Set Up Google Drive DLP Alerts For Shared Out Files

Drive Audit & Management · https://gatlabs.com/knowledge/tech-tips/set-up-google-drive-dlp-alerts-for-shared-out-files/

Introduction

GAT+ audit tool provides an extensive and detailed overview of the entire Google Workspace domain. Drive audit allows a global and detailed view of **Google Drive**.

Our tool provides an alternative solution to Google Admin Console alerting, within our tool we call it **Alert Rules**.

In GAT+ we have different types of alerts

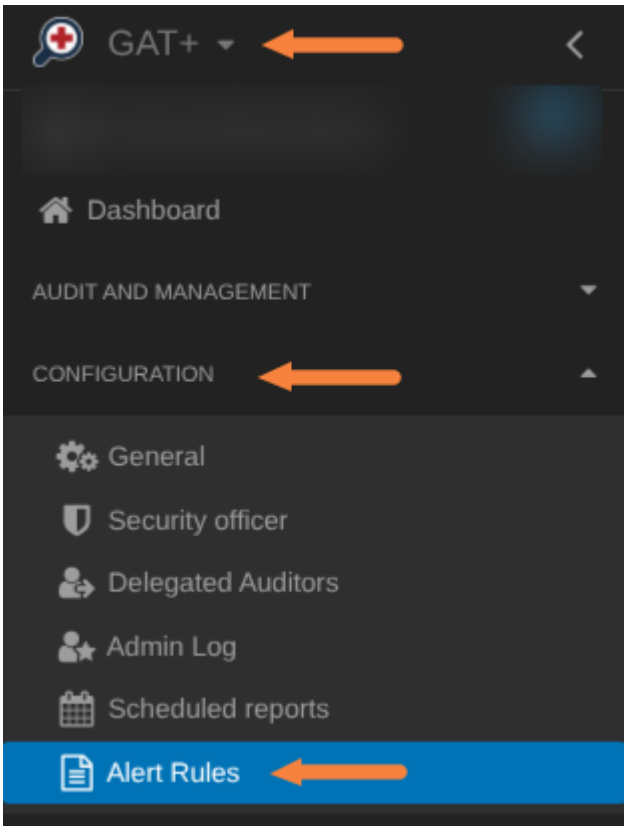
- Applications
- Emails
- Drive
- YouTube
- Mobile device
- Users
- Users Logins

The **Drive Alert rules** are based on a number of different activities:

- The number of files Downloaded - per day
- A number of files Shared out - per day
- **Alert if the regex matches newly shared out files (google native files, PDF, and TXT files)**
- Aler if "share to" address matches a specific pattern

Configuring Alert Rules

Open **GAT+** and navigate to **Alert rules** under the **Configuration** tab



Select users

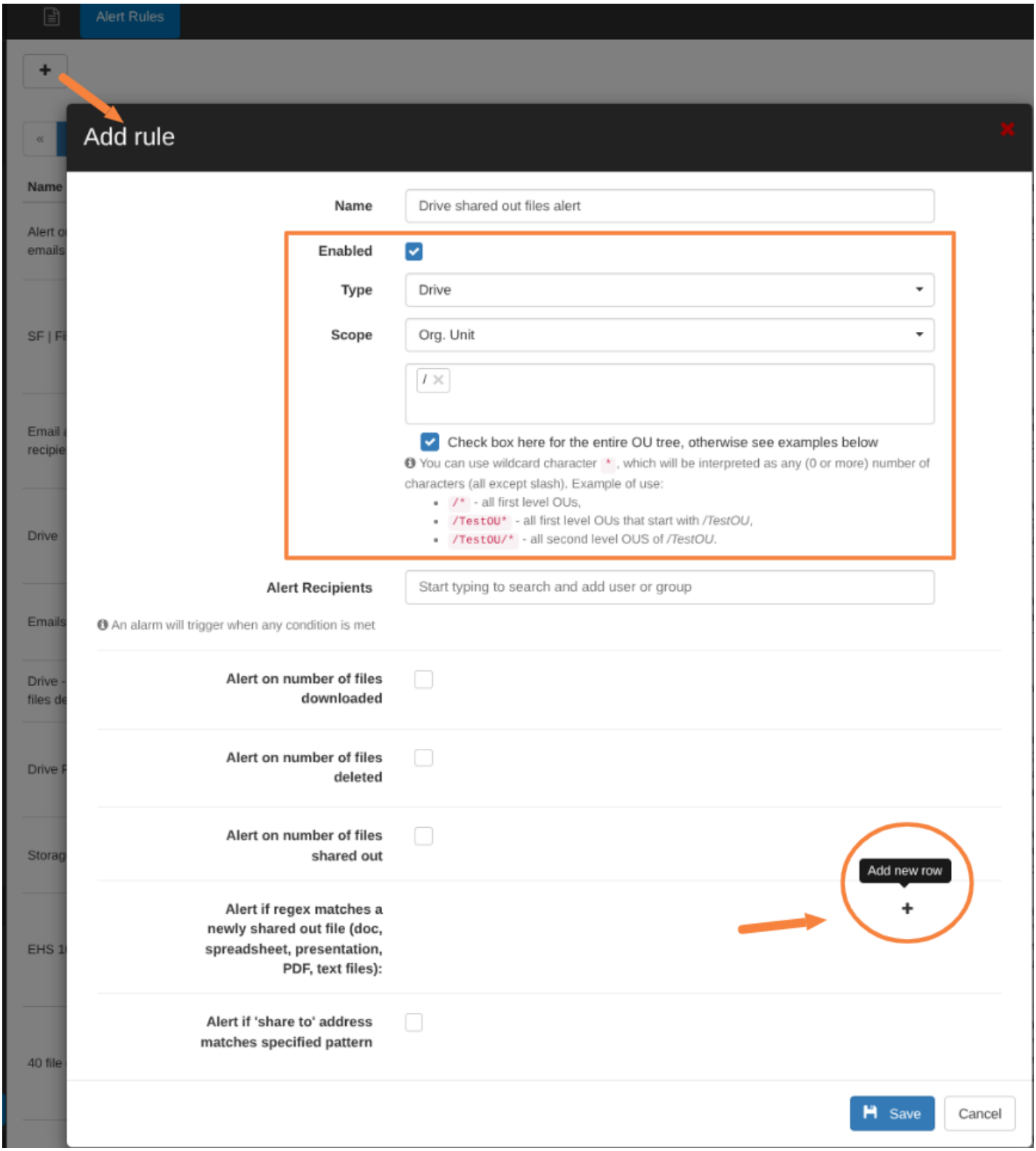
Click on the **+ sign** and a new window will be displayed, fill in the details as shown below:

- Set up a **Name** for the rule
- Set the checkmark to **Enabled**
- Set the **Type** to Drive

Choose the **scope** who will be affected by this alert rule

- It can be a user, group, or org. unit.

To apply this option to all users in the domain, select the top OU ("/") and check the box below to include all sub-OUs in the scope.



Pick and select the **Recipients** it can be any local user email or group email from your domain or someone from outside.

> Note: If no recipient selects the alerts will be simply reported in the **Alerts** tab on the left-hand side menu.

The rules on which an alert will be generated are:

- Alert on number of files downloaded (files in a 24 hour period)
- Alert on number of files shared out(files in a 24 hour period)
- Alert rule can be added as an **alert if the regex matches a newly shared out file (doc, spreadsheet, presentation, PDF, text files):**
- Alert if "share to" address matches specified pattern.

Set up the rule

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

Click on the **+ button** to add a rule.

Two options will be displayed:

Custom: Select and add **custom Regex pattern**

Click on the **Select** button and **predefined Regex pattern** examples will be displayed.

Pick any of the rule examples and click on the "**Select**" button beside it

> Note: If you would like us to add additional **Regex patterns** that you think is important, please email us at support@gatlabs.com with your suggestion.

The rule will be added

Click on the **+ sign** underneath to add multiple Regex patterns.

Additional rules

Additionally, you can set extra actions:

- **Notify the user** if you want to show a custom message to the end-user who shared out this document.
- **Remove shares** if you want to remove the external shares automatically.

Click on the **Save button** to activate the rule.

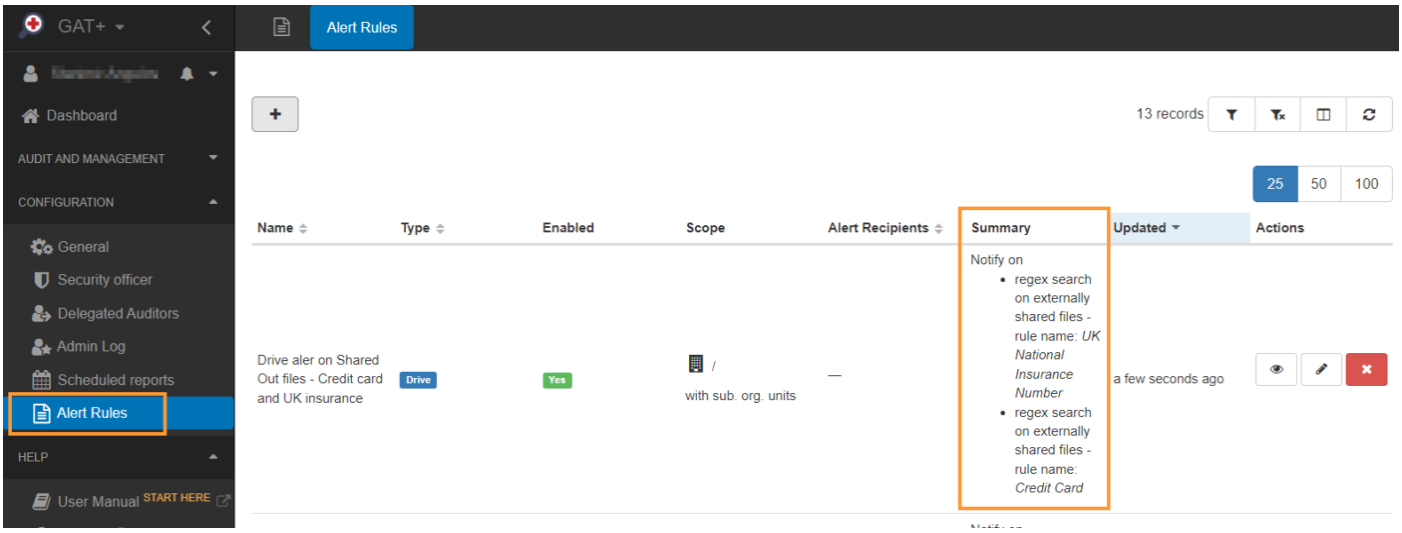
Viewing Alert Rules

Alert rules can be found in the **Alert rules** under the **configuration**

An admin can quickly see the name of the rule, the type of the rule if it is enabled, what scope, and the recipients.

Under the summary tab, an admin can see exactly the alerts enabled for this rule.

Under the **actions** tab, the rule can be viewed (**eye icon),** it can be **edited** from the **pen** icon or deleted from the **x** button.



Result

When the rules are violated the **Recipients** will receive email notifications and a record for the rule will be generated and placed under **Alerts**

The recipient will receive an email notification below.

All the **Alerts** can be seen under the **Audit and Management** area in GAT+.

Video how-to

In the example below we will create the **Drive Alert rule for newly Shared Out files.**

Embedded media:

https://www.youtube.com/embed/1AgTjpupiAY?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_loa