Track and Trace Administrator Guide

Draft extracted 2011-2-14 2:16

Symantec

Track and Trace

This document includes the following topics:

- About Track and Trace
- Logging On and Off ClientNet
- Locating the Track and Trace pages
- Searching for details of an email
- Viewing the results of a search
- Viewing the details of an email
- Enabling a non-Administrator to use Track and Trace

About Track and Trace

Track and Trace enables you to search the details of a specific email and to see if and when your Email Security services process it.

Track and Trace uses the criteria you provide to search for details of the emails that are sent to and from your organization. You can then select an entry from the results page to view more information.

The search results page shows the email delivery date and time. The page also shows details of your Email Security service that intercepted the email e.g. Email Content Control.

You can find Track and Trace in ClientNet under the **Tools** tab.

Track and Trace offers two methods of searching for details of a specific email; standard search and message ID search.

- **Search** - You can search by:

- Sender's email address
- Recipient's email address
- Date and time range
- Subject line
- Attachment file name
- Receiving Server IP address
- Sending Server IP address
- Service e.g. Email Content Control
- Helo string
- Attachment MD checksum

- **Search by ID** – You can search by the message ID generated by the email client. This search pinpoints an individual email.

Your Email Security service does not store copies of any emails that pass through its infrastructure but logs key information about each email when it is processed. The details that Track and Trace provides include:

- Whether and when an email was received onto the Email Security infrastructure.
- Whether and when one of your Email Security services accepted the email.

Note: Address Registration rejects emails that are sent to an address in your domains that are not on a database of known valid email addresses. Emails that are sent to an unregistered address are not accepted and generate error SMTP 550. SMTP Error 550 indicates to the sending mail server that the address is invalid. If the recipient email address is not included in your list of valid addresses, Address Registration rejects the email.

- Whether and when the email was delivered successfully, or in the event of an unsuccessful first delivery attempt, whether retry attempts are in progress.
- When the first delivery attempt and the final delivery attempt were made.

Track and Trace enables you to search for the emails that have been processed within the last 30 days. An email is typically searchable within 30 minutes of entering the Email Security infrastructure.

ClientNet enforces a strict security policy within Track and Trace to ensure that you can only search for details of the emails that you have rights to view. The policies are based on:

- The organization you work for.
- The access privileges that are associated with your ClientNet login ID.
- Your Track and Trace user role.

Administrators with the Edit Configuration permission have access to Track and Trace. In addition, an Administrator can grant other users with permission to use Track and Trace.

Note: Track and Trace access applies across all of the domains that are provisioned for your account.

Logging On and Off ClientNet

To log on to ClientNet, you need a user name and password.

ClientNet is located at:

https://clients.messagelabs.com/

To log on to ClientNet

1. Enter your user name.
2. Enter your password.
3. Click **Log in**.

To log out ClientNet

- From any screen in ClientNet, click the **Log Out** link at the top right of the screen.

Locating the Track and Trace pages

To locate Track and Trace:

1. Log into ClientNet.

   See "Logging On and Off ClientNet" on page 5.
2. In the top navigation bar, click **Tools**.
3. Click **Track & Trace**.

The Track and Trace section in the ClientNet portal presents two tabbed options: **Search** and **Search by ID**.

Searching for details of an email

To be able to search, you must specify one of the following criteria:

- Sent to (recipient's email address).
- Sent from (sender's email address).
- Subject line.

To search for an email

1. Click **Tools.**
2. Select **Track and Trace**.
3. Enter your search criteria as described in the table below. If you know the Message ID of the email, you can select **Search by ID**.
4. Select **Show All** to display additional search options, if required.
5. Select how you want to receive your results (on screen or by email).
6. Click **Search**

You can choose to view your results on-screen or to have them emailed to you.

To request the results to be emailed to you in CSV format

1. Select **Email the results as a CSV file**, at the bottom of the search page.
2. Enter a valid email address.
3. Create a password for your CSV file.

Table 1-1 Search criteria

Sear ch options	Description
Sent to	If you know the recipient of the email, you can search by entering the recipient's email address. The asterisk wildcard is supported. Please note *@* is not supported. The maximum field length is 255 characters.
Sent from	If you know the sender of the email, you can search by entering the sender's email address. The asterisk wildcard is supported. Please note *@* is not supported. The maximum field length is 255 characters.
Subject line	If you know the subject line of the email, you can search by entering this parameter. If you only know part of the subject line, this field has a drop-down menu with three options to choose from: "Contains"; "Begins with" and "Ends with". The asterisk wildcard is not supported.

Table 1-1 Search criteria *(continued)*

Sear ch options	Description
Attachment file name	If you know that the email contained an attachment, you can search by entering the name of the attachment file. The asterisk wildcard is supported. You can also use the wildcard, if you only know the file extension of the attachment e.g. *.ppt. The maximum field length is 255 characters.
Select specific date and times	Specify the time range for your search. Track and Trace enables you to search for emails processed within the last 30 days . An email is typically searchable within 30 minutes of it entering the infrastructure.
Receiving Server IP/Hostname	If you know the IP address or host name of the receiving mail server, you can search using this information. Wildcards are not supported and the maximum field length is 255 characters.
Sending Server IP	If you know the IP address of the sending mail server, you can search using this information. Wildcards are not supported. Please note: You cannot search using the sending host name details.
Service	If you suspect that an email may have been intercepted by one of your email security services, you can search by the name of the service e.g. Email Content Control.
Helo string	You can use the Helo string as one of your search parameters (part of the SMTP receiving server identification process). Asterisk wildcards are not supported.
Attachment MD5 checksum	If you know the unique MD5 checksum string for an email attachment, you can search using this information. The Checksum field must contain 32 alphanumeric characters.

To identify a specific email, we recommend that you provide as much information as possible when defining your search criteria.

Your search criteria remains on screen when your results are displayed, enabling you to refine your search if necessary.

To modify a search

1. Click on the **Modify Search** link in the results page.
2. Add or amend search criteria as required.
3. Click **Search** to submit your new search.

Viewing the results of a search

The results are available in ClientNet for 24 hours. If you cannot find the specific record that you looked for in the results provided, refine your search criteria and try again.

When your search results are displayed on the screen, you can download them in CSV format.

You also have the opportunity to have your search results emailed to you, while your search is in progress. You need to enter a valid email address and to create a password for your CSV file.

The **Search Results** page displays a list of entries that match your search criteria.

If an email was sent to multiple recipients, each instance of the email is shown in the list.

For each email, the following information is displayed:

- **Subject** – the subject line of the email.
- **Sent from** –email address of the sender.
- **Sent to** – email address of the recipient.
- **Accepted** – the date and time when the mail was received onto the infrastructure.
- **Delivered** The date and time the email when the email was delivered.

To sort the results

- Click on the column heading on the results page to sort your results.

To download the results in CSV format

- Select **Download results (CSV)**, at the top of the results page.

Viewing the details of an email

You can view detailed information about a specific email by clicking on a row in your list of results.

A green tick means that the delivery was successful, whilst a red cross indicates that an email has been blocked or cannot be delivered.

Note: Emails that are blocked prior to reaching our infrastructure will not be included in the Track and Trace results.

To view full delivery information

1 Select **Tools > Track and Trace.**.

Enter your search criteria and submit your search.

2 When you have received your search results, click on the required entry in the results page. A pop-up window displays the **Delivery detail** tab.

3 Click on the **Attachments** tab for information about any email attachment.

The following table describes the details that are provided in the **Delivery** tab:

Table 1-2 Delivery details

Detail	Description
Sent from	The email address of the sender
Sent to	The email address of the recipient
Subject	The subject line of the email
Email Size	The total size of the email, including any attachments
Message ID	The message ID as shown in the header of most emails
Helo	The Helo string identifies the sending SMTP server
The sending server	The IP address of the sending mail server
Accepted	Whether and when the email was accepted to the infrastructure. An inbound email may not be accepted for scanning by your Email Security services. For example, SMTP heuristics or Address Registration may block an email.
Scanning service	If the email triggered one or more of your Email Security services, the service that applied the most severe action is detailed here
Delivery Result	Whether the email was delivered successfully, the date and time of the first and last delivery attempts and the details of the receiving mail server

Enabling a non-Administrator to use Track and Trace

You can enable a ClientNet user who is not an Administrator to use Track and Trace.

To enable a user for Track and Trace

- Click **Administration > User Management**, first add the new user and then assign the Track and Trace custom role to them.