Tracking Messages

This chapter contains the following sections:

Message Tracking Overview

Message tracking helps resolve help desk calls by giving a detailed view of message flow. For example, if a message was not delivered as expected, you can determine if it was found to contain a virus or placed in a spam quarantine — or if it is located somewhere else in the mail stream.

You can search for a particular email message or a group of messages that match criteria that you specify.

Note You cannot use message tracking to read the content of messages.

Enabling Message Tracking

Note Message tracking data is preserved only for messages that are processed after you enable this feature.

Before you Begin

- In order to search for and display attachment names in Message Tracking and view attachment names in log files, you must configure and enable at least one body scanning process, such as a message filter or content filter.

- To support searching by subject, log files must be configured to record subject headers. For more information, see Logging.
- If you are setting up Centralized Tracking: Set up your Cisco Secure Manager Email and Web Gatewayto support centralized message tracking for this email gateway. See the Cisco Secure Manager Email and Web Gateway User Guide.

Procedure

Step 1 Click **Security Services > Message Tracking**.

Use this path even if you do not plan to centralize this service.

Step 2 Select **Enable Message Tracking Service**.

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

Step 4 Choose a Message Tracking Service:

Option	Description
Local Tracking	Use message tracking on this email gateway.
Centralized Tracking	Use Cisco Secure Manager Email and Web Gateway to track messages for multiple email gateways including this one.

Step 5 (Optional) Select the check box to save information for rejected connections.

For best performance, leave this setting disabled.

Step 6 Submit and commit your changes.

What to do next

If you selected Local Tracking:

- Choose who can access content related to DLP violations. See Controlling Access to Sensitive Information in Message Tracking.
- (Optional) Adjust the disk space allocation for storing messages. See Managing Disk Space.

Searching for Messages on the Legacy Interface

Procedure

Step 1 Choose **Monitor > Message Tracking**

Step 2 Enter search criteria.

- To view all options, click the **Advanced** link.

- Tracking does not support wildcard characters or regular expressions.
- Tracking searches are not case sensitive.
- Unless otherwise specified, the query is an "AND" search: The query returns messages that match *all* 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.
- Search criteria include:

Option	Description
Envelope Sender	Select **Begins With**, **Is**, or **Contains**, then enter an email address, username, or domain of a message sender to find. You can enter any character(s). No validation of your entry is performed.
Envelope Recipient	Select **Begins With**, **Is**, or **Contains**, and enter an email address, username, or domain of a message recipient to find. You can enter any character(s). No validation of your entry is performed.
Subject	Select **Begins With**, **Is**, or **Contains**, and enter a text string to search for in the message subject line. **Warning**: Do not use this type of search in environments where regulations prohibit such tracking.
Message Received	Specify a date and time range. 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. Use the local date and time that the message was received by the email gateway.
Advanced options:	
Sender IP Address/ Domain / Network Owner	Specify the IP address, domain, or network owner of a remote host. You can search within rejected connections only or search all messages.

Option	Description
Attachment	Select **Begins With**, **Is**, or **Contains**, and enter an ASCII or Unicode text string for one attachment to find. Leading and trailing spaces are *not* stripped from the text you enter. You can search for messages by attachment filenames only if you have performed: • Body scan using a message filter • Body scan using a content filter • Advanced Malware Protection (AMP) scan. For more information about identifying files based on SHA-256 hash, see Identifying Files by SHA-256 Hash. You can search for messages that are detected as malicious by the Advanced Malware Protection engine based on the threat name. In the **Threat Name** field, enter *Simple_Custom_ Detection* or *Custom_Threshold* to search for messages that are detected as malicious based on the Custom Detection and Custom Threshold categories. You can also search for messages by the virus name if a particular file is detected as virus positive by the Advanced Malware Protection engine.
Message Event	Select one or more message processing events. For example, you can search for messages that have been delivered, quarantined, or hard bounced. Message events are added with an "OR" operator: Selecting multiple events finds messages that match *any* of the conditions you specify.
Message ID Header	Enter a text string for the SMTP Message-ID header. This RFC 822 message header uniquely identifies each email message. It is inserted in the message when the message is first created.
Cisco IronPort MID	Enter a message number to search for. An IronPort MID uniquely identifies each email message on the email gateway.
Cisco IronPort Host	Select an Email Security appliance to restrict the search to messages processed by that email gateway, or select all email gateways.

Step 3 Click **Search** to submit the query.

The query results are displayed at the bottom of the page.

What to do next

Related Topics

- Working with Message Tracking Search Results , on page 7

Searching for Email Messages on the New Web Interface

The tracking service of the email gateway 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 Click **Tracking** tab.

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 email gateway, they are displayed in the local time of the email gateway.

  Messages appear in the results only after they have been logged on the email gateway and retrieved by the Cisco Secure Email and Web Gateway. 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 gateways, 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 gateways or select the required email gateway 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. For example, you can search for messages that have been delivered, quarantined, or hard bounced. Message events are added with an “OR” operator: Selecting multiple events finds messages that match any of the conditions you specify.

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 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.

What to do next

- Working with Message Tracking Search Results , on page 7

Working with Message Tracking Search Results

Keep the following points in mind:

- Messages appear in the results only after they have been logged on the email gateway and retrieved by the Cisco Secure Manager Email and Web Gateway. 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.
- For information about searches involving Advanced Malware Protection (file reputation scanning and file analysis), see About Message Tracking and Advanced Malware Protection Features.

Actions you can take when working with search results:

- Show more than 250 search results by returning to the search criteria, clicking Advanced, scrolling to the Query Settings, and setting the maximum number of results to 1000.
- Show more results per page by choosing an option from the top right side of the search results section.
- Navigate through multiple pages of search results from the top right side of the search results section.
- Narrow your search results by floating the cursor over a value in the search results that you want to add as a condition. If an orange highlight appears, you can click that value to narrow the search by that criterion. This adds the additional criterion to the search criteria. For example, if you search for messages sent to a particular recipient, you can then click on a sender name in the search results to find all messages to that recipient from that sender within the time range (and meeting any other criteria) that you originally specified.
- If more than 1000 messages match your search criteria, you can click Export All (a link at the top right of the search results section) and export up to 50,000 search results as a comma-separated values file and work with the data in another application.
- View more details for a message by clicking Show Details in the row for that message. A new browser window opens with the message details.
- For quarantined messages, you can click a link in the message tracking search results to view details such as the reason the message was quarantined.
- Remediate the malicious messages from the user mailbox using the Mailbox Search and Remediate action. For more information, see Search and Remediate Messages in the Mailboxes

Note If you clicked a link in a report page to view message details in Message Tracking, and the set of results is not what you expected, this can occur if reporting and tracking were not both simultaneously and continuously enabled during the time period you are reviewing.

Related Topics

- Message Tracking Details , on page 8

Message Tracking Details

Item	Description
Envelope and Header Summary section:	
Received Time	Time that the email gateway received the message. Dates and times are displayed using the local time configured on the email gateway.
MID	Unique IronPort message ID.
Message Size	Message size.
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 log files are not configured to record subject headers. For more information, see Logging
Envelope Sender	Address of the sender in the SMTP envelope.
Envelope Recipients	If your deployment uses the alias table for alias expansion, the search finds the expanded recipient addresses rather than the original envelope addresses. For more information about Alias Tables, see "Creating Alias Tables" in the "Configuring Routing and Delivery Features" chapter . In all other cases, message tracking queries find the original envelope recipient addresses.
Message ID Header	The RFC 822 message header.
SMTP Auth User ID	SMTP authenticated username of the sender, if the sender used SMTP authentication to send the message. Otherwise, the value is "N/A."

Item	Description
Attachments	The names of files attached to the message. Messages that contain at least one attachment with the queried name will appear in the search results. 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. Situations in which an attachment name will not appear in search results 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. For performance reasons, the names of files within attachments, such as OLE objects or archives such as .ZIP files, are not searched.
[New Web Interface Only] **Message Event**	Select multiple events to include messages that match each event type.
Sending Host Summary section	
Reverse DNS Hostname	Name of the sending host, as verified by reverse DNS (PTR) lookup.
IP Address	IP address of the sending host.
IP Reputation **Score**	IP 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. For more information about IP Reputation Service, see IP Reputation Filtering
Processing Details section	
Summary information (If one of the tabs below is displayed, this information is displayed in a tab. Summary information always displays.)	The Summary tab displays status events logged 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 and custom log entries added by a content or message filter. If the message was delivered, the details of the delivery are displayed here. The last recorded event is highlighted in the processing details.

Item	Description
DLP Matched Content tab	This tab displays only for messages that were caught by DLP policies. This tab includes information about the match, as well as the sensitive content that triggered the DLP policy match. You must configure the email gateway to display this information. See Displaying Sensitive DLP Data in Message Tracking. To control access to this tab, 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. 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 must configure the email gateway to display this information. See Displaying URL Details in Message Tracking. To control access to this tab, see Controlling Access to Sensitive Information in Message Tracking.

Related Topics

- Searching for Messages on the Legacy Interface , on page 2

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] Click the gear icon on the upper right corner of the page to load the legacy web interface.

Step 2 Select **Monitor** > **Message Tracking**.

Step 3 Look for **Data in time range:** in the upper right corner of the Search box.

Step 4 Click the value shown for **Data in time range:**.

What to do next

Related Topics

• About Message Tracking and Upgrades , on page 11

About Message Tracking and Upgrades

New message tracking features may not apply to messages that were processed before upgrade, because the required data may not have been retained for those messages. For possible limitations related to message tracking data and upgrades, see the Release Notes for your release.

Troubleshooting Message Tracking

Related Topics

• Attachments Do Not Appear in Search Results , on page 11
• Expected Messages Are Missing from Search Results , on page 11

Attachments Do Not Appear in Search Results

Problem

Attachment names are not found and displayed in search results.

Solution

See configuration requirements at Enabling Message Tracking, on page 1 . Also see limitations for attachment name searches in Message Tracking Details , on page 8.

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, and especially searches that involve Message Events, depend on your email gateway 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 gateway properly to achieve the behavior that you expected. For example, check your mail policies, content and message filters, and quarantine settings.
- If expected information is missing after you clicked a link in a report, see Troubleshooting Email Reports.