Tracking Messages

This chapter contains the following sections:

- Tracking Service Overview, on page 1
- Setting Up Centralized Message Tracking , on page 2
- Checking Message Tracking Data Availability , on page 5
- Searching for Email Messages, on page 5
- Understanding Tracking Query Results, on page 13
- Troubleshooting Message Tracking, on page 17
- Exporting Message Service, on page 18

Tracking Service Overview

The tracking service of the Cisco Secure Email and Web Managerappliance complements Email Security appliances. With the Security Management appliance, email administrators have a single place to track the status of messages that traverse any of their Email Security appliances.

The Security Management appliance makes it easy to find the status of messages that Email Security appliances process. Email administrators can quickly resolve help desk calls by determining the exact location of a message. With the Security Management appliance, an administrator can determine if a particular message was delivered, found to contain a virus, or placed in a spam quarantine — or if it is located somewhere else in the mail stream.

Instead of having to search through log files using grep or similar tools, you can use the flexible tracking interface of the Security Management appliance to locate messages. You can use a variety of search parameters in combination

Tracking queries can include:

- **Time Frame:** Find a message that was sent between specified dates and times.
- **Envelope Information:** Find messages from particular envelope senders or recipients by entering the text strings to match.
- **Subject:** Match a text string in the subject line. Warning: Do not use this type of search in environments where regulations prohibit such tracking.
- **Attachment Name**: You can search for messages based on an attachment name. Messages that contain at least one attachment with the queried name will appear in the search results.

For performance reasons, the names of files within attachments such as OLE objects or archives such as .ZIP files are not tracked.

Some attachments may not be tracked. For performance reasons, scanning of attachment names occurs only as part of other scanning operations, for example message or content filtering, DLP, or disclaimer stamping. Attachment names are available only for messages that pass through body scanning while the attachment is still attached. Some examples when an attachment name will not appear include (but are not limited to):

- if the system only uses content filters, and a message is dropped or its attachment is stripped by anti-spam or anti-virus filters
- if message splintering policies strip the attachment from some messages before body scanning occurs.

- **File SHA256**: Find messages with the SHA-256 value of the message file
- **Cisco Host**: Narrow search criteria to particular Email Security appliances, or search across all managed appliances.
- **Message ID Header and Cisco MID**: Find messages by identifying the SMTP “Message-ID:” header or the Cisco message ID (MID).
- **Sender IP Address/ Domain/ Network Owner**: Search for messages from a particular IP address, domain name or network owner.
- **Message Event**: Find messages that match specified events, such as messages flagged as virus positive, spam positive, or suspected spam, and messages that were delivered, hard bounced, soft bounced, or sent to the Virus Outbreak Quarantine
- **Rejected Connections**: Search for messages from a particular IP address, domain name or network owner of the rejected connections in the search results

Setting Up Centralized Message Tracking

To set up centralized message tracking, complete the following procedures in order:

1. Enabling Centralized Email Tracking, on page 2
2. Configuring Centralized Message Tracking on Email Security Appliances , on page 3
3. Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance , on page 4

Enabling Centralized Email Tracking

- Enabling Centralized Email Tracking on the Legacy Web Interface, on page 3
- Enabling Centralized Email Tracking on the New Web Interface, on page 3

Enabling Centralized Email Tracking on the Legacy Web Interface

Procedure

Step 1 Choose **Management Appliance > Centralized Services > Email> Centralized Message Tracking**.

Step 2 In the Message Tracking Service section, click **Enable**.

Step 3 If you are enabling centralized email tracking for the first time after running the System Setup Wizard, review the end user license agreement, and click **Accept**.

Step 4 Submit and commit your changes.

What to do next

Configuring Centralized Message Tracking on Email Security Appliances , on page 3

Enabling Centralized Email Tracking on the New Web Interface

Procedure

Step 1 On the Security Management appliance, click **Service Status** and hover over the ⚙ corresponding to **Message Tracking** card.

Step 2 Click **Edit Settings**.

Step 3 If you are enabling centralized email tracking for the first time after running the System Setup Wizard, review and accept the license agreement, and click **Proceed**.

Step 4 Click the toggle switch to enable Centralized Email Tracking.

Step 5 Select the appropriate fields and click **Submit**.

What to do next

Configuring Centralized Message Tracking on Email Security Appliances , on page 3

Configuring Centralized Message Tracking on Email Security Appliances

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Verify that Message Tracking is configured and working properly on the Email Security appliance.

Step 3 Go to **Security Services > Message Tracking**.

Step 4 Click **Edit Settings**.

Step 5 Select **Centralized Tracking**.

Step 6 Click **Submit**.

Step 7 If you want to be able to search for and log the names of email attachments:

Make sure you have at least one incoming content filter or other body scanning feature configured and enabled on the Email Security appliance. For information about content filters and body scanning, see the documentation or online help for your Email Security appliance.

Step 8 Submit and commit your changes.

Step 9 Repeat for each Email Security appliance to manage.

What to do next

Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance , on page 4

Adding the Centralized Message Tracking Service to Each Managed Email Security Appliance

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

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Management Appliance > Centralized Services > Security Appliances**.

Step 3 If you have already added the Email Security appliance to the list on this page:

a) Click the name of an Email Security appliance.

b) Select the **Centralized Message Tracking** service.

Step 4 If you have not yet added the Email Security appliance:

a) Click Add Email Appliance.

b) In the Appliance Name and IP Address text fields, type the appliance name and the IP address for the Management interface of the Email Security appliance.

Note
If you enter a DNS name in the IP Address text field, it will be immediately resolved to an IP address when you click **Submit**.

c) The Centralized Message Tracking service is pre-selected.

d) Click **Establish Connection.**

e) Enter the user name and passphrase for an administrator account on the appliance to be managed, then click **Establish Connection**.

Note
You enter the login credentials to pass a public SSH key for file transfers from the Security Management appliance to the remote appliance. The login credentials are not stored on the Security Management appliance.

f) Wait for the Success message to appear above the table on the page.
g) Click **Test Connection**.
h) Read test results above the table.

Step 5 Submit and commit your changes.

Step 6 Repeat this procedure for each Email Security appliance for which you want to enable Centralized Message Tracking.

Managing Access to Sensitive Information

If you will distribute administrative tasks to other people and you want to restrict their access to sensitive information that may appear in email messages that violate Data Loss Prevention (DLP) policies, see Controlling Access to Sensitive Information in Message Tracking.

Checking Message Tracking Data Availability

You can determine the date range that your message tracking data includes, as well as identify any missing intervals in that data.

Procedure

Step 1 [New Web Interface Only] On the Security Management appliance, click ⚙ to load the legacy web interface.

Step 2 Choose **Email** > **Message Tracking** > **Message Tracking Data Availability**.

Searching for Email Messages

Note After upgrading to AsyncOS 13.6.1, the state of the messages that were in quarantine prior to the upgrade does not change.

- Searching for Email Messages on the New Web Interface, on page 5
- Searching for Email Messages on the Legacy Web Interface, on page 8
- Remediating Messages in Mailboxes, on page 10

Searching for Email Messages on the New Web Interface

The tracking service of the appliance lets you search for a particular email message or group of messages that match specified criteria, such as the message subject line, date and time range, envelope sender or recipient, or processing event (for example, whether the message was virus positive, spam positive, hard bounced, delivered, and so forth). Message tracking gives you a detailed view of message flow. You can also drill down

on particular email messages to see message details, such as the processing events, attachment names, or the envelope and header information.

Note Although the tracking component provides detailed information about individual email messages, you cannot use it to read the content of messages.

Procedure

Step 1 On the Security Management appliance, choose **Tracking** > **Search**.

Step 2 Select **Messages** tab or **Rejected Connections** tab to narrow your search results.

Note
You can search for rejected connections based on the sender IP address, domain or network owner.

Step 3 (Optional) Click the **Advanced Search** to display additional search options.

Step 4 Enter the following search criteria:

Note
Tracking searches do not support wildcard characters or regular expressions. Tracking searches are not case sensitive.

- [For Messages and Rejected Connections] **Message Received**: Specify a date and time range for the query using "Last Day," "Last 7 Days," or "Custom Range." Use the "Last Day" option to search for messages within the past 24 hours, and use the "Last 7 Days" option to search for messages within the past full seven days, plus the time that has passed on the current day.

  If you do not specify a date, the query returns data for all dates. If you specify a time range only, the query returns data for that time range across all available dates. If you specify the current date and 23:59 as the end date and time, the query returns all data for the current date.

  Dates and times are converted to GMT format when they are stored in the database. When you view dates and times on an appliance, they are displayed in the local time of the appliance.

  Messages appear in the results only after they have been logged on the Email Security appliance and retrieved by the Security Management appliance. Depending on the size of logs and the frequency of polling, there could be a small gap between the time when an email message was sent and when it actually appears in tracking and reporting results.

- **Envelope Sender**: Select Begins With, Is, or Contains, and enter a text string to search for in the envelope sender. You can enter email addresses, user names, or domains. Use the following formats:
  - For email domains: *example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]*
  - For full email addresses: *user@example.com, user@[203.0.113.15] or user@[ipv6:2001:db8:80:1::5]*.
  - You can enter any character(s). No validation of your entry is performed.

- **Subject**: Select Begins With, Is, Contains, or Is Empty, and enter a text string to search for in the message subject line.

- **Envelope Recipient**: Select Begins With, Is, or Contains, and enter text to search for in the envelope recipient. You can enter email addresses, user names, or domains.

If you use the alias table for alias expansion on your Email Security appliances, the search finds the expanded recipient addresses rather than the original envelope addresses. In all other cases, message tracking queries find the original envelope recipient addresses.

Otherwise, valid search criteria for Envelope Recipient are the same as those for Envelope Sender.

You can enter any character(s). No validation of your entry is performed.

- **Attachment Name**: Select Begins With, Is, or Contains, and enter an ASCII or Unicode text string for one Attachment Name to find. Leading and trailing spaces are not stripped from the text you enter.
- **Reply-To**: Select Begins With, Is, or Contains, and enter a text string to search for messages based on the `Reply-To` header of the message.
- **File SHA256**: Enter a File SHA-256 value of the message.

  For more information about identifying files based on SHA-256 hash, see Identifying Files by SHA-256 Hash.
- **Cisco Host**: Select All Host to search across all email security appliances or select the required email security appliance from the drop-down menu.
- **Message ID Header and Cisco MID**: Enter a text string for the message ID header, the Cisco IronPort message ID (MID), or both.
- [For Messages and Rejected Connections] **Sender IP Address/ Domain/ Network Owner**: Enter a sender IP address, domain or nework owner details.
  - An IPv4 address must be 4 numbers separated by a period. Each number must be a value from 0 to 255. (Example: 203.0.113.15).
  - An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons.

    You can use zero compression in one location, such as 2001:db8:80:1::5.
  - **Message Event**: Select the events to track. Options are Virus Positive, Spam Positive, Suspect Spam, contained malicious URLs, contained URL in specified category, DLP Violations (you can enter the name of a DLP policy and select violation severities or action taken), DMARC violations, Delivered, Advanced Malware Protection Positive (for malware found in an attachment), Hard Bounced, Soft Bounced, currently in a policy, virus, or outbreak quarantine, caught by message filters or content filters, and Quarantined as Spam. Unlike most conditions that you add to a tracking query, events are added with an “OR” operator. Selecting multiple events expands the search.

You do not need to complete every field. Except for the Message Event options, the query is an “AND” search. The query returns messages that match the “AND” conditions specified in the search fields. For example, if you specify text strings for the envelope recipient and the subject line parameters, the query returns only messages that match both the specified envelope recipient and the subject line.

Note
In the new web interface, to perform a partial URL search, you need to add "*" before and after the search string to retrieve the results.

Step 5 Click **Search**.

Each row corresponds to an email message. Scroll down to load more messages in the view.

If necessary, you can refine your search by entering new search criteria, and run the query again. Alternatively, you can refine the search by narrowing the result set, as described in the following section.

Click Export to export the search results.

What to do next

- Narrowing the Result Set, on page 11
- About Message Tracking and Advanced Malware Protection Features , on page 12
- Understanding Tracking Query Results, on page 13

Searching for Email Messages on the Legacy Web Interface

The Security Management appliance's tracking service lets you search for a particular email message or group of messages that match specified criteria, such as the message subject line, date and time range, envelope sender or recipient, or processing event (for example, whether the message was virus positive, spam positive, hard bounced, delivered, and so forth). Message tracking gives you a detailed view of message flow. You can also drill down on particular email messages to see message details, such as the processing events, attachment names, or the envelope and header information.

Note Although the tracking component provides detailed information about individual email messages, you cannot use it to read the content of messages.

Procedure

Step 1 Choose **Email > Message Tracking > Message Tracking**.

Step 2 (Optional) Click the Advanced link to display more search options.

Step 3 Enter search criteria:

Note
Tracking searches do not support wildcard characters or regular expressions. Tracking searches are not case sensitive.

- Envelope Sender: Select Begins With, Is, or Contains, and enter a text string to search for in the envelope sender. You can enter email addresses, user names, or domains. Use the following formats:
  - For email domains: example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]
  - For full email addresses: user@example.com, user@[203.0.113.15] or user@[ipv6:2001:db8:80:1::5].
  - You can enter any character(s). No validation of your entry is performed.
- Envelope Recipient: Select Begins With, Is, or Contains, and enter text to search for in the envelope recipient. You can enter email addresses, user names, or domains.

If you use the alias table for alias expansion on your Email Security appliances, the search finds the expanded recipient addresses rather than the original envelope addresses. In all other cases, message tracking queries find the original envelope recipient addresses.

Otherwise, valid search criteria for Envelope Recipient are the same as those for Envelope Sender.

You can enter any character(s). No validation of your entry is performed.

- Subject: Select Begins With, Is, Contains, or Is Empty, and enter a text string to search for in the message subject line.
- Message Received: Specify a date and time range for the query using “Last Day,” “Last 7 Days,” or “Custom Range.” Use the “Last Day” option to search for messages within the past 24 hours, and use the “Last 7 Days” option to search for messages within the past full seven days, plus the time that has passed on the current day.

If you do not specify a date, the query returns data for all dates. If you specify a time range only, the query returns data for that time range across all available dates. If you specify the current date and 23:59 as the end date and time, the query returns all data for the current date.

Dates and times are converted to GMT format when they are stored in the database. When you view dates and times on an appliance, they are displayed in the local time of the appliance.

Messages appear in the results only after they have been logged on the Email Security appliance and retrieved by the Security Management appliance. Depending on the size of logs and the frequency of polling, there could be a small gap between the time when an email message was sent and when it actually appears in tracking and reporting results.

- Sender IP Address: Enter a sender IP address and select whether to search messages or to search rejected connections only.
  - An IPv4 address must be 4 numbers separated by a period. Each number must be a value from 0 to 255. (Example: 203.0.113.15).
  - An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons. You can use zero compression in one location, such as 2001:db8:80:1::5.
- Message Event: Select the events to track. Options are Virus Positive, Spam Positive, Suspect Spam, contained malicious URLs, contained URL in specified category, DLP Violations (you can enter the name of a DLP policy and select violation severities or action taken), DMARC violations, Delivered, Advanced Malware Protection Positive (for malware found in an attachment), Hard Bounced, Soft Bounced, currently in a policy, virus, or outbreak quarantine, caught by message filters or content filters, Macro File Types Detected, Geolocation, Low Risk and Quarantined as Spam. Unlike most conditions that you add to a tracking query, events are added with an “OR” operator. Selecting multiple events expands the search.
- Message ID Header and Cisco IronPort MID: Enter a text string for the message ID header, the Cisco IronPort message ID (MID), or both.
- Query Settings: From the drop-down menu, select how long you want the query to run before it times out. Options are “1 minute,” “2 minutes,” “5 minutes,” “10 minutes,” and “No time limit.” Also, select the maximum number of results you want the query to return (up to 1000).
- Attachment name: Select Begins With, Is, or Contains, and enter an ASCII or Unicode text string for one Attachment Name to find. Leading and trailing spaces are not stripped from the text you enter.

You do not need to complete every field. Except for the Message Event options, the query is an “AND” search. The query returns messages that match the “AND” conditions specified in the search fields. For example, if you specify text strings for the envelope recipient and the subject line parameters, the query returns only messages that match both the specified envelope recipient and the subject line.

Step 4 Click **Search**.

The query results appear at the bottom of the page. Each row corresponds to an email message.

Your search criteria are highlighted in each row.

If the number of returned rows is greater than the value specified in the “Items per page” field, the results appear on multiple pages. To navigate through the pages, click the page numbers at the top or bottom of the list.

If necessary, refine the search by entering new search criteria, and run the query again. Alternatively, you can refine the search by narrowing the result set, as described in the following section.

What to do next

- Narrowing the Result Set, on page 11
- About Message Tracking and Advanced Malware Protection Features , on page 12
- Understanding Tracking Query Results, on page 13

Remediating Messages in Mailboxes

Cisco Secure Email and Web Managerappliance provides the capability to remediate the malicious messages that are already delivered to the user mailbox. You can configure your appliance to remediate the messages by using the Message Tracking filter.

You can perform remedial actions manually on messages that are already delivered to the user mailbox. For example, an administrator monitoring the incoming messages can perform remedial actions on messages in the user mailbox using the Message Tracking filter.

You can also use the Message Tracking page to search and remediate the messages that are delivered to the user mailbox. The Message Tracking page is a unified place to search for all messages delivered to the mailboxes. From the search result, you can choose the messages you want to remediate and apply the action you want to perform on the messages.

Search and Remediate Messages Workflow

1. Message reaches the appliance and is delivered to the recipient.
2. The user searches for the message delivered to the recipient using the Message Tracking filter.
3. The user selects the message to be remediated from the recipient's mailbox and applies the remedial action on the message.

Search and Remediate Actions on Messages in the Mailboxes

Before you begin

- Make sure that you have enabled mailbox remediation and configured the account settings on Cisco Email Security Gateway.
- Enable Message Tracking on your appliance. See Setting Up Centralized Message Tracking , on page 2.
- If you are using the Centralized Message Tracking service, make sure that you have enabled the trailblazer port and AsyncOS API HTTP port on the managed Cisco Email Security Gateway and the Cisco Secure Email and Web Managerappliance can access the trailblazer port. If the trailblazer port is disabled, ensure that the Cisco Secure Email and Web Manager appliance can access the AsyncOS API HTTP(S) port on the managed Cisco Email Security Gateway.

- If the managed Cisco Email Security appliance is using a certificate whose Certificate Authority does not exist in the Cisco Secure Email and Web Manager appliance trust store, the server certificate validation on the Content Security Management appliance fails. To allow communication, add the Certificate Authority of the signed certificate used by the Cisco Email Security appliance to the Cisco Secure Email and Web Manager appliance. To add the Certificate Authority, use `certconfig` > `CERTAUTHORITY` sub command in the CLI.

  CAUTION: If you want to disable the server certificate validation on the Secure Email and Web Manager appliance, use the `esaapiconfig` command in the CLI. Cisco does not recommend you to disable the certificate validation for security reasons.

Procedure

Step 1 On the Security Management appliance, click on the **Tracking** tab on the new web interface of the appliance.

Step 2 Click the **Messages** tab to narrow your search results. For more information, see Searching for Email Messages on the New Web Interface, on page 5.

Step 3 Select the messages you want to remediate. You can select a maximum of 1000 messages at a time. You can remediate the messages that are only in the delivered state.

Step 4 Click **Remediate**.

Step 5 Enter the following details:

- Enter a batch name for the remediation.
- Select anyone of the following remediation action:
  - Delete the messages. Select this option to permanently delete the messages from the end user's mailbox.
  - Forward to an email address. Select this option to forward the messages to a specified user, for example, an email administrator.
  - Forward to an email address and delete the messages. Select this option to forward the messages to a specified user, for example, an email administrator and permanently delete that messages from the end user's mailbox.

Step 6 Click **Apply**.

After you click **Apply**, you can view the Remediation Report Status widget at the bottom-right corner of the Message Tracking page. Use this widget to check the status of the Remediation Report generation. After the Remediation Report generation is complete, click View Details on the widget to go to the Remediation Report to view the remediation results.

Note
You can also view Remediation Report directly by navigating to **Reports** > **User Reports** > > **Remediation Report** and click the Mailbox Search And Remediate tab.

Narrowing the Result Set

After you run a query, you might find that the result set includes more information than you need. Instead of creating a new query, narrow the result set by clicking a value within a row in the list of results. Clicking a value adds the parameter value as a condition in the search. For example, if the query results include messages

from multiple dates, click a particular date within a row to show only messages that were received on that date.

Procedure

Step 1 Float the cursor over the value that you want to add as a condition. The value is highlighted in yellow.

Use the following parameter values to refine the search:

- Date and time
- Message ID (MID)
- Host (the Email Security appliance)
- Sender
- Recipient
- The subject line of the message, or starting words of the subject

Step 2 [New Web Interface Only] In the Message Tracking search criteria, click **Modify**.

Use the following parameter values to refine the search:

- Date and time
- Message ID (MID)
- Cisco Host (the Email Security appliance)
- Sender
- Recipient
- The subject line of the message, or starting words of the subject
- Message Event
- Additional Details (Message Last State, SBRS, Sender IP, and Group)

Step 3 Click the value to refine the search.

The Results section displays the messages that match the original query parameters *and* the new condition that you added.

Step 4 If necessary, click additional values in the results to further refine the search.

Note
To remove query conditions, click **Clear** and run a new tracking query.

About Message Tracking and Advanced Malware Protection Features

When searching for file threat information in Message Tracking, keep the following points in mind:

- To search for malicious files found by the file reputation service, select **Advanced Malware Protection Positive** for the Message Event option in the Advanced section in Message Tracking.

- Message Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a message was processed. For example, if a file was initially found to be clean, then a verdict update found the file to be malicious, only the clean verdict appears in Tracking results.

  In Message Tracking details, the Processing Details section shows:

  - The SHA-256 of each attachment in the message, and
  - The final Advanced Malware Protection verdict for the message as a whole, and
  - Any attachments which were found to contain malware.

    No information is provided for clean or unscannable attachments.

- Verdict updates are available only in the AMP Verdict Updates report. The original message details in Message Tracking are not updated with verdict changes. To see messages that have a particular attachment, click a SHA-256 in the verdict updates report.
- Information about File Analysis, including analysis results and whether or not a file was sent for analysis, are available only in the File Analysis report.

  Additional information about an analyzed file may be available from the cloud. To view any available File Analysis information for a file, select **Monitor > File Analysis** and enter the SHA-256 to search for the file. If the File Analysis service has analyzed the file from any source, you can see the details. Results are displayed only for files that have been analyzed.

  If the appliance processed a subsequent instance of a file that was sent for analysis, those instances will appear in Message Tracking search results.

Understanding Tracking Query Results

If results are not what you expected, see Troubleshooting Message Tracking, on page 17.

Tracking query results list all of the messages that match the criteria specified in the tracking query. Except for the Message Event options, the query conditions are added with an “AND” operator. The messages in the result set must satisfy all of the “AND” conditions. For example, if you specify that the envelope sender begins with J and you specify that the subject begins with T , the query returns a message only if both conditions are true for that message.

To view detailed information about a message, click the **More Details** link in the new web interface or **Show Details** link in the legacy web interface, for that message. For more information, see the Message Details, on page 14.

Note

- Messages with 50 or more recipients will not appear in tracking query results. This issue will be resolved in a future release.
- [New Web Interface Only] You can scroll down to display the search results when you specify your query. More results are displayed in the view as you scroll down.
- You can export the search results to a .csv file using the **Export** link above the search results section.

  You can choose to display up to 1000 search results when you specify your query. To view up to 50,000 messages that match your criteria, click the **Export All** link above the search results section and open the resulting .csv file in another application.
- If you clicked a link in a report page to view message details in Message Tracking, and the results are unexpected, this can occur if reporting and tracking were not both simultaneously and continuously enabled during the time period you are reviewing.
- For information about printing or exporting message tracking search results, see Exporting Reporting and Tracking Data.

Related Topics

Message Details, on page 14

Message Details

To view detailed information about a particular email message, including the message header information and processing details, click **More Details** linkfor any item in the search results list. A new window opens with the message details.

The message details include the following sections:

- Verdict Chart and Last State Verdicts, on page 14
- Envelope and Header Summary, on page 15
- Sending Host Summary, on page 16
- Processing Details, on page 16

Verdict Chart and Last State Verdicts

A Verdict Chart displays information of the various possible verdicts triggered by each engine of the email security appliance.

Note Verdict charts for AsyncOS prior to 12.0 will not be displayed and last state verdicts is displayed as "Last State Not Available".

The following table shows the various verdicts of each engine:

Table 1: Verdict Charts

Connection Behavior	Message Filter	Anti-Spam	Anti-Virus	AMP	Graymail	Content Filter	Outbreak Filter	DLP
Not Applicable Accepted Relayed	Not Evaluated Match No Match	Not Evaluated Negative Suspect Bulk Mail Social Mail Marketing Mail Positive	Not Evaluated Negative Repaired Encrypted Unscanable Positive	Not Evaluated Clean FA Pending Unknown Skipped Malicious Unscannable Low Risk	Not Evaluated Negative Positive	Not Evaluated Match No Match	Not Evaluated Match No Match	Not Evaluated No Trigger Violation No Violation

The Last State verdict of the message determines the final verdict that is triggered after all the possible verdicts of each of the engine in your appliance.

Following are some of the last state verdicts:

- **Delivered**: When a message is delivered.
- **Dropped**: When a message is dropped.
- **Aborted**: When a message is aborted. (Example: Due to Mail Policy restrictions)
- **Bounced**: When a message is bounced back.
- **Splintered**: When the MID of a message is split into multiple MIDs having multiple final states.
- **Quarantined**: When a message is quarantined by engines.
- **Queued**: When a message is queued for delivery either to end recipient or to an off-box Spam quarantine or Centralized Policy, Virus or Outbreak quarantine.
- **Processing**: When a message is not completely processed by all the engines; or when a message is waiting in a queue of a particular engine.
- **Last State Not Available**: When last state of message cannot be retrieved. (Example: When message is still being processed by the engine and has not reached any final state.

Envelope and Header Summary

This section displays information from the message envelope and header, such as the envelope sender and recipients. It includes the following information:

Received Time: Time that the Email Security appliance received the message.

MID: Message ID.

Subject: Subject line of the message.

The subject line in the tracking results may have the value "(No Subject)" if the message does not have a subject or if the Email Security appliances are not configured to record the subject lines in log files.

Envelope Sender: Address of the sender in the SMTP envelope.

Envelope Recipients: Addresses of the recipients in the SMTP envelope.

Message ID Header: "Message-ID:" header that uniquely identifies each email message. It is inserted in the message when the message is first created. The "Message-ID:" header can be useful when you are searching for a particular message.

Cisco Host: Email Security appliance that processed the message.

SMTP Auth User ID: SMTP authenticated user name of the sender, if the sender used SMTP authentication to send the email. Otherwise, the value is "N/A."

Attachments: The names of files attached to the message.

Sender Group: The sender group that received the message.

Message Size: The size of the message.

Policy Match (Incoming or Outgoing): The policy that received the message.

Note If the engine is not able to fetch the details, the value is displayed as "N/A".

Sending Host Summary

Reverse DNS Hostname: Hostname of the sending host, as verified by reverse DNS (PTR) lookup.

IP Address: IP address of the sending host.

SBRS Score: (SenderBase Reputation Score). The range is from 10 (likely a trustworthy sender) to -10 (apparent spammer). A score of "None" indicates that there was no information about this host at the time the message was processed.

Processing Details

This section displays various logged status events during the processing of the message.

Entries include information about mail policy processing, such as anti-spam and anti-virus scanning, and other events such as message splitting.

If the message was delivered, the details of the delivery appear here. For example, a message may have been delivered and a copy kept in quarantine.

The last recorded event is highlighted in the processing details.

Summary Tab

This tab displays the summary logs of all the events during the processing of message.

DLP Matched Content Tab

This tab displays content that violates Data Loss Prevention (DLP) policies.

Because this content typically includes sensitive information, such as corporate confidential information or personal information including credit card numbers and health records, you may want to disable access to

this content for users who have access, but not Administrator-level access, to the Security Management appliance. See Controlling Access to Sensitive Information in Message Tracking.

URL Details Tab

This tab displays only for messages caught by URL Reputation and URL Category content filters and by outbreak filters not message filters.

This tab displays the following information:

- The reputation score or category associated with the URL
- The action performed on the URL (rewrite, defang, or redirect)
- If a message contains multiple URLs, which URL has triggered the filter action.

You can see this tab only if you have configured your Email Security appliance to display this information. See *User Guide for AsyncOS for Cisco Email Security Appliances* .

To control access to this tab, see Controlling Access to Sensitive Information in Message Tracking

SMTP Log Tab

This section displays a log of messages when the sender of the email fails SMTP authentication.

AMP Log Tab

This section displays a log of messages caught by the Advanced Malware Protection file reputation and file analysis service.

Troubleshooting Message Tracking

- Expected Messages Are Missing from Search Results , on page 17
- Attachments Do Not Appear in Search Results , on page 17

Expected Messages Are Missing from Search Results

Problem

Search results did not include messages that should have met the criteria.

Solution

- Results for many searches, especially Message Event searches, depend on your appliance configuration. For example, if you search for a URL Category for which you have not filtered, no results will be found, even if a message contains a URL in that category. Verify that you have configured the Email Security appliance properly to achieve the behavior that you expected. For example, check your mail policies, content and message filters, and quarantine settings.
- See Checking Message Tracking Data Availability , on page 5.

Attachments Do Not Appear in Search Results

Problem

Attachment names are not found and displayed in search results.

Solution

At least one incoming content filter or other body scanning feature configured and enabled on the ESA. See configuration requirements at Enabling Centralized Email Tracking on the Legacy Web Interface, on page 3 and limitations for attachment name searches in Tracking Service Overview.

Exporting Message Service

You can view additional fields to perform analysis and investigation on related mails using the Export file option along with messages.

Procedure

Step 1 Choose **Tracking** > **Messages.**

Step 2 Select your criteria.

Step 3 Click **Export**.

You can view additional fields to perform analysis and investigation on related mails using the Export file option along with the message. The additional fields you can view include:

- Message Size- The size of the message.
- Attachment Details- The name of the files attached to the message.
- Delivery Details- Delivery information, such as the number of messages from a particular domain that were bounced.
- Source IP/FQDN- The IP address of the sender.
- Sender Group- The sender group that received the message.
- DKIM, SPF, or DMARC Status- Authentication method to verify if the email was actually sent by the owner.
- URL List- Cisco Secure Email and Web Manager displays only 1024 characters of the URL.