Generate Reports to Monitor End-user Activity

This chapter contains the following sections:

Overview of Reporting

The Web Security appliance generates high-level reports, allowing you to understand what is happening on the network and also allowing you to view traffic details for a particular domain, user, or category. You can run reports to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals.

Related Topics

- Printing and Exporting Reports from Report Pages, on page 6

Working with Usernames in Reports

When you enable authentication, reports list users by their usernames when they authenticate with the Web Proxy. By default, usernames are written as they appear in the authentication server. However, you can choose to make usernames unrecognizable in all reports.

Note Administrators always see usernames in reports.

Step 1 Choose **Security Services > Reporting**, and click **Edit Settings**.

Step 2 Under Local Reporting, select **Anonymize usernames in reports**.

Step 3 Submit and Commit Changes.

Report Pages

The Web Security appliance offers the following reports:

- My Dashboard (the reporting “homepage”; can also be accessed by clicking the Home icon in the left edge of the menu bar)
- Overview
- Users
- User Count
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Advanced Malware Protection
- File Analysis
- AMP Verdict Updates
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- SOCKS Proxy
- Reports by User Location
- Web Tracking
- System Capacity
- System Status
- Scheduled Reports
- Archived Reports

Using the Reporting Pages

The various report pages provide an overview of system activity and support multiple options for viewing the system data. You can also search each page for Website and client-specific data.

You can perform the following tasks on most report pages:

Option	Link to Task
Change the time range displayed by a report	Changing the Time Range, on page 3
Search for specific clients and domains	Searching Data, on page 4
Choose which data to display in charts	Choosing Which Data to Chart , on page 4
Export reports to external files	Printing and Exporting Reports from Report Pages, on page 6

Changing the Time Range

You can update the data displayed for each security component using the Time Range field. This option allows you to generate updates for predefined time ranges and it allows you to define custom time ranges from a specific start time to a specific end time.

Note The time range you select is used throughout all of the report pages until you select a different value in the Time Range menu.

Time Range	Data is returned in...
Hour	Sixty complete minutes plus up to 5 additional minutes.
Day	One-hour intervals for the last 24 hours and including the current partial hour.
Week	On- day intervals for the last 7 days plus the current partial day.
Month (30 days)	One-day intervals for the last 30 days plus the current partial day.
Yesterday	The last 24 hours (00:00 to 23:59) using the time zone defined on the Web Security appliance.
Custom Range	The custom time range you defined. When you choose Custom Range, a dialog box appears to let you enter start and end times.

Note All reports display date and time information based on the system's configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT only to accommodate multiple systems in multiple time zones around the world.

Choosing a Time Range for Reports

Most predefined report pages allow you to choose a Time Range for the data to include. The time range that you select is used for all of the report pages until you select a different value in the Time Range menu.

Available Time Range options differ by appliance and differ for Email and Web reporting on the Security Management appliance:

Note Time ranges on report pages are displayed as a Greenwich Mean Time (GMT) offset. For example, Pacific time is GMT + 7 hours (GMT + 07:00).

Note All reports display date and time information based on the systems configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT to accommodate multiple systems in multiple time zones around the world.

Searching Data

Some reports include a field you can use to search for particular data points. When you search for data, the report refines the report data for the particular data set you are searching. You can search for values that exactly match of the string you enter, or for values that start with the string you enter. The following report pages include search fields:

Search Fields	Description
Users	Search for a user by user name or client IP address.
Web Sites	Search for a server by domain or server IP address.
URL Categories	Search for a URL category.
Application Visibility	Search for an application name that the AVC engine monitors and blocks.
Client Malware Risk	Search for a user by user name or client IP address.

Note You need to configure Authentication to view client user IDs as well as client IP addresses.

Choosing Which Data to Chart

The default charts on each Web Reporting page display commonly referenced data, but you can choose to chart different data instead. If a page has multiple charts, you can change each chart. The chart options are the same as the columns headings of the table(s) in the report.

Step 1 Click the **Chart Options** link below a chart.

Step 2 Choose the data to display.

Step 3 Click **Done**.

Custom Reports

You can create a custom report page by assembling charts (graphs) and tables from existing report pages.

To	Do This
Add modules to your custom report page	See: • Modules That Cannot Be Added to Custom Reports , on page 5. • Creating Your Custom Report Page , on page 5
View your custom report page	1. Choose **Monitor** > **Email or Web** > **Reporting** > **Reporting** > **My Reports.** 2. Select the time range to viewThe time range selected applies to all reports, including all modules on the My Reports page. Newly-added modules appear at the top of the relevant section.
Rearrange modules on your custom report page	Drag and drop modules into the desired location.
Delete modules from your custom report page	Click the [X] in the top right corner of the module.
Generate a PDF or CSV version of your custom report	Choose **Reporting** > **Archived Reports** and click **Generate Report Now**.
Periodically generate a PDF or CSV version of your custom report	Choose **Reporting** > **Scheduled Reports.**

Modules That Cannot Be Added to Custom Reports

- Search results , including Web Tracking search results

Creating Your Custom Report Page

Before you begin

- Ensure that the modules that you want to add can be added. See Modules That Cannot Be Added to Custom Reports , on page 5.
- Delete any default modules that you do not need by clicking the [**X**] in the top right corner of those module.

Step 1 Use one of the following methods to add a module to your custom report page:

Note Some modules are available only using one of these methods. If you cannot add a module using one method, try another method.

- Navigate to the report page under the that has the module you want to add, then click the [+] button at the top of the module.
- Go to **Reporting** > **My Reports**, click the [+] button at the top of one of the sections, then select the report module that you want to add. You may need to click the [+] button in each section on the My Reports page in order to find the module that you are looking for.

  You can add each module only once; if you have already added a particular module to your report, the option to add it will not be available.

Step 2 If you add a module that you have customized (for example, by adding, deleting, or reordering columns, or by displaying non-default data in the chart), customize the modules on the My Reports page.

Modules are added with default settings. Time range of the original module is not maintained.

Step 3 If you add a chart that includes a separate legend (for example, a graph from the Overview page), add the legend separately. If necessary, drag and drop it into position beside the data it describes.

Subdomains vs. Second-level Domains in Reporting and Tracking

In reporting and tracking searches, second-level domains (regional domains listed at http://george.surbl.org/two-level-tlds) are treated differently from subdomains, although the two domain types may appear to be the same. For example:

- Reports will not include results for a two-level domain such as `co.uk` , but will include results for `foo.co.uk` . Reports include subdomains under the main corporate domain, such as `cisco.com` .
- Tracking search results for the regional domain `co.uk` will not include domains such as `foo.co.uk` , while search results for `cisco.com` will include subdomains such as `subdomain.cisco.com` .

Printing and Exporting Reports from Report Pages

You can generate a printer-formatted PDF version of any report page by clicking the **Printable (PDF)** link at the top-right corner of the page. You can also export raw data as a comma-separated value (CSV) file by clicking the **Export** link.

Because CSV exports include only raw data, exported data from a Web-based report page may not include calculated data such as percentages, even if that data appears in the Web-based report.

Exporting Report Data

Most reports include an **Export** link that allows you to export raw data to a comma-separated values (CSV) file. After exporting the data to a CSV file, you can access and manipulate the data in it using applications such as Microsoft Excel.

The exported CSV data displays all message tracking and reporting data in Greenwich Mean Time (GMT) regardless of the time zone set on the Web Security appliance. The purpose of the GMT time conversion is to allow data to be used independently from the appliance, or when referencing data from appliances in multiple time zones.

The following example is an entry from a raw data export of the Anti-Malware category report, where Pacific Daylight Time (PDT) is displayed as GMT 07:00 hours:

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name,
 Transactions Monitored, Transactions Blocked, Transactions Detected
 1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100,
2625
```

Category Header	Value	Description
`Begin Timestamp`	`1159772400.0`	Query start time in number of seconds from epoch.
`End Timestamp`	`1159858799.0`	Query end time in number of seconds from epoch.
`Begin Date`	`2006-10-02 07:00 GMT`	Date the query began.
`End Date`	`2006-10-03 06:59 GMT`	Date the query ended.
`Name`	`Adware`	Name of the malware category.
`Transactions Monitored`	`525`	Number of transactions monitored.
`Transactions Blocked`	`2100`	Number of transactions blocked.
`Transactions Detected`	`2625`	Total number of transactions = (Number of transactions detected) + (Number of transactions blocked).

Note - Category headers are different for each type of report.

- If you export localized CSV data, the headings may not be rendered properly in some browsers. This occurs because some browsers may not use the proper character set for the localized text. To work around this problem, you can save the file to your local machine, and open the file in any Web browser using **File > Open**. When you open the file, select the character set to display the localized text.

Enabling Reporting

If your organization has multiple Web Security appliances and uses a Cisco Content Security Management Appliance to manage and view aggregated report data, you must enable centralized reporting on each Web Security appliance.

You can choose the type of reporting based on the appliance setup. You can choose to retain all reports locally, or access them through Cisco Defense Orchestrator if the appliance has been on-boarded to it. If your organization has multiple Web Security appliances and uses a Cisco Content Security Management Appliance, you can choose centralized reporting to manage and view aggregated report data. If you choose Centralized Reporting or local reporting through Cisco Defense Orchestrator, you have to apply these selections on each Web Security appliance.

Step 1 Choose **Security Services** > **Reporting**, and click **Edit Settings**.

a) Select **Local Reporting** to enable reporting on the appliance. The reports will be accessible after logging in to the appliance portal.

b) Select **Local Reporting**, and **Cisco Defense Orchestrator Reporting** to enable reporting through Cisco Defense Orchestrator.

c) Select **Centralized Reporting** to enable reporting through Cisco Content Security Management Appliance.

The Web Security appliance only stores all its collected data for local reporting. If Centralized Reporting is enabled on the appliance, then the Web Security appliance retains *only* System Capacity and System Status data, and those are the only reports available on the Web Security appliance locally.

See the chapter "Using Centralized Web Reporting and Tracking" in your Cisco Content Security Management Appliance user guide for information about configuring this feature on the management appliance.

Step 2 **Submit** and Commit Changes.

Scheduling Reports

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, or previous month.

You can schedule reports for the following types of reports:

- Overview
- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Advanced Malware Protection
- Advanced Malware Protection Verdict Updates
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- SOCKS Proxy
- Reports by User Location
- System Capacity
- My Dashboard

Adding a Scheduled Report

Step 1 Choose **Reporting > Scheduled Reports** and click **Add Scheduled Report**.

Step 2 Choose a report **Type**.

Step 3 Enter a descriptive **Title** for the report.

Avoid creating multiple reports with the same name.

Step 4 Choose a time range for the data included in the report.

Step 5 Select the **Format** for the generated report.

The default format is PDF. Most reports also allow you to save raw data as a CSV file.

Step 6 Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.

Step 7 In the **Schedule** section, choose whether to run the report daily, weekly, or monthly, and at what time.

Step 8 In the **Email to** field, enter the email address(es) to which the generated report is to be sent.

If you do not specify an email address, the report is simply archived.

Step 9 Choose a **Report Language** for the data.

Step 10 Submit and Commit Changes.

Editing Scheduled Reports

Step 1 Choose **Reporting** > **Scheduled Reports**.

Step 2 Select the report title from the list.

Step 3 Modify settings.

Step 4 Submit and Commit Changes.

Deleting Scheduled Reports

Step 1 Choose **Reporting** > **Scheduled Reports**.

Step 2 Select the check boxes corresponding to the reports that you want to delete.

Step 3 To remove all scheduled reports, select the **All** check box.

Step 4 **Delete** and **Commit** Changes.

Note Archived versions of deleted reports are not deleted.

Generating Reports On Demand

Step 1 Choose **Reporting** > **Archived Reports**.

Step 2 Click **Generate Report Now.**

Step 3 Choose a report **Type**.

Step 4 Enter a descriptive **Title** for the report.

Avoid creating multiple reports with the same name.

Step 5 Choose a time range for the data included in the report.

Step 6 Select the **Format** for the generated report.

The default format is PDF. Most reports also allow you to save raw data as a CSV file.

Step 7 Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.

Step 8 Select one of the **Delivery Options**:

- **Archive** the report (the report will appear on the Archived Reports page).
- **Email now to recipients**; provide one or more email addresses.

Step 9 Choose a **Report Language** for the data.

Step 10 Click **Deliver this Report** to generate the report.

Step 11 Commit Changes.

Archived Reports

The **Reporting > Archived Reports** page lists available archived reports. Each name in the Report Title column provides a link to a view of that report. The **Show** menu filters the types of reports that are listed. The column headings can be clicked to sort the data in each column.

The appliance stores up to 12 instances of each scheduled report (up to a total of 1000 reports). Archived reports are stored in the `/periodic_reports` directory on the appliance. Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 12 instances applies to each scheduled report with the same name and time range.

Troubleshooting L4 Traffic Monitor Reports

If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy's data port is recorded and displayed as the client IP address in reports. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses. To do this, see the IronPort AsyncOS for Web User Guide.

Related Topics

- Client Malware Risk Page
- Searching for Transactions Processed by the L4 Traffic Monitor