



How to search and analyse email data with Egress Investigate

Egress Investigate helps administrators and end-users search and report on plaintext and encrypted message contents and attachments, then leverage that data to meet compliance requirements and improve organisational security policy.

In Egress Investigate, data investigations are conducted by creating **scopes**, which are parameters that refine searches of the data in the source email archive. This guide shows administrators how to start a new investigation, create a scope, view results and understand the resulting analytics.

Starting a new investigation

1. To start a new investigation, first sign in to **Egress Investigate** via a web browser.
2. At the main dashboard, choose Investigation scopes then press the **Create New Scope** button.

Investigations work by narrowing down the data according to the scope of the search. There are many parameters available to you for finding the intended data.

The screenshot displays the 'INVESTIGATION SCOPES' section of the Egress Investigate interface. On the left, a sidebar menu includes options like Dashboard, Messages, My messages, Investigations, Investigation scopes, PST import, Audit, Documents, Reports, GDPR, and Other. The main content area shows a list of active investigation scopes, such as 'All variants of employment con', 'Variants of Contract', and 'Emails with NI and postcode - N'. A 'Create Investigation Scope' button is visible in the top right. The 'DETAILS' form for creating a new scope includes the following fields and options:

- Scope name:** A text input field.
- Description:** A text input field.
- Assigned to:** A dropdown menu with 'john.doe@company.com' selected and an 'Add' button.
- Expires at:** A date and time field set to '24/10/2019 10:27' with a trash icon.
- Scope permissions:** A list of checkboxes:
 - Run analysis and report
 - List messages
 - View message contents
 - Download messages
 - Decrypt messages
- Search Query:** A text input field.
- Senders:** A text input field with a placeholder '*@*' and a trash icon.
- Recipients:** A text input field with a placeholder '*@*' and a trash icon. Below it is a checkbox for 'Must contain all these recipients'.
- Date ranges:** A text input field with a placeholder 'Date ranges separated by comma e.g. 2001..2002, 2013-Feb..2013-Feb'.
- Archived before:** A date and time field set to '24/10/2018 10:27' with a trash icon.
- With All Tags:** A text input field.

3. Choose a name and description for the investigation scope, as well as the users permitted to search within the scope. Put an expiry date on the search if required.

4. Scope permissions represent the actions administrators are permitted to perform with the results of the search. Choose the actions you wish to perform.

5. Add any specific search terms and any sender or recipient email addresses to display results for. Wildcards are allowed here, e.g. "*@egress.com."

Senders	*@* x
Recipients	*@egress.com x

6. Choose a date range to investigate.

7. After filling out all of the search fields, press **Review and Create**.

Review And Create

Back To List

8. After reviewing the search scope, press **Create**. The investigation scope may require approval from other administrator-level users.

Approving investigation scopes

Investigations awaiting final approval are found under the Pending tab in the Investigation scopes menu.

Egress Secure Vault

Dashboard

Messages

My messages

Investigations

Investigation scopes

PST import

Audit

INVESTIGATION SCOPES

ACTIVE PENDING SYSTEM EXPIRED OR DELETED

These scopes require additional votes to be completely approved.

Subject Access Request

Created by john.doe@company.com at 24/10/2018 17:38

To review a scope:

1. Find the scope in the **Pending** section and select it.

2. Examine the parameters of the search and the permissions to be granted.

3. If the investigation is acceptable, press **Review and Vote**, then press **Vote** in the confirmation box.

Review scope

You are about to vote for investigation scope 'Pending Example'.

In this scope there are **804,356** messages, **119** of those are encrypted, sent between **31/03/1614 02:40** and **09/04/2107 01:15** by **306,524** senders.

After voting, scope will be allowed to:

- Run analysis and report
- List messages
- View message contents
- Download messages
- Decrypt messages

Cancel Vote

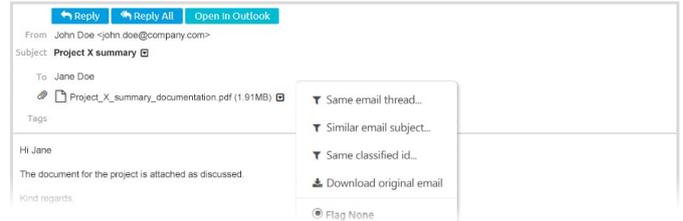
Viewing the results

1. When an investigation has been approved, access it by going to **Investigations**.

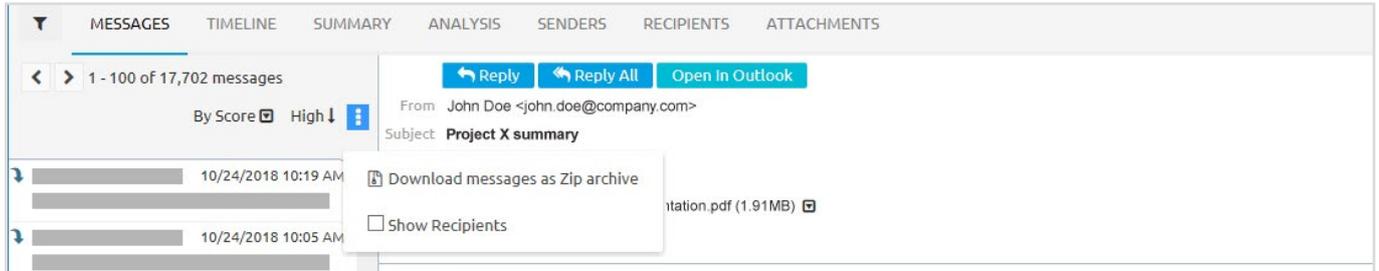
2. The relevant messages will be displayed, with search terms highlighted in the content.

1 - 11 of 11 messages		By Score	High ↓
↑ john.smith@egressdemo.com	Conference call notes	Tue, Jan 24	3.4KB
↑ john.smith@egressdemo.com	Our meeting	Tue, Jan 24	5.7KB
↑ jane.smith@egressdemo.com	Email address	Tue, Jan 24	3.6KB
↑ jane.smith@egressdemo.com	Urgent	Tue, Jan 24	3.4KB
↓ john.smith@egressdemo.com	Quick question	Tue, Jan 24	7.7KB

Email attachments are downloadable via the drop down arrow next to the file.

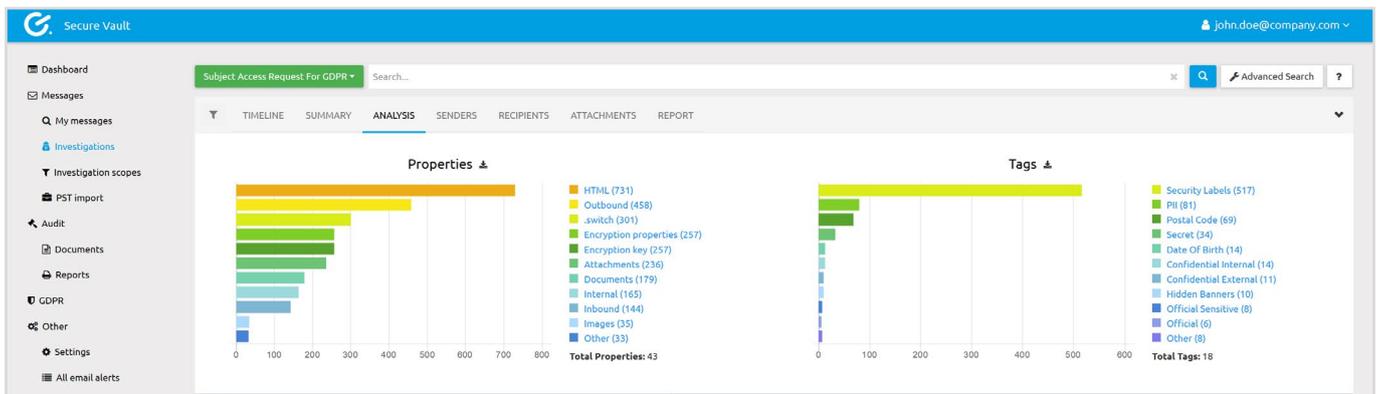


3. To download the emails discovered in the search, select the options icon and then choose **Download messages as Zip archive**.



4. To view analytics, use the tabs above the email inbox. All charts and graphs can be clicked on and drilled down for further refined results. Analytics are organised into the following tabs:

- **Timeline** shows a chart of when the emails were sent.
- **Summary** provides data on various metrics, such as policy rules matches and attachment sizes.
- **Analysis** shows a chart of message properties.
- **Senders, Recipients** and **Attachments** tabs show charts concerning their respective topics.



5. Select a tab to view the corresponding analytics.

6. To view a summary report of the investigation, select the **Report** tab.

Learn more about the Egress platform

Visit www.egress.com/online-tutorials for video tutorials on using the Egress platform, including how to:

- Access a secure message
- Manage your messages and control access to them in real time
- Send large files securely
- Approve or deny access requests to secure messages

Technical support

Should you encounter any problems using Egress Investigate or have any technical questions, please contact Egress Support at www.egress.com/support.

www.egress.com | info@egress.com | 0844 800 0172 | [@EgressSoftware](https://twitter.com/EgressSoftware)