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.

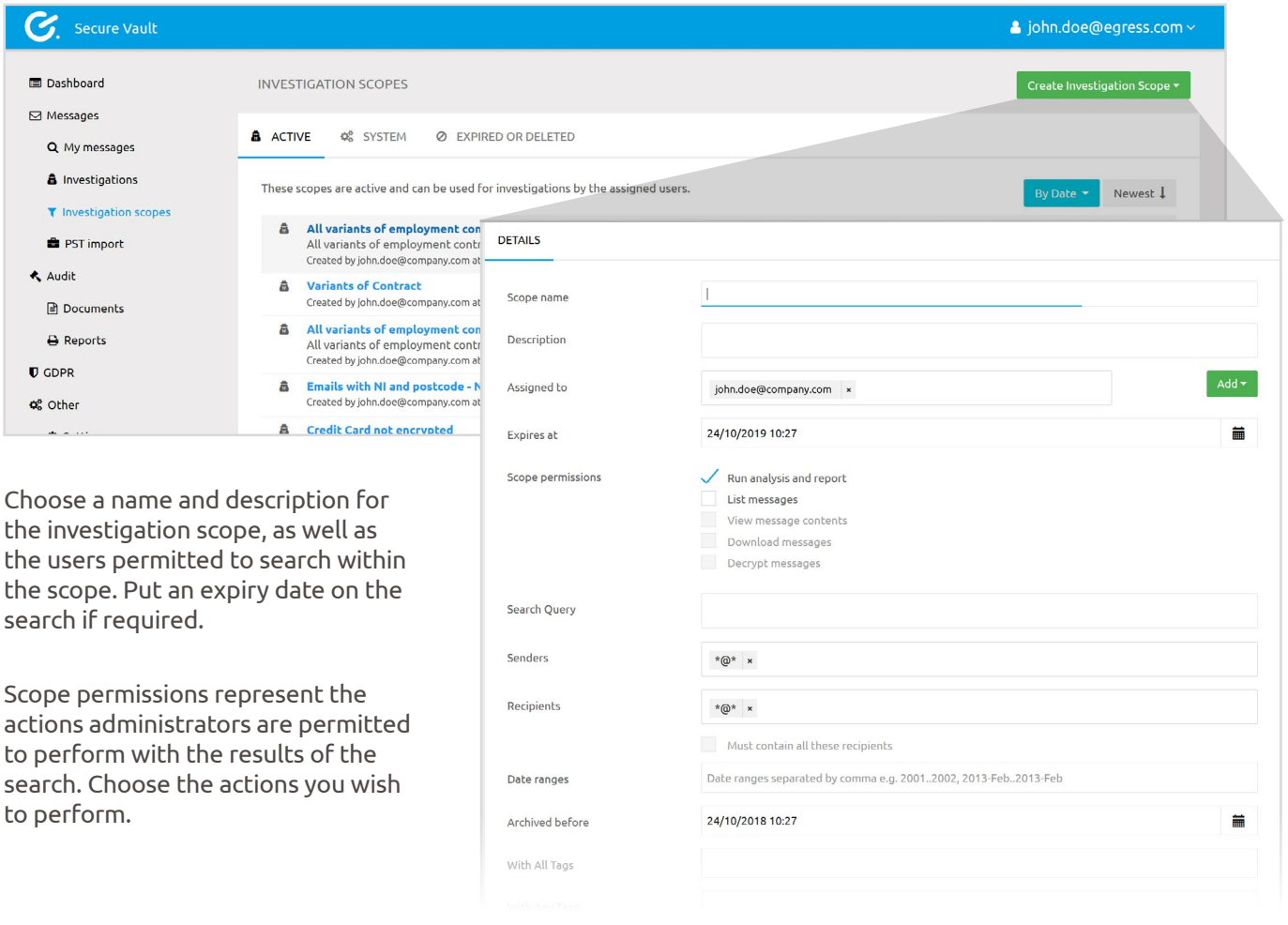
In Egress Investigate, data investigations are conducted by creating **scopes**, which are parameters that refine searches of the data in the source email archive. This guide shows administrators how to start a new investigation, create a scope, view results and understand the resulting analytics.

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.



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."

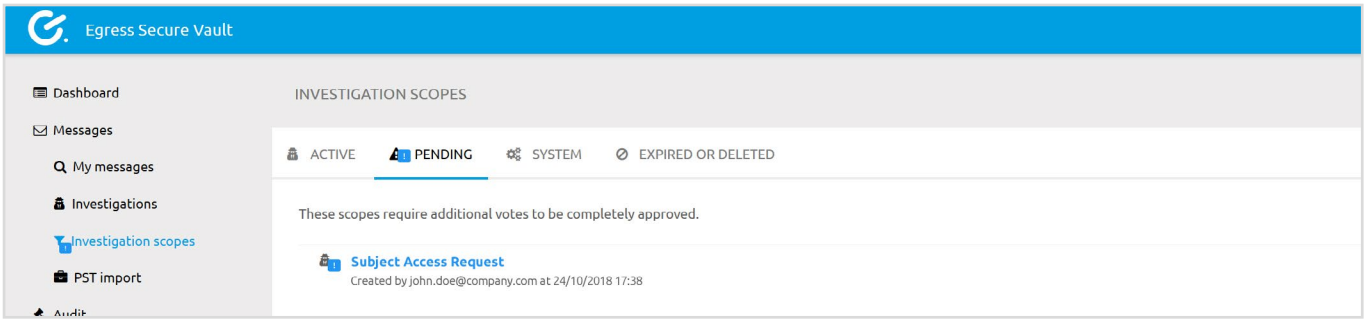
6. Choose a date range to investigate.

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

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.

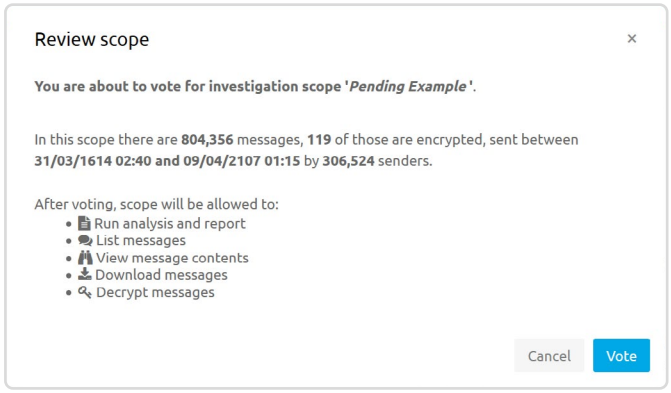


To review a scope:

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

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

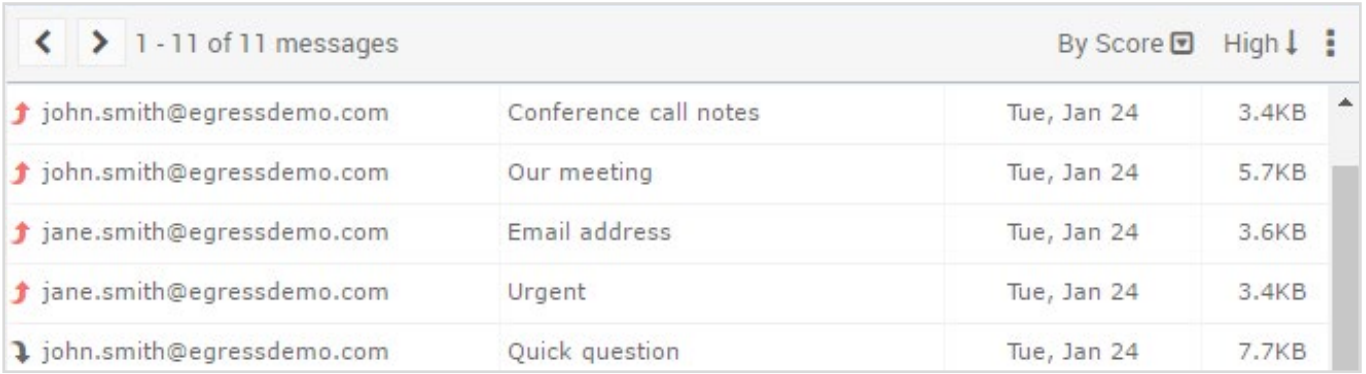
3. If the investigation is acceptable, press **Review and Vote**, then press **Vote** in the confirmation box.



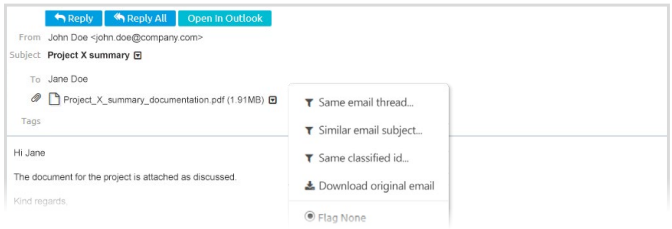
Viewing the results

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

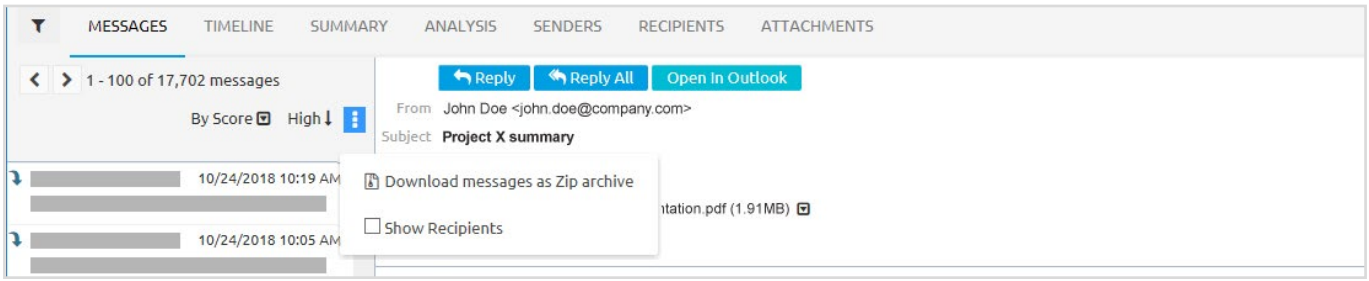
2. The relevant messages will be displayed, with search terms highlighted in the content.



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

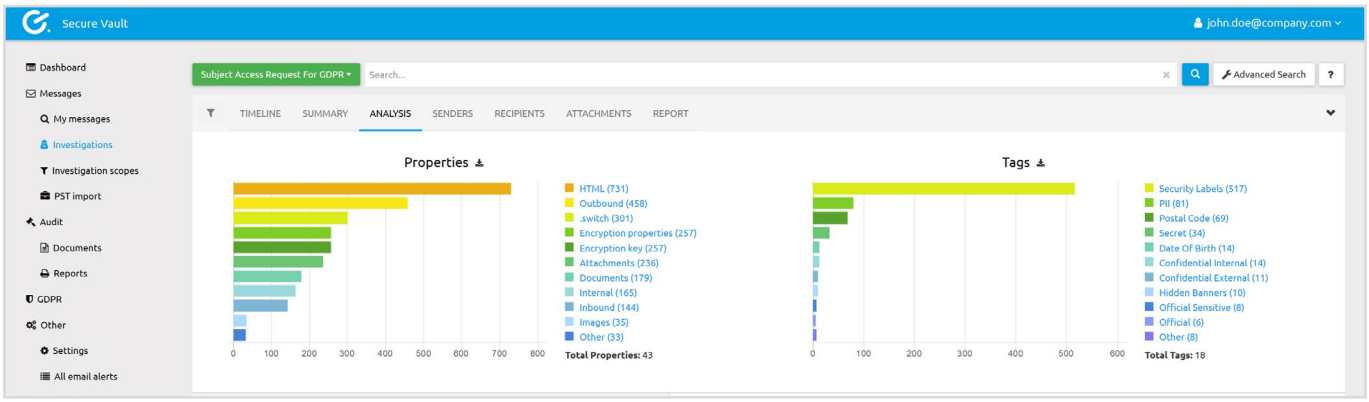


3. To download the emails discovered in the search, select the options icon and then choose **Download messages as Zip archive**.



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