Using Centralized Email Security Reporting

This chapter contains the following sections:

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:

- Enabling Centralized Email Reporting on the Security Management Appliance , on page 2
- Adding the Centralized Email Reporting Service to Each Managed Email Security Appliance , on page 3
- Creating Email Reporting Groups, on page 3
- Enabling Centralized Email Reporting on Email Security Appliances , on page 4

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 On the Security Management appliance, choose **Management Appliance > Centralized Services > Email > Centralized Reporting**.

Step 2 Click **Enable**.

Step 3 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 4 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 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 2 If you have already added the Email Security appliance to the list on this page:

a) Click the name of an Email Security appliance.

b) Select the **Centralized Reporting** service.

Step 3 If you have not yet added Email Security appliances:

a) Click Add Email Appliance.

b) 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**.

c) The Centralized Reporting service is pre-selected.

d) Click **Establish Connection.**

e) 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.

f) Wait for the Success message to appear above the table on the page.

g) Click **Test Connection.**.

h) Read test results above the table.

Step 4 Click **Submit**.

Step 5 Repeat this procedure for each Email Security appliance for which you want to enable Centralized Reporting.

Step 6 Commit your changes.

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

Step 2   Click **Add Group** .

Step 3   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 4   Click **Add** to add the appliances to the Group Members list.

Step 5   Submit and commit your changes.

Enabling Centralized Email Reporting on Email Security Appliances

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

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 search for specific information within your data, see Searching and the Interactive Email Report Pages , on page 5.

- To print or export report information, see Printing and Exporting Reporting and Tracking Data

- To understand the various interactive report pages, see Understanding the Email Reporting Pages, on page 5.

- To generate a report on demand, see Generating Email Reports On Demand , on page 47.

- To schedule reports to run automatically at intervals and times that you specify, see Scheduling Email Reports, on page 45.

- To view archived on-demand and scheduled reports, see Viewing and Managing Archived Email Reports , on page 48.

- 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 Tab Options

Email Reporting Menu	Action
Email Reporting Overview Page	The Overview page provides a synopsis of the activity on your Email Security appliances. It includes graphs and summary tables for the incoming and outgoing messages. For more information, see the Email Reporting Overview Page, on page 11.
Incoming Mail Page	The Incoming Mail 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. For more information, see the Incoming Mail Page, on page 15.
Sender Groups Report 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. For more information, see the Sender Groups Report Page, on page 18.
Outgoing Destinations Page	The Outgoing Destinations 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). For more information, see the Outgoing Destinations Page, on page 19.
Outgoing Senders Page	The Outgoing Senders page provides information about the quantity and type of mail being sent from IP addresses and domains in your network. For more information, see the Outgoing Senders Page, on page 19.
Internal Users Page	The Internal Users 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. For more information, see the Internal Users Page, on page 20.
DLP Incidents	The DLP Incident Summary page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. For more information, see the DLP Incidents , on page 22.
Message Filters	The Message Filters page shows information about the top message filter matches (which message filters had the largest number of matching messages) for incoming and outgoing messages. For more information, see the Message Filters , on page 23

Email Reporting Menu	Action
Geo Distribution	The Geo Distribution page shows the: • Top incoming mail connections based on country of origin in graphical format. • Total incoming mail connections based on country of origin in tabular format. For more information, see the Geo Distribution, on page 23.
High Volume Mail	The High Volume Mail 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 High Volume Mail , on page 24.
Content Filters Page	The Content Filters 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. Using the Content Filters page, you can review your corporate policies on a per-content-filter or per-user basis. For more information, see the Content Filters Page, on page 24.
DMARC Verification	The DMARC Verification 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. For more information, see the DMARC Verification , on page 25.
Macro Detection	The Macro Detection Report page shows the top incoming and outgoing macro-enabled attachments by file type detected by the content or message filters. For more information, see the Macro Detection, on page 25
Virus Types Page	The Virus Types 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 more information, see the Virus Types Page, on page 25.
URL Filtering Page	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. For more information, see the URL Filtering Page , on page 26.

Email Reporting Menu	Action
Web Interaction Tracking Page	Identifies the end users who clicked URLs rewritten by policy or Outbreak Filter, and the action associated with each user click.
	For more information, see the Web Interaction Tracking Page, on page 27.
Forged Email Detection Page	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.
	See Forged Email Detection Page, on page 27.
Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages	There are three reporting pages showing file reputation and analysis data.
	For more information, see the Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages , on page 28.
Mailbox Auto Remediation	Use this page to view the details of the mailbox remediation results.
	See Mailbox Auto Remediation, on page 32
TLS Connections Page	The TLS Connections 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.
	For more information, see the TLS Connections Page, on page 33.
Inbound SMTP Authentication Page	The Inbound SMTP authentication 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.
	For more information, see Inbound SMTP Authentication Page, on page 34.
Outbreak Filters Page	The Outbreak Filters page shows information about recent outbreaks and the messages quarantined by Outbreak Filters. Use this page to monitor your defense against virus attacks.
	For more information, see the Outbreak Filters Page, on page 35.
Rate Limits Page	The Rate Limits page shows the mail senders (based on MAIL-FROM address) who exceed the threshold you set for the number of message recipients per sender.
	For more information, see the Rate Limits Page , on page 34.
System Capacity Page	Allows you to view the overall workload that is sending reporting data to the Security Management appliance.
	For more information, see the System Capacity Page, on page 38.

Email Reporting Menu	Action
Reporting Data Availability Page	Allows you to get a glimpse of the impact of the reporting data on the Security Management appliance for each appliance. For more information, see the Reporting Data Availability Page, on page 41.
Scheduling Email Reports	Allows you to schedule reports for a specified time range. For more information, see the Scheduling Email Reports, on page 45.
Viewing and Managing Archived Email Reports	Allows you to view and manage archived reports. For more information, see the Viewing and Managing Archived Email Reports , on page 48. Also allows you to generate on-demand reports. See Generating Email Reports On Demand , on page 47.

Table Column Descriptions for Email Reporting Pages

Table 2: Table Column Descriptions for Email Reporting Pages

Column Name	
Incoming Mail Details	
Connections Rejected	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.
Connections Accepted	All connections accepted,
Total Attempted	All accepted and blocked connections attempted.
Stopped by Recipient Throttling	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.

Column Name	
Stopped by Reputation Filtering	The value for Stopped by Reputation Filtering is calculated based on several factors: • Number of "throttled" messages from this sender • Number of rejected or TCP refused connections (may be a partial count) • A conservative multiplier for the number of messages per connection 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 were stopped. **Note** The Stopped by Reputation Filtering total on the Overview page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.
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
Stopped by Content Filter	The total count of messages that were stopped by a content filter.
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.
Clean	All clean messages. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.
User Mail Flow Details (Internal Users Page)	
Incoming Spam Detected	All incoming spam that is detected
Incoming Virus Detected	The incoming virus that has been detected.
Incoming Content Filter Matches	The incoming content filter matches that have been detected.

Column Name	
Incoming Stopped by Content Filter	The Incoming messages that were stopped due to content filters that have been set.
Incoming Clean	All incoming clean messages.
Outgoing Spam Detected	The outgoing spam that was detected.
Outgoing Virus Detected	The outgoing viruses that have been detected.
Outgoing Content Filter Matches	The outgoing content filter matches that have been 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.
Incoming and Outgoing TLS Connections: TLS Connections Page	
Required TLS: Failed	All required TLS connections that failed.
Required TLS: Successful	All required TLS connections that are successful.
Preferred TLS: Failed	All preferred TLS connections that failed.
Preferred TLS: Successful	All preferred TLS connections that are successful.
Total Connections	Total number of TLS connections.
Total Messages	The total number of TLS messages.
Outbreak Filters	
Outbreak Name	The name of the outbreak.
Outbreak ID	The outbreak ID.
First Seen Globally	The first time the virus has been seen globally.
Protection Time	The time the virus has been protected.
Quarantined Messages	Messages related to the quarantine.

Email Reporting Overview Page

The **Email > Reporting > Overview** page on the Security Management appliance provides a synopsis of the email message activity from your Email Security appliances. The Overview page includes graphs and summary tables for the incoming and outgoing messages.

At a high level the **Overview** page shows you the incoming and outgoing mail graphs, and well as incoming and outgoing mail summaries.

The mail trend graphs provide a visual representation of the mail flow. You can use the mail trend graphs on this page to monitor the flow of all mail into and out of your appliances.

Note The Domain-Based Executive Summary Report and the Executive Summary report are based on the Email Reporting Overview Page, on page 11. For more information, see the Domain-Based Executive Summary Report, on page 43 and Executive Summary Report , on page 45

Table 3: Details on the Email Reporting Overview Page

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

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 Overview Page

Messages reported in the Incoming Mail Summary on the Overview report page are categorized as follows:

Table 4: Email Categories on Overview Page

Category	Description
Stopped by Reputation Filtering	All connections blocked by HAT policies multiplied by a fixed multiplier (see the How Incoming Mail Messages are Counted, on page 12) plus all recipients blocked by recipient throttling. The value for Stopped by Reputation Filtering is calculated based on several factors: • Number of "throttled" messages from this sender • Number of rejected or TCP refused connections (may be a partial count) • A conservative multiplier for the number of messages per connection 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 were stopped. The Stopped by Reputation Filtering total on the Overview page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.
Invalid Recipients	All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.
Spam Messages Detected	The total count of messages detected by the anti-spam scanning engine as positive or suspect. Additionally, messages that are both spam and virus positive.
Virus Messages Detected	The total count and percentage of messages detected as virus positive and not also spam. The following messages are counted in the "Virus Detected" category: • Messages with a virus scan result of "Repaired" or "Infectious" • Messages with a virus scan result of "Encrypted" when the option to count encrypted messages as containing viruses is selected • Messages with a virus scan result of "Unscannable" when the action for unscannable messages is NOT "Deliver" • 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 • Messages that are deleted from the Outbreak quarantine, either manually or by timing out.
Detected by Advanced Malware Protection	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.
Messages with Malicious URLs	One or more URLs in the message were found to be malicious by URL filtering.
Stopped by Content Filter	The total count of messages that were stopped by a content filter. If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.
Stopped by DMARC	The total count of messages that failed DMARC verification.

Category	Description
S/MIME Verification/Decryption Failed	The total count of messages that failed S/MIME verification, decryption, or both.
Marketing Messages	The total count of advertising messages sent by recognized professional marketing groups, for example Amazon.com. This list item appears on the page only if marketing data are present in the system. This number includes marketing messages identified both by Email Security appliances on which the graymail feature is enabled and by appliances on which Marketing Email Scanning under anti-spam settings is enabled.
Social Networking Messages	The total count of notification messages from social networks, dating websites, forums, and so on. Examples include LinkedIn and CNET forums. This information is determined by the graymail feature.
Bulk Messages	The total count of advertising messages sent by unrecognized marketing groups, for example, TechTarget, a technology media company. This information is determined by the graymail feature.
Graymail Messages	This number includes marketing messages detected by the graymail feature, plus social networking messages and bulk mail. It does not include marketing messages identified on appliances on which the graymail feature is not enabled, even if those totals are included in the Marketing Messages value. Click on the number corresponding to any of the graymail categories to view a list of messages belonging to that category using Message Tracking. See also Reporting of Graymail , on page 36.
S/MIME Verification/Decryption Successful	The total count of messages that were successfully verified, decrypted, or decrypted and verified using S/MIME.
Clean Messages Accepted	This category is mail that is accepted and deemed to be virus and spam free. The most accurate representation of clean messages accepted when taking per-recipient scanning actions (such as splintered messages being processed by separate mail policies) into account. However, because messages that are marked as spam or virus positive and still delivered are not counted, the actual number of messages delivered may differ from the clean message count. 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. Messages processed on appliances on which the graymail feature is not enabled are counted as clean.
Total Attempted Messages	This number includes spam, marketing messages (whether found by the graymail feature or by Marketing Email Scanning functionality in the anti-spam feature), social networking messages, bulk mail, and clean messages.

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.

Incoming Mail Page

The **Email > Reporting > Incoming Mail**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 perform a Sender Profile search on IP addresses, domains, or organizations that have sent mail to you.

The Incoming Mail Details interactive table displays detailed information about the particular IP address, domain, or network owner (organization). You can access a Sender Profile page for any IP address, domain, or network owner by clicking the corresponding link at the top of the **Incoming Mail** page, or on other Sender Profile pages.

From the Incoming Mail pages you can:

- Perform a search on IP addresses, domains, or network owners (organizations) that have sent mail to your Security Management appliances. See Searching and the Interactive Email Report Pages , on page 5.
- View the Sender Groups report to monitor connections according to the specific sender group and mail flow policy actions. See the Sender Groups Report Page, on page 18 for more information.
- See detailed statistics on senders that have sent mail to your appliances. The statistics include the number of attempted messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth).
- Sort by senders who have sent you a high volume of spam or virus email, as determined by anti-spam or anti-virus security services.
- Use the SenderBase Reputation Service to examine the relationship between specific IP addresses, domains, and organizations to obtain information about a sender.
- Obtain more information about a sender from the SenderBase Reputation Service, including a sender's SenderBase Reputation Score (SBRS) and which sender group the domain matched most recently. Add senders to sender groups.
- Obtain more information about a specific sender who has sent a high volume of spam or virus email, as determined by the anti-spam or anti-virus security services.

Views Within the Incoming Mail Page

The **Incoming Mail** 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.

Additionally, in the Incoming Mail Details section of the Incoming Mail Page, you can click on a Sender's IP Address, Domain name, or Network Owner Information to retrieve specific Sender Profile Information. For more information on Sender Profile information, see the Sender Profile Pages, on page 17.

![note icon]

Note   *Network owners* are entities that contain domains. *Domains* are entities that contain IP addresses.

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.

Click an IP address, domain, or network owner to access details about the sender on the Sender Profile page. The Sender Profile page is an Incoming Mail page that is specific to a particular IP address, domain, or network owner.

To access the mail flow information by sender group, click the **Sender Groups Report** link at the bottom of the Incoming Mail page. See Sender Profile Pages, on page 17.

In some cases, some of the report pages contain several unique sub-reports that can be accessed from the top-level page. For example, the Incoming Mail report page on the Security Management appliance allows you to see information for individual IP Addresses, Domains and Network Owners. Each of these are sub-pages are accessed from the Incoming Mail report page.

Results for each of these sub-report pages are generated on one consolidated report when you click on the Printable PDF link at the top-right of the top-level page; in this case the Incoming Mail report page. See important information in Understanding the Email Reporting Pages, on page 5.

The **Email > Reporting > Incoming Mail** page offers the following views: **IP Addresses**, **Domains**, or **Network Owners**

See the Incoming Mail Details Table, on page 17 for an explanation of the data included in the Incoming Mail Details interactive table.

From the **Incoming Mail** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the Understanding the Email Reporting Pages, on page 5.

![note icon]

Note   You can generate a scheduled report for the Incoming Mail report page. See the Scheduling Email Reports, on page 45.

"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 Details Table

The interactive Incoming Mail Details table at the bottom of the **Incoming Mail** 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. Click the column headings to sort the data.

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 documentation or online help for your Email Security appliance.

For senders, that is Network Owner, IP Address or Domain, listed in the first column of the Incoming Mail Details table, or on the Top Senders by Total Threat Messages, click the **Sender** or **No Domain Information** link to view more information about the sender. The results appear on a **Sender Profile** page, which includes real-time information from the SenderBase Reputation Service. From the Sender Profile page, you can view for more information about specific IP addresses or network owners. For more information, see the Sender Profile Pages, on page 17.

You can also view the Sender Groups report, by clicking **Sender Groups report** at the bottom of the Incoming Mail page. For more information about the Sender Groups report page, see the Sender Groups Report Page, on page 18.

If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.

Sender Profile Pages

When you click a sender in the Incoming Mail Details interactive table, on the **Incoming Mail** page, the Sender Profile page appears. It shows detailed information about the particular IP address, domain, or network owner (organization). You can access a Sender Profile page for any IP address, domain, or network owner by clicking the corresponding link on the Incoming Mail page or on other Sender Profile pages.

Network owners are entities that contain domains. *Domains* are entities that contain IP addresses.

The Sender Profile pages displayed for IP addresses, domains, and network owners vary slightly. For each, the page contains a graph and summary table for incoming mail from the particular sender. Below the graph, a table lists the domains or IP addresses associated with the sender. (The Sender Profile page for an individual IP address does not contain a more granular listing.) The Sender Profile page also includes an information section with the current SenderBase, sender group, and network information for the sender.

- Network Owner profile pages contain information for the network owner, as well as the domains and IP addresses associated with that network owner.
- Domain profile pages contain information for the domains and IP addresses associated with that domain.
- IP address profile pages contain information about the IP address only.

Each Sender Profile page contains the following data in the Current Information table at the bottom of the page:

- The global information from the SenderBase Reputation Service, including:

  - IP address, domain name, and/or network owner
  - Network owner category (network owner only)
  - CIDR range (IP addresses only)
  - Daily magnitude and monthly magnitude for the IP address, domain, and/or network owner
  - Days since the first message was received from this sender

• Last sender group and whether DNS verified (IP address sender profile page only)

Daily magnitude is a measure of how many messages a domain has sent over the last 24 hours. Similar to the Richter scale used to measure earthquakes, SenderBase magnitude is a measure of message volume calculated using a log scale with a base of 10. The maximum theoretical value of the scale is set to 10, which equates to 100% of the world's email message volume. Using the log scale, a one-point increase in magnitude equates to a 10x increase in actual volume.

Monthly magnitude is calculated using the same approach as daily magnitude, except the percentages are calculated based on the volume of email sent over the last 30 days.

- Average magnitude (IP addresses only)
- Lifetime volume / 30 day volume (IP address profile pages only)
- Bonded sender status (IP address profile pages only)
- SenderBase Reputation Score (IP address profile pages only)
- Days since first message (network owner and domain profile pages only)
- Number of domains associated with this network owner (network owner and domain profile pages only)
- Number of IP addresses in this network owner (network owner and domain profile pages only)
- Number of IP addresses used to send email (network owner pages only)

Click **More from SenderBase** to see a page with all information supplied by the SenderBase Reputation Service.

• Details about the domains and IP addresses controlled by this network owner appear on network owner profile pages. Details about the IP addresses in the domain appear on domain pages.

From a domain profile page, you can click on a specific IP address to view specific information, or view an organization profile page.

Sender Groups Report 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 **Email > Reporting > Sender Groups**.

From the **Sender Group Report** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the .

Note You can generate a scheduled report for the Sender Group report page. See the .

Outgoing Destinations Page

The **Email > Reporting > Outgoing Destinations** page provides information about the domains that your organization sends mail to.

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?

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

Table 5: Details on the Email Reporting Outgoing Destinations Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Destination by Total Threat	The top destination domains of outgoing threat messages (spam, antivirus, etc.) sent by your organization. Total threat include threats that are spam or virus positive or that triggered a content filter.
Top Destination by Clean Messages	The top destination domains of clean outgoing messages sent by your organization.
Outgoing Destination 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. If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.

From the **Outgoing Destinations** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the Understanding the Email Reporting Pages, on page 5.

✎ **Note**   You can generate a scheduled report for the Outgoing Destinations page. See the Scheduling Email Reports, on page 45.

Outgoing Senders Page

The **Email > Reporting > Outgoing Senders** page provides information about the quantity and type of mail being sent from IP addresses and domains in your network.

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

- Which IP addresses are sending the most virus-positive, or spam-positive or malware email?
- Which IP addresses trigger content filters the most frequently?
- Which domains are sending the most mail?
- What are the total number of recipients that are being processed where a delivery was attempted.

To view the **Outgoing Senders** page, perform the following:

You can see the results of the Outgoing senders with two types of views:

- **Domain**: This view allows you to see the volume of mail that is being sent by each domain
- **IP address**: This view allows you to see which IP addresses are sending the most virus messages or triggering content filters.

The following list explains the various sections on the **Outgoing Senders** page for both views:

Table 6: Details on the Email Reporting Outgoing Sender Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Senders by Total Threat Messages	The top senders (by IP address or domain) of outgoing threat messages (spam, antivirus, etc.) in your organization.
Top Sender by Clean Messages	The top senders (by IP address or domain) of clean outgoing messages sent in your organization.
Sender Details	All details on the senders (by IP address or domain) of all outgoing messages sent by your organization. Details include detected spam, viruses, clean messages, etc. If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the DLP and Content Filter violations in this report, click a blue number link in the table.

> **Note** This page does not display information about message delivery. To track delivery information, such as the number of messages from a particular domain that were bounced, log in to the appropriate Email Security appliance and choose **Monitor > Delivery Status**.

From the **Outgoing Senders** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the Understanding the Email Reporting Pages, on page 5.

> **Note** You can generate a scheduled report for the **Outgoing Senders** page. See the Scheduling Email Reports, on page 45.

Internal Users Page

The **Email > Reporting > Internal Users** 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.

Use the Internal Users 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?

Table 7: Details on the Email Reporting Internal Users Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Users by Clean Incoming Messages	The top users by (by IP address or domain) of clean incoming messages sent in your organization.
Top Users by Clean Outgoing Messages	The top users (by IP address or domain) of clean outgoing messages sent in your organization.
User Mail Flow Details	The User Mail Flow Details interactive section breaks down the mail received and sent by each email address. You can sort the listing by clicking the column headers.
	To view details for a user, click the user name in the Internal User column. For more information, see the Internal User Details Page, on page 21.
	If your access privileges allow you to view Message Tracking data: To view Message Tracking details for the Content Filter violations in this report, click a blue number link in the table.

From the **Internal Users** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the Understanding the Email Reporting Pages, on page 5.

✎

Note You can generate a scheduled report for the Internal Users page. See the Scheduling Email Reports, on page 45.

Internal User Details Page

The Internal User detail page shows detailed information about a user, including a breakdown of incoming and outgoing messages showing the number of messages in each category (such as spam detected, virus detected, detected by Advanced Malware Protection, 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.

Click a content filter name to view detailed information for that filter on the corresponding content filter information page (see Content Filters Page, on page 24). You can use this method to view a list of all users who sent or received mail that matched the particular content filter.

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

Searching for a Specific Internal User

With the search form at the bottom of the Internal Users page and the Internal User detail 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 Incidents

The **Email > Reporting > DLP Incidents (DLP Incident Summary)** 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.

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

Table 8: Details on the Email Reporting DLP Incident Summary Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Incidents by Severity	The top DLP incidents listed by severity.
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	The DLP Incident Details table shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped.
	For more information on the DLP Incidents Details table, see the DLP Incidents Details Table, on page 23.

Click the name of a DLP policy to view detailed information on the DLP incidents detected by the policy. You can use this method to get a list of users who sent mail that contained sensitive data detected by the policy.

DLP Incidents Details Table

The DLP Incident Details table is an interactive table that shows the total number of DLP incidents per policy, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped. Click the column headings to sort the data.

To find out more information about any of the DLP Policies listed in this table, click the name of the DLP Policy and the DLP Policy Page appears.For more information, see DLP Policy Detail Page, on page 23.

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

DLP Policy Detail Page

If you click on a name of a DLP policy in the DLP Incident Details table, the resulting DLP Policy Detail page displays the DLP incidents data for the policy. The page displays graphs on the DLP Incidents based by Severity.

The page also includes an Incidents by Sender table at the bottom of the page that lists each internal user who has sent a message that violated the DLP policy. The table also shows the total number of DLP incidents for this policy per user, with a breakdown by severity level, and whether any of the messages were delivered in the clear, delivered encrypted, or dropped. You can use the Incidents by Sender table to find out which users may be sending your organization's sensitive data to people outside your network.

Clicking the sender name on the incident detail page opens up the Internal Users page. See the Internal Users Page, on page 20 for more information.

Message Filters

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

Geo Distribution

You can use the Geo Distribution report page to view:

- Top incoming mail connections based on country of origin in graphical format.

- Total incoming mail connections based on country of origin in tabular format.

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.

High Volume Mail

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.

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.

Related Topics

- Rate Limits Page , on page 34

Content Filters Page

The **Email > Reporting > Content Filters** 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 page, you can review your corporate policies on a per-content-filter or per-user basis and 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 more information about a specific filter, click the name of the filter. The Content Filter Details page appears. For more information on Content Filter details page, see the Content Filter Details Page, on page 24.

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

From the **Content Filters** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the Understanding the Email Reporting Pages, on page 5.

Note You can generate a scheduled report for the Content Filter page. See the Scheduling Email Reports, on page 45.

Content Filter Details Page

The Content Filter Detail page displays matches for the filter over time, as well as matches by internal user.

In the Matches by Internal User section, click the name of a user to view the detail page for the internal user (email address). For more information, see Internal User Details Page, on page 21.

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

DMARC Verification

The DMARC Verification 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 were taken on messages that failed DMARC verification?

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

Macro Detection

You can use the Macro Detection report page to view:

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

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

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.

Virus Types Page

The **Email > Reporting > Virus Types** 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.

Note Outbreak Filters can quarantine these types of virus-infected messages with no user intervention.

If you run multiple virus scanning engines, the Virus Types 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.

Table 9: Details on the Email Reporting Virus Types Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Top Incoming Virus Types Detected	This section displays a chart view of the viruses that have been sent to your network.
Top Outgoing Virus Types Detected	This section displays a chart view of the viruses that have been sent from your network.
Virus Types Detail	An interactive table that shows the details of each virus type.

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. Similarly, to see which IP addresses have sent virus positive email within your network, view the Outgoing Senders page and sort by virus positive messages.

From the **Virus Types** page you can also generate a PDF or export raw data to a CSV file. For information on printing or exporting a file, see the Understanding the Email Reporting Pages, on page 5.

Note   You can generate a scheduled report for the **Virus Types** page. See the Scheduling Email Reports, on page 45.

URL Filtering Page

- 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 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.

Web Interaction Tracking Page

- Web Interaction Tracking report modules are populated only if the Web Interaction Tracking feature is enabled on managed Email Security appliances.
- Web Interaction Tracking 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 Rewritten Malicious URLs clicked by End Users. Click on a URL to view a detailed report that contains the following information:

- A list of end users who clicked on the rewritten malicious URL.
- Date and time at which the URL was clicked.
- Whether the URL was rewritten by a policy or an outbreak filter.
- Action taken (allow, block, or unknown) when the rewritten URL was clicked. Note that, if a URL was rewritten by outbreak filter and the final verdict is unavailable, the status is shown as unknown.

> **Note**   Due to a limitation, status of all outbreak rewritten URLs are shown as unknown.

Top End Users who clicked on Rewritten Malicious URLs

Tracking Web Interaction Details. Includes the following information:

- A list of all the rewritten URLs (malicious and unmalicious). Click on a URL to view a detailed report.
- 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. Click a number to view a list of all messages that contain the clicked 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.

Forged Email Detection Page

- 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.

Advanced Malware Protection (File Reputation and File Analysis) Reporting Pages

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 Fire 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 Select **Management Appliance > Centralized Services > Security Appliances**.

Step 2 Scroll to the File Analysis section.

Step 3   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 4   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 5   Click **Group Now**.

Step 6   Configure the same group on each Email Security appliance that will share data with this appliance.

What to do next

Related Topics

(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).

File Reputation and File Analysis Report Pages

Report	Description
Advanced Malware Protection	Shows 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.
	Note From AsyncOS 9.6.5 onwards, Advanced Malware Protection report has been enhanced to display additional fields, graphs, and so on. The report displayed after the upgrade does not include the reporting data prior to the upgrade. To view the Advanced Malware Protection report prior to AsyncOS 9.6.5 upgrade, click on the hyperlink at the bottom of the page.
	The **Incoming Malware Files by Category** section shows the percentage of blacklisted file SHAs received from the AMP for Endpoints console that are categorised as **Custom Detection**.
	The threat name of a blacklisted file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report.
	You can click on the link in the More Details section of the report to view the file trajectory details of a blacklisted file SHA in the AMP for Endpoints console
	You can view the **Low Risk** verdict details in the Incoming Files Handed by AMP section of the report.

Report	Description
Advanced Malware Protection File Analysis	Displays 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.
	To view details on the server that analyzed a file, see Requirements for File Analysis Report Details , on page 28.
	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.
	Note From AsyncOS 9.6.5 onwards, File Analysis report has been enhanced to display additional fields, graphs, and so on. The report displayed after the upgrade does not include the reporting data prior to the upgrade. To view the File Analysis report prior to AsyncOS 9.6.5 upgrade, click on the hyperlink at the bottom of the page.
Advanced Malware Protection Verdict Updates	Because Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data provides more information.
	The AMP Verdict Updates report lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about this situation, see the documentation for your Email Security appliance.
	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.

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 **Security Services > File Reputation and Analysis** page.
Web Security appliance	Advanced Settings for File Analysis section on the **Security Services > Anti-Malware and Reputation** page.
Cisco Content Security Management appliance	At the bottom of the **Management Appliance > Centralized Services > Security Appliances** page.

Related Topics

Mailbox Auto Remediation

You can view the details of the mailbox remediation results using the Mailbox Auto Remediation report page. Use this report to view details such as:

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

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

- The recipient is not a valid Office 365 user or the recipient does not belong to the Office 365 domain account configured on your appliance.
- The message containing the attachment is no longer available in the mailbox, for example, the end user deleted the message.
- 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.

TLS Connections Page

The **Email > Reporting > TLS Connections** 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.

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?

Table 10: Details on the Email Reporting TLS Connections Page

Section	Description
Time Range (drop-down list)	A drop-down list that can range from a day to 90 days or a custom range. For more information on time ranges and customizing this for your needs, see the Choosing a Time Range for Reports.
Incoming TLS Connections Graph	The graph displays a view of incoming TLS encrypted and unencrypted connections over the last hour, day, or week depending on the time frame that you have selected.
Incoming TLS Connections Summary	This table displays the total volume of incoming messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed incoming TLS encrypted messages.
Incoming TLS Message Summary	This table displays a summary of the total volume of incoming messages.
Incoming TLS Connections Details	The 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 were successful or failed. You can also view the percentage of successful and failed connections for each domain.
Outgoing TLS Connections Graph	The graph displays a view of outgoing TLS encrypted and unencrypted connections over the last hour, day, or week depending on the time frame that you have selected.
Outgoing TLS Connections Summary	This table displays the total volume of outgoing messages, the volume of encrypted and unencrypted messages, and the volume of successful and failed outgoing TLS encrypted messages.
Outgoing TLS Message Summary	This table shows the total volume of outgoing messages
Outgoing TLS Connections Details	The 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 were successful or failed, and the last TLS status. You can also view the percentage of successful and failed connections for each domain.

Inbound SMTP Authentication Page

The Inbound SMTP Authentication 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.

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

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.

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.

The SMTP Authentication details table displays details for the domains whose users 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. You can use the links at the top of the page to display this information by domain name or domain IP address.

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.

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 , on page 24

Outbreak Filters Page

The **Email > Reporting > Outbreak Filters** 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.

Use the Outbreak Filters page to answer the following types of questions:

- How many messages are quarantined and by which Outbreak Filters rule?
- How much lead time has the Outbreak Filters feature been providing for virus outbreaks?
- How do the local outbreaks compare to the global outbreaks?
- How long do messages stay in the Outbreak Quarantine?
- Which potentially malicious URLs are most frequently seen?

The Threats By Type section shows the different types of threat messages received by the appliance. The Threat Summary section shows a breakdown of the messages by Virus, Phish, and Scam.

The Past Year Outbreak Summary lists global as well as local outbreaks over the past year, allowing you to compare local network trends to global trends. The listing of global outbreaks is a superset of all outbreaks, both viral and non-viral, whereas local outbreaks are limited to virus outbreaks that have affected your appliance. Local outbreak data does not include non-viral threats. Global outbreak data represents all outbreaks detected by the Threat Operations Center which exceeded the currently configured threshold for the outbreak quarantine. Local outbreak data represents all virus outbreaks detected on this appliance which exceeded the currently configured threshold for the outbreak quarantine. The Total Local Protection Time is always based on the difference between when each virus outbreak was detected by the Threat Operations Center and the release of an anti-virus signature by a major vendor. Note that not every global outbreak affects your appliance. A value of "--" indicates either a protection time does not exist, or the signature times were not available from the anti-virus vendors (some vendors may not report signature times). This does not indicate a protection time of zero, rather it means that the information required to calculate the protection time is not available.

The Quarantined Messages section summarizes Outbreak Filters quarantining, and is a useful gauge of how many potential threat messages Outbreak Filters are catching. Quarantined messages are counted at time of release. Typically, messages will be quarantined before anti-virus and anti-spam rules are available. When released, they will be scanned by the anti-virus and anti-spam software and determined to be positive or clean. Because of the dynamic nature of Outbreak tracking, the rule under which a message is quarantined (and even

the associated outbreak) may change while the message is in the quarantine. Counting the messages at the time of release (rather than the time of entry into the quarantine) avoids the confusion of having counts that increase and decrease.

The Threat Details listing displays information about specific outbreaks, including the threat category (virus, scam, or phishing), threat name, a description of the threat, and the number of messages identified. For virus outbreaks, the Past Year Virus Outbreaks include the Outbreak name and ID, time and date a virus outbreak was first seen globally, the protection time provided by Outbreak filters, and the number of quarantined messages. You can choose whether to view global or local outbreaks.

The First Seen Globally time is determined by the Threat Operations Center, based on data from the SenderBase, the world's largest email and web traffic monitoring network. The Protection Time is based on the difference between when each threat was detected by the Threat Operations Center and the release of an anti-virus signature by a major vendor.

A value of "--" indicates either a protection time does not exist, or the signature times were not available from the anti-virus vendors (some vendors may not report signature times). This does not indicate a protection time of zero. Rather, it means that the information required to calculate the protection time is not available.

Other modules on this page provide:

- 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.

- Severity of threats caught by Outbreak Filters.

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.

- Length of time messages spent in the Outbreak Quarantine.

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.

- The URLs 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.

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.

Note In order to correctly populate the tables on the Outbreak Filters reporting page, the appliance must be able to communicate with the Cisco update servers specified in Management Appliance > System Administration > Update Settings.

For more information, see the Outbreak Filters chapter.

Reporting of Graymail

Graymail statistics are reflected in the following reports:

Report	Contains the Following Graymail Data
Overview page > Incoming Mail Summary	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages.
Incoming Mail page > Top Senders by Graymail Messages	The top graymail senders.
Incoming Mail page > Incoming 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 IP addresses, domain names, or network owners.
Incoming Mail page > Incoming Mail Details > Sender Profile (drill down view)	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for a given IP address, domain name, or network owner.
Internal Users page > Top Users by Graymail	The top end users who receive graymail.
Internal Users page > User Mail Flow 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.
Internal Users page > User Mail Flow Details > Internal User (drill down view)	The number of incoming graymail messages under each graymail category (Marketing, Social, and Bulk) and the total number of graymail messages for a given user.

Related Topics

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.

System Capacity Page

The **Email > Reporting > System Capacity** 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 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, on page 39 and System Capacity – Outgoing Mail, on page 39.
- **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, on page 39.
- **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 , on page 40.

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, on page 40
- Memory Page Swapping, on page 40
- Resource Conservation Activity , on page 40

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 C170appliances). 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.

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 24.
- DLP Incident Summary—For information on what is included on this page, see the DLP Incidents , on page 22.
- 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 Email Reporting Overview Page, on page 11, and is limited to a group of specified domains. For information on what is included, see the Domain-Based Executive Summary Report, on page 43.
- Executive Summary—This report is based on the information from the Email Reporting Overview Page, on page 11. For information on what is included, see the Domain-Based Executive Summary Report, on page 43.
- Incoming Mail Summary — For information on what in included on this page, see the Incoming Mail Page, on page 15.

- Internal Users Summary—For information on what is included on this page, see the Internal Users Page, on page 20.
- Outbreak Filters—For information on what is included on this page, see the Outbreak Filters Page, on page 35.
- Outgoing Destinations—For information on what is included on this page, see the Outgoing Destinations Page, on page 19.
- Outgoing Mail Summary—For information on what is included on this page, see the Outgoing Senders Page, on page 19.
- Outgoing Senders: Domains —For information on what is included on this page, see the Outgoing Senders Page, on page 19.
- Sender Groups —For information on what is included on this page, see the Sender Groups Report Page, on page 18.
- System Capacity—For information on what is included on this page, see the System Capacity Page, on page 38.
- TLS Connections—For information on what is included on this page, see the TLS Connections Page, on page 33.
- Virus Types—For information on what is included on this page, see the Virus Types Page, on page 25.

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 and Tracking 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 , on page 48.

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, on page 43
- Executive Summary Report , on page 45

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) Choose **Email > Reporting > Scheduled Reports**.
b) Click **Add Scheduled Report**.

To create an on-demand report:

- 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 , on page 43.

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 and Tracking 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 Email Reporting Overview Page, on page 11. For more information on the Email Reporting Overview page, see Email Reporting Overview Page, on page 11.

Scheduled Reports Page

Scheduling Email Reports

You can schedule any of the reports listed in About Scheduled and On-Demand Email Reports , on page 41.

To manage report scheduling, see the following:

Adding Scheduled Reports

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

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

Step 2   Click **Add Scheduled Report**.

Step 3   Choose your report type.

For descriptions of the report types, see About Scheduled and On-Demand Email Reports , on page 41.

Note   - For information about the settings for a Domain-Based Executive Summary report, see Domain-Based Executive Summary Report, on page 43.

- 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 4   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 5   Choose the time range for the report from the **Time Range to Include** drop-down menu.

Step 6   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 7   Depending on the report, for Number of Rows, choose the amount of data to include.

Step 8   Depending on the report, choose the column by which to sort the report.

Step 9   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 10   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 11   Choose a language for the report.

For Asian languages, see important information at Printing and Exporting Reporting and Tracking Data.

Step 12   Click **Submit**.

Editing Scheduled Reports

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

Step 2   Click the report name link in the Report Title column that you want to modify.

Step 3   Modify the report settings.

Step 4   Submit and commit your changes.

Discontinuing Scheduled Reports

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

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

Step 2   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 3   Click **Delete**.

> **Note**   Any archived versions of deleted reports are *not* automatically deleted. To delete previously-generated reports, see Deleting Archived Reports, on page 49.

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 5, you can save PDFs or raw-data CSV files for the reports listed in About Scheduled and On-Demand Email Reports , on page 41 at any time, for the time frame that you specify.

To generate an on-demand report perform the following:

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

Step 2   Click **Generate Report Now**.

Step 3   Choose a report type.

For descriptions of the report types, see About Scheduled and On-Demand Email Reports , on page 41.

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.

> **Note**   For information about the settings for a Domain-Based Executive Summary report, see Domain-Based Executive Summary Report, on page 43.
>
> 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   From the Time Range to Include drop-down list, select a time range for the report data.

Note the custom time range option.

Step 6   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 7 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 8 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 9 Select a language for this report. For generating PDFs in Asian languages, see important information at Printing and Exporting Reporting and Tracking Data.

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

Archived Email Reports Page

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.

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

Step 2   To locate a particular report if the list is long, filter the list by choosing a report type from the **Show** menu, or click a column heading to sort by that column.

Step 3   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 , on page 48. However, you can manually delete unneeded reports.

To manually delete Archived reports, perform the following:

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

The Archived reports that are available are displayed.

Step 2   Select the checkbox for one or more reports to delete.

Step 3   Click **Delete**.

Step 4   To prevent future instances of scheduled reports from being generated, see Discontinuing Scheduled Reports , on page 47.

Troubleshooting Email Reports

- Outbreak Filters Reports Do Not Show Information Correctly , on page 49
- Message Tracking Results Do Not Match Report Results After Clicking a Link in a Report , on page 50
- Advanced Malware Protection Verdict Updates Report Results Differ , on page 50
- Issues Viewing File Analysis Report Details , on page 50

See also Troubleshooting All Reports.

Outbreak Filters Reports Do Not Show Information Correctly

Problem

Outbreak Filters reports do not show threat information correctly.

Solution

Verify that the appliance can communicate with the Cisco update servers specified in Management Appliance > System Administration > Update Settings.

Message Tracking Results Do Not Match Report Results After Clicking a Link in a Report

Problem

Message tracking results when drilling down from reports do not match expected results.

Solution

This can occur 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. Data for each feature (reporting, tracking) is captured only while that feature is enabled.

Related Topics

- Checking Message Tracking Data Availability

Advanced Malware Protection Verdict Updates Report Results Differ

Problem

A Web Security appliance and an Email Security appliance sent the same file for analysis, and the AMP Verdict Updates reports for Web and Email show different verdicts for that file.

Solution

This situation is temporary. Results will match once all verdict updates have been downloaded. Allow up to 30 minutes for this to occur.

Issues Viewing File Analysis Report Details

- File Analysis Report Details Are Not Available , on page 50
- Error When Viewing File Analysis Report Details, on page 50
- Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance , on page 51
- Logging of File Analysis-Related Errors , on page 51

File Analysis Report Details Are Not Available

Problem

File Analysis report details are not available.

Solution

See Requirements for File Analysis Report Details , on page 28.

Error When Viewing File Analysis Report Details

Problem

No cloud server configuration is available error appears when you attempt to view File Analysis report details.

Solution

Go to **Management Appliance > Centralized Services > Security Appliances** and add at least one Email Security appliance that has the File Analysis feature enabled.

Error When Viewing File Analysis Report Details with Private Cloud Cisco AMP Threat Grid Appliance

Problem

You see an API key, registration, or activation error when attempting to view File Analysis report details.

Solution

If you are using a private cloud (on-premises) Cisco AMP Threat Grid appliance for file analysis, see (On-Premises File Analysis) Activate the File Analysis Account , on page 29.

If your Threat Grid appliance hostname changes, you must repeat the process in the referenced procedure.

Logging of File Analysis-Related Errors

Registration and other File Analysis-related errors are logged in the GUI logs.

Total Graymail or Marketing Messages Appears To Be Incorrect

Problem

The count of Marketing, Social and Bulk mail exceeds the total number of graymail messages.

Solution

The total number of Marketing Messages includes marketing messages received both before and after upgrade to AsyncOS 9.5, but the total number of graymail messages includes only messages received after upgrade. See Reporting of Marketing Messages after Upgrade to AsyncOS 9.5 , on page 37.

Total Graymail or Marketing Messages Appears To Be Incorrect