CHAPTER 57

Working with Reports

The FireSIGHT System provides a flexible reporting system that allows you to quickly and easily generate multi-section reports with the event views or dashboards that appear on your Defense Center. You can also design your own custom reports from scratch. Reporting is available only on Defense Centers.

A report is a document file formatted in PDF, HTML, or CSV with the content you want to communicate. A report template specifies the data searches and formats for the report and its sections. The FireSIGHT System includes a powerful report designer that automates the design of report templates. You can replicate the content of any event view table or dashboard graphic displayed in the web interface.

You can build as many report templates as you need. Each report template defines the individual sections in the report and specifies the database search that creates the report's content, as well as the presentation format (table, chart, detail view, and so on) and the time frame. Your template also specifies document attributes, such as the cover page and table of contents and whether the document pages have headers and footers (available only for reports in PDF format). You can export a report template in a single configuration package file and import it for reuse on another Defense Center.

You can include input parameters in a template to expand its usefulness. Input parameters allow you to produce tailored variations of the same report. When you generate a report with input parameters, the generation process prompts you to enter a value for each input parameter. The values you type constrain the report contents on a one-time basis. For example, you can place an input parameter in the destination IP field of the search that produces an intrusion event report; at report generation time, you can specify a department's network segment when prompted for the destination IP address. The generated report then contains only information concerning that particular department.

See the following sections for more information on reports and report templates:

Understanding Report Templates

License: Any

The FireSIGHT System's reporting feature allows you to quickly capture the content of any event view, dashboard, or workflow from your Defense Center and present it in report format. You use report templates to define the content and format of the data in each of the report's sections, as well as the document attributes of the report file (cover page, table of contents, and page headers and footers). After you generate a report, the template stays available for reuse until you delete it.

Your reports contain one or more information sections. You choose the format (text, table, or chart) for each section individually. The format you select for a section may constrain the data that can be included. For example, you cannot show time-based information in certain tables using a pie chart format. You can change the data criteria or format of a section at any time to obtain optimum presentation.

You can base a report's initial design on a predefined event view, or you can start your design by importing content from any defined dashboard, workflow, or summary. You can also start with an empty template shell, adding sections and defining their attributes one by one.

All sections in a report template have a title bar and various attribute fields that control the section's contents and appearance. For more information, see the following:

- the Report Section Title Bar Elements table
- the Report Section Fields table

The following table describes the controls on the title bar for each template section.

Table 57-1 Report Section Title Bar Elements

Attribute	Definition
section title	Contains the name of the section as it appears in the report. Change it by clicking it and typing a new name. To avoid display issues, the system truncates long section title names when viewed on the Report Sections page.
section title icons	Click the duplicate icon (+) to add a duplicate of the section to the report template. Click the minimize icon (−) to minimize the section. Click the delete icon (✖) to delete the section, after confirmation.

The following table defines the fields in each section of a report template.

Table 57-2 Report Section Fields

Field Name	Definition
Table	Presents a drop-down menu that allows you to select the table from which the section data is extracted.
Preset	Presents a drop-down menu of predefined searches. You can select an appropriate preset to initialize the search criteria when you define a new search.

Table 57-2 Report Section Fields (continued)

Field Name	Definition
Format	Presents icons that allow you to select the format of the section data. Options include: 📊 Bar chart: Compares quantities of the selected variables. 📈 Line chart: Shows trends/changes over time of a selected variable. Available only for time-based tables. ◔ Pie chart: Shows each selected variable as a percentage of the whole. Variables with quantities of zero are dropped from the chart. Very small quantities are clustered into a category labeled **Other**. ▦ Table view: Shows values of attributes for each record. Not available for summary or statistical data. 🗎 Detail view: Shows complex object data associated with certain events, such as packets (for intrusion events) and host profiles (for host events). Format is available only for certain event types that involve such objects. Output may degrade performance if large numbers are requested.
Search or Filter	Presents a drop-down menu of searches or application filters. For most tables, you can constrain a report using a predefined or saved **Search**. You can also create a new search by clicking the edit icon (✎); see Working with Searches in Report Template Sections, page 57-17. For the Application Statistics table, you use a user-defined application **Filter** to constrain a report; for information on creating filters, see Working with Application Filters, page 3-14.
X-Axis	Presents a drop-down menu of available data columns for the X-axis of the selected chart. Appears only when you select a chart format. For line charts, the X-axis value is always **Time**. For bar and pie charts, you cannot select **Time** as the X-axis value.
Y-Axis	Presents a drop-down menu of available data columns for the Y-axis of the selected chart.
Section Description	Defines the descriptive text that precedes the search data in the section. Enter a combination of text and input parameters. Default for a new section is the following set of two input parameters: `$<Time Window>` and `$<Constraints>`. For more information on input parameters, see Using Input Parameters, page 57-18.
Time Window	Defines the time window for the data that appears in the section. If the section searches time-based tables, you can select the check box to inherit the report's global time window. Alternatively, you can set a specific time window for the section. For information about setting the time window, see Editing the Sections of a Report Template, page 57-12.
Results	Select either **Top** or **Bottom** and enter the maximum number of records to be included in the section.
Color	Defines the colors for graphed data in the section. Select one or more colors, as applicable.

Creating and Editing Report Templates

License: Any

You can build a new report template in any of the following ways:

- Creating a New Report Template, page 57-4
- Creating a Report Template from an Existing Template, page 57-6
- Creating a Report Template from an Event View, page 57-9
- Creating a Report Template by Importing a Dashboard or Workflow, page 57-11

To modify and customize a report template, see the following sections:

- Editing the Sections of a Report Template, page 57-12
- Working with Searches in Report Template Sections, page 57-17
- Using Input Parameters, page 57-18
- Editing Document Attributes in a Report Template, page 57-22
- Customizing a Cover Page, page 57-23
- Managing Logos, page 57-24

Creating a New Report Template

License: Any

If you do not want to copy an existing report template, you can create an entirely new template. First, you create a default template shell. Then, in the order you prefer, you design the individual template sections and set attributes for the report document. For information on these steps, see the following sections:

- Creating a Template Shell, page 57-4
- Configuring the Content of the Template Sections, page 57-5
- Setting Attributes for PDF and HTML Report Documents, page 57-5

Creating a Template Shell

License: Any

A report template is a framework of sections, each independently built from its own database query. The first step in creating a template is to generate the framework shell that allows you to add and format the sections.

To create a template shell:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Click the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click **Create Report Template**.

The Report Sections page appears with the default template name, `New Report`, in the **Report Title** field.

Step 4 Optionally, type a name for your new template in the **Report Title** field and click **Save**. The report title can contain any combination of alphanumeric characters and spaces.

An entry with the new template name appears on the Report Templates page list.

Step 5 The report title can also contain input parameters. To add an input parameter, place your cursor at the spot in the title where the value of the parameter should appear, then click the insert input parameter icon (⊕).

The added input parameters appear in the **Report Title** field. For information on input parameters, see Using Input Parameters, page 57-18.

Step 6 Use the set of add icons under the Report Sections title bar to insert section shells as necessary. For information on section formatting, see the Report Section Fields table.

Each added section appears at the bottom of the template. Drag it to the correct location.

Step 7 Click the section title on the section title bar and type a name for the section (using a maximum of 120 characters).

Step 8 Click **Save** to save the template.

Your template is saved.

Configuring the Content of the Template Sections

License: Any

Each template section consists of a dataset generated by a search or filter, and has a format specification (table, pie chart, and so on) that determines the mode of presentation. You further determine section content by selecting the fields in the data records you want to include in the output, as well as the time frame and number of records to show.

To configure report template sections:

Access: Admin/Any Security Analyst

Step 1 Edit the section attributes as described in Editing the Sections of a Report Template, page 57-12.

Step 2 Optionally, click **Preview** at the bottom of the section window to view the column layout or graphic format you selected.

Note Use the section preview utility to check the column selection and output characteristics such as pie chart colors. It is not a reliable indicator of the correctness of your configured search.

Setting Attributes for PDF and HTML Report Documents

License: Any

The report you generate from the template has several document attributes that span all sections and control features, such as the cover page, headers and footers, page numbering, and so on.

To set attributes for the report documents:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Click the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click **Edit** for the report template you want to use to generate the report.

The Report Sections page for your template appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears.

Step 5 For documents in PDF or HTML format, perform the tasks described in Editing Document Attributes in a Report Template, page 57-22.

If you selected CSV as your document format, you have no document attributes to set.

Creating a Report Template from an Existing Template

License: Any

If you identify a good model among your existing templates, you can copy the template and edit its attributes to create a new report template. Cisco also provides a set of predefined report templates, visible on the **Reports Tab** in the list of templates. For a description of their attributes, see Using Predefined Report Templates, page 57-7.

To create a report template from an existing template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Click the **Report Templates** tab.

The Report Templates page appears. For information about Cisco-provided report templates, see Using Predefined Report Templates, page 57-7.

Step 3 Click the copy icon (⧉) next to the report template you want to copy as a model.

The copied template appears as a new report template.

Step 4 In the **Report Title** field, type a name for your new report template.

Step 5 Click **Save**.

The report template is saved and an entry for the new report template appears on the Report Templates page.

Step 6 Make changes to the template as needed.

For information on defining the sections of the template and the document attributes, see:

- Editing the Sections of a Report Template, page 57-12

- Editing Document Attributes in a Report Template, page 57-22

Using Predefined Report Templates

License: Any

You can use the following predefined report templates as-is, edit them, or use them as the basis for your own templates:

- Host Report: $<Host>
- User Report: $<User>
- Attack Report: Attack $<Attack SID>
- Malware Report
- FireSIGHT Report: $<Customer Name>
- Files Report

Host Report: $<Host>

The Host Report: $<Host> report template provides information about a specific host on the network. This report template contains the following sections:

- Server Applications
- Client Applications
- Intrusion Events Originating from This Host
- Intrusion Events Destined to This Host
- Connections Originating from This Host
- Connections Destined to This Host
- Users of This Host
- White List Violations by This Host

User Report: $<User>

The User Report: $<User> report template provides information about a specific user on the network. This report template contains the following sections:

- Client Applications Used by This User
- Web Applications Used by This User
- Application Protocols Used by This User
- Comprehensive List of Applications Used by This User
- Intrusion Events Originated By This User’s Machines
- Intrusion Events Destined to This User’s Machines
- Connections Originating from This User’s Machines
- Connections Destined to This User’s Machines
- Hosts for This User

Attack Report: Attack $<Attack SID>

The Attack Report: Attack $<Attack SID> report template provides information about a specific attack on the network. This report template contains the following sections:

- General Information About This Attack
- Number of Attacks
- Number of Machines Initiating Attack
- Number of Machines Being Attacked
- Sources of This Attack
- Destinations of This Attack
- Traffic Patterns of This Attack

Malware Report

The Malware Report report template provides information about network and endpoint-based malware events. This report template contains the following sections:

- Malware Threats
- Threat Detections over Time
- Application Protocols Transferring Malware
- Hosts Receiving Malware
- Hosts Sending Malware
- Users Affected by Malware
- Malware Intrusions
- File Types Infected with Malware
- Applications Introducing Malware
- Table View of Malware Events

Note that neither Series 2 devices nor the DC500 Defense Center support network-based malware protection, which can affect the data detected and displayed. For example, a Series 3 Defense Center managing only Series 2 devices can display only endpoint-based malware events.

FireSIGHT Report: $<Customer Name>

The FireSIGHT Report: $<Customer Name> report template provides overall information about an organization's network. This report template contains the following sections:

- Summary of Application Traffic by Risk
- Risky Applications with Low Business Relevance
- Users of Risky Applications
- Anonymizers and Proxies
- Typically High Bandwidth Applications
- Applications by Total Bandwidth
- Hosts Accessing Sensitive Network
- Users Accessing Sensitive Network
- Applications on Sensitive Network

- Ports and Protocols Related to Sensitive Network
- Hosts Visiting Malicious URLs
- Users Visiting Malicious URLs
- Granular Application Usage
- Web Applications
- Client Applications
- Application Protocols
- Web Browser Versions
- Operating System Versions
- Overall User Activity
- Intrusion Events by Impact
- Intrusion Events by Impact (After Blocking)
- Intrusion Events by Application
- Top Intrusion Events
- Comprehensive Application List

Files Report

The Files Report report template provides information about files detected in network traffic by managed devices. This report template contains the following sections:

- File Transfers over Time
- Application Protocols Used by File Transfers
- File Dispositions
- File Actions
- Hosts Receiving Files
- Hosts Sending Files
- Users Transferring Files
- File Categories
- File Types
- File Names
- Table View of File Events

Creating a Report Template from an Event View

License: Any

Before you generate a report, the reporting system creates a report template that you can modify to meet your needs. You can add additional sections, modify automatically included sections, and delete sections.

To create a report template from an event view:

Access: Admin/Any Security Analyst

Step 1 Populate an event view with the events you want in the report. You can do this in various ways:

- Use an event search to define the events you want to view. For details on using the event search, see Searching for Events, page 60-1.
- Drill down through a workflow until you have the appropriate events in your event view. For details on workflows and how to constrain events within a workflow, see Understanding and Using Workflows, page 58-1.

Step 2 From the event view page, click **Report Designer**.

The Report Sections page appears with a section for each view in the captured workflow.

Step 3 Optionally, type a new name in the **Report Title** field and click **Save**.

Step 4 Optionally, delete any template sections that you want to exclude from the report by clicking the delete icon (✖) in the section's title bar, and confirm the deletion.

The deleted sections disappear.

Note The last report section in some workflows contains detail views that show packets, host profiles, or vulnerabilities, depending on the workflow. Retrieving large numbers of events with these detail views when generating your report may affect performance of the Defense Center.

Step 5 Optionally, adjust the settings of the fields in your report sections.

For details on configuring the fields in a report section, see Editing the Sections of a Report Template, page 57-12.

Tip To view the current column layout or chart formatting for a section, click the section's **Preview** link.

Step 6 Optionally, change the title of any section by clicking the section title in the title bar.

The Set Section Title pop-up window appears. Type the section title and click **OK**.

Step 7 Optionally, add page breaks. Click the add page break icon ( ).

A new page break object appears at the bottom of the template. Drag it in front of the section that should start the new page. For information on using page breaks, see Editing the Sections of a Report Template, page 57-12.

Step 8 Optionally, add text sections. Click the add text section icon ( ).

A new text section appears at the bottom of the template. Drag it to the place where it should appear in the report template. For information about editing a text section, see Editing the Sections of a Report Template, page 57-12.

Tip Text sections, which support rich text (bold, italics, variable font size, and so on) as well as imported images, are useful for introductions to your report or your report sections.

Step 9 Optionally, click **Advanced Settings** to add a cover page, table of contents, starting page number, or header and footer text. For more information, see Editing Document Attributes in a Report Template, page 57-22.

Step 10 When the report template is correct, click **Save**.

The report template is saved and an entry for the report template appears on the Report Templates page.

Creating a Report Template by Importing a Dashboard or Workflow

License: Any

You can quickly create a new report by importing dashboards, workflows, and statistics summaries. The import creates a section for each widget graphic in your dashboard and each event view in your workflow. You can delete any unnecessary sections to focus on the most important information. The following table describes the import options.

Table 57-3 Data Source Options on Import Report Sections Window

Select this option...	To import...
Import Dashboard	any custom analysis widget on the selected dashboard.
Import Workflow	any predefined or custom workflow. **Tip** Selections have the format: `Table - Workflow name` For example, `Connection Events - Traffic by Port` imports the views in the Traffic by Port workflow generated from the Connection Events table.
Import Summary Sections	any of the following generic summaries: • Intrusion Detailed Summary • Intrusion Short Summary • Discovery Detailed Summary • Discovery Short Summary

To create a report template from a dashboard, workflow, or statistics summary:

Access: Admin/Any Security Analyst

Step 1 Identify the dashboard, workflow, or summary you want to replicate in your report.

Step 2 Select **Overview > Reporting**.

Step 3 Click the **Report Templates** tab.

The Report Templates page appears.

Step 4 Click **Create Report Template**.

The Report Sections page appears.

Step 5 Type a name for your new report template in the **Report Title** field.

Step 6 Click **Save** to save the report template under the new name.

The report template is saved and an entry for the report template appears on the Report Templates page.

Step 7 Click the import sections from dashboard, summaries and workflows icon ( ).

The Import Report Sections pop-up window appears. You can choose any of the data sources described in the Data Source Options on Import Report Sections Window table.

Step 8 Select a dashboard, workflow or summary from the drop-down menus.

Step 9 For the data sources you want to add, click **Import**.

The Report Sections page for your template reappears with a section for each element of the selected data source. For dashboards, each widget graphic will have its own section; for workflows, each event view will have its own section.

Step 10 Make changes to the content of your sections as needed.

For information on editing a report template, see Editing the Sections of a Report Template, page 57-12.

Note The last report section in some workflows contains detail views that show packets, host profiles, or vulnerabilities, depending on the workflow. Retrieving large numbers of events with these detail views when generating your report may affect performance of the Defense Center.

Step 11 When the report template is correct, click **Save**.

The report template is saved and an entry for the report template appears on the Report Templates page.

Editing the Sections of a Report Template

License: Any

You can modify a variety of report section attributes to adjust the content of the section and its data presentation. For information, see the following sections:

- Setting the Table and Data Format for a Template Section, page 57-12
- Specifying the Search or Filter for a Template Section, page 57-13
- Setting the Search Fields that Appear in Table Format Sections, page 57-14
- Adding a Text Section to a Report Template, page 57-14
- Adding a Page Break to a Report Template, page 57-15
- Setting the Time Window for a Template and Its Sections, page 57-15
- Renaming a Template Section, page 57-16
- Previewing a Template Section, page 57-17

Note Security Analysts can edit only report templates they created.

Setting the Table and Data Format for a Template Section

License: Any

Each section in a report template queries a database table to generate content for that section. Changing the section’s data format uses the same data query, but modifies the fields that appear in the section according to the analytical purpose of the format type. For example, the table view of intrusion events populates the section with a large number of data fields per event record, while a pie chart section shows the portion of all matching records that each selected attribute represents, with no details about individual events. Bar chart sections compare the total counts of matching records that have specific attributes. Line charts summarize changes in the matching records over time with respect to a single attribute. Line charts are available only for data that is time-based, not for information about hosts, users, third-party vulnerabilities, and so on.

For information on the different available formats, see the Report Section Fields table.

To select the table and output format for a template section:

Access: Admin/Any Security Analyst

Step 1 Use the **Table** drop-down menu to select the table to query in this section.

Icons appear in the **Format** field for each of the output formats available for the selected table.

Step 2 Select the applicable output format icon for the section. For information about these formats, see the Report Section Title Bar Elements table.

The fields included in the output appear.

Step 3 To change the search constraints, click the edit icon (✎) next to the **Search** or **Filter** field.

The Search Editor pop-up window appears with options for constraining the search. For information on using this window, see Working with Searches in Report Template Sections, page 57-17.

Step 4 For graphic output formats (pie chart, bar chart, and so on), adjust the **X-Axis** and **Y-Axis** parameters using the drop-down menus.

When you select a value for the X-axis, only compatible values appear in the Y-axis drop-down menu, and vice versa.

Step 5 For table output, select the columns, order of appearance, and sort order in your output. For detailed information, see Setting the Search Fields that Appear in Table Format Sections, page 57-14.

Step 6 Click **Save** to save the template.

Your template is saved.

Specifying the Search or Filter for a Template Section

License: Any

The search or filter in a report section specifies the database query on which the section content is based. For most tables, you can constrain a report using a predefined or saved search, or you can create a new search on the fly:

- Predefined searches serve as examples for searching certain event tables and can provide quick access to important information about your network that you may want to include in reports.
- Saved event searches include all public event searches that you or others have created, plus all your saved private event searches. For information on defining, naming, and using saved event searches, see Searching for Events, page 60-1.
- Saved searches for the current report template are accessible only in the report template itself. The search names of saved report template searches end with the string “Custom Search.” Users create these searches while designing reports.

For the Application Statistics table, you use a user-defined application filter to constrain a report; for information on creating filters, see Working with Application Filters, page 3-14.

To specify a search or filter for a template section:

Access: Admin/Any Security Analyst

Step 1 Select the database table to query from the **Table** drop-down menu:

- For most tables, the **Search** drop-down list appears.
- For the Application Statistics table, the **Filter** drop-down list appears.

Step 2 Select the search or filter you want to use to constrain the report.

You can view the search criteria or create a new search by clicking the edit icon (✏). For more information, see Working with Searches in Report Template Sections, page 57-17.

Setting the Search Fields that Appear in Table Format Sections

License: Any

If you include table data in a section, you can choose which fields in the data record to show. All fields in the table are available for inclusion or exclusion. You select fields that accomplish the purpose of the report, then order and sort them accordingly.

To add and delete the fields in a table format section:

Access: Admin/Any Security Analyst

Step 1 For table format sections, click the edit icon (✏) next to the **Fields** parameter.

The Table Field Selector window appears.

Step 2 Optionally, add and delete fields, and drag the field icons into the column order you want.

Step 3 Optionally, change the sort order of any column. Use the drop-down lists on each field icon to set the sort order and priority.

Step 4 When the fields are in the right order and have the necessary sort characteristics, click **OK**.

The Report Sections page appears.

Adding a Text Section to a Report Template

License: Any

You can add text sections to your templates to provide custom text, such as an introduction, for the whole report or for individual sections. Text sections can have rich text with multiple font sizes and styles (bold, italic, and so on) as well as input parameters and imported images. For information on input parameters, see Using Input Parameters, page 57-18.

To add a text section to a report template:

Access: Admin/Any Security Analyst

Step 1 Click the add text section icon ( ).

A text section appears at the bottom of the template.

Step 2 Drag the new text section to its intended position in the report template.

Step 3 Optionally, add page breaks before and after the text section. For information on page breaks, see Adding a Page Break to a Report Template, page 57-15.

Step 4 Optionally, click the text section's generic name in the title bar to type a new name.

Step 5 Add formatted text and images to the body of the text section. You can include input parameters that dynamically update when you generate the report.

Step 6 Click **Save** when finished.

Your template is saved.

Adding a Page Break to a Report Template

License: Any

You can add page breaks before or after any section in the template. This feature is particularly helpful for multi-section reports with text pages that introduce the various sections.

To add a page break:

Access: Admin/Any Security Analyst

Step 1 Click the add page break icon ( ).

A page break appears at the bottom of the template.

Step 2 Drag the page break to its intended location, before or after a section.

Step 3 Repeat the process for all page breaks you add to the template.

Setting the Time Window for a Template and Its Sections

License: Any

A report template's time window defines the template's reporting period. Report templates with time-based data (such as intrusion or discovery events) have a global time window, which the time-based sections in the template inherit by default when created. Changing the global time window changes the local time window for the sections that are configured to inherit the global time window. You can disable time window inheritance for an individual section by clearing its **Inherit Time Window** check box. You can then edit the local time window.

Note Global time window inheritance applies only to report sections with data from time-based tables, such as intrusion events and discovery events. For sections that report on network assets (hosts and devices) and related information (such as vulnerabilities), you must set each time window individually.

To change a report template's global time window:

Access: Admin/Any Security Analyst

Step 1 On the Report Templates page, click the edit icon ( ) next to the report template you want to edit.

The Report Sections page appears.

Step 2 Click **Generate**.

The Generate Report pop-up window appears.

Step 3 To modify the global time window, click the time window icon (🕒).

The Events Time Window page appears in a new window. For information about using this page, see Setting Event Time Constraints, page 58-23.

Step 4 When you are finished, click **Apply** on the Events Time Window.

The Generate Report pop-up window reappears with the new time window.

Step 5 Click **Cancel** to return to the Report Sections page, or **OK** to generate the report.

Your report can have different time ranges per section. For example, your first section could be a summary for the month, and the remaining sections could drill down into details at the week level. In such cases, you set the section-level time windows individually.

To configure a section's local time window:

Access: Admin/Any Security Analyst

Step 1 On the Report Sections page of a template, clear the **Inherit Time Window** check box for the section if it is present.

The local section time window icon appears.

Step 2 To change the section's local time window, click the time window icon (🕒).

The Events Time Window page appears. For information about using this page, see Setting Event Time Constraints, page 58-23.

Note Sections with data from statistics tables can have only sliding time windows.

Step 3 When you have set a new local time window, click **Apply** on the Events Time Window.

Step 4 Click **Save**.

The Report Sections page appears for further editing.

Renaming a Template Section

License: Any

When you create a new template, the sections you add receive generic section names and should be renamed to indicate their content.

To rename a template section:

Access: Admin/Any Security Analyst

Step 1 Click the current section name in the section header.

The Set Section Title pop-up window appears.

Step 2 Type a new name for the section (using a maximum of 120 characters) and click **OK**.

The name in the section title bar is changed.

Previewing a Template Section

License: Any

The preview function shows the field layout and sort order for table views and important legibility characteristics of graphics, such as pie chart colors.

To preview a template section:

Access: Admin/Any Security Analyst

Step 1 At any time while editing a section, click **Preview** for the section.

The Preview pop-up window appears.

Step 2 Close the preview by clicking **OK** at the bottom of the window.

The Report Sections page appears.

Working with Searches in Report Template Sections

License: Any

The key to generating successful reports is defining the searches that populate the report's sections. The FireSIGHT System provides a search editor to view the searches available in your report templates and to define new custom searches.

Tip The custom searches you make in a report template are specific to the template where you create them. You can make searches that are reusable across all report templates in the event viewer. When you save a custom search in the event viewer, it appears in the **Search** drop-down menu of all report templates. For details on using the event viewer to create and save custom searches, see Searching for Events, page 60-1.

To create a custom search:

Access: Admin/Any Security Analyst

Step 1 From the relevant section in the report template, click the edit icon (✎) next to the **Search** field.

The Search Editor page appears with the table to be searched selected.

Step 2 Optionally, from the **Saved Searches** drop-down menu, select a predefined search.

The drop-down presents all available predefined searches for this table, including system-wide and report-specific predefined searches.

Step 3 Edit the search criteria in the appropriate fields. For certain fields, your constraints can include the same operators (<, <>, and so on) as event searches. For the syntax of search criteria, see Searching for Events, page 60-1.

If you enter multiple criteria, the search returns only the records that match all the criteria.

Step 4 Optionally, where the input parameter icon (⊕) appears, you can insert an input parameter from the drop-down menu instead of typing a constraint value. For information on using input parameters in report designs, see Using Input Parameters, page 57-18.

For some search fields, the drop-down menu may contain user-defined managed objects instead of, or with, input parameters. Managed objects, which have distinctive icons depending on their type, are system configuration variables you can use as values in constraining searches. However, they do not produce the generation-time query for user input that occurs with input parameters. For information on managed objects, see Managing Reusable Objects, page 3-1.

Note When you edit the constraints of a reporting search, the system saves your edited search under the following name: `*section* custom search`, where *`section`* is the name in the section title bar followed by the string `custom search`. To have meaningful names for your saved custom searches, be sure you change the section name before you save the edited search. You cannot rename a saved reporting search.

Step 5 When finished modifying the fields in the search editor, click **OK.**

The Report Sections page reappears and a new predefined search appears in the section's **Search** drop-down menu.

Using Input Parameters

License: Any

You can use input parameters in a report template that the report can dynamically update at generation time. The input parameter icon (⊕) indicates the fields that can process them. There are two kinds of input parameters:

- Predefined — see the Predefined Input Parameters table
- User-defined — see User-Defined Input Parameter Types table

Predefined Input Parameters

License: Any

Predefined input parameters are resolved by internal system functions or configuration information. For example, at report generation time, the system replaces the `$<Time>` parameter with the current date and time. The following table defines the parameters available for use. You might, for example, include `$<Month>` in the title of a monthly summary report that generates automatically under scheduler control. Your report title then automatically updates with the correct month.

Table 57-4 Predefined Input Parameters

Insert this parameter...	...to include this information in your template:
`$<Logo>`	The selected uploaded logo
`$<Report Title>`	The report title
`$<Time>`	The date and time of day the report ran, with one-second granularity
`$<Month>`	The current month

Table 57-4 Predefined Input Parameters (continued)

Insert this parameter...	...to include this information in your template:
`$<Year>`	The current year
`$<System Name>`	The name of the Defense Center
`$<Model Number>`	The model number of the Defense Center
`$<Time Window>`	The time window currently applied to the report section
`$<Constraints>`	The search constraints currently applied to the report section

The following table lists the valid input parameters that can be used in different areas within the Report Templates page.

Table 57-5 Predefined Input Parameter Usage

Parameter	Report Template Cover Page	Report Template Report Title	Report Template Section Description	Report Template Text Section	Generate Report File Name	Generate Report Email Subject, Body
`$<Logo>`	yes	no	no	no	no	no
`$<Report Title>`	yes	no	yes	yes	yes	yes
`$<Time>`	yes	yes	yes	yes	yes	yes
`$<Month>`	yes	yes	yes	yes	yes	yes
`$<Year>`	yes	yes	yes	yes	yes	yes
`$<System Name>`	yes	yes	yes	yes	yes	yes
`$<Model Number>`	yes	yes	yes	yes	yes	yes
`$<Time Window>`	no	no	yes	no	no	no
`$<Constraints>`	no	no	yes	no	no	no

User-Defined Input Parameters

License: Any

You can create your own input parameters to supply as constraints in section searches. Constraining a search with an input parameter instructs the system to collect a value at generation time from the person who requests the report. In this way, you can dynamically tailor a report at generation time to show a particular subset of data without changing the template. For example, you can provide an input parameter for the **Destination IP** field of a report section's search. Then, when you generate the report, you can type the IP network segment for a particular department to get data for that department only.

Tip You can also type `*` in an input parameter field, with the effect of ignoring the constraint.

You can also define string-type input parameters to add dynamic text in certain fields of your report, such as in emails (subject or body), report file names, and text sections. You can personalize reports for different departments, with customized report file names, email addresses, and email messages, using the same template for all.

Each input parameter you define has a name and a type. The following table describes the parameter types.

Table 57-6 User-Defined Input Parameter Types

Use this parameter type...	With fields with this data...
Network/IP	any IP address or network segment in CIDR format
Application	name of an application protocol, client application, or web application
Event Message	any event view message
Device	3D appliance (Defense Center or FireSIGHT System managed device)
Username	user identification such as initiator user and responder user
Number (VLAN ID, Snort ID, Vuln ID)	any VLAN ID, Snort ID, or vulnerability ID
String	text fields such as application or OS version, notes, or descriptions

An input parameter's type determines the search fields where you can use it. You can use a given type only in appropriate fields, as described in the User-Defined Input Parameter Types table. For example, a user parameter you define as a string type is available for insertion in text fields but not in fields that take an IP address.

To create user-defined input parameters for a report template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✏) for the template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears.

Step 5 Click the Add Input Parameter icon (⊕).

The Add Input Parameter pop-up window appears.

Step 6 Type the parameter name in the **Name** field and use the **Type** drop-down menu to select the type, then click **OK**.

The new parameter appears in the **Input Parameters** menu.

Step 7 Repeat the steps above until you have defined all the parameters you need.

Step 8 Click **OK**.

Your new input parameters are saved for this template and the Report Sections page reappears.

If you reuse a report template, you can change the name and type for any input parameters to better reflect the purpose of the new report.

To edit user-defined input parameters for a report template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✎) for the template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears. The **Input Parameters** section lists all available user-defined parameters for the report template.

Step 5 Click the edit icon (✎).

The Edit Input Parameter pop-up window appears.

Step 6 Change the parameter name in the **Name** field and the parameter type using the **Type** drop-down menu, then click **OK**.

The changed parameter appears in the **Input Parameters** section.

Step 7 Repeat the steps above until you have defined all the parameters you need. Click **OK**.

Your changes are saved and the Report Sections page reappears.

To delete user-defined input parameters for a report template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✎) for the template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears. The **Input Parameters** section lists all available user-defined parameters for the report template.

Step 5 Click the delete icon (🗑) next to the input parameter and confirm.

Step 6 Click **OK**.

The input parameter is deleted and the Report Sections page reappears.

You use input parameters to expand the usefulness of your searches. The input parameter instructs the system to collect a value at generation time from the person who requests the report. In this way, you can dynamically constrain a report at generation time to show a particular subset of data without changing the search. For example, you can provide an input parameter for the **Destination IP** field of a report section that drills down on security events at a department level. When you generate the report, you can type the IP network segment for a particular department to get data for that department only.

To constrain the search in a report template with user-defined input parameters:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✎) for the template you want to edit.

The Report Sections page appears.

Step 4 Click the edit icon (✎) next to the **Search** field within the section.

The Search Editor pop-up window appears. Fields that can take an input parameter are marked with the input parameter icon (⊕).

Step 5 Click the input parameter icon (⊕) next to the field, then select the input parameter from the drop-down menu. User-defined input parameters are marked with the icon (📄).

The input parameter appears in the field.

Note Input parameters you define are available only for search fields that match their parameter type. For example, a parameter of type **Network/IP** is available only for fields that accept IP addresses or network segments in CIDR format.

Step 6 Click **OK** when you have added all necessary input parameters.

The Report Sections page appears with your changes.

Editing Document Attributes in a Report Template

License: Any

Before you generate your report, you can set document attributes that affect the report's appearance. These attributes include the optional cover page and table of contents. Support for some attributes depends on the selected report format: PDF, HTML, or CSV. The following table provides further details on attribute support by format.

Table 57-7 Document Attribute Support

Attribute	PDF Support?	HTML Support?	CSV Support?
Cover page	yes, with optional logo and custom appearance	yes, with optional logo and custom appearance	no
Table of contents	yes	yes	no

Table 57-7 Document Attribute Support (continued)

Attribute	PDF Support?	HTML Support?	CSV Support?
Page headers and footers	yes, with optional text or logo in any field	no	no
Custom starting page number	yes	no	no
Option to suppress numbering of first page	yes	no	no

To set the document attributes for PDF and HTML reports:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✏) for the report template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears.

Step 5 Select **Include Cover Page** to add a cover page.

Step 6 Click the edit icon (✏) next to the **Cover Page Design** field to edit the cover page design.

For more information, see Customizing a Cover Page, page 57-23.

Step 7 Select **Include Table of Contents** to add a table of contents.

Step 8 Configure the header and footer using the drop-downs of the three **Header** and **Footer** fields. You select header and footer content from the drop-down menus: logo, date, page number, and so on.

If you select **Logo**, the default logo image appears in the selected field. To change the default logo image, see Managing Logos, page 57-24.

Step 9 In the **Page Number Start** field, select the page number of the report's first page.

Select **Number First Page?** to show the page number on the first page following the cover page. If selected, the cover page is not numbered.

Step 10 Click **OK**.

The document attributes are saved and the Report Sections page reappears.

Customizing a Cover Page

License: Any

You can customize a report template's cover page. Cover pages can have rich text with multiple font sizes and styles (bold, italic, and so on) as well as input parameters and imported images. For information on input parameters, see Using Input Parameters, page 57-18.

To customize a report template cover page:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears and displays the list of templates.

Step 3 Click the edit icon (✎) for a report template.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears.

Step 5 Click the edit icon (✎) next to **Cover Page Design**.

The Edit Cover Page window appears, displaying the default cover page design.

Step 6 Edit the cover page design within the rich text editor.

Step 7 Click **OK**.

The cover page design is saved and the Advanced Settings window reappears.

Managing Logos

License: Any

You can store multiple logos on the Defense Center and associate them with different report templates. You set the logo association when you design the template. If you export the template, the export package contains the logo.

For information on where you can insert a logo in reports, see Editing Document Attributes in a Report Template, page 57-22.

See the following related procedures for more information:

- Adding a New Logo, page 57-24
- Changing the Logo for a Report Template, page 57-25
- Deleting a Logo, page 57-26

Adding a New Logo

License: Any

Logos uploaded to your Defense Center are available for all report templates on that Defense Center. Logo images must be in JPG format.

To add a logo to a Defense Center:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✏) for the report template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears. The logo currently associated with the template appears under **Logo** in **General Settings**.

Step 5 Click the edit icon (✏) for the logo.

The Select Logo pop-up window appears with images of currently uploaded logos.

Step 6 Click **Upload Logo**.

The Upload Logo pop-up window appears.

Step 7 Select the logo file to upload by doing one of the following:

- type the location of the logo file
- click the **Browse** button and browse to the file's location

Step 8 Click **Upload**.

The image is uploaded to the Defense Center and appears in the Select Logo pop-up window.

Step 9 Optionally, associate the new logo with the current template by selecting it and clicking **OK**.

The Advanced Settings window reappears with the associated logo image.

Changing the Logo for a Report Template

License: Any

You can change the logo in a report to any JPG image uploaded to your Defense Center. For example, if you reuse a template, you can associate a logo for a different organization with the report.

To change the logo for a report template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✏) for the report template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears. The logo currently associated with the template appears under **Logo** in **General Settings**.

Step 5 Click the edit icon (✏) for the logo.

The Select Logo pop-up window appears with images of currently uploaded logos.

Step 6 Select the logo to associate with the report template.

The selected logo is highlighted.

Step 7 Click **OK**.

The Advanced Settings window reappears with the associated logo image.

Deleting a Logo

License: Any

You can delete logos from your Defense Center. Deleting a logo removes it from all templates where it is used. The deletion cannot be undone.

Note that you cannot delete the predefined Cisco logo.

To delete a logo from a Defense Center:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the edit icon (✎) for the report template you want to edit.

The Report Sections page appears.

Step 4 Click **Advanced**.

The Advanced Settings pop-up window appears. The logo currently associated with the template appears under **Logo** in **General Settings**.

Step 5 Click the edit icon (✎) for the logo.

The Select Logo pop-up window appears with images of currently uploaded logos.

Step 6 Select the logo you want to delete.

The selected logo is highlighted.

Step 7 Click **Delete Logo**.

The deleted logo disappears from the Select Logo pop-up window.

Step 8 Click **OK**.

Your changes are saved and the Advanced Settings window reappears.

Generating and Viewing Reports

License: Any

After you create and customize your report template, you are ready to generate the report itself. The generation process lets you select the report's format (HTML, PDF, or CSV). You can also adjust the report's global time window, which applies a consistent time frame to all sections except those you exempt. For information on setting the report time window, see Setting the Time Window for a Template and Its Sections, page 57-15.

If the report template includes user input parameters in its search specification, the generation process prompts you to enter values, which tailor this run of the report to a subset of the data. For information on input parameters, see Using Input Parameters, page 57-18.

The Reports tab lists all previously generated reports, with report name, date and time of generation, generating user, and whether the report is stored locally or remotely. A status column indicates whether the report is already generated, is in the generation queue (for example, for scheduled tasks), or failed to generate (for example, due to lack of disk space).

The Reports tab page shows all locally stored reports. It shows remotely stored reports as well, if remote storage is currently configured. The location of your currently configured report storage appears at the bottom of the page, with disk usage for local, NFS, and SMB storage. If you access remote storage using SSH, disk usage data is not available. For information on setting up remote storage, see Using Remote Storage for Reports, page 57-30.

Note If you store remotely and then switch back to local storage, the reports in remote storage do not appear on the Reports tab list. Similarly, if you switch from one remote storage location to another, the reports in the previous location do not appear in the list.

File names using Unicode (UTF-8) characters are not supported in PDF reports. If you generate a report in PDF format, any report sections that include special Unicode file names (such as those appearing in file or malware events) display these file names in transliterated form.

If you have a DNS server configured and IP address resolution enabled, reports contain host names if resolution was successful. For more information, see Configuring Management Interfaces, page 64-8 and Event Preferences, page 71-3.

Use the following procedures to generate and view reports. Note that users with Administrator access can view all reports; other users can view only the reports they generated. For information about managing your report files, see Downloading Reports, page 57-33 and Deleting Reports, page 57-33.

To generate a report from a report template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Click the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the generate report icon (📄) for the template you want to use.

The Generate Report pop-up dialog appears.

Step 4 Optionally, type a new name in the **File Name** field. This sets the name of the generated report file. You may also use the input parameter icon (⊕) to add one or more input parameters to the file name. For information on input parameters, see Using Input Parameters, page 57-18.

Step 5 Select the output format for the report by clicking the corresponding icon: HTML, PDF, or CSV.

Step 6 Optionally, change the global time window by clicking the time window icon (🕒).

The Events Time Window pop-up window appears. For information on setting the events time window, see Setting Event Time Constraints, page 58-23.

Note Setting the global time window affects the content of individual report sections only if they are configured to inherit the global setting. For information on report section inheritance of the global time window, see Setting the Time Window for a Template and Its Sections, page 57-15.

Step 7 Type values for any fields that appear in the **Input Parameters** section.

Tip You can ignore user parameters by typing the `*` wildcard character in the field. This eliminates the user parameter's constraint on the search.

Step 8 Optionally, if an email relay host is configured in your system policy, click **Email** to automate email delivery of the report when it generates. For details about email delivery features, see Distributing Reports by Email at Generation Time, page 57-29.

Step 9 Click **OK** and confirm when prompted.

The Report Generation Complete pop-up window appears with a link to view your report.

Step 10 Click either:

- the report link, which opens a new window to display the report, or
- **OK** to return to the Report Section page, where you can modify your report design.

You can review completed reports after initial generation, as well.

Step 11 Optionally, manage your report files. For more information, see Downloading Reports, page 57-33 and Deleting Reports, page 57-33.

To view a generated report:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Click the **Reports** tab.

The Reports page appears.

Step 3 Click the name of the report.

The default program on your local host opens the report in a new window.

Step 4 When finished viewing the document, use your browser to return to the **Reports** tab.

Using Report Generation Options

License: Any

You have several additional options when generating reports. You can automatically schedule report generation, send reports via email, and store generated reports remotely. For more information, see the following sections:

- Generating Reports Using the Scheduler, page 57-29

- Distributing Reports by Email at Generation Time, page 57-29
- Using Remote Storage for Reports, page 57-30

Generating Reports Using the Scheduler

License: Any

You can use the FireSIGHT System scheduler to automate report generation. You can customize the schedule on a full range of time frames such as daily, weekly, monthly, and so on. For more information, see Automating Report Generation, page 62-8.

If you also want to distribute email reports using the scheduler, you must configure your report template and a mail relay host **before** scheduling the task. For more information, see Distributing Reports by Email at Generation Time, page 57-29 and Configuring a Mail Relay Host and Notification Address, page 63-18.

Distributing Reports by Email at Generation Time

License: Any

When you generate a report from its template, you can choose to automatically send the report as an email attachment to a list of recipients.

Note You must have a properly configured mail relay host to deliver a report by email. If you have not previously set up a mail host, see Configuring a Mail Relay Host and Notification Address, page 63-18.

To email a report at generation time:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Click the generate report icon (📋) for the template you want to generate from.

The Generate Report pop-up window appears.

Step 4 Expand the **Email** section of the window.

Step 5 In the **Email Options** field, select **Send Email**.

Step 6 In the **Recipient List, CC**, and **BCC** fields, type recipients’ email addresses in comma-separated lists.

Step 7 In the **Subject** field, type a subject for your email.

Tip You can provide input parameters in the **Subject** field and the message body to dynamically generate information in the email, such as a timestamp or the name of the Defense Center. For further information, see Using Input Parameters, page 57-18.

Step 8 Type a cover letter in the email body as necessary. The available rich text features include a wide range of fonts, numbered and bullet lists, and so on.

Step 9 When all fields in the Generate Report window are correct, click **OK** and confirm.

The system distributes the generated report by email. You can configure the email's From address under **Email Notification** in the system policy. For more information, see Managing System Policies, page 63-1.

Using Remote Storage for Reports

License: Any

You can configure the reporting system to place newly generated report files in your configured remote storage location. You can also move any locally stored report to your remote storage location.

Note You cannot move reports in remote storage back to local storage.

To use remote storage, you must first configure a remote storage location. When configured, the remote storage location appears at the bottom of the report list. The location includes current disk usage for NFS and SMB mounted storage, but not for SSH. For configuration information, see Managing Remote Storage, page 64-15.

To store reports remotely as they are generated:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Reports** tab.

The Reports page appears.

Step 3 Select the **Enable Remote Storage of Reports** check box at the bottom of the page.

The Defense Center stores newly generated reports in the remote location indicated at the bottom of the page. The **Location** column data for these reports is `Remote`.

You can move your reports in local storage to a remote storage location in batch mode or singly.

To move generated reports from local to remote storage:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Reports** tab.

The Reports page appears.

Step 3 Select the check boxes next to the reports you want to move, then click **Move**.

Tip Select the check box at the top left of the page to move all reports on the page. If you have multiple pages of reports, a second check box appears that you can select to move all reports on all pages.

Step 4 Confirm that you want to move the reports.

The reports are moved.

Managing Report Templates and Report Files

License: Any

In addition to creating and editing templates, you can perform the following template management tasks:

- Exporting and Importing Report Templates, page 57-31
- Deleting Report Templates, page 57-32

You can also perform the following management tasks for your generated report files:

- Downloading Reports, page 57-33
- Deleting Reports, page 57-33

Exporting and Importing Report Templates

License: Any

The file that you generate when you export a report template contains all necessary data to create the same report on another Defense Center. The export file, which is in a proprietary SFO format, includes:

- the report template, with all section design elements and document attributes
- all saved searches used in the report
- all images used in the report
- all custom tables used in the report

The only configuration that may be required after you import the template on another Defense Center is automatic report generation scheduling.

Note Importing and exporting report templates requires both Defense Centers to be at the same software version level.

To export a report template:

Access: Admin

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 For the template you want to export, click the export icon (🖫).

The system produces a configuration package file with `.sfo` extension and opens an Opening Object pop-up window that displays the package's file name.

Step 4 Select **Save file** and **OK** to save the file to your local computer.

Step 5 You can change the name of the `.sfo` package to a more descriptive one for your convenience. When you import the package, regardless of its name, the importing Defense Center will give the template the same name it had on the source Defense Center.

The SFO files exported from a Defense Center contain all elements necessary to add the report template to another Defense Center. The import process therefore requires only uploading the package to the second Defense Center and running the import process.

To import a report template:

Access: Admin

Step 1 Select **System > Tools > Import/Export**.

The Import/Export page appears, including a list of the report templates on the Defense Center.

Step 2 Click **Upload Package**.

The Package Name page appears.

Step 3 You have two options:

- Type the path to the package you want to upload.
- Click **Browse** to locate the package.

Step 4 Click **Upload**.

The **Report Template** section of the configuration list appears, showing the template to be imported.

Step 5 Select the check box next to the template and click **Import**.

The template appears in the list of configurations on the destination Defense Center.

Deleting Report Templates

License: Any

Report templates remain listed on the Report Templates tab for reuse until you delete them. Note that you cannot delete Cisco-provided report templates.

Note Security Analysts can delete only report templates they created.

To delete a report template:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Report Templates** tab.

The Report Templates page appears.

Step 3 Next to the template you want to delete, click the delete icon (🗑) and confirm.

The template name disappears from the list.

Downloading Reports

License: Any

You can download any report file to your local computer. From there, you can email it or distribute it electronically by other available means. For information on distributing reports automatically by email at generation time, see Distributing Reports by Email at Generation Time, page 57-29.

To download reports:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Reports** tab.

The Reports page appears.

Step 3 Select the check boxes next to the reports you want to download, then click **Download**.

Tip Select the check box at the top left of the page to download all reports on the page. If you have multiple pages of reports, a second check box appears that you can select to download all reports on all pages.

Step 4 Follow your browser's prompts to download the reports.

If you select multiple reports, they are downloaded in a single `.zip` file.

Deleting Reports

License: Any

You can delete your report files at any time. The procedure completely removes the files, and no recovery is possible. Although you still have the report template that generated the report, it may be difficult to regenerate a particular report file if the time window was expanding or sliding. For information on the time window, see Editing the Sections of a Report Template, page 57-12. Regeneration may also be difficult if your template uses input parameters. For information on using input parameters, see Using Input Parameters, page 57-18.

To delete reports:

Access: Admin/Any Security Analyst

Step 1 Select **Overview > Reporting**.

Step 2 Select the **Reports** tab.

The Reports page appears.

Step 3 Select the check boxes next to the reports you want to delete, then click **Delete**.

Tip Select the check box at the top left of the page to delete all reports on the page. If you have multiple pages of reports, a second check box appears that you can select to delete all reports on all pages.

Step 4 Confirm the deletion.

The reports are deleted.