



# Using Centralized Email Security Reporting on the Cloud Email Security Management Console

---

This chapter contains the following sections:

- [Centralized Email Reporting Overview, page 1](#)
- [Setting Up Centralized Email Reporting, page 2](#)
- [Working with Email Report Data , page 4](#)
- [Understanding the Email Reporting Pages, page 6](#)
- [About Scheduled and On-Demand Email Reports , page 49](#)
- [Scheduled Reports Page , page 53](#)
- [Scheduling Email Reports, page 53](#)
- [Generating Email Reports On Demand , page 55](#)
- [Archived Email Reports Page , page 56](#)
- [Viewing and Managing Archived Email Reports , page 57](#)

## Centralized Email Reporting Overview

Your Cisco Content Security Management appliance shows aggregated information from individual or multiple Email Security appliances so that you can monitor your email traffic patterns and security risks. You can run reports in real-time 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. Reporting functionality also allows you to export raw data to a file.

This feature centralizes the reports listed under the Monitor menu of the Email Security appliance.

The Centralized Email Reporting feature not only generates high-level reports, allowing you to understand what is happening on their network, but it also allows you to drill down and see traffic details for a particular domain, user, or category.

The Centralized Tracking feature allows you to track email messages that traverse multiple Email Security appliances.

**Note**

The Email Security appliance only stores data if local reporting is used. If centralized reporting is enabled for the Email Security appliance then the Email Security appliance does NOT retain any reporting data except for System Capacity and System Status. If Centralized Email Reporting is not enabled, the only reports that are generated are System Status and System Capacity.

For more information about availability of report data during and after the transition to centralized reporting, see the “Centralized Reporting Mode” section of the documentation or online help for your Email Security appliance.

## Setting Up Centralized Email Reporting

To set up centralized email reporting, complete the following procedures in order:

**Note**

If reporting and tracking are not consistently and simultaneously enabled and functioning properly, or are not consistently and simultaneously either centralized or stored locally on each Email Security appliance, then the message tracking results when drilling down from reports will not match expected results. This is because the data for each feature (reporting, tracking) is captured only while that feature is enabled.

## Enabling Centralized Email Reporting on the Security Management Appliance

### Before You Begin

- All Email Security appliances should be configured and working as expected before you enable centralized reporting.
- Before enabling centralized email reporting, ensure that sufficient disk space is allocated to that service. See the [Managing Disk Space](#).

**Step 1**

[New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.

**Step 2**

Choose **Management Appliance > Centralized Services > Centralized Reporting**.

**Step 3**

Click **Enable**.

**Step 4**

If you are enabling centralized email reporting for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.

**Step 5**


Submit and commit your changes.

**Note**

If you have enabled email reporting on the appliance, and there is no disk space allocated for this action, centralized email reporting will not work until disk space is allocated. As long as the quota you are setting the Email Reporting and Tracking to is larger than the currently used disk space, you will not lose any reporting and tracking data. See the [Managing Disk Space](#) section, for more information.

## Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance

The steps you follow depend on whether or not you have already added the appliance while configuring another centralized management feature.

- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** If you have already added the Email Security appliance to the list on this page:
- Click the name of an Email Security appliance.
  - Select the **Centralized Reporting** service.
- Step 4** If you have not yet added Email Security appliances:
- Click Add Email Appliance.
  - In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Security Management appliance.  
**Note** If you enter A DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.
  - The Centralized Reporting service is pre-selected.
  - Click **Establish Connection**.
  - Enter the user name and password for an administrator account on the appliance to be managed, then click **Establish Connection..**  
**Note** You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.
  - Wait for the Success message to appear above the table on the page.
  - Click **Test Connection..**
  - Read test results above the table.
- Step 5** Click **Submit**.
- Step 6** Repeat this procedure for each Email Security appliance for which you want to enable Centralized Reporting.
- Step 7** Commit your changes.
- 

## Enabling Centralized Email Reporting on Email Security Appliances

You must enable centralized email reporting on each managed Email Security appliance.

For instructions, see the “Configuring an Email Security Appliance to Use Centralized Reporting” section of the documentation or online help for your Email Security appliance.


## Creating Email Reporting Groups

You can create groups of Email Security appliances for which to view reporting data from the Security Management appliance.

A group can include one or more appliances, and an appliance may belong to more than one group.

### Before You Begin

Make sure centralized reporting is enabled for each appliance. See [Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance](#), on page 3.

- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Management Appliance > Centralized Services > Centralized Reporting**.
- Step 3** Click **Add Group**.
- Step 4** Enter a unique name for the group.  
The Email Security appliance list displays the Email Security appliances that you added to the Security Management appliance. Select the appliances that you want to add to the group.  
  
The maximum number of groups that can be added is smaller than or equal to the maximum number of email appliances that can be connected.
- Note** If you added an Email Security appliance to the Security Management appliance, but you do not see it in the list, edit the configuration of the Email Security appliance so that the Security Management appliance is collecting reporting data from it.
- Step 5** Click **Add** to add the appliances to the Group Members list.
- Step 6** Submit and commit your changes.
- 

## Working with Email Report Data

- For options for accessing and viewing report data, see [Ways to View Reporting Data](#).
- To customize your view of report data, see [Customizing Your View of Report Data](#).
- To print or export report information, see [Printing and Exporting Reporting Data](#).
- To understand the various interactive report pages, see [Using the Interactive Report Pages](#).
- To generate a report on demand, see [Generating Email Reports On Demand](#).
- To schedule reports to run automatically at intervals and times that you specify, see [Scheduling Email Reports](#).
- To view archived on-demand and scheduled reports, see [Viewing and Managing Archived Email Reports](#).
- For background information, [How the Security Management Appliance Gathers Data for Reports](#).
- To improve performance when working with large amounts of data, see [Improving Performance of Email Reports](#).

- To get details about an entity or number that appears as a blue link in a chart or table, click the entity or number.

For example, if your permissions allow you to do so, you can use this feature to view details about messages that violate Content Filtering or Data Loss Prevention policies. This performs the relevant search in Message Tracking. Scroll down to view results.

## Searching and the Interactive Email Report Pages

Many of the interactive email reporting pages include a ‘**Search For:**’ drop-down menu at the bottom of the page.

From the drop-down menu, you can search for several types of criteria, including the following:

- IP address
- Domain
- Network owner
- Internal user
- Destination domain
- Internal sender domain
- Internal sender IP address
- Incoming TLS domain
- Outgoing TLS domain
- SHA-256

For most searches, choose whether to exactly match the search text or look for items starting with the entered text (for example, starts with “ex” will match “example.com”).

For IPv4 searches, the entered text is always interpreted as the beginning of up to four IP octets in dotted decimal format. For example, ‘17.\*’ will search in the range 17.0.0.0 through 17.255.255.255, so it will match 17.0.0.1 but not 172.0.0.1. For an exact match search, enter all four octets. IP address searches also support Classless Inter-Domain Routing (CIDR) format (17.16.0.0/12).

For IPv6 searches, you can enter addresses using the formats in the following examples:

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

# Understanding the Email Reporting Pages



## Note

This list represents the reports available in the latest supported release of AsyncOS for Email Security appliances. If your Email Security appliances are running earlier releases of AsyncOS, not all of these reports are available.

**Table 1: Email Reporting Drop-down Options**

Email Reporting Menu	Action
Mail Flow Summary Page	<p>The Mail Flow Summary report page provides a synopsis of the activity on your Email Security appliances. It includes graphs and summary tables for the incoming and outgoing messages.</p> <p>For more information, see the <a href="#">Mail Flow Summary Page</a>, on page 9.</p>
<b>Email Threat Reports</b>	
DMARC Verification Page	<p>The DMARC Verification report page shows the top sender domains that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification, and a summary of the actions taken for incoming messages from each domain.</p> <p>For more information, see the <a href="#">DMARC Verification Page</a>, on page 14.</p>
Outbreak Filtering Page	<p>The Outbreak Filters page shows information about recent outbreaks and the messages quarantined by Outbreak Filters. Use this page to monitor your defense against phishing, scam, virus and malware attacks.</p> <p>For more information, see the <a href="#">Outbreak Filtering Page</a>, on page 15.</p>
URL Filtering Page	<p>Use this page to view the URL categories most frequently occurring in messages, the most common URLs in spam messages, and the number of malicious and neutral URLs seen in messages.</p> <p>For more information, see the <a href="#">URL Filtering Page</a>, on page 16.</p>
Forged Email Detection Page	<p>The Forged Email Detection report page includes the following reports:</p> <ul style="list-style-type: none"> <li>• <b>Top Forged Email Detection.</b> Displays the top ten users in the content dictionary that matched the forged From: header in the incoming messages.</li> <li>• <b>Forged Email Detection: Details.</b> Displays a list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched.</li> </ul> <p>For more information, see the <a href="#">Forged Email Detection Page</a>, on page 18.</p>

Email Reporting Menu	Action
<b>File and Malware Reports</b>	
Advanced Malware Protection Page (File Reputation and File Analysis)	<p>The Advanced Malware Protection report page shows reporting views that displays details of Summary, File Reputation, File Analysis, File Retrospection and Mailbox Auto Remediation, for incoming and outgoing file-based threats.</p> <p>For more information, see the <a href="#">Advanced Malware Protection Page</a> , on page 18.</p>
Virus Filtering Page	<p>The Virus Filtering report page provides an overview of the viruses that are sent to and from your network. This page displays the viruses that have been detected by the virus scanning engines running on the Email Security appliances and are displayed on the Security Management appliance. Use this report to take action against a particular virus.</p> <p>For more information, see the <a href="#">Virus Filtering Page</a>, on page 23.</p>
Macro Detection Page	<p>The Macro Detection report page shows the top incoming and outgoing macro-enabled attachments by file type detected by the content filter and message filters.</p> <p>For more information, see the <a href="#">Macro Detection Page</a>, on page 25.</p>
<b>Connection and Flow Reports</b>	
Mail Flow Details Page	<p>The Mail Flow Details report page provides interactive reporting on the real-time information for all remote hosts connecting to your managed Email Security appliances. You can gather information about the IP addresses, domains, and network owners (organizations) sending mail to your system.</p> <p>For more information, see the <a href="#">Mail Flow Details Page</a>, on page 25.</p>
Sender Groups Page	<p>The Sender Groups report page provides a summary of connections by sender group and mail flow policy action, allowing you to review SMTP connection and mail flow policy trends.</p> <p>For more information, see the <a href="#">Sender Groups Page</a>, on page 31.</p>
Outgoing Destinations Page	<p>The Outgoing Destinations report page provides information about the domains that your organization sends mail to. The top of the page includes graphs depicting the top destinations by outgoing threat messages and top destinations by outgoing clean messages. The bottom of the page displays a chart with columns sorted by total recipients (default setting).</p> <p>For more information, see the <a href="#">Outgoing Destinations Page</a>, on page 31.</p>
TLS Encryption Page	<p>The TLS Encryption report page shows the overall usage of TLS connections for sent and received mail. The report also shows details for each domain sending mail using TLS connections.</p> <p>For more information, see the <a href="#">TLS Encryption Page</a>, on page 33.</p>

Email Reporting Menu	Action
Inbound SMTP Authentication Page	<p>The Inbound SMTP authentication report page shows the use of client certificates and the SMTP AUTH command to authenticate SMTP sessions between the Email Security appliance and users' mail clients.</p> <p>For more information, see the <a href="#">Inbound SMTP Authentication Page</a>, on page 36.</p>
Rate Limits Page	<p>The Rate Limits report page shows the mail senders (based on MAIL-FROM address) who exceed the threshold you set for the number of message recipients per sender.</p> <p>For more information, see the <a href="#">Rate Limits Page</a>, on page 37.</p>
Connections by Country Page	<p>The Connections by Country report page shows the:</p> <ul style="list-style-type: none"> <li>• Top incoming mail connections based on country of origin in graphical format.</li> <li>• Total incoming mail connections and messages based on country of origin in tabular format.</li> </ul> <p>For more information, see the <a href="#">Connections by Country Page</a>, on page 38.</p>
<b>User Reports</b>	
User Mail Summary Page	<p>The User Mail Summary report provides information about the mail sent and received by your internal users per email address. A single user can have multiple email addresses. The email addresses are not combined in the report.</p> <p>For more information, see the <a href="#">User Mail Summary</a>, on page 38.</p>
DLP Incident Summary Page	<p>The DLP Incident Summary report page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail.</p> <p>For more information, see the <a href="#">DLP Incident Summary Page</a>, on page 41.</p>
Web Interaction Page	<p>The Web Interaction report page identifies the end users who clicked URLs rewritten by policy or Outbreak Filter, and the action associated with each user click.</p> <p>For more information, see the <a href="#">Web Interaction Page</a>, on page 42.</p>
<b>Filter Reports</b>	
Message Filters Page	<p>The Message Filters report page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages.</p> <p>For more information, see the <a href="#">Message Filters Page</a>, on page 43.</p>



Email Reporting Menu	Action
High Volume Mail Page	The High Volume Mail report page identifies attacks involving a large number of messages from a single sender, or with identical subjects, within a moving one-hour period.  For more information, see the <a href="#">High Volume Mail Page, on page 44</a> .
Content Filters Page	The Content Filters report page shows information about the top incoming and outgoing content filter matches (which content filter had the most matching messages). This page also displays the data as both bar charts and listings.  For more information, see the <a href="#">Content Filters Page, on page 44</a> .
System Capacity Page	The System Capacity report page shows detailed information about the overall workload of the reporting data, sent to the Security Management appliance.  For more information, see the <a href="#">System Capacity Page, on page 45</a> .

## Mail Flow Summary Page

The Mail Flow Summary report page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Mail Flow Summary report page includes graphs and summary tables for the incoming and outgoing messages.

The Mail Flow Summary: Incoming report page shows the incoming mail graphs for the total number of messages that are processed and blocked by the appliance, as well as the summary of the incoming mails.

You can use the mail trend graphs on this page to monitor the flow of all the incoming mails that are processed and blocked by your appliances, based on the selected time range. For more information, see [Choosing a Time Range for Reports](#).

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#)

The following mail trend graphs provide a visual representation of the incoming mail flow:

- Threat Detection Summary
- Content Summary

You can view the mail trend of the incoming messages based on the required counters for the respective categories. For more information, see [Using Counters to Filter Data on the Trend Graphs](#).

The Mail Flow Summary: Outgoing report page shows the outgoing mail graphs for the total number of messages that are processed and delivered by the appliance, as well as the summary of the outgoing mail.

You can use the mail trend graphs on this page to monitor the flow of all the outgoing mails that are processed and delivered by your appliances, based on the selected time range. For more information, see [Choosing a Time Range for Reports](#).

The following mail trend graphs provide a visual representation of the mail flow of the Outgoing Mails.

You can view the mail trend of the outgoing messages based on the required counters of the processed messages. For more information, see [Using Counters to Filter Data on the Trend Graphs](#).

The following list explains the various sections on the Mail Flow Summary report page:

**Table 2: Details on the Mail Flow Summary Page**

Section	Description
<b>Mail Flow Summary: Incoming</b>	
Number of Messages	The Number of Messages graph provides a visual representation of the total number of messages processed, including the messages that are processed as threat messages.
Threat Messages	The Threat Messages graph provides a visual representation of the total number of messages that are blocked by the Email Security appliance.
Threat Detection Summary	<p>The Threat Detection Summary mail trend graph provides a visual representation based on the following categories:</p> <ul style="list-style-type: none"> <li>• <b>Connection and Reputation Filtering:</b> Messages that are categorized as threat by the Reputation Filtering and Invalid Recipients.</li> <li>• <b>Spam Detection:</b> Messages that are categorized as threat by the Anti-spam scanning engine.</li> <li>• <b>Email Spoofing:</b> Messages which are categorized as threat due to DMARC Verification failure.</li> <li>• <b>Outbreak Threat Summary:</b> Messages which are categorized as phishing, scam, virus or malware, by the Outbreak Filtering engine.</li> <li>• <b>Attachment and Malware Detection:</b> Messages that are categorized as threat by the Anti-virus and AMP engines.</li> <li>• <b>All Categories:</b> All the messages that are categorized as threat.</li> </ul>
Content Summary	<p>The Content Summary mail trend graph provides a visual representation based on the following categories:</p> <ul style="list-style-type: none"> <li>• <b>Graymail:</b> Messages that are categorized as marketing, bulk or social networking.</li> <li>• <b>Content Filters:</b> Messages that are categorized by the content filters.</li> <li>• <b>All Categories:</b> All the messages that are categorized by graymail engines and content filters.</li> </ul>
<b>Mail Flow Summary: Outgoing</b>	

Section	Description
Number of Messages	The Number of Messages graph provides a visual representation of the total number of messages processed, including the messages that are processed as clean.
Message Delivery	The Message Delivery graph provides a visual representation of the total number of messages that are delivered, including hard bounces.
Outgoing Mails	The Outgoing Mails trend graph provides a visual representation based on the following categories: <ul style="list-style-type: none"> <li>• Spam Detected</li> <li>• Virus Detected</li> <li>• Detected by AMP</li> <li>• Stopped by Content Filters</li> <li>• Stopped by DLP</li> </ul>

## How Incoming Mail Messages are Counted

Counts of incoming messages are dependent on the number of recipients per message. For example, an incoming message from example.com sent to three recipients is counted as three messages coming from that sender.

Because the messages blocked by sender reputation filtering do not actually enter the work queue, the appliance does not have access to the list of recipients for an incoming message. In this case, a multiplier is used to estimate the number of recipients. This multiplier is based on research of a large sampling of existing customer data.

## How Email Messages Are Categorized by the Appliances

As messages proceed through the email pipeline, they can apply to multiple categories. For example, a message can be marked as spam or virus positive; it can also match a content filter. The precedence of the various filters and scanning activities greatly impacts the results of message processing.

In the example above, the various verdicts follow these rules of precedence:

- Spam positive
- Virus positive
- Matching a content filter

Following these rules, if a message is marked as spam positive, and your anti-spam settings are set to drop spam positive messages, the message is dropped and the spam counter is incremented.

Further, if your anti-spam settings are set to let the spam positive message continue on in the email pipeline, and a subsequent content filter drops, bounces, or quarantines the message, the spam count is still incremented. The content filter count is only incremented if the message is not spam or virus positive.

Alternately, if the message were quarantined by Outbreak Filters, it would not be counted until it was released from the quarantine and again processed through the work queue.

For complete information about message processing precedence, see chapter about the email pipeline in the online help or user guide for your Email Security appliance.

## Categorizing Email Messages on the Mail Flow Summary Page

Incoming messages that are considered as threat, and outgoing messages that are delivered in the Mail Flow Summary report page are categorized as follows:

**Table 3: Email Categories on Mail Flow Summary Page**

Category	Description
<b>Mail Flow Summary: Incoming</b>	
Reputation Filtering	<p>All connections blocked by HAT policies, multiplied by a fixed multiplier, (see the <a href="#">How Incoming Mail Messages are Counted</a>) and added with all recipients blocked by recipient throttling.</p> <p>The value for Stopped by Reputation Filtering is calculated based on the following factors:</p> <ul style="list-style-type: none"> <li>• Number of “throttled” messages from this sender.</li> <li>• Number of rejected or TCP refused connections (may be a partial count).</li> <li>• A conservative multiplier for the number of messages per connection.</li> </ul> <p>When the appliance is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval. In this situation, the value shown can be interpreted as an indicative value of the least number of messages are stopped.</p> <p>The Reputation Filtering total count and percentage on the Mail Flow Summary report page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.</p>
Invalid Recipients	The total count and percentage of all mail recipients rejected by conversational LDAP rejection in addition to all RAT rejections.
Anti-Spam	The total count and percentage of incoming messages detected by the anti-spam scanning engine as positive or suspect. Additionally, messages that are both spam and virus positive.

Category	Description
Anti-Virus	<p>The total count and percentage of incoming messages detected as virus positive and not also spam.</p> <p>The following messages are counted in the "Virus Detected" category:</p> <ul style="list-style-type: none"> <li>• Messages with a virus scan result of "Repaired" or "Infectious"</li> <li>• Messages with a virus scan result of "Encrypted" when the option to count encrypted messages as containing viruses is selected</li> <li>• Messages with a virus scan result of "Unscannable" when the action for unscannable messages is NOT "Deliver"</li> <li>• Messages with a virus scan result of "Unscannable" or "Encrypted" when the option to deliver to an alternate mail host or an alternate recipient is selected</li> <li>• Messages that are deleted from the Outbreak quarantine, either manually or by timing out.</li> </ul>
Advanced Malware Protection	<p>The total count and percentage of incoming messages blocked by the file analysis service.</p> <p>A message attachment was found to be malicious by file reputation filtering. This value does not include verdict updates or files found to be malicious by file analysis.</p>
Content Filter	The total count and percentage of incoming messages that are stopped by message and content filters.
DMARC Policy	The total count and percentage of incoming messages that failed DMARC verification policy.
S/MIME Verification/Decryption Failed	The total count and percentage of incoming messages that failed S/MIME verification, decryption, or both.
<b>Mail Flow Summary: Outgoing</b>	
Hard Bounces	The total count and percentage of outgoing messages that are permanently undeliverable.
Delivered	The total count and percentage of outgoing messages that are delivered.

**Note**

If you have configured your anti-virus settings to deliver unscannable or encrypted messages, these messages will be counted as clean messages and not virus positive. Otherwise, the messages are counted as virus positive.

Additionally, if messages match a message filter and are not dropped or bounced by the filter, they are treated as clean. Messages dropped or bounced by a message filter are not counted in the totals.

**Related Topics**

[Mail Flow Details Page](#), on page 25

## DMARC Verification Page

The DMARC Verification report page shows the top sender domains that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification, and a summary of the actions taken for incoming messages from each domain. You can use this report to fine-tune your DMARC settings and answer these kinds of questions:

- Which domains sent the most messages that failed DMARC verification?
- For each domain, what actions are taken on messages that failed DMARC verification?

To view the DMARC Verification report page, select DMARC Verification from the Email and Threat Reports section of the Reporting drop-down.

You can use the DMARC Verification report page to view:

- Top Domains by DMARC verification failures in graphical format.
- Total domains by DMARC verification details in tabular format. For more information, see [Domains by DMARC Verification Details Table](#), on page 14.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

From the DMARC Verification report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

For more information about DMARC verification, see the Email Authentication chapter in the online help or user guide for your Email Security appliance.

### Domains by DMARC Verification Details Table

The Domains by DMARC Verification Details table is an interactive table that shows the details of the sender domains that have failed (by either being rejected, quarantined, or no action), attempted, and passed the Domain-based Message Authentication, Reporting and Conformance (DMARC) verification.

To customize and sort information on the table, see [Customizing Tables on Report Pages](#).

To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

## Outbreak Filtering Page

The Outbreak Filtering report page shows information about recent outbreaks and messages quarantined due to Outbreak Filters. You can use this page to monitor your defense against targeted virus, scam, and phishing attacks.

To view the Outbreak Filtering report page, select Outbreak Filtering from the Email Threat Reports section of the Reports drop-down.

Use the Outbreak Filtering report page to answer the following types of questions:

- How many messages are quarantined and by which Outbreak Filters rule?
- How long do messages stay in the Outbreak Quarantine?
- Which potentially malicious URLs are most frequently seen?

The following table explains the various sections on the Outbreak Filtering report page:

**Table 4: Details on the Outbreak Filtering Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Threats By Type	The Threats by Type section shows the different types of threat messages received by the appliance.
Threat Summary	The Threat Summary section shows a breakdown of the messages by Malware, Phish, Scam and Virus. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.
Threat Details	The Threat Details interactive table shows details about specific outbreaks, including the threat category (virus, scam, or phishing), threat name, a description of the threat, and the number of messages identified. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.
Hit Messages from Incoming Messages	The Hit Messages from Incoming Messages section shows the chart and summary of the number of incoming messages processed by Outbreak Filters in the selected time period. Non-viral threats include phishing emails, scams, and malware distribution using links to an external website.

Section	Description
Hit Messages by Threat Level	<p>The Hit Messages by Threat Level section shows the chart and summary of the severity of threats caught by Outbreak Filters.</p> <p>Level 5 threats are severe in scope or impact, while Level 1 represents low threat risk. For descriptions of threat levels, see the online help or user guide for your Email Security appliance.</p>
Messages resided in Outbreak Quarantine	<p>The Messages resided in Outbreak Quarantine shows the length of time messages spent in the Outbreak Quarantine.</p> <p>This duration is determined by the time it takes the system to compile enough data about the potential threat to make a verdict on its safety. Messages with viral threats typically spend more time in the quarantine than those with non-viral threats, because they must wait for anti-virus program updates. The maximum retention time that you specify for each mail policy is also reflected.</p>
Top URL's Rewritten	<p>The Top URL's Rewritten section shows the URLs that are most frequently rewritten to redirect message recipients to the Cisco Web Security Proxy for click-time evaluation of the site if and when the recipient clicks a potentially malicious link in a message.</p> <p>This list may include URLs that are not malicious, because if any URL in a message is deemed malicious, then all URLs in the message are rewritten.</p> <p>To view Message Tracking details for the messages that populate this report, click a blue number link in the table.</p>

**Note**

In order to correctly populate the tables on the Outbreak Filtering report page, the appliance must be able to communicate with the Cisco update servers.

For more information, see the Outbreak Filters chapter in the online help or user guide for your Email Security appliance.

## URL Filtering Page

To view the URL Filtering report page, select **URL Filtering** from the Email Threat Reports section of the Reports drop-down.

- URL Filtering report modules are populated only if URL filtering is enabled.
- URL Filtering reports are available for incoming and outgoing messages.
- Only messages that are scanned by the URL filtering engine (either as part of anti-spam/outbreak filter scanning or through message/content filters) are included in these modules. However, not all of the results are necessarily specifically attributable to the URL Filtering feature.



- The Top URL Categories module includes all categories found in messages that have been scanned, whether or not they match a content or message filter.
- Each message can be associated with only one reputation level. For messages with multiple URLs, the statistics reflect the lowest reputation of any URL in the message.
- URLs in the global whitelist configured at Security Services > URL Filtering page of the email security appliance, are not included in reports.  
URLs in whitelists used in individual filters are included in reports.
- Malicious URLs are URLs that Outbreak Filters have determined to have poor reputation. Neutral URLs are those that Outbreak Filters have determined to require click-time protection. Neutral URLs have therefore been rewritten to redirect them to the Cisco Web Security proxy.
- Results of URL category-based filters are reflected in content and message filter reports.
- Results of click-time URL evaluations by the Cisco Web Security proxy are not reflected in reports.

The following table explains the various sections on the URL Filtering report page:

**Table 5: Details on the URL Filtering Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Top URL Categories	This section displays the graphical view and summary of the top URL categories of the incoming and outgoing messages. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.
Top URL Spam Messages	This section displays the graphical view and summary of the top incoming and outgoing URL spam messages.
Malicious and Neutral URLs	This section displays the chart view and the summary of malicious and neutral URLs of the incoming and outgoing messages. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

From the URL Filtering report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

## Forged Email Detection Page

To view the Forged Email Detection report page, select **Forged Email Detection** from the Email Threat Reports section of the Reports drop-down.

- The Forged Email Detection page includes the following reports:
  - **Top Forged Email Detection.** Displays the top ten users in the content dictionary that matched the forged From: header in the incoming messages.
  - **Forged Email Detection: Details.** Displays a list of all the users in the content dictionary that matched the forged From: header in the incoming messages and for a given user, the number of messages matched.
- The Forged Email Detection reports are populated only if you are using the Forged Email Detection content filter or the `forged-email-detection` message filter.

From the Forged Email Detection report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

## Advanced Malware Protection Page

Advanced Malware Protection protects against zero-day and targeted file-based threats in email attachments by:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.
- Evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

This feature is available for incoming and outgoing messages.

For more information on the file reputation filtering and file analysis, see the *User Guide or Online Help for AsyncOS for Email Security Appliances*.

To view the Advanced Malware Protection report page, select **Advanced Malware Protection** from the Filter and Malware Reports section of the Reports drop-down.

The Advanced Malware Protection report page shows the following reporting views:

- [Advanced Malware Protection – Summary, on page 19](#)
- [Advanced Malware Protection – AMP Reputation, on page 19](#)
- [Advanced Malware Protection – File Analysis, on page 20](#)
- [Advanced Malware Protection – File Retrospection, on page 20](#)
- [Advanced Malware Protection – Mailbox Auto Remediation, on page 21](#)

See Also:

- [Identifying Files by SHA-256 Hash](#)

- [Requirements for File Analysis Report Details](#)
- [Viewing File Reputation Filtering Data in Other Reports](#)

## Advanced Malware Protection – Summary

The Advanced Malware Protection – Summary page shows the complete summary of the incoming and outgoing file-based threats that are identified by the file reputation and file analysis service.

For more information, see [Advanced Malware Protection – AMP Reputation](#), on page 19 and [Advanced Malware Protection – File Analysis](#), on page 20.

## Advanced Malware Protection – AMP Reputation

The Advanced Malware Protection - AMP Reputation page shows incoming and outgoing file-based threats that were identified by the file reputation service.

For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.

If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.

You can use the AMP Reputation view of the Advanced Malware Protection: Incoming report page to view:

- The summary of incoming files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- A trend graph for all the incoming malware threat files based on the selected time range.
- The top incoming malware threat files.
- The top incoming threat files based on the file types.
- The Incoming Malware Threat Files interactive table that lists the top incoming malware threat files.

Drill down to view detailed analysis results, including the threat characteristics for each file.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

You can use the AMP Reputation view of the Advanced Malware Protection: Outgoing report page to view:

- The summary of outgoing files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- A trend graph for all the outgoing malware threat files based on the selected time range.
- The top outgoing malware threat files.
- The top outgoing threat files based on the file types.
- The Outgoing Malware Threat Files interactive table that lists the top outgoing malware threat files that are identified by the file reputation service.

Drill down to view detailed analysis results, including the threat characteristics for each file.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

## Advanced Malware Protection – File Analysis

The Advanced Malware Protection - File Analysis page shows the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.

To view more than 1000 File Analysis results, export the data as a .csv file.

For deployments with an on-premises Cisco AMP Threat Grid Appliance: Files that are whitelisted on the AMP Threat Grid appliance show as "clean". For information about whitelisting, see the AMP Threat Grid documentation or online help.

Drill down to view detailed analysis results, including the threat characteristics for each file.

You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file. For more information, see [Identifying Files by SHA-256 Hash](#).

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click the **Details** link in the table.

To view details on the server that analyzed a file, see [Requirements for File Analysis Report Details](#).

If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.

You can use the File Analysis view of the Advanced Malware Protection report page to view:

- The number of incoming and outgoing files that are uploaded for file analysis by file analysis service of the Advanced Malware Protection engine.
- A list of incoming and outgoing files that have completed file analysis requests.
- A list of incoming and outgoing files that have pending file analysis requests.

## Advanced Malware Protection – File Retrospection

The Advanced Malware Protection - File Retrospection page lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about on this scenario, see the documentation for your Email Security appliance.

As Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data might unveil more information.

To view more than 1000 verdict updates, export the data as a .csv file.

In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.

To view all affected messages for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click a SHA-256 link.

You can use the File Retrospection view of the Advanced Malware Protection report page to view:

- A list of incoming and outgoing files with retrospective verdict changes.

## Advanced Malware Protection – Mailbox Auto Remediation

The Advanced Malware Protection - Mailbox Auto Remediation report page shows the details of the mailbox remediation results for the incoming files.

You can use the Advanced Malware Protection - Mailbox Auto Remediation page to view retrospective security details such as:

- The filenames associated with a SHA-256 hash.
- Remedial actions taken on messages.
- A list of recipients for whom the mailbox remediation was successful or unsuccessful.

The Recipients for whom remediation was unsuccessful field is updated in the following scenario:

- There was a connectivity issue between your appliance and Office 365 services when the appliance was trying to perform the configured remedial action.

Click on a SHA-256 hash to view the related messages in Message Tracking.

## Requirements for File Analysis Report Details

### (Cloud File Analysis) Ensure That the Management Appliance Can Reach the File Analysis Server


In order to obtain File Analysis report details, the appliance must be able to connect to the File Analysis server over port 443. See details in [Firewall Information](#)

If your Cisco Content Security Management appliance does not have a direct connection to the internet, configure a proxy server for this traffic (See [Upgrade and Update Settings](#).) If you have already configured the appliance to use a proxy to obtain upgrades and service updates, the existing settings are used.

If you use an HTTPS proxy, the proxy must not decrypt the traffic; use a pass-through mechanism for communications with the File Analysis server. The proxy server must trust the certificate from the File Analysis server, but need not provide its own certificate to the File Analysis server.

### (Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Results

In order to allow all content security appliances in your organization to display detailed results in the cloud about files sent for analysis from any Cisco Email Security appliance or Cisco Web Security appliance in your organization, you need to join all appliances to the same appliance group.

- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Select **Management Appliance > Centralized Services > Security Appliances**.
- Step 3** Scroll to the File Analysis section.
- Step 4** If your managed appliances are pointed at different File Analysis cloud servers, select the server from which to display result details.  
Result details will not be available for files processed by any other cloud server.
- Step 5** Enter the Analysis Group ID.

- If you enter the Group ID incorrectly or need to change it for any other reason, you must open a case with Cisco TAC.
- This change takes effect immediately; it does not require a Commit.
- It is suggested to use your CCOID for this value.
- This value is case-sensitive.
- This value must be identical on all appliances that will share data about files that are uploaded for analysis.
- An appliance can belong to only one group.
- You can add a machine to a group at any time, but you can add it only once.

**Step 6** Click **Group Now**.

**Step 7** Configure the same group on each Email Security appliance that will share data with this appliance.

---

### What to Do Next

#### Related Topics

[For Which Files Are Detailed File Analysis Results Visible in the Cloud?](#)

### (On-Premises File Analysis) Activate the File Analysis Account

If you have deployed an on-premises (private cloud) Cisco AMP Threat Grid Appliance, you must activate the File Analysis account for your Cisco Content Security Management appliance in order to view report details available on the Threat Grid appliance. You generally only need to do this once.

#### Before You Begin

Ensure that you are receiving System alerts at Critical level.

---

**Step 1** The first time you attempt to access File Analysis report details from the Threat Grid appliance, wait a few minutes and you will receive an alert that includes a link.

If you do not receive this alert, go to **Management Appliance > System Administration > Alerts** and click **View Top Alerts**.

**Step 2** Click the link in the alert message.

**Step 3** Activate your management appliance account.

---

### Additional Requirements

For any additional requirements, see the Release Notes for your Security Management appliance release, available from

<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>

## Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format).

## Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A Detected by Advanced Malware Protection column may be hidden by default in applicable reports. To display additional columns, click the Columns link at the bottom of the table.

## For Which Files Are Detailed File Analysis Results Visible in the Cloud?

If you have deployed public-cloud File Analysis, you can view detailed results for all files uploaded from any managed appliance that has been added to the appliance group for File Analysis.

If you have added your management appliance to the group, you can view the list of managed appliances in the group by clicking the button on the **Management Appliance > Centralized Services > Security Appliances** page.

Appliances in the analysis group are identified by the File Analysis Client ID. To determine this identifier for a particular appliance, look in the following location:

Appliance	Location of File Analysis Client ID
Email Security appliance	Advanced Settings for File Analysis section on the <b>Security Services &gt; File Reputation and Analysis</b> page.
Web Security appliance	Advanced Settings for File Analysis section on the <b>Security Services &gt; Anti-Malware and Reputation</b> page.
Cisco Content Security Management appliance	At the bottom of the <b>Management Appliance &gt; Centralized Services &gt; Security Appliances</b> page.

### Related Topics

- [\(Cloud File Analysis\) Configure the Management Appliance to Display Detailed File Analysis Results](#)

## Virus Filtering Page

The Virus Filtering report page provides an overview of the viruses that are sent to and from your network. The Virus Types page displays the viruses that have been detected by the virus scanning engines running on the Email Security appliances and are displayed on the Security Management

appliance. Use this report to take action against a particular virus. For example, if you see that you are receiving a high volume of viruses known to be embedded in PDF files, you can create a filter action to quarantine messages with PDF attachments.

To view the Virus Filtering report page, select **Virus Filtering** from the File and Malware Reports section of the Reports drop-down.

If you run multiple virus scanning engines, the Virus Filtering report page includes results from all enabled virus scanning engines. The name of the virus that appears on the page is determined by the virus scanning engines. If more than one scanning engine detects a virus, it is possible to have more than one entry for the same virus.

The following list explains the various sections on the Virus Filtering report page:

**Table 6: Details on the Virus Filtering Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Top Incoming Virus Types Detected	This section displays a chart view of the detected viruses in messages sent to your network.
Top Outgoing Virus Types Detected	This section displays a chart view of the detected viruses in messages sent from your network.
Virus Types Detail	An interactive table that shows the details of each virus type. For more information, see <a href="#">Virus Types Detail Table</a> , on page 24



#### Note

To see which hosts sent virus-infected messages to your network, go to the Incoming Mail page, specify the same reporting period, and sort by virus positive messages. Similarly, to see which IP addresses have sent virus positive emails within your network, go to the Outgoing Senders page and sort by virus positive messages.

From the Virus Filtering report page, you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

You can generate a scheduled report for the Virus Filtering report page. See the [Scheduling Email Reports](#).

## Virus Types Detail Table

The Virus Types Detail table is an interactive table that shows the total number of virus-infected messages, with a breakdown by incoming and outgoing messages. Click the column headings to sort the data.

The following table shows the table column descriptions for the Virus Types Detail table:



**Table 7: Table Column Descriptions for Virus Types Detail Table**

Column Name	Description
Virus Type	The name of the virus type.
Incoming Messages	Number of incoming messages detected as virus.
Outgoing Messages	Number of outgoing messages detected as virus.
Total Infected Messages	Total number of infected messages (incoming and outgoing).

## Macro Detection Page

You can use the Macro Detection report page to view:

- Top Incoming Macro-Enabled Attachments by File Type in graphical and tabular format.
- Total Incoming Macro-Enabled Attachments by File Type in tabular format.
- Top Outgoing Macro-Enabled Attachments by File Type in graphical and tabular format.
- Total Outgoing Macro-Enabled Attachments by File Type in tabular format.

To view the Macro Detection report page, select **Macro Detection** from the File and Malware Reports section of the Reports drop-down.

From the Macro Detection report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

You can click on the number of macro-enabled attachments to view the related messages in Message Tracking.

**Note**

During report generation:

- If one or more macros are detected within an archive file, the Archive Files file type is incremented by one. The number of macro-enabled attachments within an archive file are not counted.
- If one or more macros are detected within an embedded file, the parent file type is incremented by one. The number of macro-enabled attachments within an embedded file are not counted.

## Mail Flow Details Page

The Mail Flow Details report page on the Security Management appliance provides interactive reporting on the real-time information for all remote hosts connecting to your managed Security Management appliances. You can gather information about the IP addresses, domains, and network owners (organizations) sending mail to your system. You can also gather information about the IP addresses and domains of the outgoing senders.

To view the Mail Flow Details report page, select **Mail Flow Details** from the Connection and Flow Reports section of the Reports drop-down.

The Mail Flow Details report page has the following tabs:

- Incoming Mail
- Outgoing Senders

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#).

From the Incoming Mail tab, you can:

- View the top senders by total threat messages in graphical format.
- View the top senders by clean messages in graphical format.
- View the top senders by graymail messages in graphical format.
- See the IP addresses, domains, or network owners (organizations) that have sent mail to your Security Management appliances.
- See detailed statistics on senders that have sent mail to your appliances. The statistics include the number of connections (accepted or rejected), attempted messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth), total threat messages, total graymails and clean messages.
- See the Incoming Mail interactive table for the detailed information about the particular IP address, domain, or network owner (organization). For more information, see [Incoming Mail Table, on page 28](#).

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a number hyperlink in the table.

From the Outgoing Senders tab, you can:

- View the top senders by total threat messages in graphical format.
- View the top senders by clean messages in graphical format.
- View the top senders (by IP address or domain) of outgoing threat messages (spam, antivirus, etc.) in your organization.
- See detailed statistics on senders that have sent mail from your appliances. The statistics include the total threat messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth) and clean messages.
- See the Sender Details interactive table for detailed information about the particular IP address or domain. For more information, see [Sender Details Table, on page 30](#).

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a number hyperlink in the table.

### Related Topics

- [“No Domain Information” Link](#)
- [Time Ranges in the Mail Trend Graphs](#)
- [Views Within the Mail Flow Details Page, on page 27](#)
- [Incoming Mail Table, on page 28](#)

- [Sender Details Table, on page 30](#)

## Views Within the Mail Flow Details Page

The Mail Flow Details: Incoming report page has three different views:

- IP Addresses
- Domains
- Network Owners

These views provide a snapshot of the remote hosts connecting to the system in the context of the selected view.

Depending on the view you select, the Incoming Mail Details interactive table displays the top IP addresses, domains, or network owners that have sent mail to all public listeners configured on the Email Security appliances. You can monitor the flow of all mail into your appliances.

See the [Incoming Mail Table, on page 28](#) for an explanation of the data included in the Incoming Mail interactive table.

From the Mail Flow Details page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).



### Note

You can generate a scheduled report for the Mail Flow Details report page. See the [Scheduling Email Reports](#).

The Mail Flow Details: Outgoing report page has two different views:

- IP Addresses
- Domains

These views provide a snapshot of the remote hosts connecting to the system in the context of the selected view.

Depending on the view you select, the Sender Details interactive table displays the top IP addresses or domains of the senders that have sent mail from the public listeners configured from the Email Security appliances. You can monitor the flow of all mail from your appliances.

See the [Sender Details Table, on page 30](#) for an explanation of the data included in the Sender Details interactive table.

### “No Domain Information” Link

Domains that have connected to the Security Management appliances and could not be verified with a double-DNS lookup are automatically grouped into the special domain called “No Domain Information.” You can control how these types of unverified hosts are managed via Sender Verification. For more information about Sender Verification, see the documentation or online help for your Email Security appliance.

You can use the Items Displayed menu to select the number of senders to display in the list.

## Time Ranges in the Mail Trend Graphs

You can select varying degrees of granularity to see your data in a mail graph. You can select a day, week, month, and year views of the same data. Because the data is monitored in real time, information is periodically updated and summarized in the database.

For more information on time ranges, see [Choosing a Time Range for Reports](#).

## Incoming Mail Table

The interactive Incoming Mail Details table at the bottom of the Mail Flow Details: Incoming page lists the top senders that have connected to public listeners on the Email Security appliances. The table shows domains, IP addresses, or network owners, based on the view selected.

The system acquires and verifies the validity of the remote host's IP address by performing a double DNS lookup. For more information about *double DNS lookups* and sender verification, see the user guide or online help for AsyncOS Email Security appliance.

To view Message Tracking details for the messages that populate this report, click a number hyperlink in the table.

The following table shows the table column descriptions for the Incoming Mail table:

**Table 8: Table Column Descriptions for Incoming Mail Table**

Column Name	Description
Sender Domain (Domains)	The domain name of the sender.
Sender IP Address (IP Addresses)	The IP address of the sender.
Hostname (IP Addresses)	The hostname of the sender.
DNS Verified (IP Addresses)	The IP addresses that are verified by the DNS.
SBRS (IP Addresses)	The SenderBase Reputation Score of the sender.
Last Sender Group (IP Addresses)	The details of the last sender group.
Last Sender Group (IP Addresses)	The details of the last sender group.
Network Owner (Network Owners)	The network owner of the sender.
Connections Rejected (Domains and Network Owners)	All connections blocked by HAT policies. When the appliance is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval.

Column Name	Description
Connections Accepted (Domains and Network Owners)	All connections accepted,
Total Attempted	All accepted and blocked connections attempted.
Stopped by Recipient Throttling (Domains and Network Owners)	This is a component of Stopped by Reputation Filtering. It represents the number of recipient messages stopped because any of the following HAT limits have been exceeded: maximum recipients per hour, maximum recipients per message, or maximum messages per connection. This is summed with an estimate of the recipient messages associated with rejected or TCP refused connections to yield Stopped by Reputation Filtering.
Stopped by Reputation Filtering	<p>The value for Stopped by Reputation Filtering is calculated based on several factors:</p> <ul style="list-style-type: none"> <li>• Number of “throttled” messages from this sender</li> <li>• Number of rejected or TCP refused connections (may be a partial count)</li> <li>• A conservative multiplier for the number of messages per connection.</li> </ul> <p>When the appliance is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval. In this situation, the value shown can be interpreted as a “floor”; that is, at least this many messages are stopped.</p> <p><b>Note</b> The Reputation Filtering total on the Mail Flow Summary page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.</p>
Stopped as Invalid Recipients	All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.
Spam Detected	Any spam that has been detected.
Virus Detected	Any viruses that have been detected
Detected by Advanced Malware Protection	The total count of messages detected by Advanced Malware Protection engines.
Stopped by Content Filter	The total count of messages that are stopped by a content filter.
Stopped by DMARC	The total count of messages that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification.
Total Threat	Total number of threat messages (stopped by reputation, stopped as invalid recipient, spam, plus virus)
Marketing	Number of messages detected as unwanted marketing messages.

Column Name	Description
Social	Number of messages detected as social messages.
Bulk	Number of messages detected as bulk.
Total Graymails	Number of messages detected as graymails.
Clean	All clean messages. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.

## Sender Details Table

The interactive Sender Details table at the bottom of the Mail Flow Details: Outgoing page lists the top senders that have connected to public listeners on the Email Security appliances. The table shows domains or IP addresses, based on the view selected.

To view Message Tracking details for the messages that populate this report, click a number hyperlink in the table.

The following table shows the table column descriptions for the Sender Details table:

**Table 9: Table Column Descriptions for Sender Details Table**

Column Name	Description
Sender Domain (Domains)	The domain name of the sender.
Sender IP Address (IP Addresses)	The IP address of the sender.
Hostname (IP Addresses)	The hostname of the sender.
Spam Detected	Any spam that has been detected.
Virus Detected	Any viruses that have been detected.
Detected by Advanced Malware Protection	The total count of messages detected by Advanced Malware Protection engines.
Stopped by Content Filter	The total count of messages that are stopped by a content filter.
Stopped by DLP	The total count of messages that are stopped by DLP engine.
Total Threat	Total number of threat messages (spam, virus)
Clean	All clean messages. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.

Column Name	Description
Total Messages	The total count of all the messages.

## Sender Groups Page

The Sender Groups report page provides a summary of connections by sender group and mail flow policy action, allowing you to review SMTP connection and mail flow policy trends. The Mail Flow by Sender Group listing shows the percentage and number of connections for each sender group. The Connections by Mail Flow Policy Action chart shows the percentage of connections for each mail flow policy action. This page provides an overview of the effectiveness of your Host Access Table (HAT) policies. For more information about the HAT, see the documentation or online help for your Email Security appliance.

To view the Sender Groups report page, select **Sender Groups** from the Connection and Flow Reports section of the Reports drop-down.

From the Sender Group report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).



### Note

You can generate a scheduled report for the Sender Group report page. See the [Scheduling Email Reports](#).

## Outgoing Destinations Page

The Outgoing Destinations report page provides information about the domains that your organization sends mail to.

To view the Outgoing Destinations report page, select **Outgoing Destinations** from the Connection and Flow Reports section of the Reports drop-down.

Use the Outgoing Destinations page to answer the following types of questions:

- Which domains are the Email Security appliances sending mail to?
- How much mail is sent to each domain?
- How much of that mail is clean, spam-positive, virus-positive, malware or stopped by a content filter?
- How many messages are delivered and how many messages are hard-bounced by the destination servers?

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#).

The following list explains the various sections on the Outgoing Destinations report page:

**Table 10: Details on the Outgoing Destinations Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .

Section	Description
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances.  See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Top Destinations by Total Threat Messages	The top destination domains of outgoing threat messages (spam, antivirus, etc.) sent by your organization. Total threat messages include spam or virus positive, or the messages that are triggered by a content filter.
Top Destinations by Clean Messages	The top destination domains of clean outgoing messages sent by your organization.
Outgoing Destinations Details	All details related to the destination domains of all outgoing messages sent by your organization, sorted by total recipients. Details include detected spam, viruses, clean messages etc.  For more information, see <a href="#">Outgoing Destinations Detail Table, on page 32</a> .  To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

From the Outgoing Destinations report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

You can generate a scheduled report for the Outgoing Destinations page. See the [Scheduling Email Reports](#).

### Related Topics

[Outgoing Destinations Detail Table, on page 32](#)

## Outgoing Destinations Detail Table

The Outgoing Destinations Detail table is an interactive table that shows the total number of messages that are processed and delivered, with a breakdown of the messages that are processed as threat (Spam, Virus, etc.) or clean, and the messages that are either hard bounced or delivered. Click the column headings to sort the data.

To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

The following table shows the table column descriptions for the Outgoing Destination Detail table:

**Table 11: Table Column Descriptions for Outgoing Destination Detail Table**

Column Name	Description
Destination Domain	The name of the destination domain.
Spam Detected	Number of messages detected as spam.



Column Name	Description
Virus Detected	Number of messages detected as spam.
Stopped by Content Filter	Number of messages stopped by content filters.
Total Threat	Total number of messages detected as threat (Spam, Virus, etc.)
Clean	Number of messages detected as clean,
Total Processed	Total number of messages processed as threat or clean.
Hard Bounces	Number of messages that are marked as permanently undeliverable.
Delivered	Number of messages that are delivered.
Total Messages Delivered	Total number of messages that are delivered (including Hard Bounces).

## TLS Encryption Page

The TLS Encryptions page shows the overall usage of TLS connections for sent and received mail. The report also shows details for each domain sending mail using TLS connections.

To view the TLS Encryption report page, select **TLS Encryption** from the Connection and Flow Reports section of the Reports drop-down.

The TLS Connections page can be used to determine the following information:

- Overall, what portion of incoming and outgoing connections uses TLS?
- Which partners do I have successful TLS connections with?
- Which partners do I have unsuccessful TLS connections with?
- Which partners have issue with their TLS certificates?
- What percentage of overall mail with a partner uses TLS?

The TLS Encryption report page has the following tabs:

- Incoming
- Outgoing

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#).

The following list explains the various sections on the TLS Encryption report page:

**Table 12: Details on the TLS Encryption Page**

Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances.  See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
TLS Connections Graph	The TLS Encryption: Incoming page displays a graph view of incoming encrypted and unencrypted TLS connections over the last hour, day, week, month or year depending on the time frame that you have selected.  The TLS Encryption: Outgoing page displays a graph view of outgoing encrypted and unencrypted TLS connections over the last hour, day, week, month, or year, depending on the time frame that you have selected.
TLS Connections Summary	The TLS Encryption: Incoming page displays a table view of the total volume of incoming messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed incoming TLS encrypted messages.  The TLS Encryption: Outgoing page displays a table view of the total volume of outgoing messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed outgoing TLS encrypted messages.
TLS Messages	The TLS Encryption: Incoming page displays a chart view of the total count and percentage of incoming TLS encrypted and unencrypted messages.  The TLS Encryption: Outgoing page displays a chart view of the total count and percentage of outgoing TLS encrypted and unencrypted messages.
TLS Messages Summary	This table displays a summary of the total count and percentage of incoming and outgoing TLS encrypted and unencrypted messages.

TLS Connections Details	<p>This table displays details for domains sending or receiving encrypted messages. For each domain, you can view the total number of connections, messages sent, and the number of TLS connections that are successful or failed. You can also view the percentage of successful and failed connections for each domain.</p> <p>For more information, see <a href="#">TLS Connections Details Table</a>, on page 35.</p>
-------------------------	---

## TLS Connections Details Table

The TLS Connections Details table is an interactive table that shows the total number of connections, messages sent, and the number of TLS connections that are successful or failed, and the last TLS status for the incoming and outgoing messages. You can also view the percentage of successful and failed connections for each domain.

The following table shows the table column descriptions for the TLS Connection Details table:

**Table 13: Table Column Descriptions for TLS Connections Details Table**

Column Name	Description
Domain	The domain name of the sender.
TLS Req. Failed	All required TLS connections that failed.
TLS Req. Success	All required TLS connections that are successful.
TLS Pref. Failed	All preferred TLS connections that failed.
TLS Pref. Success	All preferred TLS connections that are successful.
Last TLS Status	<p>The status of the TLS connections mapped based on the following:</p> <ul style="list-style-type: none"> <li>• 0: N/A</li> <li>• 1: Required - Fail</li> <li>• 2: Preferred - Fail</li> <li>• 3: Required - Success</li> <li>• 4: Preferred - Success</li> </ul>
Total TLS Connections	Total number of TLS connections.
Unencrypted Connections	Total number of unencrypted TLS connections.
% TLS of all Connections	The percentage of TLS encryptions for all TLS connections.

Column Name	Description
Messages by TLS	The total number of TLS messages.

## Inbound SMTP Authentication Page

The Inbound SMTP Authentication report page shows the use of client certificates and the SMTP AUTH command to authenticate SMTP sessions between the Email Security appliance and users' mail clients. If the appliance accepts the certificate or SMTP AUTH command, it will establish a TLS connection to the mail client, which the client will use to send a message. Since it is not possible for the appliance to track these attempts on a per-user basis, the report shows details on SMTP authentication based on the domain name and domain IP address.

To view the Inbound SMTP Authentication report page, select **Inbound SMTP Authentication** from the Connection and Flow Reports section of the Reports drop-down.

Use this report to determine the following information:

- Overall, how many incoming connection use SMTP authentication?
- How many connections use a client certificated?
- How many connections use SMTP AUTH?
- What domains are failing to connect when attempting to use SMTP authentication?
- How many connections are successfully using the fall-back when SMTP authentication fails?

The Inbound SMTP Authentication has two different views:

- Domains
- IP Addresses

These views provide a snapshot of the SMTP authentications in the context of the selected view.

The Inbound SMTP Authentication report page includes a graph for received connections, a graph for received recipients who attempted an SMTP authentication connection, and a table with details on the attempts to authenticate connections.

The following list explains the various sections on the Inbound SMTP Authentication report page:

**Table 14: Details on the Inbound SMTP Authentication Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances.  See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .

Section	Description
Received Connection Graph	The Received Connections graph shows the incoming connections from mail clients that attempt to authentication their connections using SMTP authentication over the time range you specify. The graph displays the total number of connections the appliance received, the number that did not attempt to authenticate using SMTP authentication, the number that failed and succeeded to authenticate the connection using a client certificate, and the number that failed and succeeded to authenticate using the SMTP AUTH command.
Received Recipient Graph	The Received Recipients graph displays the number of recipients whose mail clients attempted to authenticate their connections to the Email Security appliances to send messages using SMTP authentication. The graph also show the number of recipients whose connections were authenticated and the number of recipients whose connections were not authenticated.
SMTP Authentication Details (By Domain Name or IP Address).	The SMTP Authentication Details (by domain name and IP address) table displays details about the users who attempt to authenticate their connections to the Email Security appliance to send messages. For each domain, you can view the number of connection attempts using a client certificate that were successful or failed, the number of connection attempts using the SMTP AUTH command that were successful or failed, and the number that fell back to the SMTP AUTH after their client certificate connection attempt failed.

## Rate Limits Page

Rate Limiting by envelope sender allows you to limit the number of email message recipients per time interval from an individual sender, based on the mail-from address. The Rate Limits report shows you the senders who most egregiously exceed this limit.

To view the Rate Limits report page, select **Rate Limits** from the Connection and Flow Reports section of the Reports drop-down.

Use this report to help you identify the following:

- Compromised user accounts that might be used to send spam in bulk.
- Out-of-control applications in your organization that use email for notifications, alerts, automated statements, etc.
- Sources of heavy email activity in your organization, for internal billing or resource-management purposes.
- Sources of large-volume inbound email traffic that might not otherwise be considered spam.

Note that other reports that include statistics for internal senders (such as Internal Users or Outgoing Senders) measure only the number of messages sent; they do not identify senders of a few messages to a large number of recipients.

The Top Offenders by Incident chart shows the envelope senders who most frequently attempted to send messages to more recipients than the configured limit. Each attempt is one incident. This chart aggregates incident counts from all listeners.

The Top Offenders by Rejected Recipients chart shows the envelope senders who sent messages to the largest number of recipients above the configured limit. This chart aggregates recipient counts from all listeners.

Rate Limiting settings, including "Rate Limit for Envelope Senders" settings, are configured on the Email Security appliance in Mail Policies > Mail Flow Policies. For more information on rate limiting, see the documentation or online help for your Email Security appliance.

#### Related Topics

[High Volume Mail Page](#), on page 44

## Connections by Country Page

You can use the Connections by Country report page to view:

- Top incoming mail connections based on country of origin in graphical format.
- Total incoming mail connections and messages based on country of origin in tabular format.

To view the Connections by Country report page, select Connections by Country from the Connection and Flow Reports section of the Reports drop-down.

The following are the scenarios when no country information is displayed for the top and total incoming mail connections:

- The sender IP address belongs to a private IP address.
- The sender IP address does not get a valid SBRS.

If your access privileges allow you to view Message Tracking data for the messages that populate this report, click a blue number link in the table.

From the Connections by Country report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

## User Mail Summary

The User Mail Summary report page provides information about the mail sent and received by your internal users per email address. A single user can have multiple email addresses. The email addresses are not combined in the report.

To view the User Mail Summary report page, select **User Mail Summary** from the User Reports section of the Reports drop-down.

Use the User Mail Summary interactive report page to answer these types of questions:

- Who is sending the most external email?
- Who receives the most clean email?
- Who receives the largest number of graymail messages?
- Who receives the most spam?
- Who is triggering which content filters?

- Whose email is getting caught by content filters?

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#).

The following list explains the various sections on the User Mail Summary report page:

**Table 15: Details on the User Mail Summary Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Top Users by Clean Incoming Messages	The top users (by domain), of clean incoming messages received by your organization.
Top Users by Clean Outgoing Messages	The top users (by domain), of clean outgoing messages sent by your organization.
Top Users by Graymail	The top users (by domain), of graymail messages.
User Mail Flow Details	The User Mail Flow Details interactive table breaks down the mails received and sent by each email address. You can sort the listing by clicking the column headers. For more information, see the <a href="#">User Mail Flow Details Table</a> , on page 39. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

From the User Mail Summary report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).



**Note**

You can generate a scheduled report for the User Mail Summary page. See the [Scheduling Email Reports](#).

## User Mail Flow Details Table

The User Mail Flow Detail table shows detailed information about a user, including a breakdown of incoming and outgoing messages, and the number of messages in each category (such as spam detected, virus detected, stopped by content filter, etc.). Incoming and outgoing content filter matches are also shown.

Inbound Internal Users are the users for which you received email, based on the Rcpt To: address. Outbound Internal Users are based on the Mail From: address, and are useful when tracking the types of email that senders on your internal network are sending.

Some outbound mail (such as bounces) has a null sender. They are counted as outbound “unknown.”

To view Message Tracking details for the messages that populate this report, click a number hyperlink in the table.

The following table shows the table column descriptions for the User Mail Flow Details table:

**Table 16: Table Column Descriptions for User Mail Flow Details Table**

Column Name	Description
Internal User	The domain name of the internal user.
Incoming Spam Detected	All incoming spam that was detected.
Incoming Virus Detected	The incoming virus that were detected.
Incoming Detected by Advanced Malware Protection	The incoming messages that are detected by Advanced Malware Protection (File Analysis and File Reputation).
Incoming Content Filter Matches	The incoming content filter matches that were detected.
Incoming Stopped by Content Filter	The incoming messages that were stopped due to content filters that have been set.
Incoming Marketing	The incoming messages that were detected as marketing.
Incoming Social Networking	The incoming messages that were detected as social networking.
Incoming Bulk	The incoming messages that were detected as bulk.
Incoming Graymails	The incoming messages that were detected as graymail.
Incoming Clean	All incoming clean messages.
Outgoing Spam Detected	The outgoing spam that was detected.
Outgoing Virus Detected	The outgoing viruses that were detected.
Outgoing Content Filter Matches	The outgoing content filter matches that were detected.
Outgoing Stopped by Content Filter	The outgoing messages that were stopped due to content filters that have been set.
Outgoing Clean	All outgoing clean messages.



## Searching for a Specific Internal User

With the search form at the bottom of the User Mail Summary page and the User Mail Flow Details page, you can search for a specific internal user (email address). Select whether to exactly match the search text or look for items starting with the entered text (for example, starts with “ex” will match “example@example.com”).

## DLP Incident Summary Page

The DLP Incidents (DLP Incident Summary) report page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The Email Security appliance uses the DLP email policies enabled in the Outgoing Mail Policies table to detect sensitive data sent by your users. Every occurrence of an outgoing message violating a DLP policy is reported as an incident.

To view the DLP Incident Summary report page, select **DLP Incidents** from the User Reports section of the Reports drop-down.

Using the DLP Incident Summary report, you can answer these kinds of questions:

- What type of sensitive data is being sent by your users?
- How severe are these DLP incidents?
- How many of these messages are being delivered?
- How many of these messages are being dropped?
- Who is sending these messages?

The DLP Incident Summary page contains two main sections:

- The DLP incident trend graphs summarizing the top DLP incidents by severity (Low, Medium, High, Critical) and policy matches.
- The DLP Incident Details listing.

From the DLP Incidents report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

To search for specific information within your data, see [Searching and the Interactive Email Report Pages](#).

The following list explains the various sections on the DLP Incident Summary report page:

**Table 17: Details on the DLP Incident Summary Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances. See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Top Incidents by Severity	The top DLP incidents listed by severity.

Section	Description
Incident Summary	The DLP policies currently enabled for each email appliance's outgoing mail policies are listed in the DLP Incident Details interactive table at the bottom of the DLP Incident Summary page. Click the name of a DLP policy to view more detailed information.
Top DLP Policy Matches	The top DLP Policies that have been matched.
DLP Incident Details	<p>The DLP Incidents Details table shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages are delivered in the clear, delivered encrypted, or dropped.</p> <p>To view Message Tracking details for the messages that populate this report, click a blue number link in the table.</p>

## Web Interaction Page

To view the Web Interaction report page, select **Web Interaction** from the User Reports section of the Reports drop-down.

- Web Interaction report modules are populated only if the Web Interaction Tracking feature is enabled on managed Email Security appliances.
- Web Interaction reports are available for incoming and outgoing messages.
- Only rewritten URLs (either by policy or Outbreak Filter) clicked by the end users are included in these modules.
- Web Interaction Tracking page includes the following reports:
  - Top Malicious URLs clicked by End Users.
  - Top Users who clicked on Rewritten Malicious URLs.
  - Web Interaction Tracking Details.

From the Web Interaction report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

The following list explains the various sections on the Web Interaction report page:

**Table 18: Details on the Web Interaction Page**

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view. For more information, see <a href="#">Choosing a Time Range for Reports</a> .

Section	Description
View Data For (drop-down list)	Choose an Email Security appliance for which you want to view the data, or choose All Email Appliances.  See also <a href="#">Viewing Reporting Data for an Appliance or Reporting Group</a> .
Top Malicious URLs clicked by End Users	This section displays the summary of the top malicious URLs clicked by end users, for incoming and outgoing messages.
Top Users who clicked on Malicious URLs	This section displays the summary of the top end users who clicked on the Rewritten Malicious URLs, for incoming and outgoing messages.
Web Interaction Tracking Details	This section displays the chart view and the summary of malicious and neutral URLs of the incoming and outgoing messages.  To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

## Web Interaction Tracking Details

The Web Interaction Tracking Details table is an interactive table which includes the following information:

- A list of all the rewritten URLs (malicious and unmalicious).
- Action taken (allow, block, or unknown) when a rewritten URL was clicked.
- If the verdict of a URL (clean or malicious) was unknown at the time when the end user clicked it, the status is shown as unknown. This could be because the URL was under further scrutiny or the web server was down or not reachable at the time of the user click.
- The number of times end users clicked on a rewritten URL.
- Note the following:
  - If you have configured a content or message filter to deliver messages after rewriting malicious URLs and notify another user (for example, an administrator), the web interaction tracking data for the original recipient is incremented if the notified user clicks on the rewritten URLs.
  - If you are sending a copy of quarantined messages containing rewritten URLs to a user other than the original recipient (for example, to an administrator) using the web interface, the web interaction tracking data for the original recipient is incremented if the other user clicks on the rewritten URLs.

To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

## Message Filters Page

The Message Filters report page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages.

You can use the Message Filters report page to view:

- Top message filter by number of matches in graphical format.
- Total message filter by number of matches in tabular format.

To view the Message Filters report page, select **Message Filters** from the Filter Reports section of the Reports drop-down.

From the Message Filters report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

## High Volume Mail Page

Use reports on this page to:

- Identify attacks involving a large number of messages from a single sender, or with identical subjects, within a moving one-hour period.
- Monitor top domains to ensure that such attacks do not originate in your own domain. If this situation occurs, one or more accounts in your organization may be compromised.
- Help identify false positives so you can adjust your filters accordingly.

To view the High Volume Mail report page, select **High Volume Mail** from the Filter Reports section of the Reports drop-down.

You can use the High Volume Mail report page to view:

- Messages with the top subjects in graphical format.
- Messages with the top envelope senders in graphical format.
- Top message filters by number of matches in graphical format.
- Total message filters by number of matches in tabular format.

From the High Volume Mail report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).

Reports on this page show data only from message filters that use the Header Repeats rule and that pass the number-of-messages threshold that you set in that rule. When combined with other rules, the Header Repeats rule is evaluated last, and is not evaluated at all if the message disposition is determined by a preceding condition. Similarly, messages caught by Rate Limiting never reach Header Repeats message filters. Therefore, some messages that might otherwise be considered high-volume mail may not be included in these reports. If you have configured your filters to whitelist certain messages, those messages are also excluded from these reports.

For more information about message filters and the Header Repeats rule, see the online help or user guide for your Email Security appliance.

## Content Filters Page

The Content Filters report page shows information about the top incoming and outgoing content filter matches (which content filter had the most matching messages). The page displays the data as both bar charts and listings. Using the Content Filters report page, you can answer the following types of questions:

- Which content filter is triggered the most by incoming or outgoing mail?

- Who are the top users sending or receiving mail that triggers a particular content filter?

To view the Content Filters report page, select Content Filters from the Filter Reports section of the Reports drop-down.

You can use the Content Filter report page to view:

- Top incoming and outgoing content filter matches in graphical format.
- Top incoming and outgoing content filter matches in tabular format.

From the Content Filters report page you can export raw data to a CSV file. For information on printing or exporting a file, see the [Printing and Exporting Reporting Data](#).


**Note**

You can generate a scheduled report for the Content Filter page. See the [Scheduling Email Reports](#).

## System Capacity Page

The System Capacity report page provides a detailed representation of the system load, including messages in the work queue, incoming and outgoing messages (volume, size, and number), overall CPU usage, CPU usage by function, and memory page swapping information.

The System Capacity report page can be used to determine the following information:

- Identify when Email Security appliances are exceeding recommended capacity; this enables you to determine when configuration optimization or additional appliances are needed.
- Identify historical trends in system behavior that point to upcoming capacity issues.
- For troubleshooting, identify which parts of the system are using the most resources.

Monitor your Email Security appliances to ensure that the capacity is appropriate to your message volumes. Over time, volume inevitably rises and appropriate monitoring ensures that additional capacity or configuration changes can be applied proactively. The most effective way to monitor system capacity is to track the overall volume, the messages in the work queue, and the incidents of Resource Conservation Mode.

- **Volume:** It is important to understand the “normal” message volume and the “usual” spikes in your environment. Track this data over time to measure volume growth. You can use the Incoming Mail and Outgoing Mail pages to track volume over time. For more information, see [System Capacity – Incoming Mail](#) and [System Capacity – Outgoing Mail](#).
- **Work Queue:** The work queue is designed to work as a “shock absorber”—absorbing and filtering spam attacks and processing unusual increases in non-spam messages. However, the work queue can also indicate a system under stress. Prolonged and frequent work queue backups may indicate a capacity problem. You can use the System Capacity – Workqueue page to track the activity in your work queue. For more information, see [System Capacity – Workqueue](#).
- **Resource Conservation Mode:** When an appliance becomes overloaded, it enters Resource Conservation Mode (RCM) and sends a CRITICAL system alert. This is designed to protect the device and allow it to process any backlog of messages. Your appliance should enter RCM infrequently and only during a very large or unusual increase in mail volume. Frequent RCM alerts may be an indication that the system is becoming overloaded. See [Resource Conservation Activity](#).

## How to Interpret the Data You See on System Capacity Page

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

- **Day Report**— The Day report queries the hour table and displays the exact number of queries that have been received by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table. This is an exact number.
- **Month Report**— The Month report queries the day tables for the 30 or 31 days (dependent on the number of days in the month), giving you an exact report on the number of queries over 30 or 31 days. Again, this is an exact number.

The 'Maximum' value indicator on the System Capacity page is the highest value seen for the specified period. The 'Average' value is the average of all values for the specified period. The period of aggregation depends on the interval selected for that report. For example, you can choose to see the Average and Maximum values for each day if the chart is for a month period.

You can click the View Details link for a specific graph to view data for individual Email Security appliances and overall data for the appliances connected to the Security Management appliance.

## System Capacity – Workqueue

The Workqueue page shows the average time a message spends in the work queue, excluding any time spent in the Spam quarantine or in a policy, virus, or outbreak quarantine. You can view time periods from an hour up to one month. This average can help in identifying both short term events delaying mail delivery and identify long term trends in the workload on the system.



### Note

If a message is released from the quarantine into the work queue, the "average time in work queue" metric ignores this time. This prevents double-counting and distorted statistics due to extended time spent in a quarantine.

The report also shows the volume of messages in the work queue over a specified time period, and it shows the maximum messages in the work queue over the same time period. The graphical representation of the maximum messages in the work queue also shows the work queue threshold level.

Occasional spikes in the Workqueue graphs are normal and expected. If the messages in the work queue remain higher than the configured threshold for a long duration, this may indicate a capacity issue. In this scenario, consider tuning the threshold level or review the system configuration.

To change the work queue threshold level, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances](#).



### Tip

When reviewing the work queue page, you may want to measure the frequency of work queue backups, and take note of work queue backups that exceed 10,000 messages.

## System Capacity – Incoming Mail

The System Capacity – Incoming Mail page shows incoming connections, the total number of incoming messages, the average message size, and the total incoming message size. You can view the results for a day,

week, month, or year. It is important to understand the trends of normal message volume and spikes in your environment. You can use the System Capacity – Incoming Mail page to track volume growth over time and plan for system capacity. You might also want to compare the incoming mail data with the sender profile data to view the trends in volumes of email messages that are sent from specific domains to your network.

**Note**

An increased number of incoming connections may not necessarily affect system load.

## System Capacity – Outgoing Mail

The System Capacity – Outgoing Mail page shows outgoing connections, the total number of outgoing messages, the average message size, and the total outgoing message size. You can view the results for a day, week, month, or year. It is important to understand the trends of normal message volume and spikes in your environment. You can use the System Capacity – Outgoing Mail page to track volume growth over time and plan for system capacity. You might also want to compare the outgoing mail data with the outgoing destinations data to view the trends in volumes of email messages that are sent from specific domains or IP addresses.

## System Capacity – System Load

The system load report shows the following:

### Overall CPU Usage

Email Security appliances are optimized to use idle CPU resources to improve message throughput. High CPU usage may not indicate a system capacity problem. If the high CPU usage is coupled with consistent, high-volume memory page swapping, you may have a capacity problem.

**Note**

This graph also indicates a threshold for CPU usage that is a visual reference only. To adjust the position of this line, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances](#). You can configure your Email Security appliances to send you alerts that will suggest actions that you can take to address capacity issues.

This page also shows a graph that displays the amount of CPU used by different functions, including mail processing, spam and virus engines, reporting, and quarantines. The CPU-by-function graph is a good indicator of which areas of the product use the most resources on your system. If you need to optimize your appliance, this graph can help you determine which functions may need to be tuned or disabled.

### Memory Page Swapping

The memory page swapping graph shows how frequently the system must page to disk, in kilobytes per second.

The system is designed to swap memory regularly, so some memory swapping is expected and is not an indication of problems with your appliance. Unless the system *consistently* swaps memory in high volumes, memory swapping is normal and expected behavior (especially on C170 appliances). To improve performance, you may need to add Email Security appliances to your network or tune your configuration to ensure maximum throughput.

**Note**

This graph also indicates a threshold for memory page swapping that is a visual reference only. To adjust the position of this line, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances](#). You can configure your Email Security appliances to send you alerts that will suggest actions that you can take to address capacity issues.

**Resource Conservation Activity**

The resource conservation activity graph shows the number of times the Email Security appliance entered Resource Conservation Mode (RCM). For example, if the graph shows *n* times, it means that the appliance has entered RCM *n* times and exited at least *n*-1 times.

Your appliances should enter RCM infrequently and only during a very large or unusual increase in mail volume. If the Resource Conservation Activity graph shows that your appliance is entering RCS frequently, it may be an indication that the system is becoming overloaded.

**System Capacity – All**

The **All** page consolidates all the previous system capacity reports onto a single page so you can view the relationship between the different reports. For example, you might see that the message queue is high at the same time that excessive memory swapping takes place. This might be an indication that you have a capacity problem. You may want to save this page as a PDF file to preserve a snapshot of system performance for later reference (or to share with support staff).

**Threshold Indicator in System Capacity Graphs**

In some graphs, a line indicates the default value that may indicate a possible problem if it is frequently or consistently crossed. To adjust this visual indicator, see [Adjusting the Reference Threshold in System Health Graphs for Email Security Appliances](#).

**Reporting Data Availability Page**

The **Email > Reporting > Reporting Data Availability** page allows you to view, update and sort data to provide real-time visibility into resource utilization and email traffic trouble spots.

All data resource utilization and email traffic trouble spots are shown from this page, including the data availability for the overall appliances that are managed by the Security Management appliance.

From this report page you can also view the data availability for a specific appliance and time range.

**Reporting of Graymail**

Graymail statistics are reflected in the following reports:

Report	Contains the Following Graymail Data
Mail Flow Summary page > Incoming tab	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages.
Mail Flow Details page > Outgoing Senders tab	The top graymail senders.



Report	Contains the Following Graymail Data
Mail Flow Details page > Incoming Mails tab	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for all the IP addresses, domain names, or network owners.
User Mail Summary page > Top Users by Graymail	The top end users who receive graymail.
User Mail Summary page > User Mail Details	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for all the users.

## Reporting of Marketing Messages after Upgrade to AsyncOS 9.5

After upgrade to AsyncOS 9.5:

- The number of marketing messages is the sum of marketing messages detected before and after the upgrade.
- The total number of graymail messages does not include the number of marketing messages detected before the upgrade.
- The total number of attempted messages also includes the number of marketing messages detected before the upgrade.
- If the graymail feature is not enabled on managed Email Security appliances, marketing messages are counted as clean messages.

## About Scheduled and On-Demand Email Reports

### Types of Reports Available

Except as noted, the following types of Email Security reports are available as both scheduled and on-demand reports:

- **Content Filters**—This report includes up to 40 content filters. For additional information on what is included on this page, see the [Content Filters Page, on page 44](#).
- **DLP Incident Summary**—For information on what is included on this page, see the [DLP Incident Summary Page, on page 41](#).
- **Delivery Status**—The report page displays information about delivery problems to a specific recipient domain or Virtual Gateway address, page displays a list of the top 20, 50, or 100 recipient domains for messages delivered by the system within the last three hours. You can sort by latest host status, active recipients (the default), connections out, delivered recipients, soft bounced events, and hard bounced recipients by clicking the links in the column heading for each statistic. For more information on what the Delivery Status page does on the Email Security appliance, see the documentation or online help for your Email Security appliance.

- Domain-Based Executive Summary—This report is based on the [Mail Flow Summary Page, on page 9](#), and is limited to a group of specified domains. For information on what is included, see the [Domain-Based Executive Summary Report](#).
- Executive Summary—This report is based on the information from the [Mail Flow Summary Page, on page 9](#). For information on what is included, see the [Domain-Based Executive Summary Report](#).
- Mail Flow Details — For information on what is included on this page, see the [Mail Flow Details Page, on page 25](#).
- User Mail Summary—For information on what is included on this page, see the [User Mail Summary, on page 38](#).
- Outgoing Destinations—For information on what is included on this page, see the [Outgoing Destinations Page, on page 31](#).
- Sender Groups —For information on what is included on this page, see the [Sender Groups Page, on page 31](#).
- TLS Encrptions—For information on what is included on this page, see the [TLS Encryption Page, on page 33](#).
- Virus Types—For information on what is included on this page, see the [Virus Filtering Page, on page 23](#).

### Time ranges

Depending on the report, these reports can be configured to include data for the previous day, previous seven days, previous month, previous calendar day (up to 250), or previous calendar month (up to 12). Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months).

Regardless of when you run a report, the data is returned from the previous time interval (hour, day, week, or month). For example, if you schedule a daily report to run at 1AM, the report will contain data from the previous day, midnight to midnight (00:00 to 23:59).

### Languages and Locales



#### Note

You can schedule a PDF report or export raw data as a CSV file with a specific locale for that individual report. The language drop-down menu on the Scheduled Reports page allows you to view or schedule a PDF report in the users current selected locale and language. See important information at [Printing and Exporting Reporting Data](#).

### Storage of Archived Reports

For information on how long reports are stored for, and when archived reports are deleted from the system, see [Viewing and Managing Archived Email Reports](#).

## Additional Report Types

Two special reports that can be generated in the **Email > Reporting** section on the Security Management appliance are:

## Domain-Based Executive Summary Report

The Domain-Based Executive Summary report provides a synopsis of the incoming and outgoing message activity for one or more domains in your network. It is similar to the Executive Summary report, but it limits the report data to the messages sent to and from the domains that you specify. The outgoing mail summary shows data only when the domain in the PTR (pointer record) of the sending server matches a domain you specify. If multiple domains are specified, the appliance aggregates the data for all those domains into a single report.

To generate reports for a subdomain, you must add its parent domain as a second-level domain in the reporting system of the Email Security appliance and the Security Management appliance. For example, if you add example.com as a second-level domain, its subdomains, such as subdomain.example.com, are available for reporting. To add second-level domains, use **reportingconfig -> mailsetup -> tld** in the Email Security appliance CLI, and **reportingconfig -> domain -> tld** in the Security Management appliance CLI.

Unlike other scheduled reports, Domain-Based Executive Summary reports are not archived.

### Domain-Based Executive Summary Reports and Messages Blocked by Sender Reputation Filtering

Because messages blocked by sender reputation filtering do not enter the work queue, AsyncOS does not process these messages to determine the domain destination. An algorithm estimates the number of rejected messages per domain. To determine the exact number of blocked messages per domain, you can delay HAT rejections on the Security Management appliance until the messages reach the recipient level (RCPT TO). This allows AsyncOS to collect recipient data from the incoming messages. You can delay rejections using **listenerconfig -> setup** command on the Email Security appliance. However, this option can impact system performance. For more information about delayed HAT rejections, see the documentation for your Email Security appliance.



#### Note

To see Stopped by Reputation Filtering results in your Domain-Based Executive Summary report on the Security Management appliance, you must have **hat\_reject\_info** enabled on both the Email Security appliance and the Security Management appliance. To enable the **hat\_reject\_info** on the Security Management appliance, run the **reportingconfig > domain > hat\_reject\_info** command.

### Managing Lists of Domains and Recipients for Domain-Based Executive Summary Reports

You can use a configuration file to manage the domains and recipients for a Domain-Based Executive Summary report. The configuration file is a text file that is stored in the configuration directory of the appliance. Each line in the file produces a separate report. This allows you to include a large number of domains and recipients in a single report, as well as define multiple domain reports in a single configuration file.

Each line of the configuration file includes a space-separated list of domain names and a space-separated list of email addresses for the report recipients. A comma separates the list of domain names from the list of email addresses. You can include subdomains by appending the subdomain name and a period at the beginning of the parent domain name, such as subdomain.example.com.

The following is a Single Report configuration file that generates three reports.

```
yourdomain.com sampledomain.com, admin@yourdomain.com
sampledomain.com, admin@yourdomain.com user@sampledomain.com
subdomain.example.com mail.example.com, user@example.com
```

**Note**



You can use a configuration file and the settings defined for a single named report to generate multiple reports at the same time. For example, a company named Bigfish purchases two other companies, Redfish and Bluefish, and continues to maintain their domains. Bigfish creates a single Domain-Based Executive Summary report using a configuration file containing three lines corresponding to separate domain reports. When the appliance generates a Domain-Based Executive Summary report, an administrator for Bigfish receives a report on the Bigfish.com, Redfish.com, and Bluefish.com domains, while a Redfish administrator receives a report on the Redfish.com domain and a Bluefish administrator receives a report on the Bluefish.com domain.

You can upload a different configuration file to the appliance for each named report. You can also use the same configuration file for multiple reports. For example, you might create separate named reports that provide data about the same domains over different time periods. If you update a configuration file on your appliance, you do not have to update the report settings in the GUI unless you change the filename.

## Creating Domain-Based Executive Summary Reports

**Step 1**

On the Security Management appliance, you can schedule the report or generate the report immediately. To schedule the report:

- a) [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- b) Choose **Email > Reporting > Scheduled Reports**.
- c) Click **Add Scheduled Report**.  
To create an on-demand report:
  - [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
  - Choose **Email > Reporting > Archived Reports**.
  - Click **Generate Report Now**.

**Step 2**

From the **Report Type** drop-down list, choose **Domain-Based Executive Summary** report type.

**Step 3**

Specify the domains to include in the report and the email addresses for the report recipients. You can select one of the following options for generating the report:

- Generate report by specifying individual domains. Enter the domains for the report and the email addresses for the report recipients. Use commas to separate multiple entries. You can also use subdomains, such as subdomain.yourdomain.com. Specifying individual domains is recommended if you create reports for a small number of domains that are not expected to change frequently.
- Generate reports by uploading file. Import a configuration file that contains a list of the domains and recipient email addresses for the report. You can select a configuration file from the configuration directory on the appliance or upload one from your local computer. Using a configuration file is recommended if you create reports for a large number of domains that change frequently. For more information on configuration files for domain-based reports, see [Managing Lists of Domains and Recipients for Domain-Based Executive Summary Reports](#).

**Note** If you send reports to an external account (such as Yahoo! Mail or Gmail), you may need to add the reporting return address to the external account's whitelist to prevent report messages from being incorrectly classified as spam.

- Step 4** In the Title text field, type the name of the title for the report.  
AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.
- Step 5** In the Outgoing Domain section, choose the domain type for the outgoing mail summary. Choices are: By Server or By Email Address.
- Step 6** From the Time Range to Include drop-down list, select a time range for the report data.
- Step 7** In the Format section, choose the format of the report.  
Choices include:
- PDF. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.
  - CSV. Create an ASCII text file that contains raw data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.
- Step 8** From the Schedule section, choose a schedule for generating the report.  
Choices include: Daily, Weekly (drop-down list for day of week included), or monthly.
- Step 9** (Optional) Upload a custom logo for the report. The logo appears at the top of the report.
- The logo should be a .jpg, .gif, or .png file that is at most 550 x 50 pixels.
  - If a logo file is not supplied, the default Cisco logo is used.
- Step 10** Select a language for this report. For generating PDFs in Asian languages, see important information at [Printing and Exporting Reporting Data](#).
- Step 11** Click **Submit** to submit your changes on the page, then click **Commit Changes** to commit your changes.
- 

## Executive Summary Report

The Executive Summary Report is a high-level overview of the incoming and outgoing email message activity from your Email Security appliances. that can be viewed on the Security Management appliance.

This report page summarizes what you can view on the [Mail Flow Summary Page, on page 9](#). For more information on the Email Reporting Overview page, see [Mail Flow Summary Page, on page 9](#).

# Scheduled Reports Page

- [Scheduling Email Reports](#)


## Scheduling Email Reports

You can schedule any of the reports listed in [About Scheduled and On-Demand Email Reports](#).


To manage report scheduling, see the following:

## Adding Scheduled Reports

To add a scheduled email report, use the following steps:


- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Email > Reporting > Scheduled Reports**.
- Step 3** Click **Add Scheduled Report**.
- Step 4** Choose your report type.  
For descriptions of the report types, see [About Scheduled and On-Demand Email Reports](#).
- Note** - For information about the settings for a Domain-Based Executive Summary report, see [Domain-Based Executive Summary Report](#).  
- Available options for scheduled reports differ by report type. Options described in the remainder of this procedure do not necessarily apply to all reports.
- Step 5** In the **Title** field, type the title of your report.  
To avoid creating multiple reports with the same name, we recommend using a descriptive title.
- Step 6** Choose the time range for the report from the **Time Range to Include** drop-down menu.
- Step 7** Choose 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 8** Depending on the report, for Number of Rows, choose the amount of data to include.
- Step 9** Depending on the report, choose the column by which to sort the report.
- Step 10** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report. Additionally, include the time that you want the report scheduled for. Time increments are based on midnight to midnight (00:00 to 23:59).
- Step 11** In the **Email** text field, type in the email address where the generated report will be sent.  
If you do not specify an email recipient, the system will still archive the reports.  
  
You can add as many recipients for reports as you want, including zero recipients. If you need to send the reports to a large number of addresses, however, you may want to create a mailing list instead of listing the recipients individually.
- Step 12** Choose a language for the report.  
For Asian languages, see important information at [Printing and Exporting Reporting Data](#).
- Step 13** Click **Submit**.
-

## Editing Scheduled Reports

- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Email > Reporting > Scheduled Reports**.
- Step 3** Click the report name link in the Report Title column that you want to modify.
- Step 4** Modify the report settings.
- Step 5** Submit and commit your changes.
- 

## Discontinuing Scheduled Reports


To prevent future instances of scheduled reports from being generated, perform the following steps:

- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Email > Reporting > Scheduled Reports**.
- Step 3** Select the check boxes corresponding to the reports that you want to discontinue generating. To remove all scheduled reports, select the **All** check box.
- Step 4** Click **Delete**.
- Note** Any archived versions of deleted reports are *not* automatically deleted. To delete previously-generated reports, see [Deleting Archived Reports](#).
- 

## Generating Email Reports On Demand

In addition to the reports that you can view (and generate PDFs for) using the interactive report pages described in [Understanding the Email Reporting Pages](#), on page 6, you can save PDFs or raw-data CSV files for the reports listed in [About Scheduled and On-Demand Email Reports](#) at any time, for the time frame that you specify.

To generate an on-demand report perform the following:

- 
- Step 1** [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface.
- Step 2** Choose **Email > Reporting > Archived Reports**.
- Step 3** Click **Generate Report Now**.
- Step 4** Choose a report type.

For descriptions of the report types, see [About Scheduled and On-Demand Email Reports](#).

- Step 5** In the Title text field, type the name of the title for the report. AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.
- Note** For information about the settings for a Domain-Based Executive Summary report, see [Domain-Based Executive Summary Report](#).
- Available options for scheduled reports differ by report type. Options described in the remainder of this procedure do not necessarily apply to all reports.
- Step 6** From the Time Range to Include drop-down list, select a time range for the report data. Note the custom time range option.
- Step 7** In the Format section, choose the format of the report. Choices include:
- PDF. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.
  - CSV. Create an ASCII text file that contains raw data as comma-separated values. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file is created for each table.
- Step 8** Select the appliances or appliance groups for which you want to run the report. If you have not created any appliance groups, this option does not appear.
- Step 9** From the Delivery Option section, choose the following:
- Archive the report by checking the **Archive Report** checkbox.
- By choosing this, the report will be listed on the Archived Reports page.
- Note** Domain-Based Executive Summary reports cannot be archived.
- Email the report, by checking the **Email now to recipients** checkbox.
- In the text field, type in the recipient email addresses for the report.
- Step 10** Select a language for this report. For generating PDFs in Asian languages, see important information at [Printing and Exporting Reporting Data](#).
- Step 11** Click **Deliver This Report** to generate the report.
- 

## Archived Email Reports Page

- [About Scheduled and On-Demand Email Reports](#)
- [Generating Email Reports On Demand](#)
- [Viewing and Managing Archived Email Reports](#)



# Viewing and Managing Archived Email Reports

Scheduled and on-demand reports are archived for a period of time.


The Security Management appliance retains the most recent reports that it generates, up to 30 instances of each scheduled report, up to 1000 total versions for all reports. The limit of 30 instances applies to each scheduled report with the same name and time range.

Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000.

Archived reports are stored in the /periodic\_reports directory on the appliance. (See [IP Interfaces and Accessing the Appliance](#) for more information.)

## Accessing Archived Reports


The **Email > Reporting > Archived Reports** page lists scheduled and on-demand reports that you have chosen to archive which have been generated and not yet purged.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface. |
| <b>Step 2</b> | Choose <b>Email &gt; Reporting &gt; Archived Reports</b> .  |
| <b>Step 3</b> | To locate a particular report if the list is long, filter the list by choosing a report type from the <b>Show</b> menu, or click a column heading to sort by that column.   |
| <b>Step 4</b> | Click the Report Title to view that report.   |
- 

## Deleting Archived Reports

Reports are automatically deleted from the system according to the rules outlined in [Viewing and Managing Archived Email Reports](#). However, you can manually delete unneeded reports.

To manually delete Archived reports, perform the following:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | [New Web Interface Only] On the Cloud Email Security Management Console, click on the gear  icon to load the legacy web interface. |
| <b>Step 2</b> | Choose <b>Email &gt; Reporting &gt; Archived Reports</b> .<br>The Archived reports that are available are displayed.  |
| <b>Step 3</b> | Select the checkbox for one or more reports to delete.  |
| <b>Step 4</b> | Click <b>Delete</b> .   |
| <b>Step 5</b> | To prevent future instances of scheduled reports from being generated, see <a href="#">Discontinuing Scheduled Reports</a> .  |
-

