



Generating Reports

Overview

You can configure the Cisco Security Agent to log an event each time a system action triggers a rule.

You can use the event logging data received from agents to generate reports that indicate overall network health. Using these reports, you can monitor how your current rule sets are working and adjust them, if necessary.

You can also generate reports related to configuration information.

This section contains the following topics.

- [Types of Reports, page 11-2](#)
- [Viewing Reports, page 11-2](#)
- [Generating Reports, page 11-3](#)
- [Events by Severity, page 11-3](#)
- [Events by Group, page 11-5](#)
- [Host Detail, page 11-6](#)
- [Policy Detail, page 11-8](#)
- [Group Detail, page 11-9](#)
- [About the ActiveX Crystal Report Viewer, page 11-10](#)

Types of Reports

CSA MC lets you generate reports using various criteria. For example, you can create reports based on event severity level, on the group that generated the event, and on the individual host systems producing events. You can sort by other parameters such as time frame, host, and event code that you configure separately.

Viewing Reports

When you generate your reports, you're given the option of selecting the type of viewer through which to display the report. From the Viewer type pulldown menu, you can select the following.

- **ActiveX:** The report viewer for ActiveX uses an ActiveX control that can be placed inside an HTML page and viewed through any browser that supports ActiveX. (Supported by Internet Explorer 3.02 and higher. Not supported by Netscape.) See [About the ActiveX Crystal Report Viewer, page 11-10](#) for more information.
- **HTML Frame:** This view is selected by default if you do not select a viewer type. Using this viewer, you can display reports in HTML using frames to illustrate category data in a left frame. (Supported by Internet Explorer 3.02 and higher and FireFox 1.5.0.x or higher.)

When you print reports, the formatting will vary depending on which view type you have selected and the printer settings on the printer you're using.

Generating Reports

You generate reports by selecting various sorting options in the CSA MC report configuration views. When you are finished selecting sorting parameters, you can generate your report. The report opens in a new browser window.

Events by Severity

You can generate reports using various selection and sorting criteria. In this case, you are creating a report based on event severity levels.

To generate an Events by Severity report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Severity** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Events by Severity report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** From the pulldown list, select an **Event Filter**. This is an Event Set you create from the Events> Event Sets configuration view (see [Event Sets, page 10-35](#)).
 - Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents (see [Figure 11-1](#)).
 - Step 6** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 7** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer. For more information, see [Viewing Reports, page 11-2](#).
 - Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 9** Click the **View Report** button and the report is automatically displayed in a new browser window.

Figure 11-1 Events by Severity Report Configuration

The screenshot shows the Management Center for Cisco Security Agents V5.1 web interface in Microsoft Internet Explorer. The browser address bar shows `https://biohazard/csamc51/webadmin`. The page title is "Management Center for Cisco Security Agents V5.1" and the breadcrumb navigation is "Reports > Events by Severity > IIS Events by severity".

The configuration form includes the following fields:

- Name:** IIS Events by severity
- Description:** IIS Events by severity report
- Criteria:**
 - Event Filter: All events in the last 24 hours [V5.1 r32]
 - Sort by: Time (Ascending)
 - Filter out similar events: Yes
 - Viewer type: ActiveX (IE only)

At the bottom of the form, there are buttons for "Save", "View report", and "Delete". A status bar indicates "No rule changes pending" and a "Generate rules" button. The user is logged in as "admin".

Events by Group

You can generate reports using various selection and sorting criteria. In this case, you are creating a report based on the groups that have generated the events.

To generate an Events by Group report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Events by Group** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Events by Group report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** From the pulldown list, select an **Event Filter**. This is an Event Set you create from the Events> Event Sets configuration view (see [Event Sets, page 10-35](#)).
 - Step 5** From the **Sort by** pulldown list, select a parameter for sorting this report's contents.
 - Step 6** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 7** Select a **Viewer type**. By default, ActiveX is selected. This is the recommended viewer. For more information, see [Viewing Reports, page 11-2](#).
 - Step 8** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 9** Click the **View Report** button and the report is automatically displayed in a new browser window.

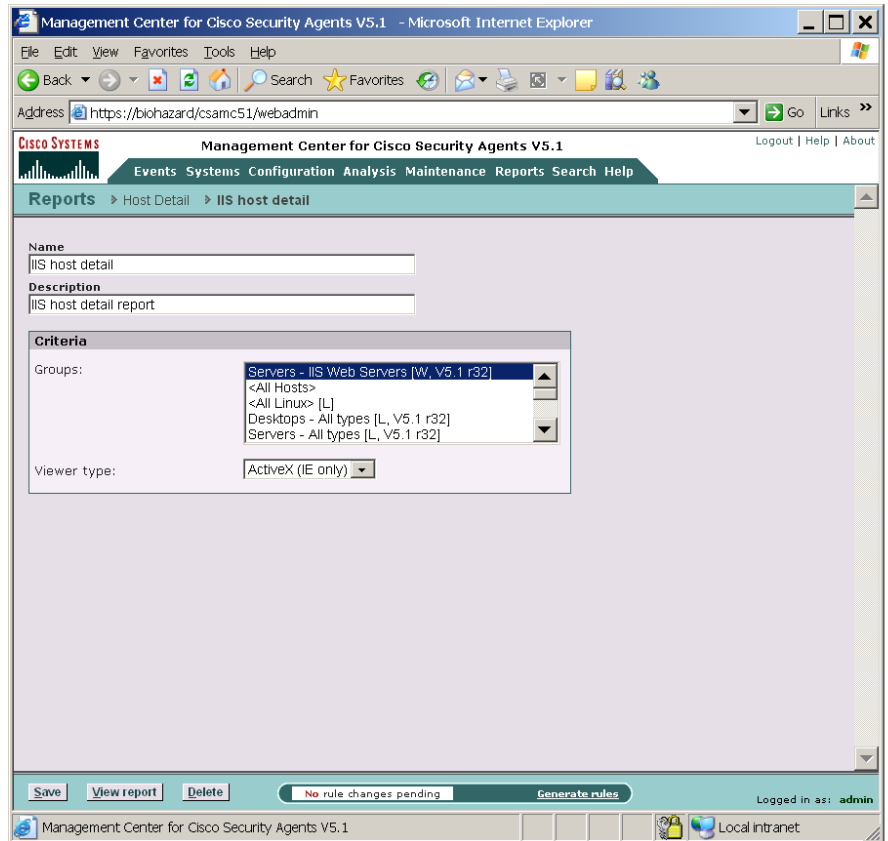
Host Detail

You can generate reports based on hosts in specific groups you select as part of the report. A host detail report provides in-depth information on the hosts in the groups you select for the report.

To generate a host detail report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar of CSA MC. Select **Host Detail** from the drop-down list that appears. Any existing reports are shown.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Host Detail report configuration view (see [Figure 11-2](#)), enter a **Name** and a **Description** for the report.
 - Step 4** Select the **Groups** for which you want to generate a report. 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. You can also select **All Hosts** here to generate a report for all registered hosts.
 - Step 5** By default, **ActiveX** is selected as the **Viewer type**. This is the recommended viewer. For more information, see [Viewing Reports, page 11-2](#).
 - Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 7** Click the **View Report** button and the report is automatically displayed in a new browser window.

Figure 11-2 Host Detail Report Configuration



Policy Detail

You can generate reports by selected policies. A policy report provides in-depth information on the policies you select for the report.

To generate a policy detail report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar and select **Policy Detail** from the drop-down list that appears.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Policy Detail report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** Select the **Policies** for which you want to generate a report. 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 and hold the **Shift** key to select multiple successive items.
 - Step 5** By default, ActiveX is selected as the **Viewer type**. This is the recommended viewer. For more information, see [Viewing Reports, page 11-2](#).
 - Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 7** Click the **View Report** button. Your report is created and is automatically displayed in a new browser window.

Group Detail

You can generate reports by a selected group or groups. A group report provides in-depth information on the groups you select for the report.

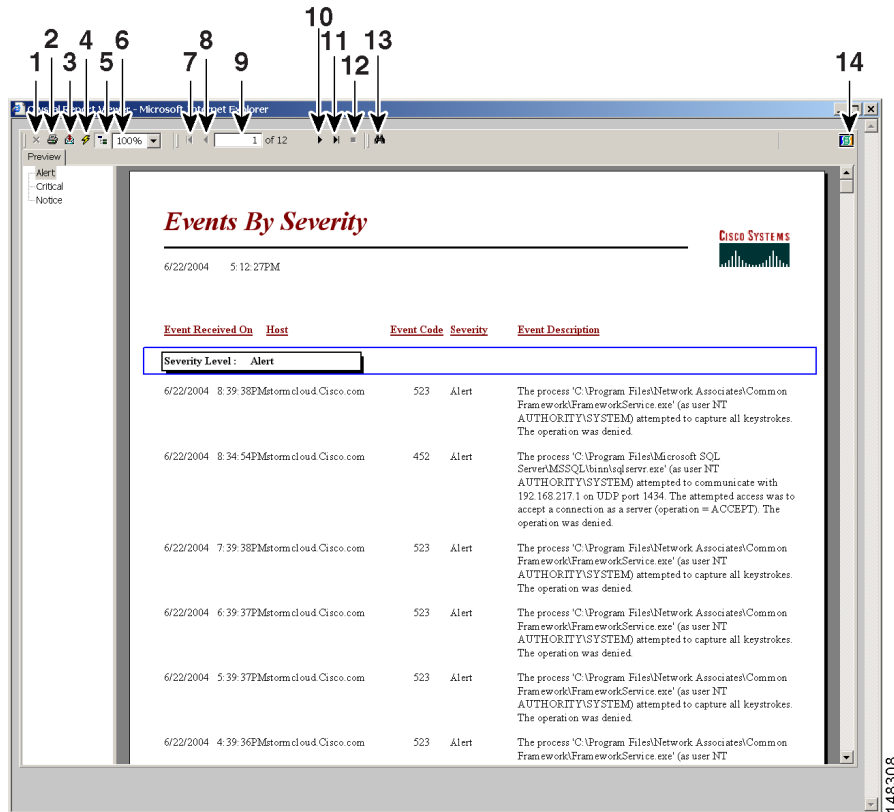
To generate a group detail report, do the following.

-
- Step 1** Move the mouse over **Reports** in the menu bar and select **Group Detail** from the drop-down list that appears.
 - Step 2** Click the **New** button to create a new report. This takes you to the configuration view.
 - Step 3** In the Group Detail report configuration view, enter a **Name** and a **Description** for the report.
 - Step 4** Select the **Groups** for which you want to generate a report. 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 and hold the **Shift** key to select multiple successive items.
 - Step 5** By default, ActiveX is selected as the **Viewer type**. This is the recommended viewer. For more information, see [Viewing Reports, page 11-2](#).
 - Step 6** Click the **Save** button to save the parameters you've just configured for generating this report.
 - Step 7** Click the **View Report** button. Your report is created and is automatically displayed in a new browser window.

About the ActiveX Crystal Report Viewer

The report viewer for Active X reports contains elements that allow you to print, export, and search reports.

Figure 11-3 Crystal Report Viewer



Descriptions of the viewer button controls are as follows:

1. Close current view: This X button is generally grayed out unless a drill down item has been viewed. When active, this button allows you to close the drill down preview.

2. **Print:** This button allows you to print the report. When you click the button, a print setup window appears. From there, you can change the page setup of the report and select the print range.
3. **Export report:** The envelope button with the red arrow line allows you to export reports. This export utility lets you export reports to four file format choices (providing the applications for those formats are installed on the client system).

To export a report, click the Export button and the "Crystal Smart Viewer Export" window appears. Select where you want to save the exported file to from the **Save in** field pulldown arrow. Then enter a name for the exported file in the **File name** field. From the **Save as type** pulldown field, select the format to save the report as. The choices are: Crystal Report, Rich Text Format, Word Document, and Excel Document.

When you've made your format selection, click the **Save** button. A progress box lets you know the report is being exported.

4. **Refresh:** The refresh button is the one with the lightning bolt on it. When you click this button, a message is sent to the server to repopulate the report with fresh data.
5. **Toggle group tree:** The toggle group tree (navigation button) appears as a miniature directory tree. Clicking this button causes the left pane of the viewer to appear or disappear.
6. **Zoom control:** This control lets you set the magnification control of the viewer. You can select levels from the pulldown menu or you can enter your own numbers here.
7. **Go to first page:** Clicking the "Go to first page" control arrow takes you to the first page of the report. (When you are on the first page, this arrow is grayed out.)
8. **Go to previous page:** Clicking the "Go to previous page" control arrow takes you to the page of the report that is directly before the page you are currently viewing.
9. **Current page out of total pages viewed:** The number that appears in this field is the number of the page that is currently displayed. If your report has several pages, this number is followed by the word "of" and another number indicating the total number of pages in the report. This field can also function as a "go to" control. Entering a number in this field and pressing the Enter key takes you to that page in the report.

10. Go to next page: This right facing arrow button, when clicked, takes the viewer to the page immediately following the current page being viewed.
11. Go to last page: This right facing arrow button touching a vertical line, when clicked, takes the viewer to the last page of the report.
12. Stop loading: This button is generally grayed out. It contains a solid square in the middle and is only active when a report is loading. Clicking this button stops the report from loading in the window but it does not stop the report from continuing to be processed on the CSA MC system.
13. Search text: Clicking this button (with binoculars on it) allows you to search for any specific text, number, or character in the report. After entering the information you're searching for and clicking the "Find next" button, any matching items in the report are enclosed in a red-lined box.
14. Logo box: This box in the upper right corner of the viewer contains the viewer logo. This logo appears as a graphical rotating image when the viewer is busy loading.