How to set up Google Drive alerts for G Suite users

Drive Audit & Management · https://gatlabs.com/knowledge/tech-tips/how-to-set-up-google-drive-alerts-for-g-suite-users/

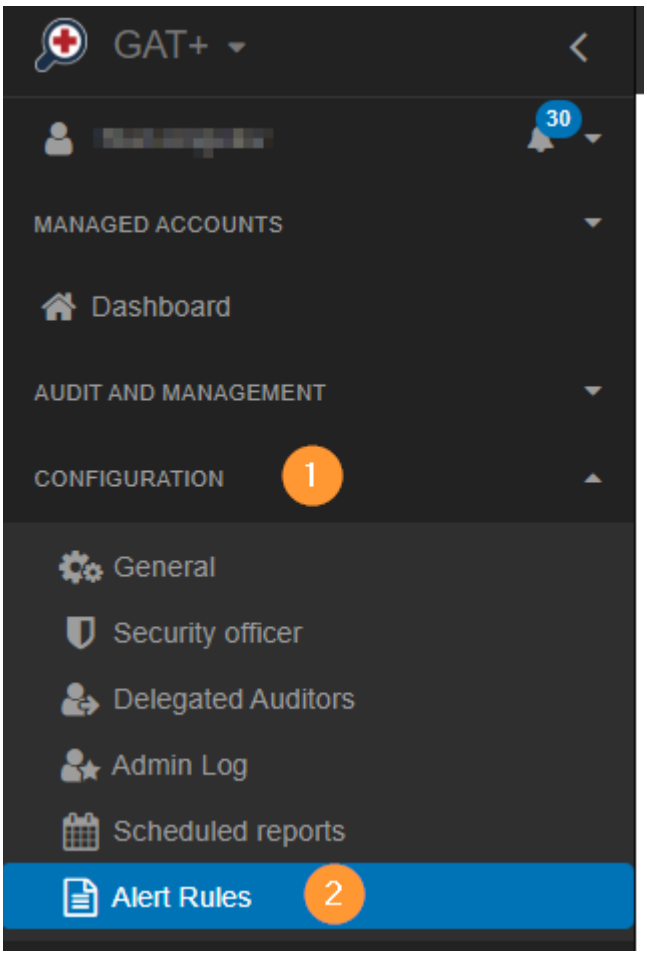
Introduction

GAT+ allows Google Workspace admins to create **Alerts** for Drive usage.

- Alert on Drive when **X number of files are downloaded** (in a 24-hour period).
- **Alert on a number of files shared out** (outside your domain) in a 24-hour period of time.

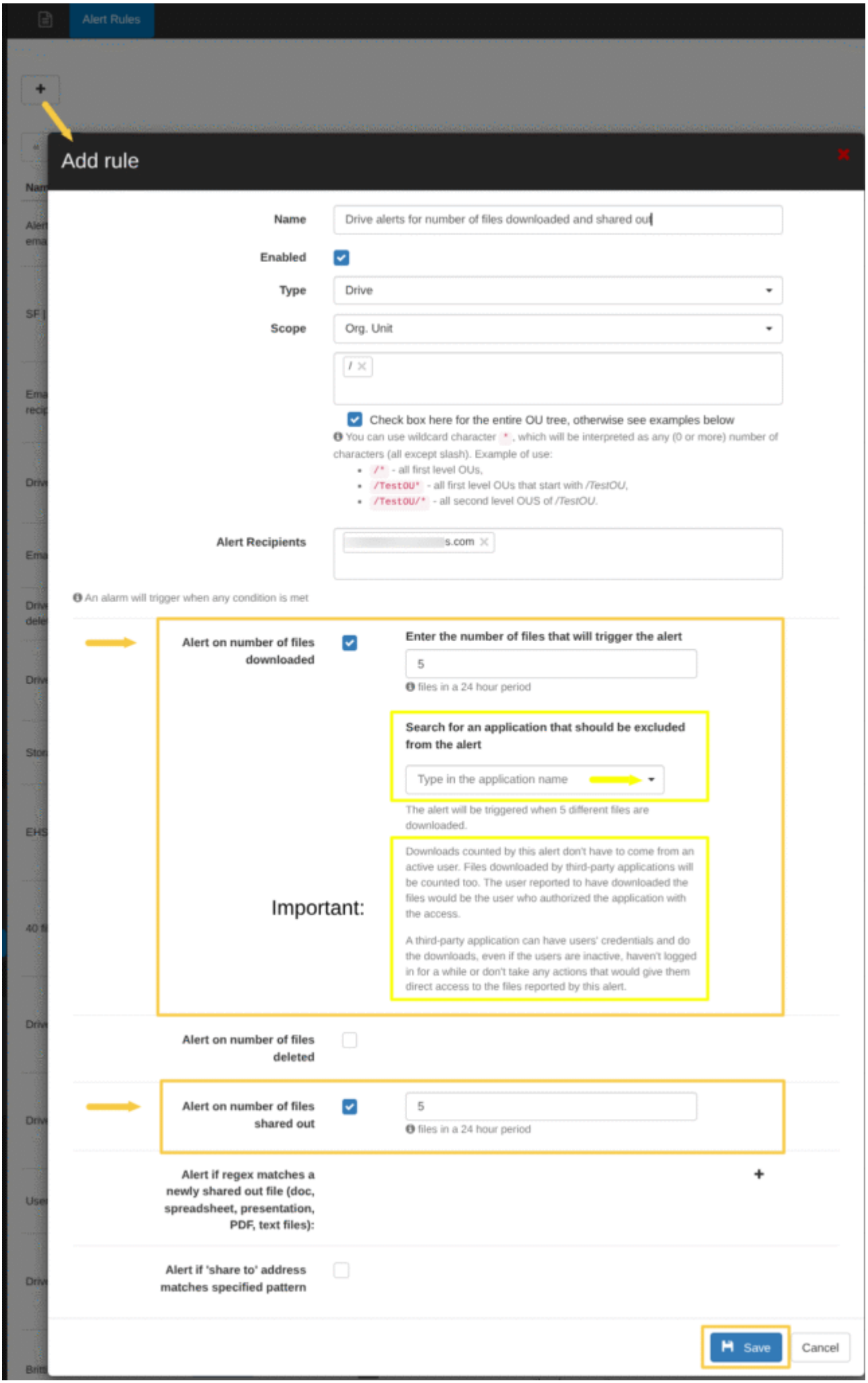
Alert if the **regex matches** a newly "shared out" file (Google type only).

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



Creating an Alert Rule within GAT+

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


Alert Rules
Add rule
Name
Drive alerts for number of files downloaded and shared out
Enabled
Type
Drive
Scope
Org. Unit
/
Check box here for the entire OU tree, otherwise see examples below
You can use wildcard character *, which will be interpreted as any (0 or more) number of characters (all except slash). Example of use:
/* - all first level OUs,
/TestOU* - all first level OUs that start with /TestOU,
/TestOU/* - all second level OUS of /TestOU.
Alert Recipients
s.com
An alarm will trigger when any condition is met
Alert on number of files downloaded
Enter the number of files that will trigger the alert
5
files in a 24 hour period
Search for an application that should be excluded from the alert
Type in the application name
The alert will be triggered when 5 different files are downloaded.
Important:
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.
Alert on number of files deleted
Alert on number of files shared out
5
files in a 24 hour period
Alert if regex matches a newly shared out file (doc, spreadsheet, presentation, PDF, text files):
Alert if 'share to' address matches specified pattern
Save
Cancel

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

Choose the **Scope** of who will be affected by this alert rule

- It can be a User, Group, or Org unit

Pick and select the **Recipient,** this can be a user or group email.

The actual rules on which an alert will be generated are:

- Alert on the number of **files downloaded** (files in a 24 hour period)
  - **Search for an application that should be excluded from the alert** - Downloads counted by this alert don't have to come from an active user. Files downloaded by third-party applications will be counted too. This option won't stop the 3rd party apps from downloading files, but it allows you to exclude apps from the alert rule to give a better view of what the actual user has downloaded.
- Alert on the number of **files shared out** (files in a 24 hour period)

An additional rule can be added as an alert if the regex matches a newly "shared out" file (Google types only). Click on **Save** to activate the rule.

Viewing Created Rules

When the rule is created, it 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 options 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.

Alert Triggered - Violation Occurred

When the rule is triggered, an email will be sent to the recipient with the rule name, the violations, and the list of files that triggered the alert.