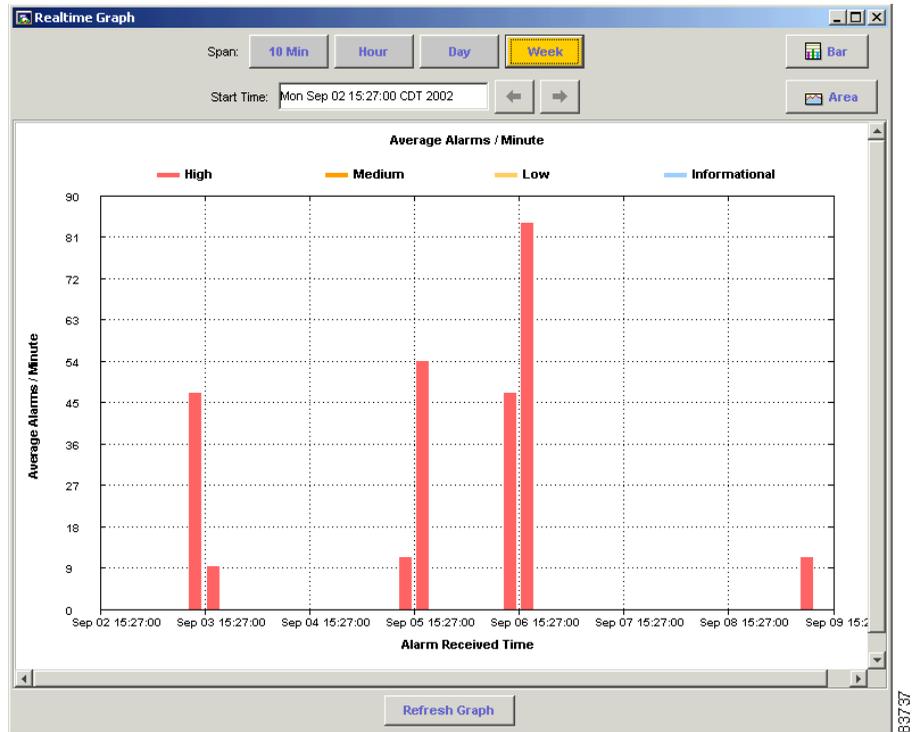
The Statistical Graph is populated with events from the data source you select. Valid data sources include the `event_realtime_table`, any archived table, or any imported table. The events displayed in the Statistical Graph reflect the average number of alarms received by IDS Event Viewer, based on the filter that is applied to the data source. Therefore, depending on the filter, the Statistical Graph may not reflect the true average number of alarms. The time stamp for these events reflects the time the sensor generated the alarm.

To view a graph, follow these steps:

Step 1 To view the Realtime Graph, select **Tools > Realtime Graph**.

The Realtime Graph appears.

Figure 6-13 Realtime Graph

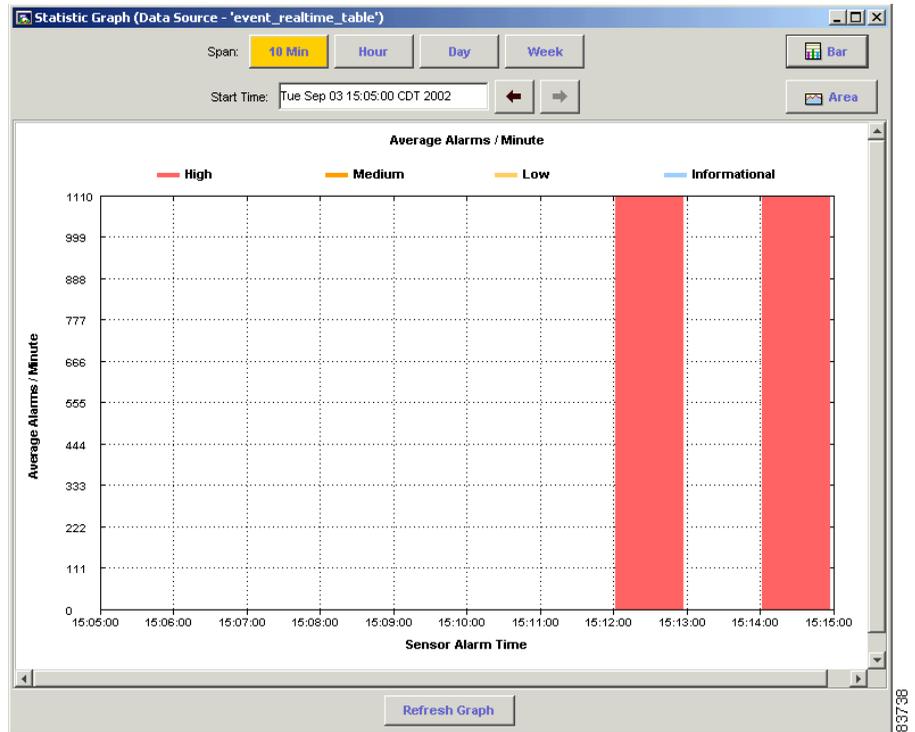


Step 2 To view the Statistical Graph, follow these steps:

- a. Expand the **Views** folder and locate the view that contains the alarm data you want to display in a graph.
- b. Right-click the view and select **Statistical Graph**.

IDS Event Viewer queries the data source for the selected view and calculates the average alarms per minute. The Statistical Graph appears and displays the result.

Figure 6-14 Statistical Graph



- Step 3** To change the range of events displayed in the graph, follow these steps:
- Specify the time span by which you want to advance the view.
 - To adjust the start time by the interval selected in SPAN, use the forward and backward arrows.
- Step 4** To change the presentation to a bar or area graph, click **Bar** or **Area**.

Viewing Events in the Realtime Dashboard

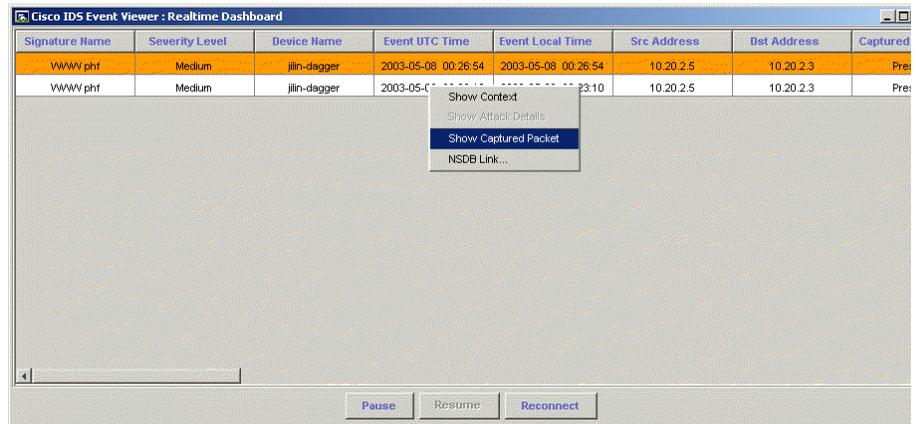
You can use the Realtime Dashboard to view a continuous stream of real-time events from the sensor.

To view events in the Realtime Dashboard, follow these steps:

Step 1 Select **Tools > Realtime Dashboard > Launch Dashboard**.

IDS Event Viewer opens a subscription request with the sensor. If the connection is successful, the Realtime Dashboard appears and displays the most recent events received by the sensor since the request was opened.

Figure 6-15 Realtime Dashboard



Step 2 To pause the stream of real-time events, click **Pause**.

IDS Event Viewer stops populating the Realtime Dashboard with events.

Step 3 To resume the stream of real-time events, click **Resume**.

IDS Event Viewer populates the Realtime Dashboard with events, beginning with the first event that was received after the stream was paused.

Step 4 To clear all existing events from the Realtime Dashboard, click **Reconnect**.

All existing events are removed from the Realtime Dashboard and IDS Event Viewer opens a new subscription with the sensor.

Configuring the Realtime Dashboard Settings

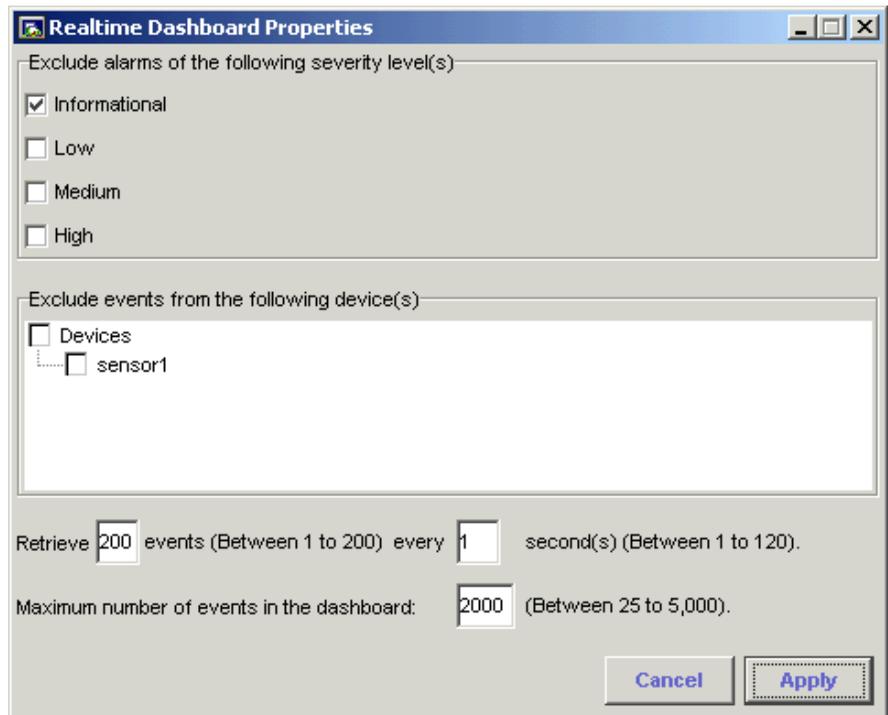
By default, the Realtime Dashboard displays the most recent events received from every device configured in IDS Event Viewer. You can configure the Realtime Dashboard to display only events from a particular device or only events of a particular severity level. You can also configure how often the Realtime Dashboard should retrieve events from the sensor(s) and the maximum number of events to display.

To configure the Realtime Dashboard settings, follow these steps:

Step 1 Select **Tools > Realtime Dashboard > Properties**.

The Realtime Dashboard Properties panel appears.

Figure 6-16 Realtime Dashboard Properties



- Step 2** To exclude alarms by severity level, select one or more of the following severity levels:
- Informational
 - Low
 - Medium
 - High
- Alarms that match the severity level(s) you selected will not appear in the Realtime Dashboard.
- Step 3** To exclude events from a particular device, select that device under Exclude events from the following sensor(s).
- IDS Event Viewer closes any open subscriptions to this device and no events are received from the sensor.
- Step 4** To configure the number of events IDS Event Viewer retrieves each second, follow these steps:
- a. Specify the number of events (between 1 and 200) IDS Event Viewer should retrieve during each request.
 - b. Specify the number of seconds (between 1 and 120) that should elapse before IDS Event Viewer retrieves more events.
- Step 5** Specify the maximum number of events to display in the Realtime Dashboard (between 25 and 5,000).
- If the maximum number is reached, the oldest alarm will be removed from the Realtime Dashboard. This process will continue until the number of alarms in the Realtime Dashboard is less than the maximum number you specified.
- Step 6** Click **Apply** to save your changes and close the Realtime Dashboard Properties panel.
-

Using Ethereal

Ethereal is a network protocol analyzer for Windows that enables you to examine data from a live network or from a captured file. You can interactively browse the captured data and view summary and detail information for each packet, including

the reconstructed stream of a TCP session. If you have Ethereal installed on the same host as IDS Event Viewer, you can start the Ethereal application from IDS Event Viewer Tools menu and view IP log files.

Working with Alarms

After you know how to manipulate views and tables to display the event data you are interested in, you can begin to manage individual alarms within those events. This task includes setting a status for alarms you have reviewed, adding notes to an alarm you want to track, or reviewing detailed alarm and signature information.

- [Viewing Individual Alarms, page 6-41](#)
- [Setting the Alarm Status, page 6-42](#)
- [Adding Notes to an Alarm, page 6-43](#)
- [Show Alarm Context, page 6-43](#)
- [Show Attack Details, page 6-43](#)
- [Accessing the NSDB, page 6-44](#)

Viewing Individual Alarms

You can view individual alarms associated with an event.

To view individual alarms, follow these steps:

Step 1

To view alarms from an alarm aggregation table, follow these steps:

- a. Expand the event details for the event containing the alarm you want to view.
The Expanded Details Dialog appears.
- b. Right-click a row in the Expanded Details Dialog, and then select **View Alarms**.

The Alarm Information Dialog appears.

- Step 2** To view alarms from any table, follow these steps:
- a. Scroll to locate the Total Alarm Count column.
 - b. Double-click the cell containing the alarms you want to view in the Total Alarm Count column.
- The Alarm Information Dialog appears.
-

Setting the Alarm Status

You can associate a status with the alarm, indicating what action should be taken by IDS Event Viewer (for alarms marked Deleted or during alarm archival) or by someone else in your organization.



Tip

You can right-click a cell in the first column of an alarm aggregation table and change the status for all alarms in that cell. This is useful for deleting several alarms at the same time.

To set the status for an alarm, follow these steps:

- Step 1** Locate the alarm for which you want to set a status.
- Step 2** To set the status for that alarm, follow these steps:
- a. Right-click the alarm and select **Set Status To**.
 - b. Select one of the following:
 - New
 - Acknowledged
 - Assigned
 - Closed
 - Deleted
 - c. Select the status in the Alarm Status column and select a status from the list.
-

Adding Notes to an Alarm

You can add notes (up to 255 characters) to an alarm entry and store these notes as part of the alarm entry in the database.

To add notes to an alarm, follow these steps:

-
- Step 1** Locate the alarm to which you want to add notes.
 - Step 2** Scroll to the Notes column.
 - Step 3** Double-click the cell in the Notes column for the alarm you want to add notes to. The cell becomes active and a cursor appears.
 - Step 4** Type the notes you want to store with this particular alarm, and then press **Enter**.
-

Show Alarm Context

Certain alarms may have context data associated with them. Context data provides a snapshot of the incoming and outgoing binary TCP traffic (up to 256 bytes in both directions) that preceded the triggering of the signature.

To view the context for an alarm, follow these steps:

-
- Step 1** From the Alarm Information Dialog or Realtime Dashboard, right-click a cell in the Context column, and then select **Show Context**. The Decoded Alarm Context panel appears.
-

Show Attack Details

Certain attacks, such as sweep attacks, affect multiple victims or are the result of multiple attackers. The alarms generated from these attacks contain summary details of the attack.

To view the attack details for an alarm, follow these steps:

-
- Step 1** From the Alarm Information Dialog or Realtime Dashboard, right-click the alarm, and then select **Show Attack Details**.

The Summary Attack Details panel appears.

Accessing the NSDB

The NSDB is a repository of information for individual signatures, including signature id, type, structure, and description.

To access the NSDB, perform one of the following steps:

-
- Step 1** From the Expanded Details Dialog, right-click any column and then select **NSDB Link**.

or

- Step 2** From the Alarm Information Dialog, right-click any column and then select **NSDB Link**.

or

- Step 3** From the Drill Down Dialog, right-click a cell in the first column and then select **NSDB Link**.

or

- Step 4** Select **Tools > NSDB Link**.
-

Database Administration

Database administration is essential to maintaining the integrity of IDS Event Viewer. Database administration includes routinely importing, exporting, and deleting event data. This section includes the following procedures:

- [Importing Log Files, page 6-45](#)
- [Exporting Tables, page 6-47](#)

- [Deleting Tables from Data Source, page 6-48](#)
- [Deleting Alarms, page 6-49](#)

Importing Log Files

To import a log file, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **File > Database Administration > Import Log Files**.

The Import Log Files panel appears.

Figure 6-17 Import Log Files



- Step 2** Click **Browse** to locate the file you want to import.

- Step 3** To specify how the data fields are separated, select **Comma (CSV)** or **Tab** from the Fields in log file are separated by list box.
- Step 4** To specify the format of the file you want to import, select the **IEV 4.0 format** or **Sensor Postoffice 3.x format** radio button under Log File Format.



Note Log files with the Sensor Postoffice 3.x format are converted to IEV 4.0 format upon import.

- Step 5** To import the log file information into a new table, follow these steps:
- Select the **Create New Table** radio button under How to Import Log Files.
 - Type a valid name for the table.
- Step 6** To import the log file information into an existing table, follow these steps:
- Select the **Append to Existing Table** radio button under How to Import Log Files.
 - Select an existing table from the list box.
- Step 7** To import the log file, click **Import**.

Depending on the option you chose, either the log file is appended to an existing table or a table is created. You can then select this table as the data source for a particular view and view the alarms in the log file.

Exporting Tables

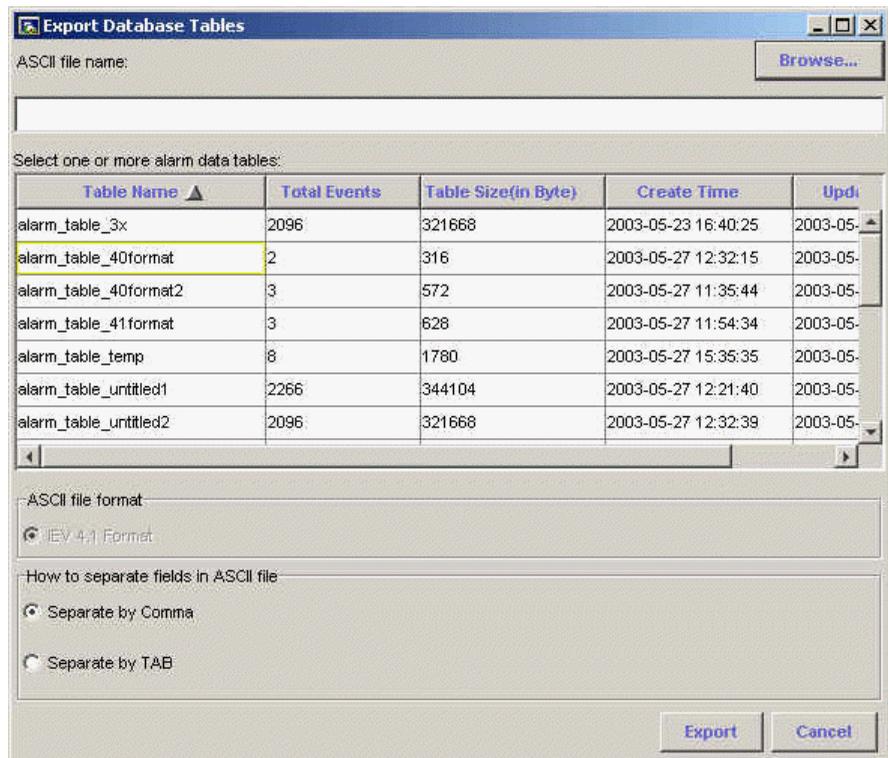
You can export data from the IDS Event Viewer tables to an ASCII file.

To export a table, follow these steps:

- Step 1** From the IDS Event Viewer main menu, select **File > Database Administration > Export Tables**.

The Export Database Tables panel appears.

Figure 6-18 Export Database Tables



- Step 2** To specify where to store the exported table, click **Browse** and choose a directory for the file.

- Step 3** To name the exported file, enter a name in the ASCII file name field.
- Step 4** Select the tables to export to the ASCII file. To select multiple tables, hold down the **Ctrl** key and click the names of the tables you want to include.



Note By default, tables are exported in the IEV 4.0 Format. This option appears dimmed.

- Step 5** To specify how the table fields should be separated in ASCII format, select the **Separate by Comma** or **Separate by TAB** radio button under How to separate fields in ASCII file.
- Step 6** To export the tables, click **Export**.
-

Deleting Tables from Data Source

You can delete an existing table from the list of available data sources for a view. To delete a table from the data source repository, follow these steps:

-
- Step 1** From the IDS Event Viewer main menu, select **File > Database Administration > Data Source Information**.
- The Data Source Information panel appears.
- Step 2** Select the row corresponding to the table you want to delete, and then click **Delete Tables**.
- The Table Deletion Confirmation dialog box appears.
- Step 3** Click **Yes** to remove the table from the data source repository.
-

Deleting Alarms

To delete alarms from a data source, follow these steps:

-
- Step 1** To delete alarms with a status set to Deleted, follow these steps:
- Verify that you have set the status of all the alarms you want to delete to Deleted.
 - From the IDS Event Viewer main menu, select **File > Database Administration > Data Source Information**.
The Data Source Information panel appears.
 - Select the row corresponding to the table containing the alarms you want to delete, and then click **Purge Tables**.
Alarms with a status set to Deleted are removed from the table.
- Step 2** To delete all alarms from a table associated with an open view, right-click the tab for the view and select **Set All Status to Deleted and Purge**.
The status of all alarms in that table is set to Deleted and the table content is purged.
- Step 3** To delete a single row from a table associated with an open view, select the row(s) you want to delete and then right-click the first column of the table and select **Delete Row (s) from Database**.



Note You can delete a single row from an Alarm Aggregation table, the Expanded Details Dialog table, or the Drill Down Dialog table.
