



CHAPTER 11

Generating Reports

Overview

Cisco Security Agents log an event each time a system action triggers a rule. You can use the event logging data received from agents to generate reports. Using these reports, you can monitor how your current rule sets are working and adjust them, if necessary.

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 11-4](#)
 - [Group Detail, page 11-5](#)
 - [Host Detail, page 11-5](#)
 - [Policy Detail, page 11-6](#)
 - [Clam AntiVirus Reports, page 11-6](#)
 - [Data Loss Prevention Reports, page 11-10](#)
 - [Signature Information Detail, page 11-13](#)
 - [Trend Chart Reports, page 11-16](#)
 - [Management Summary Reports, page 11-17](#)

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 reports, you are given the option of selecting the type of viewer in which to display the report. From the Viewer type pulldown menu, you can select PDF or HTML.

- **PDF:** This option will generate the complete report as a PDF file that can be viewed, printed, and saved using the browser PDF plug-in. If you do not have a PDF plug-in installed on your browser, you will have to install a PDF browser plug-in to view this report type. We recommend that you use the most recent version of Adobe Reader to view the reports.
- **HTML:** This option breaks the report into individual HTML pages which can be viewed one page at a time in a browser window. Only the currently viewed report page can be printed. (Supported by Internet Explorer 6.0 or 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.



Note

When you print reports, it is recommended that you print using Landscape mode. Reports do not print correctly using Portrait mode.



Caution

CSA MC requires and installs Sun JRE (Java Runtime Environment) to generate reports using the Jasper reporting tool. If you remove the Java directory from the CSA MC system, you cannot generate reports.

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.

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.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Events by Severity**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** From the **Event Filter** pulldown list box, select an event set from which to generate the report. The list contains event sets provided by default with this release and event sets that you have created. If you want to create a new event set from which to generate a report, click the blue **New** link next to the pulldown list box. See [Event Sets, page 10-25](#) for more information.
 - Step 7** From the **Sort by** pulldown list box, select a parameter for sorting this report's contents: **Time**, **Host** or **Event Code**.
 - Step 8** In the **Filter out similar events** box, select **Yes** to filter out similar events from the report or **No** to include all events. "Similar events" have the same rule ID, are of the same event type, and are reported for the same application. For the purpose of grouping similar events, CSA MC ignores the drive letter or share name of the application.
 - Step 9** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the "[Viewing Reports](#)" section on page 11-2 for information more information about these output choices.
 - Step 11** Click the **Save** button to save the parameters you just configured for this report.
 - Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

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.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Events by Group**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** From the **Event Filter** pulldown list box, select an event set from which to generate the report. The list contains event sets provided by default with this release and event sets that you have created. If you want to create a new event set from which to generate a report, click the blue **New** link next to the pulldown list box. See [Event Sets, page 10-25](#) for more information.
 - Step 7** From the **Sort by** pulldown list box, select a parameter for sorting this report's contents: **Time**, **Severity** or **Event Code**.
 - Step 8** Enable or Disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 9** In the **Filter out Similar events** pull-down list, select **Yes** or **No**.
 - Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
 - Step 11** Click the **Save** button to save the parameters you just configured for this report.
 - Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new 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.

-
- Step 1** Log on to the CSA MC as any user and switch to **Advanced Mode**.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Group Detail**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** 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 7** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
 - Step 8** Click the **Save** button to save the parameters you just configured for this report.
 - Step 9** Click the **View Report** button. Your report is created and is automatically displayed in a new 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.

-
- Step 1** Log on to the CSA MC as an user. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Host Detail**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** 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 7** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
 - Step 8** Click the **Save** button to save the parameters you just configured for this report.
 - Step 9** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Policy Detail

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

-
- Step 1** Log on to the CSA MC as any user and switch to **Advanced Mode**.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Policy Detail**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** 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 7** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
 - Step 8** Click the **Save** button to save the parameters you just configured for this report.
 - Step 9** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Clam AntiVirus Reports

These reports provide information about the age of signature files on hosts and the number of infected hosts in the deployment. These are the AntiVirus reports available:

- AntiVirus Update
- AntiVirus Summary
- Restored Infection Details
- Virus Infections
- Virus Infections Details

Creating an AntiVirus Update Detail Report

This report shows how old signature files are on hosts in a group. The bar chart breaks down the number of hosts using signatures that are older than X days.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **AntiVirus > AntiVirus Update**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.

- Step 6** In the Criteria area, select a **Host Filter** from the drop down menu. The report will include all the hosts described by the selection in the Host Filter drop down menu. Only one Host Filter can be applied to one report.
- Step 7** In the Group Filter area, select one of these two radio buttons:
- **No Group Filter** - if you do not want to restrict your reports to hosts in certain groups.
 - **Groups Matching** - if you do want to restrict your report to hosts in certain groups. You may pick one or more groups from the Groups Matching menu.
- Step 8** From the **Sort by AV Update Date** menu select ascending or descending.
- Step 9** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
- Step 10** Click the **Save** button to save the parameters you just configured for this report.
- Step 11** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Creating an AntiVirus Summary Report

This report can identify the most frequently occurring virus infections and the most infected hosts in your enterprise. The **Top 10 Infected Hosts** and the **Top 10 Virus Infections** reports are provided by default. To create your own report, follow this procedure:

-
- Step 1** From the CSA MC menu bar, mouseover **Reports** menu, navigate **AntiVirus > AntiVirus Summary**. Any existing reports are shown.
- Step 2** Click the **New** button to create a new report. This takes you to the report’s configuration view.
- Step 3** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 4** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 5** From the **Report type** list box, select the kind of report you want to create.
- Step 6** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 7** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
- Step 8** Click the **Save** button to save the parameters you just configured for this report.
- Step 9** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Creating a Restored Infection Details Report

This report provides administrators with a list of files which have been tagged with signature-based or behavior-based AntiVirus tags but that users have chosen to remove from quarantine through their local agent interface. This report allows an administrator to identify trends in these restored files. For example, if the same file is being restored by many users in one particular group, then an exception may be warranted for this file.

The report identifies the name of the virus that was found, the file that was restored, the user that restored the file, the host on which the file was restored, and the time at which the file was restored.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.

- Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **AntiVirus > Restored Infection Details**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 7** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check **All times** if you do not want to limit the time frame of the report.
- You can specify the **From** and **Until** parameters in these ways:
- 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.
 - You can 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.
 - You can 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.
- Step 8** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
- Step 9** Click the **Save** button to save the parameters you just configured for this report.
- Step 10** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Creating Virus Infections Reports

The **Virus Infections report** graphically displays the number of infected files found on a host. You can configure the report to sort the information by tag or by host.

The information in the report is based on the events passed from the agents to the CSA MC when the agents last polled. The information from the latest polling event overwrites the information from the previous polling event.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **AntiVirus > Virus Infections**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 7** If you know the name of the virus you want to search for, enter it in the **Virus Name** field, otherwise leave the * entry to search for all viruses.

To obtain a virus name:

1. Launch the CSA interface on a host infected with the virus.

2. Click the **AntiVirus** task button.
 3. Click the **Quarantined** files tab.
 4. Look in the **Virus name** field for the virus's name.
- Step 8** You can choose to group the report output by **Host Name** or **Virus Name** by selecting one or the other in the **Group by** field.
- Step 9** Select **Order by number of infections** if you would like the report presenting the viruses with the highest number of occurrences first.
- Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
- Step 11** Click the **Save** button to save the parameters you just configured for this report.
- Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Creating Virus Infections Details Reports

The **Virus Infection Details** report lists the locations of infected files. The information in the report is derived from events, generated by a scan event log rule that is set to “monitor” or “notify.” These events are collected by the CSA MC. This information can be sorted by host or by virus.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **AntiVirus > Virus Infection Details**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Groups matching** field, select the group, or groups, which you want to include in this report.
- Step 7** If you know the name of the virus you want to search for, enter it in the **Virus Name** field, otherwise leave the * entry to search for all viruses.
- To obtain a virus name:
1. Launch the CSA interface on a host infected with the virus.
 2. Click the **AntiVirus** task button.
 3. Click the **Quarantined** files tab.
 4. Look in the **Virus name** field for the virus's name.
- Step 8** Specify the time frame for the report by entering the **From** and **Until** parameters in the Time Frame area. Alternatively, you may check **All times** if you do not want to limit the time frame of the report.
- You can specify the **From** and **Until** parameters in these ways:
- 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.
 - You can 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.

- You can 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.
- Step 9** You can choose to group the report output by **Host Name** or **Virus Name** by selecting one or the other in the **Group by** field.
- Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
- Step 11** Click the **Save** button to save the parameters you just configured for this report.
- Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Data Loss Prevention Reports

Data Loss Prevention reports can be generated for any host that is running a data loss prevention policy. To use this policy, the CSA MC has to have an available data loss prevention license for that host.

These procedures create reports describing files that have been tagged with scanning data tags or static data tags.

- [Creating Data Discovery Reports, page 11-10](#)
- [Creating a Data Justification Details Report, page 11-11](#)
- [Creating a Protected Data Movement Report, page 11-12](#)

Creating Data Discovery Reports

The Data Discovery report graphically displays the number of files, with a particular scanning data tag or static data tag, found on the fixed local drives of a host. You can configure the report to sort the information by tag or by host.

The information in the report is based on the events passed from the agents to the CSA MC when the agents last polled. The information from the latest polling event overwrites the information from the previous polling event.

Data Loss Prevention reports can be generated for any host that is running a data loss prevention policy. To use this policy, the CSA MC has to have an available data loss prevention license for that host.

Reports for Credit card and SSN information and Sensitive data details are provided for you by default.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **Data Loss Prevention > Data Discovery**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report’s configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Groups matching** field, select the group which you want to include in this report. You may choose more than one group. You may also choose <All Groups>.
- Step 7** In the **Tags matching** field, select the tag, or tags, for which you want to create a report. You may also choose <All tags>.

- Step 8** Choose to group the report output by **Host Name** or **Tag Name** by selecting one of those items from the **Group by** field. If you select **Host Name**, the report displays one pie chart, per host, per report page. The name of the data tags and the number of files with that tag are listed below the chart. If you select **Tag Name**, the report is a bar chart indicating the tag and the number of files with that tag. The host name and number of files with that tag are listed below the chart.
- Step 9** Select **Order by number of tags** if you would like the report presenting the tags with the highest number of occurrences first.
- Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about these output choices.
- Step 11** Click the **Save** button to save the parameters you just configured for this report.
- Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Creating a Data Justification Details Report

The **Data Justification Details report** reports the explanations users provide when acting on files tagged with scanning data tags or static data tags.

Data Justification Details reports can be generated for any host that is running a data loss prevention policy and that is using at least one scan event log rule or file access control rule that queries or notifies the user and asks for a justification of their action. (See [Scan Event Log](#), page 6-47 for more information.) The host must also have a data loss prevention license assigned to it.

The Data Justification Details report lists the date of the justification, the username that was prompted for the justification, the application that was acting, the file on which the application was acting, and the justification message if one was provided.



Note If a host is part of a group which is configured to filter user info from events, the username will not appear in the report.

- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and **Data Loss Prevention > Data Justification Details**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report’s configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Groups matching** field, select the group which you want to include in this report. You may select more than one group. You may also choose <All Groups>.
- Step 7** In the **Tags matching field**, select the tag, or tags, for which you want to create a report. You may also choose <All tags>.
- Step 8** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check **All times** if you do not want to limit the time frame of the report. You can specify the **From** and **Until** parameters in these ways:
- 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.

- You can 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.
 - You can 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.
- Step 9** Choose to group the report output by **Host Name** or **Tag Name** by selecting one of those items from the **Group by** field. If you select Host Name, the report lists the directory locations of tagged files grouped by host and then by tag. If you select Tag Name, the report lists the directory locations of the tagged files grouped by tag and then by host.
- Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about these output choices.
- Step 11** Click the **Save** button to save the parameters you just configured for this report.
- Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Creating a Protected Data Movement Report

Protected Data Movement reports gather information generated by monitoring events and notification events of Scan Event Log Rules (SACLs). These events are triggered if the SACL detects a user performing a file operation on a file with a data loss prevention tag.

The Protected Data Movement report shows which files, with data tags, were accessed. This report can be sorted by host or by tag name.

Protected Data Movement reports can be generated for any host that is running the Data Loss Prevention policy and that is using at least one scan event log rule that monitors events or notifies the user of file movement.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and nativity **Data Loss Prevention > Protected Data Movement**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report’s configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Groups matching** field, select the group which you want to include in this report. You may choose more than one group. You may also choose <All Groups>.
- Step 7** In the **Tags matching** field, select the tag, or tags, for which you want to create a report. You may also choose <All tags>.
- Step 8** Specify the time frame for the report by entering the **From** and **Until** parameters in the **Time Frame** area. Alternatively, you may check **All times** if you do not want to limit the time frame of the report. You can specify the From and Until parameters in these ways:
- 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.
 - You can 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.

- You can 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.
- Step 9** Choose to group the report output by **Host Name** or **Tag Name** by selecting one of those items from the Group by field. If you select Host Name, the report lists the directory locations of tagged files grouped by host and then by tag. If you select Tag Name, the report lists the directory locations of the tagged files grouped by tag and then by host.
- Step 10** In the **Viewer type** field, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about these output choices.
- Step 11** Click the **Save** button to save the parameters you just configured for this report.
- Step 12** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Signature Information Detail

You can generate reports related to the automatic signature generation feature. Signature reports provide in-depth information on these signature details:

- [Denial of Service Detail](#)
- [Filtering Detail](#)
- [Generation Detail](#)

Denial of Service Detail

Denial of service (DoS) detail reports the number of times payloads have been associated with the @highrisk_signatures token.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **Signatures > DoS Detail**. Any existing reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report’s configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Time Frame** area, specify the time period that the report should address in the **From** and **Until** fields. Alternatively, you may check **All times** if you do not want to limit the time frame of the report. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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.

- Step 7 In the **Viewer type** field, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about these output choices.
- Step 8 Click the **Save** button to save the parameters you just configured for this report.
- Step 9 Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Filtering Detail

Filter Detail reports describe the number of times CSA acted as a result of a matching an attack payload to an existing signature.

-
- Step 1 Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and navigate **Signatures > Filtering Detail**. Any existing reports are shown.
 - Step 3 Click the **New** button to create a new report. This takes you to the report’s configuration view.
 - Step 4 In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5 If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6 Select an **Event Filter** from the drop down menu list.
 - Step 7 From the **Sort by** pulldown list, select a parameter for sorting this report’s contents.
 - Step 8 Enable or disable the **Ascending** checkbox depending on the order in which you want to view your reports.
 - Step 9 Choose whether or not to remove similar events from the report by choosing Yes or No in the **Filter out Similar Events** field.
 - Step 10 In the **Time Frame** area, specify the time period that the report should address in the **From** and **Until** fields. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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.

Or you can select **All times** checkbox if you do not want to limit the time frame of the report.
 - Step 11 In the **Viewer type** field, select **PDF** or **HTML** output. See the “[Viewing Reports](#)” section on page 11-2 for information more information about these output choices.
 - Step 12 Click the **Save** button to save the parameters you just configured for this report.
 - Step 13 Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Generation Detail

Generation Detail reports identify the number of times CSA correlated a signature.

-
- Step 1** Log on to the CSA MC as any user. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and navigate **Signatures > Generation Detail**. Any existing reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** In the **Signature Type** field select **Local** or **Global**.
 - Step 7** For **Local** signature generation details, provide a **Correlation start time** and **Correlation end time**. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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.
 - Global** signature details are not defined by Correlation Start and End Times.
 - Step 8** In the **Sort by Sig update time** field, select **Ascending** or **Descending**.
 - Step 9** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about these output choices.
 - Step 10** Click the **Save** button to save the parameters you just configured for this report.
 - Step 11** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Trend Chart Reports

Creating Hosts by Events Reports

This report identifies the hosts that have generated the most or least number of events, throughout your deployment, in a particular time frame.

-
- Step 1 Log on to the CSA MC as a user with any level of privileges and switch to **Advanced Mode**.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and navigate **Trend Charts > Hosts by Events**.
 - Step 3 Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4 In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5 If you would like to place a link to this report in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6 In the **Number of Hosts** fields, select **Top** for the hosts with the most number of events or select **Bottom** for the hosts with the least number of events. Then, select the number of hosts for which you want to generate this report.
 - Step 7 Specify the time frame for the report by entering the starting time in the **Date From** field and the ending time in the **Date Until** fields. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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.
 - Step 8 In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about PDF and HTML output choices.
 - Step 9 Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 10 Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Hosts by Delta Events

This report identifies the hosts that have been reporting the greatest increase in events over the specified time period and the hosts that have been reporting the greatest decrease in events over the specified time period. This report measures the difference in number of reported events by subtracting the events reported on the **Date on** time from those reported on the **And** time; the report does not consider events reported in between the two times.

-
- Step 1 Log on to the CSA MC as a user with any level of privileges and switch to **Advanced Mode**.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and navigate **Trend Charts > Hosts by Delta Events**.
 - Step 3 Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4 In the configuration view, enter a **Name** and a **Description** for the report.

- Step 5** If you would like to place a link to this report in the **Favorite Reports** section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the **Number of Hosts** fields, select **Top** to identify the hosts with the greatest increase in number of events or select **Bottom** to identify the hosts with the greatest decrease in number of events over the time period.
- Step 7** Specify the time frame for the report by entering the starting time in the **Date On** field and the ending time in the **And** fields. 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 specify a relative time using any of the following terms: tomorrow, yesterday, today, now, next, ago, year, month, week, day, hour, minute, and second.
 - You can 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.
 - You can 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.
- Step 8** In the **Viewer type** field, select **PDF** or **HTML** output. See the [“Viewing Reports” section on page 11-2](#) for information more information about PDF and HTML output choices.
- Step 9** Click the **Save** button to save the parameters you just configured for generating this report.
- Step 10** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Management Summary Reports

Management Summary reports are designed to provide administrators with the information they need most often. They are brief targeted reports, no more than a page in length.

The reports can be generated in HTML or in PDF formats. These are the Management Summary Reports provided with this release:

- [Daily Events by Event Type](#). Use this report to view trends in the number of triggered events from different types of rules.
- [Events by Enforcement Action Over Time](#). Use this report to view trends in the number and type of enforcement actions reported throughout your deployment.
- [Host Count Summary](#). Use this report to see total numbers of hosts reporting different statuses, broken down by group and operating system.
- [Queried Events by Response Type Over Time](#). Use this report to view trends in the number and type of user responses to queries reported throughout your deployment.
- [Summary of Queried Events by Response Type Over Time](#). Use this report to view total numbers and types of user responses to queries reported throughout your deployment.
- [Summary of Events by Enforcement Action](#). Use this report to view total numbers and types of enforced actions reported throughout your deployment.
- [Top 20 Infected Hosts](#). Use this report to view the 20 hosts infected with the most number of viruses, found by CSA AV, throughout your CSA deployment. The report could include signature-based viruses, behavior-based viruses, and Potentially Unwanted Applications (PUAs).
- [Top 20 Identified Viruses](#). Use this report to view the 20 most frequently occurring viruses, found by CSA AV, throughout your CSA deployment. The report could include signature-based viruses, behavior-based viruses, and Potentially Unwanted Applications (PUAs).

Daily Events by Event Type

Use this report to view trends in the number of triggered events, from different types of rules, over time.

A pre-configured Daily Events by Event Type Over Time report is provided with this release. The report provides the number of triggered events for Agent Service Control rules, Application Control Rules, File Access Control rules, and Network Access control rules for Windows operating systems during the previous week. The report is displayed in HTML.

To view the report provided, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3** Click the link to the **Daily Events by Event Type** report.
 - Step 4** Click **View** report.

To create a new report, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** In the Select Report Type list box, select **Daily Events By Event Type**.
 - Step 7** In the Select Rule Types list box, select up to five rule types for which you want to see event information. You can specify rules for UNIX and Windows operating systems in the same report.
 - Step 8** In the **Start Date** and **End Date** fields, enter the beginning and ending dates for this report. The report can span one to seven days. The time frame must indicate whole days. You can specify the Start Date and End Date parameters in these ways:
 - You can specify a relative time using any of the following terms: tomorrow, yesterday, today, next, ago, week, and day.
 - You can 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.
 - Step 9** In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 10** Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 11** Click the **View Report** button. Your report is created and is automatically displayed in a new window.



Tip

If the report identifies event activity that you want to investigate further, you could create an event set, specifying the event types for the rules you specified in the report. This will give you more information about the events, actions, and hosts involved.

Events by Enforcement Action Over Time

Use this report to view trends in the number and type of enforcement actions reported throughout your deployment. The report allows you to look at this information over time.

A pre-configured Events by Enforcement Action Over Time report is provided with this release. The report provides information on one week of events and it is displayed in HTML.

To view the report provided, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3** Click the link to the **Events by Enforcement Action Over Time** report.
 - Step 4** Click View report.

To create a new report, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** In the Select Report Type list box, select **Events by Status Type Over Time**.
 - Step 7** In the Select Enforcement Action list box, select up to five enforcement actions for which you want to see event information.
 - Step 8** In the **Start Date** and **End Date** fields, enter the beginning and ending dates for this report. The report can span one to seven days. The time frame must indicate whole days. You can specify the Start Date and End Date parameters in these ways:
 - You can specify a relative time using any of the following terms: tomorrow, yesterday, today, next, ago, week, and day.
 - You can 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.
 - Step 9** In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 10** Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 11** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Host Count Summary

Use this report to see total numbers of hosts reporting different statuses, broken down by group and operating system. Hosts that are members of groups that are “hidden” will not be counted in this report.

A pre-configured Host Count Summary report is provided with this release. The report provides information on hosts in all group with these status types: Active, Audit Mode, Disabled, Latest Software, and Learn Mode. The report is displayed in HTML.

To view the report provided, follow this procedure:

-
- Step 1 Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3 Click the link to the **Host Count Summary** report.
 - Step 4 Click View report.

To create a new report, follow this procedure:

-
- Step 1 Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3 Click the **New** button to create a new report. This takes you to the report’s configuration view.
 - Step 4 In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5 If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6 In the Select Report Type list box, select **Host Count Summary**.
 - Step 7 In the Groups matching field, select any number of groups for which you want to run the report.
 - Step 8 In the Select Host Status Types list box, specify up to 5 host statuses that you want to include in the report.
 - Step 9 In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 10 Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 11 Click the **View Report** button. Your report is created and is automatically displayed in a new window.



Tip

Once you have the results of your report, you can locate the hosts by performing a host search and tailoring the search for status, operating system, or group. See [Searching for Hosts, page 3-24](#) for more information.

Queried Events by Response Type Over Time

Use this report to view trends in the number and type of user responses to queries reported throughout your deployment. The report allows you to look at this information over time.

A pre-configured **Queried Events by Response Type Over Time** report is provided with this release. The report provides information on one week of events and it is displayed in HTML. To view the report provided, follow this procedure:

To view the report provided, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3** Click the link to the **Queried Events by Response Type Over Time** report.
 - Step 4** Click **View** report.

To create a new report, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** In the Select Report Type list box, select **Queried Events by Response Type Over Time**.
 - Step 7** In the Select Response Types list box, select up to five response types for which you want to see event information.
 - Step 8** In the **Start Date** and **End Date** fields, enter the beginning and ending dates for this report. The report can span one to seven days. The time frame must indicate whole days. You can specify the Start Date and End Date parameters in these ways:
 - You can specify a relative time using any of the following terms: tomorrow, yesterday, today, next, ago, week, and day.
 - You can 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.
 - Step 9** In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 10** Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 11** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Summary of Events by Enforcement Action

Use this report to view total numbers and types of enforced actions reported throughout your deployment.

A pre-configured Summary of Events by Enforcement Action report is provided with this release. The report provides summary information on all available events and it is displayed in HTML.

To view the report provided, follow this procedure:

- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
- Step 3** Click the link to the **Summary of Events by Enforcement Action** report.
- Step 4** Click **View** report.

To create a new report, follow this procedure:

- Step 1** Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
- Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
- Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
- Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
- Step 5** If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
- Step 6** In the Select Report Type list box, select **Summary of Events by Enforcement Action**.
- Step 7** In the **Start Date** and **End Date** fields, enter the beginning and ending dates for this report. The time frame must indicate whole days. You can specify the Start Date and End Date parameters in these ways:
 - You can specify a relative time using any of the following terms: tomorrow, yesterday, today, next, ago, week, and day.
 - You can 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.Alternatively, you may check All times if you do not want to limit the time frame of the report.
- Step 8** In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
- Step 9** Click the **Save** button to save the parameters you just configured for generating this report.
- Step 10** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Summary of Queried Events by Response Type Over Time

Use this report to view total numbers and types of user responses to queries reported throughout your deployment.

A pre-configured **Summary of Queried Events by Response Type Over Time** report is provided with this release. The report provides summary information on all available events and it is displayed in HTML.

To view the report provided, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3** Click the link to the **Summary of Queried Events by Response Type Over Time** report.
 - Step 4** Click **View** report.

To create a new report, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** In the Select Report Type list box, select **Summary of Queried Events by Response Type Over Time**.
 - Step 7** In the **Start Date** and **End Date** fields, enter the beginning and ending dates for this report. The report can span one to seven days. The time frame must indicate whole days. You can specify the Start Date and End Date parameters in these ways:
 - You can specify a relative time using any of the following terms: tomorrow, yesterday, today, next, ago, week, and day.
 - You can 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.Alternatively, you may check All times if you do not want to limit the time frame of the report.
 - Step 8** In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 9** Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 10** Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Top 20 Infected Hosts

Use this report to view the 20 hosts infected with the most number of viruses, found by CSA AV, throughout your CSA deployment. The report could include signature-based viruses, behavior-based viruses, and Potentially Unwanted Applications (PUAs). If an end user has restored a file that CSA-AV previously quarantined, that file is not counted by this report.

A pre-configured **Top 20 Infected Hosts** report is provided with this release. The report is displayed in HTML.

To view the report provided, follow this procedure:

-
- Step 1 Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3 Click the link to the **Top 20 Infected Hosts** report.
 - Step 4 Click **View** report.

To create a new report, follow this procedure:

-
- Step 1 Log on to the CSA MC as a user with any level of privileges This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2 From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3 Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4 In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5 If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6 In the Select Report Type list box, select **Top 20 infected hosts**.
 - Step 7 In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 8 Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 9 Click the **View Report** button. Your report is created and is automatically displayed in a new window.

Top 20 Identified Viruses

Use this report to view the 20 most frequently occurring viruses, found by CSA AV, throughout your CSA deployment. The report could include signature-based viruses, behavior-based viruses, and Potentially Unwanted Applications (PUAs). If an end user has restored a file that CSA-AV previously quarantined, that file is not counted by this report.

A pre-configured Top 20 Identified Viruses report is provided with this release. The report is displayed in HTML.

To view the report provided, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. The existing Management Summary reports are shown.
 - Step 3** Click the link to the **Top 20 Viruses Found Across All the Hosts** report.
 - Step 4** Click **View** report.

To create a new report, follow this procedure:

-
- Step 1** Log on to the CSA MC as a user with any level of privileges. This report can be generated in either Advanced Mode or Simple Mode.
 - Step 2** From the CSA MC menu bar, mouseover **Reports** and select **Management Summary**. All existing Management Summary reports are shown.
 - Step 3** Click the **New** button to create a new report. This takes you to the report's configuration view.
 - Step 4** In the configuration view, enter a **Name** and a **Description** for the report.
 - Step 5** If you would like a link to this report to appear in the Favorite Reports section of the Home page, select **Put this report on the Home page favorite list**.
 - Step 6** In the Select Report Type list box, select **Top 20 Identified Viruses**.
 - Step 7** In the Viewer Type field select **PDF** or **HTML** output. See [Viewing Reports, page 11-2](#) for more information about these output choices.
 - Step 8** Click the **Save** button to save the parameters you just configured for generating this report.
 - Step 9** Click the **View Report** button. Your report is created and is automatically displayed in a new window.



Tip

If you would like to see which hosts are infected with the viruses reported, copy the name of the virus in the report and use the Virus Infections Report, sorted by Virus.

