Create DLP Alert on Externally Shared Google Docs in Drive

DLP (Data Loss Prevention) · https://gatlabs.com/knowledge/tech-tips/how-to-create-a-dlp-alert-on-externally-shared-google-docs-in-drive/

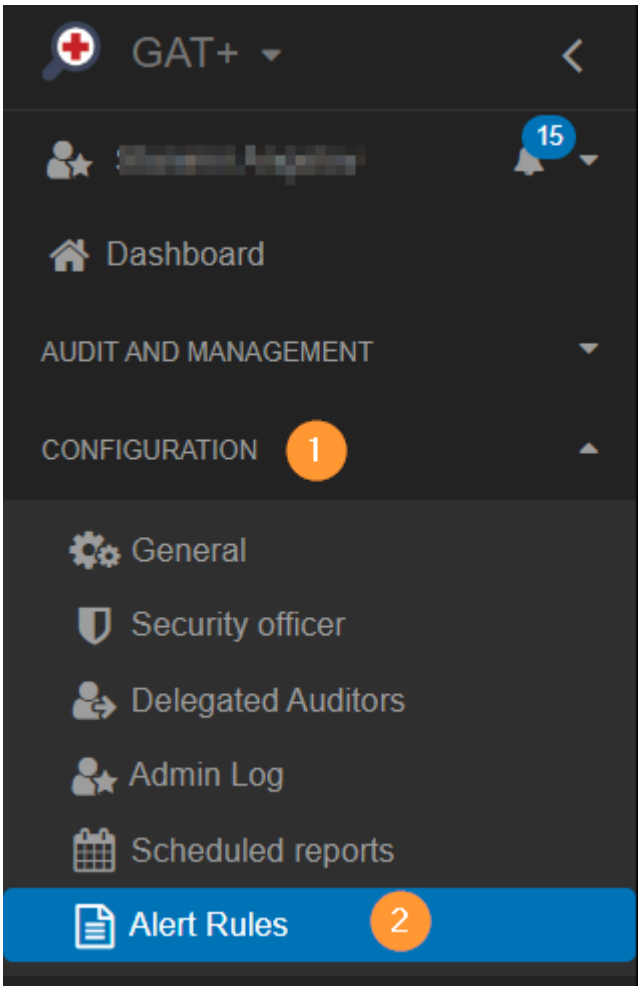
GAT+ provides an extensive and detailed audit of the entire Google drive of a domain including DLP alert.

The Admin can set up a Google DLP alert every time a document that contains sensitive information is shared outside your Google Workspace Domain.

This allows an Alert to be triggered if a regex matches a newly shared out file.

Set up alert

Navigate to **GAT+ > Configuration > Alert rules**

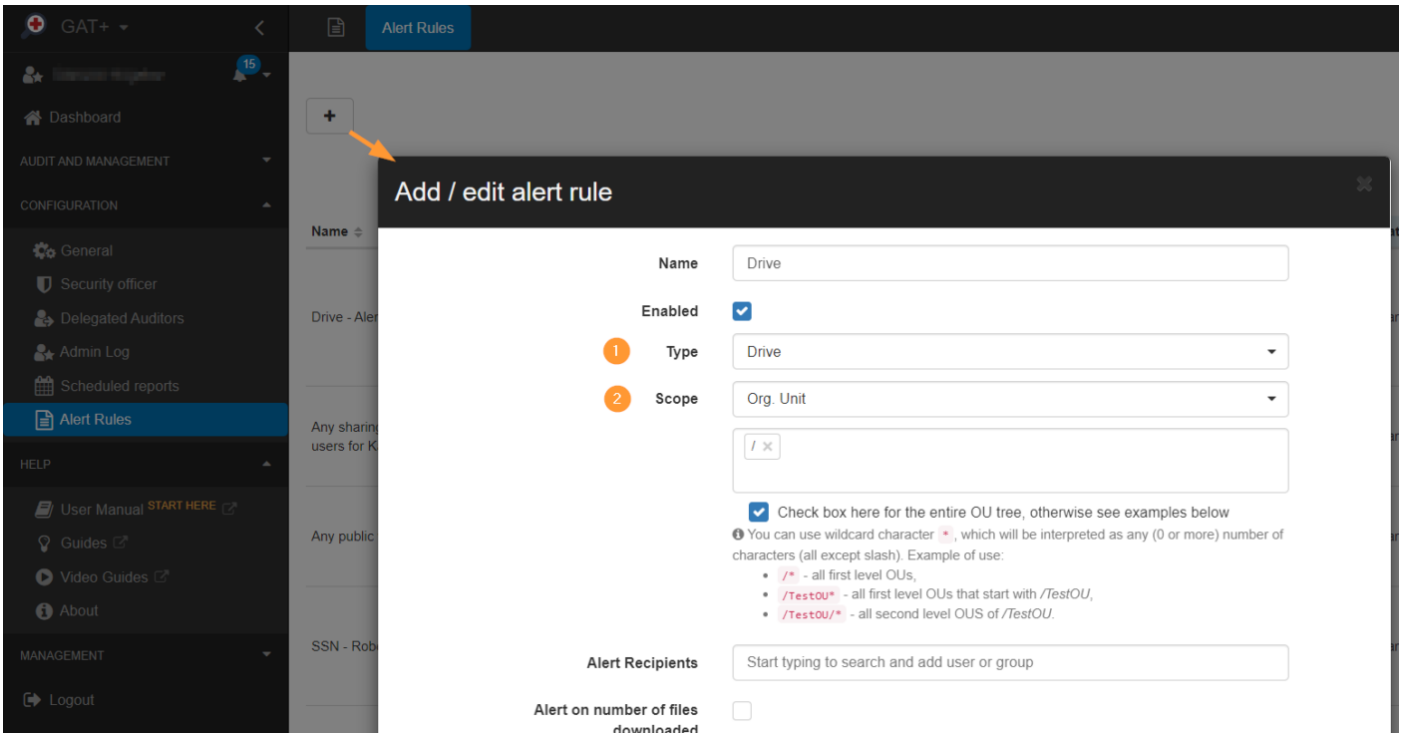


A new window will be displayed.

On the top left, click on the **+ sign.**

A new window will be displayed.

Fill in the details, and click and **Save.**

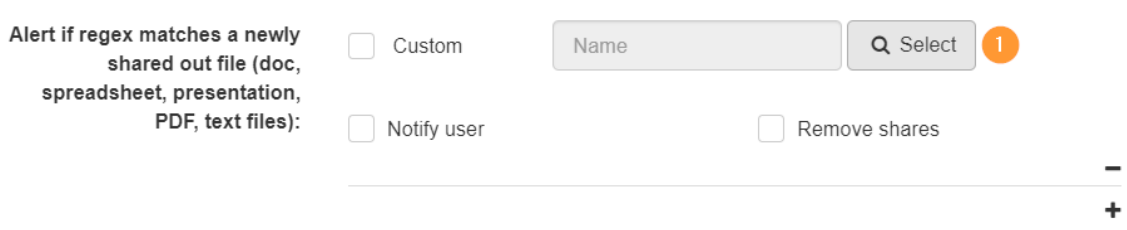


- **Name** - enter a name for the Alert rule
- **Enabled** - enable or disable the alert
- **Type** - select to create a Drive alert
- **Scope** - select to whom to apply the alert for
  - Select a user, a group, or an org. unit of users
  - **Check box here for entire OU tree** – to address all users of an organizational unit, including users of child units
- **Optional - Alert recipients** - pick and select recipients for the alert

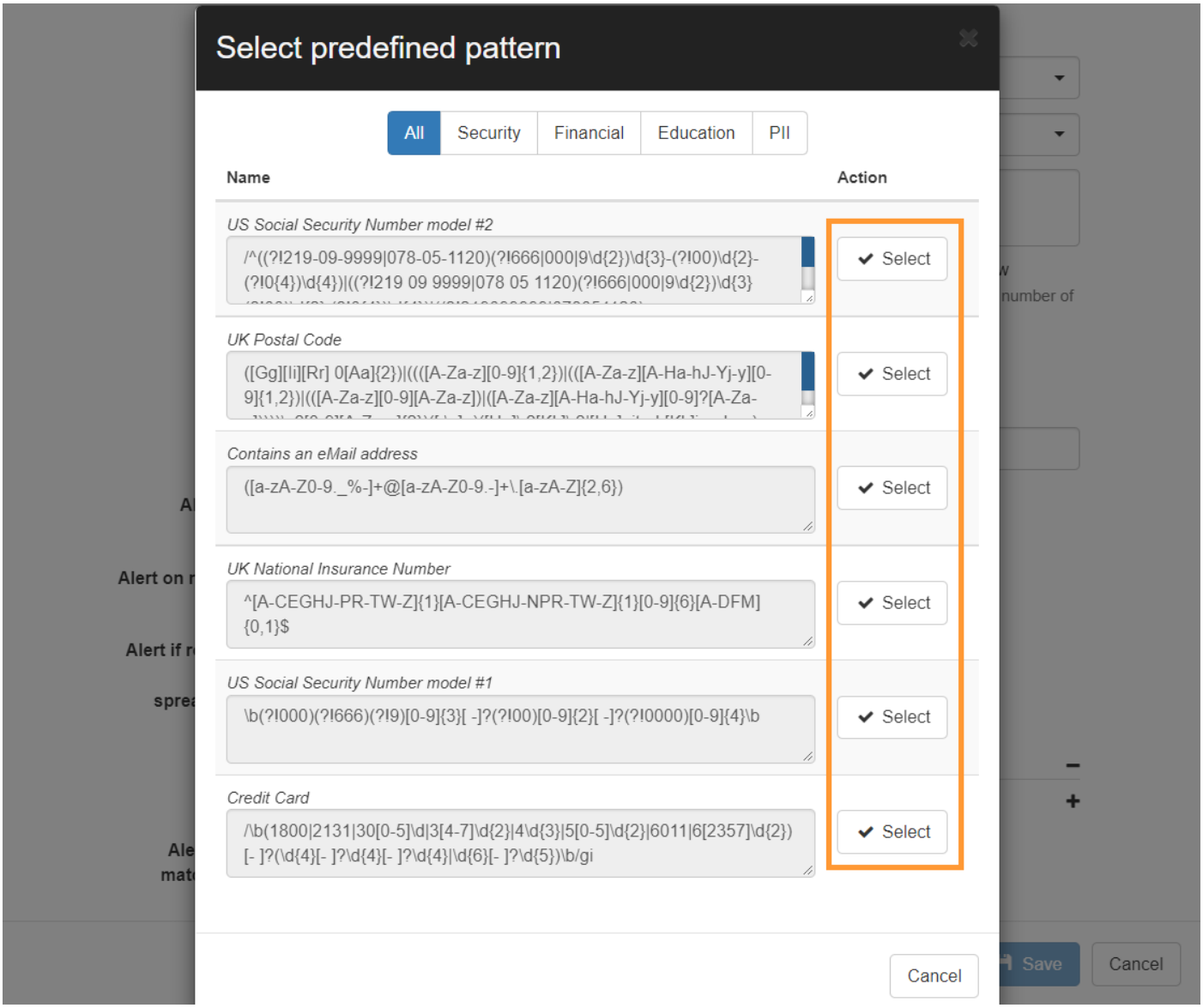
Alert on regex match

Click on the **Alert if regex matches a newly shared out file (doc, spreadsheet, presentation, PDF, text files)**:

Click on the "**Select**" button.



A new window will be displayed **Select predefinded regex patterns**

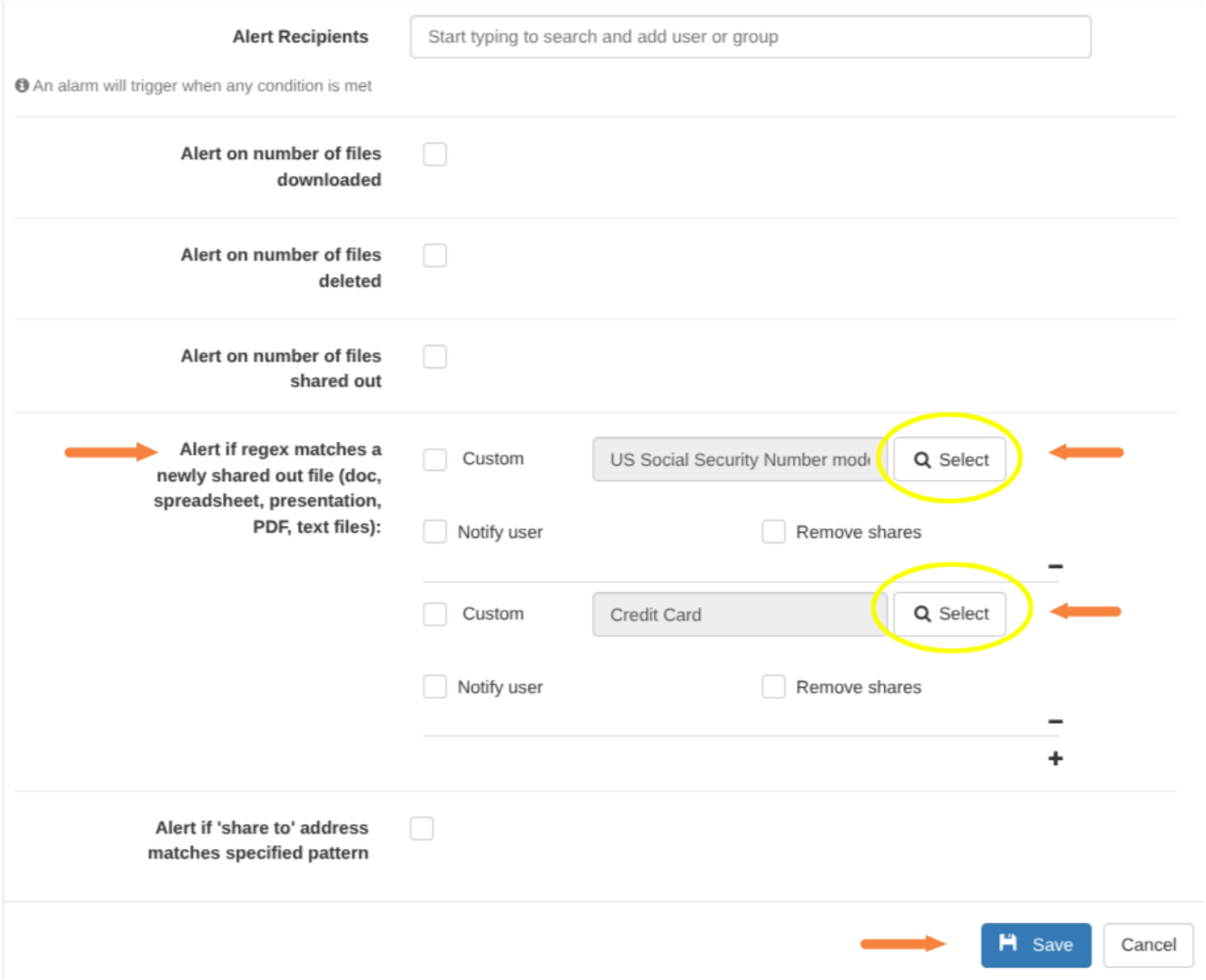


We have a few examples **prepared for regex examples** that can be used.

- *US Social Security Number model #1* - ***\b(?!000)(?!666)(?!9)[0-9]{3}[-]?(?!00)[0-9]{2}[-]?(?!0000)[0-9]{4}\b***
- *UK National Insurance Number* - ***^[A-CEGHJ-PR-TW-Z]{1}[A-CEGHJ-NPR-TW-Z]{1}[0-9]{6}[A-DFM]{0,1}$***
- *US Social Security Number model #2* - ***/^((?!219-09-9999|078-05-1120)(?!666|000|9\d{2})\d{3}-(?!00)\d{2}-(?!0{4})\d{4})|((?!219 09 9999|078 05 1120)(?!666|000|9\d{2})\d{3} (?!00)\d{2} (?!0{4})\d{4})|((?!219099999|078051120)(?!666|000|9\d{2})\d{3}(?!00)\d{2}(?!0{4})\d{4***
- *Contains an eMail address* - ***([a-zA-Z0-9._%-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6})***
- *UK Postal Code* - ***([Gg][Ii][Rr] 0[Aa]{2})|((([A-Za-z][0-9]{1,2})|(([A-Za-z][A-Ha-hJ-Yj-y][0-9]{1,2})|(([A-Za-z][0-9][A-Za-z])|([A-Za-z][A-Ha-hJ-Yj-y][0-9]?[A-Za-z])))))\s?[0-***

9][A-Za-z]{2})([,\s]+)([Uu]\.?[Kk]\.?|[Uu]nited [Kk]ingdom)

- *Credit Card - /\b(1800|2131|30[0-5]\d|3[4-7]\d{2}|4\d{3}|5[0-5]\d{2}|6011|6[2357]\d{2})[-]?(\d{4}[-]?\d{4}[-]?\d{4}|\d{6}[-]?\d{5})\b/gi*

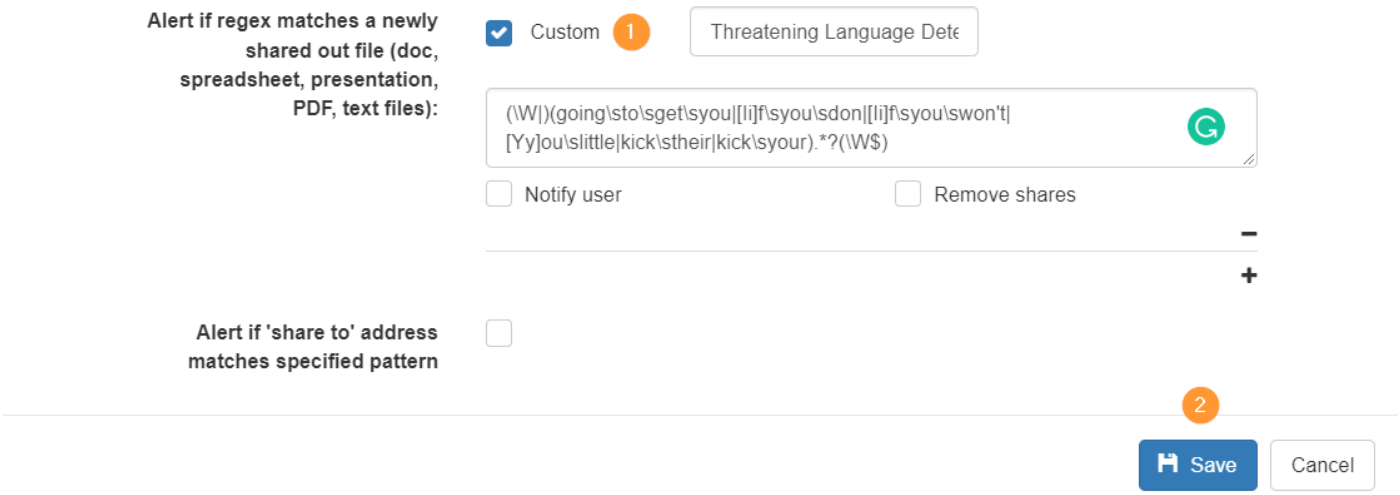


Custom regex

The Admin can also create a custom regex-specific use case for their domain.

Click on the **Custom** button

An example: Threatening language used



Notify user

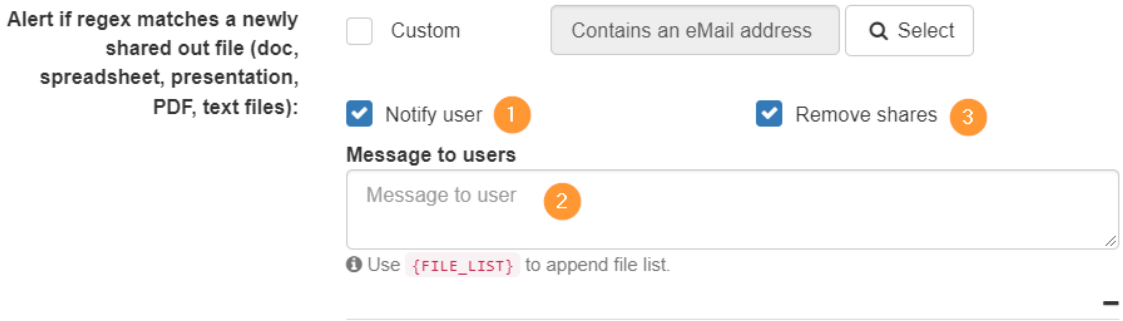
The Admin can also enable the option to **Notify users.**

This will send an email to the user who "breaks" the Alert rule.

You can use **{FILE_LIST} to include the actual file the user shared**

Remove shares

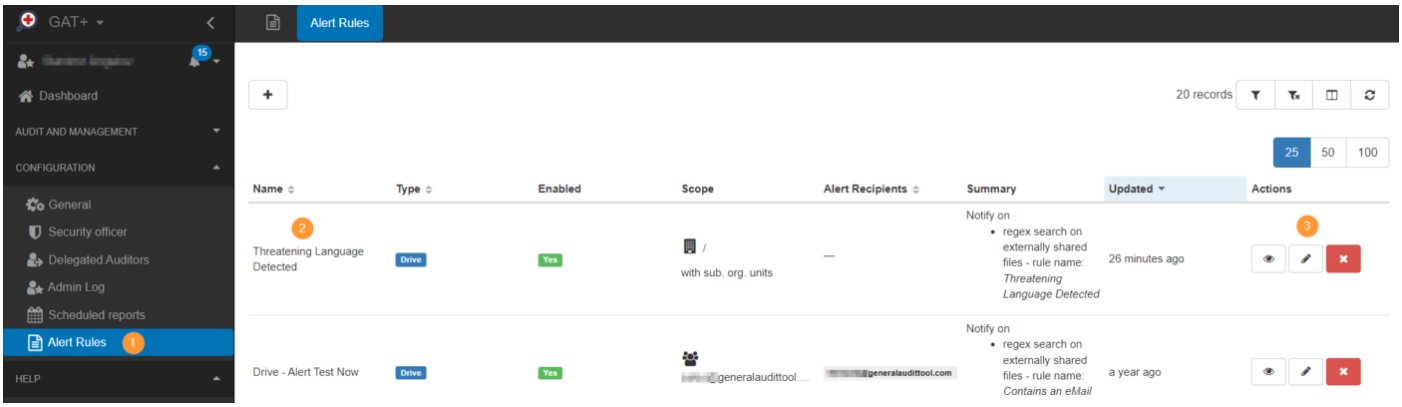
This option will automatically remove the external user (share) from the files for which the alert was triggered.



Result

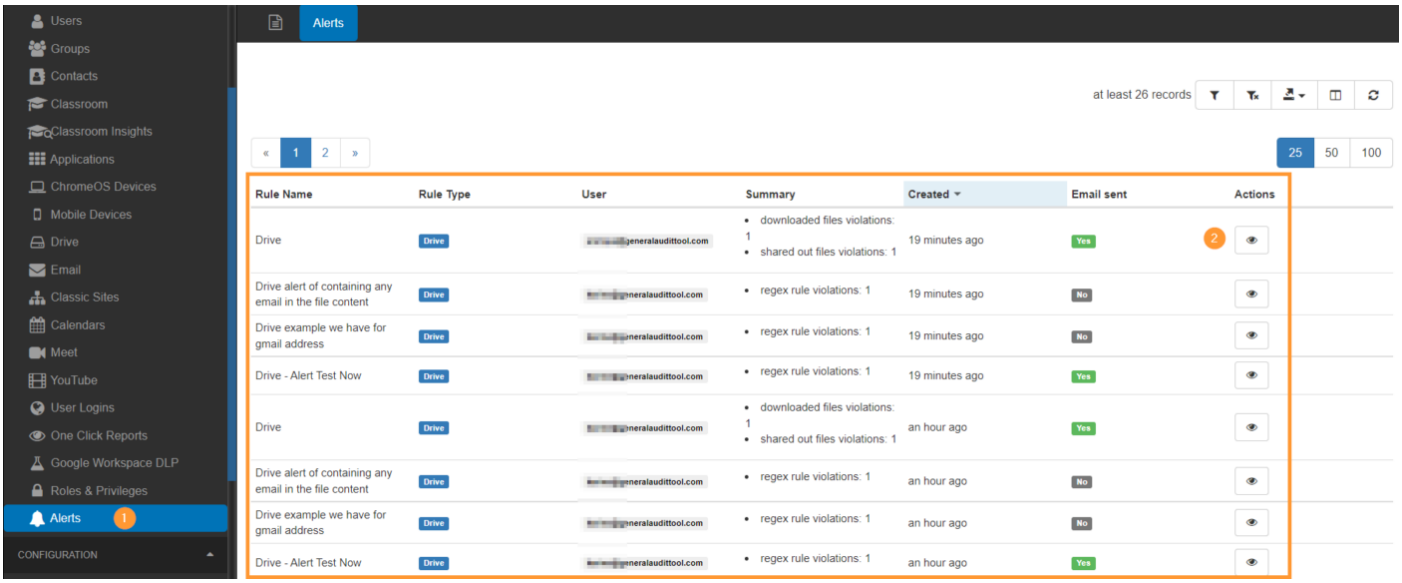
When the rule is created it can be found in the **Alert rules** under the **configuration.**

Under **Actions**, the alert can be **viewed, edited, or removed**



When the Alert rule is triggered it **will be displayed in the Alerts tab in GAT+**

Under Actions, additional details can be seen.



Related Posts

- Set Up Google Drive DLP Alerts For Shared Out Files
- Create Alerts for Inactive Devices
- Allow non-admin users to review Shield Alerts and Site Access Events