



CHAPTER 10

Event Logging and Alerts

Overview

Events and messages logged by Cisco Security Agents can be viewed from CSA MC. You can also control the type of alert sent out based on the severity level of the logged event, the specific event, and the host that generated the alert. You can configure CSA MC to send email, issue SNMP traps, log to a text file, and execute custom programs.



Note

Cisco Security Agent events are also stored in the NT event log on an agent system in a localized format.

This section contains the following topics.

- [The Event Log, page 10-2](#)
- [Event Aggregation and Suppression, page 10-6](#)
- [Event Monitor, page 10-9](#)
- [Event Log Management, page 10-11](#)
- [How Logging Works, page 10-15](#)
- [Verbose Logging, page 10-16](#)
- [Logging and Query User Rules, page 10-16](#)
- [About the Event Management Wizard, page 10-17](#)
- [Creating an Exception Rule, page 10-19](#)

- [Creating a Logging Exception Rule, page 10-25](#)
- [Perform a Behavior Analysis, page 10-28](#)
- [Event Sets, page 10-36](#)
- [Third Party Access to Events, page 10-40](#)
- [Configuring Alerts, page 10-43](#)
- [Generate an Alert Log File for Third Party Applications, page 10-48](#)

The Event Log

The Event Log view, available from the Events category in the menu bar, lets you view system events provided by registered agents according to designated time frames, event severity levels, and the system that generated the event.

The information displayed at the top of the Event Log page (controlled by the settings in the Change Filter window, see next section) tells you the following:

- **Filter by eventset:** This displays the name of the Event Set, if any, used to filter the event log view.

or Define a filter with the following parameters:

- **Time range:** This is the current time range set for the event log filter.
- **Severity:** This is the current minimum and maximum severity range set for the event log filter.
- **Host:** This displays which hosts have generated the events viewable in the event log (set as part of the filter).
- **Rule Module:** From the pulldown list, select a rule module to search for events generated by that module.
- **Rule ID:** Enter the ID number for a rule to search for events generated by that rule.
- **Events per page:** This is the current value set for the number of events displayed on each page of the event log (set as part of the filter).
- **Filter text:** Enter a text string here to either include or exclude in your event message search.
- **Filter out similar events:** When event filtering is enabled (it's enabled by default), the event log displays an aggregation of events.

Start date and End date

To search events, click the **Change Filter** link to access a pop-up window from which you can enter search criteria such as Start and End Date time frames. You can refer to the following points for entering time frame information, but note that most reasonable time frames are recognized by CSA MC:

- You can select a preconfigured Event Set by which to filter the event log or
- You can specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
- Enter a specific time using any of the follow time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.
- Enter a specific month and day with optional year in the formats: mm/dd/yy, monthname dd , yy. Specifying the year is optional. The default year is the current year.

Minimum and Maximum Severity Settings

From the Minimum and Maximum Severity pulldown list, select a severity level and click the View button to see all events within the designated severity levels that have been logged within the time frame you've specified. Select from the following.

- Informational
- Notice
- Warning
- Error
- Alert
- Critical
- Emergency

Host

You can filter the Event Log by host systems. All is the default here. All events generated by systems registered with the server are displayed. You can enter a specific host name to search for that host. Click the **change** link beside the Host field for a host selection box.

Events / page

Enter the number of events per page you want to display up to a *maximum of 500 events* per page. The event log displays the most recent number of events based on the value you enter. You can page forward through links to view additional pages matching the query.

**Note**

You can configure the CSA MC Event Log to display events from the agent system's NT Event Log. See [NT Event Log, page 6-54](#).

Filter out similar events

When event filtering is enabled (it's enabled by default), the event log displays an aggregation of events. This aggregation means that one representative event is displayed for all events that are considered similar on the MC. Similar events are defined as having the same rule ID and the same application name and path (excluding drive letter). When similar events are filtered from the event log view in this way, there is italicized text below the viewable representative event. This text displays the number of filtered events that are not visible. Clicking the **Find Similar** link below the event causes all events of this similar type to be displayed in a new event log window.

**Note**

This event filtering feature is enabled by default. Accessible from the **Change filter** link at the top of the Event log page, you can change the **Filter out similar events** radio button to **No** to turn this feature off.

Figure 10-1 Event Log View

The screenshot displays the Management Center for Cisco Security Agents V5.2 interface. The main window shows the 'Event Log' section with a list of 17 events. A 'Filter Events' dialog box is open, allowing users to filter events by eventset, date range, severity, host, and rule module. The event log shows a 'biohazard Alert' at 11:11:01 AM on 11/30/2006, with details about a connection attempt to TCP port 139.

#	Date	Severity	Event Log generation time
17	12/1/2006 10:52:28 AM		
16	12/1/2006 12:01:49 AM		
15	11/30/2006 11:57:23 AM		
14	11/30/2006 11:52:57 AM		
13	11/30/2006 11:52:57 AM		
12	11/30/2006 11:11:01 AM	biohazard Alert	

The event log screen (see Figure 10-1) displays event messages within the time frame and severity level you specify and optionally by a specific host. These event messages explain the event that occurred and they provide a link to the rule that triggered the event. It also provides the exact time the event was recorded and a link to the registered host view for the host that generated the event.

Some Event Log messages contain a **Details** link you can click to view more information on the event that generated the message. (The details contained here can be useful to customer support.) Log messages also contain a **Rule number** link. Clicking a Rule number link takes you to the rule that was triggered when the message in question logged.

Some Event Log messages contain a **Details** link you can click to view more information about the event that generated the message. (The details contained here can be useful to customer support.) Read [Reading Event Details, page 10-8](#), for more information. The Details link also provides packet information when appropriate. By installing Wireshark (<http://www.wireshark.org>) on the same server in which CSA MC is installed, you will be able to read the contents of a packet in a human-readable form rather than in hexadecimal notation. Read [Reading Packet Details, page 10-9](#) for more information.

Log messages also contain a **Rule number** link. Clicking a Rule number link takes you to the rule that was triggered when the message in question logged.

Use the **Wizard** link where available, to edit the rule that caused the event. See [About the Event Management Wizard, page 10-17](#) for details.

A **System State** link appears with an event when the rule in question has triggered due to a system state condition. (Note that it is not always advisable to generate a wizard exception based on an event that is appearing due to a system state condition triggering. Rather, if you intend to configure an exception, you should create it for the original rule that caused the system state to apply.) Use the pop-up that appears when you click **System State** from an event to trace back to the original rule (if available) that triggered the system state condition.

Event Aggregation and Suppression

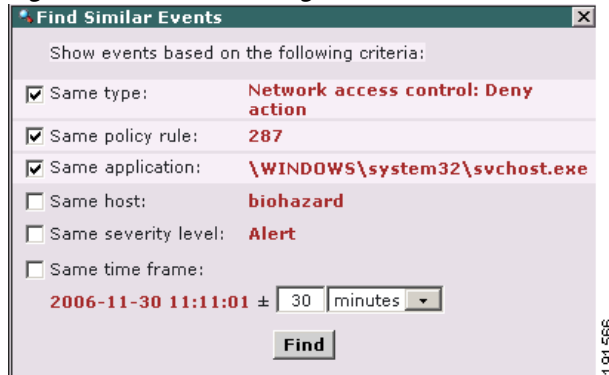
When first deploying rules to agents, it is not unusual to have an overwhelming flurry of events appearing in the event log. In some cases, most of these events are similar events or simply "noisy", not useful events to view. If this is the case, the event log provides two mechanisms for paring down the number of events that appear. They are as follows:

- **Event Filtering (aggregation of events)**

When event filtering is enabled, the event log displays an aggregation of events. This aggregation means that one representative event is displayed for all events that are considered similar on the MC. Similar events are defined as having the same rule ID and the same application name and path (excluding drive letter). When similar events are filtered from the event log view in this way, there is italicized text below the viewable, representative

event. This text displays the number of filtered events that are not visible. Clicking the **Find Similar** link allows you to view all events of this similar type in a new event log window.

Figure 10-2 Event Log Find Similar



Note

This event filtering feature is enabled by default. Accessible from the **Change filter** link at the top of the Event log page, you can select the “Filter out similar events” **No** radio button to turn this feature off.

A "similar" event is defined as follows (The event must meet all of the following criteria.):

- Same event code type.
- Same rule ID.
- Same application name and path (excluding drive letter).

- **Event Suppression**

When event suppression is enabled, all chosen events are no longer displayed in the event log. Event suppression is best used when you have a reoccurring event that is more noisy than useful to you. This is something you are aware of, but no longer wish to see. Suppressing the event removes all viewable instances of that event and causes further events of the same type to be hidden. Note that these events remain in the database, they are simply not displayed. The visibility of the suppressed events is controlled by Administrator Preference settings. Refer to [Configuring Role-Based Administration, page 2-5](#).



Note Event suppression is configured through the Event Log Wizard. See [About the Event Management Wizard, page 10-17](#). Clicking the **Wizard** link from the event you wish to suppress allows you to create a suppression filter for the event. The filters you create can be removed by clicking the link at the top of the Event Log page that displays the number of filters in place. That link launches a window from which you can select filters that you want to remove.

Reading Event Details

To view the details of an Event Log entry, follow this procedure:

-
- Step 1** Move the mouse over **Events** in the menu bar of CSA MC. Select **Event Log** from the drop-down list that appears. All events are displayed by default in the event log.
 - Step 2** Click the **Details** link for the event about which you want more information. The details of the event are displayed in a separate page.
 - Step 3** (Optional) If you want more information about an entry in the details, you can use the Google search engine to search the Internet. Do this in one of two ways:
 - With your mouse, highlight the string of text, in the details page, about which you want more information. Then click the Google icon at the bottom of the details page. A new browser window opens with the results of the Google search.
 - Drag the Google icon at the bottom of the details page over one of the fields in the details page. (Fields that are highlighted white can be searched by Google.) Release the mouse button. A new browser window opens with the results of the Google search.

Reading Packet Details

CSA MC provides a mechanism which allows you to use “Wireshark” software to translate packets into a readable format. Wireshark is a third-party tool that analyzes protocols and works with WinPcap to analyze packets. Before you can view packet information in readable form, you must first install Wireshark on the same server that runs CSA MC.

To install Wireshark, follow the installation instructions found at <http://www.wireshark.org>. Install the latest released version of Wireshark and the version of WinPcap recommended by Wireshark.

After you have installed Wireshark, you can read packet details by following this procedure:

-
- Step 1** Move the mouse over **Events** in the menu bar of CSA MC. Select **Event Log** from the drop-down list that appears. All events are displayed by default in the event log.
 - Step 2** Click the **Details** link for the event about which you want more information. The details of the event are displayed in a separate page.
 - Step 3** Scroll down to the **NetPacket** details row to read a description of the contents of the packet that triggered the event.

Event Monitor

Similar to the Event Log, the Event Monitor, available from the Events category in the menu bar, lets you view system events provided by registered agents according to designated severity levels, and the host that generated the event. You can also enter the number of events to be displayed (default value is the last 50 events). Click the **Change** link to access a pop-up window from which you can edit these values and change the event filter. Refer back to [The Event Log, page 10-2](#) for more information on these fields.

Unlike the Event Log page, the Event Monitor page automatically refreshes itself at set intervals. The event list is updated with the latest events each time the page refreshes.

The footer of this page provides a **Refresh** button and a **Pause** button. Use the Refresh button to refresh the page immediately without waiting for the set refresh interval to occur. Use the Pause button to immediately stop the page from refreshing. The set refresh interval will then stop at wherever it is in the countdown. This pause feature is useful when you are testing policies and you want to mark a certain place as a starting point for receiving new events. When you click it, the Pause button becomes a Resume button.

**Note**

The administrator inactivity timeout value is still in effect when you leave the Event Monitor screen displayed on your system. The automatic page refresh does not constitute activity.

The Event Monitor will continue to refresh even after the timeout expires. However, you will not be able to navigate to any other page. This allows you to leave the Event Monitor on screen without worrying about anyone being able to access CSA MC after the session timeout.

Event Log Management

The **Event Log Management** feature, available from the **Events** category in the menu bar, lets you create event database management tasks to manage the size of your event log. As your event log grows, specifying parameters for deleting events will help prevent this log from growing too large and from maintaining stale information.

**Note**

You can configure global event insertion threshold parameters from the global **Event Insertion Tasks** page. This page already contains default settings for stopping the insertion of additional events for each event level when the specified threshold setting is reached. You can change these settings, if necessary. The thresholds on this page only trigger if the Event Log Management parameters you configure (described in the second section on this page) do not adequately keep events pruned below configured levels. For example, if there is a sudden flurry of events and configured pruning parameters do not trigger immediately, the global thresholds will kick in.

To access the global Event Insertion Tasks page:

Step 1 Move the mouse over **Events** in the menu bar and select **Event Log Management** from the drop-down list that appears.

Step 2 Click the top bracketed link **<Event Insertion Tasks>** to access the page. See [Figure 10-4](#).

This page displays the total number of events in the Event Log. It also breaks events out to the number of events that exist for each severity level. Beneath this graphical event display are the default threshold settings for each event level. These thresholds represent the upper limit of events which must be reached for each severity level before no more events of this type will log. Event pruning must occur in order for these event types to once again be written to the Event Log.

To configure an event auto-pruning task, do the following. See [Figure 10-3](#).

Step 1 Move the mouse over **Events** in the menu bar and select **Event Log Management** from the drop-down list that appears.

Step 2 Click the **New** button to create a new entry. This takes you to the auto-pruning configuration view.

- Step 3** Enter a **Name** for the auto-pruning task.
- Step 4** Enter a **Description**. This is a useful line of text that is displayed in the list view and helps you to identify this particular configuration.
- Step 5** Use the **Enabled** checkbox to enable this event auto-pruning configuration. (It is enabled by default.) By not selecting this checkbox, you can save this item, but it will not be active.
- Step 6** Enter a value in the **Delete Events - Older than** field. This is the value for which events, once having been in the log for this number of days, are deleted. Before these events are removed, they must also match the parameters of the event set selected on this page.
- Step 7** **And Matching the following Event Set**. Select the preconfigured event set for the event type you want to prune from the event log. Configuring event sets provides flexibility in selecting the events for auto-pruning.
- Step 8** **And The database size exceeds <##> MB**. Use this field to specify database size limits that should not be exceeded. Before events are removed due to size, they must also match the other parameters selected on this page.
- Step 9** Click the **Save** button.

**Note**

This purging of events will occur periodically based upon the configured auto-pruning items. Generally, this pruning will take place at a time when the least activity is registered on the MC. When event auto-pruning occurs, a message appears in the event log notifying you of this action.

Figure 10-3 Event Auto-Pruning

The screenshot displays the Management Center for Cisco Security Agents V5.2 web interface in Microsoft Internet Explorer. The browser address bar shows `https://biohazard/csamc52/webadmin`. The page title is "Management Center for Cisco Security Agents V5.2" and the breadcrumb navigation is "Events > Event Managing Tasks > Configured auto-pruning".

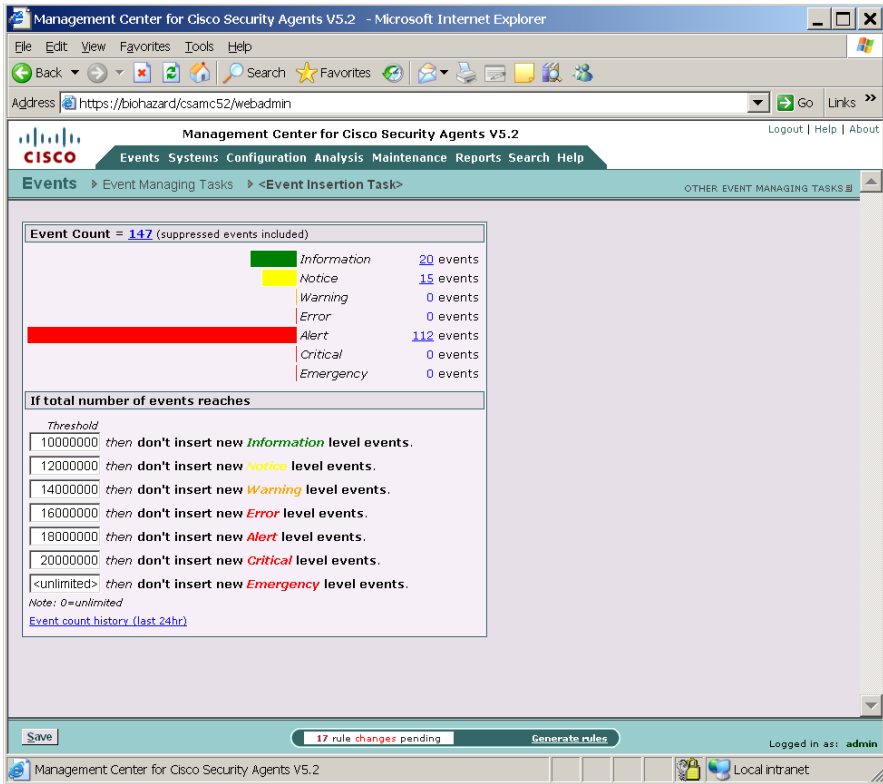
The main content area shows the configuration for "Configured auto-pruning" (Version 5.2 r119). The description is "Prune all events older than 90 days". The "Enabled" checkbox is checked.

The "Delete Events" section is expanded, showing the following configuration:

- After: 90 day(s)
- AND
- Matching the following event set: <All Events> [New]
- AND
- The database size exceeds: 3072 MB

Below the configuration, it states "No deletion recorded so far." At the bottom of the page, there are "Save" and "Delete" buttons, a status message "17 rule changes pending", and a "Generate rules" button. The user is logged in as "admin".

Figure 10-4 Event Insertion Task



191564

How Logging Works

The CSA MC Event Log does not contain every occurrence of an event from a system. Duplicate events are not logged for an hour after the first occurrence.

**Caution**

In some cases, when an event is logging continuously, the agent will suppress this logging temporarily. Before it does this, a log message informing you of this suppression appears in the event log.

The following information is logged for each rule type.

- File access control logging—Process path and file names and file operation are logged.
- Network access control logging—Process path, network address, port and direction are logged.

**Note**

No network access control rule denial events are logged for any TCP or UDP port resulting from multicast packet signals.

- Registry access control logging—Process path and registry key are logged.
- COM component access control logging—Process path and COM component PROGID/CLSID are logged.

A duplicate event is defined as follows:

- For file access controls, the name of the application and the file being accessed are the same.
- For network access controls, the name of the application, the remote address, and the network service port are the same.
- For registry access controls, the name of the application and the registry key name and value name are the same.
- For COM component access controls, the name of the application and the COM component PROGID or CLSID are the same.

Verbose Logging

Enable Verbose Logging Mode in the Group configuration view to change the event log timer to log *all* recurring events rather than only logging recurring events once every hour. Verbose logging applies to all policies that are attached to the group that have logging turned on.

For normal operations, you would not want to enable Verbose logging. Verbose logging is useful for troubleshooting and for analyzing how applications work with rule sets, i.e. related processes and subprocesses. In the latter case, using Verbose logging with Test Mode can be very useful for monitoring how a rule set would work before deploying it.

**Note**

Verbose logging is enabled on a host if any group in which the host is a member has Verbose logging turned on.

Logging and Query User Rules

When a user responds to a Query User box (by pressing Yes, No, or Terminate), the agent remembers the response and caches it for an hour. This way, if the same rule is triggered again within that hour, the action is allowed or denied based on what the user answered previously, with no pop-up query box appearing again. When the user responds to a triggered Query User pop-up box, the system action that triggered the pop-up, as well as the user's response, are logged in the CSA MC event log. With Verbose logging turned on, all subsequent automatic allows or denies are logged as well. Otherwise, the one hour logging timer prevents agents from logging the automatic allowed or denied system action if it occurs again within the hour.

About the Event Management Wizard

Use the Event Management Wizard to accomplish the following:

- To change the action of a rule that triggered a specific event. If an action is being denied on end user systems and you want to allow this action, you can automatically generate an "exception" allow rule which takes the application class and resource information in the event and creates an allow rule to counteract the rule that caused the deny.
- To perform a Behavior Analysis Investigation for the application that caused the event. The Event Management Wizard is available for events triggered by Deny rules and Query User rules.
- To create an exception rule that stops a specific event from logging. The Wizard makes use of the **Take precedence over other <action type> rules** feature to manipulate rule precedence and prevent logging of an event.
- To suppress an event from the event log. Event suppression is configured using the Rule ID of the event and the application (including file path) as the criteria for suppressing the event in question and all similar events. See [Event Aggregation and Suppression, page 10-6](#) for more information.
- To purge similar events from the Event Log. Use this wizard feature to purge all events similar to the event from which the Wizard link was clicked. This purges all similar events but leaves one, most recent, representative event in the event log. All but one of these events are purged from the Event Log.

Figure 10-5 Event Management Wizard Link

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

Address: https://biohazard/csamc52/webadmin

Management Center for Cisco Security Agents V5.2

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Log

17 events [change filter](#)

Event log generation time: 12/1/2006 2:18:39 PM
 Severity: Information - Emergency
 Host: All
 Rule Module: All
 Events per page: 50
 Sort by: Order received
 Filter out similar events: Yes (filtered out ~88% of 147 events)

#	Date	Host	Severity	Event
17	12/1/2006 10:52:28 AM	-	Information	Administrator 'admin' logged in from 172.31.10.12 (S9). 8 similar events (same Type/Rule ID/Application) Find Similar
16	12/1/2006 12:01:49 AM	-	Information	Application Deployment Analysis data has been purged and archived(if set) successfully. 2 similar events (same Type/Rule ID/Application) Find Similar
15	11/30/2006 11:57:23 AM	biohazard	Notice	The process 'C:\Program Files\Cisco Systems\CSAgent\bin\okclient.exe' (as user BIOHAZARD\Administrator) attempted to access a resource which resulted in the user being asked the following question. 'An attempt is being made to disable security for the Cisco Security Agent. Do you wish to allow this?' The user was queried and a 'Yes' response was received. Details Rule 707 Wizard 1 similar event (same Type/Rule ID/Application) Find Similar
14	11/30/2006 11:52:57 AM	biohazard	Information	The process 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user BIOHAZARD\Administrator) attempted to initiate a connection as a client on TCP port 80 to 10.86.189.238 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation was allowed. Details Rule 256 Wizard 5 similar events (same Type/Rule ID/Application) Find Similar
13	11/30/2006 11:52:57 AM	biohazard	Notice	The process 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user BIOHAZARD\Administrator) attempted to access a resource which resulted in the user being asked the following question. 'The process C:\Program Files\Internet Explorer\IEXPLORE.EXE is attempting to communicate on the network using TCP/80. Do you wish to allow this?' The user was queried and a 'Yes' response was received. Details Rule 256 Wizard 6 similar events (same Type/Rule ID/Application) Find Similar
12	11/30/2006 11:11:01 AM	biohazard	Alert	The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\LOCAL SERVICE) attempted to initiate a connection as a client on TCP port 139 to 172.31.20.76 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation

17 rule changes pending [Generate rules](#) Logged in as: admin

Local intranet

191578

Creating an Exception Rule

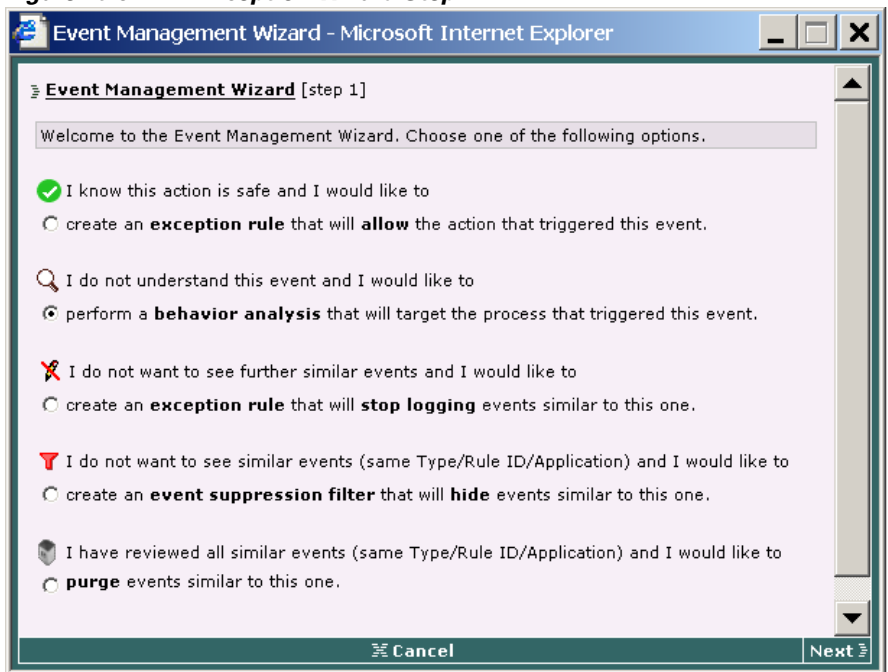
When you click the **Wizard** link from the Event Log page, you can choose to create an exception rule, an exception logging rule, or to configure a behavior analysis (see [Figure 10-6](#)). If you select to create an exception rule, when you click **Next** you are shown a summary of the rule that triggered the event. You click **Next** to continue to create the rule. The exception rule is an Allow rule that will be added to an existing rule module or to a new rule module and it will take precedence over the Deny or Query User rule that caused the event.

You can create exception rules for the following rule types:

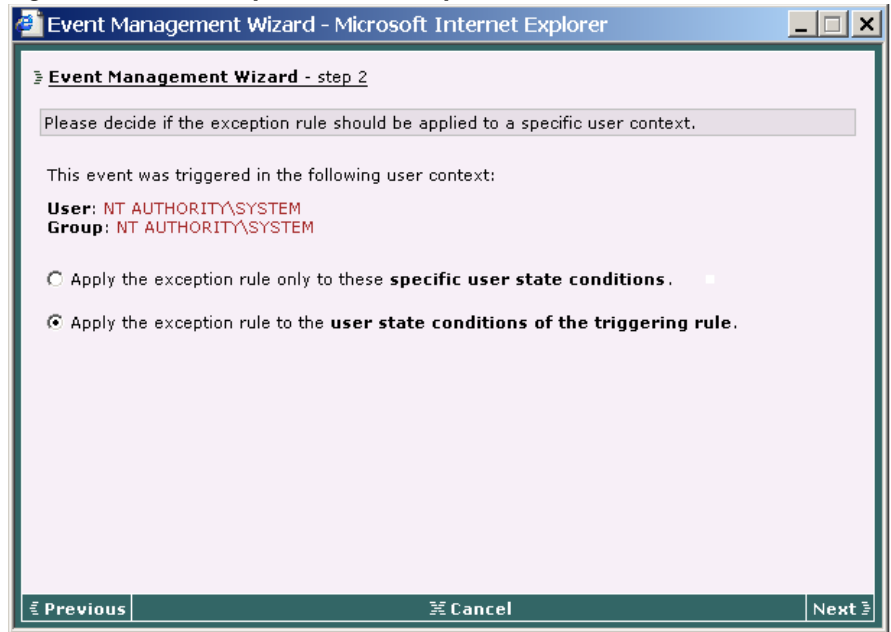
- Application control
- Buffer overflow
- COM component access control
- File access control
- Network access control
- Registry access control
- Rootkit/kernel protection
- System API control

The wizard then takes you through a step by step procedure for affecting the changes you wish to make.

Figure 10-6 Exception Wizard Step 1



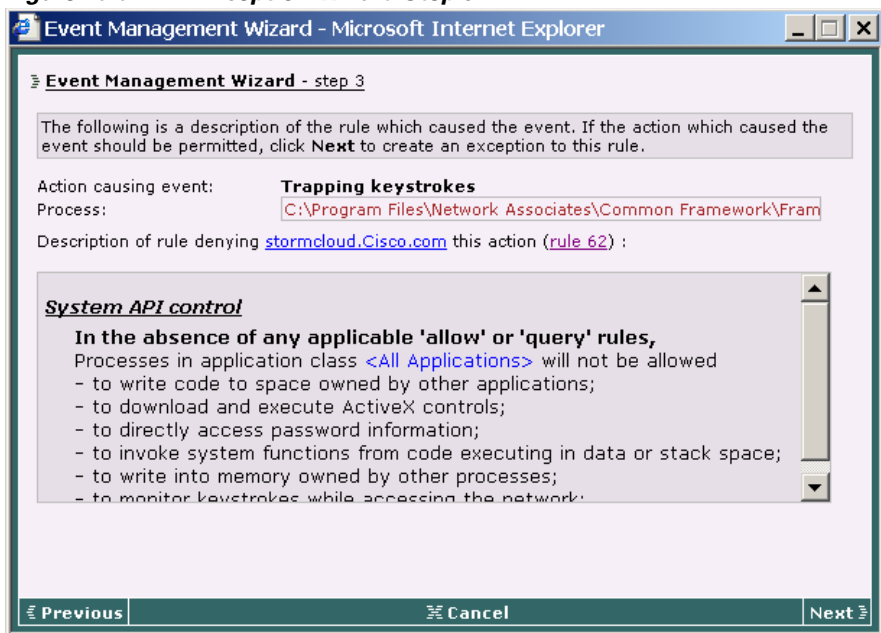
The next wizard page prompts you to optionally apply your changes to state conditions.

Figure 10-7 Exception Wizard Step 2

191571

The third step provides a summary of the rule for which you are creating an exception.

Figure 10-8 Exception Wizard Step 3



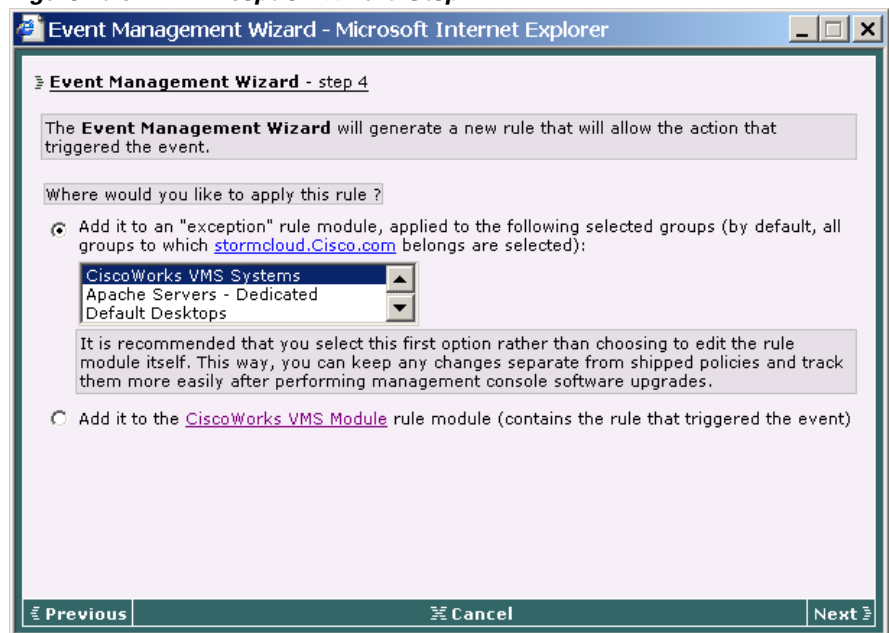
181575

In the fourth step (see [Figure 10-9](#)), you are given two choices as to where you would like to apply this new rule. You can create a new rule module (an "exception rule module") which would contain the new exception rule. (This is the default and recommended choice.)

This new module would be attached to a new exception policy which is then attached to the group(s) containing the host from which the event was received. If you choose to create this exception module, all subsequent exception rules you create through the wizard will be added to the same exception module and policy if the group it is to be applied to is also the same. Therefore, a group could only have one exception policy, but contain an exception rule module with any number of exception allow rules created through the wizard.

Your second choice is to add this new exception rule directly to the module which contains the rule that caused the event. This would be a change to the module itself.

Figure 10-9 Exception Wizard Step 4

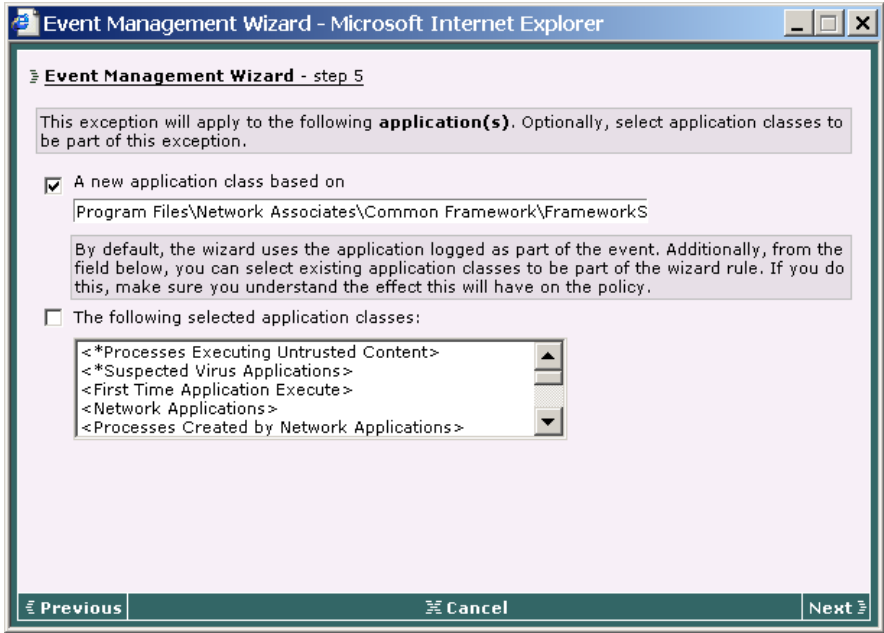


191576

As you continue through the wizard, you can simply click Next and accept the defaults which create an allow rule for the exact application and resource named in the event. You can also select to include more groups to receive the exception and edit the process path of the application and/or include more application classes in the rule (see Figure 10-10).

When the wizard completes, it takes you to the new rule as it appears in CSA MC.

Figure 10-10 Exception Wizard Step 5



191577

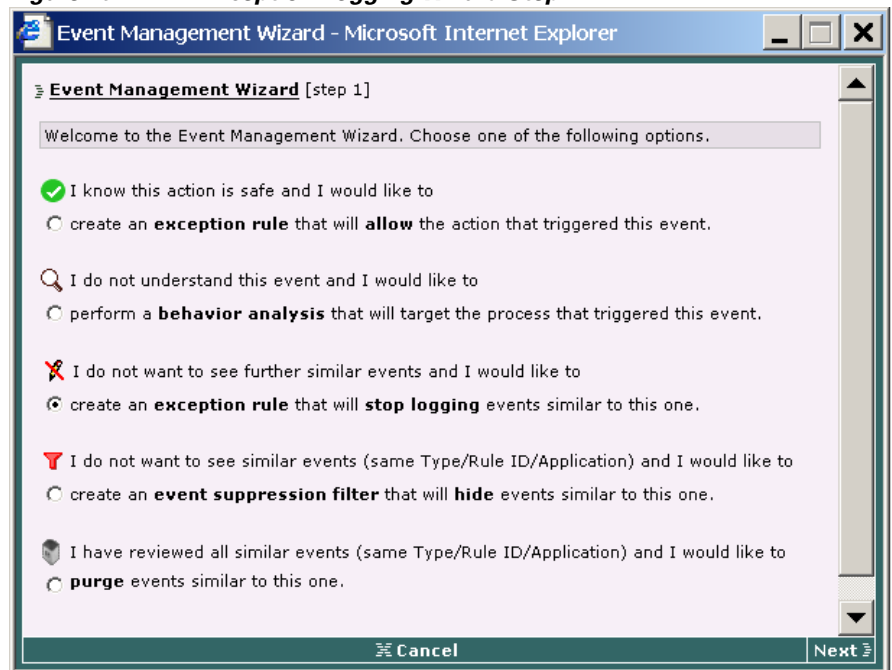
Creating a Logging Exception Rule

The Wizard makes use of the **Take precedence over other <action type> rules** feature available in some rule types to manipulate rule precedence and prevent the logging of an event. The following rule types make use of precedence manipulation: File access control, Network access control, Registry access control, COM component access control, Application control, and System API control.

See [Rules: Manipulating Precedence, page 5-42](#) for more information on the manipulating precedence feature.

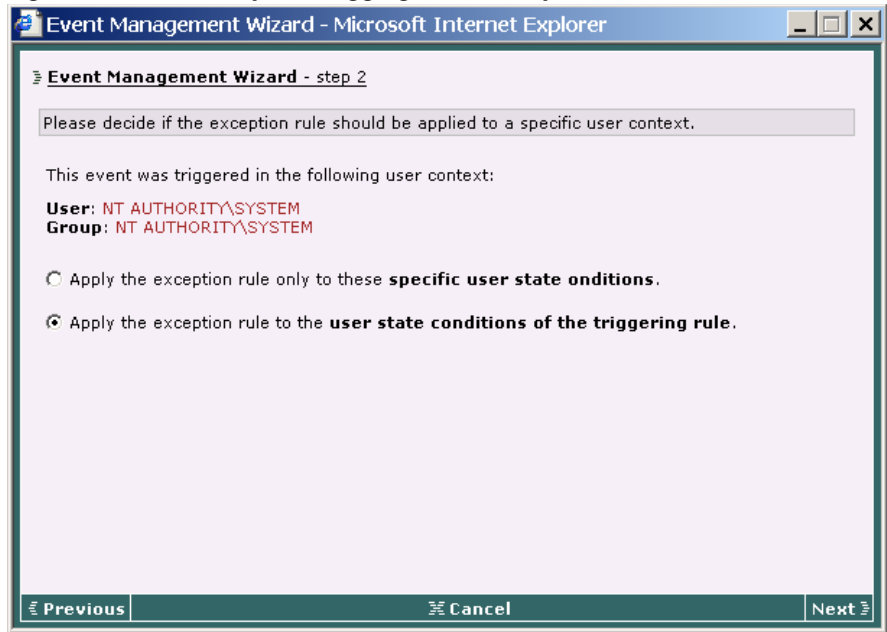
If you select to create an exception logging rule (see [Figure 10-11](#)), when you click **Next** you are shown a summary of the rule that triggered the event. You click **Next** to continue to create the exception logging rule.

Figure 10-11 Exception Logging Wizard Step 1



The next wizard page prompts you to optionally apply your changes to state conditions.

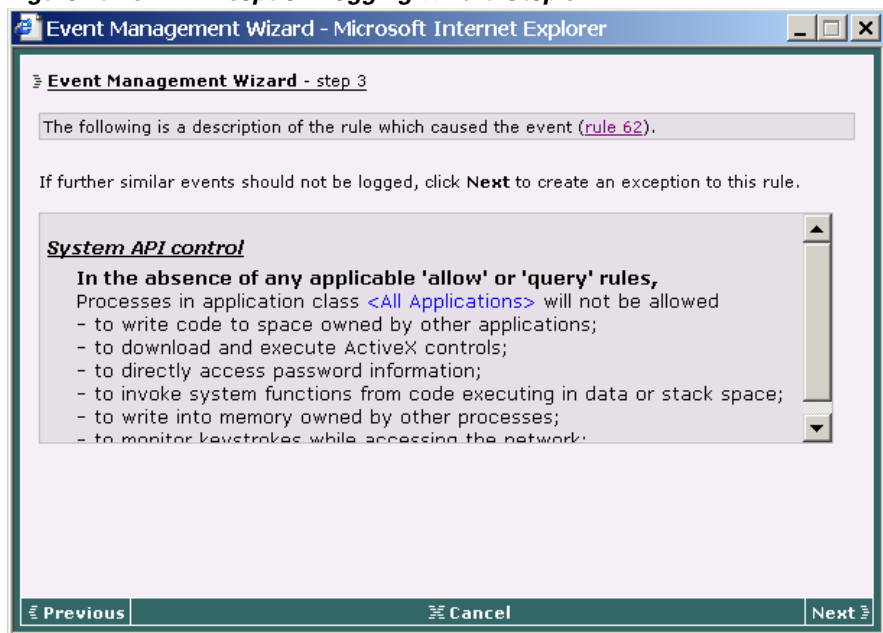
Figure 10-12 Exception Logging Wizard Step 2



1915 70

The exception logging rule is a rule that is added to an existing policy or to a new policy. This rule is an exact copy of the rule that triggered the event. The one difference is that the rule created by the wizard has the **Take precedence over other <action type> rules** checkbox selected and the **Log** checkbox is unselected. This causes the rule created by the wizard to remain in effect, in the correct precedence within the policy, but not log an event when triggered.

Figure 10-13 Exception Logging Wizard Step 3



191574

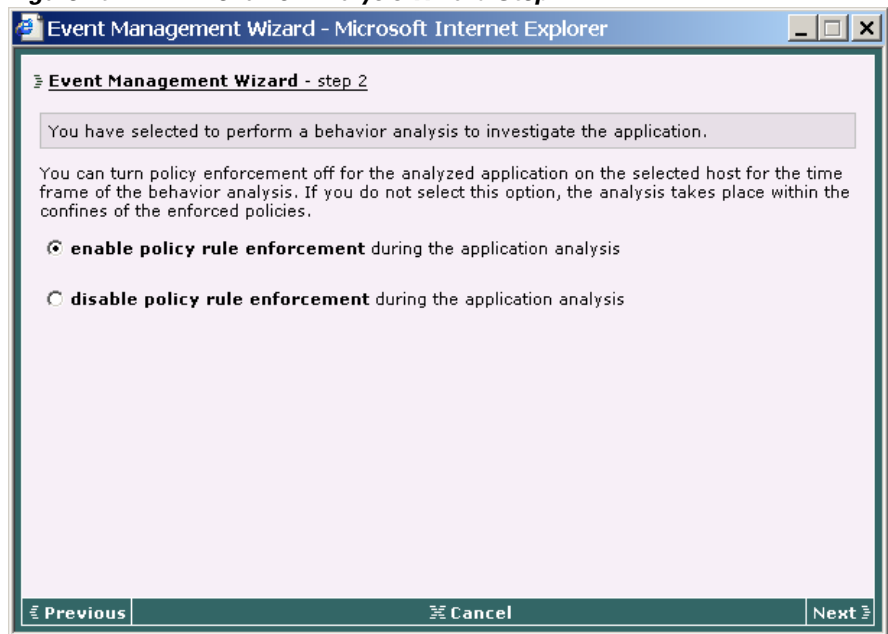
Perform a Behavior Analysis

When you click the **Wizard** link from the Event Log page, you can choose to configure a behavior analysis to investigate the application that triggered the event (see [Figure 10-6](#)).

If you select to create a behavior analysis, optionally you can choose to **Disable policy rule enforcement** for the time frame of the analysis. Otherwise, the analysis takes place only within the confines of enforced policies. In that case, some events may be denied by rules during the analysis and therefore the analysis may not be complete.

If you select the Disable policy rule enforcement checkbox, when the logging agent receives an analysis, any policies relevant to the application being analyzed are disabled on the selected host until the behavior analysis is completed. You should understand that if the application being analyzed is untrusted or potentially a virus, you will allow it to run unimpeded during the analysis if you disable policy rule enforcement.

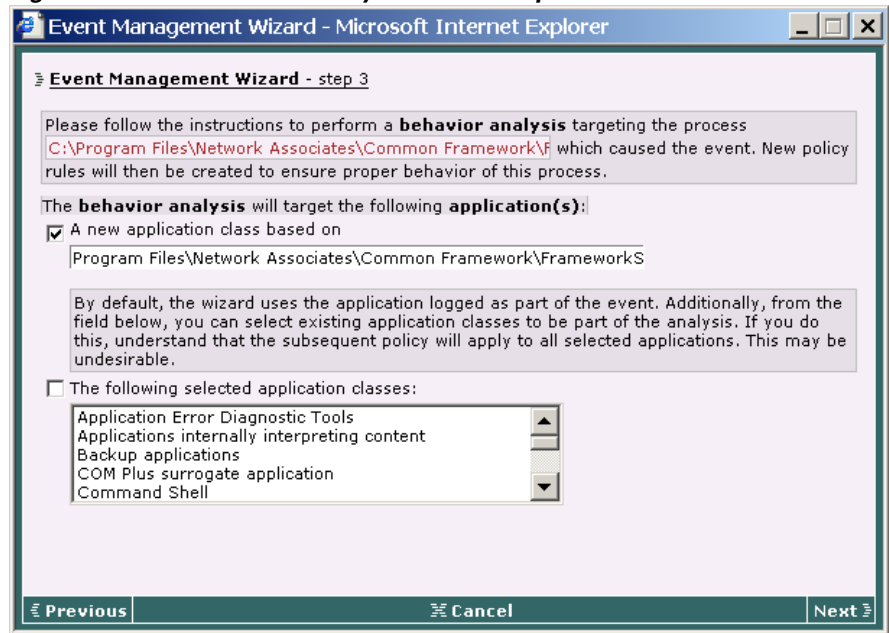
Figure 10-14 Behavior Analysis Wizard Step 2



181569

If you decide that the application is not dangerous and it can run without any policy restrictions, you can begin to configure the behavior analysis.

Figure 10-15 Behavior Analysis Wizard Step 3



The next behavior analysis wizard page (see [Figure 10-15](#)) displays the application that triggered the event. This is the application the behavior analysis will investigate. Optionally, you can select other application classes to be analyzed. But in that case, the policy created would apply equally to all applications included in the analysis. For example, if the application class you are analyzing contains both Microsoft Word and Microsoft Outlook, the policy generated by the behavior analysis would be a combination of the resources required by both applications.

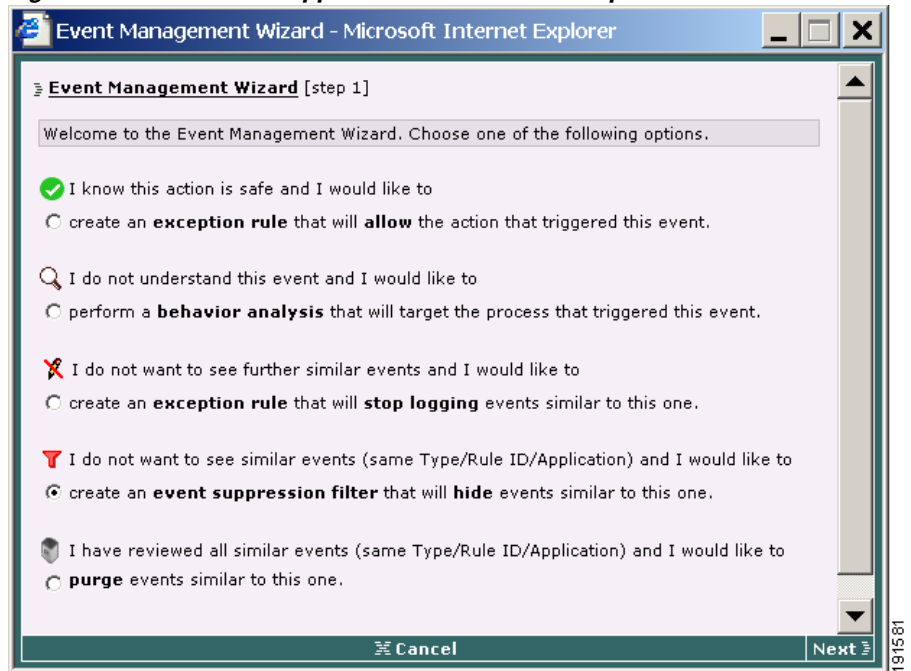
Continuing to click the **Next** button through the behavior analysis wizard configures the analysis with chosen defaults for analysis workstation and time frame. You can choose to edit these defaults or to accept them by making no changes.

When the wizard completes, it takes you to the new behavior analysis configuration page as it appears in CSA MC. You can edit it at this time or you can deploy the analysis by doing the following:

- **Generate rule programs** to distribute the behavior analysis to the host.
- Wait for the logging process to stop or click the **Stop logging** button to force the stop.
- Click the **Start analysis** button to start the analysis of the logged data.
- Optionally, use the **Import** button to import the policy, examine it and, if appropriate, deploy it to hosts.

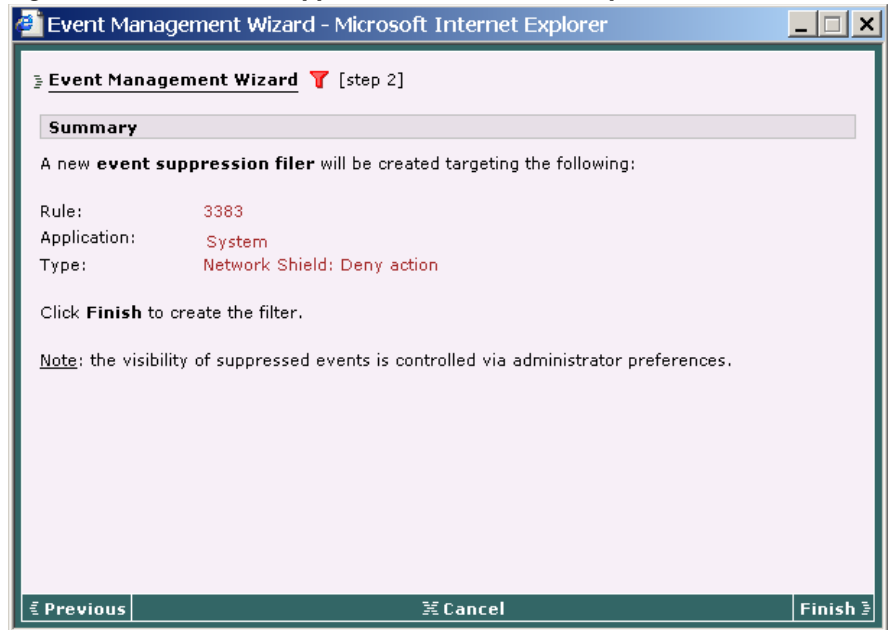
Create an Event Suppression Filter

When you click the **Wizard** link from the Event Log page, you can choose to create an event suppression filter based on the event from which you click the Wizard link (see [Figure 10-16](#)). Event suppression is best used when you have a reoccurring event that is more noisy than useful to you. This is something you are aware of, but no longer wish to see. Suppressing the event removes all viewable instances of that event and causes further events of the same type to be hidden. Note that these events remain in the database, they are simply not displayed.

Figure 10-16 Event Suppression Filter Wizard Step 1

Click the **Next** button through the event suppression wizard to configure the event filter with the chosen defaults.

Figure 10-17 Event Suppression Filter Wizard Step 2



191572

Click **Finish** to create the filter based on the criteria viewable in the Summary section, including Rule ID, Application, and Rule type.

View an Event Suppression Filter

Once you create the event suppression filter using the Wizard, that filter is viewable from a pop-up window accessible from the Show suppressed events: Yes <#> **event suppression filters defined** link at the top of the Event Log page. See [Figure 10-18](#).

Figure 10-18 Show suppressed events link

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

Address: https://biohazard/csamc52/webadmin

Management Center for Cisco Security Agents V5.2

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Log

16 events [change filter](#)

Event log generation time: 12/1/2006 2:33:21 PM
 Severity: Information - Emergency
 Host: All
 Rule Module: All
 Events per page: 50
 Sort by: Order received
 Filter out similar events: Yes (filtered out ~89% of 140 events)
 Show suppressed events: No [[1 event suppression filter defined](#)]

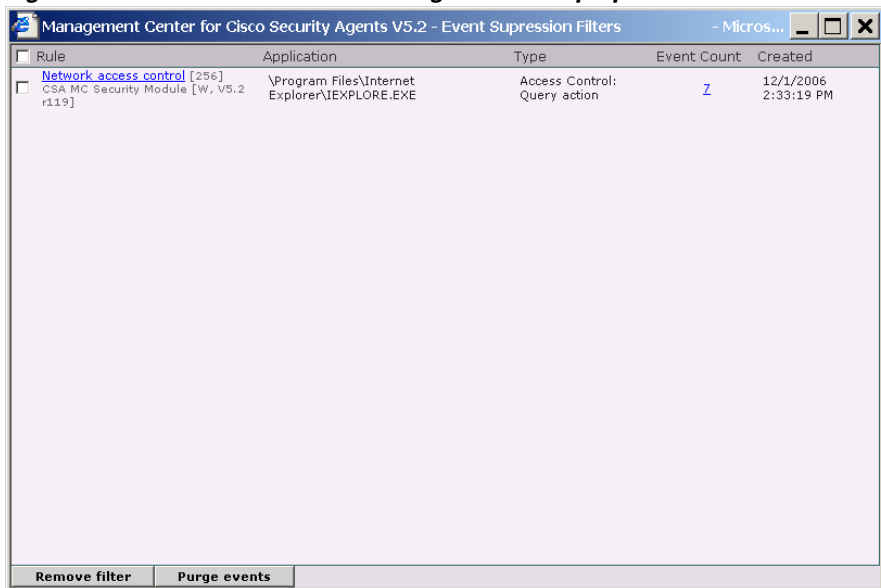
#	Date	Host	Severity	Event
16	12/1/2006 10:52:28 AM	-	Information	Administrator 'admin' logged in from 172.31.10.12 (S9). <i>3 similar events (same Type/Rule ID/Application)</i> Find Similar
15	12/1/2006 12:01:49 AM	-	Information	Application Deployment Analysis data has been purged and archived(if set) successfully. <i>2 similar events (same Type/Rule ID/Application)</i> Find Similar
14	11/30/2006 11:57:23 AM	biohazard	Notice	The process 'C:\Program Files\Cisco Systems\CSAgent\bin\okclient.exe' (as user BIOHAZARD\Administrator) attempted to access a resource which resulted in the user being asked the following question. 'An attempt is being made to disable security for the Cisco Security Agent. Do you wish to allow this?' The user was queried and a 'Yes' response was received. Details Rule 707 Wizard <i>1 similar event (same Type/Rule ID/Application)</i> Find Similar
13	11/30/2006 11:52:57 AM	biohazard	Information	The process 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user BIOHAZARD\Administrator) attempted to initiate a connection as a client on TCP port 80 to 10.86.189.238 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation was allowed. Details Rule 256 Wizard <i>5 similar events (same Type/Rule ID/Application)</i> Find Similar
12	11/30/2006 11:11:01 AM	biohazard	Alert	The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\LOCAL SERVICE) attempted to initiate a connection as a client on TCP port 139 to 172.31.10.90 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation was denied. Details Rule 287 Wizard <i>54 similar events (same Type/Rule ID/Application)</i> Find Similar
11	11/30/2006 10:58:52 AM	biohazard	Alert	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 172.31.10.90 using interface Wired3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible). The operation was denied.

[17 rule changes pending](#) [Generate rules](#) Logged in as: admin

Management Center for Cisco Security Agents V5.2 Local Intranet

When you click the Show suppressed event [<#> event suppression filters defined](#) link, a pop-up window appears from which you can either remove the filter to once again show all the events or purge all the events that have been filtered out. See [Figure 10-19](#).

Figure 10-19 Remove Filter or Purge Events Pop-up



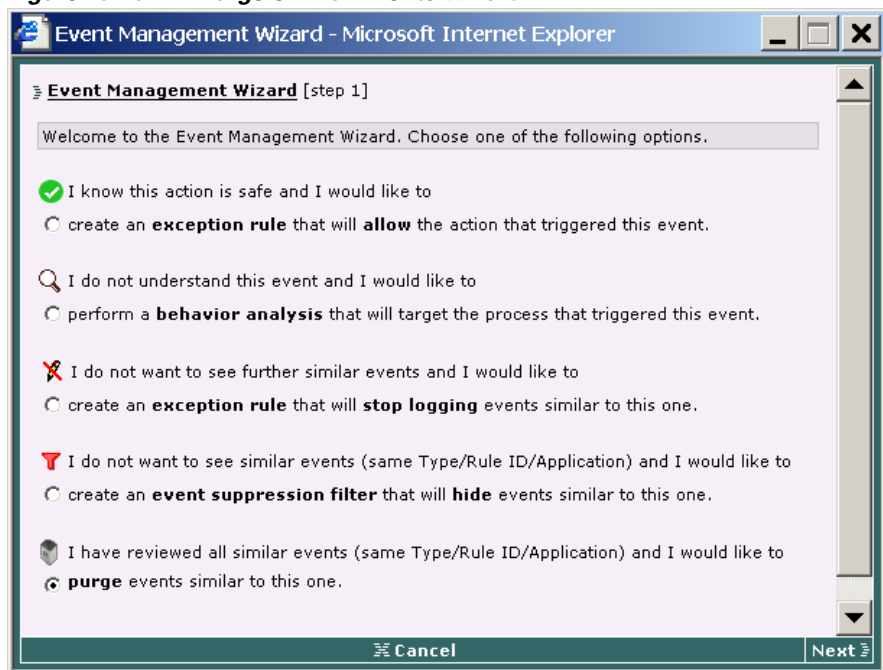
18/1568

Purge Similar Events

When you click the **Wizard** link from the Event Log page, you can choose to purge all similar events based on the event from which you click the Wizard link (see [Figure 10-20](#)). This purges all similar events but leaves one, most recent, representative event in the event log. All but one of these events are purged from the Event Log. Once purged, they cannot be recovered.

The wizard displays a representation of the events to be purged. Click Finish to purge the events.

Figure 10-20 Purge Similar Events Wizard



191579

Event Sets

Configure event sets for use in alerts, reports, and event logs. When configuring alerts, event sets cause CSA MC to trigger alerts based on specified events. Once configured, these event set configurations become available in corresponding alert selection fields.

**Note**

CSA MC ships with several preconfigured event sets you can use. If the included event sets do not suit your needs, use the instructions in the following pages to configure new event sets or to edit existing ones.

When creating your event sets, it's a good idea to adopt a naming convention that lets you quickly recognize event sets in your Alert configuration view.

**Note**

To learn more about how event sets are used for generating reports, see [Chapter 11, “Generating Reports”](#).

To configure event sets, do the following.

-
- Step 1** Move the mouse over **Events** in the menu bar of CSA MC. Select **Event Sets** from the drop-down list that appears. All existing event set configurations are shown.
- Step 2** Click the **New** button to create a new event set. This takes you to the configuration view.
- Step 3** In the available edit fields, enter the following information (see [Figure 10-21](#)):
- **Name**—This is a unique name for this event set. Generally, it's a good idea to adopt a naming convention that lets you quickly recognize Event Sets in Alert configuration fields.
 - **Description**—This is a line of text that is displayed in the list view and helps you to identify this particular Event Set configuration in the event set list view.

Under the **Event Specification** section, enter optional filtering parameters.



Note To select multiple items in a list box, hold down the Ctrl key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the Shift key to select multiple successive items.

Step 4 Select **Filter by event** specifications.

Leave the Include all event types radio button selected to have events of all types included or select the Include only the following selected event types radio button. If you select the second radio button, then you must also select specific event log messages to filter by. These messages represent the spectrum of generated events that appear in the Event Log view.

Step 5 Select **Filter by severity** specifications.

Leave the **Include all severity levels** radio button selected to have events of all severity levels included or select the **Include only the following selected severity levels** radio button. If you select the second radio button, then you must also select the severity level(s) that will trigger an alert for this event set. Available levels are: Information, Notice, Warning, Error, Alert, Critical, Emergency.

Step 6 Select **Filter by group** specifications.

Leave the **Include all hosts** radio button selected to have events generated by all hosts included or select the **Include only hosts in the following selected groups** radio button. If you select the second radio button, then you must select the group(s) that trigger an alert for this event set. Any groups selected here that log the event in question will trigger an alert.

Step 7 Select **Filter by rule module** specifications.

Leave the **Include all rule modules** radio button selected to have events generated by all rules modules included or select the **Include only rules in the following selected rule modules** radio button. If you select the second radio button, then you must select the rule module(s) that trigger an alert for this event set. Any rule modules selected here that log the event in question will trigger an alert.

Step 8 Select **Filter by time** specifications.



Note

If you do NOT have "Include all timestamps" selected, the Event Set is not available for use in Alerts.)

Leave the **Include all timestamps** radio button selected to have events generated at all times included or select the **Include only these timestamps** radio button. If you select the second radio button, then you can create a custom time here or select from available times, Today, Last 24 hours, Last 7 days, Last 30 days, and Events older than <you specify #> days to trigger an alert when an event occurs with the specified time range.

You can also enter **Custom start** and **Custom end** times in the following manner:

- Specify a relative time using any of the following terms: tomorrow, yesterday, today, now, last, this, next, ago, year, month, week, day, hour, minute, and second.
- Enter a specific time using any of the following time formats: hh:mm:ss. If no meridian (AM or PM) is specified, hh is interpreted on a 24 hour clock (0-23). Note that entering minutes and/or seconds is optional.
- Enter a specific month and day with optional year in the formats: mm/dd/yy, monthname dd, yy. The default year is the current year.



Note

When you select multiple categories to filter by, all selections have to match.

Step 9 When all required information is entered, click the **Save** button to enter and save your event set in the CSA MC database.

In the Event Sets configuration page, the CSA MC frame at the bottom of the page provides a **View** button and a **Purge events** button.

- When you click the **View** button, all events that match the configured event set are displayed.

**Caution**

When you click the **Purge events** button, all events that match the configured event set are deleted from the event log. If you make changes to an existing Event Set and click the Purge events button without saving those changes, all edits are saved and events are purged.

Figure 10-21 Event Set Configuration View

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://biohazard/csamc52/webadmin> Go Links

Management Center for Cisco Security Agents V5.2 Logout | Help | About

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Sets > Critical events of all types OTHER EVENT SETS

Name
Critical events of all types **Version**
5.2 r119

Description
Events with severity levels of Critical or higher

Event Specification

Include all event types
 Include only the following selected **event types**:
 @DYNAMIC: file added
 @DYNAMIC: ip address added
 Access Control - Query action
 Administrator account created
 Administrator account deleted

Include all severity levels
 Include only the following selected **severity levels**:
 Information
 Notice
 Warning
 Error
 Alert
 Critical
 Emergency

Include all hosts
 Include only hosts in the following selected **groups**:
 <All Linux> [L]
 Desktops - All types [L, V5.2 r119]
 Servers - All types [L, V5.2 r119]
 Servers - Apache Web Servers [L, V5.2 r119]
 Servers - Externally deployed [L, V5.2 r119]

Include all policy rules
 Include only rules in the following selected **rule modules**:
 Agent UI Module (Linux) [U, V5.2 r119]
 Agent UI Module (Solaris) [U, V5.2 r119]
 Apache Web Server (Generic Apache2 on Linux) [U, V5.2 r119]
 Apache Web Server (Red Hat Enterprise Linux) [U, V5.2 r119]
 Apache Web Server (Solaris) [U, V5.2 r119]

Include all timestamps
 Include only these **timestamps**:
 Custom Custom start time e.g.: 24 hours ago, mm/dd/yyyy
 Today
 Last 24 Hours Custom end time e.g.: 24 hours ago, mm/dd/yyyy
 Last 7 Days
 Last 30 Days

Save View Purge events Delete 17 rule changes pending Generate rules Logged in as: admin

Local intranet 191166

Third Party Access to Events

To access events in the database for exporting to a different format (or for your own reports), connect to the database using ODBC DSN "csame52dsn."

You can access events through the database view EventListView. (This is a SQL server view.) The columns defined in this view are as follows:



Note

SNMP and Log file alert types can be used by third party event management applications. See [page 10-46](#) for more details on those alert fields. (Note that the fields in the SNMP and Log file alerts are the same as those described in [Table 10-1](#).)

Table 10-1 *EventList View Fields*

Field	Description
EventId	An ID uniquely identifying the event. Increasing, in order of event arrival at CSA MC.
EventTime	The time at which the event occurred, using the clock of the host that generated the event.
HostId	An integer uniquely identifying the host that generated the event. This is NULL for events generated by CSA MC.
HostName	A non-unique string name for the host that generated the event.
HostOSType	The OS type for the host that generated the event, 'W' for Windows, 'U' for UNIX
CurrentHostIPAddress	The most recently recorded IP address for the host that generated the event.
SeverityCode	An integer, as follows in increasing severity -- Information (1), Notice (2), Warning (3), Error (4), Alert (5), Critical (6), Emergency (7)
SeverityName	The string representation of SeverityCode.
ProcessName	When applicable, the full path of the process that generated the event.
FileName	When applicable, the name (not path) of the relevant file from a file event.
SourceIPAddress	When applicable, the source IP address of a network event.

Field	Description
DestinationIPAddress	When applicable, the destination IP address of a network event.
RuleId	An integer uniquely identifying the rule that caused the event.
EventType	A string representing the type of the rule that caused the event, as discussed in Chapters 4 and 5. This field can be used as a broad-level categorization of CSA MC events. Possible values are as follows: File access control, Network access control, Network shield, Registry access control, System API control, Sniffer and protocol detection, File version control, COM component access control, Clipboard access control, Service restart, NT Event log, Application control, Agent service control, Agent UI control, Data access control, Connection rate limit, Analysis, Kernel protection, Network interface control, Rootkit / kernel protection, Buffer overflow, Syslog control, Resource access control, Downloaded content, Global virus scan, Global event log, Global network scan, Global email worm, Global IP address quarantine, Self-protection, Administrative.
RuleDescription	The user-specified string description for the rule that caused the event.
RuleModuleId	An integer uniquely identifying the rule module which contains the rule that caused the event.
RuleModuleName	The string name of the rule module which contains the rule that caused the event.
EventCode	An integer which uniquely defines the event code.
EventCodeTag	A short string representing the event code.
EventText	The complete formatted text of the event. (A Test Mode event is preceded by the string "TESTMODE".)
SourcePort	When applicable, the port used by the source of a network event.
DestinationPort	When applicable, the port used by the destination of a network event.
ButtonCode	The bottom 16 bits of this field represent the button that was pressed, with short integer values as follows, Yes (1), No (2), Terminate Process (3), OK (4). The upper 16 bits of this field represent whether the button was selected by default. A zero value indicates that the user actually pressed the button, while a non-zero value indicates that the default was chosen, e.g. because the query timed out.

Field	Description
Username	The name of the logged-in user at the time of the event.
RulePriority	The priority of the rule in question.

Configuring Alerts

You can configure CSA MC to send various types of alerts to specified recipients when a policy triggers an event. Available alert types include: Email, SNMP, Log to file, Named pipes and a Custom program that you provide.

Each alert type requires you to enter specific information. See [Table 10-2](#) for details.

To configure CSA MC to issue alerts when specified system events occur, do the following.

-
- Step 1** Move the mouse over **Events** in the menu bar and select **Alerts** from the drop-down list that appears. The list of Alerts (if any) appears.
 - Step 2** Click the **New** button to create a new alert. This takes you to the configuration view.
 - Step 3** In the Alert configuration view (see [Figure 10-22](#)), enter a **Name** and a useful **Description**. This information is displayed in the list view and helps you to identify this particular alert.
 - Step 4** From the **Send alerts for the following event set** list box, select the event set(s) you want to trigger the alert you're creating. Configuring Event Sets provides flexibility in selecting the events for which you want to be alerted.



Note The "time" filter in an event set is ignored for alerts. Alerts are generated as events are logged.

To select multiple items in a list box, hold down the **Ctrl** key as you select each item. To unselect a single item, hold down the Ctrl key when you click on the item in question. Press the **Shift** key to select multiple successive items.

If the available options here do not meet your needs, you can configure event set variables which become selectable in this field.

- Step 5** In the available alert configuration fields, enter data for *one or more* of the following alert types: Email, SNMP, Log, Named pipe, Custom (for alert configuration information, refer to [Table 10-2](#)).

For each alert type you want to send, select the corresponding **checkbox** and enter the required alert-specific information.



Note Although you can enter data into all available alert edit fields, if you do not check the corresponding checkbox, the alert in question is not enabled; however, the information you've entered is stored in the database. You can enable the alert type at a later time.

Step 6 When your information is entered, click the **Save** button to save your new alert(s).



Note Use the **Clear Pending Alerts** button to clear all alerts that have been triggered by events but not yet sent. You might want to do this if several events are occurring simultaneously or continuously, you have already disabled the alert, and you have no further need for the continual notifications that are pending.

Figure 10-22 Alert Configuration View

Management Center for Cisco Security Agents V5.2 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <https://biohazard/csamc52/webadmin> Go Links >>

Management Center for Cisco Security Agents V5.2 Logout | Help | About

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Alerts > Events from critical systems

Name
Events from critical systems

Description
Alert when critical system events are logged.

Send Alerts

For the following event sets:

- Critical events of all types [V5.2 r119]
- All events [V5.2 r119]
- All events of severity notice and lower [V5.2 r119]
- Analysis - Application Behavior [V5.2 r119]
- Analysis - Application Deployment [V5.2 r119]

(double-click event set to view)

Alert Method

Email

Recipient(s) email address(es)
jsmith@example.com

Sender address to use **Address of mail server**
biohazard@example.com 209.165.201.0

Message subject
Important message from Management Center for Cisco Security Age

SNMP

Community name

Manager IP address

Log

Log file

Custom

Custom program

Named Pipe

Named Pipe
\\pipe_____

Save Delete 17 rule changes pending Generate rules Logged in as: admin

Done Local intranet

191661

Table 10-2 Alert Type Descriptions

Alert Type	Information	Description
Email	Recipient	Enter the email address of the mail recipient. Using brackets is optional. CSA MC will automatically enter them if you do not. You can enter multiple addresses separated by commas: <dpaul@example.com>
	Sender address to use	Enter the mail sender in brackets. Some mail servers require this to be specified: <jsmith@example.com >
	Address of SMTP server	Enter the IP address or DNS name of the SMTP server.
SNMP	Community Name	Enter the community name. This is a text string agreed upon by the SNMP manager: <code>public</code>
	Manager IP Address	Enter IP address of the system where the SNMP trap should be sent. Optionally, you can put a colon and a port number (“:<port number>”) after the IP address if you are using a non-standard port. (Standard port is 162.) Refer to the CSAMC-SNMPv2.mib document in the CSAMC\CSAMC52\doc directory for SNMP-MIB definitions for Cisco specific objects. Also see Third Party Access to Events, page 10-40 for third party event management details.
Log	Log file name (using full path)	Enter a name for the flat logging file that events will be written to. <code>c:\alerts\logfile.txt</code> This file can then be used by third party event management applications. See Third Party Access to Events, page 10-40 for details. *In a distributed configuration, the path must correspond to the polling server system.

Alert Type	Information	Description
Custom	Custom Program	<p>Enter a custom alert program name here.</p> <p>The server calls the program as it appears in this field. You must enter the full pathname so that CSA MC can locate the program.</p> <p>Your custom program must be an executable file. c:\Program Files\Cisco Systems\CSAMC\CSAMC52\program.exe</p> <p>The program passes the event message in a file whose name is passed to the program as its first parameter. Alternately, the program can also read the event message from its standard input. The file containing the event is automatically deleted when the program exits or closes its standard input.</p> <p>FEATURE NOTES:</p> <ul style="list-style-type: none"> * The custom program must exist on the same system as CSA MC in the CSAMC52 directory or subdirectory. *Custom programs cannot require any user input. *If a custom program is triggered and fails for some reason, it could take several minutes before the program closes itself and attempts to launch again. (If you are testing custom program alerts, one way to tell if the program has launched and is running, is to watch for it in the Task Manager.) *In a distributed configuration, the path must correspond to the polling server system.
Named Pipe	Named Pipe	<p>A named pipe is a form of internal communication. This alert type allows the integration of third party software for the purpose of receiving alerts over Windows named pipes. Consult your third party documentation for further configuration details.</p> <p>Note that this feature is for use with third party vendors that support alerts over Windows named pipes.</p>

Generate an Alert Log File for Third Party Applications

Using the **Log** checkbox and the **Log file** edit field in the Alerts configuration page (see [Figure 10-22](#)), you can have CSA MC generate a flat logging file to which events are written. Third party event management applications can then parse the information found in this file.

To generate this file, select the Log checkbox and enter the Log file name, using the full path that you want to write event data to. For example, enter

```
c:\alerts\logfile.txt
```

Event data is written to this file as follows:

```
EventId,EventTime,HostId,HostName,  
CurrentHostIPAddress,HostOSType,Severity,EventType,  
EventText,EventCodeTag,FileName,ProcessName,  
SourceIPAddress,DestinationIPAddress,SourcePort,  
DestinationPort,RuleId,RuleDescription,RulePriority,  
RuleModuleId,RuleModuleName,ButtonCode,UserName
```

Entry fields are separated by a delimiter of a comma. Event entries themselves are separated by a carriage return/line feed (ASCII Hex 0D 0A).

Once a log file exceeds 1 MB, it is closed and its name is suffixed with a time stamp. A new file, using the same file name entered in the CSA MC Alerts Log file field, is then created. Events continue to be written to this new file until it reaches 1 MB. The third party application that consumes the log files is expected to manage the deletion and archiving of these files once processing is complete.



Note

This file data is encoded in UTF-8 format.
