Using Email Security Monitor

This chapter contains the following sections:

- Email Security Monitor Overview, on page 1
- Email Security Monitor Pages, on page 2
- Email Security Monitor Pages on the New Web Interface, on page 35
- Reporting Overview, on page 76
- Managing Reports, on page 78
- Troubleshooting Email Reports, on page 81

Email Security Monitor Overview

The Email Security Monitor feature collects data from every step in the email delivery process. The database identifies and records each email sender by IP address, while interfacing with the IP Reputation Service for real-time identity information. You can instantly report on any email sender's local mail flow history and show a profile that includes the sender's global record on the Internet. The Email Security Monitor feature allows your security team to "close the loop" on who is sending mail to your users, the amount of mail sent from and received by your users, and the effectiveness of your security policies.

This chapter explains how to:

- Access the Email Security Monitor feature to monitor inbound and outbound message flow.
- Make mail flow policy decisions (update allowed lists, blocked lists, and greylists) by querying for a sender's IP Reputation Score. You can query on network owners, domains, and even individual IP addresses.
- Report on mail flow, system status, and mail sent to and from your network.

For any given email sender for incoming mail, the Email Security Monitor database captures critical parameters such as:

- Message volume
- Connection history
- Accepted vs. rejected connections
- Acceptance rates and throttle limits
- Sender reputation filter matches
- Number of anti-spam messages for suspected spam and positively identified spam
- Number of virus-positive message detected by anti-virus scanning

See Managing Spam and Graymail for more information on Anti-Spam scanning and Anti-Virus for more information on anti-virus scanning.

The Email Security Monitor feature also captures information on which content filter a particular message triggers, including the internal user (email recipient) to or from which the message was sent.

The Email Security Monitor feature is available in the GUI only, and provides a view into your email traffic and the status of your email gateway (including quarantines, work queues, and outbreaks). The email gateway identifies when a sender falls outside of the normal traffic profile. Senders that do are highlighted in the interface, allowing you to take corrective action by assigning that sender to a sender group or refining the access profile of the sender; or, you can let AsyncOS's security services continue to react and respond. Outbound mail has a similar monitoring capability, providing you a view into the top domains in the mail queue and the status of receiving hosts (see Delivery Status Details Page, on page 17).

Note Information for messages present in the work queue when the email gateway is rebooted is not reported by the Email Security Monitor feature.

Related Topics

- Email Security Monitor and Centralized Management, on page 2

Email Security Monitor and Centralized Management

To view aggregated report data, deploy a Cisco Secure Email and Web Manager.

You cannot aggregate Email Security Monitor reports of clustered appliances. All reports are restricted to machine level. This means they cannot be run at the group or cluster levels — only on individual machines.

The same is true of the Archived Reports page — each machine in effect has its own archive. Thus, the "Generate Report" feature runs on the selected machine.

The Scheduled Reports page is not restricted to machine level; therefore, settings can be shared across multiple machines. Individual scheduled reports run at machine level just like interactive reports, so if you configure your scheduled reports at cluster level, every machine in the cluster will send its own report.

The "Preview This Report" button always runs against the login-host.

Email Security Monitor Pages

The Email Security Monitor feature is comprised of all the pages available on the Monitor menu except the Quarantines pages.

You use these pages in the GUI to monitor domains that are connecting to the appliance's listeners. You can monitor, sort, analyze, and classify the "mail flow" of your email gateway and differentiate between high-volume senders of legitimate mail and potential "spammers" (senders of high-volume, unsolicited commercial email) or virus senders. These pages can also help you troubleshoot inbound connections to the system (including important information such as IP Reputation score and most recent sender group match for domains).

These pages help you classify mail relative to the email gateway, and also relative to the services that exist beyond the scope of the gateway, such as the IP Reputation Service, the Anti-Spam scanning service, the Anti-Virus scanning security services, content filters, and Outbreak Filters.

You can generate a printer-friendly formatted .PDF version of any of the Email Security Monitor pages by clicking on the Printable PDF link at the top-right of the page. For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

You can export graphs and other data to CSV (comma separated values) format via the **Export** link.

The exported CSV data will display all message tracking and reporting data in GMT regardless of what is set on the email gateway. The purpose of the GMT time conversion is to allow data to be used independently from the email gateway or when referencing data from appliances in multiple time zones.

Note If you export localized CSV data, the headings may not render properly in some browsers. This occurs because some browsers may not use the correct character set for the localized text. To work around this problem, you can save the file to disk, and open the file using File > Open. When you open the file, select the character set to display the localized text.

For more information about automating the export of report data, see Retrieving CSV Data, on page 33).

List of Email Security Monitor Pages

- My Dashboard Page , on page 5
- Overview Page, on page 6
- Incoming Mail Page, on page 9
- Outgoing Destinations, on page 15
- Outgoing Senders, on page 15
- Delivery Status Page, on page 16
- Internal Users Page, on page 17
- DLP Incidents Page, on page 18
- Content Filters Page, on page 20
- DMARC Verification Page, on page 20
- Outbreak Filters Page, on page 21
- Virus Types Page, on page 23
- URL Filtering Page , on page 23
- Web Interaction Tracking Page, on page 24
- File Reputation and File Analysis Reports, on page 25
- TLS Connections Page, on page 25
- Inbound SMTP Authentication Page, on page 26

- Rate Limits Page , on page 27
- System Capacity Page, on page 27
- System Status Page, on page 30
- High Volume Mail Page, on page 32
- Message Filters Page, on page 32
- Geo Distribution Page , on page 16
- Safe Print Page , on page 33

Searching and Email Security Monitor

Many of the Email Security Monitor pages include a search form. You can search for different types of items:

- IP Address (IPv4 and IPv6)
- domain
- network owner
- internal users
- destination domain
- internal sender domain
- internal sender IP address
- outgoing domain deliver status

For domain, network owner, and internal user searches, choose whether to exactly match the search text or look for items starting with the entered text (for instance, starts with “ex” will match “example.com”).

For IPv4 address searches, the entered text is always interpreted as the beginning of up to four IP octets in dotted decimal format. For instance, “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, simply enter all four octets. IP address searches also support CIDR format (17.16.0.0/12).

For IPv6 address searches, AsyncOS supports the following formats:

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

All searches are bounded by the time range currently selected on the page.

Viewing Details of Messages Included in Reports

This functionality works only if reporting and tracking are both local (not centralized on a Cisco Secure Email and Web Manager.)

Procedure

Step 1 Click any blue number in a table on a report page.

(Not all tables have these links.)

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

Step 2 Scroll down to see the list.

What to do next

Related Topics

- Working with Message Tracking Search Results

My Dashboard Page

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

To	Do This
Add modules to your custom report page	1. Go to **Monitor > My Dashboard** and delete any sample modules that you do not need by clicking the [**X**] in the top right corner of the module. 2. Do one of the following: • Click the [**+**] button on a module in a report page under the Monitor menu to add it to your custom report. • Go to **Monitor > My Dashboard**, click the [**+**] button in one of the sections, then select the report module that you want to add. You may need to check the **+ Report Module in** each section to find the report that you are looking for. 3. Modules are added with default settings. If you add a module that you have customized (for example, by adding, deleting, or reordering columns), customize these modules again after adding them. Time range of the original module is not maintained. 4. If you add a chart that includes a separate legend (for example, a graph from the Overview page), add the legend separately. If necessary, drag and drop it into position beside the data it describes. Notes: • Some modules on some report pages are available only using one of the above methods. If you cannot add a module using one method, try the other method. • You can add each module only once; if you have already added a particular module to your report, the option to add it will not be available.
View your custom report page	1. Choose **Monitor > My Dashboard** 2. For reports in the Time Range section: The time range selected for all report pages applies to all modules on the My Dashboard page. Select the time range to view. Newly-added modules appear at the top of the relevant section.

To	Do This
Rearrange modules on your custom report page	Drag and drop modules into the desired location.
Delete modules from your custom report page	Click the [X] in the top right corner of the module.

Overview Page

The Overview page provides a synopsis of the message activity of your email gateway, including an overview of your quarantines and Outbreak Filters status (in the System Overview section of the page). The Overview page also includes graphs and detailed message counts for incoming and outgoing messages. You can use this page to monitor the flow of all mail into and out of your gateway.

The Overview page highlights how the email gateway is integrated with the IP Reputation Service for incoming mail (messages stopped by reputation filtering, for example). On the **Overview** page, you can:

- View a mail trend graph of all mail "flowing" into or out of your gateway.
- View a graph showing the number of attempted messages, messages stopped by IP reputation filtering, messages with invalid reipients, messages marked as spam, messages marked as virus positive, and clean messages, over time.
- View the summary of the system status and local quarantines.
- See current virus and non-virus outbreak information based on information available at the Threat Operations Center (TOC).

The Overview page is divided into two sections: System Overview and Incoming and Outgoing Mail graphs and summary.

Related Topics

- System Overview, on page 6
- Incoming and Outgoing Summary and Graph, on page 7
- Categorizing Email, on page 8
- How Messages are Categorized, on page 9

System Overview

The System Overview section of the Overview page serves as a system dashboard, providing details about the email gateway including system and work queue status, quarantine status, and outbreak activity.

Related Topics

- Status, on page 6
- System Quarantines, on page 7
- Virus Threat Level, on page 7

Status

This section provides an overview of the current state of the email gateway and inbound mail processing.

System Status: One of the following states:

- Online
- Resource Conservation
- Delivery Suspended
- Receiving Suspended
- Work Queue Paused
- Offline

See the Managing and Monitoring Using the CLI for more information.

Incoming Messages: The average rate of incoming mail per hour.

Work Queue: The number of messages awaiting processing in the work queue.

Click the System Status Details link to navigate to the System Status page.

System Quarantines

This section displays information about the top three quarantines by disk usage on the email gateway, including the name of the quarantine, how full the quarantine is (disk space), and the number of messages currently in the quarantine.

Click the Local Quarantines link to navigate to the Local Quarantines page.

Virus Threat Level

This section shows the Outbreak status as reported by the Threat Operations Center (TOC). Also shown is the status of the Outbreak quarantine, including how full it is (disk space) and the number of messages in the quarantine. The Outbreak quarantine is only displayed if you have enabled the Outbreak Filters feature on your email gateway.

Note In order for the Threat Level indicator to function, you need to have port 80 open on your firewall to "`downloads.ironport.com`." Alternatively, if you have specified a local update server, the Threat Level indicator will attempt to use that address. The Threat Level indicator will also update correctly if you have configured a proxy for downloads via the Service Updates page. For more information, see Service Updates.

Click the Outbreak Details link to view the external Threat Operations Center web site. Note that in order for this link to work, your email gateway must be able to access the Internet. Note that the Separate Window icon indicates that a link will open in a separate window when clicked. You may need to configure your browser's pop-up blocker settings to allow these windows.

Incoming and Outgoing Summary and Graph

The Incoming and Outgoing summary sections provide access to real-time activity of all mail activity on your system and is comprised of the Incoming and Outgoing Mail Graphs and Mail Summaries. You can select the time frame on which to report via the Time Range menu. The time range you select is used throughout all of the Email Security Monitor pages. The explanations of each type or category of message are below (see Categorizing Email, on page 8).

While the mail trend graph displays a visual representation of the mail flow, the summary table provides a numeric breakdown of the same information. The summary table includes the percentage and actual number of each type of message, including the total number of attempted, threat, and clean messages.

The outgoing graph and summary show similar information for outbound mail.

Related Topics

- Notes on Counting Messages in Email Security Monitor, on page 8

Notes on Counting Messages in Email Security Monitor

The method Email Security Monitor uses to count incoming mail depends on the number of recipients per message. For example, an incoming message from example.com sent to three recipients would count as three messages coming from that sender.

Because messages blocked by sender reputation filtering do not actually enter the work queue, the email gateway 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 was determined by Cisco and based upon research of a large sampling of existing customer data.

Categorizing Email

Messages reported in the Overview and Incoming Mail pages are categorized as follows:

- **Stopped by IP Reputation Filtering**: All connections blocked by HAT policies multiplied by a fixed multiplier (see Notes on Counting Messages in Email Security Monitor, on page 8) plus all recipients blocked by recipient throttling.
- **Stopped by Domain Reputation Filtering**: The total count of messages blocked based on the reputation verdict of the sender domain.
- **Invalid Recipient**s: All 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 and also those that were both spam and virus positive.
- **Virus Messages Detected**: The total count and percentage of messages detected as virus positive and not also spam.

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.

- **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.
- **Stopped by DMARC**: The total count of messages that were stopped after DMARC verification.

Note The email gateway displays the total count of 'Stopped by DMARC' messages based on the ‘Failed - Rejected,’ ‘Failed - Quarantined,’ and ‘Failed - No Action’ results.

- **S/MIME Verification/Decryption Failed**: The total count of messages that failed S/MIME verification, decryption, or both.

- **S/MIME Verification/Decryption Successful**: The total count of messages that were successfully verified, decrypted, or decrypted and verified using S/MIME.
- **Clean Messages**: Mail that is accepted and is 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.
- Graymail Messages
  - **Marketing Messages**: The total count of advertising messages sent by professional marketing groups, for example Amazon.com.
  - **Social Networking Messages**: The total count of notification messages from social networks, dating websites, forums, and so on. Examples include LinkedIn and CNET forums.
  - **Bulk Messages**: The total count of advertising messages sent by unrecognized marketing groups, for example, TechTarget, a technology media company.

  Click on the number corresponding to any of the above mentioned graymail categories to view a list of messages belonging to that category using Message Tracking.

Note Messages that match a *message* filter and are not dropped or bounced by the filter are treated as clean. Messages dropped or bounced by a message filter are not counted in the totals.

How Messages are Categorized

As messages proceed through the email pipeline, they can apply to multiple categories. For example, a message can be marked as spam, virus, or malware positive, and it can also match a content filter. The various verdicts follow these rules of precedence: Outbreak Filters quarantining (in this case the message is not counted until it is released from the quarantine and again processed through the work queue), followed by spam positive, virus positive, malware positive, and matching a content filter.

For example, if a message is marked as spam positive, and the anti-spam settings are set to drop spam positive messages, the message is dropped and the spam counter is incremented. Further, if the anti-spam settings are set to let the spam positive message continue on in the 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, virus, or malware positive.

Incoming Mail Page

The **Incoming Mail** page provides a mechanism to report on the real-time information being collected by the Email Security Monitor feature for all remote hosts connecting to your email gateway. This allows you to gather more information about an IP address, domain, and organization (network owner) sending mail to you. You can perform a Sender Profile search on IP addresses, domains, or organizations that have sent mail to you.

The Incoming Mail page has three views: Domain, IP Address, and Network Owner and provides a snapshot of the remote hosts connecting to the system in the context of the selected view.

It displays a table (Incoming Mail Details) of the top domains (or IP addresses, or network owners, depending on the view) that have sent mail to all public listeners configured on the email gateway. You can monitor the

flow of all mail into your gateway. You can click on any domain/IP/network owner to drill down to access details about this sender on a Sender Profile page (this is an Incoming Mail page, specific to the domain/IP/network owner you clicked on).

Not all available columns are displayed by default. You can show a different set of information by clicking the Columns link below the table. For example, you can show the "Detected by Advanced Malware Protection" column, which is hidden by default.

The Incoming Mail page extends to include a group of pages (Incoming Mail, Sender Profiles, and the Sender Group Report). From the **Incoming Mail** pages, you can:

- Perform a search on IP addresses, domains, or organizations (network owners) that have sent mail to you.
- View the Sender Groups report to see connections via a specific sender group and mail flow policy actions. See Sender Groups Report, on page 14 for more information.
- See detailed statistics on senders which have sent mail to you, including the number of attempted messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, graymail, and so on).
- 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 IP Reputation service to drill down on and examine the relationship between specific IP addresses, domains, and organizations to obtain more information about a sender.
- Drill down on specific senders to obtain more information about a sender from the IP Reputation Service, including a sender's IP Reputation Score and which sender group the domain matched most recently. Add senders to sender groups.
- Drill down on a specific sender who sent a high volume of spam or virus email, as determined by the anti-spam or anti-virus security services.
- Once you have gathered information on a domain, you can add the IP address, domain, or organization to an existing sender group (if necessary) by clicking "Add to Sender Group" from a domain, IP address, or network owner profile page. See Configuring the Gateway to Receive Email.

Related Topics

- Incoming Mail, on page 10
- Incoming Mail Details Listing, on page 11
- Reporting Pages Populated with Data: Sender Profile Pages, on page 13
- Sender Groups Report, on page 14

Incoming Mail

The Incoming Mail page provides access to real-time activity of all public listeners configured on your system and is comprised of two main sections: the mail trend graphs summarizing the top sender domains received (by total threat messages, total clean messages, and total graymail messages) and the Incoming Mail Details listing.

See Incoming Mail Details Listing, on page 11 for an explanation of the data included in the Incoming Mail Details listing.

Related Topics

Notes on Time Ranges in the Mail Trend Graph, on page 11

Notes on Time Ranges in the Mail Trend Graph

The Email Security Monitor feature constantly records data about the mail flowing into your gateway. The data are updated every 60 seconds, but the display shown is delayed by 120 seconds behind the current system time. You can specify the time range to include in the results shown. Because the data is monitored in real time, information is periodically updated and summarized in the database.

Choose from the time range options in the following table.

Table 1: Time Ranges Available in the Email Security Monitor Feature

This time range selected in the GUI	...is defined as:
Hour	the last 60 minutes + up to 5 minutes
Day	the last 24 hours + the last 60 minutes
Week	the last 7 days + the elapsed hours of the current day
30 days	the last 30 days + the elapsed hours of the current day
90 days	the last 90 days + the elapsed hours of the current day
Yesterday	00:00 to 23:59 (midnight to 11:59 PM)
Previous Calendar Month	00:00 of the first day of the month to 23:59 of the last day of the month
Custom Range	the range enclosed by the start date and hour and the end date and hour that you specify

The time range options that you see will differ if you have enabled Centralized Reporting. For details, see information about Centralized Reporting Mode in Centralizing Services on a Cisco Secure Email and Web Manager (M-Series)

Incoming Mail Details Listing

The top senders which have connected to public listeners of the email gateway are listed in the External Domains Received listing table at the bottom of the Incoming Mail page, based on the view selected. Click the column headings to sort the data. See Categorizing Email, on page 8 for an explanation of the various categories.

The system acquires and verifies the validity of the remote host's IP address (that is, the domain) by performing a *double DNS lookup* . For more information about double DNS lookups and sender verification, see Configuring the Gateway to Receive Email.

The Sender Detail listing has two views, Summary and All.

The default Sender Detail view shows the total number of attempted messages for each sender, and includes a breakdown by category (the same categories as the Incoming Mail Summary graph on the Overview page.

The value for Stopped by IP 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 email gateway 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"; in other words, at least this many messages were stopped.

Note The Stopped by IP 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 ever limited due to load.

Additional columns that you can display are:

Connections Rejected: All connections blocked by HAT policies. When the email gateway 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

Stopped by Domain Reputation Filtering: All messages blocked by the reputation verdict of the sender domain.

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.

Detected by Advanced Malware Protection: Messages with attachments that were found to be malicious by file reputation filtering. This value does not include verdict updates or files found to be malicious by file analysis.

Total Threat: Total number of threat messages (stopped by sender reputation, stopped as invalid recipient, spam, plus virus).

Show or hide columns by clicking the Column link at the bottom of the table.

Sort the listing by clicking the column header links. A small triangle beside the column header indicates the column by which the data is currently sorted.

Related Topics

- "No Domain Information", on page 12
- Querying for More Information, on page 12

"No Domain Information"

Domains which have connected to the email gateway and could not be verified with a double-DNS lookup are automatically grouped into the special domain "No Domain Information." You can control how these types of unverified hosts are managed via Sender Verification. See Configuring the Gateway to Receive Email.

You can select the number of senders to show in the listing via the Items Displayed menu.

Querying for More Information

For senders listed in the Email Security Monitor table, click the sender (or "No Domain Information" link) to drill down for more information on the particular sender. The results are displayed on a Sender Profile page which includes real-time information from the IP Reputation Service. From the Sender Profile page, you can

drill down for more information on specific IP addresses or network owners (see Reporting Pages Populated with Data: Sender Profile Pages, on page 13).

You can also view another report, the Sender Groups report, by clicking the Sender Groups report link at the bottom of the Incoming Mail page. For more information about Sender Groups reports, see Sender Groups Report, on page 14.

Reporting Pages Populated with Data: Sender Profile Pages

If you clicked a sender in the Incoming Mail Details table on an Incoming Mail page, the resulting *Sender Profile page* is listed with data for the particular IP address, domain, or organization (network owner). Sender Profile pages show detailed information for the sender. You can access a Sender Profile page for any network owner, domain, or IP address by clicking on the specified item in the Incoming Mail or other Sender Profile pages. Network owners are entities that contain domains; domains are entities that contain IP addresses. For more information on this relationship and how it relates to the IP Reputation Service, see Configuring the Gateway to Receive Email.

The Sender Profile pages displayed for IP addresses, network owners, and domains vary slightly. For each, the page contains a graph and summary table for incoming mail from this sender. Below the graph is a table listing domains or IP addresses associated with the sender (the Sender Profile page for individual IP addresses does not contain the detailed listing) and 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 IP 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 (approximately 10 billion messages/day). 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)
  - IP 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 the "More from SenderBase" link to see a page with all information supplied by the IP Reputation Service.

- The **Mail Flow Statistics** information, with Email Security Monitor information collected about the sender over the time range that you specify.
- **Details** about the domains and IP addresses controlled by this network owner are displayed on network owner profile pages. Details about the IP addresses in the domain are displayed on domain pages.

  From a domain profile page, you can drill down to a specific IP address, or drill up to view an organization profile page. You can also display the DNS Verified status, IP Reputation Score, and Last Sender Group for each sender address in the IP Addresses table by clicking the Columns link at the bottom of that table. You can also hide any columns in that table.

  From a network owner profile page, you can display information such as Connections Rejected, Connections Accepted, Stopped by Recipient Throttling, and Detected by Advanced Malware Protection for each domain in the Domains table by clicking the Columns link at the bottom of that table. You can also hide any columns in that table.

  If you are an administrator of the system, on each of these pages, you can choose to add the network owner, domain, or IP address to a sender group by clicking the check box for the entity (if necessary) and then clicking Add to Sender Group.

  You can also add a sender to a sender group by clicking the **Add to Sender Group** link below the Sender Group Information in the Current Information table for the sender and clicking Add to Sender Group. For more information about adding senders to sender groups, see Configuring the Gateway to Receive Email. Of course, you do not have to make any changes — you can let the security services handle incoming mail.

Related Topics

- Sender Profile Search, on page 14

Sender Profile Search

Type an IP address, a domain, or an organization name in the Quick Search box to search for a specific sender.

A Sender Profile page is displayed with the information for sender. See Reporting Pages Populated with Data: Sender Profile Pages, on page 13.

Sender Groups Report

The Sender Groups report 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 Configuring the Gateway to Receive Email.

Sender Domain Reputation Page

You can use the Sender Domain Reputation report page to view:

- Incoming messages based on the verdict received from the SDR service in graphical format.
- Summary of incoming messages based on the threat category and verdict received from the SDR service in tabular format.
- Incoming messages based on the threat category received from the SDR service in graphical format.

Note Only the messages whose SDR verdict is 'untrusted' or 'questionable' are classified under the SDR threat category, such as, 'spam,' 'malicious,' and so on.

- Summary of incoming messages based on the threat category received from the SDR service in tabular format.

In the Summary of Incoming Messages handled by SDR section, you can click on the number of messages corresponding to a particular verdict to view the related messages in Message Tracking.

Outgoing Destinations

The Outgoing Destinations page provides information about the domains your company sends mail to. The page consists of two section. The top half of the page consists of graphs depicting the top destinations by outgoing threat messages and top destinations by outgoing clean messages on the top half of the page. The bottom half of the page displays a chart showing all the columns sorted by total recipients (default setting).

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

The Outgoing Destinations page can be used to answer the following types of questions:

- What domains is the email gateway 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 server?

Outgoing Senders

The Outgoing Senders page provides information about the quantity and type of mail being sent from IP addresses and domains in your network. You can view the results by domain or IP address when you view this page. You might want to view the results by domain if you want to see what volume of mail is being sent by each domain, or you might want to view the results by IP address if you want see which IP addresses are sending the most virus messages or triggering content filters.

The page consists of two sections. On the left side of the page is a graph depicting the top senders by total threat messages. Total threat messages include messages that are spam-positive, virus-positive, malware or triggered a content filter. On the right side of the page is a graph displaying top senders by clean messages on the top half of the page. The bottom half of the page displays a chart showing all the columns sorted by total messages (default setting).

Note This page does not display information about message delivery. Delivery information, such as how many messages from a particular domain were bounced can be tracked using the Delivery Status page.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

The Outgoing Senders page can be used to answer the following types of questions:

- Which IP addresses are sending the most virus-positive, spam-positive or malware email?
- Which IP addresses trigger content filters the most frequently?
- Which domains are sending the most mail?

Geo Distribution Page

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.

You can click on the number of incoming mail connections of a specific geolocation to view the related messages in Message Tracking.

The "Total Messages" column only displays those messages that are accepted at the SMTP connection level.

Note During report generation:

- If one or more incoming mail connections are detected as private IP address, the incoming mail connections are categorized as “Private IP Addresses” in the report.
- If one or more incoming mail connections are detected as not a valid IP Reputation score, the incoming mail connections are categorized as ‘No Country Info’ in the report.

Delivery Status Page

If you suspect delivery problems to a specific recipient domain or if you want to gather information on a Virtual Gateway address, the Monitor > Delivery Status Page provides monitoring information about email operations relating to a specific recipient domain.

The **Delivery Status Page** displays the same information as the tophosts command within the CLI. (For more information, see “Determining the Make-up of the Email Queue” in Managing and Monitoring Using the CLI)

This 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.

- To search for a specific domain, type the name of the domain in the Domain Name: field and click **Search**.

- To drill down on a domain shown, click the domain name link.

The results are shown in an Delivery Status Details Page.

Note Any activity for a recipient domain results in that domain being "active" and thus present in the overview page. For example, if mail remains in the outbound queue due to delivery problems, that recipient domain continues to be listed in the outgoing mail overview.

Related Topics

- Retrying Delivery, on page 17
- Delivery Status Details Page, on page 17

Retrying Delivery

Messages that are scheduled for later delivery can be immediately retried by clicking **Retry All Delivery**. Retry All Delivery allows you to reschedule messages in the queue for immediate delivery. All domains that are marked as "down" and any scheduled or soft bounced messages are queued for immediate delivery.

To retry delivery to a specific destination domain, click the domain name link. On the Delivery Status Details page, click **Retry Delivery**.

You can also use the delivernow command in the CLI to reschedule messages for immediate delivery. For more information, see Scheduling Email for Immediate Delivery.

Delivery Status Details Page

Use the **Delivery Status Details Page** to look up statistics on a specific recipient domain. This page displays the same information as the **`hoststatus`** command within the CLI: Mail Status, Counters and Gauges. (For more information, see Managing and Monitoring Using the CLI) To search for a specific domain, type the name of the domain in the Domain Name: field and click **Search**. Virtual Gateway address information appears if you are using the **`altsrchost`** feature.

Internal Users Page

The Internal Users page provides information about the mail sent and received by your internal users, *per email address* (a single user may have multiple email addresses listed — the email addresses are not combined in the report).

The page consists of two sections:

- Graphs depicting the top users by clean incoming and outgoing messages and top users receiving graymail.
- User mail flow details

You can select a time range on which to report (hour, day, week, or month). As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link. You can also display hidden table columns or hide default columns by clicking the Columns link below the table.

The User Mail Flow Details listing breaks down the mail received and sent by each email address into clean, spam (incoming only), virus, malware, content filter matches, and graymail (incoming only). You can sort the listing by clicking on the column headers.

Using the Internal Users report, you can answer these kinds of questions:

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

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.

Note that some outbound mail (like bounces) have a null sender. They are counted under outbound and "unknown."

Click on an internal user to view the Internal User detail page for that user.

Click the Columns link below the table to show columns that are hidden by default, such as the Incoming Detected by Advanced Malware Protection column or Outgoing Detected by Advanced Malware Protection column.

Related Topics

- Internal User Details, on page 18
- Searching for a Specific Internal User, on page 18

Internal User Details

The Internal User detail page shows detailed information about the specified user, including a breakdown of incoming and outgoing messages showing the number of messages in each category (spam detected, virus detected, detected by Advanced Malware Protection, stopped by content filter, graymail detected, and clean). Optionally, for incoming messages, you can click the Columns link below the table to show the Incoming Detected by Advanced Malware Protection column. This value reflects the number messages that contained attachments that were determined by file reputation filtering to be malicious. It does not include verdict updates or files found to be malicious by file analysis. Incoming and outgoing content filter and DLP policy matches are also shown.

Click on a content filter name to view detailed information for that filter in the corresponding content filter information page (see Content Filters Page, on page 20). You can use this method to get a list of users who also sent or received mail that matched that particular content filter.

Searching for a Specific Internal User

You can search for a specific internal user (email address) via the search form at the bottom of the Internal Users page and the Internal User detail page. Choose whether to exactly match the search text or look for items starting with the entered text (for instance, starts with "ex" will match "example.com").

DLP Incidents Page

The DLP Incidents page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The email gateway 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 Incidents 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 Incidents page is comprised of two main sections:

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

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link or PDF format by clicking the **Printable (PDF)** link. For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

Click on 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.

Related Topics

- DLP Incidents Details, on page 19
- DLP Policy Detail Page, on page 19

DLP Incidents Details

The DLP policies currently enabled in the email gateway's outgoing mail policies are listed in the DLP Incidents Details table at the bottom of the DLP Incidents page. Click on the name of a DLP policy to view more detailed information.

The DLP Incidents Details table shows the total number of DLP incidents per policy, with a breakdown by severity level. The severity level also includes the number of bounced messages and the number of messages delivered in the clear, delivered encrypted, or dropped. Click on the column headings to sort the data.

DLP Policy Detail Page

If you clicked the name of a DLP policy in the DLP Incidents 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 on severity.

The page also includes an Incidents by Sender listing at the bottom of the page that lists each internal user who has sent a message that violated the DLP policy. The listing 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 listing to find out which users may be sending your organization’s sensitive data to people outside your network.

Clicking on the sender name opens up the Internal Users page. See Internal Users Page, on page 17 for more information.

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) in two forms: a bar chart and a listing. Using the Content Filters page, you can review your corporate policies on a per-content filter or per-user basis and answer questions like:

- Which content filter is being triggered the most by incoming or outgoing mail?
- Who are the top users sending or receiving mail that is triggering a particular content filter?

You can click the name of the content filter in the listing to view more information about that filter on the Content Filter detail page.

Related Topics

- Content Filter Details, on page 20

Content Filter Details

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

In the Matches by Internal User section, you can click the name of a user to view that internal user's (email address) Internal User details page (see Internal User Details, on page 18).

DMARC Verification Page

The DMARC Verification page shows the top domains that failed DMARC verification and the details of actions AsyncOS performed on the messages that failed DMARC verification. You can use this report to fine-tune your DMARC settings and answer these kinds of questions:

- Which are the domains that sent maximum number of messages that are not DMARC compliant?
- For each domain, what are the actions AsyncOS performed on the messages that failed DMARC verification?

The DMARC Verification page contains:

- A bar chart showing top domains by DMARC verification failures.
- Tabular representation of the following, for each domain:
  - Number of messages that were rejected, quarantined, or accepted without taking any action. Click on the number to view a list of messages under the selected category.
  - Number messages that passed DMARC verification.
  - Total number of DMARC verification attempts.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link or PDF format by clicking the **Printable (PDF)** link.

Macro Detection Page

You can use the Macro Detection report page to view:

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

- 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.

External Threat Feeds Page

You can use the External Threat Feeds report page to view:

- Top ETF sources used to detect threats in messages in graphical format
- Summary of ETF sources used to detect threats in messages in tabular format.
- Top IOCs that matched threats detected in messages in graphical format.
- Top ETF sources used to filter malicious incoming mail connections in graphical format.
- Summary of ETF sources used to filter malicious incoming mail connections in tabular format.

In the 'Summary of External Threat Feed Sources' section:

- You can click on the number of messages for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular threat feed source to view the distribution of the ETF source based on the IOCs.

In the 'Summary of Indicator of Compromise (IOC) Matches' section:

- You can click on the number of IOCs for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular IOC to view the distribution of the IOC based on the ETF sources.

Outbreak Filters Page

The Outbreak Filters page shows the current status and configuration of Outbreak Filters on your email gateway as well as 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.

The Threats By Type section shows the different types of threat messages received by the email gateway.

The Threat Summary section shows a breakdown of the threat messages by Malware, Phish, Scam, and Virus. Click on the number to view a list of all the messages that are included in that number using Message Tracking.

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 email gateway. 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 email gateway. 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 select either global or local outbreaks as well as the number of messages to display via the menu on the left. You can sort the listing by clicking on the column headers. Click on the number to view a list of all the messages that are included in that number using Message Tracking.

The First Seen Globally time is determined by the Threat Operations Center, based on data from 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.

Hit Messages from Incoming Messages section shows the percentage and number of viral attachment, other threats (non-viral), and clean incoming messages.

Hit Messages by Threat Level section shows the percentage and number of incoming threat messages (viral and non-viral) based on threat levels (Level 1 through 5).

Messages resided in Outbreak Quarantine section shows the number of threat messages resided in the Outbreak Quarantine based on the duration.

Top URL's Rewritten section shows the list of top 10 URLs that were rewritten based on the number of occurrences. Use the Items Displayed drop-down to view more rewritten URLs. Click on the number to view a list of all the messages that contain the selected rewritten URL on the Message Tracking page.

Using the Outbreak Filters page, you can answer questions like:

- How many messages are being quarantined and what type of threats were they?

- How much lead time has the Outbreak Filter feature been providing for virus outbreaks?
- How do my local virus outbreaks compare to the global outbreaks?

Virus Types Page

The Virus Types page provides an overview of the viruses entering and being sent from your network. The Virus Types page displays the viruses that have been detected by the virus scanning engines running on your email gateway. You might want to use this report to take a specific action against a particular virus. For example, if you see that you are receiving a high volume of a viruses known to be embedded in PDF files, you might want to create a filter action to quarantine messages with PDF attachments.

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

The Virus Types page gives you an overview of the viruses entering or being sent from or to your network. The Top Incoming Virus Detected section shows a chart view of the viruses that have been sent to your network in descending order. The Top Outgoing Virus Detected section shows a chart view of the viruses that have been sent from your network in descending order.

Note To see which hosts sent virus-infected messages to your network, you can 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, you can view the Outgoing Senders page and sort by virus-positive messages.

The VirusTypes Details listing displays information about specific viruses, including the infected incoming and outgoing messages, and the total infected messages. The details listing for infected incoming messages displays the name of the virus and the number of incoming messages infected with this virus. Similarly, the outgoing messages displays the name of the virus and the number of outgoing messages infected with the virus. You can sort the Virus Type details by Incoming Messages, Outgoing Messages, or Total Infected Messages.

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 URL reputation level. For messages with multiple URLs, the statistics reflect the lowest reputation of any URL in the message.
- URLs in the global allowed list configured at Security Services > URL Filtering are not included in reports.

  URLs in allowed lists 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.
- Web Interaction Tracking report modules are not updated in real-time and are refreshed every 30 minutes. Also, after clicking a rewritten URL, it may take up to two hours for the Web Interaction Tracking report to report this event.
- Web Interaction Tracking report is not updated in real-time. After clicking a cloud re-directed rewritten URL, it may take up to two hours for the Web Interaction Tracking report to report this event.
- Web Interaction Tracking reports are available for incoming and outgoing messages.
- Only cloud re-directed 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.

Top End Users who clicked on Rewritten Malicious URLs

Web Interaction Tracking Details. Includes the following information:

- A list of all the cloud re-directed rewritten URLs (malicious and unmalicious). Click on a URL to view a detailed report.
- Action taken (allow, block, or unknown) when a cloud re-directed rewritten URL was clicked.

For the data to show up, perform the following:

- Choose **Incoming Mail Policies > Outbreak Filters** to configure an outbreak filter and enable message modification and URL rewriting.
- Configure a content filter with the "**Redirect to Cisco Security Proxy**" action.

Note that, 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 on a number to view a list of all the messages that contain the clicked URL.
- While using Web Interaction Tracking reports, keep in mind the following limitations:

- 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 of the original recipient is incremented even if the notified user clicks on the rewritten URLs.
- If you are sending a copy of quarantined messages containing rewritten URLs to a user (for example, an administrator) using web interface, the web interaction tracking data of the original recipient is incremented even if the user (to whom the copy of the messages were sent) clicks on the rewritten URLs.
- At any point, if you plan to modify the time of your email gateway, make sure that the system time is synchronized with Coordinated Universal Time (UTC).

Forged Email Matches Report

See Monitoring Forged Email Detection Results.

File Reputation and File Analysis Reports

For the following reports, see File Reputation and File Analysis Reporting and Tracking:

- Advanced Malware Protection
- File Analysis
- AMP Verdict Updates

Mailbox Auto Remediation Report

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

- Remedial actions taken on messages
- The filenames associated with a SHA-256 hash
- A list of profile names defined for the recipients for whom the mailbox remediation was successful or unsuccessful
- Reason for the remediation failure
- No profile mapped to the domain

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

For more information, see Remediating Messages in Mailboxes

TLS Connections Page

The TLS Connections pages 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 use TLS?
- What partners do I have successful TLS connections with?
- What partners do I have unsuccessful TLS connections with?

- What partners do I have successful TLS connections with DANE support?
- What partners do I have unsuccessful TLS connections with DANE support?
- What partners have issue with their TLS certificates?
- What percent of overall mail with a partner uses TLS?
- What percent of outgoing TLS connections with DANE support are successful?
- What percent of outgoing connections with DANE support are unsuccessful?

The TLS Connections page is divided into a section for incoming connections and a section for outgoing connections. Each section includes a graph, summaries, and a table with details.

The graph displays a view of incoming or outgoing TLS-encrypted and non-encrypted connections over the time range you specify. The graph displays the total volume of messages, the volume of encrypted and unencrypted messages, the volume of successful and failed TLS encrypted messages and the volume of successful and failed DANE connections. The graphs distinguish between connections in which TLS was required and connections in which TLS was merely preferred.

The table displays details for domains sending or receiving encrypted messages. For each domain, you can view the number of required and preferred TLS connections that were successful and that failed, the total number of TLS connections attempted (whether successful or failed), the total number of unencrypted connections, and the total number of unencrypted connections, and the total number of DANE connections (depending on whether successful or failed). You can also view the percentage of all connections in which TLS was attempted, and the total number of encrypted messages sent successfully, regardless of whether TLS was preferred or required. You can show or hide columns by clicking the Columns link at the bottom of this table.

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 gateway and users' mail clients. If the email gateway 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 email gateway 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 email gateway 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 gateways 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 gateway 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.

To configure rate limiting by envelope sender or modify the existing rate limit, see Defining Rules for Incoming Messages Using a Mail Flow Policy.

System Capacity Page

The System Capacity page provides a detailed representation of the system load, including messages in the work queue, average time spent 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 an email gateway is exceeding recommended capacity and configuration optimization or additional email gateways are needed.
- Identify historical trends in system behavior which point to upcoming capacity issues.

- Identify which part of the system is using the most resources to assist with troubleshooting.

It is important to monitor your email gateway to ensure that your capacity is appropriate to your message volumes. Over time, volume will inevitably rise and appropriate monitoring will ensure that additional capacity or configuration changes can be applied proactively. The most effective way to monitor system capacity is to track overall volume, messages in the work queue and incidents of Resource Conservation Mode.

- **Volume**: It is important to have an understanding of 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 29 and System Capacity-Outgoing Mail, on page 29.
- **Work Queue**: The work queue is designed to work as a "shock absorber"-- absorbing and filtering spam attacks and processing unusual increases in ham messages. However, the work queue is also the best indicator of a system under stress, prolonged and frequent work queue backups may indicate a capacity problem. You can use the WorkQueue page to track the average time messages spend in the work queue and the activity in your work queue. For more information, see System Capacity- Workqueue, on page 28.
- **Resource Conservation Mode**: When an email gateway becomes overloaded, it will enter "Resource Conservation Mode" (RCM) and send a CRITICAL system alert. This is designed to protect the device and allow it to process any backlog of messages. Your email gateway 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 System Capacity-System Load, on page 29.

Related Topics

- System Capacity- Workqueue, on page 28
- System Capacity- Incoming Mail, on page 29
- System Capacity-Outgoing Mail, on page 29
- System Capacity-System Load, on page 29
- Note about Memory Page Swapping, on page 30
- System Capacity- All, on page 30

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.

For instructions to change the work queue threshold level, see Setting Thresholds for System Health Parameters.

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 incoming mail page shows incoming connections, the total number of incoming messages, the average message size, and the total incoming message size. You can limit the results to the time range that you specify. It is important to have an understanding of the trends of normal message volume and spikes in your environment. You can use the incoming mail page to help 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 emails that are being 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 outgoing mail page shows outgoing connections, the total number of outgoing messages, the average message size, and the total outgoing message size. You can limit the results to the time range that you specify. It is important to have an understanding of the trends of normal message volume and spikes in your environment. You can use the outgoing mail page to help 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 emails that are being sent from specific domains or IP addresses.

System Capacity-System Load

The system load report shows the following:

- Overall CPU Usage
- Memory Page Swapping
- Resource Conservation Activity

Overall CPU Usage

The email gateway is 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 shows the threshold level for CPU usage. If you want to change the threshold level, use the **System Administration** > **System Health** page in web interface or **`healthconfig`** command in CLI. See Setting Thresholds for System Health Parameters.

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 email gateway, 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. This graph also shows the threshold level for memory page swapping. If you want to change the threshold level, use the **System Administration** > **System Health** page in web interface or **`healthconfig`** command in CLI. See Setting Thresholds for System Health Parameters.

Resource Conservation Activity

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

Your email gateway 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 email gateway is entering RCS frequently, it may be an indication that the system is becoming overloaded.

Note about Memory Page Swapping

The system is designed to swap memory regularly, so some memory swapping is expected and is not an indication of problems with your email gateway. Unless the system *consistently* swaps memory in high volumes, memory swapping is normal and expected behavior, especially on C170 and C190 appliances. To improve performance, you may need to add email gateways to your network or tune your configuration to ensure maximum throughput.

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 view 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 PDF to preserve a snapshot of system performance for later reference (or to share with support staff). For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

System Status Page

The **System Status** page provides a detailed representation of all real-time mail and DNS activity for the system. The information displayed is the same information that is available by using the status detail and **`dnsstatus`** commands in the CLI. For more information, see “Monitoring Detailed Email Status” for the status detail command and “Checking the DNS Status” for the **`dnsstatus`** command in Managing and Monitoring Using the CLI

The System Status page is comprised of four sections: System Status, Gauges, Rates, and Counters.

Related Topics

- System Status, on page 31
- Gauges, on page 31
- Rates, on page 31

- Counters, on page 32

System Status

The system status section shows Mail System Status and Version Information.

Related Topics

- Mail System Status, on page 31
- Version Information, on page 31

Mail System Status

The Mail System Status section includes:

- System Status (for more information about system status, see Status, on page 6)
- The last time the status was reported.
- The uptime for the email gateway.
- The oldest message in the system, including messages that have not yet been queued for delivery.

Version Information

The Version Information section includes:

- The email gateway model name.
- The version and build date of the AsyncOS operating system installed.
- The installation date of the AsyncOS operating system.
- The serial number of the system to which you are connected.

This information is useful if you are contacting Cisco Customer Support. (See Working with Technical Support.)

Gauges

The Gauges section shows queue and resource utilization.

- Mail Processing Queue
- Active Recipients in Queue
- Queue Space
- CPU Utilization

Mail Gateway Appliance refers to the percentage of the CPU that AsyncOS processes are consuming. CASE refers to several items, including the Anti-Spam scanning engine and Outbreak Filters processes.

- General Resource Utilization
- Logging Disk Utilization

Rates

The Rates section shows rate handling for recipients.

- Mail Handling Rates
- Completion Rates

Counters

It is recommended that you avoid resetting counters on Cloud Email Security appliance.

You can reset the cumulative email monitoring counters for system statistics and view the last time the counters were reset. The reset affects system counters as well as per-domain counters. The reset does not affect the counters on messages in the delivery queue related to retry schedules.

Note Only user accounts that are in the administrator or operator group have access to reset the counters. User accounts you create in the guest group will not be able to reset the counters. For more information, see Working with User Accounts.

Click Reset Counters to reset the counters. This button offers the same functionality as the **`resetcounters`** command in the CLI. For more information, see Resetting Email Monitoring Counters.

- Mail Handling Events
- Completion Events
- Domain Key Events
- DNS Status

High Volume Mail Page

Note The High Volume Mail page shows data only from message filters that use Header Repeats rule.

The High Volume Mail page contains the following reports in the form of bar charts:

- **Top Subjects**. You can use this chart to understand the top subjects of messages that AsyncOS received.
- **Top Envelope Senders**. You can use this chart to understand the top envelope senders of messages that AsyncOS received.
- **Top Message Filters by Number of Matches**. You can use this chart to understand the top message filter (that uses Header Repeats rule) matches.

The High Volume Mail page also provides a tabular representation of the top message filters and the number of matches for the respective message filters. Click on the number to view a list of all the messages that are included in that number using Message Tracking.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link or PDF format by clicking the **Printable (PDF)** link.

Message Filters Page

The Message Filters page shows information about the top message filter matches (which message filter had the most matching messages) in two forms: a bar chart and a tabular representation.

Using the bar chart, you can find the message filters that are being triggered the most by incoming and outgoing messages. The tabular representation shows the top message filters and the number of matches for the respective

message filters. Click on the number to view a list of all the messages that are included in that number using Message Tracking.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link or PDF format by clicking the **Printable (PDF)** link.

Safe Print Page

You can use the Safe Print report page to view:

- Number of safe-printed attachments based on the file type in graphical format.
- Summary of safe-printed attachments based on the file type in tabular format.

In the 'Summary of Safe Print File Types' section, click the total number of safe-printed attachments to view the message details in Message Tracking.

Retrieving CSV Data

You can retrieve the data used to build the charts and graphs in the Email Security Monitor in CSV format. The CSV data can be accessed in two ways:

- **CSV reports delivered via email**. You can generate a CSV report that is delivered via email or archived. This delivery method is useful when you want separate reports for each table represented on an Reports page, or when you want to send CSV data to users who do not have access to internal networks.

  The comma-separated values (CSV) Report Type is an ASCII text file which contains the tabular data of the scheduled report. Each CSV file may contain up to 100 rows. If a report contains more than one type of table, a separate CSV file will be created for each table. Multiple CSV files for a single report will be compressed into a single .zip file for the archived file storage option or will all be attached to separate e-mail messages for e-mail delivery.

- **CSV files retrieved via HTTP**. You can retrieve the data used to build the charts and graphs in the Email Security Monitor feature via HTTP. This delivery method is useful if you plan to perform further analysis on the data via other tools. You can automate the retrieval of this data, for example, by an automatic script that will download raw data, process, and then display the results in some other system.

Related Topics

- Retrieving CSV Data Via Automated Processes, on page 33

Retrieving CSV Data Via Automated Processes

The easiest way to get the HTTP query you will need is to configure one of the Email Security Monitor pages to display the type of data you want. You can then copy the **Export** link. This is the download URL. When automating data retrieval like this it is important to note which parameters in the download URL should be fixed and which should change (see below).

The download URL is encoded in such a way that it can be copied to an external script that can execute the same query (using proper HTTP authentication) and get a similar data set. The script can use Basic HTTP Authentication or cookie authentication. Keep the following in mind when retrieving CSV data via automated processes:

- Time range selection (past hour, day, week, etc) in relation to when the URL is used again. If you copy the URL to retrieve a CSV data set for "Past Day," the next time you use that URL you will get a new data set that covers the "Past Day" from the time you send the URL again. The date range selection is retained, and appears in the CSV query string (e.g. date_range=current_day).
- Filtering and grouping preferences for the data set. Filters are retained and appear in the query string. Note that filters in reports are rare — one example is the "Global / Local" outbreaks selector in the Outbreaks report.
- The CVS download returns all rows of data in the table for the selected time range.
- The CSV download returns the rows of data in the table ordered by timestamp and key. You can perform further sorting in a separate step such as via a spreadsheet application.
- The first row contains column headers that match the display names shown in the report. Note that timestamps (see Timestamps, on page 34) and keys (see Keys, on page 35) also appear.

Related Topics

- Sample URL, on page 34
- Adding Basic HTTP Authentication credentials, on page 34
- File Format, on page 34
- Timestamps, on page 34
- Keys, on page 35
- Streaming, on page 35

Sample URL

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=
MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0
&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

Adding Basic HTTP Authentication credentials

To specify basic HTTP Authentication credentials to the URL:

```
http://example.com/monitor/
```

becomes:

```
http://username:password@example.com/monitor/
```

File Format

The downloaded file is in CSV format and has a .csv file extension. The file header has a default filename, which starts with the name of the report, then the section of the report.

Timestamps

Exports that stream data show begin and end timestamps for each raw "interval" of time. Two begin and two end timestamps are provided — one in numeric format and the other in human-readable string format. The timestamps are in GMT time, which should make log aggregation easier if you have email gateways in multiple time zones.

Note that in some rare cases where the data has been merged with data from other sources, the export file does not include timestamps. For example, the Outbreak Details export merges report data with Threat Operations Center (TOC) data, making timestamps irrelevant because there are no intervals.

Keys

Exports also include the report table key(s), even in cases where the keys are not visible in the report. In cases where a key is shown, the display name shown in the report is used as the column header. Otherwise, a column header such as “key0,” “key1,” etc. is shown.

Streaming

Most exports stream their data back to the client because the amount of data is potentially very large. However, some exports return the entire result set rather than streaming data. This is typically the case when report data is aggregated with non-report data (e.g. Outbreaks Detail.)

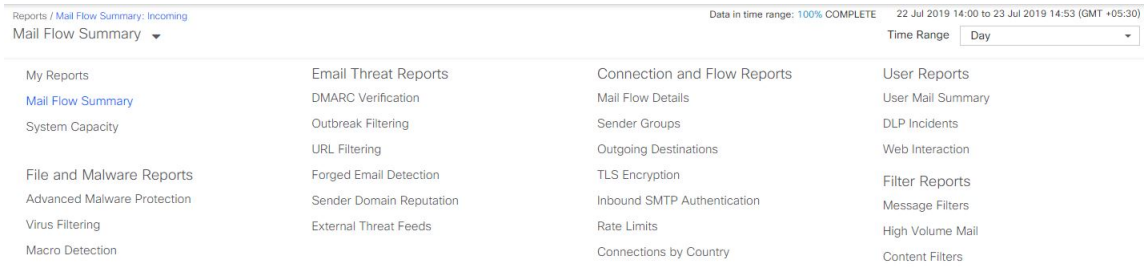
Email Security Monitor Pages on the New Web Interface

To access the new web interface, click the **Secure Email Gateway is getting a new look. Try it!!** link on the leagcy web interface. For more information, see Accessing the Web-Based Graphical User Interface (GUI).

You can view the reports for the email gateway using the **Reports** drop-down as shown in the following figure:

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

Figure 1: Reports Drop-down



You use these pages in the GUI to monitor domains that are connecting to the email gateway listeners. You can monitor, sort, analyze, and classify the “mail flow” of your email gateway and differentiate between high-volume senders of legitimate mail and potential “spammers” (senders of high-volume, unsolicited commercial email) or virus senders. These pages can also help you troubleshoot inbound connections to the system (including important information such as IP Reputation score and most recent sender group match for domains).

These pages help you classify mail relative to the email gateway, and also relative to the services that exist beyond the scope of the gateway, such as the IP Reputation Service, the Anti-Spam scanning service, the Anti-Virus scanning security services, content filters, and Outbreak Filters.

You can export graphs and other data to CSV (comma separated values) format via the **Export** link.

The exported CSV data will display all message tracking and reporting data in GMT regardless of what is set on the email gateway. The purpose of the GMT time conversion is to allow data to be used independently from the email gateway or when referencing data from email gateways in multiple time zones.

Note If you export localized CSV data, the headings may not render properly in some browsers. This occurs because some browsers may not use the correct character set for the localized text. To work around this problem, you can save the file to disk, and open the file using File > Open. When you open the file, select the character set to display the localized text.

For more information about automating the export of report data, see Retrieving CSV Data, on page 33).

List of Email Security Monitor Pages

- My Favorite Reports Page, on page 39
- Mail Flow Summary Page, on page 41
- System Capacity Page, on page 27
- Advanced Malware Protection Page , on page 49
- Virus Filtering Page, on page 53
- Macro Detection Page, on page 54
- DMARC Verification Page, on page 54
- Outbreak Filtering Page, on page 56
- URL Filtering Page , on page 55
- URL Retrospection Page, on page 55
- Forged Email Detection Page, on page 57
- Sender Domain Reputation Page, on page 57
- External Threat Feeds Page, on page 58
- Mail Flow Details Page, on page 58
- Sender Groups Report, on page 66
- Outgoing Destinations, on page 66
- TLS Encryption Page, on page 66
- Inbound SMTP Authentication Page, on page 67
- Rate Limits Page , on page 68
- Connections by Country Page , on page 68
- User Mail Summary Page, on page 69
- DLP Incident Summary Page, on page 70
- Web Interaction Page, on page 71
- Message Filters Page, on page 74
- High Volume Mail Page, on page 74

• Content Filters Page, on page 75
• Advanced Phishing Protection Report Page, on page 75
• Mail Policy Details Report Page, on page 76

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
- Verdict
- Message ID
- Network owner
- Internal user
- Destination domain
- Internal sender domain
- Internal sender IP address
- Outgoing Domain Delivery Status
- Incoming TLS domain
- Outgoing TLS domain
- SHA-256
- Batch ID
- Incoming URL
- Outgoing URL
- URL Retrospection Report

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

Viewing Details of Messages Included in Reports

This functionality works only if reporting and tracking are both local (not centralized on a Cisco Secure Email and Web Manager.)

Procedure

Step 1 Click any blue number in a table on a report page.

(Not all tables have these links.)

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

Step 2 Scroll down to see the list.

What to do next

Related Topics

- Working with Message Tracking Search Results

Time Range for Reports

The Email Security Monitor feature constantly records data about the mail flowing into your gateway. The data are updated every 60 seconds, but the display shown is delayed by 120 seconds behind the current system time. You can specify the time range to include in the results shown. Because the data is monitored in real time, information is periodically updated and summarized in the database.

Choose from the time range options in the following table.

Table 2: Time Ranges Available in the Email Security Monitor Feature

This time range selected in the GUI	...is defined as:
Hour	the last 60 minutes + up to 5 minutes
Day	the last 24 hours + the last 60 minutes
Week	the last 7 days + the elapsed hours of the current day
30 days	the last 30 days + the elapsed hours of the current day
90 days	the last 90 days + the elapsed hours of the current day
Yesterday	00:00 to 23:59 (midnight to 11:59 PM)
Previous Calendar Month	00:00 of the first day of the month to 23:59 of the last day of the month

This time range selected in the GUI	...is defined as:
Custom Range	the range enclosed by the start date and hour and the end date and hour that you specify

My Favorite Reports Page

You can create a custom report page by assembling charts (graphs) and tables from all your existing email security reports, on the My Reports page.

To	Do This
Add modules to My Favorite Reports page	See: • Modules That Cannot Be Added to the My Reports Page, on page 39 • Adding Reports on the My Favorite Reports Page, on page 40
View My Favorite Reports page	1. Select **My Favorite Reports** from the Reports drop-down. 2. Select the time range to view. The time range selected applies to all reports, including all modules on the My Favorite Reports page. Newly-added modules appear at the top of the custom report. **Note** The report modules that you add on the My Favorite Reports page of the new web interface differs from the report modules added on the legacy web interface. It can also differ based on the User roles that you assign.
Rearrange modules on the My Favorite Reports page	On the My Favorite Reports page, drag and drop the modules into the desired location.
Delete modules from the My Favorite Reports page	You can delete the report modules from the My Favorite Reports page in any one of the following ways: • Click the ★ in the top right corner of the required report module. • Go to the **My Favorite Reports** page and select **Manage Favorites** to remove the required report module.

Modules That Cannot Be Added to the My Reports Page

- All modules on the System Status page.
- All modules on the Reporting Data Availability page.

- All modules on the Message Tracking Data Availability page.
- The following per-domain modules from the Sender Profile detail report page: Current Information from SenderBase, Sender Group Information, and Network Information.
- The Past Year Virus Outbreak Summary chart and Past Year Virus Outbreaks table on the Outbreak Filters report page.

Adding Reports on the My Favorite Reports Page

Before you begin

- Ensure that the modules that you want to add can be added. See Modules That Cannot Be Added to the My Reports Page, on page 39.
- Click ★ on the top right corner of a module to delete any default modules that you do not need.

Procedure

Step 1 You can add a report module on the My Favorite Reports page in any one of the following ways:

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

- Go to the report page under the Reports drop-down and click ★ on the top of the report module.
- From the Reports drop-down, select **My Reports** and click **Manage Favorites**.

  The report modules are listed as per the tables and charts on email report pages. Select the required report modules and click **Add** to add to the My Favorite Reports page. If you do not want any reports to be displayed on the My Favorite Report page, select the report module and click **Remove**.

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

  Note
  You can add a maximum of 10 report modules on the My Favorite Reports page.

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

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

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

Mail Flow Summary Page

The Mail Flow Summary report page provides a synopsis of the email message activity from your email gateway. The Mail Flow Summary report page includes graphs and summary tables for the incoming and outgoing messages.

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

You can use the mail trend graphs on this page to monitor the flow of all the incoming mails that are processed and blocked by your email gateways, based on the selected time range. For more information, see Time Range for Reports, on page 38.

To search for specific information within your data, see Searching and the Interactive Email Report Pages , on page 37

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

- Threat Detection Summary
- Content Summary

You can view the mail trend of the incoming messages based on the required counters for the respective categories. For more information, see Using Counters to Filter Data on the Trend Graphs, on page 46.

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

You can use the mail trend graphs on this page to monitor the flow of all the outgoing mails that are processed and delivered by your email gateways, based on the selected time range. For more information, see Time Range for Reports, on page 38.

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

You can view the mail trend of the outgoing messages based on the required counters of the processed messages. For more information, see Using Counters to Filter Data on the Trend Graphs, on page 46.

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

Table 3: Details on the Mail Flow Summary Page

Section	Description
Mail Flow Summary: Incoming	
Number of Messages	The Number of Messages graph provides a visual representation of the total number of messages processed, including the messages that are processed as threat messages.
Threat Messages	The Threat Messages graph provides a visual representation of the total number of messages that are blocked by the email gateway.

Section	Description
Threat Detection Summary	The Threat Detection Summary mail trend graph provides a visual representation based on the following categories: • **Connection and IP Reputation Filtering**: Messages that are categorized as threat by the IP Reputation Filtering and Invalid Recipients. • **Spam Detection**: Messages that are categorized as threat by the Anti-spam scanning engine. • **Email Spoofing**: Messages which are categorized as threat due to DMARC Verification failure. • **Outbreak Threat Summary**: Messages which are categorized as phishing, scam, virus or malware, by the Outbreak Filtering engine. • **Attachment and Malware Detection**: Messages that are categorized as threat by the Anti-virus and AMP engines. • **All Categories**: All the messages that are categorized as threat.
Content Summary	The Content Summary mail trend graph provides a visual representation based on the following categories: • **Graymail**: Messages that are categorized as marketing, bulk or social networking. • **Content Filters**: Messages that are categorized by the content filters. • **All Categories**: All the messages that are categorized by graymail engines and content filters.
Mail Flow Summary: Outgoing	
Number of Messages	The Number of Messages graph provides a visual representation of the total number of messages processed, including the messages that are processed as clean.
Message Delivery	The Message Delivery graph provides a visual representation of the total number of messages that are delivered, including hard bounces.
Outgoing Mails	The Outgoing Mails trend graph provides a visual representation based on the following categories: • Spam Detected • Virus Detected • Detected by AMP • Stopped by Content Filters • Stopped by DLP

Related Topics

- How Email Messages Are Categorized by the Email Gateways, on page 43
- Incoming and Outgoing Summary and Graph, on page 7
- Categorizing Email Messages on the Mail Flow Summary Page, on page 44
- Using Counters to Filter Data on the Trend Graphs, on page 46

How Email Messages Are Categorized by the Email Gateways

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 the chapter about the email pipeline in the online help or user guide for your email gateway.

Incoming and Outgoing Summary and Graph

The Incoming and Outgoing summary sections provide access to real-time activity of all mail activity on your system and is comprised of the Incoming and Outgoing Mail Graphs and Mail Summaries. You can select the time frame on which to report via the Time Range menu. The time range you select is used throughout all of the Email Security Monitor pages. The explanations of each type or category of message are below (see Categorizing Email, on page 8).

While the mail trend graph displays a visual representation of the mail flow, the summary table provides a numeric breakdown of the same information. The summary table includes the percentage and actual number of each type of message, including the total number of attempted, threat, and clean messages.

The outgoing graph and summary show similar information for outbound mail.

Related Topics

- Notes on Counting Messages in Email Security Monitor, on page 8

Notes on Counting Messages in Email Security Monitor

The method Email Security Monitor uses to count incoming mail depends on the number of recipients per message. For example, an incoming message from example.com sent to three recipients would count as three messages coming from that sender.

Because messages blocked by sender reputation filtering do not actually enter the work queue, the email gateway 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 was determined by Cisco and based upon research of a large sampling of existing customer data.

Categorizing Email Messages on the Mail Flow Summary Page

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

Table 4: Email Categories on Mail Flow Summary Page

Category	Description
Mail Flow Summary: Incoming	
IP Reputation Filtering	All connections blocked by HAT policies, multiplied by a fixed multiplier, and added with all recipients blocked by recipient throttling. The value for Stopped by IP Reputation Filtering is calculated based on the following 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 email gateway is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval. In this situation, the value shown can be interpreted as an indicative value of the least number of messages are stopped. The IP Reputation Filtering total count and percentage on the Mail Flow Summary report page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.
Sender Domain Reputation Filtering	The total count of messages blocked based on the reputation verdict of the sender domain.
Invalid Recipients	The total count and percentage of all mail recipients rejected by conversational LDAP rejection in addition to all RAT rejections.
Anti-Spam	The total count and percentage of incoming messages detected by the anti-spam scanning engine as positive or suspect. Additionally, messages that are both spam and virus positive.

Category	Description
Anti-Virus	The total count and percentage of incoming 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.
Advanced Malware Protection	The total count and percentage of incoming messages blocked by the file analysis service. 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.
Content Filter	The total count and percentage of incoming messages that are stopped by message and content filters.
DMARC Policy	The total count and percentage of incoming messages that failed DMARC verification policy.
S/MIME Verification/Decryption Failed	The total count and percentage of incoming messages that failed S/MIME verification, decryption, or both.
Mail Flow Summary: Outgoing	
Hard Bounces	The total count and percentage of outgoing messages that are permanently undeliverable.
Delivered	The total count and percentage of outgoing messages that are delivered.

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

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

Related Topics

Mail Flow Details Page, on page 58

Using Counters to Filter Data on the Trend Graphs

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

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

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

System Capacity Page

The System Capacity page provides a detailed representation of the system load, including messages in the work queue, average time spent 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 an email gateway is exceeding recommended capacity and configuration optimization or additional email gateways are needed.
- Identify historical trends in system behavior which point to upcoming capacity issues.
- Identify which part of the system is using the most resources to assist with troubleshooting.

It is important to monitor your email gateway to ensure that your capacity is appropriate to your message volumes. Over time, volume will inevitably rise and appropriate monitoring will ensure that additional capacity or configuration changes can be applied proactively. The most effective way to monitor system capacity is to track overall volume, messages in the work queue and incidents of Resource Conservation Mode.

- **Volume**: It is important to have an understanding of 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 29 and System Capacity-Outgoing Mail, on page 29.
- **Work Queue**: The work queue is designed to work as a “shock absorber”-- absorbing and filtering spam attacks and processing unusual increases in ham messages. However, the work queue is also the best indicator of a system under stress, prolonged and frequent work queue backups may indicate a capacity problem. You can use the WorkQueue page to track the average time messages spend in the work queue and the activity in your work queue. For more information, see System Capacity- Workqueue, on page 28.
- **Resource Conservation Mode**: When an email gateway becomes overloaded, it will enter “Resource Conservation Mode” (RCM) and send a CRITICAL system alert. This is designed to protect the device and allow it to process any backlog of messages. Your email gateway 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 System Capacity-System Load, on page 29.

Related Topics

- System Capacity- Workqueue, on page 28
- System Capacity- Incoming Mail, on page 29
- System Capacity-Outgoing Mail, on page 29
- System Capacity-System Load, on page 29
- Note about Memory Page Swapping, on page 30
- System Capacity- All, on page 30

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.

For instructions to change the work queue threshold level, see Setting Thresholds for System Health Parameters.

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 incoming mail page shows incoming connections, the total number of incoming messages, the average message size, and the total incoming message size. You can limit the results to the time range that you specify. It is important to have an understanding of the trends of normal message volume and spikes in your environment. You can use the incoming mail page to help 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 emails that are being 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 outgoing mail page shows outgoing connections, the total number of outgoing messages, the average message size, and the total outgoing message size. You can limit the results to the time range that you specify. It is important to have an understanding of the trends of normal message volume and spikes in your environment. You can use the outgoing mail page to help 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 emails that are being sent from specific domains or IP addresses.

System Capacity-System Load

The system load report shows the following:

- Overall CPU Usage
- Memory Page Swapping
- Resource Conservation Activity

Overall CPU Usage

The email gateway is 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 shows the threshold level for CPU usage. If you want to change the threshold level, use the **System Administration** > **System Health** page in web interface or **`healthconfig`** command in CLI. See Setting Thresholds for System Health Parameters.

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 email gateway, 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. This graph also shows the threshold level for memory page swapping. If you want to change the threshold level, use the **System Administration** > **System Health** page in web interface or **`healthconfig`** command in CLI. See Setting Thresholds for System Health Parameters.

Resource Conservation Activity

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

Your email gateway 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 email gateway is entering RCS frequently, it may be an indication that the system is becoming overloaded.

Note about Memory Page Swapping

The system is designed to swap memory regularly, so some memory swapping is expected and is not an indication of problems with your email gateway. Unless the system *consistently* swaps memory in high volumes, memory swapping is normal and expected behavior, especially on C170 and C190 appliances. To improve performance, you may need to add email gateways to your network or tune your configuration to ensure maximum throughput.

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 view 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 PDF to preserve a snapshot of system performance for later reference (or to share with support staff). For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

Reporting Data Availability

The **Reporting Data Availability** page allows you to view 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 email gateways that are managed by the Cisco Secure Email and Web Manager.

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

Advanced Malware Protection Page

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

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

This feature is available for incoming and outgoing messages.

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

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

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

- Advanced Malware Protection – Summary, on page 50
- Advanced Malware Protection – AMP Reputation, on page 50
- Advanced Malware Protection – File Analysis, on page 51
- Advanced Malware Protection – File Retrospection, on page 52
- Advanced Malware Protection – Mailbox Auto Remediation, on page 52

The Advanced Malware Protection report page displays a metrics bar that provides real time data of the email gateway connected to the Cisco Secure Malware Analytics (Threat Grid) appliance.

Note

- You must use the `trailblazerconfig > enable` command on the CLI to populate data on the metrics bar. For more information, see the *Cisco Email Security Command Reference Guide*.
- You can only view the data from the Cisco Secure Malware Analytics (Threat Grid) appliance for the day, week and month.

Related Topics

- Identifying Files by SHA-256 Hash , on page 53
- Viewing File Reputation Filtering Data in Other Reports , on page 53

Advanced Malware Protection – Summary

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

For more information, see Advanced Malware Protection – AMP Reputation, on page 50 and Advanced Malware Protection – File Analysis, on page 51.

Advanced Malware Protection – AMP Reputation

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

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

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

The **Incoming files handled by AMP**section shows the incoming malware files by different categories such as malicious, clean, unknown, unscanable, and low risk.

Incoming malicious files are categorized as the following:

- The percentage of block listed file SHAs received from the AMP reputation server that are categorized as **Malware**.
- The percentage of block listed file SHAs received from the AMP for Endpoints console that are categorised as **Custom Detection**. The threat name of a block listed file SHA obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report.
- The percentage of block listed file SHAs based on the threshold settings that are categorised as **Custom Threshold**.

You can click on the link in the More Details section of the report to view the file trajectory details of a block listed 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.

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

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

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

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

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

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

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

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

Advanced Malware Protection – File Analysis

The Advanced Malware Protection - File Analysis page shows the time and verdict (or interim verdict) for each file sent for analysis. The email gateway 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 Secure Malware Analytics (Threat Grid) Appliance: Files that are allow listed on the Secure Malware Analytics (Threat Grid) appliance show as "clean". For information about allow listing, see the Secure Malware Analytics (Threat Grid) documentation or online help.

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

You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file. For more information, see Identifying Files by SHA-256 Hash , on page 53.

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

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

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

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

Advanced Malware Protection – File Retrospection

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

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

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

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

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

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

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

Advanced Malware Protection – Mailbox Auto Remediation

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

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

- 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
- A list of profile names defined for the recipients for whom the mailbox remediation was successful or unsuccessful
- Reason for the remediation failure
- No profile mapped to the domain

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

- *Invalid Mailbox*: The recipient is not a valid Microsoft Exchange online or Microsoft Exchange on-premise user, or the recipient does not belong to the Microsoft Exchange online or an Microsoft Exchange on-premise domain account configured on your email gateway.
- The message containing the attachment is no longer available in the mailbox, for example, the end user deleted the message.

- *Authentication Error*: The user account provided on your email gateway to connect to the Microsoft Exchange on-premise mailbox is incorrect.
- *Connection Error*: There is a connectivity issue between your email gateway and Microsoft Exchange online or Microsoft Exchange on-premise services when the email gateway attempts to perform the remedial action.
- *Permission Error*:
    - In case of a Microsoft Exchange on-premise account, the user account provided on your email gateway to connect to the Microsoft Exchange on-premise mailbox is not assigned the impersonator role.
    - In case of a Microsoft Exchange online account, the Office 365 application does not have the required permission to access the recipient mailbox.
- *No Profile Mapped for domain*: There is no profile mapped to the recipient domain.
- *Mailbox is Inaccessible or Invalid*:
    - The profile type of the account profile that is used to access the mailbox is incorrect.
    - The recipient is not a valid Microsoft Exchange online or Microsoft Exchange on-premise user.
    - The recipient does not belong to the Microsoft Exchange online or an Microsoft Exchange on-premise domain account configured on your email gateway.

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

Identifying Files by SHA-256 Hash

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

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

Viewing File Reputation Filtering Data in Other Reports

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

Virus Filtering Page

The Virus Filtering page provides an overview of the viruses entering and being sent from your network. The Virus Filtering page displays the viruses that have been detected by the virus scanning engines running on your email gateway. You might want to use this report to take a specific action against a particular virus. For example, if you see that you are receiving a high volume of a viruses known to be embedded in PDF files, you might want to create a filter action to quarantine messages with PDF attachments.

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

The Virus Filtering page gives you an overview of the viruses entering or being sent from or to your network. The Top Incoming Virus Detected section shows a chart view of the viruses that have been sent to your

network in descending order. The Top Outgoing Virus Detected section shows a chart view of the viruses that have been sent from your network in descending order.

Note To see which hosts sent virus-infected messages to your network, you can 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, you can view the Outgoing Senders page and sort by virus-positive messages.

The VirusTypes Details listing displays information about specific viruses, including the infected incoming and outgoing messages, and the total infected messages. The details listing for infected incoming messages displays the name of the virus and the number of incoming messages infected with this virus. Similarly, the outgoing messages displays the name of the virus and the number of outgoing messages infected with the virus. You can sort the Virus Type details by Incoming Messages, Outgoing Messages, or Total Infected Messages.

Macro Detection Page

You can use the Macro Detection report page to view:

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

To view the Macro Detection report page on the email gateway, select **Macro Detection** from the Reports drop-down.

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.

DMARC Verification Page

The DMARC Verification page shows the top domains that failed DMARC verification and the details of actions AsyncOS performed on the messages that failed DMARC verification. You can use this report to fine-tune your DMARC settings and answer these kinds of questions:

- Which are the domains that sent maximum number of messages that are not DMARC compliant?
- For each domain, what are the actions AsyncOS performed on the messages that failed DMARC verification?

The DMARC Verification page contains:

- A graphical representation showing top domains by DMARC verification failures.
- Tabular representation of the following, for each domain:
  - Number of messages that were rejected, quarantined, or accepted without taking any action. Click the number to view a list of messages under the selected category.
  - Number messages that passed DMARC verification.
  - Total number of DMARC verification attempts.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

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 URL reputation level. For messages with multiple URLs, the statistics reflect the lowest reputation of any URL in the message.
- URLs in the global allowed list configured at Security Services > URL Filtering are not included in reports.

  URLs in allowed lists 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.

URL Retrospection Page

The URL Retrospection Report page shows URLs processed by the URL Retrospective Service. This page lists the following details:

- URL - The URLs sent to the URL Retrospective Service analysis by Cisco Secure Email Gateway.
- Verdict Received - Date and time when Cisco Secure Email Gateway receives a verdict from the URL Retrospective Service.
- Remediation Status of Impacted Messages - Action taken for the malicious URLs and the number of messages against each remediation status. The possible remediation statuses are: In Progress, Success, Failed, and Skipped.

Outbreak Filtering Page

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

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

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

To view the Outbreak Filtering report page , select **Outbreak Filtering** from the Reports drop-down.

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

Table 5: Details on the Outbreak Filtering Page

Section	Description
Time Range (drop-down list)	A drop-down list with options for choosing a time range to view.
Threats By Type	The Threats by Type section shows the different types of threat messages received by the email gateway.
Threat Summary	The Threat Summary section shows a breakdown of the messages by Malware, Phish, Scam and Virus. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.
Threat Details	The Threat Details interactive table shows details about specific outbreaks, including the threat category (virus, scam, or phishing), threat name, a description of the threat, and the number of messages identified. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.
Hit Messages from Incoming Messages	The Hit Messages from Incoming Messages section shows the chart and summary of the number of incoming messages processed by Outbreak Filters in the selected time period. Non-viral threats include phishing emails, scams, and malware distribution using links to an external website.
Hit Messages by Threat Level	The Hit Messages by Threat Level section shows the chart and summary of the 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 gateway.

Section	Description
Messages resided in Outbreak Quarantine	The Messages resided in Outbreak Quarantine shows the 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.
Top URL's Rewritten	The Top URL's Rewritten section shows the URLs that are most frequently rewritten to redirect message recipients to the Cisco Web Security Proxy for click-time evaluation of the site if and when the recipient clicks a potentially malicious link in a message. 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. To view Message Tracking details for the messages that populate this report, click a blue number link in the table.

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

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.

To view the Forged Email Detection report page on the Security Management appliance, select **Forged Email Detection** from the Reports drop-down.

The Forged Email Detection reports are populated only if you are using the Forged Email Detection content filter or the `forged-email-detection` message filter.

From the Forged Email Detection report page you can export raw data to a CSV file. Click **Export** link on the top of a report page. Select the required report module that you want to export and click **Download**.

Sender Domain Reputation Page

You can use the Sender Domain Reputation report page to view:

- Incoming messages based on the verdict received from the SDR service in graphical format.

- Incoming messages based on the threat category received from the SDR service in graphical format.

Note Only the messages whose SDR verdict is 'untrusted' or 'questionable' are classified under the SDR threat category, such as, 'spam,' 'malicious,' and so on.

- Summary of incoming messages based on the threat category received from the SDR service in tabular format.

To view the Sender Domain Reputation report page on the Security Management appliance, select **Sender Domain Reputation** from the Reports drop-down.

External Threat Feeds Page

You can use the External Threat Feeds report page to view:

- Top ETF sources used to detect threats in messages in graphical format
- Summary of ETF sources used to detect threats in messages in tabular format.
- Top IOCs that matched threats detected in messages in graphical format.
- Top ETF sources used to filter malicious incoming mail connections in graphical format.
- Summary of ETF sources used to filter malicious incoming mail connections in tabular format.

In the 'Summary of External Threat Feed Sources' section:

- You can click on the number of messages for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular threat feed source to view the distribution of the ETF source based on the IOCs.

In the 'Summary of Indicator of Compromise (IOC) Matches' section:

- You can click on the number of IOCs for a particular ETF source to view the related messages in Message Tracking.
- You can click on a particular IOC to view the distribution of the IOC based on the ETF sources.

To view the External Threat Feeds report page, select **External Threat Feeds** from the Reports drop-down.

Mail Flow Details Page

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

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

The Mail Flow Details report page has the following tabs:

- Incoming Mails
- Outgoing Senders

To search for specific information within your data, see Searching and the Interactive Email Report Pages , on page 37.

From the Incoming Mails tab, you can:

- View the top senders by total threat messages in graphical format.
- View the top senders by clean messages in graphical format.
- View the top senders by graymail messages in graphical format.
- See the IP addresses, domains, or network owners (organizations) that have sent mail to your Cisco Secure Email and Web Manager.
- See detailed statistics on senders that have sent mail to your email gateways. The statistics include the number of connections (accepted or rejected), attempted messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth), total threat messages, total graymails and clean messages.
- See the Incoming Mails interactive table for the detailed information about the particular IP address, domain, or network owner (organization). For more information, see Incoming Mails Table, on page 61.

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

From the Outgoing Senders tab, you can:

- View the top senders by total threat messages in graphical format.
- View the top senders by clean messages in graphical format.
- View the top senders (by IP address or domain) of outgoing threat messages (spam, antivirus, etc.) in your organization.
- See detailed statistics on senders that have sent mail from your email gateways. The statistics include the total threat messages broken down by security service (sender reputation filtering, anti-spam, anti-virus, and so forth) and clean messages.
- See the Sender Details interactive table for detailed information about the particular IP address or domain. For more information, see Sender Details Table, on page 65.

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

Related Topics

- Incoming Mails Table, on page 61
- “No Domain Information”, on page 61
- Time Range for Reports, on page 38
- Views Within the Mail Flow Details Page, on page 60

Views Within the Mail Flow Details Page

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

- IP Addresses
- Domains
- Network Owners

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

Additionally, in the Incoming Mail table of the Mail Flow Details 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 64.

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 gateways. You can monitor the flow of all mail into your email gateways.

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 Mail Flow Details page that is specific to a particular IP address, domain, or network owner.

See the Incoming Mails Table, on page 61 for an explanation of the data included in the Incoming Mails interactive table.

From the Mail Flow Details page you can export raw data to a CSV file.

Note You can generate a scheduled report for the Mail Flow Details report page. See the Scheduled Reports, on page 78.

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

- IP Addresses
- Domains

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

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

See the Sender Details Table, on page 65 for an explanation of the data included in the Sender Details interactive table.

"No Domain Information"

Domains which have connected to the email gateway and could not be verified with a double-DNS lookup are automatically grouped into the special domain "No Domain Information." You can control how these types of unverified hosts are managed via Sender Verification. See Configuring the Gateway to Receive Email.

You can select the number of senders to show in the listing via the Items Displayed menu.

Time Range for Reports

The Email Security Monitor feature constantly records data about the mail flowing into your gateway. The data are updated every 60 seconds, but the display shown is delayed by 120 seconds behind the current system time. You can specify the time range to include in the results shown. Because the data is monitored in real time, information is periodically updated and summarized in the database.

Choose from the time range options in the following table.

Table 6: Time Ranges Available in the Email Security Monitor Feature

This time range selected in the GUI	...is defined as:
Hour	the last 60 minutes + up to 5 minutes
Day	the last 24 hours + the last 60 minutes
Week	the last 7 days + the elapsed hours of the current day
30 days	the last 30 days + the elapsed hours of the current day
90 days	the last 90 days + the elapsed hours of the current day
Yesterday	00:00 to 23:59 (midnight to 11:59 PM)
Previous Calendar Month	00:00 of the first day of the month to 23:59 of the last day of the month
Custom Range	the range enclosed by the start date and hour and the end date and hour that you specify

Incoming Mails Table

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

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

For senders, that is Network Owner, IP Address or Domain, listed in the first column of the Incoming Mails 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 IP 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 64.

You can also view the Sender Groups report, by clicking Sender Groups report at the bottom of the Mail Flow Details page. For more information about the Sender Groups report page, see the Sender Groups Report, on page 66.

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

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

Table 7: Table Column Descriptions for Incoming Mail Table

Column Name	Description
Sender Domain (Domains)	The domain name of the sender.
Sender IP Address (IP Addresses)	The IP address of the sender.
Hostname (IP Addresses)	The hostname of the sender.
DNS Verified (IP Addresses)	The IP addresses that are verified by the DNS.
IP Reputation Score (IP Addresses)	The IP Reputation Score of the sender.
Last Sender Group (IP Addresses)	The details of the last sender group.
Last Sender Group (IP Addresses)	The details of the last sender group.
Network Owner (Network Owners)	The network owner of the sender.
Connections Rejected (Domains and Network Owners)	All connections blocked by HAT policies. When the email gateway 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 (Domains and Network Owners)	All connections accepted,
Total Attempted	All accepted and blocked connections attempted.
Stopped by Recipient Throttling (Domains and Network Owners)	This is a component of Stopped by Reputation Filtering. It represents the number of recipient messages stopped because any of the following HAT limits have been exceeded: maximum recipients per hour, maximum recipients per message, or maximum messages per connection. This is summed with an estimate of the recipient messages associated with rejected or TCP refused connections to yield Stopped by Reputation Filtering.

Column Name	Description
Stopped by IP Reputation Filtering	The value for Stopped by IPReputation 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 email gateway is under heavy load, an exact count of rejected connections is not maintained on a per-sender basis. Instead, rejected connections counts are maintained only for the most significant senders in each time interval. In this situation, the value shown can be interpreted as a “floor”; that is, at least this many messages are stopped. **Note** The IP Reputation Filtering total on the Mail Flow Summary page is always based on a complete count of all rejected connections. Only the per-sender connection counts are limited due to load.
Stopped by Domain Reputation Filtering	The total count of messages blocked based on the reputation verdict of the sender domain.
Stopped as Invalid Recipients	All mail recipients rejected by conversational LDAP rejection plus all RAT rejections.
Spam Detected	Any spam that has been detected.
Virus Detected	Any viruses that have been detected
Detected by Advanced Malware Protection	The total count of messages detected by Advanced Malware Protection engines.
Stopped by Content Filter	The total count of messages that are stopped by a content filter.
Stopped by DMARC	The total count of messages that failed Domain-based Message Authentication, Reporting and Conformance (DMARC) verification. **Note** The email gateway displays the total count of 'Stopped by DMARC' messages based on the ‘Failed - Rejected,’ ‘Failed - Quarantined,’ and ‘Failed - No Action’ results.
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.
Social	Number of messages detected as social messages.
Bulk	Number of messages detected as bulk.
Total Graymails	Number of messages detected as graymails.

Column Name	Description
Clean	All clean messages. Messages processed on email gateways on which the graymail feature is not enabled are counted as clean.

Sender Profile Pages

When you click a sender in the Incoming Mail Details interactive table, on the **Mail Flow Details** [New Web Interface] or **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 IP 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)
- IP 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 IP 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 Details Table

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

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

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

Table 8: Table Column Descriptions for Sender Details Table

Column Name	Description
Sender Domain (Domains)	The domain name of the sender.
Sender IP Address (IP Addresses)	The IP address of the sender.
Hostname (IP Addresses)	The hostname of the sender.
Spam Detected	Any spam that has been detected.
Virus Detected	Any viruses that have been detected.
Detected by Advanced Malware Protection	The total count of messages detected by Advanced Malware Protection engines.
Stopped by Content Filter	The total count of messages that are stopped by a content filter.
Stopped by DLP	The total count of messages that are stopped by DLP engine.
Total Threat	Total number of threat messages (spam, virus)

Column Name	Description
Clean	All clean messages. Messages processed on email gateways on which the graymail feature is not enabled are counted as clean.
Total Messages	The total count of all the messages.

Sender Groups Report

The Sender Groups report 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 Configuring the Gateway to Receive Email.

Outgoing Destinations

The Outgoing Destinations page provides information about the domains your company sends mail to. The page consists of two sections. The top half of the page consists of graphs depicting the top destinations by outgoing threat messages and top destinations by outgoing clean messages on the top half of the page. The bottom half of the page displays a chart showing all the columns sorted by total recipients (default setting).

You can select a time range on which to report, such as a day, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

The Outgoing Destinations page can be used to answer the following types of questions:

- What domains is the email gateway 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 server?

TLS Encryption Page

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

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

- Overall, what portion of incoming and outgoing connections use TLS?
- What partners do I have successful TLS connections with?
- What partners do I have unsuccessful TLS connections with?
- What partners do I have successful TLS connections with DANE support?
- What partners do I have unsuccessful TLS connections with DANE support?
- What partners have issue with their TLS certificates?

- What percent of overall mail with a partner uses TLS?
- What percent of outgoing TLS connections with DANE support are successful?
- What percent of outgoing connections with DANE support are unsuccessful?

The TLS Encryption page is divided into a section for incoming connections and a section for outgoing connections. Each section includes a graph, summaries, and a table with details.

The graph displays a view of incoming or outgoing TLS-encrypted and non-encrypted connections over the time range you specify. The graph displays the total volume of messages, the volume of encrypted and unencrypted messages, the volume of successful and failed TLS encrypted messages and the volume of successful and failed DANE connections. The graphs distinguish between connections in which TLS was required and connections in which TLS was merely preferred.

The table displays details for domains sending or receiving encrypted messages. For each domain, you can view the number of required and preferred TLS connections that were successful and that failed, the total number of TLS connections attempted (whether successful or failed), the total number of unencrypted connections, and the total number of unencrypted connections, and the total number of DANE connections (depending on whether successful or failed). You can also view the percentage of all connections in which TLS was attempted, and the total number of encrypted messages sent successfully, regardless of whether TLS was preferred or required. You can show or hide columns by Customize Columns icon at the top right side of the table.

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 gateway and users' mail clients. If the email gateway 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 email gateway 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 email gateway 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 gateways 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 gateway 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 tabs 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.

To configure rate limiting by envelope sender or modify the existing rate limit, see Defining Rules for Incoming Messages Using a Mail Flow Policy.

Connections by Country Page

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

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

You can click on the number of incoming mail connections of a specific geolocation to view the related messages in Message Tracking.

The "Total Messages" column only displays those messages that are accepted at the SMTP connection level.

Note During report generation:

- If one or more incoming mail connections are detected as private IP address, the incoming mail connections are categorized as “Private IP Addresses” in the report.
- If one or more incoming mail connections are detected as not a valid IP Reputation score, the incoming mail connections are categorized as ‘No Country Info’ in the report.

User Mail Summary Page

The User Mail Sumamry page provides information about the mail sent and received by your internal users, *per email address* (a single user may have multiple email addresses listed — the email addresses are not combined in the report).

The page consists of two sections:

- Graphs depicting the top users by clean incoming and outgoing messages and top users receiving graymail.
- User mail flow details

You can select a time range on which to report (hour, day, week, or month). As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link. You can also display hidden table columns or hide default columns by clicking the Customize Column icon on the top right side of the table.

The User Mail Flow Details listing breaks down the mail received and sent by each email address into clean, spam (incoming only), virus, malware, content filter matches, and graymail (incoming only). You can sort the listing by clicking on the column headers.

Using the Internal Users report, you can answer these kinds of questions:

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

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.

Note that some outbound mail (like bounces) have a null sender. They are counted under outbound and “unknown.”

Click on an internal user to view the Internal User detail page for that user.

Click the Customize Columns icon on the top right side of the table to show columns that are hidden by default, such as the Incoming Spam Detected by Intelligent Multi-Scan column or Outgoing Spam Detected by Intelligent Multi-Scan column.

Related Topics

- User Mail Flow Details, on page 70
- Searching for a Specific Internal User, on page 18

User Mail Flow Details

The User Mail Flow details section shows detailed information about the specified user, including a breakdown of incoming and outgoing messages showing the number of messages in each category (spam detected, virus detected, detected by Advanced Malware Protection, stopped by content filter, graymail detected, and clean). Optionally, for incoming messages, you can click the Customize Columns icon on the top right side of the table to show the Incoming Spam Detected by Intelligent Multi-Scan column. This value reflects the number messages that contained attachments that were determined by file reputation filtering to be malicious. It does not include verdict updates or files found to be malicious by file analysis. Incoming and outgoing content filter and DLP policy matches are also shown.

Click a content filter name to view detailed information for that filter in the corresponding content filter information page (see Content Filters Page, on page 20). You can use this method to get a list of users who also sent or received mail that matched that particular content filter.

Searching for a Specific Internal User

You can search for a specific internal user (email address) via the search form at the bottom User Mail Summary page. Choose whether to exactly match the search text or look for items starting with the entered text (for instance, starts with “ex” will match “example.com”).

DLP Incident Summary Page

The DLP Incident Summary page shows information on the incidents of data loss prevention (DLP) policy violations occurring in outgoing mail. The email gateway 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 Incidents 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 is comprised of two main sections:

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

- the DLP Incidents Details listing.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link. For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

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.

Related Topics

- DLP Incident Details, on page 71
- DLP Policy Detail Page, on page 71

DLP Incident Details

The DLP policies currently enabled in the email gateway's outgoing mail policies are listed in the DLP Incident Details table. Click the name of a DLP policy to view more detailed information.

The DLP Incident Details table shows the total number of DLP incidents per policy, with a breakdown by severity level. The severity level also includes the number of bounced messages and the number of messages delivered in the clear, delivered encrypted, or dropped. Click the column headings to sort the data.

DLP Policy Detail Page

If you clicked the 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 on severity.

The page also includes an Incidents by Sender listing at the bottom of the page that lists each internal user who has sent a message that violated the DLP policy. The listing 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 listing to find out which users may be sending your organization’s sensitive data to people outside your network.

Clicking on the sender name opens up the Internal Users page. See #unique_1558 for more information.

Web Interaction Page

- Web Interaction Tracking report modules are populated only if the web interaction tracking feature is enabled.
- Web Interaction Tracking report modules are not updated in real-time and are refreshed every 30 minutes. Also, after clicking a rewritten URL, it may take up to two hours for the Web Interaction Tracking report to report this event.
- Web Interaction Tracking report is not updated in real-time. After clicking a cloud re-directed rewritten URL, it may take up to two hours for the Web Interaction Tracking report to report this event.
- Web Interaction Tracking reports are available for incoming and outgoing messages.
- Only cloud re-directed rewritten URLs (either by policy or Outbreak Filter) clicked by the end users are included in these modules.

- Web Interaction Tracking page includes the following reports:

Top Malicious URLs clicked by End Users. 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.

Top End Users who clicked on Malicious URLs

This section displays the summary of the top end users who clicked on the Rewritten Malicious URLs, for incoming and outgoing messages.

Web Interaction Tracking Details. Includes the following information:

- A list of all the cloud re-directed rewritten URLs (malicious and unmalicious). Click on a URL to view a detailed report.
- Action taken (allow, block, or unknown) when a cloud re-directed rewritten URL was clicked.

For the data to show up, perform the following:

- Choose **Incoming Mail Policies > Outbreak Filters** to configure an outbreak filter and enable message modification and URL rewriting.
- Configure a content filter with the "**Redirect to Cisco Security Proxy**" action.

Note that, 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 on a number to view a list of all the messages that contain the clicked URL.
- While using Web Interaction Tracking reports, keep in mind the following limitations:
  - 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 of the original recipient is incremented even if the notified user clicks on the rewritten URLs.
  - If you are sending a copy of quarantined messages containing rewritten URLs to a user (for example, an administrator) using web interface, the web interaction tracking data of the original recipient is incremented even if the user (to whom the copy of the messages were sent) clicks on the rewritten URLs.
  - At any point, if you plan to modify the time of your email gateway, make sure that the system time is synchronized with Coordinated Universal Time (UTC).

Remediation Report Page

You can use the Remediation report to monitor the remediation results for Mailbox Auto Remediation, Email Threat Defense Remediation, and Mailbox Search and Remediate.

- To view the list of messages that are attempted for Mailbox Auto Remediation and Mailbox Search and Remediate.
- To know the reason for remediation failure. For example, connections errors, authentication errors, and so on.

Use this report:

The following list explains the various sections on the Rate Limit report:

Section	Description
Summary	The Summary section displays the following: • Total number of messages attempted for remediation using Mailbox Auto Remediation, Email Threat Defense Remediation, and Mailbox Search and Remediate. • Number of messages successfully remediated for a configured remedial action. • Number of messages for which the remediation failed.
Mailbox Auto Remediation	The Mailbox Auto Remediation report section displays the following: • A list of recipients for whom the mailbox auto remediation was successful or unsuccessful. • Auto Remedial actions taken on messages. • The filenames associated with a SHA-256 hash. Click the SHA-256 hash to view the related messages in the Message Tracking page. • A list of profile names defined for the recipients for whom the mailbox auto remediation was successful or unsuccessful. • Reason for the auto remediation failure.
Email Threat Defense Remediation	The Email Threat Defense Remediation report section displays the following: • A list of Email Threat Defense verdict remediated messages. • The message ID of each message. Click the Message ID to view more details in the **Message Tracking** page. • Email Threat Defense Verdict. • Action taken on the messages - forward, delete, or forward and delete. • A list of profile names defined for the recipients. • Time when the action was taken. • Reason for the Email Threat Defense Remediation failure (if any).

Section	Description

Mailbox Search and Remediate	The Mailbox Search and Remediate section displays the following details:
	• The list of remediation batches that are in progress or completed.
	• The remediation status of the messages in the batches.
	• The batch name and the batch ID. Click the batch name to view the batch details:
	  • The date and time when the Mailbox Search and Remediate was initiated.
	  • The source from which the Mailbox Search and Remediate was initiated.
	  • The host who initiated the Mailbox Search and Remediate.
	  • The remedial action taken on the messages.
	  • The Cisco Ironport Message ID of the message.
	  • A read receipt icon to show if the message was read by the recipient before the message was remediated successfully.
	  • The remediation status of the message in the particular batch as Success, Failed, or In Progress.
	  • The email address of the sender who sent the message.
	  • The email addresses of the recipients for whom the message was delivered and later attempted for remediation.
	  • The date and time when the message was sent to the recipient.

Message Filters Page

The Message Filters page shows information about the top message filter matches (which message filter had the most matching messages) in two forms: a bar chart and a tabular representation.

Using the bar chart, you can find the message filters that are being triggered the most by incoming and outgoing messages. The tabular representation shows the top message filters and the number of matches for the respective message filters. Click on the number to view a list of all the messages that are included in that number using Message Tracking.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

High Volume Mail Page

Note The High Volume Mail page shows data only from message filters that use Header Repeats rule.

The High Volume Mail page contains the following reports in the form of bar charts:

- **Top Subjects**. You can use this chart to understand the top subjects of messages that AsyncOS received.
- **Top Envelope Senders**. You can use this chart to understand the top envelope senders of messages that AsyncOS received.

- **Top Message Filters by Number of Matches**. You can use this chart to understand the top message filter (that uses Header Repeats rule) matches.

The High Volume Mail page also provides a tabular representation of the top message filters and the number of matches for the respective message filters. Click the number to view a list of all the messages that are included in that number using Message Tracking.

You can select a time range on which to report, such as an hour, a week, or a custom range. As with all reports, you can export the data for the graphs or the details listing to CSV format via the **Export** link.

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) in two forms: a bar chart and a listing. Using the Content Filters page, you can review your corporate policies on a per-content filter or per-user basis and answer questions like:

- Which content filter is being triggered the most by incoming or outgoing mail?
- Who are the top users sending or receiving mail that is triggering a particular content filter?

You can click the name of the content filter in the listing to view more information about that filter on the Content Filter detail page.

Related Topics

- Content Filter Details, on page 75

Content Filter Details

Click the content filter name link to view the content filter details. The Content Filter detail page displays matches for that filter over time, as well as matches by internal user.

In the Matches by Internal Users section, you can click the name of a user to view that internal user's (email address) Internal User details page (see #unique_1558).

Safe Print Page

You can use the Safe Print report page to view:

- Number of safe-printed attachments based on the file type in graphical format.
- Summary of safe-printed attachments based on the file type in tabular format.

In the 'Summary of Safe Print File Types' section, click the total number of safe-printed attachments to view the message details in Message Tracking.

Advanced Phishing Protection Report Page

The **Reports > Mail Flow Summary > Advanced Phishing Protection** report page displays the following:

- Total number of messages successfully forwarded to the Cisco Advanced Phishing Protection cloud service.

- Total number of messages that are not forwarded to the Cisco Advanced Phishing Protection cloud service.

Note If the forwarding of message metadata has failed, you must validate the configurations of the Advanced Phishing Protection feature. For more information, see How to Integrate Email Gateway with the Cisco Advanced Phishing Protection Cloud Service

You can use the Advanced Phishing Protection report page to view:

- Total number of messages that are sent from all email gateways at the organizational level to the Cisco Advanced Phishing Protection cloud service in a dashboard.
- Total number of messages attempted to be forwarded to the Cisco Advanced Phishing Protection cloud service, in a graphical format.

To view the detailed information on the metadata of the message that is forwarded to the Cisco Advanced Phishing Protection cloud service, click on the link and login to the Cisco Advanced Phishing Protection cloud service. For more information, see Monitoring Message Metadata on the Cisco Advanced Phishing Protection Cloud Service.

Mail Policy Details Report Page

You can use the Mail Policy Details report page to view:

- Top incoming messages that matched a configured mail policy in graphical and tabular format.
- Top outgoing messages that matched a configured mail policy in graphical and tabular format.

In the 'Incoming Policies' section, click the total number of incoming messages that matched a specific mail policy to view the message details in Message Tracking.

In the 'Outgoing Policies' section, click the total number of incoming messages that matched a specific mail policy to view the message details in Message Tracking.

Reporting Overview

Reporting in AsyncOS involves three basic actions:

- You can create Scheduled Reports to be run on a daily, weekly, or monthly basis.
- You can generate a report immediately ("on-demand" report).
- You can view archived versions of previously run reports (both scheduled and on-demand).

Configure scheduled and on-demand reports via the Monitor > Scheduled Reports page. View archived reports via the Monitor > Archived Reports page.

Your email gateway will retain the most recent reports it generates, up to 1000 total versions for all reports. You can define as many recipients for reports as you want, including zero recipients. If you do not specify an email recipient, the system will still archive the reports. If you need to send the reports to a large number of addresses, however, it may be easier to create a mailing list rather than listing the recipients individually.

By default, the email gateway archives the twelve most recent reports of each scheduled report. Reports are stored in the /saved_reports directory of the email gateway. (See FTP, SSH, and SCP Access for more information.)

Related Topics

- Scheduled or Archived Report Types, on page 77
- Setting the Return Address for Reports, on page 78

Scheduled or Archived Report Types

You can choose from the following report types:

- AMP Reputation
- Advanced Malware Protection File Analysis
- Advanced Malware Protection File Retrospection
- Connections by Country
- Content Filters
- DLP Incident Summary
- DMARC Verification Report
- Delivery Status
- Executive Summary
- External Threat Feeds
- Forged Email Detection
- High Volume Mail
- Inbound SMTP Authentication
- Marco Detection
- Mail Flow Summary:Incoming
- Mailbox Auto Remediation
- Mail Flow Details (Outgoing senders: domain)
- Mail Flow Summary: Outgoing
- Message Filters
- My Email Reports
- Outgoing Destinations
- Rate Limits
- Sender Domain Reputation
- Sender Groups
- System Capacity
- TLS Encryption
- User Mail Summary
- URL Filtering
- Outbreak Filters
- Virus Filtering
- Web Interaction

Each of the reports consists of a summary of the corresponding Email Security Monitor page.

Related Topics

- Notes on Reports, on page 78

Notes on Reports

Content Filter reports in a PDF format are limited to a maximum of 40 content filters. You can obtain the full listing via reports in a CSV format.

Note To generate PDFs in Chinese, Japanese, or Korean on Windows computers, you must also download the applicable Font Pack from Adobe.com and install it on your local computer.

Setting the Return Address for Reports

To set the return address for reports, see Configuring the Return Address for Email Gateway Generated Messages. From the CLI, use the **`addressconfig`** command.

Managing Reports

You can create, edit, delete, and view archived scheduled reports. You can also run a report immediately (on-demand report). Managing and viewing these reports is discussed below.

Note When in Cluster Mode, you are unable to view reports. You may view reports when in machine mode.

The Monitor > Scheduled Reports page shows a listing of the scheduled reports already created on the email gateway.

Related Topics

- Scheduled Reports, on page 78
- Archived Reports, on page 80

Scheduled Reports

Scheduled reports can be scheduled to run on a daily, weekly, or monthly basis. You can select a time at which to run the report. Regardless of when you run a report, it will only include data for the time period that you specify, for example the past 3 days or the previous calendar month. Note that a daily report scheduled to run at 1AM will contain data for the previous day, midnight to midnight.

Your email gateway ships with a default set of scheduled reports —you can use, modify, or delete any of them.

Related Topics

- Scheduling a Report to be Generated Automatically , on page 79
- Editing Scheduled Reports , on page 79

• Deleting Scheduled Reports, on page 80

Scheduling a Report to be Generated Automatically

Procedure

Step 1 On the Monitor > Scheduled Reports page, click **Add Scheduled Report**.

Step 2 Select a report type. Depending on the report type you select, different options may be available.

For more information about the available types of scheduled reports, see Scheduled or Archived Report Types, on page 77.

Step 3 Enter a descriptive 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 4 Select a time range for the report data. (This option is not available for Outbreak Filters reports.)

Step 5 Select a format for the report:

- 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.

  For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

- CSV. Create an ASCII text file that contains the tabular 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 6 Specify the report options, if available. Some reports do not have report options.

Step 7 Specify scheduling and delivery options. If you do not specify an email address, the report is archived but is not sent to any recipients.

Note
If you are sending reports to an external account (such as Yahoo or Gmail, etc.), you may need to add the reporting return address to the external account's allowed list to prevent report emails from being incorrectly classified as spam.

Step 8 Click **Submit**. Commit your changes.

Editing Scheduled Reports

Procedure

Step 1 Click the report title in the listing on the Services > Centralized Reporting page.

Step 2 Make your changes.

Step 3 Submit and commit your changes.

Deleting Scheduled Reports

Procedure

Step 1 On the Services > Centralized Reporting page, select the check boxes corresponding to the reports that you want to delete.

Note
Select the All check box to remove all scheduled reports.

Step 2 Click **Delete**.

Step 3 Confirm the deletion and then commit your changes.

Any archived versions of deleted reports are *not* automatically deleted.

Archived Reports

The **Monitor > Archived Reports** page lists the available archived reports. You can view a report by clicking its name in the Report Title column. You can generate a report immediately by clicking **Generate Report Now**

Use the Show menu to filter which type of reports is listed. Click the column headings to sort the listing.

Archived reports are deleted automatically — up to 30 instances of each scheduled report (up to 1000 reports) are kept and as new reports are added, older ones are deleted to keep the number at 1000. The 30 instances limit is applied to each individual scheduled report, not report type.

Related Topics

- Generating On-Demand Reports, on page 80

Generating On-Demand Reports

You can generate a report without scheduling it. These on-demand reports are still based on a specified time frame, but they are generated immediately.

Procedure

Step 1 Click **Generate Report Now** on the Archived Reports page.

Step 2 Select a report type and edit the title if desired. AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.

For more information about the available types of scheduled reports, see Scheduled or Archived Report Types, on page 77.

Step 3 Select a time range for the report data. (This option is not available for Virus Outbreak reports.)

If you create a custom range, the range will appear as a link. To modify the range, click the link.

Step 4 Select a format for the report.

- 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.

  For information about generating PDFs in languages other than English, see the Notes on Reports, on page 78.

- CSV. Create an ASCII text file that contains the tabular 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.Specify any report options.

Step 5 Select whether to archive the report (if so, the report will shown on the Archived Reports page).

Step 6 Specify whether to email the report and to which email addresses to send the report.

Step 7 Click **Deliver this Report** to generate the report and deliver it to recipients or archive it.

Step 8 Commit your changes.

Troubleshooting Email Reports

- Link to Message Tracking Gives Unexpected Results , on page 81
- File Analysis Details in the Cloud Are Incomplete, on page 81

Link to Message Tracking Gives Unexpected Results

Problem

Drilling down from a report to view details in message tracking yields unexpected results.

Solution

This can occur if reporting and message tracking were not simultaneously enabled, functioning properly, and storing data locally (as opposed to being stored centrally on a Cisco Secure Email and Web Manager). Data for each feature (reporting and message tracking) is stored only while that feature is enabled and functioning on that email gateway, independently of whether the other feature (reporting or message tracking) is enabled and functioning. Therefore, reports may include data that is not available in Message Tracking and vice-versa.

File Analysis Details in the Cloud Are Incomplete

Problem

Complete file analysis results in the public cloud are not available for files uploaded from other email gateways in my organization.

Solution

Be sure to group all email gateways that will share file analysis result data. See (Public Cloud File Analysis Services Only) Configuring Appliance Groups. This configuration must be done on each appliance in the group.