Viewing Events

Event Viewer enables you to selectively monitor, view, and examine events from ASA (including ASA-SM), FWSM and IPS devices. Events are organized into views that you can filter or search to find events that interest you. You can create customized views and filters to fit your needs, or use the predefined views included in the application.

This chapter contains the following topics:

Introduction to Event Viewer Capabilities

Event Viewer monitors your network for syslog (system log) events from ASA and FWSM devices and security contexts and SDEE (Secure Device Event Exchange) events from IPS devices and virtual sensors. Event Viewer collects these events and provides an interface by which you can view them, group them, and examine their details.

Note Beginning with version 4.5, Security Manager enables you to forward syslogs to one local collector and two remote collectors. For more information, see Event Management Page, page 11-27.

Tip Event Viewer and its related applications, Report Manager and Health and Performance Monitor, are useful for operational monitoring and troubleshooting of certain types of Cisco devices in your network. These applications do not provide extensive event correlation, compliance reporting, long-term forensics, or the integrated monitoring of both Cisco and non-Cisco devices.

When working with IPS events, the Report Manager component of Cisco Security Manager reports events individually; the Event Viewer component of Cisco Security Manager displays alerts. In the Event Viewer component, the IPS Summarizer groups events into a single alert, thus decreasing the number of alerts that the IPS sensor sends out.

Tip Cisco IPS Manager Express (IME) and Cisco Security Manager do not summarize events in precisely the same way.

This section briefly describes some key activities that Event Viewer can facilitate.

This section contains the following topics:

Historical View

An historical view is one that displays events from a selected period of time (for example, the last 10 minutes) and does not automatically update as new events are collected. You must refresh the view to see newer events.

Consider the following activities among the many possibilities for employing Event Viewer with an historical view:

- **Troubleshoot Connectivity**—When a report comes in that a user cannot reach a particular server, you can set an historical view (for example, the last 10 minutes) that displays all events that affect that user's IP address as a source or destination. Then, you can go from a particular displayed event to the policy denying that user's access to the resource.
- **Tune Signatures**—After setting a view of all IPS messages, or all IPS messages of a given category, you might decide that an event is actually a false positive. You can then cross launch into the associated policy and either tune the signature to exclude the host or lessen the reported severity of the particular event.

  Also consider creating an event action filter to modify how the alert is handled. Frequently, event action filters are a better way of dealing with false positives than editing the actual signature. For more information, see Configuring Event Action Filters, page 40-4.
- **Validate Policy Deployment**—After deploying a new or changed policy, you might want to confirm that it is operating effectively by selecting events corresponding to the given policy. For example, you could identify firewall-deny messages triggered by the new policy.

Real-Time View

A real-time view displays events as they are received and automatically updates the Event Table in waterfall fashion. Keep in mind that the term "real-time" is not precise. System latency and other factors prevent true real-time system response.

Consider the following activities among the many possibilities for employing Event Viewer with a real-time view:

- **Investigate Attacks in Near Real-time**—By isolating details of a particular source IP address, or a source/destination pair, Event Viewer can provide details about attacks on your monitored devices, or attacks that are going through those devices.
- **Validate Device Activity**—You can examine a device in your network and determine whether it is present and whether it is sending events.
- **View High Threat IPS Events**—You can filter a view to display all events that exceed a certain threat level. On a properly tuned IPS sensor, this should be a manageable flow of events to watch in a real-time view.

Views and Filters

When you view events in Event Viewer, you open a view. A *view* is a set of filters and other properties, including color rules, selected columns and their positions and widths, and the default time window, that let you define a subset of events. Views help to limit the scope of the events list so that you can more easily find what you are looking for.

Event Viewer includes a number of predefined views. Although you cannot change the filter rules for these views, you can create copies of the views and change the filter rules in your copy. Views you create are called custom views. For more information, see Creating Custom Views, page 68-40.

Using filters is key to getting the most from Event Viewer. You can distill from all the events being received a view of only the information that you need or want. You can use the various methods of filtering to reduce the events list, filtering lists that have already been filtered. The following list explains the general filtering features; for more information, see Filtering and Querying Events, page 68-42.

- **Time filters**—You can use time filters to limit the events that are loaded into your client as well as to limit the events displayed in the Event Table. With time filtering you can select predefined values, such as **the last hour**, or specify a particular time range by dates and times. For more information, see Selecting the Time Range for Events, page 68-42.
- **Column filters**—You can use column filters to filter events based on a particular value of an event. For example, you could filter on a particular source or destination, or both. For certain columns you can also filter on a range of values or on a policy object. Column filters are part of the view settings for a view. For more information, see Creating Column-Based Filters, page 68-44.
- **Quick filters**—You can use quick filters to execute a text-based filter on events listed in the event table. The search is not column-sensitive, showing all events in which the string appears in any column. You can use the Quick Filter drop-down list (shown as a magnifier) to modify the scope of the filter. For more information, see Filtering on a Text String, page 68-47.
- **Drilling down with filters**—Aggregating additional filters allows you to become more and more selective, to “drill down” until you can view a particular event or set of events that meet your requirements. The View Settings pane at the top of the Event Monitoring window updates with each additional filter choice you make to show the current aggregate filter definition of the view selected.

Policy Navigation

You can navigate from a particular event to the policy within Security Manager that governs that event. You can also navigate from certain policies to events associated with those policies. For more information, see Looking Up a Security Manager Policy from Event Viewer, page 68-53 and Looking Up Events for a Security Manager Policy, page 68-54.

Understanding Event Viewer Access Control

The user privileges assigned to your username control what you can do in Event Viewer. If you use local users, or other types of non-ACS access control, then all users have access to Event Viewer. However, the following access limits are imposed:

- You must have system administrator, network administrator, or approver privileges to select or deselect devices for monitoring. See Selecting Devices to Monitor, page 68-34.
- You must have system administrator privileges to change the Event Management administrative settings page, where you enable or disable the service and configure storage location and other settings, as described in Starting, Stopping, and Configuring the Event Manager Service, page 68-30 and Event Management Page, page 11-27

If you use ACS to control access to Security Manager, you can also control the following:

- You can control access to the Event Viewer application using the View Event Viewer privilege. Using this privilege, you could prevent certain users from accessing Event Viewer, or create roles that allow access to Event Viewer without allowing access to Report Manager. All default ACS roles are permitted to use Event Viewer.
- You can control which users can enable or disable monitoring for devices using the Modify > Manage Event Monitoring privilege. A user must have this privilege to select devices for monitoring as described in Selecting Devices to Monitor, page 68-34. The default ACS roles that have this permission are system administrator, network administrator, approver, security administrator, and security approver.
- You can control the use of the policy lookup feature. Users must have View Device privileges to the device, and also View privileges to the firewall or IPS policy, to perform policy lookup. If users do not have all permissions, they will get an “Unable to Find Matching Rule” error if they try to look up a matching rule. For more information about policy lookup, see Looking Up a Security Manager Policy from Event Viewer, page 68-53.
- Users can view events on devices only if they have at least View privileges to the device.
- You can control access to the Event Management administrative settings page, where you enable or disable the service and configure storage location and other settings, as described in Starting, Stopping, and Configuring the Event Manager Service, page 68-30 and Event Management Page, page 11-27. The user must have Admin privileges to access this page (or any other administrative settings page). All default ACS roles except help desk can view the page, but only system administrators can change settings.
- You can control the use of network/host and service policy objects for column filters (such as the Device, Source, Destination, Source Service, and Destination Service columns). Users must have the appropriate View Object permissions for network/host, network/host-IPv6, and service objects to use them in filters. For more information on creating column filters, see Creating Column-Based Filters, page 68-44.

For information on integrating Security Manager with Cisco Secure ACS, see the *Installation Guide for Cisco Security Manager*.

Scope and Limits of Event Viewer

The following table provides details on the functional scope and limits of Event Viewer:

Table 68-1 Event Viewer Scope and Limits

Item	Description
Device Support	You can view events collected from the following types of devices. Although Event Viewer has been tested with the indicated software releases, you might be able to use it with older software releases. • **ASA devices (including ASA-SM) and security contexts**—All 8.x releases. • **FWSM devices and security contexts**—Releases 3.1.17, 3.2.17, 4.0.10, and 4.1.1 and higher. • **IPS devices and virtual sensors**—Releases 6.1 and higher. IPS support does not include IOS IPS.
Event Data Store Size and Location	You can control the location and disk space allocated to holding events collected from monitored devices. After the Event Data Store is 90 percent filled, newest events replace oldest events. You can also configure an extended storage, or archive, location on attached storage devices. Security Manager automatically copies events into the extended storage; when you view historical events, they are automatically retrieved from extended storage if they no longer reside on the local disk. For more information on configuring these settings, see the Event Management Page, page 11-27
Event Limit	You can control the maximum number of events that can be viewed at one time in the events table using the Event Data Pagination Size option. For information on configuring the option, see Event Management Page, page 11-27.
Policy Objects	You can use some types of policy objects, such as network/host and services objects, when creating column filters. You can also view host object names instead of IP addresses in the source and destination columns by selecting **View > Show Network Host Objects**. This option is selected by default. IP address to host name mapping is supported only for the source and destination of events. Also, the mapping applies to Host objects only; Event Viewer will not show an object name when the source or destination of an event matches a Network object, Group object, or Address Range object. **Tip** Hover over a host object name to view the IP address associated with that object.
Views	A single Event Viewer client can open at most four historical views and one real-time view at a time.
Clients	For a single Security Manager server, a maximum of 5 Security Manager clients can open Event Viewer at one time, and a Security Manager client can open one copy of Event Viewer.

Deeply Parsed Syslogs

The structure and contents of standard syslogs and the elements comprised by each are detailed in the System Logs documentation for the device and software version you are using.

You can find the documentation on Cisco.com at these locations:

- ASA Devices: http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html
- FWSM Devices: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_system_message_guides_list.html

Syslogs other than those listed here are presented as raw syslogs. Only deeply parsed syslogs present the full content carried by the syslog.

The deeply parsed syslogs in Security Manager are detailed in the following table.

Table 68-2 Deeply Parsed Syslogs

Syslog Category	Syslog ID	Total Number of Syslogs
Flow, Session Syslogs	110002-110003, 209003-209005, 302003-302004, 302009-302010, 302012-302018, 302020-302021, 302035-302036, 302303-302306, 302033-302034, 303002-302005, 313001, 313004, 313005, 313008, 324000-324006, 337001-337009, 431001-431002, 407001-407002, 416001, 418001-418002, 419001-419003, 424001-424002, 450001, 448001, 609001-609002 **Note** The 302303-302306 state-bypass syslog has been deep parsed only for event manager. However, the event description in the event manager for TCP, UDP, and SCTP state-bypass syslogs, does not display the "State-bypass" keyword. **Note** Reporting, Event to Policy, and Policy to Event are not supported for state-bypass syslog.	66
Botnet	338001-338004, 338101-338104, 338201-338202, 338301	11
ACL	106100, 106023, 106002, 106006, 106018	5
Denied Firewall	106001, 106007, 106008, 106010-106017, 106020-106022, 106025-106027	12
Identity Firewall	746003, 746005, 746010, 746016	4
AAA	109001-109010, 109012, 109016-109020, 109023-109029, 109031-109035, 113001-113025	44
Inspect	108002-108007, 303004-303005, 400000-400050, 406001-406002, 415001-415020, 500001-500005, 508001-508002, 608001-608005, 607001- 607003, 703001-703002, 726001	99
NAT	201002-201006, 201009-201013, 202005, 202011, 305005-305012	21

Table 68-2 Deeply Parsed Syslogs (Continued)

Syslog Category	Syslog ID	Total Number of Syslogs
IPSec VPN	402114-402122, 602103-602104, 602303-602304, 702305, 702307	15
Failover (HA)	101001-101005, 102001, 103001-103007, 104001-104004, 311001-311004, 709001-709007, 210001-210022 (except 210008, 210010)	49
SSL VPN	725001-725009, 725012-725013, 716001-716020, 716023 -716039, 716041-716060, 722001-722023, 722026-722044, 722046-722051, 723001-723002, 723009-723012, 723014, 724001-724004	8
Etherchannel	426001-426003	3
Cluster	302022- 302027	6

Overview of Event Viewer

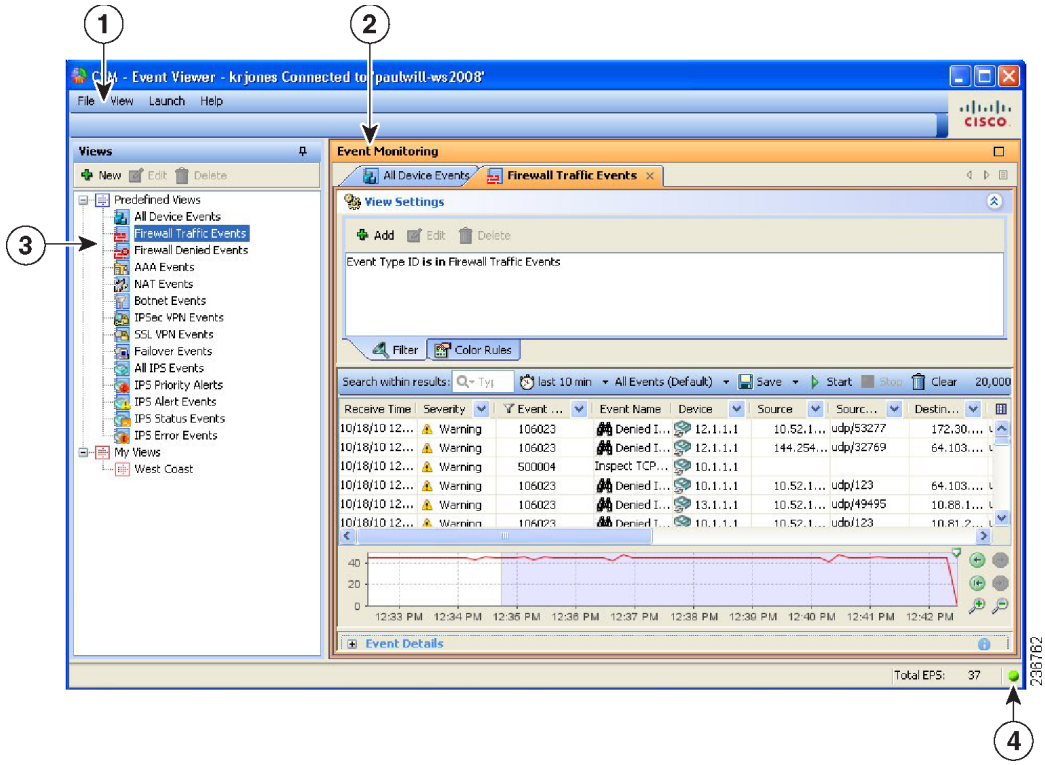
Use Event Viewer to view events and alerts collected from monitored firewall and IPS devices. For more information about selecting devices for monitoring, see Selecting Devices to Monitor, page 68-34.

To open Event Viewer, do any of the following:

- Select **Start > All Programs > Cisco Security Manager Client > Event Viewer** from the Windows Start menu (your exact command path might differ), or double-click the Event Viewer icon on the desktop. You are prompted to log in. For more information about starting a Security Manager client application, see Logging In to and Exiting the Security Manager Client, page 1-12.
- Select **Launch > Event Viewer** from the Configuration Manager or Report Manager applications, or click the Event Viewer button on the Configuration Manager toolbar. Event Viewer is opened using the same user account that you used to log into the other application.

The following illustration and subsequent list explain the basics of Event Viewer.

Figure 68-1 Event Viewer Main Window



The following list explains the main Event Viewer window in more detail.

- **(1) Menu Bar**—General commands for performing actions in Event Viewer, including the following menus:
  - File, for operations on views. For information on the commands, see Event Viewer File Menu, page 68-9.
  - View, for operations within a view and general system management. For information on the commands, see Event Viewer View Menu, page 68-10.
  - Launch, for opening the Configuration Manager or Report Manager applications.
  - Help, for opening the online help or for viewing copyright and licensing information.
- **(2) Event Monitoring Window**—The right pane shows the open views. Each open view is represented on separate tabs (you can have up to four open historical views and one real-time view). Note that you can arrange views horizontally or vertically in this space, or even make a view float to a separate window. For more information about how you can arrange or float views, see Floating and Arranging Views, page 68-37.

  For detailed information about the many parts of the event monitoring window, see Event Monitoring Window, page 68-14.
- **(3) View List**—The left pane is a list of views. The list is organized into folders that separate the predefined views from the custom views, which are listed in the My Views folder. The simplest way to open a view is to double-click it, which replaces the currently open view. To open a view without replacing the currently open view, right-click the view and select **Open in New Tab**. For more information on opening views, see Opening Views, page 68-37.

  For information about other things you can do with the view list pane, see View List, page 68-12.

- **(4) Status Information**—The lower right portion of the status bar shows the current events per second (EPS) rate and an icon that indicates the current health of the monitoring system. Click the alert status icon to open a bubble that shows statistics for the past five minutes and any current system alerts. From this view, you can click the Details link to see more detailed information; click the alert status icon again to close the bubble. For more information, see Monitoring the Event Manager Service, page 68-31.

Note The Events per Second (EPS) information that is displayed on the Status Bar is calculated based on the number of events received every two seconds. Whereas, the EPS information that is displayed on the Time Slider graph is calculated by performing an aggregation of all the events that are available in a selected time range. Therefore, the numbers displayed on the Status Bar and the Time Slider graph might differ.

See an example below:

Example of EPS information display on the Status Bar

Assume at time T1, the Event Viewer application received 192 events. The Events per second (EPS) that will be displayed on the Status Bar is 192 / 2 = 96. This is because Security Manager collects events every 2 seconds and displays the Events per Second on the Status Bar. Let us say at T1 + 2 seconds, the Event Viewer application received 384 events. The EPS that will be displayed on the Status Bar is equal to (384 - 192)/2 = 96. This is the difference between current and previous value divided by 2.

Example of EPS information display on the Time Slider graph

Security Manager persists the events per second at an interval of 10 seconds. For example, if the Event Viewer application received 352 events in 10 seconds interval, the EPS is equal to 352 / 10 = 35. This value is persisted by Security Manager. For the next 10 seconds interval, if the Event Viewer receives 1056 events, the EPS will be equal to (1056 – 352)/ 10 = 70, which is persisted by Security Manager.

Displaying values on the Time Slider graph

The Time Slider graph displays the information for a period of time which has a Start Time and an End Time. All events per second that were collected in the given time interval are aggregated and plotted on the graph. In the given example, 35 and 70 are the values stored every 10 seconds. Therefore the Time Slider graph displays EPS as 35 and 70, which are different from the values displayed in the Status Bar.

Event Viewer File Menu

The following table describes the commands on the File menu in Event Viewer.

Table 68-3 File Menu in Event Viewer

Command	Description
New View	Creates a new custom view. You are prompted for a name and description. See Creating Custom Views, page 68-40. Alternatively, click the **New (+)** button in the view list.

Table 68-3 File Menu in Event Viewer (Continued)

Command	Description
Open View	Opens a view on a new tab. You are prompted to select the view to open. You can open at most four historical views and one real-time view. See Opening Views, page 68-37. **Tip** You can double-click in the view list to open the view and replace the view that is displayed.
Save	Saves changes made to the active view, including filters (for custom views only), table preferences such as selected columns, column width, and sort order, the time range, and color rules. See Saving Views, page 68-41. If you want to save filter changes for a predefined view, you must use Save As to create a new custom view.
Save As	Saves as a custom view the changes you have made to the displayed view. See Saving Views, page 68-41.
Close View	Closes the displayed view.
Close All Views	Closes all open views.
Exit	Closes Event Viewer. Exiting the application closes any floating Event Viewer window that is open.

Event Viewer View Menu

The following table describes the commands on the View menu in Event Viewer.

Table 68-4 View Menu in Event Viewer

Command	Description
Mode	Specifies the time interval for selecting the events to display in the event table. From the submenu, select one of the following options: • **last 10 minutes** • **last 1 hour** • **last 12 hours** • **last 1 day** • **last 1 week** • **is today** • **is yesterday** • **is on . . .** (Opens a calendar on which you click to specify a single date.) • **is between** (Opens two calendars on which to specify a beginning and ending date and time.) • **Real Time** (Sets the mode to display events as they are received.) Alternatively, click the **Time Selector** control on the toolbar and select from the same options. See Event Table Toolbar, page 68-16.
Customize Column	Changes the columns shown in the event table. The Choose Columns to Display dialog box opens, where you can select the columns that you want to display. For details on the columns available, see Columns in Event Table, page 68-18.
Start	Initiates retrieving events to update the current view's event table. The event table then displays events received from the moment you clicked **Start** back to either the limit of the time mode or the event table pagination limit. Alternatively, click the **Start** button on the event table toolbar.
Stop	Stops event retrieval. The event table then displays the events received until the moment you clicked Stop. Alternatively, click the **Stop** button on the event table toolbar.
Show View Settings	Opens the View Settings pane, which displays the filters and color settings for the current view. You can alter these settings using the View Settings pane. Alternatively, click anywhere in the View Settings pane title bar, such as on the icon, on the text, or on the double arrow on the right side of the title bar. Clicking the heading opens and closes the pane.

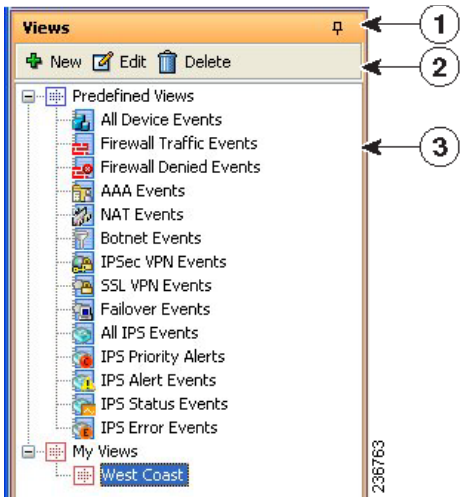
Table 68-4 View Menu in Event Viewer (Continued)

Command	Description
Show Event Details	Opens the Event Details pane and displays the selected event's details. Alternatively: • Click the expand icon (+) on the left of the Event Details pane title bar. • Double-click an event in the event table to display the event details data in a pop-up window. **Tip** From the Event Details dialog box you can print the event details or you can copy one or more of the detail rows to your clipboard. You can also scroll through the events list using the Next and Previous buttons.
Manage Monitored Devices	Allows you to select which devices, or groups of devices, can have events displayed in Event Viewer. For more information, see Selecting Devices to Monitor, page 68-34. **Note** By default, any ASA, FWSM, or IPS device added to the Security Manager inventory is monitored.
Show Event Store Disk Usage	Opens a window that displays the amount of disk space used as well as the age of the oldest event stored. See Monitoring Event Data Store Disk Space Usage, page 68-34.
Show Network Host Objects	When selected, the host object name is displayed, if available, instead of the Source or Destination IP address. This option is selected by default. **Tip** Hover over a host object name to view the IP address associated with that object.
Reset Layout	Re-establishes the width of the view list pane to its original setting after it has been hidden or manually narrowed or widened

View List

The left pane of the Event Viewer main window displays a list of available views as shown in the following illustration. A *view* is a set of filters and other properties, including color rules, selected columns and their positions and widths, and the default time window, that let you define a subset of events.

Figure 68-2 Event Viewer View List



The view list includes the following controls:

- **(1) Push Pin button**—Click the Push Pin icon to control whether the view list pane is opened or closed. If the pin is vertical, the view list remains open unless you maximize the event monitoring window (the right pane). If the pin is horizontal, the view list collapses to the left margin, and you must click the Views heading in the left margin to open the list.
- **(2) Toolbar**—The toolbar contains these buttons:
  - **New button**—Click the New button to create a new custom view. You are prompted for a view name and description. For more information, see Creating Custom Views, page 68-40.
  - **Edit button**—Click the Edit button to change the name or description of the selected custom view. You can edit custom views only. For more information, see Editing a Custom View Name or Description, page 68-41.
  - **Delete button**—Click the Delete button to delete the selected custom view. You can delete custom views only. For more information, see Deleting Custom Views, page 68-42
- **(3) List of views**—The list is organized into folders that separate the predefined views from the custom views, which are listed in the My Views folder. The simplest way to open a view is to double-click it, which replaces the currently open view. To open a view without replacing the currently open view, right-click the view and select **Open in New Tab**. For more information on opening views, see Opening Views, page 68-37.
- **Right-click shortcut menu**—If you right-click on a view, you get a list of additional commands that you can perform:
  - Open—Opens the view and uses it to replace the currently active view. If the currently active view contains unsaved changes, you are prompted to save them. If the view is already open, it is brought to the foreground. See Opening Views, page 68-37.
  - Open in New Tab—Opens the view in a new tab, so that no existing open views are closed. See Opening Views, page 68-37.
  - Save As—Saves the view as a new custom view. See Saving Views, page 68-41.
  - Edit—Edits the custom view name and description. See Editing a Custom View Name or Description, page 68-41.
  - Delete—Deletes the custom view. See Deleting Custom Views, page 68-42.

– View Description—Displays the description for the view.

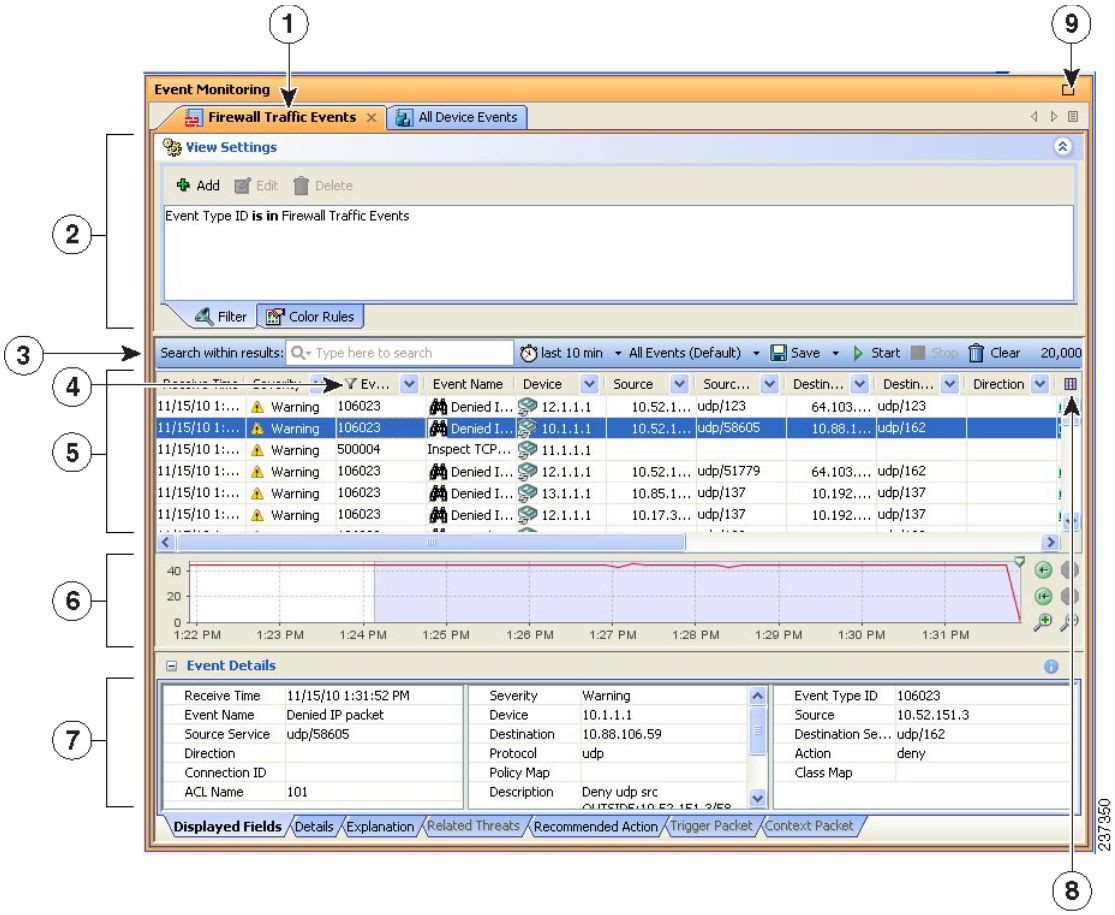
Related Topics

- Views and Filters, page 68-3
- Overview of Event Viewer, page 68-7
- Floating and Arranging Views, page 68-37

Event Monitoring Window

The Event Monitoring window shows the event views that you have opened. From this window, you can configure views and analyze and filter events.

Figure 68-3 Event Monitoring Window



1	View tabs.	**6**	Time slider.
2	View Settings pane.	**7**	Event Details pane.
3	Event table toolbar.	**8**	Column selector button.
4	Filtered column icon.	**9**	Open view scroll buttons and list.
5	Event table.		

The Event Monitoring window contains these main elements:

- **View tabs (1, 9)**—When you open a view, it is represented as a tab in the window. To change views, click the tab, click the left or right arrow buttons to scroll through the tabs, or click the Open View List button and select the desired view. You can arrange views to be side by side or to float to separate windows by right-clicking the tab name and selecting an appropriate command; for more details, see Floating and Arranging Views, page 68-37.

Note You can open at most four historical views and one real-time view.

- **View Settings pane (2)**—Use the View Settings pane to define the column filters and color rules to use in a view. You can open and close the pane by clicking anywhere in the heading or by toggling the **View > Show View Settings** command.

  The View Settings pane contains two tabs: Filter and Color Rules. These tabs are shown along the bottom of the pane. On each tab, the body of the tab shows the current filter or rules; to change a rule, you select it and click the Edit or Delete buttons along the top of the pane, as appropriate. To create new rules, click the Add button.

  You can also add filters using the column filtering controls in the events table, as described in Creating Column-Based Filters, page 68-44. For more information on color rules, see Configuring Color Rules for a View, page 68-39.
- **Event Table Toolbar (3)**—The toolbar above the event table includes shortcut buttons and other controls that relate specifically to the events listed in the table. For a description of the toolbar controls, see Event Table Toolbar, page 68-16.
- **Event Table (4, 5, 8)**—The event table shows the events that match your filter criteria, one event per row. These events might be retrieved from the primary or the extended data store; you do not have to explicitly request data from the extended data store. To see events from a device, you must have View Device privileges to the device.

  The columns that make up the event table can be hidden, resized, reordered, and sorted upon as described in Customizing the Event Table Appearance, page 68-38. For a description of the columns, and how to use the column selector button to choose which columns are shown, see Columns in Event Table, page 68-18.

  If a column has a filter applied to it, an icon appears in the column heading.
- **Time Slider (6)**—For historical views, the time slider shows the current slice of time displayed in the table and the events per second rate as a linear graph. For more information about using the time slider, see Time Slider, page 68-25.
- **Event Details Pane (7)**—The event details pane shows detailed information about the currently selected event. You can open and close the pane by clicking anywhere in the heading or by toggling the **View > Show Event Details** command. For more information, see Event Details Pane, page 68-26.

Event Table Toolbar

The following illustration and table explain the elements in the toolbar that resides immediately above the event table in Event Viewer.

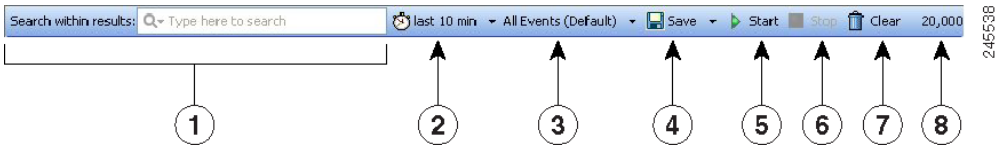


Table 68-5 Event Table Toolbar Elements

Callout	Name	Description
1	Search Within Results Field (Quick Filter)	This tool is also known as the *Quick Filter*. Use it to search for a word or phrase as well as to limit the scope of the search to certain columns. Further, you can select whether the search term used should be considered case sensitive, whether wildcards may be used, and whether a match may be partial, case sensitive, exact, or anywhere within a string. This search operates only on the selected view and within the data loaded. For more information, see Filtering on a Text String, page 68-47.
2	Time Selector (Mode) (Equivalent to **View > Mode**.)	You use the time selector to do the following: • Filter the events shown in the event table pane according to the time they were received. See Selecting the Time Range for Events, page 68-42. • Select between a real-time view or historical views. See Switching Between Real-Time and Historical Views, page 68-41. • Determine the time interval loaded in the client. If you are using one of the modes that shows events from the current time into the past, hovering the pointer over the field shows the start and end times for the displayed events. If you are using a specific time interval, the interval is shown in the toolbar.
3	Events by IP Address Type Selector	You use the events by IP address type selector to filter the list based on the type of IP address included in the events. Options are: • **All Events (Default)**—Show all events regardless of the address type. This is the default option. • **IPv4 Events Only**—Show events only if all addresses in the event are in IPv4 format. • **IPv6 Events Only**—Show events only if at least one address in the event is in IPv6 format. **Tip** You cannot save your selection. The next time you open the view, you need to reselect your option if you want something other than the default.
4	Save (Equivalent to **File > Save** or **File > Save As**.)	Click **Save** to save changes to the current view, including filters (for custom views only), table preferences such as selected columns, column width, and sort order, the time range, and color rules. Alternatively, click the down arrow and select **Save As** to save changes as a new custom view. If you want to save filter changes for a predefined view, you must use Save As to create a new custom view. For more information, see Creating Custom Views, page 68-40.

Table 68-5 Event Table Toolbar Elements (Continued)

Callout	Name	Description
5	Start (Equivalent to **View > Start**.)	Click **Start** to reload or restart the listing of events in the Event Table. Clicking Start retrieves any events that have occurred since you originally loaded the table.
6	Stop (Equivalent to **View > Stop**.)	Click **Stop** to halt the listing of events in the Event Table. If you are in a real-time view, the Time Selector indicates the time stopped as well as the time interval that is loaded. Clicking on stop can also halt a query and display the set of events currently loaded in event viewer.
7	Clear	Click **Clear** to empty the event table.
8	Event Enumerator and messages	The number shown on the right of the toolbar indicates how many events are loaded onto the Event Viewer client. The number grows as events are loaded until either all events matching the filter criteria are displayed, or the pagination limit is reached, whichever is lowest. If you change the pagination limit (see Event Management Page, page 11-27), you must exit Event Viewer and open it again for the new limit to be in effect. If your query requires that events be retrieved from the extended event storage area, a message such as "Data being fetched from extended store" appears. Fetching events from the extended storage area typically takes longer than fetching them from the primary storage area.

Columns in Event Table

The following table lists alphabetically, and describes, all the columns that you can display in a view in Event Viewer. The columns applicable to a particular device vary, as does the presence or absence of event data for a particular event type.

When you save a view, the columns you selected, and their order, are preserved and displayed the next time you open the view. To select which columns to display in the open (and active) view, do one of the following:

- (Preferred method.) Click the **Column Chooser** icon in the far right of the event table header row (see Event Monitoring Window, page 68-14). The Choose Columns to Display dialog box that opens lists the columns in alphabetical order. You can select or deselect the columns either individually or by using the **Select/Unselect All** check box. Also, you can click Revert to return to the default column selection for the view.
- Select **View > Customize Columns**.
- Right-click any column heading and select or deselect a column individually, or select More to open the same dialog box that is used by the View > Customize Columns command.

Note Most columns other than Description, Event Name, and Receive Time include a filtering function. For more information, see Creating Column-Based Filters, page 68-44.

Table 68-6 Event Viewer Column Descriptions

Column Label	Description
AAA Group	The AAA group policy.
AAA Server	The server that handles user requests for access; it performs authentication, authorization, and accounting.
AAA User	The AAA username.
ACE Hash1 ACE Hash2	The hashcode1 and hashcode2 of the access control list entry (ACE). Hash codes are required for successful policy lookups from syslog 106023 and 106100 events. These hash codes are available only if you deployed the configuration using Security Manager.
ACL Name	The name or ID of the access control list (ACL).
Action	The action performed on the flow. For example: Terminated or denied.
Alert Details	The details regarding the alerts.
App Name	The name of the application originating the event.
App Stop Reason	An explanation of how or why the application was shut down.
App Version	The version of the application originating the event.
Attack Relevance Rating	A numerical value used to indicate an attack's relevance to its destination target or targets.
Backplane Interface	The backplane interface, which is identified only when the backplane interface differs from the physical interface.
Botnet Category	The category showing the reason a domain name is blacklisted, for example, botnet, Trojan, spyware, and so on.
Botnet Domain	The domain name or IP address in the dynamic filter database to which the traffic was initiated. It can be black listed, white listed, or grey listed.
Build Time	The date and time of the software build.
Build Type	The type of build. Typically this is a word such as "release" or "debug." In some cases, it is the ID of the builder of the application.
Byte Count	The number of bytes in the data transfer of the connection.
Call Id	The peer's Call ID for the session to which this packet belongs.
Class Map	The class map name.
Connection Duration	The lifetime of the connection.
Connection ID	A unique identifier for the connection.
Connection Limit	The maximum number of connections or sessions.
Connection Termination Value	A factor for which the connection is terminated, for example, incorrect version or invalid payload-type.
Current Connection Count	The number of current connections.
Description	For syslogs this shows the raw message, for IPS it shows a description of the event.

Table 68-6 Event Viewer Column Descriptions (Continued)

Column Label	Description
Destination	The IP Address or hostname of the traffic destination (for ASA and FWSM) or the attack target (for IPS). It can be multi-valued and contain IPv4 or IPv6 addresses. If View > Show Network Host Objects is selected and a host object is defined that matches the destination IP address, the host object name is displayed. **Tip** Hover over a host object name to view the IP address associated with that object.
Destination Context Data	Context buffer indicating the data that was sent just prior to, and immediately after, the alert was triggered. A Base64-encoded representation of the stream data that was sourced by the target.
Destination FQDN	The fully-qualified domain name of the destination IP address, if any.
Destination Interface	The destination interface. For Etherchannel alerts (426001-426003), this is the name of the Etherchannel interface for which this event occurred. The member interface is identified in the Source Interface column.
Destination Locality	Whether the target address is located inside or outside of a given network as specified by the intrusion.
Destination OS	The target's operating system information.
Destination OS Relevance	A numerical value indicating the relevance of the destination target OS value.
Destination OS Source	The source of the Target OS data. Possible values are: learned, imported, or configured.
Destination Service	The destination port. It can be multi-valued.
Destination User Identity	The user name for the traffic destination, if any.
Device	The source of the event; usually the device ID. A device identified as Not Available has been deleted from the Security Manager inventory.

Table 68-6 Event Viewer Column Descriptions (Continued)

Column Label	Description
Device Identifier	For a cluster of ASA devices, the ID of the event's source node, which is based on the "Enable Syslog Device ID" configuration on the Server Setup Page, page 53-21. You can use a "Device Identifier" to filter the syslogs generated by a failover device. In the event of a failover, the IP address of the failover device, that generated the syslog messages is displayed here. However, the Device Identifier column will be blank for syslog messages generated by failover device managed in Cisco Security Manager. **Note** Enable the **Process Syslogs from Failover Standby Device** check box in the **Event Management Page** in **Tools > Cisco Security Manager Administration**. A cluster is managed by Security Manager as a single device with multiple nodes. Thus, all the node's events are mapped to the cluster virtual IP and are displayed with the cluster virtual IP in Event Viewer. You can use "Device Identifier" to filter the syslogs generated by a specific cluster member of a node.
Direction	The direction of the traffic: inbound or outbound.
Event ID	A unique sequential number for each event, assigned internally.
Event Name	A user-friendly name given to the event.
Event Summary	Specifies that this is a summary alert, representing one or more alerts with common characteristics. The numeric value indicates the number of times the signature fired since the last summary alert with a matching initialAlert attribute value.
Event Type ID	For ASA or FWSM, the syslog ID. For IPS, this value could be: • A combination of Sig Id & Sub-Sig ID (for IPS Alert Events) • IPS Status (for IPS Status Events) • IPS Error (for IPS Error Events).
Execution State	The execution status of the application.
Final Alert	Applies to a summary alert, representing one or more alerts with common characteristics. It indicates whether this is the last event alert containing the same value in the initialAlert attribute.
Generation Time	Represents device local event generation time (available only for IPS events).
Global Correlation Audit Mode	Whether the alert was handled with audit mode processing: true or false.
Global Correlation Deny Attacker	Whether a deny-attacker action occurred (or would have occurred) because an internal override was exceeded due to the calculated risk rating: true or false.
Global Correlation Deny Packet	Whether a deny-packet action occurred (or would have occurred) because an internal override was exceeded due to the calculated risk rating: true or false.

Table 68-6 Event Viewer Column Descriptions (Continued)

Column Label	Description
Global Correlation Modified Risk Rating	Whether the risk rating was adjusted by adding the reputation risk delta due to the risk rating: true or false.
Global Correlation Other Overrides	Whether any other defensive actions were taken because an override threshold was exceeded due to the calculated risk rating: true or false.
Global Correlation Risk Delta	A value from 0 to 99 that indicates how much the risk rating was increased due to the reputation score. If audit-mode is enabled, then it indicates how much the risk rating would have been adjusted had audit-mode not been enabled.
Hit Count	The number of times the flow was permitted or denied by the ACL entry in the configured time interval. The value is 1 when the ASA or FWSM generates the first syslog message for a particular flow.
Hit Count Info	ACL Hit Count information, for example, *First hit*.
Host ID	The globally unique identifier for the host that originated the event.
ICMP Code	The code of the ICMP type. For example, ICMP Type 3 and Code 0 is Net Unreachable or Code 1 is Host Unreachable.
ICMP Type	The type of ICMP message. For example, 3 for Destination unreachable, 8 for Echo.
Initial Alert	This field applies to a summary alert, representing one or more alerts with common characteristics. The value of InitialAlert provides the event ID of the last non-summary evIdsAlert with the same characteristic (sigid/subsigid).
Ip Log ID	The IP Log Identifier that uniquely identifies (with host-scope) an iplog document.
IpLog Address	The IPv4 or IPv6 address associated with the IP log.
IpLog Alert Reference	The global event ID of the evAlert event that triggered the log to be initiated.
IpLog Begin Time	The start of the time range that is currently available in the log document.
IpLog Bytes Captured	The total bytes captured. Note that some packets that were captured may have already been deleted from the log due to memory limitations.
IpLog Bytes Remaining	The number of bytes remaining until the log will be terminated.
IpLog End Time	The end of the time range that is currently available in the log document.
IpLog Minutes Remaining	The minutes remaining until the log will be terminated.
IpLog Packets Captured	The total number of packets captured and logged.
IpLog Packets Remaining	The packets remaining until the log will be terminated.
IpLog Status	A string that represents the log status.
IPS Category	The SEE event category.
IPS User	The username of the user initiating the operation.
License Limit	The maximum number of licenses.

Table 68-6 Event Viewer Column Descriptions (Continued)

Column Label	Description
List Name	The list that includes the domain name, administrator whitelist, blacklist, or IronPort list.
Login Action	The login action that occurred: loggedIn, loggedOut, or loginFailed.
Malicious Host	The hostname of the malicious host.
Malicious IP	The IP address of malicious device.
Max Connection	The maximum number of NAT connections.
MaxEmbryonic Connection	The maximum number of embryonic connections.
NAT Destination	The translated (also called natted) destination IP address. The host name of the translated destination.
NAT Destination Service	The translated (or natted) destination port.
NAT Global IP	The global address. It can contain IPv4 or IPv6 addresses.
NAT Source	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses. The host name of the translated source.
NAT Source Service	The translated (or natted) source port.
NAT Type	The type of network address translation, for example *Static* or *Dynamic*.
New Time	The time to which the device clock was changed.
New Version	The system software version after an upgrade installation.
No.	The number of the event (row) in the current display. This is a simple sequential number and is not related to the content of the event. See the Event ID and Event Name fields for information about the type of event.
Old Time	The device clock time prior to a change.
Old Version	The system software version before an upgrade was uninstalled.
Operation Successful	Indicates whether an operation was successfully performed.
Package File	The name of package file to be auto-downloaded and installed.
Physical Interface	The physical interface, which is identified only if physical interface is different from the respective value in the Interface column.
Policy Map	The policy map name.
Protocol	The Level-3 or Level-4 protocol.
Protocol Version	The protocol version.
Protocol (Non L3)	Some non-Level-3 or -4 protocol seen in the event, for example, TACACS, RADIUS, FTP, or H245.
Reason	A rationale associated with certain events. For example, a connection tear down may have an associated reason.
Receive Time	The time the event was received by Security Manager.

Table 68-6 Event Viewer Column Descriptions (Continued)

Column Label	Description
Reputation	The attacker's reputation score in the range -10.0 to +10.0. A lower (more negative) score indicates a greater likelihood that the host is malicious.
Result Status	The status of an operation, which indicates whether the operation successfully completed.
Risk Rating	A value that represents the calculated risk associated with the event.
Role in Cluster	The role of this member of an ASA load-balancing cluster: Cluster, Master, or Slave.
Security Context	The security context with which the named interface, specified in the corresponding Interface column, is associated.
Sensor Event ID	The serial number for an event, which is guaranteed unique within the scope of the originating host.
Severity	The firewall or IPS severity values.
SIA Event Name	The event that occurred for the service identified in the SIA Service Name field.
SIA Service Name	The name of the Service Insertion Architecture (SIA) service for which this event occurred.
Sig Details	The details of the reported signature that was triggered and resulted in the generation of the alert.
Sig ID	The Sig ID value is used by the alert originator to identify the activity. It identifies the pre-defined signature defined for this activity.
Signature Version	The version of the signature definition used to generate an alert.
Source	The IP Address or hostname of the traffic source (for ASA and FWSM) or the attacker (for IPS). It can be multi-valued and contain IPv4 or IPv6 addresses. If View > Show Network Host Objects is selected and a host object is defined that matches the source IP address, the host object name is displayed. **Tip** Hover over a host object name to view the IP address associated with that object.
Source Context Data	The context buffer indicating the data that was sent just prior to and immediately after the alert was triggered. A Base64-encoded representation of the data stream that was sourced by the attacker.
Source FQDN	The fully-qualified domain name of the source IP address, if any.
Source Interface	The source interface. For Etherchannel alerts (426001-426003), this is the name of the interface that is part of the Etherchannel bundle for which this event occurred. The Etherchannel interface is identified in the Destination Interface column.
Source Locality	Identifies whether the attacker address is located inside or outside of a given network, as specified by the intrusion detection device's configuration.

Table 68-6 Event Viewer Column Descriptions (Continued)

Column Label	Description
Source Service	The source port.
Source User Identity	The username associated with the traffic source, if any.
SSO Server	The single sign-on (SSO) server name.
SSO Server Type	The single sign-on (SSO) server type, for example, SiteMinder.
Sub SigId	The sub-sig ID value, which is used by the alert originator in combination with the signature ID (sigId) to identify the activity.
Summary Type	Defines the common characteristics of all alerts in a summary alert.
Target Value Rating	The asset values associated with targets identified in alerts.
Threat Level	Shows one of the following values, if any threat level pertains: none, very-low, low, moderate, high, or very-high.
Threat Rating	The threat rating of the event, if any.
Time Zone	The local time zone at the originating host's location.
Translated Call ID	The peer's Translated Call ID for the session to which this packet belongs.
Trigger Packet	The single, complete packet (in base64 binary format) that triggered the alert.
Truncated	Whether the trigger packet contained in the event is truncated.
Tunnel Type	The VPN tunnel type.
Type	The AAA type, for example authentication, authorization, or accounting.
Upgrade Name	The name of the upgrade package that was uninstalled.
URI	The URI of the auto-upgrade server directory.
UTC Offset	The offset attribute of sensor local time indicates the number of minutes that must be added to the UTC time to convert to local time at the originating host.
Virtual Sensor	The name of the virtual sensor associated with the event.
VLAN Id	The VLAN number associated with packets involved in the activity that triggered the alert.
VPN Group	The VPN group policy.
VPN IPSec SPI	The IPSec Security Parameter Index.
VPN User	The VPN username.
Watchlist Delta	The amount that the risk rating value was increase due to the source of the activity associated with the alert being on a watchlist.

Time Slider

The time slider resides below the events table when you are using an historical view; it is not used with real-time views. The following illustration explains the time slider; the pagination controls on the right are explained in Table 68-7.

Figure 68-4 Time Slider Elements

You can use the time slider to do the following:

- View the EPS (events per second) trends for the server. You can use the controls on the right to zoom in or out to get a better view of the EPS trends over the time frame that concerns you.

  You can also click and drag the background of the time slider to position the time ranges within the window. Moving the background does not affect the selected time range.

- Select a slice of time for displaying events in the table, either by moving the vertical slider or by using the pagination controls. The position of the vertical slider determines the most recent event displayed in the event table. Whenever you alter the time slice, the event table is reloaded with the events that match the time period.

  The time range of the events displayed in the event table is determined by the selected time interval. For more information, see Selecting the Time Range for Events, page 68-42.

The following table explains the pagination controls to the right of the time slider.

Table 68-7 Time Slider Paging Controls

Element	Description
	Previous page (earlier) and next page (later). The size of page varies according to the selected time mode. **Note** Using the page controls alternately, for example forward and then back, causes the sort order in the event table to reverse. That is, the latest events go from the top of the table to the bottom, or from the bottom to the top.
	First page (earliest) and last page (most recent).
	Zoom in (smaller total time interval shown) and zoom out (greater time interval shown). Zooming does not change the content of the event table. A shaded blue area indicates the time interval currently displayed in the event table.

Event Details Pane

The Event Details pane (illustrated in Event Monitoring Window, page 68-14) presents information contained within a single event. The information, which is displayed in multiple tabs within the pane, varies according to the richness of the event and the capability of Event Viewer to parse the data. Components include:

- **Displayed Fields Tab**—Displays the fields shown in the Event Table.
- **Details Tab**—Displays all available fields for the selected event. The fields are presented in alphabetical order.

- **Explanation Tab**—Displays a generic explanation for this event type.
- **Related Threats Tab**—Displays threats correlated to the event. (IPS Events only.)
- **Recommended Action Tab**—Displays a generic recommendation for an event of this type. (Syslogs only.)
- **Trigger Packet Tab**—Displays trigger packet data. (IPS Events only.)
- **Context Packet Tab**—Displays context packet data from the Source (Attacker) and Destination (Target). (IPS events only.)
- **Notes**—Enables you to add a note so that you can revisit particular signatures later to see what you or other users have added for a signature or an event. For more detailed information, refer to Signatures Page, page 39-4

Note The notes added here will be persistent when you cross-launch to Configuration Manager.

Note If you have more than one event for a particular signature, then annotating one event will annotate all the events related to that signature.

Preparing for Event Management

Before you can view events generated from a device, you must configure the device to work with Event Viewer.

Ensuring Time Synchronization

Standard network management practice includes consideration of time differences and network device synchronization. Typically, this includes the use of a Network Time Protocol (NTP) server. Event Viewer is most easily used with a common time standard. However, it is worth noting that you can view the time an event is received by Security Manager (Receive Time), and for IPS devices, the time the event was generated by a device (Generation Time).

Whenever possible, configure the Security Manager server and the devices it is monitoring with the same NTP server.

Differences between the clock on the Security Manager server and the clock on a Security Manager client at the time the client is opened are taken into account while translating/mapping event data from the server time to the client time. If the time difference changes dynamically due to the Security Manager server time moving ahead, for example, the data retrieved from the server will show an updated timestamp, but the client will continue to map the time difference based on the times on the server and the client when the client was opened. In such a situation, no data will be seen on Event Viewer for a brief interval that corresponds to the time change on the server. For this reason, we recommend that Security Manager server clock changes are done less frequently and at a time that would be the least impacting.

Configuring ASA and FWSM Devices for Event Management

Before you can use Event Viewer, or any other application that analyzes syslog events, to view events generated from an ASA (including ASA-SM) or FWSM device, you must configure the logging policies on the device to generate and transmit syslog messages.

Note A cluster device with a Virtual IP address (beginning with Security Manager version 4.4) can be added if configured in both Security Manager and on the virtual device.

Tip Although you can configure devices individually to specify the appropriate logging configuration, it is likely that more than one ASA or FWSM device in your network would use the same logging configuration. Although this topic describes how to configure an individual device, you can also create shared policies and assign them to multiple devices. For more information about configuring and assigning shared policies, see Creating a New Shared Policy, page 5-54 and Modifying Policy Assignments in Policy View, page 5-54.

Besides the logging configuration described here, you can also configure logging for individual access control entries when you configure them either in firewall policies or ACL policy objects. The default is to log denied access only, but you can configuring ACL logging options to provide increased logging.

Note To reliably report events from contexts in multiple-context mode, Cisco Event Viewer requires an IP address for the management interface of each context.

Step 1 (Device view) Select the ASA or FWSM device or security context, then select **Platform > Logging > Syslog > Logging Setup** from the Policies selector.

In the policy, select **Enable Logging**. You can configure other options as needed. For detailed information about the options, see Logging Setup Page, page 53-15.

Step 2 Select **Platform > Logging > Syslog > Syslog Servers**.

Add the Security Manager server's IP address to the syslog servers table. Configure the server to use the UDP protocol. The default port, 514, is correct unless you configure a different port on the Security Manager Administration Event Management Page, page 11-27.

If you are using other event management applications, such as CS-MARS, also add those servers to this policy.

Note You can use EMBLEM message format if you desire; both traditional and EMBLEM formats are supported. Keep in mind that EMBLEM is not supported by CS-MARS, so do not send EMBLEM-formatted messages to a CS-MARS server.

For detailed information about the options in the Syslog Servers policy, see Syslog Servers Page, page 53-26.

Step 3 If you want to configure non-default syslog server settings, such as adding time stamps to syslog messages, changing the severity level of messages, or suppressing the generation of specific messages altogether, configure the **Platform > Logging > Syslog > Server Setup** policy. For detailed information, see Server Setup Page, page 53-21

Step 4 (Optional)You can configure the **Platform > Logging > Syslog > Logging Filters** policy to fine-tune the kinds of messages sent to syslog servers. For detailed information about this policy, see Logging Filters Page, page 53-12 and Edit Logging Filters Dialog Box, page 53-13.

Following are some tips for configuring this policy:

- When adding the logging filter, select **Syslog Servers** for Logging Destination.
- You can create a simple filter based on message severity, or you can configure a much more complex filter based on event classes. If you elect to use event classes, you can do the configuration directly in the Logging Filters policy, or you can configure event lists separately in the **Event Lists** policy (see Event Lists Page, page 53-9).

Step 5 (Optional) You can configure the **Platform > Logging > Syslog > Rate Limit** policy to limit the quantity of messages generated per time interval, either by message severity or message number. This can help you avoid flooding the syslog server. See Rate Limit Page, page 53-18.

Step 6 (Optional, but recommended) You can configure the **Platform > Device Admin > Server Access > NTP** policy to specify a network time protocol server for ASA devices. Using NTP ensures consistent date and time information for easy event correlation. Specify the same NTP server you use for the Security Manager server. If you use different servers, ensure the servers are synchronized. See NTP Page, page 52-21.

Configuring IPS Devices for Event Management

Before you can use Event Viewer to view events generated from an IPS device, you must configure the Allowed Hosts policy on the device to allow the Security Manager server access to the device. Because Security Manager also needs to be configured in the Allowed Hosts policy to allow configuration access, your IPS devices might already be configured correctly. You should also configure the network time protocol (NTP).

Configure the following policies for IPS devices in Device view to enable effective event management on those devices:

- **Platform > Device Admin > Device Access > Allowed Hosts**—(Required) Add the Security Manager server to the table. You can either identify the Security Manager server by its host IP address (for example, 10.100.10.10), or you can specify the network that it is on (for example, 10.100.10.0/24).

  If you are using other event management applications with the device, such as CS-MARS, ensure that you also add those servers to the policy.

  For more information about configuring the Allowed Hosts policy, see Identifying Allowed Hosts, page 36-7.
- **Platform > Device Admin > Server Access > NTP**—(Recommended) Configure the same NTP server that you use for the Security Manager server to ensure consistent date and time information for easy event correlation. If you use different servers, ensure the servers are synchronized. For more information, see Identifying an NTP Server, page 36-23.

Tip Although you can configure devices individually to specify the appropriate allowed hosts and NTP configuration, it is likely that more than one IPS device in your network would use the same configuration. Although this topic describes how to configure an individual device, you can also create shared versions of these policies and assign them to multiple devices. For more information about configuring and assigning shared policies, see Creating a New Shared Policy, page 5-54 and Modifying

Policy Assignments in Policy View, page 5-54.

Managing the Event Manager Service

The Event Manager service enables the use of the Event Viewer application. For Event Viewer to function, the service must be started. There are several tasks that you can perform to configure and manage the overall functioning of the service.

This section contains the following topics:

Starting, Stopping, and Configuring the Event Manager Service

The Event Manager service must be running for you to use Event Viewer or Report Manager.

When you install Security Manager, the Event Manager service is automatically enabled unless the server does not meet the minimum memory requirements that are documented in the *Installation Guide for Cisco Security Manager*. Although you can manually start the service on a system that does not meet the minimum memory requirements, you might find the performance to be dissatisfactory. The key factors are the number of devices managed and their rate of event generation.

Tip If you get a message that Event Viewer is unavailable when you select Launch > Event Viewer, but the **Enable Event Management** option is selected in the Tools > Security Manager Administration > Event Management page, try restarting the Event Manager Service. First, deselect the Enable option and click Save. Wait for the service to stop. Then, select the Enable option, click Save, and wait for the service to finish restarting. You can then try opening Event Viewer again.

The following procedure explains how to start, stop, and configure the Event Manager service.

Related Topics

- Monitoring Event Data Store Disk Space Usage, page 68-34

Step 1 In the main Security Manager window (not Event Viewer), select **Tools > Security Manager Administration** and select **Event Management** from the table of contents.

Step 2 Do one of the following:

- To enable, or start, the Event Manager service, select **Enable Event Management**.
- To disable, or stop, the Event Manager service, deselect **Enable Event Management**.

You can also change the other settings, such as the event data store location and maximum size, the syslog port to which devices should send events, and the pagination size (which determines the maximum number of events loaded into the event table). You can also configure an extended event storage location to augment your primary storage location. For detailed information about these settings, see Event Management Page, page 11-27.

Note Beginning with version 4.5, Security Manager enables you to forward syslogs to one local collector and two remote collectors. For more information, see Event Management Page, page 11-27.

Step 3 Click **Save** to save your changes.

If you changed the Enable Event Management option, you are prompted to confirm that you want to start or stop the Event Manager Service. If you click **Yes**, the service is started or stopped immediately, and you are shown a progress indicator and told when the change is completed. Wait until the status change is completed before continuing.

If you change other settings, with the exception of the pagination size, the Event Manager service must be briefly stopped and restarted. You are shown a progress indicator.

Monitoring the Event Manager Service

The Event Manager service processes incoming syslog messages and retrieves SDEE alerts from monitored IPS devices. The amount of data processed varies depending on network activity. There can be times when the events per second (EPS) generated in the network is higher than the service can handle, in which case the service goes into throttle mode, selectively dropping events.

You can monitor the status of the service to identify congestion and address problems that arise. The status of the service is shown in an icon in the lower right corner of the status bar in Event Viewer, as shown in Overview of Event Viewer, page 68-7. The Total EPS indicates the current events per second rate that the service is experiencing. The alert status icon color indicates the following:

- Green dot—There are no problems. All events are being processed normally.
- Yellow dot—There are some warnings, for example, low severity events are being dropped.
- Orange dot—There are more serious issues, for example, low and medium severity events are being dropped.
- Red dot—There is a critical situation, for example, high severity events are being dropped or there is a significant problem with the system, such as problems with the syslog port or with the event data store location.
- Disconnected network wire—The Event Manager service is disabled, either intentionally or due to some server problem; no events are being stored or retrieved. If this is not intentional, restart the Event Manager service as described in Starting, Stopping, and Configuring the Event Manager Service, page 68-30.

To view detailed information, click on the alert status icon. A bubble opens that shows summary statistics for the past five minutes, including the number of events received and dropped and event server alert messages, if any. Click the alert status icon again to close the bubble.

When the bubble is open, you can click the **Details** link in the bubble to view more detailed information. Clicking the Details link opens the Event Statistics Details dialog box, which shows the following information:

- **Last 5 Minutes Statistics:**
  - **Events Received**—The total number of syslog events Received and SDEE alerts retrieved in the past five minutes by the service.
  - **Events Dropped**—The total number of events or alerts that the service had to drop due to congestion. This number indicates drops from monitored devices only, so the number should be zero in normal circumstances. A non-zero number indicates that the service is in throttle mode; look for messages in the Event Server Alerts section.
  - **Events from Unmonitored Devices**—The number of syslog messages sent to the server that came from devices that are not selected for monitoring (as described in Selecting Devices to Monitor, page 68-34).

    Events from unmonitored devices are always dropped, but they do place a load on the service. The IP address of the last unmonitored device detected is shown; use the IP address to determine the source of the messages. You can then determine if the device should be added to the monitored devices list, or if you need to alter the device's configuration to remove the Security Manager server from its list of syslog servers.

    If the device that is sending messages is outside of your network, adjust the firewall configuration to prevent this syslog traffic from entering your network.
- **Status Information:**
  - **Total Events Per Second (EPS)**—The rate at which events are currently being processed. This measure does not include dropped events.
  - **Event Buffer Used**—The percentage of the shared event buffer that is currently being used to process events. The bar is color-coded to indicate the throttle level:

    Green—Not in throttle mode.

    Yellow—Low severity events are being dropped.

    Orange—Low and medium severity events are being dropped.

    Red—High severity events are being dropped.
- **Event Server Alerts**—These messages indicate specific status problems that you might need to address. Table 68-8 explains the messages that you might see with possible solutions.
- **Copy button**—Click the Copy button to copy the information to the clipboard. The copied information includes HTML markup. You can paste the information into an HTML file.

Table 68-8 Event Manager Status Messages

Alert Message	Alert Level	Possible Action
UDP port <514> could not be acquired, therefore syslog events cannot be collected.	High	Some external application might already be using the indicated port (the default syslog port is 514). You might need to stop that external application. You can use the netstat command to identify the PID of the process, for example, **netstat -ao | findstr 514**.

Table 68-8 Event Manager Status Messages (Continued)

Alert Message	Alert Level	Possible Action
The event data store location does not exist, therefore events cannot be stored.	High	The event data store location as configured in the Security Manager Administrative Settings does not exist or the Security Manager server does not have the required read/write permissions to the location. For more information about configuring the location, see Event Management Page, page 11-27.
Low severity events are being dropped.	Low	Either events are being received at a very high rate or the system is under a heavy load. To identify if a device is sending events too frequently, you can open the All Device Events view and switch to real-time mode, as described in Switching Between Real-Time and Historical Views, page 68-41. To identify if the server is under a heavy load, log into Windows on the server and use Task Manager or another tool to see if there is an application other than Security Manager that is taxing the system. If possible, disable or stop the application. If the problem occurs frequently, consider uninstalling the other application from the server.
Low and medium severity events are being dropped.	Medium	
All events are being dropped.	High	
Events from unknown devices are being received.	Low	Syslog events are being sent to the Security Manager server from devices that are not selected for monitoring as described in Selecting Devices to Monitor, page 68-34. These devices might not be supported device types for monitoring and they might not even be in the Security Manager inventory. The message varies based on the EPS rate for these devices. A low severity message indicates the EPS rate is between 500 and 5,000; a medium indicates an EPS rate between 5,000 and 10,000; a high indicates an EPS rate greater than 10,000. The **Events from Unmonitored Devices** statistic in the Last 5 Minutes Statistics shows the number of these events and the IP address of the last unsupported device. Either select the device for monitoring or change the syslog policy for the device to remove the address of the Security Manager server. You will need to repeat the process if more than one unmonitored device is sending messages.
Events from unknown devices are being received at a high rate.	Medium	
Events from unknown devices are being received at a very high rate.	High	

Selecting Devices to Monitor

All ASA and FWSM devices and security contexts, and IPS devices and virtual sensors, that are added to the Security Manager database are automatically selected for monitoring in Event Viewer.

Note To reliably report events from contexts in multiple-context mode, Cisco Event Viewer requires an IP address for the management interface of each context.

If you do not want to use Event Viewer with a device, you can deselect the device for monitoring. Note that if an ASA or FWSM device or security context is not configured to use the Security Manager server as a syslog server, you will not get events from the device or security context anyway, so you might not need to deselect an ASA or FWSM that you do not want to monitor.

Tip You cannot monitor Cisco IOS IPS devices in Event Viewer.

Related Topics

- Adding Devices to the Device Inventory, page 3-6
- Configuring ASA and FWSM Devices for Event Management, page 68-28
- Configuring IPS Devices for Event Management, page 68-29

Step 1 In Event Viewer, select **View > Manage Monitored Device** to open the Manage Monitored Devices dialog box.

The device list shows all devices in the Security Manager inventory to which you have view permissions. You cannot see any devices for which you have no permissions. Any selections you make are limited to the displayed devices. If you do not have permission to select or deselect any devices, the list is read-only and you cannot select devices for monitoring. For more information on access permissions, see Understanding Event Viewer Access Control, page 68-4.

Step 2 Ensure that only those devices whose events you want to monitor in Event Viewer are selected. Deselect any undesired devices.

You can change the selection status for all devices in a device group by selecting or deselecting the group.

Step 3 Click **OK**.

You might need to wait for the changes take effect in Event Viewer.

Monitoring Event Data Store Disk Space Usage

The Event Manager service uses a specified amount of disk space for the primary and extended event data stores. This ensures that the service does not overwhelm the server computer or the extended storage location. You configure the size of the primary and extended event data stores on the **Tools > Security Manager Administration > Event Management** page as described in Event Management Page, page 11-27.

For both the primary and extended locations, when the allocated space is 90% full, the oldest event data is deleted from storage to make room for new data. Data is copied from the primary store to the extended store, if you configure one, so in most cases events deleted from the primary storage continue to be available for querying from the extended storage location, until they are rotated out of the extended storage. (The timing of the copy from the primary to extended data store depends on a number of factors, including the events per second (EPS) rate, the relative size of the primary store to the extended store, and the percentage of the primary data that has already been copied to the extended store.)

You can monitor how much of the allocated space is currently being used, and the age of the oldest event, by selecting **View > Show Event Store Disk Usage** in Event Viewer. The information is displayed as a pie chart that shows the used and unused space in gigabytes (GB) for each location. There is also an indication of the oldest event currently stored in each location.

You can use this information to help you decide whether to increase or decrease the space allocated to each location.

Tip If you decrease the size of either location, and your new size is less than the amount of space currently being used, the oldest events are immediately deleted until your new target size is reached.

Archiving or Backing Up and Restoring the Event Data Store

The event data store is not included with the regular Security Manager database backup. If you want to archive or back up the event data store, whether the primary or extended location, you must do so separately. You can restore the backups if necessary.

This procedure explains the steps required for backup and restore for the event data store.

Tip When you disable the Event Manager service, events are not written to the data store, so you will miss any events generated during the backup or restore process.

Step 1 To back up the event data store:

a. Using the Security Manager client, select **Tools > Security Manager Administration**, and select **Event Management** from the table of contents.

b. Determine the name of the event data store folder. The folder is shown in the Event Data Store Location field; the default is *NMSROOT***MDC\eventing\database**, where NMSROOT is the installation directory (usually C:\Program Files\CSCOpx).

   If you are backing up the extended data store, the location is identified in the Extended Data Store Location field.

c. Deselect the Enable Event Management check box to stop the Event Manager service. Click **Save** to save your changes. You are prompted to verify that you want to stop the service; click **Yes** and wait until you are notified that the service has stopped.

d. Outside of Security Manager, make a copy of the *NMSROOT***MDC\eventing\config\collector.properties** file and the event data store folder. Place the copy on a separate server so that the backup is available in case of hardware failure.

   If you are also backing up the extended data store, make a copy of that folder as well.

e. In the Security Manager client's **Tools > Security Manager Administration > Event Management** page, select the **Enable Event Management** check box and click **Save**. You are prompted to verify that you want to start the service; click **Yes** and wait until you are notified that the service has started.

Step 2 To restore the event data store, use the same process you used to back up the data with the following exceptions:

- Instead of making a copy of the existing event data store, copy the backup into the event data store location. You can optionally delete the existing data before copying in the backup data. However, as long as you do not exceed the data store size limit, you can mix the backup and existing data. (The data store limit is configured in the **Tools > Security Manager Administration > Event Management** page.)

  Note Mixing old and new data works only if you are preserving the existing copy of collector.properties (that is, you are not restoring the file), and the new and old data are from the same server. You cannot merge the data store from two or more separate servers.

- Do not restore collector.properties unless you are recovering from a hardware failure or some other event that required you to reinstall Security Manager.

Using Event Viewer

Use Event Viewer to help troubleshoot network problems involving monitored devices. Using views and filtering, you can analyze problems to help identify the cause and possible remedies.

This section contains the following topics:

Using Event Views

When you view events in Event Viewer, you open a view. A *view* is a set of filters and other properties, including color rules, selected columns and their positions and widths, and the default time window, that let you define a subset of events. Views help to limit the scope of the events list so that you can more easily find what you are looking for.

This section contains the following topics:

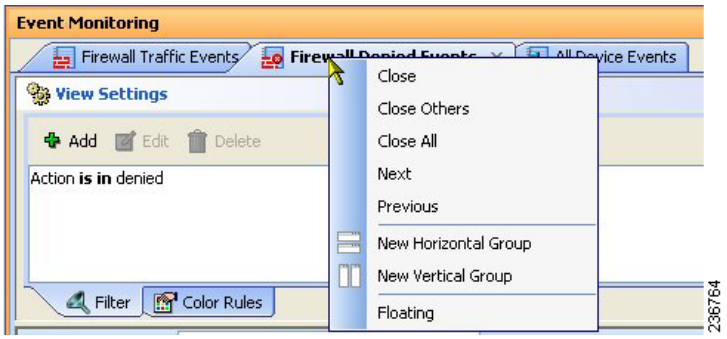
Opening Views

You can open up to four historical views and one real-time view in Event Viewer. When you open a view, Event Viewer uses the view settings and time range to retrieve events from the event data store and display them in the event table.

- To open a view so that it replaces the currently active open view, do one of the following in Event Viewer:
  - Double-click the view in the views list.
  - Right-click the view in the view list and select **Open**.
- To open a view in a new tab, do one of the following:
  - Select **File > Open View** from the menu bar. The Open a View dialog box opens, which is essentially the same as the view list. Select the view and click **OK**.
  - Right-click the view in the views list and select **Open In New Tab**.

Floating and Arranging Views

You can open up to four historical views and one real-time view at one time. When you have multiple views open, they are opened as tabbed windows in the right pane of the main Event Viewer window, in the most recently used area ("tabbed group") if there is more than one area. The commands to arrange the windows appear if you right-click the tab for the view window as shown in the following illustration.



You have many options for arranging view windows based on your requirements. For example, you might want to compare two views side-by-side, or remove a view from the main window without closing it.

You can use the following techniques to arrange the view windows to get the display that you desire:

- Floating a view—To remove a view from the main Event Viewer window without closing it, right-click the view tab and select **Floating**. The view is moved to its own window.

If you have already floated a view, you can select **Floating to** and choose one of the already-floated windows. The view becomes a new tab in that window.

- Docking a view—To move a floating view back to the main Event Viewer window, right-click the view tab and select **Docking**.
- Arranging views horizontally or vertically for side-to-side comparison—To create a vertical or horizontal arrangement of views to allow for easy comparison, without floating the views, right-click the view tab and select **New Horizontal Group** or **New Vertical Group**. These commands split the current tabbed group into the selected layout. You must have at least two views open to use these commands. If you have more than two open views, and you want all of them in separate windows, you need to use the command multiple times.
- Move views to different tabbed groups—If you have several open views, and you have arranged them into horizontal or vertical groups, you can move views among the groups by right-clicking the view tab and selecting **Move to Next Tab Group** or **Move to Previous Tab Group**. The commands appear only if views are arranged in a manner where such movement is possible:
- Change the orientation of groups—You can switch between horizontal and vertical layouts by right-clicking the view tab and selecting **Change Tab Groups Orientation**.

Customizing the Event Table Appearance

You can customize the appearance of predefined or custom views in the event table to meet your requirements. You can save these changes even in the predefined views.

You can do the following to customize the event table:

- Create column filters to limit the type of events listed. Use the down arrows in the column heading to define the filter as described in Creating Column-Based Filters, page 68-44.
- Create color rules to highlight events based on severity, as described in Configuring Color Rules for a View, page 68-39.
- Change which columns appear in the table by clicking the Column Selector icon to the right of the table heading row, as described in Columns in Event Table, page 68-18.
- Change the width of a column by clicking the right edge of the column heading and dragging it to the desired size.
- Change the order of the columns by clicking the column heading and dragging the column to the position you want.
- Sort the events list by a column by clicking the column heading. The column sorts based on a three-click cycle: ascending, descending, and default order (which is by event reception time).
- Reset the width of the View Selector and Event Monitoring window to their default values by selecting **View > Reset Layout**.
- Change whether the source and destination columns show IP addresses or host object names, as described in Switching Between Source/Destination IP Addresses and Host Object Names, page 68-39.

Related Topics:

- Creating Custom Views, page 68-40
- Saving Views, page 68-41

Switching Between Source/Destination IP Addresses and Host Object Names

You can view source and destination IP addresses or you can view the host object name of objects that match a source or destination IP address. By default, the Event Viewer shows host object names when available.

IP address to host name mapping is supported only for the source and destination of events. Also, the mapping applies to Host objects only; Event Viewer will not show an object name when the source or destination of an event matches a Network object, Group object, or Address Range object.

Please clarify the type and content of the object. E.g. is this feature for host type network/host objects only, that is, the single-value host version of the object? does it work for single-value group objects, or for network or range objects?

To switch between source/destination IP addresses and host object names, do the following:

- To see host objects names for any objects that match a source or destination IP address, select **View > Show Network Host Objects**. This option is selected by default.

Tip Hover over a host object name to view the IP address associated with that object.

Note An IP address to host object name cache is created when Event Viewer is launched. If you define new host objects, you must submit those changes to the database and then close and relaunch Event Viewer for those mappings to be used.

- To see IP addresses in the source and destination columns, deselect **View > Show Network Host Objects**.

Configuring Color Rules for a View

You can use color rules to color-code events shown in the event table based on the severity of the event. Color-coding can help you quickly identify the events that you most want to know about.

You can selectively enable and disable color rules by editing them. This allows you to turn them on and off without deleting them.

Tip You can configure color rules for both predefined and custom views. However, you cannot share color rules between views: all color rules are unique to a view. If you want to apply the same rules to multiple views, you must recreate the rules in each view.

To define and enable a color rule, follow these steps:

Step 1 Open the view in which you want to define the color rule (see Opening Views, page 68-37).

Step 2 Click the **Color Rules** tab in the View Settings pane (see Event Monitoring Window, page 68-14).

Step 3 Do any of the following:

- To add a new rule, click the **Add** button. In the Add Color Rule dialog box, configure the rule as follows:
  - Select **Enable** to make the rule active.
  - Select the severity level for which the rule applies from the **Severity** list.

  - Use the **Foreground** (which is the text color), **Background**, and **Font Type** (either Bold or Italics) controls to define how the severity should be presented in the table. The Preview Text area shows how your rule will look.
- To edit a rule, select it and click the **Edit** button.
- To delete a rule, select it and click the **Delete** button.

Creating Custom Views

A custom view is one in which you define the filters in the view settings. Using custom views, you can configure filter rules to pin-point specific areas for monitoring and analysis. Custom views are private and cannot be shared between users.

You basically have two options for creating custom views, creating a view from scratch or from an existing view:

- To create a custom view that has no predefined column filters, do one of the following:
  - Select **File > New View** from the menu bar.
  - Click the **New** button above the view list.

  Then, enter a name for the view and optionally a description of the view and click **OK**. The view is added to the My Views folder in the views list.
- To create a custom view based on an existing view, do one of the following:
  - With the desired base view open, click the down arrow on the Save button in the event table toolbar and select **Save As**, or select **File > Save As** from the menu bar.
  - Right-click the desired base view in the views list and select **Save As**.

  Then, enter a name for the view and optionally a description of the view and click **OK**. The view is added to the My Views folder in the views list. The new view has the same filters as the base view.

Note View names can be up to 128 characters and contain alphanumeric characters, spaces, hyphens (-), underscore characters (_), plus signs (+), periods, and ampersands (&). The description can be up to 1024 characters.

After you create the new view, you can customize it the same way that you can an existing view:

- Define filters in the view settings. See Creating Column-Based Filters, page 68-44.
- Define color rules in the view settings. See Configuring Color Rules for a View, page 68-39.
- Select the columns to display in the event table. See Columns in Event Table, page 68-18.
- Customize the event table appearance. See Customizing the Event Table Appearance, page 68-38.

Related Topics

- Views and Filters, page 68-3
- Event Table Toolbar, page 68-16
- Editing a Custom View Name or Description, page 68-41
- Deleting Custom Views, page 68-42

Editing a Custom View Name or Description

To change the name of a custom view, or the custom view's description, do one of the following:

- Select the custom view in the view list and click the **Edit** button above the list.
- Right-click the custom view in the view list and select **Edit**.

Then, make the desired changes to the custom view name or description and click **OK**.

Note View names can be up to 128 characters and contain alphanumeric characters, spaces, hyphens (-), underscore characters (_), plus signs (+), periods, and ampersands (&). The description can be up to 1024 characters.

You cannot change the name or description of a predefined view.

Switching Between Real-Time and Historical Views

You can update the events table for any view using either real-time or historical time periods. A real-time view shows events as they are received, whereas an historical view shows a static list of events that is not updated until you click the **Start** button in the event table toolbar.

To switch between real-time and historical time periods in an open view, do the following:

- To see events in real-time, select **View > Mode > Real Time**, or click the Time Selector control in the event table toolbar and select **Real Time**. For help in locating the control on the toolbar, see Event Table Toolbar, page 68-16.
- To see events in an historical period, select the desired time frame from the **View > Mode** menu or from the Time Selector control on the event table toolbar. All options other than Real Time are historical views. For more information, see Selecting the Time Range for Events, page 68-42.

Saving Views

If you edit the settings for a view, you must save it to make those changes permanent. Saving a view saves changes to filters (for custom views only), table preferences such as selected columns, column width, and sort order, the time range, and color rules. If you make filter changes to a predefined view, you must use Save As to create a new custom view.

- To save changes to a view, do one of the following in Event Viewer:
  - Select **File > Save** from the menu bar.
  - Click the **Save** button in the event table toolbar.

  You are asked to confirm that you want to save your changes.
- To save your changes as a new custom view, do one of the following to open the Save View As dialog box:
  - Select **File > Save As** from the menu bar.
  - Click the down arrow on the Save button in the event table toolbar and select **Save As**.
  - Right-click the view in the views list and select **Save As**.

  Then, enter a name for the view and optionally a description of the view and click **OK**. The view is added to the My Views folder in the views list.

Note View names can be up to 128 characters and contain alphanumeric characters, spaces, hyphens (-), underscore characters (_), plus signs (+), periods, and ampersands (&). The description can be up to 1024 characters.

Deleting Custom Views

You can delete custom views, but you cannot delete predefined views. To delete a custom view, do one of the following:

- Select it in the view list and click the **Delete** (trash can) button above the list.
- Right-click it in the view list and select **Delete**.

You are asked to confirm your deletion.

Filtering and Querying Events

There are many options for filtering the events that appear in the event table. You can reduce the list of events by selecting the appropriate time range, by filtering on elements in specific columns, or even by searching on a text string.

This section contains the following topics:

Selecting the Time Range for Events

Use the Time Selector control in the event table toolbar, or the equivalent **View > Mode** command, to select the time range for displaying events. The event table lists only those events that occur within the selected time range. For help in locating the Time Selector control on the toolbar, see Event Table Toolbar, page 68-16.

Tip For historical views, the time is based on server time, not the time configured on your workstation.

When you change the time range, the table reloads to show events in the selected range. For historical views, you can refresh the events list by clicking **Start** or by doing the other actions described in Refreshing the Event Table, page 68-43.

The following are your options for the time range:

- To view events from the present time into the past, select one of the following time periods: **last 10 minutes**, **last 1 hour**, **last 12 hours**, **last 1 day**, or **last 1 week**.
- To view events from today or yesterday, select **today** or **yesterday**, as desired.

- To view events from a specific day, select **is on** and then select the date from the displayed calendar.
- To view events from a specific date and time range, select **is between** and select the first and last days and times from the displayed calendars.
- To view real-time events, select Real Time.

Using the Time Slider with Filtering

You can use the vertical slider control in the time slider to change the start time for the events shown in the event table. This is particularly useful when you want to locate events and you know the approximate time they occurred.

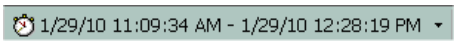
For details on the operation of the time slider, see Time Slider, page 68-25.

To use the time slider to aid filtering, follow these steps:

Step 1 Open an historical view, or use the Time Selector in the toolbar, or the **View > Mode** command, to select an appropriate time range, such as Last 10 Minutes. For more information, see Selecting the Time Range for Events, page 68-42.

Step 2 Move the vertical slider to the approximate time of the events you want to examine.

The event table is reloaded to display events on or before the time you specified with the vertical slider. This time range is shaded in the time slider, and the length of time selected is based on the length of time selected in the Time Selector (for example, 10 minutes for a Last 10 Minute view, or the same length of time selected for an "is between" view). The time range is noted in the Time Selector control, for example:



Step 3 To locate the events, you can now do any of the following:

- Apply custom column filters. See Creating Column-Based Filters, page 68-44.
- Use the quick filter to search on a text string. See Filtering on a Text String, page 68-47.
- Scroll or page through the event table.
- Use the time slider paging controls to reset the time range forward or back. For more information, see Time Slider, page 68-25.

Note The distance moved forward or back when paging in the time slider depends either on the mode (time range) that is set or the number of events the event table can hold. The position of the vertical slider denotes the most recent event loaded in the event table.

Refreshing the Event Table

When you are using an historical mode, such as "last 10 minutes," the latest events displayed correspond to the time you selected the time range or opened the view. Similarly, if you are in real-time mode and have clicked Stop, the event table does not include events that arrived after you stopped the event stream.

To refresh the events listed in the event table, so that they are current with your selected time range, do any of the following:

- Click **Start** in the toolbar, or select **View > Start**. The table is refreshed based on your currently selected time range. For real-time views, the event stream restarts.
- Select a different time range using the Time Selector in the toolbar or the **View > Mode** command.
- Select a different time slice using the vertical slider or the pagination controls in the time slider below the event table. For more information on using these controls, see Time Slider, page 68-25.

Creating Column-Based Filters

You can filter the event table in Event Viewer based on the contents of specific columns. Column filters are the type of filter contained in the view settings; they define the basic content of the view. Whenever you apply a column filter, the view settings for the view are updated to include the newly selected filter: you must save the view before closing it if you want the new filter to become a permanent part of the view's definition.

There are many ways in which to define a column filter:

- In the View Settings pane, click the **Add** button. You are first prompted to select the column on which to base the filter. When you click **OK**, you are prompted to create the filter.
- In the View Settings pane, select a filter and click the **Edit** button to change it.
- In the event table, click the down arrow button in the heading of a column and select any of the following from the drop-down list:
  - A specific entry. The drop-down list contains all values currently displayed in the events listed in the table.
  - (All). Select (All) to remove a filter from this column. The event table is updated to show the events that meet your other filter criteria.
  - (Custom). Select (Custom) to create a filter that might have multiple values, negative values, or be based on data not currently contained in the column in the current event table. Selecting (Custom) is essentially the same as creating a filter directly in the View Settings pane.
- In the event table, you can right-click a value and select **Filter This Value**. This action has the same effect as selecting the value from the drop-down list for the column.

  You can alternatively select **Filter Not This Value** to create a filter that excludes a value,
- In the event table, you can right-click a value and select **Create Filter from Event**. You are prompted to select the specific columns to include; the column on which you right-clicked is initially selected, but you can deselect it.

The following procedure explains how to build a custom column-based filter, one in which you are not simply selecting a value from the column's drop-down list.

Tips

- Column filters are cumulative: for an event to appear in the event table for a view, the event must meet all column filter criteria. You cannot create a set of OR'ed column filters.
- Some columns allow you to select network/host or service policy objects to define the filter criteria. Selecting policy objects can simplify your filters. However, for a policy object to be selectable in a filter, the object must be committed to the database. If you create a new object for filtering purposes, ensure that you submit your changes in Configuration Manager (and if using Workflow mode with an approver, get the changes approved) before attempting to create the filter in Event Viewer.

  When using policy objects, the filtering recognizes whether a device-level override is defined for the object. For example, if you use a network/host object that contains 10.10.10.10, and Device A has an override to change the address to 10.10.10.12, events from Device A appear in the list only if the

event matches 10.10.10.12. For devices that do not have overrides, the events must match 10.10.10.10. Furthermore, if Device A has an event that matches 10.10.10.10, that event is not listed because it does not match the device-level override. Thus, using policy objects can provide results that vary by device and therefore match more closely to your policy definitions.

If your organization is using ACS to control user access, you must have the appropriate View Object privileges for network/host, network/host-IPv6, and service objects to use them in filters.

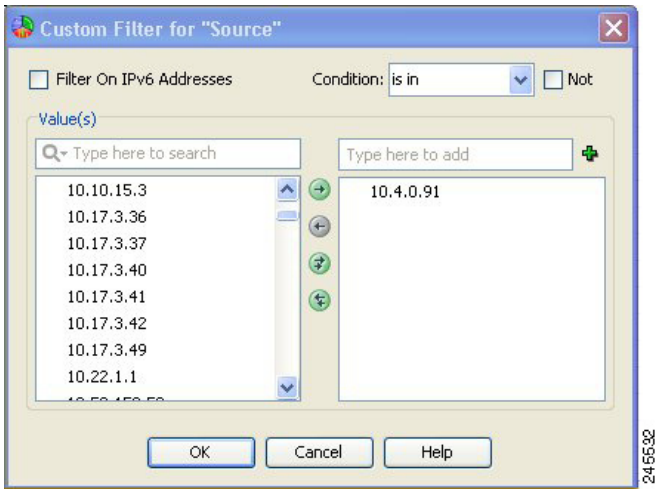
- You can filter on the contents of most but not all columns. If a column does not have a down arrow, you cannot filter on it. For example, you cannot filter on Description, Event Name, Generation Time, or Receive Time.
- The filter icon (a funnel) appears in the heading of a filtered column.
- For a description of the available columns, see Columns in Event Table, page 68-18.

Step 1 Do one of the following:

- In the View Settings pane, click the **Add** button. The Add Custom Filter to a Column dialog box opens. Select the column on which to base the filter and click **OK**.
- In the View Settings pane, select a filter you want to change and click the **Edit** button.
- From the drop-down list for a column, select **(Custom)**.
- Right-click any cell in the desired column and select **Custom Filter**.

The Custom Filter dialog box opens for the selected column.

Step 2 In the Custom Filter dialog box, select the desired values. The following illustration shows a typical example of this dialog box, for the Source column.



Following is a description of the controls you might find in the Custom Filter dialog box. Not all controls appear for every column:

- **Available and Selected Items lists**—In most cases, to select an item you highlight it in the left list, which contains the available values, and click the right arrow to move it to the list of selected values. You can select multiple values. The right list defines the filtered values.

The items listed in the available values column are determined by the values currently present in the events listed in the events table. For address and service fields, the list also includes policy objects. If there are a lot of available values, you can search for the desired value by typing into the edit box above the list; the list is filtered as you type. Click the down arrow next to the Q to change how your search string is evaluated for matches.

You can also select, or deselect, values using the following techniques:

- Type the item into the edit box above the selected values list and click the + button. This technique is useful if there is a large number of available values, or if you want to filter on a value that is not present in the current events list.
- Double-click an item in either list to move it to the other list.
- Click the double-arrow buttons to move all items, regardless of your selection.

Note In a limited number of cases, the Custom Filter dialog box contains a single list. For example, the dialog boxes for the Event Type ID and Device columns contain single selectors. In these cases, make your selection using the check boxes next to the items; selecting a folder selects all items in the folder.

- **Filter on IPv6 Addresses**—For columns that contain addresses, use this option to toggle between listing IPv4 and IPv6 addresses and network/host objects in the available values column. You can filter on either IPv4 addresses or IPv6 addresses, but not both, in a single view.
- **Condition, Not**—Defines the condition applied to the selected items, typically "is in."

  To create a negative condition, so that selected values define the events to not include in the events table, select the Not option.

Step 3 Click **OK**.

The view settings are updated to include the new filter, and the events table is updated to show only those events that satisfy all filters.

Filtering Based on a Specific Event's Values

You can base a new filter on information contained within an event, or a single cell within an event, by right-clicking and choosing a filter command. When you filter using these commands, a column filter is added to the view settings. You can do the following:

- To create a filter based on multiple values in the selected event, select **Create Filter from Event**, then select from the dialog box the values on which to filter. The dialog box lists only those columns that are displayed in the table; the current values are shown in parentheses. For an explanation of the columns, see Columns in Event Table, page 68-18.
- To filter on only the value in the cell on which you right-click, select **Filter This Value**.
- To filter to exclude the value in the cell on which you right-click, select **Filter Not this Value**. All events that do not contain the selected value in this column, including all empty cells, are shown in the table.
- To filter on the flow of the selected event, based on source, source service, destination, and destination service, select **Filter This Flow**.

Filtering on a Text String

Use the quick filter to search for text strings in events. As you type a search keyword, the events table automatically excludes non-matching events as you type. You can search on all columns (the default), or you can select a specific column in which to search.

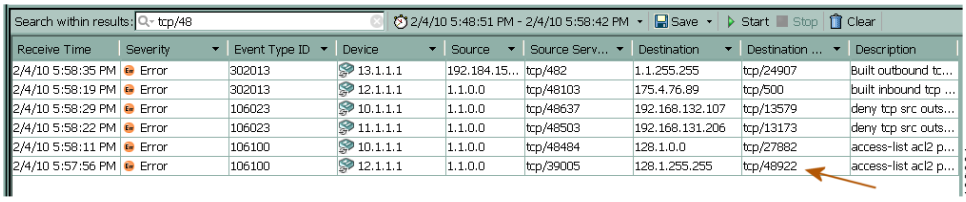
The following illustration shows the quick filter, which is on the right of the event table toolbar (see Event Table Toolbar, page 68-16).

To perform a search, simply type in the search string. To change how the string is evaluated, click the down arrow next to the Q (magnifying glass) in the left of the edit box. You can limit the search scope using these controls:

- Column name—Select a specific column to search only within that column. The list includes all columns currently displayed in the table. The default is to search all columns.
- Case sensitivity—Select **Case sensitive** or **Case insensitive** to control whether capitalization is considered when selecting matches. The default is case insensitive.
- Wild card usage—Select **Use Wild Cards** to have the following characters evaluated as wild cards:
  - * (asterisk)—matches 0 or more characters.
  - ? (question mark)—matches one character.
- Match method—Select one of the following to determine the location within a cell that the search string should reside:
  - Match from start—The string must be at the beginning of the cell.
  - Match exactly—The cell must contain all and only the search string.
  - Match anywhere—The string can appear anywhere within the cell.

To remove the search string, simply delete it from the quick filter edit box.

For example, if you want to find events that relate to ports that start with tcp/48, type **tcp/48** into the quick filter. In the following illustration, note that all but six events are filtered out of the table. In this example, the search string is found in the Source Service column for the first five events, but in the Destination Service column for the sixth event. If you know beforehand that you are interested in destination services only, you could select **Destination Service** from the quick filter drop-down list and the table would show the last event only.



Clearing Filters

When you apply filters to the event table, non-matching events are not displayed. You might find that you need to see the non-matching events. You can either open a different view that applies different (or no) filters, or you can clear filters from the current view.

When clearing filters, the filter definition is removed from the view settings, but the change is not permanent until you click **Save**. Thus, you can remove filters temporarily without redefining the view settings.

You can clear filters one at a time or clear all filters:

- To clear a single filter, so any of the following:
  - Select the filter in the View Settings pane and click **Delete**.
  - Select **(All)** from the drop-down list of a filtered column.
  - Right-click in the filtered column and select **Clear This Filter**.
- To clear all filters, right click in the events table and select **Clear all filters**.

Performing Operations on Specific Events

You can operate upon a single event in the event table in a variety of ways, which include the following:

- **Right-click**—Right-clicking a single event in the event table opens a context menu with commands that you can use on the event. For more information about what you can do from the right-click menu, see the following topics:
  - Event Context (Right-Click) Menu, page 68-49
  - Examining Details of a Single Event, page 68-51
  - Copying Event Records, page 68-52
  - Saving Events to a File, page 68-52
  - Filtering Based on a Specific Event's Values, page 68-46

  Note You can hover your mouse over a valid IPv4 address in Event Viewer to launch the IP Intelligence tool for that IP address. The IP Intelligence tool provides various pieces of information about an IPv4 address, such as the fully qualified domain name (FQDN), geographic location information, and WHOIS information. For more information on the IP Intelligence tool, see IP Intelligence, page 71-33.

- **Select an event**—When you click a single event in the event table it is highlighted and the Event Details pane displays details for that particular event. Hold the **Ctrl** key to select additional events, or hold the **Shift** key to select a range of events.
- **Double-click an event**—Double-clicking a single event in the event table opens the Event Details dialog box, which shows the event information in an easier-to-read format. From the Event Details dialog box, you can print the displayed details or copy some, or all, of the details to the clipboard for pasting into another program. You can use the Next and Previous buttons to scroll through the events listed in the event table. For information on the meaning of the attributes, see Columns in Event Table, page 68-18.

  Alternatively, you can right-click on an event and select **Show All Details** to open the Event Details dialog box.

Event Context (Right-Click) Menu

When you right-click an event in the Event Table, a context menu appears that provides commands that you can use with the selected event. The specific list of available commands depends on the type of event and also the specific cell on which you right-click. The following table explains all of the available commands.

Note In addition to the right-click options listed below, you can also hover your mouse over a valid IPv4 address in Event Viewer to launch the IP Intelligence tool for that IP address. The IP Intelligence tool provides various pieces of information about an IPv4 address, such as the fully qualified domain name (FQDN), geographic location information, and WHOIS information. For more information on the IP Intelligence tool, see IP Intelligence, page 71-33.

Table 68-9 Event Context Menu

Command	Description
Clear This Filter	Removes the filter defined for this column. The command is available only if you right-click on a cell that is in a filtered column. The filter is removed from the view settings. You must save the view to make your change permanent.
Clear All Filters	Removes all filters from the view settings. This command is available only if there is at least one column filter. You must save the view to make your change permanent.
Filter This Value Filter Not This Value	Creates a column filter based on the value in the cell that you right click. You can create either a positive or negative filter based on the value. The view settings are updated with the new filter and replace any existing filter for this column. You must save the view to make your change permanent.
Create Filter from Event	Creates a set of column filters based on the values in the selected event. You are prompted to select the specific columns to include; the column on which you right-clicked is initially selected, but you can deselect it. The view settings are updated with the new filters and any existing column filters for the selected columns are replaced. You must save the view to make your changes permanent.
Custom Filter	Creates a custom column filter, as described in Creating Column-Based Filters, page 68-44. The view settings are updated with the new filter and any existing filters for the selected columns are replaced. You must save the view to make your changes permanent.
Filter This Flow	Creates a set of column-based filters that present the events related to a specific traffic flow. Filtered columns are source and source service and destination and destination service. The view settings are updated with the new filter and any existing filters for the selected columns are replaced. You must save the view to make your changes permanent.

Table 68-9 Event Context Menu (Continued)

Command	Description
Show IPLogs	Opens the IP log for an IPS Alert event using an external packet analyzer tool. You must have a packet analyzer installed and associated with *.pcap file extension.
Show All Details	Opens the Event Details dialog box for the event, which shows all event information in an easier-to-read format. You can also print the details or copy them to the clipboard. The details are the same as those shown in the Event Details pane below the event table.
Copy commands	You can use the following commands to copy event data to the clipboard. You can then paste the data into a spreadsheet or other program for your use. For more information, see Copying Event Records, page 68-52. • **Copy Cell**—Copies the contents of the cell you right-click to the clipboard. • **Copy Selected Events**—Copies the contents of all selected (high-lighted) events to the clipboard. • **Copy All Events**—Copies the contents of all listed events to the clipboard. This command is useful only if you have filtered the event table to a manageable number of events.
Save Selected Events as HTML Save All Events as HTML Save Selected Events as CSV Save All Events as CSV	Saves either all events listed in the event table, or all selected (high-lighted) events, to an HTML or comma-separate values (CSV) file on your workstation. You are prompted to select the folder and enter the file name for the export file. For more information, see Saving Events to a File, page 68-52.
Go To Policy	Finds the policy that generated this event in the device's policy configuration in Configuration Manager. This command is available only for events where a binoculars icon appears in the Event Name cell. For detailed information, see Looking Up a Security Manager Policy from Event Viewer, page 68-53.
Packet Capture	Opens the packet capture tool, where you can define criteria for capturing packets on the device.
Ping and TraceRoute	Opens the Ping, TraceRoute, and NS Lookup tool, where you can use these applications with the device from which the event was sent. For detailed information, see Analyzing Connectivity Issues Using the Ping, Trace Route, or NS Lookup Tools, page 71-25

Table 68-9 Event Context Menu (Continued)

Command	Description
Tune Signature	Opens the IPS Signature Quick Tune dialog box where you can enable or disable the signature associated with the selected event, and modify the Base Risk Rating of the signature that is assigned to the device or shared policy. To tune a signature you must create or open a ticket. For more information see Working with Activities/Tickets, page 4-7. The Base Risk Rating value of the signature is calculated by multiplying the fidelity rating and the severity factor and dividing them by 100 (Fidelity Rating x Severity Factor /100). This value is read only; you cannot directly change it. To change the Base Risk Rating, you must alter the Severity and Fidelity values. • Severity: The severity level that the signature will report: High, Medium, Low, or Informational, where, – High = 100 – Medium = 75 – Low = 50 – Informational = 25 • Fidelity: The Fidelity Rating, or Signature Fidelity Rating (SFR), identifies the weight associated with how well this signature might perform in the absence of specific knowledge of the target. This rating can be any number from 0 to 100, with 100 indicating the most confidence in the signature. After you enable or disable the signature or modify the Base Risk Rating you must redeploy the configuration to the device, using Configuration Manager, for the change to take effect on the device. Note that such changes will affect only real time events and not the historical events. For information about deploying configuration, see Chapter 8, "Managing Deployment".

IPS Signature Quick Tune Dialog Box

Use the IPS Signature Quick Tune dialog box to enable or disable the signature associated with the selected event, and modify the Base Risk Rating of the signature that is assigned to the device or shared policy.

Navigation Path

In Event Viewer, right-click a row (an event) and click **Tune Signature**. For more information, see Event Context (Right-Click) Menu, page 68-49.

Examining Details of a Single Event

Each event contains a lot of specific information in many separate fields. Typically, you display a subset of these fields in the event table. When you want to see the complete details of an event, you can use either of the following:

- **Event Details pane**—Select the event and open the Event Details pane below the event table. You can open the pane by clicking anywhere in the "Event Details" title row, or you can select **View > Show Event Details** from the menu. The Event Details pane organizes the information in tabs. For more information about this pane, see Event Details Pane, page 68-26.
- **Event Details dialog box**—You can open this dialog box by double-clicking the event, or by right-clicking the event and selecting **Show All Details**. The information is presented as a flat list and shows the information that would be shown on the Details tab in the Event Details pane. For information on the meaning of the attributes, see Columns in Event Table, page 68-18.

  The Event Details dialog box includes the following controls:

  - Print button—Click this button to print the information. You are prompted to select a printer.
  - Copy button—Click the down arrow on this button and select **All Rows** or **Selected Rows**. The information is copied to the clipboard, and you can paste it into another application. Note that the Selected Rows command works only if you select at least one row in the table.
- Next, Previous buttons—Click these buttons to scroll through the events currently displayed in the event table. Next moves up and Previous moves down in the table.

Copying Event Records

You can copy single events, multiple events, all events, or even the contents of a single cell to the clipboard. You can then paste the information into another application, such as a spreadsheet or an e-mail message.

You can do the following from the event table:

- **Copy selected events**—To copy one or more selected events, right-click in the event table and select **Copy Selected Events**. The event you right-click does not matter, the copied events are those that are selected (highlighted) in the table.

  Click an event to select it. Hold **Ctrl** key to select additional events, or hold the **Shift** key to select a range of events.
- **Copy the contents of a single cell**—To copy the contents of a single cell in one event, right-click the cell and select **Copy Cell**. You cannot copy cell contents if there is more than one event selected in the table.
- **Copy all events**—To copy all the events shown in the event table, right-click anywhere in the table and select **Copy All Events**.

Saving Events to a File

Rather than copying events to the clipboard and pasting them into another application, you can directly save events to an HTML or comma-separated values (CSV) file. HTML files are useful for viewing information, whereas you can open a CSV file in a spreadsheet application for further analysis and report generation.

When saving event data, you are prompted to select a folder and enter a file name.

You can do the following from the event table:

- **Save selected events**—To save one or more selected events, right-click in the event table and select either **Save Selected Events as HTML** or **Save Selected Events as CSV**. The event you right-click does not matter, the saved events are those that are selected (highlighted) in the table.

  Click an event to select it. Hold **Ctrl** key to select additional events, or hold the **Shift** key to select a range of events.

- **Save all events**—To save all the events shown in the event table, right-click anywhere in the table and select either **Save All Events as HTML** or **Save All Events as CSV**.

Looking Up a Security Manager Policy from Event Viewer

In Event Viewer, if an event was generated from an IPS signature policy, or from certain actions related to explicit access rules (such as denied access), you can quickly locate the related signature or access rule from the event itself.

The main reason you would want to perform policy lookup is to adjust a policy based on the events that it is generating. For example, an access rule might be dropping traffic that you actually want to allow. Because you are looking at the event, you know there is a policy that is causing the event, so with a few clicks, you can get from that event to the policy that you need to reconfigure.

You can look up policies from the following types of events:

- Firewall events—You can look up policies for the following syslog messages:
  - 106023—Denied IP packet.
  - 106100—Permit/Denied by ACL.
  - 302013—Built TCP (started a TCP session).
  - 302015—Built UDP (started a UDP session).
- IPS alert events—All IPS events that have valid signature and sub-signature identifiers.

Tips and Caveats

- You cannot look up firewall policies for events that contain IPv6 addresses. You can look up IPS policies for IPv6 addresses, however.
- When a policy that is based on IP address alone and not on a user name triggers an event, the device looks up the IP address in the Active Directory and if a user name is associated with that IP address, the user name is added to the syslog. Hence, even if a policy does not contain a user name, the resulting syslog might contain it. Policies cannot be created with a destination user and, as a result, this field will not be used during policy lookup.
- If an event is generated for a policy that is configured based on source/destination FQDN, the resulting syslog will not contain the FQDN because of a device defect. In such cases, policy lookup will not work.
- If an event is generated for a policy that is based on user groups, the syslog will contain the specific user name that triggered the event and not the user group. In such cases, policy lookup will not work.
- Hash codes are required for successful policy lookups from syslog 106023 and 106100 events. These hash codes are available only if you deployed the configuration using Security Manager. If policy lookup fails, try deploying the configuration (either to the device or to a file), then try the policy lookup again.
- If you had applied a filter to the device's policy table, and the rule or signature that generated an event is filtered from the current view, Security Manager cannot highlight it. Clear the filter and try again.
- If the event is caused by an implicit rule, such as the implicit **deny any** at the end of access rules, Security Manager cannot highlight the rule. It is considered good practice to create an explicit deny any rule at the end of access lists.
- The target policy is always found in Device view, even if the device uses a shared policy. Device view is opened if necessary to highlight the policy.

- For IPS signatures, you might not be able to edit the signature if it is a default signature.
- For access rules, the selected rule is the best match for the event. It is possible that more than one rule would generate the same event if you have overlapping or redundant rules. In these cases, editing the selected rule might not completely eliminate the event, because a subsequent rule might perform the same action. Use the access rules tools to analyze and combine overlapping rules.
- For access rules, multiple rules might permit a packet during session creation, but the first rule only is highlighted.
- If your organization is using ACS to control access, you must have View Device privileges to the device, and also View privileges to the firewall or IPS policy, to perform policy lookup. If you do not have all permissions, you will get an "Unable to Find Matching Rule" error if you try to look up a matching rule.

Step 1 Right-click the event in Event Viewer and select **Go To Policy**.

Tip You can identify whether you can look up policies from the event by looking at the Event Name cell in the table. If there is a binoculars icon before the event name, policy lookup is available. Also, if the Go To Policy command is greyed out, you cannot look up policies for that type of event.

Step 2 Security Manager finds the related access rule or IPS signature for the device and highlights it in the policy table. From here, you can edit the policy to view or change it; for detailed instructions, see Configuring Access Rules, page 16-7 and Configuring Signatures, page 39-4.

Your changes do not take effect until you submit and deploy the updated configurations.

Looking Up Events for a Security Manager Policy

You can look up events in Event Viewer that relate to specific firewall access rules or IPS signatures. You can also look up events that relate to specific devices or site-to-site tunnels in Health and Performance Monitor.

When Event Viewer receives events, they are parsed, "sessionized," written to an event buffer, and then written to the database. Sessionizing takes two forms: with a session-oriented protocol, such as TCP, the session encompasses the initial handshake to the connection tear-down; with a sessionless protocol, such as UDP, the session start and end times are based more on first and last packets tracked within a restricted time period—packets that fall outside of the time period are considered parts of other sessions.

Because there is a difference between newly-received and fully processed data, you can look up either real-time or historical events:

- **Real-time**—Because sessionization takes time, keeping an event in cache for up to two minutes, you can use the real-time event query to view events right after parsing, providing access to the most current data received.
- **Historical**—Historical event reports help you identify trends over longer periods of time than is possible with real-time monitoring. For historical events, the Result Format is the All Matching Events option, and the Filter By Time value is set to the previous 10 minutes.

The following topics explain event lookup in more detail:

- Viewing Events for an Access Rule, page 68-55

- Viewing Events for an IPS Signature, page 68-56
- Viewing Events for HPM Devices and Site-to-Site VPNs, page 68-57

Viewing Events for an Access Rule

From the **Firewall > Access Rules** policy in Security Manager, you can select an access rule and view related event information in Event Viewer. You can view real-time or historical events matching the rule. You can view events for ASA (including ASA-SM) and FWSM devices.

Firewall access rules are presented in the form of an ordered list or table. When deployed, this policy becomes an access-control list (ACL), with each entry in the list known as an access-control entry (ACE). (For more detailed information, see Understanding Access Rules, page 16-1.)

When deciding whether to forward or drop a packet, a device tests the packet against each access rule in the ordered listed. If you enable logging for an access rule, the results of the test are recording according to your per-rule log settings. Some devices, such as ASA, generate log entries for denied access even if you do not configure logging explicitly. For information on creating access rules, including logging options, see Configuring Access Rules, page 16-7.

If logging is enabled for the rule (in the Advanced and Edit Options Dialog Boxes, page 16-17), the device sends syslog messages to Event Viewer to record the logged events. This query includes the access-rule parameters, including available keyword information. Reported events do not include connection set-up and tear-down.

To view rule-related events, use the following right-click commands:

- **Show Events > Realtime**—To view real-time query results in Event Viewer for events matching this rule. You can change the query criteria in the Event Monitoring window at any time, applying new parameters to alter the real-time results.
- **Show Events > Historical**—To view historical query results in Event Viewer for events matching this rule. You can change the query criteria in the Event Monitoring window at any time, applying new parameters to alter the historical results.

Security Manager provides the following information to Event Viewer as criteria for access-rule event queries:

- Device details—General information about the device, such as host name, domain name, management IP address, and display name.
- Source addresses—Source addresses of hosts and the network/host objects expanded to display the networks or collections of IP addresses.
- Destination addresses—Destination addresses of hosts and the network/host objects expanded to display the networks or collections of IP addresses.
- Service—Protocol and port information.
- Event Type—“Built/teardown/permitted IP connection” for permit rules and “Deny packet due to security policy” for deny rules.

Notes:

- You can query on only one access rule at a time.
- When NAT or PAT is configured on a security device, the source and destination addresses are mapped to pre-translation and post-translation addresses, respectively, and the translated addresses are used when Security Manager sends a query to Event Viewer. For inbound access rules, the destination address is considered the pre-translation address, and for outbound access rules, the source address is considered the post-translation address.

- Filtering with multiple services (like UDP, TCP, and ICMP) might not give accurate results. To work around this problem, you can remove some of the filters after Event Viewer is launched.
- Filtering based on ICMP sub types is not supported. For example, if an ACE has 'ICMP Echo' in service, the filter is applied only for the protocol (ICMP), but not for type column (Echo) in Event Viewer.
- Service ports with 'eq', 'neq', 'gt', and 'lt' are not supported in cross launch to Event Viewer.

Related Topics

- Access Rules Page, page 16-10
- Looking Up Events for a Security Manager Policy, page 68-54
- Viewing Events for an IPS Signature, page 68-56
- Viewing Events for HPM Devices and Site-to-Site VPNs, page 68-57

Viewing Events for an IPS Signature

When an IPS device detects and reports a network intrusion by comparing incoming traffic to a configured signature, a syslog message is generated on the device. If the device is monitored by Security Manager, an incident is generated in Event Viewer after the log associated with the signature is obtained from the device. Looking up the events associated with a specific signature lets you quickly identify attacks and tune your device configuration to minimize or prevent intrusions.

To view reported network intrusion events in Event Viewer, you can select one or more entries in the Signatures policy for a device in Security Manager and navigate to the Event Viewer to view real-time and historical events.

Related Topics

- Looking Up Events for a Security Manager Policy, page 68-54
- Viewing Events for an Access Rule, page 68-55
- Viewing Events for HPM Devices and Site-to-Site VPNs, page 68-57

Step 1 (Device view) With an IPS device selected, select **IPS > Signatures > Signatures** to display the Signatures Page, page 39-4.

Step 2 Right-click the desired entry in the signatures table, or select multiple entries before right-clicking one of them, and choose one of the following commands from the **Show Events** menu:

- **Realtime**—To view real-time query results in Event Viewer for events matching this signature. Use this option to view raw events as they stream to Event Viewer.

  You can change the query criteria in the Event Monitoring window at any time, applying new parameters to alter the real-time results.
- **Historical**—To view historical query results in Event Viewer for events matching this signature.

  You can change the query criteria in the Event Monitoring window at any time, applying new parameters to alter the results.

Tips:

- If a signature is disabled, you are warned and asked if you want to proceed to event lookup.

- Events of type Packet Data and Context Data are not displayed in the query results because these events are not triggered by signature rules.

Viewing Events for HPM Devices and Site-to-Site VPNs

From Health and Performance Monitor, you can quickly access events for a monitored device or for site-to-site VPNs that have had a tunnel up/down event.

To view events for a monitored device, select a device from the All Devices, Firewall Devices, IPS Devices, Priority Devices, or custom device-related view, and with the Summary tab selected in the device details area, click the **View Events** button. Event Viewer opens and the Event Monitoring window lists events filtered by the selected device and the time period specified by the slider bar.

To view related events for a site-to-site VPN that has had a tunnel up/down event, do one of the following:

- From the Site-to-Site Tunnels view, click on the Down notification hyperlink in the Status column.
- From the Alerts view, click on the hyperlink in the Description column for tunnel up/down alerts.

Event Viewer will show IPSec VPN Events for the device within a time range depending on the polling interval for that device. If it is a priority device, the time range will be 5 minutes before until 5 minutes after the first up/down notification was received. For non-priority devices, the time range will be +/- 10 minutes instead of 5 minutes.

Related Topics

- Chapter 70, "Health and Performance Monitoring"
- Looking Up Events for a Security Manager Policy, page 68-54
- Viewing Events for an Access Rule, page 68-55
- Viewing Events for an IPS Signature, page 68-56

Examples of Event Analysis

There are many different techniques you can use to analyze and respond to events generated by your network devices. The examples in this section can help you understand some of the things you can do with the Security Manager Event Viewer.

This section contains the following topics:

- Help Desk: User Access To a Server Is Blocked By the Firewall, page 68-57
- Monitoring and Mitigating Botnet Activity, page 68-60
- Removing False Positive IPS Events from the Event Table, page 68-65

Help Desk: User Access To a Server Is Blocked By the Firewall

In this example, the help desk gets a call from a user who cannot access a server.

There are many reasons that a user might not be able to access a server, such as:

- Problems at the server's end of the network, including server down, no network connection, or the server's firewall is actively preventing access by policy.

- Problems in the network cloud between the user and the server, such as routing problems.
- Problems in the user's network, which could include workstation problems, physical problems with a network connection (for example, broken wires), problems with the switch port or wireless access point, DNS lookup failures, and so forth.

The Security Manager Event Viewer cannot identify or resolve these problems. However, it can identify whether a firewall that you control is blocking access to the server. This can help you either to rule out the firewall as being the source of the problem, or if it is blocking access, to fix the problem or to inform the user that the server is blocked by policy.

This procedure assumes that you have first determined that access to the server is not being denied by policy and that the firewall should allow access to the server.

Step 1 Ask the user for the IP address of the workstation and server.

Step 2 Open Event Viewer, for example, by selecting **Launch > Event Viewer** in Configuration Manager.

Step 3 Double-click the **Firewall Traffic Events** view to open it. Optionally, you can use the **All Device Events** view if you also want to see if there are any IPS events related to the workstation.

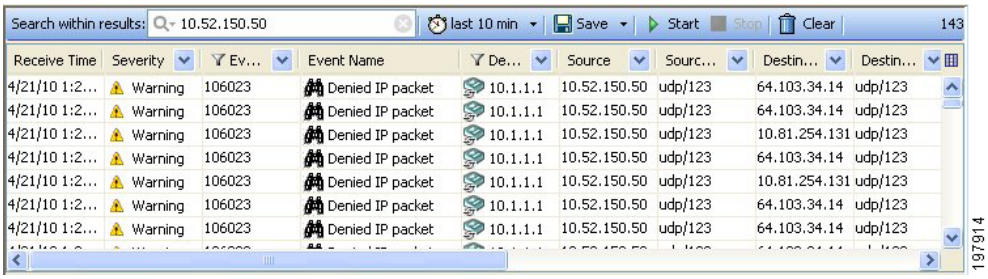
Tip You can also select the **Firewall Denied Events** view to see just denial events. However, you might want to see other events related to the user's workstation.

Step 4 Ask the user to retry the server access.

Step 5 Click the **Start** button, or select **View > Start**, to refresh the event table with the latest events.

Step 6 Type the user's IP address into the **Search within Results** box. The list of events is filtered as you type, and presents events in which the search string appears in any column. In the following illustration, the event list shows all events in the past 10 minutes for the IP address 10.52.150.50.

Figure 68-5 Restricting the Events List to One IP Address



Tip You can also select the IP address from the Source column's drop-down list, and the server's IP address from the Destination column's drop-down list (or the reverse), to show only events with both the source and destination that interests you. Use the column filters if the search string does not sufficiently reduce the event list for easy analysis.

Step 7 Look for an event that indicates that traffic from the user's workstation to the server, or from the server to the workstation, was denied. Syslog **106xxx** messages indicate denial actions.

Select the event in the table and open the Event Details pane at the bottom of the window. The tabs in this pane show the complete message information and include plain-language explanations and recommended actions.

Step 8 If the event is message **106023** or **106100**, you can quickly locate the access rule that is denying the connection and fix it. You can identify whether you can look up policies from the event by looking at the Event Name cell in the table. If there is a binoculars icon before the event name, policy lookup is available. Also, if the Go To Policy command is greyed out, you cannot look up policies for that type of event.

Tip If the traffic is denied because of the implicit **deny any** rule at the end of the access list, the Go To Policy command cannot take you to the rule. For tips about rule lookup, see Looking Up a Security Manager Policy from Event Viewer, page 68-53.

a. Right-click the event and select **Go To Policy**. You are taken to Device view with the rule selected. You are notified if a matching rule cannot be found.

b. Modify the rule so that it allows the desired access. This might be as simple as deleting the rule, or you might have to add a new rule that specifically allows traffic to or from the destination server (place the permit rule above the deny rule). Your organization's security policy determines the allowable changes. For more information about configuring the access rules policy, see Configuring Access Rules, page 16-7.

c. Submit and deploy the updated configuration to the device. For more information on the deployment process, see Deploying Configurations in Non-Workflow Mode, page 8-28 or Deploying Configurations in Workflow Mode, page 8-34.

   Wait for deployment to complete successfully.

Step 9 Ask the user to try to access the server again. If access is again denied, click **Start** in Event Viewer to refresh the events list and find the latest denial event.

Tip There might be more than one access rule that can deny communications with the server. The access rule policy is processed in order, top to bottom, so deleting a rule that prevents access can result in a rule that previously was not being hit suddenly becoming active. If you have a very long access rule policy, you could have several rules that you will have to remove one after the other. Alternatively, you could use the Rule Combiner tool to consolidate and simplify your access rules policy; for more information, see Combining Rules, page 12-22.

Step 10 Continue to resolve access denial events until the firewall is no longer blocking access.

Tip You can also use the Packet Tracer tool to simulate traffic going through the ASA device from the workstation to the server. In Device view, right-click the device that is denying access and select **Packet Tracer**. For more information, see Analyzing an ASA or PIX Configuration Using Packet Tracer, page 71-23.

After resolving all events, if the user still cannot reach the server, you know that the firewall is no longer one of the network elements that is blocking access. Consider other intervening network devices; perhaps a router includes an access rule that blocks the traffic.

Monitoring and Mitigating Botnet Activity

After you configure Botnet Traffic Filtering as described in Chapter 19, "Managing Firewall Botnet Traffic Filter Rules", you want to monitor it and resolve any problems identified in your network. You can use Security Manager and ASDM to monitor Botnet activity, and mitigate identified problems, as explained in the following sections:

Understanding the Syslog Messages That Indicate Actionable Events

Botnet Traffic Filter events use syslog message numbers 338xxx. However, some messages are informational and require no action on your part.

When viewing syslogs for botnet events, you should be most concerned with the following message numbers. For information on dealing with messages that indicate blacklisted or whitelisted traffic, see Mitigating Botnet Traffic, page 68-63. For detailed descriptions of syslog messages, see the Syslog Message document for your ASA software version at http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html.

- **338001 to 338004**—Indicate blacklisted traffic that the ASA is logging, but the ASA is not stopping the traffic. These messages require immediate attention if you want to stop botnet activity that is in progress.
- **338005 to 338008**—Indicate blacklisted traffic that the ASA is logging and dropping. This indicates that the traffic was covered by a drop rule. Thus, your network is being protected, although you still need to disinfect the victim computer.
- **338201, 338202**—Indicate greylisted traffic that the ASA is logging but not dropping. These messages can indicate an active botnet connection that needs to be handled immediately.
- **338203, 338204**—Indicate greylisted traffic that the ASA is logging and dropping. Your network is protected from this traffic. However, if the greylisted site is legitimate, the fact that the traffic is being dropped might be a problem that requires immediate attention. You can whitelist the greylisted address if you determine it is legitimate and redeploy the configuration, as described in Adding Entries to the Static Database, page 19-5.
- **338305 to 338307, 338310**—The ASA could not download the dynamic filter database. Ensure that you configured DNS lookup on the device, and that there is a routable network path to the Cisco Intelligence Security Operations Center. You might need to contact Cisco Technical Support.
- **338309**—The Botnet Traffic Filter license is not current, and you cannot download the dynamic database. Purchase and install the appropriate license. The Botnet Traffic Filter license is time-based, so you might have had a valid license that expired.

Monitoring Botnet Using the Security Manager Event Viewer

You can use the Event Viewer application to monitor syslog events generated by an ASA device. The Event Viewer has a predefined view that shows just botnet events.

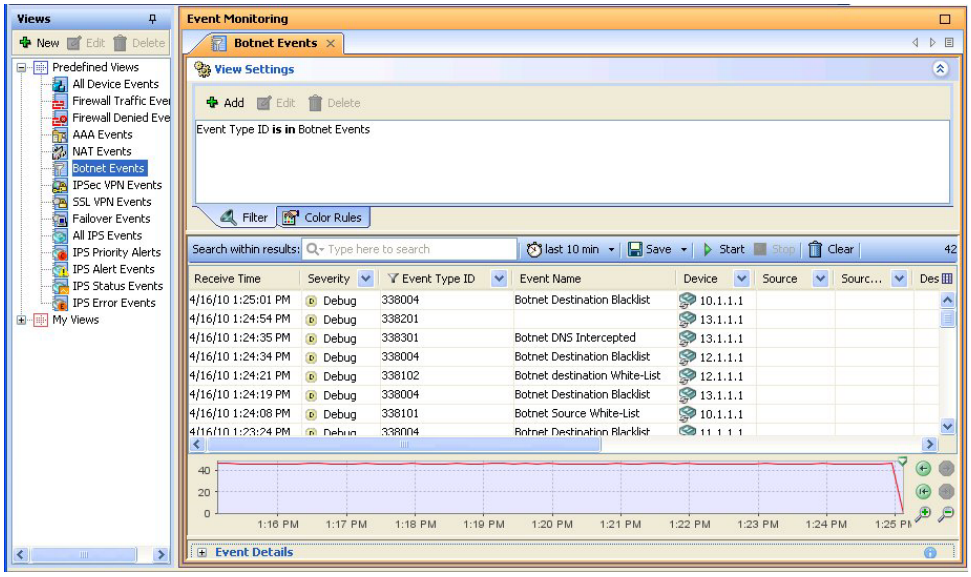
Botnet messages are in the informational to debug severity levels and are numbered 338xxx.

Tip This procedure assumes the Event Manager service is enabled. If it is not, enable it using the **Tools > Security Manager Administration > Event Management** page.

Step 1 Open Event Viewer, for example, by selecting **Launch > Event Viewer** in Configuration Manager.

Step 2 Double-click **Botnet Events** from the list of predefined views in the left pane. You must double-click to activate the view and load it into the right pane. To verify the view has been opened, ensure that the tab name for the view in the right pane says "Botnet Events." The following illustration shows an example of the botnet events view.

Figure 68-6 Botnet Events View in the Security Manager Event Viewer

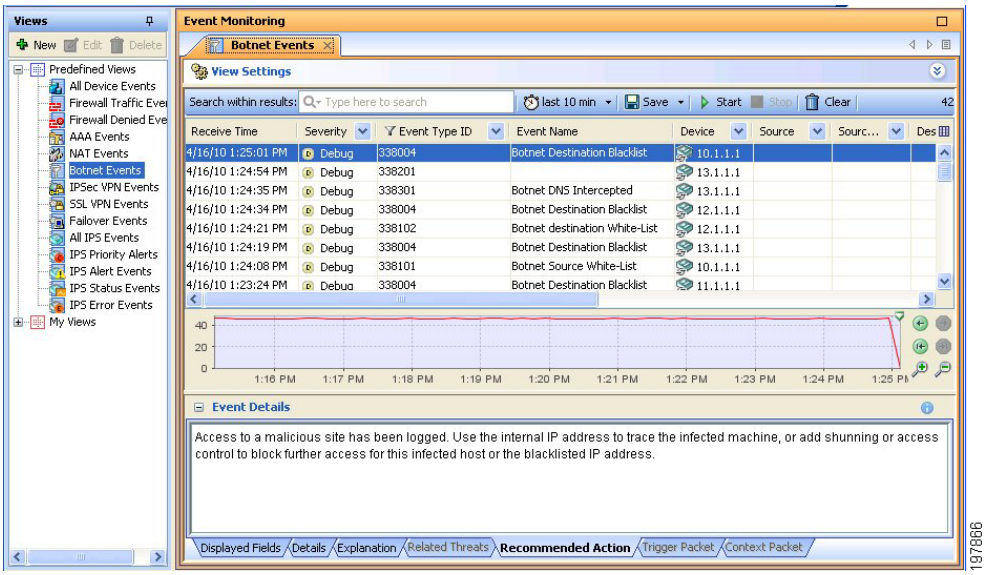


Step 3 To see the details of a specific event, select it in the table. You can then do the following:

- Double-click the event to see the tabular information presented in a more readable format.
- Open the **Event Details** section at the bottom of the window. The details pane shows information about the event organized on tabs. The Explanation and Recommended Action tabs include plain-language information about the event and what you might want to do about it.

The following illustration shows the Event Details pane for the Botnet Destination Blacklist message 338004. In this example, the recommended action is shown. The explanation for this message is "This syslog message is generated when traffic to a blacklisted IP address in the dynamic filter database appears." For information on dealing with this type of event, see Mitigating Botnet Traffic, page 68-63.

Figure 68-7 Botnet Event Details for Message 338004, Botnet Destination Blacklist



Step 4 To narrow the list of events to those generated by a single ASA, click the drop-down arrow in the Device column and select the desired device from the list. If you want to narrow the list to multiple ASAs, select Custom from the drop-down list and select the desired devices in the dialog box that appears.

You can also narrow the list using filters for any of the other columns. Filtering works the same way for all columns: either select the desired value from the drop-down list, or select Custom to create a more complex column filter.

Monitoring Botnet Using the Security Manager Report Manager

You can use the Report Manager application to generate reports on botnet activity. There are predefined reports that show the top infected hosts, the top malware ports, and the top malware sites. For a description of these reports, see Understanding Firewall Summary Botnet Reports, page 69-15.

Tip This procedure assumes the Event Manager service is enabled. If it is not, enable it using the **Tools > Security Manager Administration > Event Management** page.

Step 1 Open Report Manager, for example, by selecting **Launch > Report Manager** in Configuration Manager.

Step 2 Open the desired report from the **System > FW > Summary Botnet** folder. You can open the report by double-clicking it or by right-clicking and selecting **Open Report**.

Step 3 (Optional) Customize the report to select the desired time range and devices to include in the report. For more information, see Editing Report Settings, page 69-22.

If you want to save your custom settings to generate the report again in the future, click **Save As** to create a custom report. For more information, see Creating Custom Reports, page 69-21.

Step 4 Click **Generate Report** to retrieve the collected information and display the graphs and tabular data. For more information, see Opening and Generating Reports, page 69-20.

If you want to generate the report on a regular basis, you can configure a schedule as described in Configuring Report Schedules, page 69-33.

Monitoring Botnet Activity Using the Adaptive Security Device Manager (ASDM)

The Adaptive Security Device Manager (ASDM) includes botnet reporting features. A read-only version of ASDM is installed with the Security Manager client as a device manager, and you can start ASDM from within Security Manager.

Tip You can also install the full ASDM application separately. However, any configuration changes that you perform in ASDM are considered out-of-band changes by Security Manager and are overwritten the next time you deploy configurations from Security Manager. If you ever find a need to make configuration changes using ASDM, be sure to rediscover policies on the device in Security Manager so that Security Manager's view of the configuration is up-to-date.

Step 1 In Device view in Configuration Manager, select the ASA device.

Step 2 Select **Launch > Device Manager** to open an ASDM connection to the ASA. You are warned that you cannot make configuration changes. Click **Yes** to continue.

Step 3 In ASDM, view Botnet Traffic Filter monitoring information in the following areas:

- **Home > Firewall Dashboard** includes a Botnet Traffic Filter summary.
- **Monitoring > Botnet Traffic Filter > Reports** includes charts on the top botnet sites, ports, and infected hosts.
- **Monitoring > Logging > Log Buffer** shows historical syslog messages.
- **Monitoring > Logging > Real-Time Log Viewer** shows syslog messages as they are generated.

Tip You can also search the dynamic database on the **Configure > Botnet Traffic Filter > Botnet Database** page. This page also allows you to manually start a database download or to purge the dynamic database. These actions do not change the device's configuration and do not require policy rediscovery in Security Manager.

Mitigating Botnet Traffic

Botnet traffic mitigation is a two step process:

1. Stop traffic from your network to the botnet control site.
2. Disinfect the victim computers.

The following procedure explains the process in more detail.

Step 1 You see syslog events that indicate that packets are traveling to or from an objectionable address, typically message numbers 338001-338008 or 338201-3382004. For detailed information about these messages, see Understanding the Syslog Messages That Indicate Actionable Events, page 68-60.

Tip Messages 338201-3382004 are for greylisted traffic. You might want to first determine if the greylisted traffic is truly objectionable before stopping the traffic.

Step 2 Stop the botnet traffic:

- Messages 338005-338008 and 338203-338204 indicate that the ASA is already dropping the traffic for you. Traffic classification drop rules cover the blacklisted or greylisted addresses. See Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6.
- Messages 338001-338004 and 338201-338202 indicate that the ASA is logging the event but not dropping the traffic. The first order of business is to stop this traffic.

You have these options for stopping the botnet traffic if the ASA is not already dropping it because of a drop rule:

- (Preferred method.) Configure a drop rule for the botnet site and redeploy the configuration. See Enabling Traffic Classification and Actions for the Botnet Traffic Filter, page 19-6.
- (Second best method.) Log into the ASA using an SSH client, enter privileged EXEC mode, and use the **shun** command to prevent traffic to or from the botnet site. You can also issue this command through ASDM in a CLI window, but you cannot do it from Security Manager. The shun command does not create a permanent rule blocking traffic.

  For example, if the botnet site is 10.1.14.14, and the internal infected computer is 10.100.10.10, issue the following commands. The first command blocks all incoming traffic from the botnet command center, the second blocks traffic from the infected computer just to the botnet site.

  shun 10.1.14.14

  shun 10.100.10.10 10.1.14.14

- (Not recommended.) Although the shun command is preferred, you can also create a permanent rule in the interface's access control list (ACL) that denies traffic to or from the botnet site. With the device selected in Security Manager, select **Firewall > Access Rule**, and create two rules: one that denies the botnet site as the source address, with any destination address; one that denies any source address with the botnet site as the destination address. For service, select IP so that all traffic is blocked. You must deploy the configuration for the rule to take effect.

  Creating an access rule is not the preferred method because it creates a permanent rule, whereas botnet sites are transient. Using the Botnet Traffic Filter to dynamically block botnet traffic is a better fit for this type of network attack compared to traditional access rules.

Step 3 Shut down network access for the infected computer. For example, find the switch port to which the computer is attached, and shut down the port using the switch's CLI. There might also be wireless access for the computer, so completely shutting down network access might not be a simple task.

Step 4 Inform the owner of the victim computer that it is infected and dispatch IT personnel to disinfect the computer. Tools and techniques for disinfecting a computer are outside the scope of this document.

Removing False Positive IPS Events from the Event Table

An IPS appliance or service module (IPS device) triggers an alarm when a given packet or sequence of packets matches the characteristics of known attack profiles defined in the IPS signatures. False positives (benign triggers) occur when the IPS reports certain benign activity as malicious. Because each event requires human intervention to diagnose, spending your time analyzing false-positive events can significantly drain resources.

Due to the nature of the IPS signatures that are used to detect malicious activity, it is almost impossible to completely eliminate false positives without severely degrading the effectiveness of the IPS or severely disrupting the computing infrastructure of an organization (such as hosts and networks). Customized tuning when an IPS is deployed minimizes false positives. Periodic re-tuning is required when the computing environment changes (for example, when new systems and applications are deployed). IPS devices provide a flexible tuning capability that can minimize false positives during steady-state operations.

An example of a false-positive is a network management station that periodically builds a network discovery map by running ping sweeps. A ping sweep triggers the ICMP Network Sweep with Echo signature (signature ID 2100). Thus, ICMP Network Sweep with Echo events that have the IP address of the network management station as the source address are actually expected and desired events.

You have the following options to remove false-positive IPS events from the event table in Event Viewer:

- **Filter out events from known "clean" sources.**

  By filtering out the events, you do not stop their generation, but you also do not see them in the table. Because they are still available (you can remove the filter), you can see the events if some particular network behavior requires that you examine activity from the excluded host.

  There are two main drawbacks to using this technique:

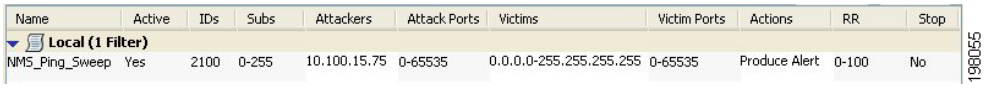
  - The events are still generated, adding events to the event store.
  - The filter excludes all events from a host. You cannot create a complex filter that excludes a host/signature ID pair.

  The procedure below shows how to filter out events from sources that you identify as clean.

- **Create event action filter rules to stop the generation of the false-positive events.**

  Event action filter rules are the easiest way to stop generating events, and are thus preferable to editing signatures or creating custom signatures, which is a more difficult task. If you exclude a host in an event action filter rule, the IPS device does not generate alarms or log records when the host triggers the event.

  Because you can target specific signatures, rather than making a blanket-exclusion of all events from a host, you can eliminate only those events that you are certain are benign. For example, the following event filter rule removes the Produce Alert action from the ICMP Network Sweep with Echo (2100) signature for the network management station 10.100.15.75. The network management host is identified as the attacker address; the action specified in an event filter rule is actually the action that is removed from the event. Note that if you create an event action override rule to add other alert-producing actions to ICMP Network Sweep with Echo events, you must also remove the override action in this rule.



For more information about configuring event action filter rules, see Configuring Event Action Filters, page 40-4.

The following procedure shows how to use filtering in Event Viewer to remove false positives from the events list. It uses network/host policy objects to accomplish the filtering.

Tip By creating source or destination address filters using network/host objects, you can update the filters simply by changing the contents of the object. You do not need to add or remove filters from your views. Another advantage is that you can proactively create filters for addresses that do not currently appear in the events table; the source/destination column filter controls in Event Viewer list only those addresses that currently appear in listed events.

Step 1 Create a network/host policy object that includes the IP address of the clean hosts or networks.

a. Select **Manage > Policy Objects** to open the Policy Object Manager window (see Policy Object Manager, page 6-4).

b. Select **Networks/Hosts** from the table of contents.

c. Click the **Add Row (+)** button beneath the table of network/host policy objects, and select **Group** as the object type.

d. In the Add Network/Host Group dialog box, enter a name for the object, for example, IPS_Safe_Hosts.

e. Select **Enter IPv4 Address Information** and enter the IP address, for example, 10.100.15.75.

f. Click **Add >>** to add the IP address to the Members in Group list.

g. Click **OK** to create the object.

h. Click **Close** to close the Policy Object Manager window.

Step 2 Select **File > Submit** to submit your changes to the database (non-Workflow mode). Keep in mind that all of your configuration changes are submitted, not just the new policy object.

If you are using Workflow mode, you must submit your activity and have it approved, if necessary.

Tip Event Viewer can see only those policy objects that have been submitted to the database, so you must submit your changes before you can create a filter using the object. If you later change the object, you must also submit your changes for the filter to use the new definition of the policy object.

Step 3 Select **Launch > Event Viewer** to open the Event Viewer application.

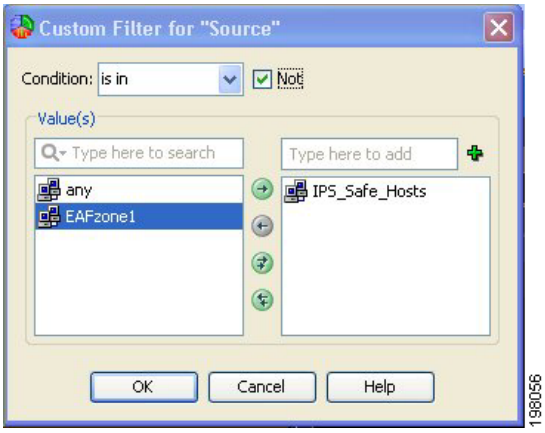
Step 4 Create a custom view that filters out the network management station:

a. Double-click the predefined view that you want to use as the basis of your custom view, for example, **All IPS Events**. Double-clicking the view in the Views list opens the view. If you already have a custom view that you want to update, open it.

b. Click the down arrow button in the title of the Source column in the events table and select **Custom** to open the Custom Filter for Source dialog box.

Tip: You can also get to this dialog box through the View Settings pane by clicking the **Add** button, then selecting Source in the Add Custom Filter to a Column dialog box and clicking **OK**.

c. In the Custom Filter for Source dialog box, select the policy object you created and click the right-arrow button to move it to the selected list. Also, select the **Not** option next to the Condition option. The following illustration shows how the dialog box should look.



d. Click **OK**. The filter is added to the view settings and is used to remove events from the table.

e. Select **File > Save As** to save the changes as a new custom view. You are prompted for a view name and description; enter the information and click **OK**.

The following illustration shows what the view settings would look like if you started with the All IPS Events predefined view and named your new view Filtered IPS Events.