



Working With Reports on the Cloud Email Security Management Console

This chapter contains the following sections:

- [Ways to View Reporting Data](#) , page 1
- [How the Security Management Appliance Gathers Data for Reports](#), page 2
- [Using the Interactive Report Pages](#), page 3
- [Customizing Your View of Report Data](#) , page 4
- [Viewing Details of Messages or Transactions Included in Reports](#) , page 6
- [Improving Performance of Email Reports](#) , page 7
- [Printing and Exporting Reporting Data](#) , page 8
- [Troubleshooting All Reports](#) , page 9

Ways to View Reporting Data

The following table shows the different ways to view reporting data:

Table 1: Ways To View Reporting Data

To	See
View and customize web-based interactive report pages	<ul style="list-style-type: none">• Using the Interactive Report Pages, on page 3• Customizing Your View of Report Data , on page 4• Using Centralized Email Security Reporting on the Legacy Web Interface
Automatically generate recurring CSV reports	Scheduling Email Reports
Generate a CSV report on demand	Generating Email Reports On Demand

To	See
Export raw data as a CSV (Comma-separated values) file	Printing and Exporting Reporting Data Exporting Report Data as a Comma Separated Values (CSV) File
Email report information to yourself and other people	Scheduling Email Reports Generating Email Reports On Demand
Find information about specific transactions	Viewing Details of Messages or Transactions Included in Reports



Note For differences between logging and reporting, see [Logging Versus Reporting](#).

How the Security Management Appliance Gathers Data for Reports

The Security Management appliance pulls data for all reports from all managed appliances approximately every 15 minutes and aggregates the data from these appliances. Depending on your appliance, it may take awhile for a particular message to be included in the reporting data on the Security Management appliance. Check the **System Status** page for information on your data.

Reporting Data includes transactions involving both IPv4 and IPv6.



Note When gathering data for reports, the Security Management appliance applies the timestamp from the information that was set when you configured the time settings on the Security Management appliance. For information on setting the time on your Security Management appliance, see the [Configuring the System Time](#).

How Reporting Data is Stored

All of the appliances store reporting data. The following table shows what time periods that each appliance stores data.

Table 2: Reporting Data Storage on the Email Security Appliances

	Minute	Hourly	Daily	Weekly	Monthly	Yearly
Local Reporting on Email Security appliance	•	•	•	•	•	

	Minute	Hourly	Daily	Weekly	Monthly	Yearly
Centralized Reporting on Email Security appliance	•	•	•	•		
Security Management appliance		•	•	•	•	•

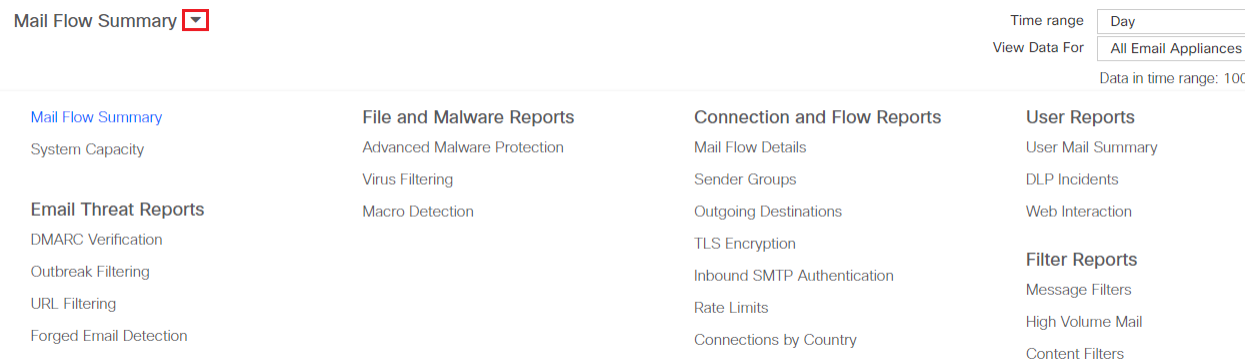
About Reporting and Upgrades

New reporting features may not apply to transactions that occurred before upgrade, because the required data may not have been retained for those transactions. For possible limitations related to reporting data and upgrades, see the Release Notes for your release.

Using the Interactive Report Pages

You can view the email reports for the Email Security appliance using the Reports drop-down as shown in the following figure:

Figure 1: Reports Drop-down



The Mail Flow Summary report page is the landing page (the page displayed after login).

Email reports are categorized into the following report pages under the reporting drop-down:

- Email Threat Reports
- File and Malware Reports
- Connection and Flow Reports
- User Reports
- Filter Reports

Customizing Your View of Report Data

You can customize your view while viewing the report data in the web interface.

To	Do This
Specify a time range	See Choosing a Time Range for Reports .
View data per appliance or reporting group	See Viewing Reporting Data for an Appliance or Reporting Group
Customize tables	See Customizing Tables on Report Pages , on page 5
Customize views	See Customizing Views on Report Pages , on page 5
Using Counters to Filter Data on Trend Graph	See Using Counters to Filter Data on the Trend Graphs , on page 6
Specify report-related preferences	See Setting Preferences
Search for specific information or a subset of data to view	<ul style="list-style-type: none"> • For Email reports, see Searching and the Interactive Email Report Pages. • Some tables include links (in blue text) to details for aggregated data. For more information, see Viewing Details of Messages or Transactions Included in Reports.



Note


All customization features are not available for every report.

Viewing Reporting Data for an Appliance or Reporting Group

For Mail Flow Summary and System Capacity reports for Email, you can view data from all appliances, or from any one centrally-managed appliance.

For Email reports, if you have created groups of Email Security appliances as described in [Creating Email Reporting Groups](#), you can view the data for each reporting group.

To specify the view, select an appliance or group from the **View Data For** list on supported pages.

If you are viewing report data on the Cloud Email Security Management Console to which you have recently taken backup from another Security Management appliance, you must first add (but do not establish a connection to) each appliance in  > **Management Appliance** > **Centralized Services** > **Security Appliances**.

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 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.






Tip You can specify a default time range that will always display each time you log in. For information, see [Setting Preferences](#).

Customizing Views on Report Pages

Most report pages allow you to choose between graphical view, tabular view or combined view. The view that you select is used to show the data on the report pages.



Table 3: Customizing Views on Report Pages

To	Do This
Show data in graph view.	Click  to view data in graphical format.
Show data in table view.	Click  to view data in tabular format.
View details about a table entry, where available	Click a blue entry in the table.
Show data in combined view.	Click  to view data in graphical and tabular format.

Customizing Tables on Report Pages

You can view, customize and sort information on the interactive tables within the report pages. The view that you select is used to show the data on the report pages.

Table 4: Customizing Tables on Report Pages

<ul style="list-style-type: none"> • Show additional columns • Hide visible columns • Determine available columns for a table 	<ol style="list-style-type: none"> 1  Click . 2 Select the columns to display, and click Close. 	<p>For most tables, some columns are hidden by default.</p> <p>Each report page offers different columns.</p> <p>See the table column descriptions for the respective tables.</p>
Sort the table by the heading of your choice.	Click a column heading.	-
View details about a table entry, where available	Click a blue entry in the table	See also Viewing Details of Messages or Transactions Included in Reports .
View details of additional rows.	Scroll down on a table to display details of additional rows.	-

Using Counters to Filter Data on the Trend Graphs

You can filter data based on the required time range and available counters on a trend graph.

The time range that you select in the Time Range drop-down, is used for a trend graph until you select a different value.

A counters on a trend graph of the Mail Flow Summary report page is used to view data specific to different filters. Click on an available counter to filter the data.

Viewing Details of Messages or Transactions Included in Reports

Step 1 Click any blue number in a table on a report page.
(Not all tables have these links.)

The messages or transactions included in that number are displayed in Message Tracking.

Step 2 Scroll down to see the list of messages or transactions.

What to Do Next

- [Tracking Messages](#)

Improving Performance of Email Reports

If the performance of aggregated reporting decreases due to a large number of unique entries over the course of a month, use reporting filters to restrict the aggregation of data in reports that cover the previous year (Last Year reports). These filters can restrict detailed, individual IP, domain, or user data in reports. Overview reports and summary information remain available for all reports.

You can enable one or more of the reporting filters using the **reportingconfig > filters** menu in the CLI. The changes must be committed to take effect.

- **IP Connection Level Detail.** Enabling this filter prevents the Security Management appliance from recording information about individual IP addresses. This filter is appropriate for systems that process a large number of incoming IP addresses due to attacks.

This filter affects the following Last Year reports:

- Sender Profile for Incoming Mail
- IP Addresses for Incoming Mail
- IP Addresses for Outgoing Senders

- **User Detail.** Enabling this filter prevents the Security Management appliance from recording information about individual users sending and receiving mail and the content filters that are applied to the users' mail. This filter is appropriate for appliances that process mail for millions of internal users or if the system does not validate recipient addresses.

This filter affects the following Last Year reports:

- Internal Users
- Internal User Details
- IP Addresses for Outgoing Senders
- Content Filters

- **Mail Traffic Detail.** Enabling this filter prevents the Security Management appliance from recording information about individual domains and networks that the appliances monitor. This filter is appropriate when the number of valid incoming or outgoing domains is measured in the tens of millions.

This filter affects the following Last Year reports:

- Domains for Incoming Mail
- Sender Profile for Incoming Mail
- Internal User Details
- Domains for Outgoing Senders

**Note**

To view up-to-the-minute reporting data for the preceding hour, you must log in to an individual appliance and view the data there.

Printing and Exporting Reporting Data

Table 5: Printing and Exporting Reporting Data

To Get This	CSV	Do This	Notes
Raw data See also Exporting Report Data as a Comma Separated Values (CSV) File	•	Click the Export link below the chart or table.	The CSV file contains all applicable data, including the data visible in the chart or table.
	•	Create a scheduled or on-demand report. See: <ul style="list-style-type: none"> • Generating Email Reports On Demand • Scheduling Email Reports 	Each CSV file may contain up to 100 rows. If a report contains more than one table, a separate CSV file is created for each table. Some extended reports are not available in CSV format.

Exporting Report Data as a Comma Separated Values (CSV) File

You can export raw data to a comma-separated values (CSV) file, which you can access and manipulate using database applications such as Microsoft Excel. For different ways to export data, see [Printing and Exporting Reporting Data](#).

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.

For email message tracking and reporting data, the exported CSV data will display all data in GMT regardless of what is set on the Security Management appliance. This simplifies using data independently from the appliance, particularly 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 - 7 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

Table 6: Viewing Raw Data Entries

Category Header	Value	Description
Begin Timestamp	1159772400.0	Query start time in number of seconds from epoch.

Category Header	Value	Description
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 on any web browser using **File > Open**. When you open the file, select the character set to display the localized text.

Troubleshooting All Reports

Unable to View Report Data on Backup Security Management Appliance

Problem

You are unable to select a single Email Security appliance for which to view report data. The **View Data For** option does not appear on the reporting page.

Solution

See also [Availability of Services During Backups](#).

Reporting Is Disabled

Problem

Canceling a backup in progress can disable reporting.

Solution

Reporting functionality will be restored after a backup is completed.

Reporting Is Disabled