Set up a Google Drive DLP Alert when the Number of Downloaded Files Exceeds X

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

GAT+ is an audit tool for Google Workspace domains, It offers many different reports for any set of data from your domain.

We also have many Alert rules that can be created.

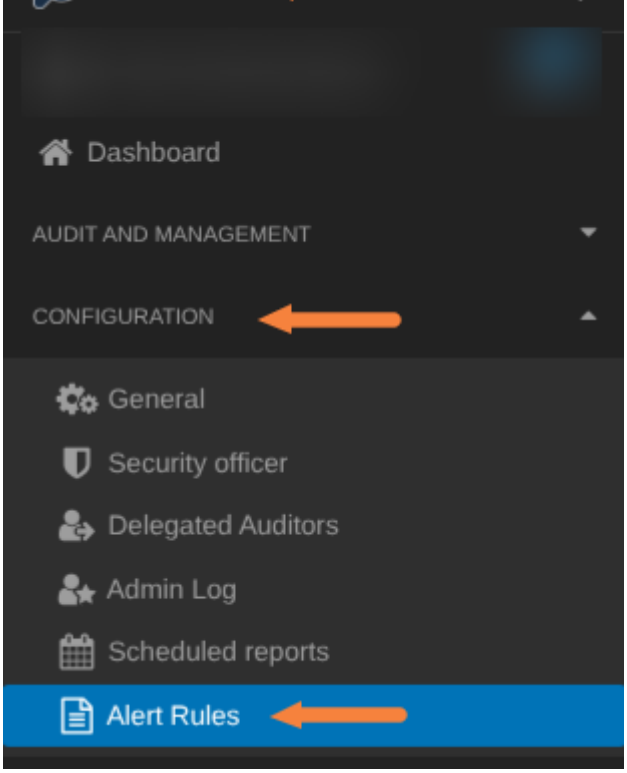
Those alerts can notify Admins or any user of the domain of different types of activity done by the end-users.

NOTE: The Download events relate to real user actions because when reading the docs https://support.google.com/a/answer/4579696#logged - Google says that previewing a PDF file can generate a download.

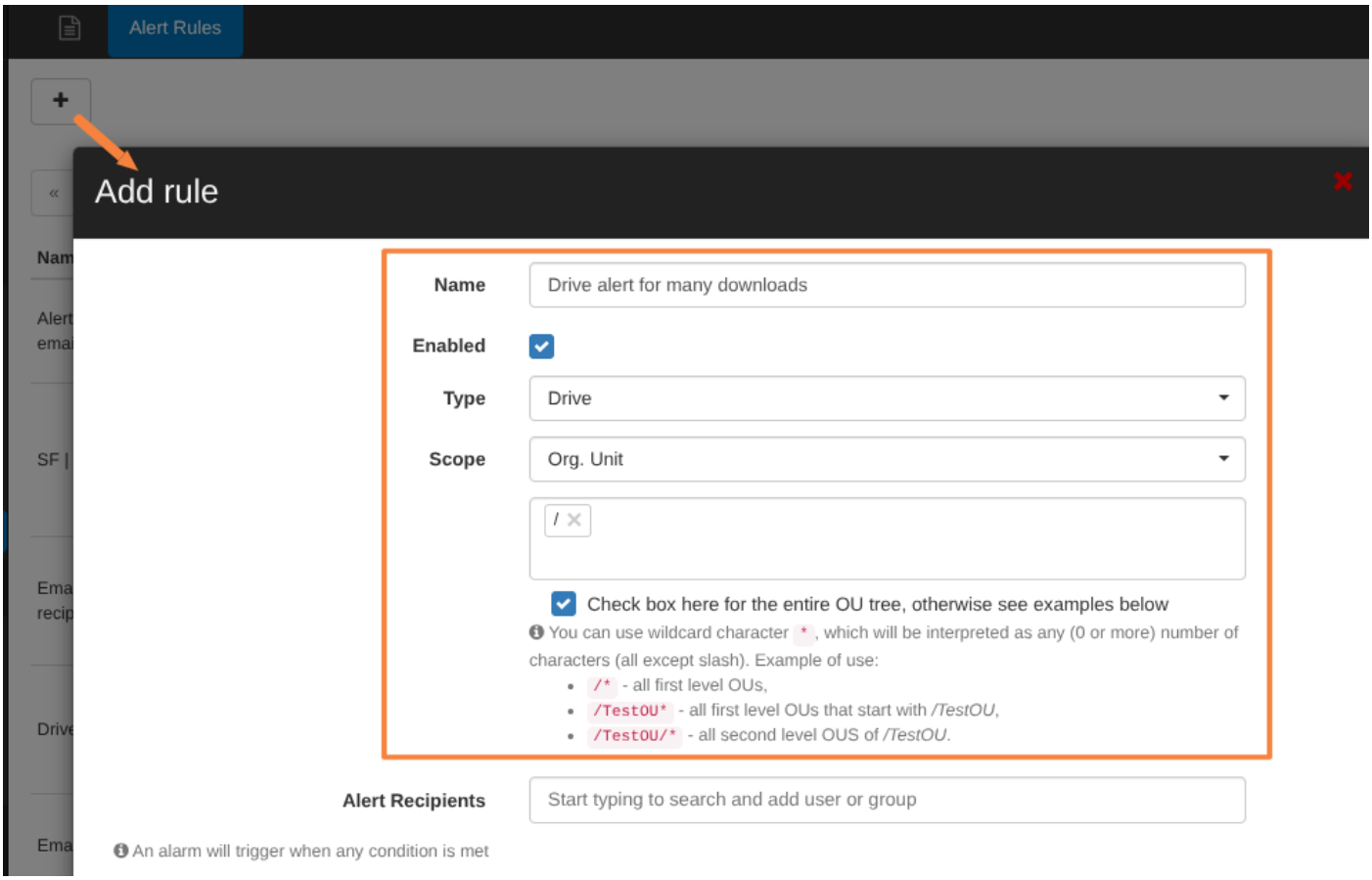
Alert rules

Here an Admin can set up the GAT+ Alert rule and get notified when users **download** more than X files from your Google Drive in a 24-hour window.

In **GAT+ > Configuration > Alert rules**



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



- **Name** - Enter a name for the alert rule

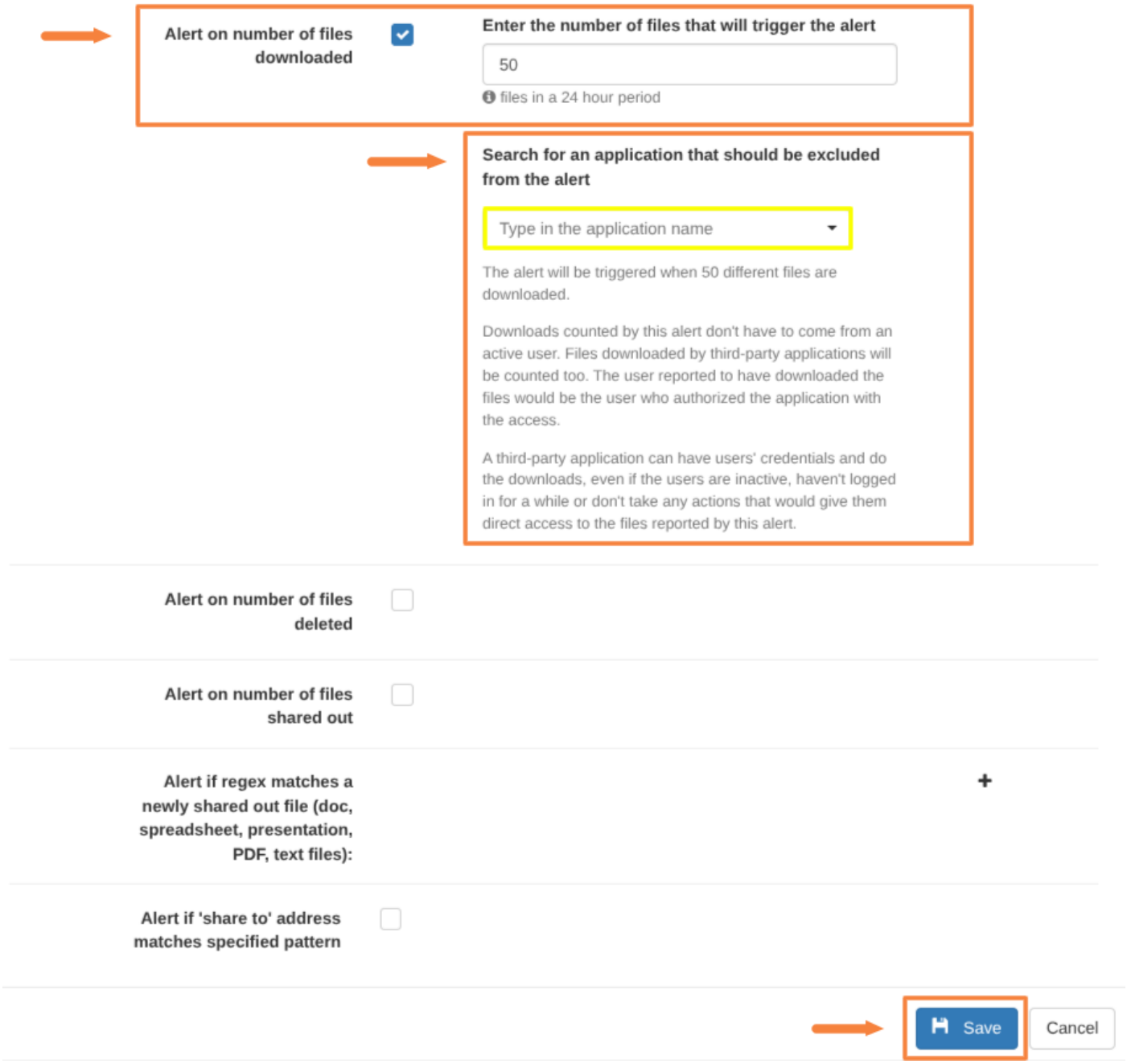
- **Enabled** - enable or disable the rule
- **Type** - select type of alert - Drive
- **Scope** - select which users to be affected by the alert rule
  - Select User, Group, or Org. Unit of users (include Sub. OU if needed).
- **Alert recipients** - Enter recipient emails who will receive an email for the alert (optional). By default, all alerts will be shown in GAT+ > Alerts

Pick and select the actions for which you want to be alerted.

Alert on the number of files downloaded

In the Alert rule - select **Alert on a number of files downloaded.** When the number of downloads **is more** than the setup number the **alert will be triggered.**

Enter the number of files that will trigger the alert



Exclude apps from which downloads will not be counted.

Search for an application that should be excluded from the alert

Search and select an Application where the Alert will not count the downloads.

For example: If your users are using **Google Drive for Desktop**- you **can exclude this app** and the **alert will not be triggered by downloads done by this app.**

> The alert will be triggered when X different files are downloaded.

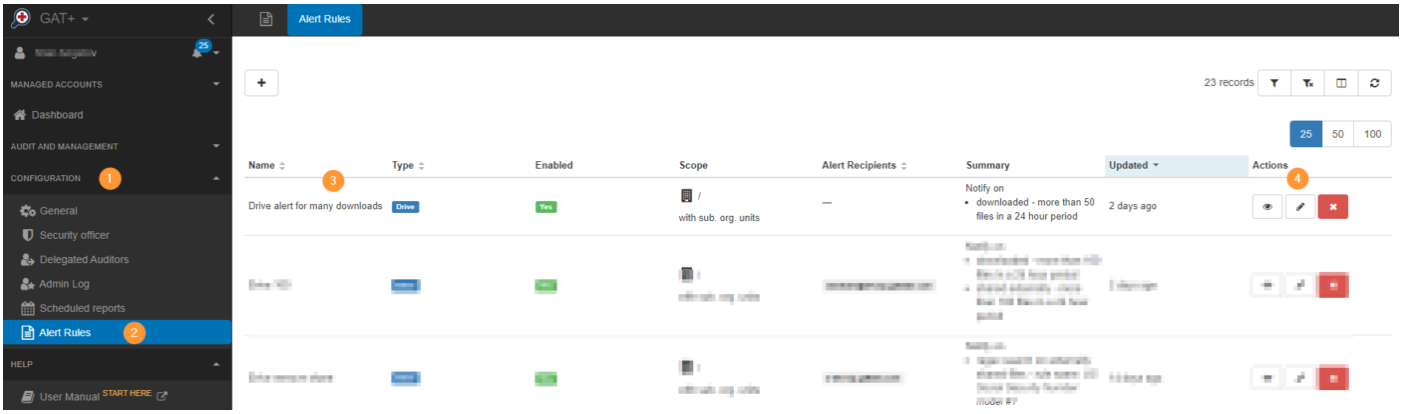
> Downloads counted by this alert don't have to come from an active user. Files downloaded by third-party applications will be counted too. The user reported to have downloaded the files would be the user who authorized the application with the access.
>
> A third-party application can have users' credentials and do the downloads, even if the users are inactive, haven't logged in for a while or don't take any actions that would give them direct access to the files reported by this alert.

Result

NOTE: The Download events relate to real user actions because when reading the docs https://support.google.com/a/answer/4579696#logged - Google says that previewing a PDF file can generate a download.

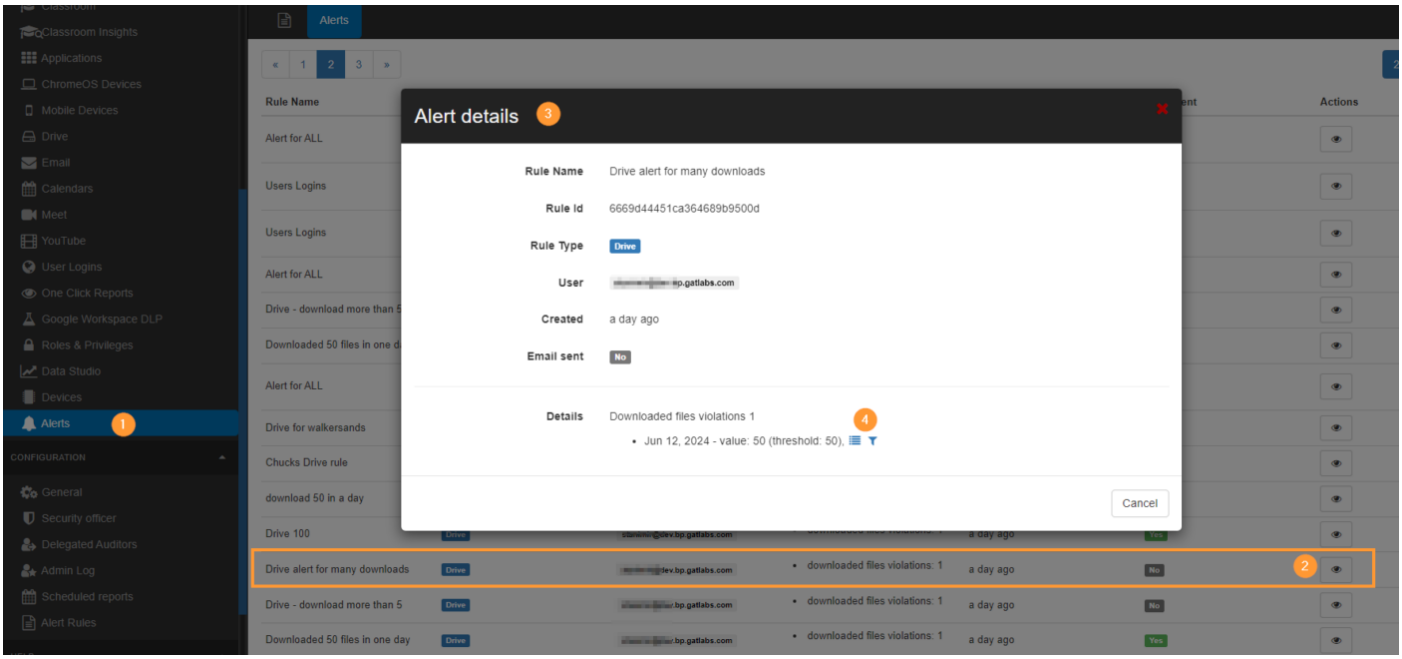
When the number of downloads **is more** than the setup number, the **alert will be triggered.**

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 from the (x button) (4)

The **Alert** will be shown in the **Alerts tab in GAT+.**



Click on the "**Toggle file list**" (4) to see a list of all the downloaded files.

Click on the "**Show those files in the Drive audit**" - (funnel icon) (4) to see all the files in GAT+ > Drive audit