Filters and Dashboards

This chapter covers the following sections:

Overview of Filters and Dashboards

Cisco Advanced Web Security Reporting lets you define custom searches of the available access, SOCKS and AMP log data, displaying the results of each search separately. This process is also known as “filtering.” As much as possible this filtering is consistent with the native reporting of the Web Security Appliance. Each custom search is displayed on its own page or “panel,” which you can save for future access.

The Cisco Advanced Web Security Reporting application also provides a number predefined searches, which you can choose to view at any time. These existing searches, as well as any saved filters, are referred to as “dashboards”; in fact, saved filters are accessed via the Custom Dashboards menu. Further, the pages or panels on which these searches are displayed are also sometimes referred to as dashboards.

Note Data presented using Cisco Advanced Web Security Reporting may show more information than is available through the Web Security Appliance alone.

Viewing Dashboards

Before you begin

Cisco Advanced Web Security Reporting administrators can control the Web Security appliances (hosts) that you see on the various dashboards. Contact your Cisco Advanced Web Security Reporting administrator with details of any hosts you would like to add, remove, or rename.

Step 1 Sign into the Cisco Advanced Web Security Reporting application using a Web browser.

The **Overview** dashboard presenting summary information is displayed.

Step 2 Either choose an existing dashboard from the other menus, including the **Custom Dashboards** menu, or choose **Custom Filter** to define a new search, which you can then save as a custom dashboard.

See Predefined Dashboards for a list of dashboards provided with Cisco Advanced Web Security Reporting. Using the **Custom Filter** option is described in Creating A Custom Filter.

Step 3 Select a time range, data source and host, if applicable.

Note Searching for data in Custom Dashboards is supported. You can search for data using the main search field with the submit button. You can filter the search results using the secondary search field in the results pane.

Predefined Dashboards

The following dashboards are provided with the Cisco Advanced Web Security Reporting application by default:

- Overview
- User Analysis
  - Overview
  - Location Based
  - User Drilldown
- Browsing Analysis
  - Domain
    - Overview
    - Location Based
    - Domain Drilldown
  - URL Category
    - Overview

        - Location Based
        - URL Category Drilldown

- Application Analysis
    - Overview
    - Application
        - Location Based
        - Application Drilldown
    - Application Type
        - Application Type Drilldown

- Security Analysis
    - L4 Traffic Monitor
        - Overview
        - L4 TM Drilldown
    - Anti Malware
        - Overview
        - Client Malware Risk
        - Location Based
        - Malware Category Drilldown
        - Malware Threat Drilldown
    - Web Reputation Filters
        - Overview
        - Location Based
    - Advanced Malware Protection
        - Overview
        - Location Based
        - File Analysis—You can click the file ID (SHA256) for any entry in the “Completed Analysis Requests from This Appliance” table to open the File Analysis Detail page for that file. The File Analysis Detail page includes a File Analysis Server URL text box in which you can specify the File Analysis server for which you wish to view data. Generally, this URL is `https://intel.api.sourcefire.com` across all Web Security appliance versions through 8.5.

        However, if you used another server for analysis of this particular file (demonstrations perhaps), you can change the server URL here to view the details for this file (as identified by its SHA, which you clicked to arrive at this drill-down report).

    - AMP Verdict Updates

- Web Tracking
    - Proxy Services
    - SOCKS
    - SOCKS Drilldown
- Settings
    - Distributed Environment
    - System
    - Data
    - Users and Authentication
    - Third Party Services
- User
    - Edit Account
- Consolidated Web Security Reports—You can view consolidated reports from Cisco Umbrella and Cisco Web Security appliances under following categories:
    - Overview
    - Activity Search
    - Security Activity
    - Top Domains
    - Top Categories
    - Top Users
    - Top Security Categories

Related Information:

- Viewing Dashboards

Save As Dashboard

On each **predefined report** page, you can save the displayed report as a another dashboard, in effect cloning the currently displayed dashboard.

Note You also can save a custom filter as a dashboard, as described in Saving a Custom Filter as a Dashboard. These dashboards can be accessed and edited like any other custom dashboard.

Step 1 On the current **report page**, modify the time, data-source and host parameters as desired, then click the **Save As Dashboard** button.

Step 2 Provide the following information in the **Save As Dashboard Panel** dialog box:

- Dashboard Title—A display name for the new dashboard.

  When saving any report page as a dashboard, you must provide a proper title to reflect the input selected in order to differentiate the custom dashboards.

- Dashboard ID—Provide a file name for saving the dashboard; cannot be changed later.
- Dashboard Description—(Optional) A short description.
- Dashboard Permissions—Select **Private** or **Shared in App**. Private dashboards are visible only to you, while Shared dashboards are visible to all users.

Step 3 Click **Save**.

The new dashboard is added to the **Custom Dashboards** menu; choose a custom dashboard from the menu to view and edit that dashboard.

Editing A Custom Dashboard

You can edit the currently displayed custom dashboard, repositioning and deleting individual report panels, changing the dashboard title and description, modifying the time range for search queries in those panels, modifying a panel’s chart type, and so on.

Step 1 Click the **Edit** button in the current custom dashboard and choose one of the following options:

- **Edit Panels**—Enable panel editing: drag a panel title bar to reposition it; click its close button to delete a panel; add a label above the panel’s title; click the appropriate button to:
  - Change the panel chart type.
  - Change chart parameters.
- **Edit Title or Description**—Change the title and description of the entire dashboard.
- **Edit Permissions** —— Change the viewing permission for the entire dashboard.
- **Schedule PDF Delivery**—Schedule regular generation of a report PDF from this dashboard; the generated PDF is then emailed to the address(es) you have specified.
- **Delete**—Delete entire dashboard.

Step 2 You aslo can click **Add Panel** to add a panel from similar custom dashboards to this dashboard.

This button is displayed after you click the custom dashboard's **Edit** button.

Step 3 Click **Done** when you are finished editing this dashboard.

Creating A Custom Filter

When you configure a custom filter, the Cisco Advanced Web Security Reporting searches the "data model" you have selected, filtering and displaying the model's data set by "data object(s)," or "attribute(s)," which you have also selected. Each available data model represents a set of logs of a specific type, while each data object represents a specific log type, or sometimes a data set, that is a child component of the current data model.

Follow these steps to filter and display a specific set of log data:

Step 1 Click **Custom Filter** in the Cisco Advanced Web Security Reporting's menu bar.

Step 2 On the Select a Data Model page, choose the data model to search:

- **AMP Access Model** – all available Advanced Malware Protection logs.
- **SOCKS Access Model** – all available SOCKS logs.
- **Web Access Data** – all other available web-related logs (for example, access logs related to user and domain).
  - The following fields in this data model contain values from Cisco Umbrella logs. These fields can be used to create a custom dashboard for Umbrella logs by selecting the *sourcetype* as *ciscoumbrella* in the filter drop-down list:

Field	Umbrella Log Data
user_id_fixed	External or internal IP. Also contains Most Granular Identity, if available.
dest_domain	Domain requested.
odnsaction	Action taken against DNS requests.
x_wbrs_threat_type_fixed	Malware category if the DNS request was for a malicious domain.
x_webcat_code_full	URL category of the domain requested.
dnsquery_fixed	Type of DNS request made.
dnsresp_fixed	DNS return code for the request.

Each data model represents the collected logs of the named type.

Step 3 On the **Select a Dataset** page:

a. Expand the list of data objects available in the selected Data Model by clicking the right-arrow preceding the Data Model Event name (for example, “Web Access Event”).

b. Click a data object (Event or Attribute) and then choose either **Top Values** or **Top Values by Time**.

If you choose **Top Values**, the chosen Attribute data is displayed in rows; each row presents a second column displaying the event count for that particular Attribute entry.

If you choose **Top Values by Time**, `_time` is the filter for **Split Rows**, and the chosen Attribute is the **Split Columns** filter. That is, each row represents an event time and each column represents a specific Attribute entry; thus, each table cell presents the number of occurrences of the given Attribute at a specific time.

Note The symbol preceding each Attribute entry indicates its type; for example, an alphanumeric or numeric value.

Step 4 If you chose **Top Values** in the previous step, you can additionally filter the displayed data by choosing another Attribute from the **Split Columns** menu.

Step 5 You can further adjust the information presented, and its presentation, on the custom filter dashboard, as desired. See Changing and Saving the Custom Filter Display for more information.

Step 6 To save this custom filter dashboard, choose **Save As** > **Dashboard Panel**; it will appear in the **Custom Dashboards** menu under the name you provide.

Note Whenever the current filter’s table or chart is being loaded or refreshed, you can click the Pause or Stop buttons. You can click Reload at any other time to reload the filtered data.

Changing and Saving the Custom Filter Display

After creating a custom filter, you can use the options presented on the **New Custom Filter** page to successively apply additional filtering, thus further refining the information displayed. For example, in addition to using the Split Rows feature to split the current data set into rows, one per data entry, and then using Split Columns to add columns to each row, representing information extracted from each row entry, you can also apply parameters and attributes using the Filters and Column Values menus.

You can also select another Data Model, or another Data Object; you can change the formatting, and export and print the data on the page; you can change the chart type; and you can save this custom filter as a dashboard. The options on the New Custom Filter panel are:

- **Chart type**—Click a button in the data-display-type strip on the left side of the application window to change how the custom-filter data is displayed; for example, you might select a bar or a pie chart.
- **Save As**—Save the current filter as a dashboard; it will be added to the Custom Dashboards menu. SeeSaving a Custom Filter as a Dashboard for more information.
- **Clear**—clears the current custom filter parameters and the data display.
- **Web Access Event**
  - You can select another Data Model; as described in Creating A Custom Filter.
  - You can select another data Object from the currently selected Data Model; as described in Creating A Custom Filter.
  - Information about the currently displayed data set is also presented.

- **Filters**—For any displayed Filter, click the edit button (pencil icon) to change the parameters applied to that filter, or to remove that filter from the display. You can click the add (+) button to choose another data Object to the current set of Filters.
- **Split Rows**—You can edit current Row object parameters, delete a Row object, and add objects to the Split Rows as described for Filters.
- **Split Columns**—Similarly, you can edit current Column object parameters, delete a Column object, and add objects to the Split Columns.
- **Column Values**—You can also edit, delete and Column Values.

Note If there are multiple objects displayed for any given option, you can drag the object boxes to re-order them. For example, if the currently chosen Filters, in order from left to right, are `All time, category is *`, and `dest_url`, you can drag `dest_url` between the other two so the order becomes `All time, dest_url`, and `category is *`.

Saving a Custom Filter as a Dashboard

On each **custom filter** page, you can save the displayed filter as a custom dashboard, making it readily available for future viewing.

Step 1 On the current **custom filter** page, modify the search parameters as desired, click the **Save As** button and then choose **Dashboard Panel**.

Step 2 In the **Save As Dashboard Panel** dialog box, specify a type for this dashboard: either **New** or **Existing**.

a. If you selected **New**, provide the following information:

- Dashboard Title—(Optional) A display name for the new dashboard.

  When saving any report page as a dashboard, you must provide a proper title to reflect the input selected in order to differentiate the custom dashboards.
- Dashboard ID—Provide a file name for saving the dashboard; this cannot be changed later.
- Dashboard Description—(Optional) A short description.
- Dashboard Permissions—Select **Private** or **Shared in App**. Private dashboards are visible only to you, while Shared dashboards are visible to all users.
- Panel Title(Optional)—This is the title displayed at the top of the panel when you view this custom dashboard.
- Panel Powered By—This is always **Inline Search**.
- Panel Content—Select **Statistics** or <*chart type*> to display this filter's information as tabular data, or as the chart type currently used for display.

b. If you selected **Existing**, provide the following information:

- Select—Choose the name of the existing custom dashboard to which this filter data is to be added.
- Panel Title—(Optional) This is the title displayed at the top of the panel when you view this custom dashboard.

- Panel Powered By—This is always **Inline Search**.
- Panel Content—Select **Statistics** or <*chart type*> to display this filter's information as tabular data, or as the chart type currently used for display.

Step 3 Click **Save**.

The new dashboard is added to the **Custom Dashboards** menu; choose a custom dashboard from the menu to view and edit that dashboard.

Exporting Data

- Exporting the Current Custom Filter Panel
- Exporting the Current Dashboard to a PDF File

Exporting the Current Custom Filter Panel

You can export the currently displayed custom-filter data as a comma-separated values (csv) file, an XML file, or a JavaScript Object Notation (json) file.

Step 1 Click the **Export** button.

Step 2 In the **Export Results** dialog box:

a. Choose the desired **Format**: **CSV**, **XML**, or **JSON**.

b. (Optional) Provide a **File Name** if desired.

If you do not enter a file name, a random-number name is generated for you.

c. Specify the **Number of Results** to be saved: click either **Unlimited** or **Limited**.

If you select **Unlimited**, all data returned by your current filter parameters are saved. If you select **Limited**, specify the **Max Results**—the maximum number of displayed values—to be saved.

Step 3 Click **Export** to close the dialog box and create the export file.

Step 4 An **Open/Save** dialog box appears; you can open the export file using the application defined on your system for files of the chosen **Format**, or you can elect to save the file to a location you specify.

Exporting the Current Dashboard to a PDF File

You can export the currently displayed dashboard as a PDF file.

Before you begin

- Verify that the Cisco Advanced Web Security Reporting administrator has enabled PDF output.

Step 1 Click the **Export PDF** button.

Step 2 An **Open/Save** dialog box appears; you can open the PDF file using the application defined on your system for PDF files (usually Adobe Reader), or you can elect to save the file to a location you specify.

Exporting the Current Dashboard to Other File Formats

You can export the currently displayed dashboard data as a comma-separated values (csv) file, an XML file, or a JavaScript Object Notation (json) file.

Step 1 Hover over the dashboard data display pane.

Step 2 Click the download icon ⤓.

a. Choose the desired **Format**: **CSV**, **XML**, or **JSON**.

b. (Optional) Provide a **File Name** if desired.

If you do not enter a file name, a random-number name is generated for you.

c. Specify the **Number of Results** to be saved: click either **Unlimited** or **Limited**.

If you select **Unlimited**, all data returned by your current filter parameters are saved. If you select **Limited**, specify the **Max Results**—the maximum number of displayed values—to be saved.

Step 3 Click **Export** to close the dialog box and create the export file.

Step 4 An **Open/Save** dialog box appears; you can open the export file using the application defined on your system for files of the chosen **Format**, or you can elect to save the file to a location you specify.

Related Information:

- Set Up Scheduled PDF Reporting (Optional)

Data Formats

In some cases, the presentation of data in Cisco Advanced Web Security Reporting differs from the presentation of data available through the native reporting in source applications.

Data	Format Example
Large numbers (greater than seven digits)	`2E11` represents 2 x 1011
Time	`d+hh:mm:ss.ms` indicates elapsed days, hours, minutes, seconds, and milliseconds. For example, `1+03:22:36.00` represents one day, three hours, 22 minutes, 36 seconds, and zero milliseconds.

Time Ranges

Tip Select a smaller time range to return results more quickly.

Timing of Data Availability

Range	Indexing Begins	Data Appears in Reports
Hour	Just past the hour	60-90 minutes after indexing begins
Day	After midnight daily	One day after indexing begins
Week	After midnight Saturday(early Sunday morning)	One week after indexing begins
90 Days	After midnight of the 90th day.	90 days after indexing begins.
Custom: Less than hourly	Just past the hour	60-90 minutes after indexing begins
Custom: Less than daily	After midnight daily	One day after indexing begins
Custom: Less than weekly	After midnight Saturday(early Sunday morning)	One week after indexing begins

Troubleshooting

- Cisco Advanced Web Security Reporting uses a set of files to populate menus. If you experience problems with the menus, verify that the application’s look-ups folder contains all the necessary files including:
  - `malware_categories.csv`
  - `transaction_types.csv`
  - `url_categories.csv`
  - `malware_categories_opendns.csv`
  - `url_categories_opendns.csv`
- The administrator can edit the list of URL categories visible within the application. When a category appears within the access log, but is not present in the look-up file, Cisco Advanced Web Security Reporting displays “Custom Category.”
- Administrators can control the options available in the drop-down fields in the Web Tracking form.

Usage Scenarios

User Investigation

This example demonstrates how a system administrator would investigate a particular user at a company. In this scenario, a manager has received a complaint that an employee is visiting inappropriate Web sites at work. To investigate this, the system administrator now needs to look at the employee's Web usage trends and transaction history:

- URL Categories by Total Transactions
- Trend by Total Transactions
- URL Categories Matched
- Domains Matched
- Applications Matched
- Malware Threats Detected
- Policies Matched for a particular User ID or Client IP
- AD Group Details

Using these reports, the system administrator can discover whether, for example, user "johndoe" was trying to access blocked URLs, which can be viewed in the Transactions Blocked column under the Domains section.

Viewing Web Usage Trends

Step 1 Select **Users** from the **Cisco Advanced Web Security Reporting** drop-down menu.

Step 2 Click the **User ID** or **Client IP address**.

Note If you do not see the **User ID** or **Client IP address** you want to investigate in the **Users** table, click any User ID or Client IP. Then search for all or part of the User ID or Client IP address.

Step 3 (Optional) Select **Actions** > **Print**.

Viewing Transaction History

Step 1 Select **Web Tracking** from the **Cisco Advanced Web Security Reporting** drop-down menu.

Step 2 Select **Proxy Services**.

Step 3 You can search with the following criteria:

- Day
- Data Source

- User ID or Client IP
- User (Enter an authentication username as it appears in reports.)
- Client IP (The client IP address that you want to track. If you leave this field empty, the search returns results for all users.)
- Website
- Transaction Type (All transactions, completed, blocked, monitored, or warned)
- Hostname
- SNI (Retrieves hierarchy)
- WBRS: Min Score Range (You can filter by web reputation score and by a particular web reputation threat. (Select the lower value of the WBRS score range that you want to filter)
- WBRS: Max Score Range (Select the upper value of the WBRS score range that you want to filter)
- (Optional) Advanced (Select this check box to see additional filter options)
- Show WBRS: No Score (You can filter and see results that have no web reputation score. To see transactions that has no WBRS score, select **Show WBRS: No Score** as “True”. To see only those transactions that has no WBRS score, select **WBRS: Min Score Range** and **WBRS: Min Score Range** as “NA” and select **Show WBRS: No Score** as “True”.)
- URL Category
- Application
- Application Type
- Policy
- Malware Threat
- Malware Category
- Reputation Threat
- User Location
- AMP File Verdict
- Filename
- File SHA256

Step 4 (Optional) Click **Export** to export the data to a CSV file. You can view and export 10000 transactions from the **Proxy Services** dashboard.

URLs Visited

In this scenario, a Sales manager wants to discover the top five visited Web sites at their company for the last week. Additionally, the manager wants to know which users are going to those Websites.

Viewing Most Visited Web Sites

Step 1 Select **Web Sites** from the Cisco Advanced Web Security Reporting drop-down menu.

Step 2 Select **Week** from the Time Range drop-down list.

Step 3 View the top 25 domains in the Domains Matched table.

Step 4 Click a domain to view the users who have visited that domain in order of frequency.

URL Categories Visited

In this scenario, the Human Resources manager wants to know what the top three URL categories all employees have visited over the past 30 days. Additionally, a network manager wants to get this information to monitor bandwidth usage, to find out what URLs are taking up the most bandwidth on the network. The example below is to show how you can gather data for several people covering several points of interest, while only having to generate one report.

Viewing Most Common URL Categories

Step 1 Select **URL Categories** from the **Cisco Advanced Web Security Reporting** drop-down menu.

Step 2 View the top ten URL Categories by Total Transactions graph.

Step 3 (Optional) Click the **Export PDF** button. Save the PDF and send it to the appropriate people.

Step 4 View the Bytes Allowed column in the URL Categories Matches table.

Step 5 (Optional) Click the **Export PDF** button. Save the PDF and send it to the appropriate people.

Step 6 For finer granularity, select a specific URL Category.