Set up a Google DLP Alert on the Number of Drive Files Shared Externally

DLP (Data Loss Prevention) · https://gatlabs.com/knowledge/tech-tips/set-up-a-google-dlp-alert-on-the-number-of-drive-files-shared-externally/

Set up a Google DLP Alert on the Number of Drive Files Shared Externally

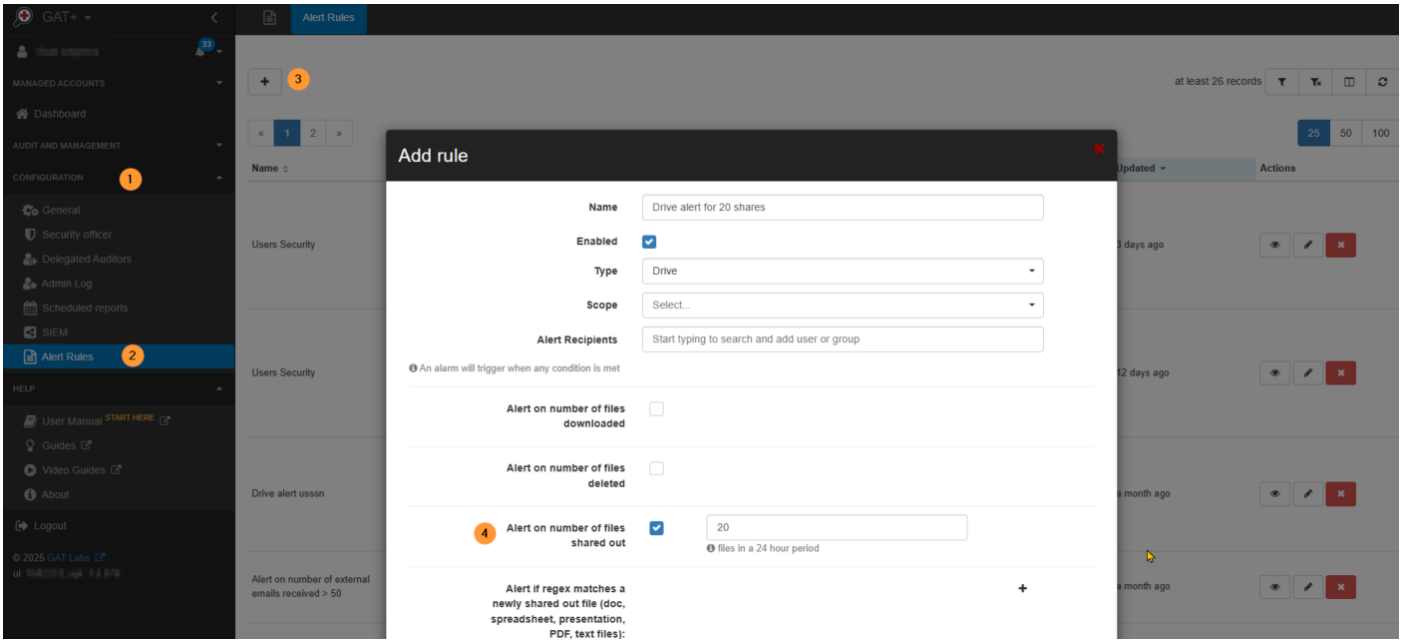
Get alerted when externally shared documents are more than X files in a given period of time, and protect your domain better from data leakage.

GAT+ provides many types of alerts that can be set up for the domain and the user activity in the domain.

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

Click on the **+ sign,** and a new window will be displayed.

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



- Set up a **Name** for the rule.
- Set the check mark to **Enabled.**

- Set the **Type** to **Drive.**
- Choose the **Scope** (of users) that will be affected by this alert rule:
  - Select a user, a group, or an org. unit of users
  - **Check the box here for the entire OU tree** - to address all users of an organizational unit, including users of child units
- Pick and select the **Recipient.** This can be a user or group email.

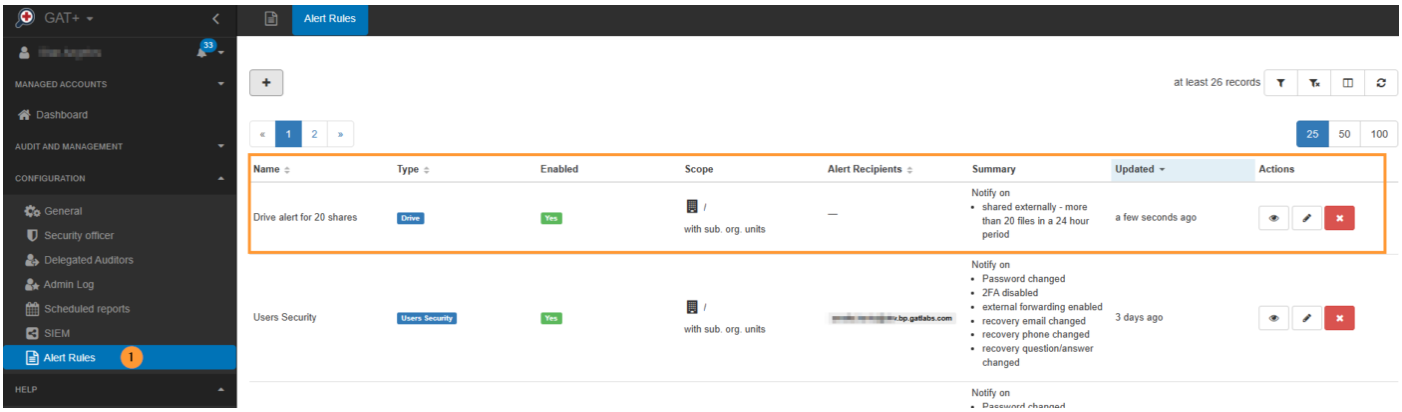
Select the checkmark for **Alert on a number of files shared out (X** number of files in a 24-hour period).

> If you place (1) as a number of files shared out - the alert will be triggered when (1) or more files are shared out

- The alert will be triggered when Google documents shared externally is more than X files in 24 hours.
- Click on **Save** to activate the rule.

Edit the rule

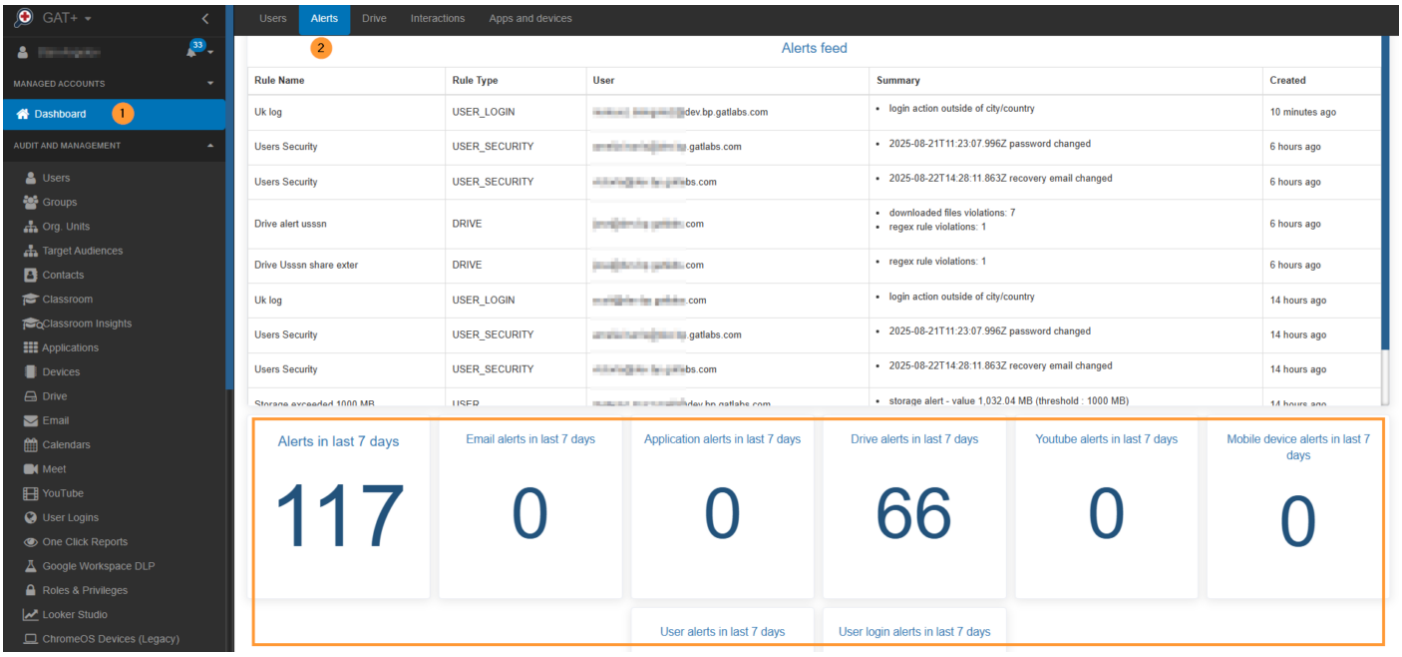
When the rule is created, it can be found in the **Alert rules** under the **configuration.**



It can be viewed (eye icon), edited (pen icon), or deleted (x button).

Audit the result of the rules

When the alerts are triggered, they will be displayed in the **Dashboard** and the **Alerts** tab.



FAQ

1. What is the main purpose of setting up a Google DLP Alert for externally shared Drive files?

The primary purpose is to protect your domain from data leakage. By setting up an alert that triggers when a certain number of Google documents are shared externally within a given period, you can proactively monitor for and respond to potential security risks, whether they are accidental or malicious.

2. How do I define who is affected by the alert and who receives the notification?

You can define the scope of the rule to affect specific users, groups, or an entire organizational unit (OU). You also have the option to include all users in child OUs. For the recipient, you can choose a user or a group email address to receive the alert notifications when the rule is triggered.

3. What happens after the alert rule is created and triggered?

Once the rule is created and saved, it becomes active. If the conditions are met (e.g., more than "X" files are shared externally in 24 hours), the alert is triggered. The alerts will then be displayed in the **Dashboard** and the **Alerts** tab within the GAT+ tool, and the designated recipient will receive an email notification. You can also view, edit, or delete the rule from the "Alert rules" section under configuration.