# Remove External Sharing on Files with Sensitive Information via Schedule Report

Drive Audit & Management · https://gatlabs.com/knowledge/tech-tips/remove-external-sharing-on-files-with-sensitive-information-via-schedule-report/

The **GAT+** tool helps every Google Workspace **Super Admin** to have an extensive and detailed view of their entire domain data.

You can access a granular overview of all files shared within and outside your domain in the Drive audit section.

Almost every feature in GAT+ allows you to set up and generate a **Scheduled report**.

This post outlines the steps to:

1. Apply a filter that returns metadata for files with "sensitive" content shared outside the domain.
2. Schedule a report to notify Admins of this specific event.
3. Set up external sharing removal to restore the confidentiality of sensitive files.

## Files filtering

To schedule the report that identifies all the external sharing of the files containing sensitive data, navigate to the **Drive (1)** auditing section of GAT+.

Next, under the Drive **Files (2)** tab apply a filter by clicking on the '**funnel**' **icon (3**).

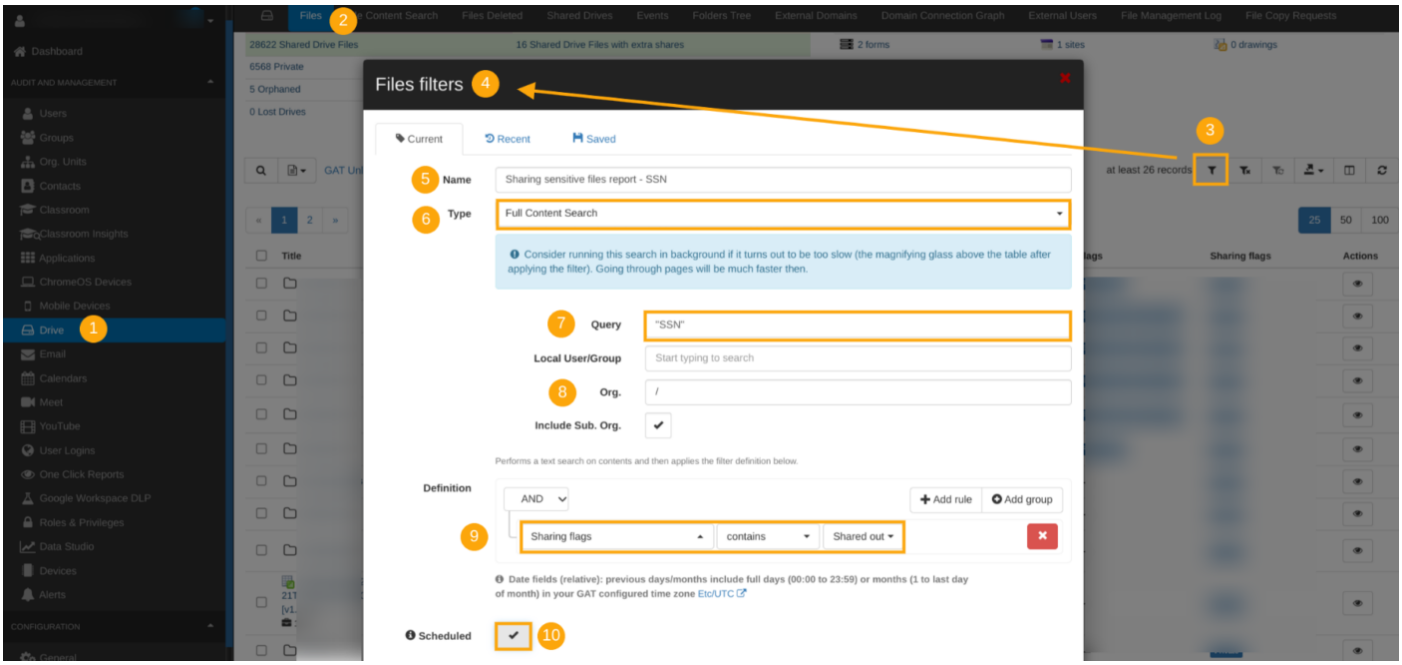
The Files filters (4) window is displayed. Type the **Name (5)** of this File filtering option, and select **Type: Full Content Search (6)**.

**Full Content Search** allows the Admin to apply a **Query (7)** and search in the “Content” of the file for the chosen “query”, e.g. "SSN".

Under **Org. (8)**, enter the Organizational Unit in which you wish the metadata to be scanned after the filter is applied. To target the entire domain, select the top-level Org. Unit "**/**" and select **Include Sub. Org.** to include all Sub-Organizational Units.

**Full Content Search** can be **combined** with search options in **the Definition** section. To target only the external shares, add the rule: **Sharing flag > contains > Shared out (9)**.

When all is set up, the schedule report can be configured by enabling the **Scheduled (10)** option.



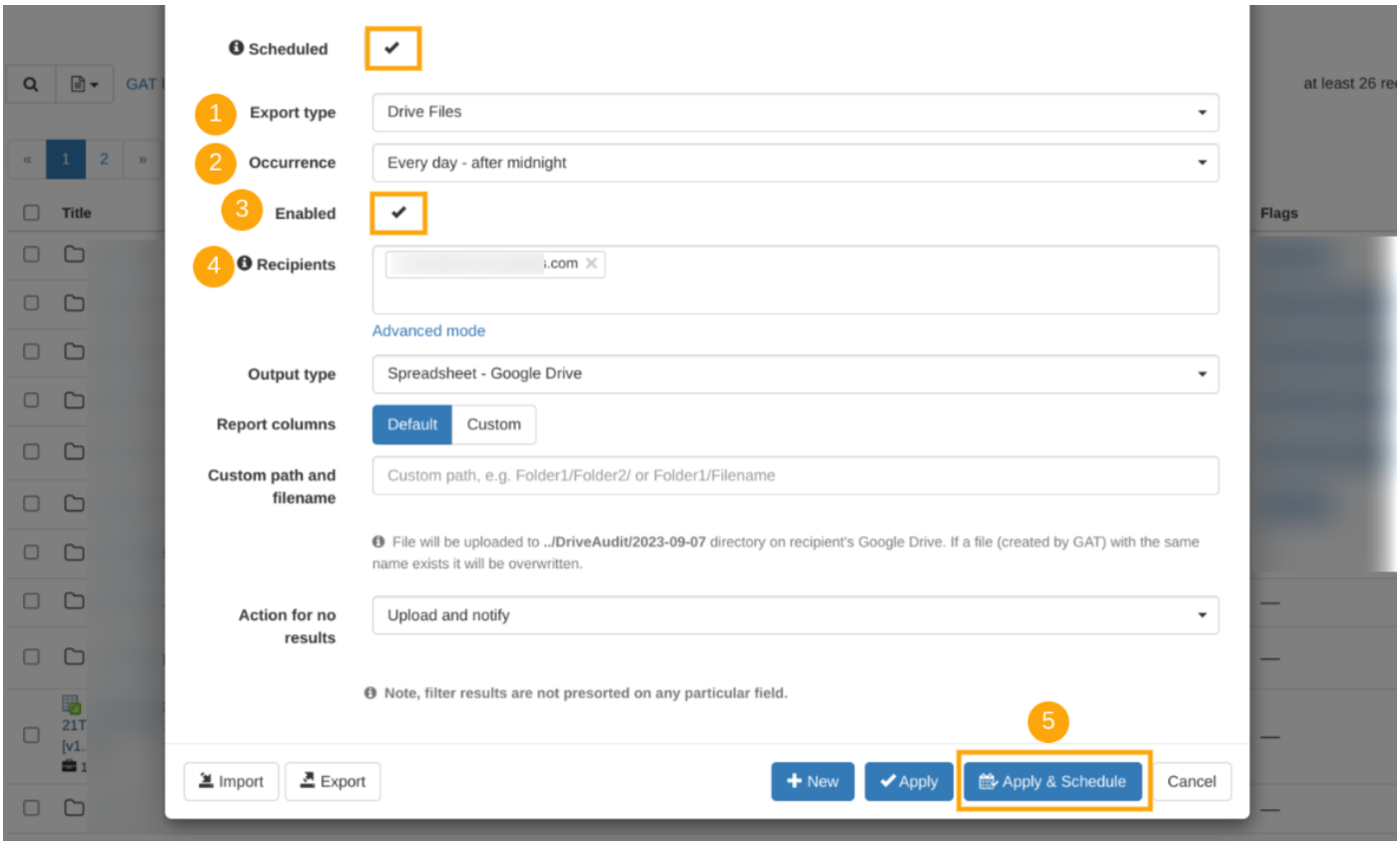

## Scheduling report

Move forward by configuring the scheduled report settings. Select the **Export type (1)**, and **Occurrence (2)** time that meet your needs (how often you want to receive the report).

Make sure to tick the **Enabled (3)** option for the scheduled report to be active as soon as the setup is complete.

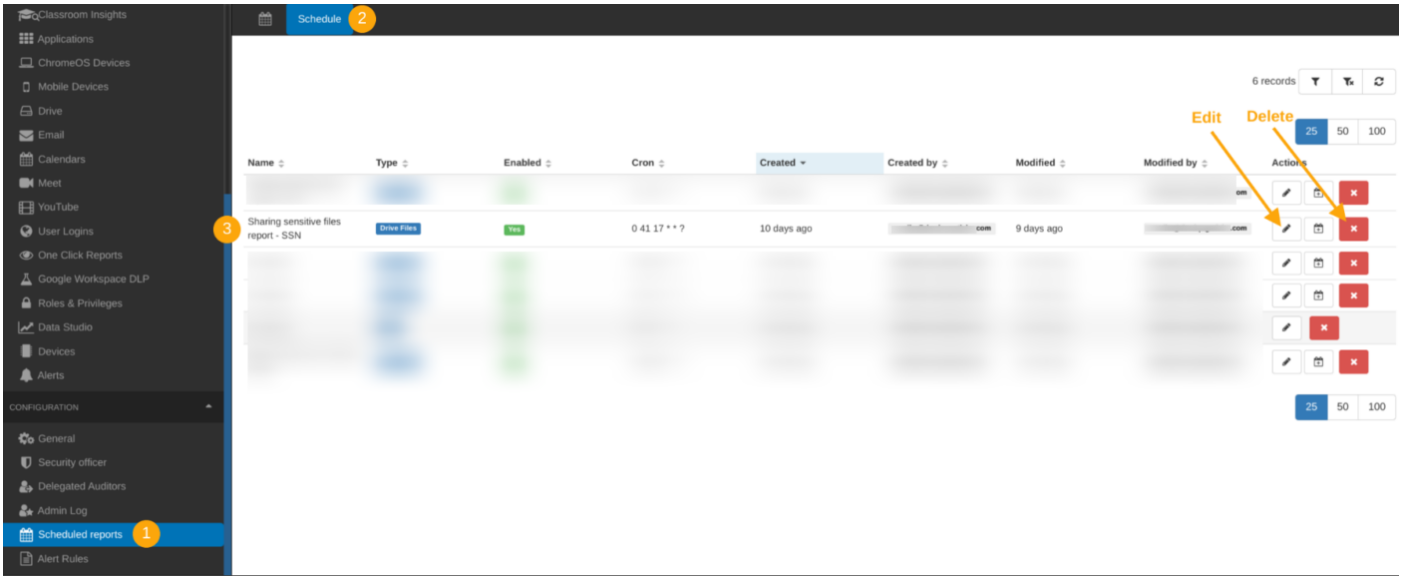
Select the **Recipient (4)** of this report.

Finalize the process by clicking on **Apply & Schedule (5)**.



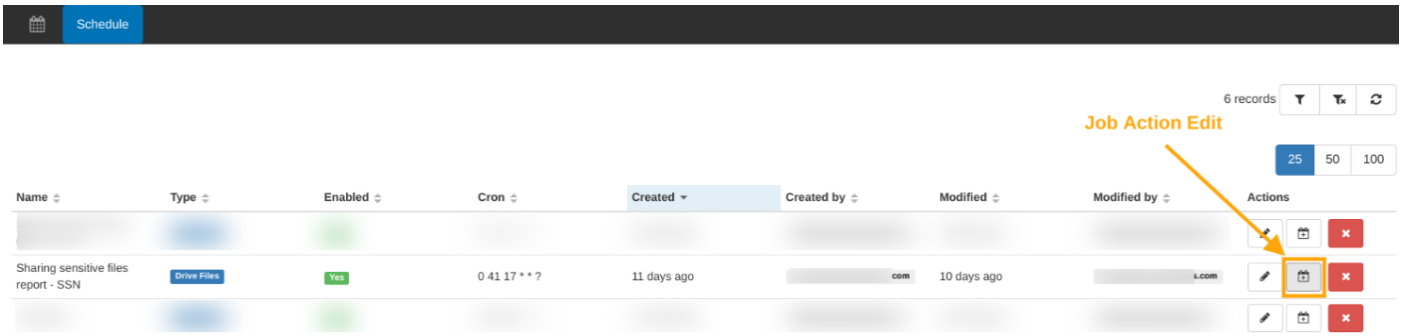

## Job action edition

You can view and edit the scheduled report setup from the **Scheduled Report** section in **GAT+.**




Furthermore, an additional configuration can be made to ensure that the external sharings identified by the filtering GAT+ are removed.

This can be set up by clicking on **Job Action Edit.**

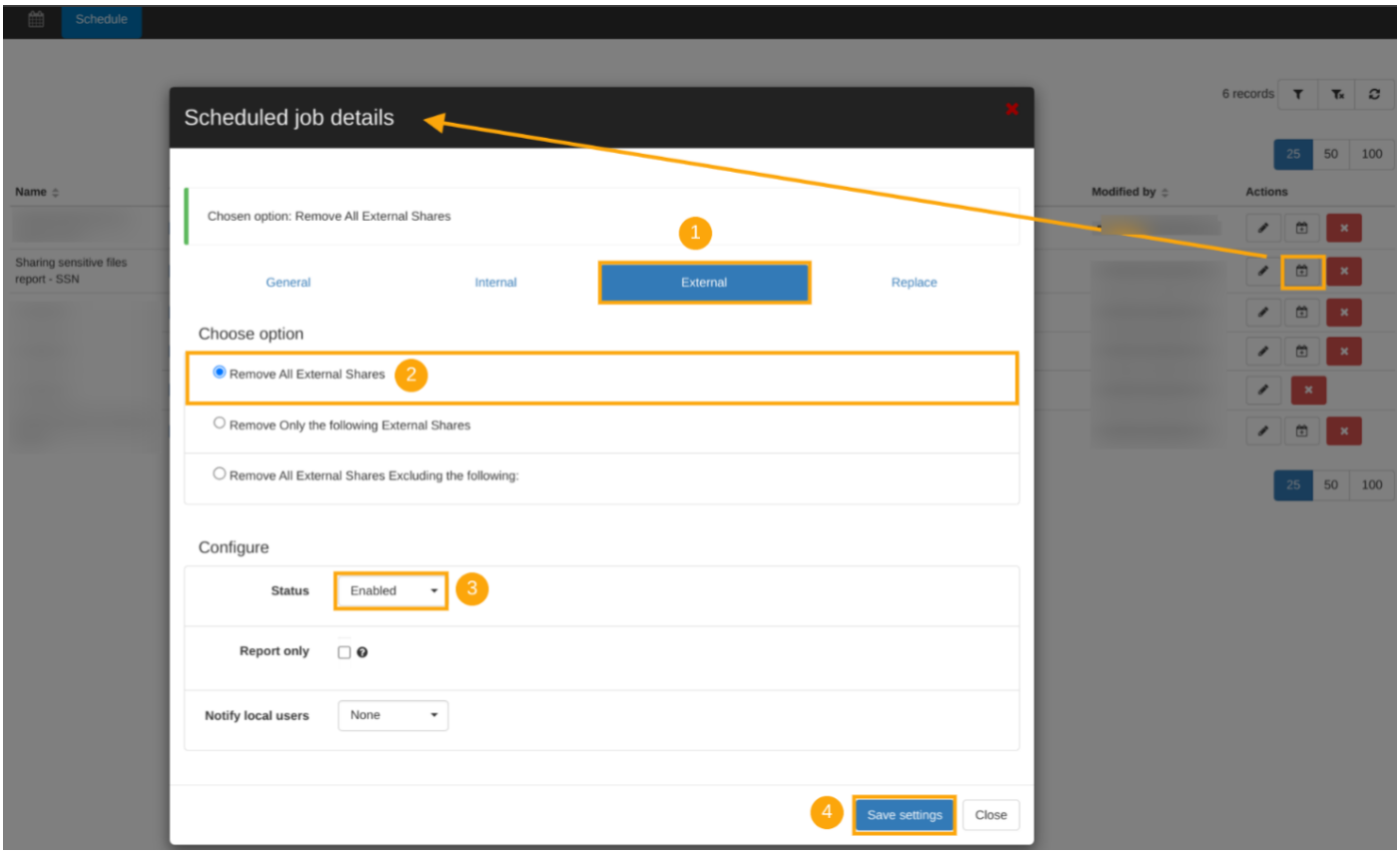



A S**cheduled job details** window appears where the further job can be configured accordingly.

Select the **External (1)** tab and tick the **Remove All External Shares (2)**.

Under the Configuration section, make sure to set the **Status to Enabled (3)**.

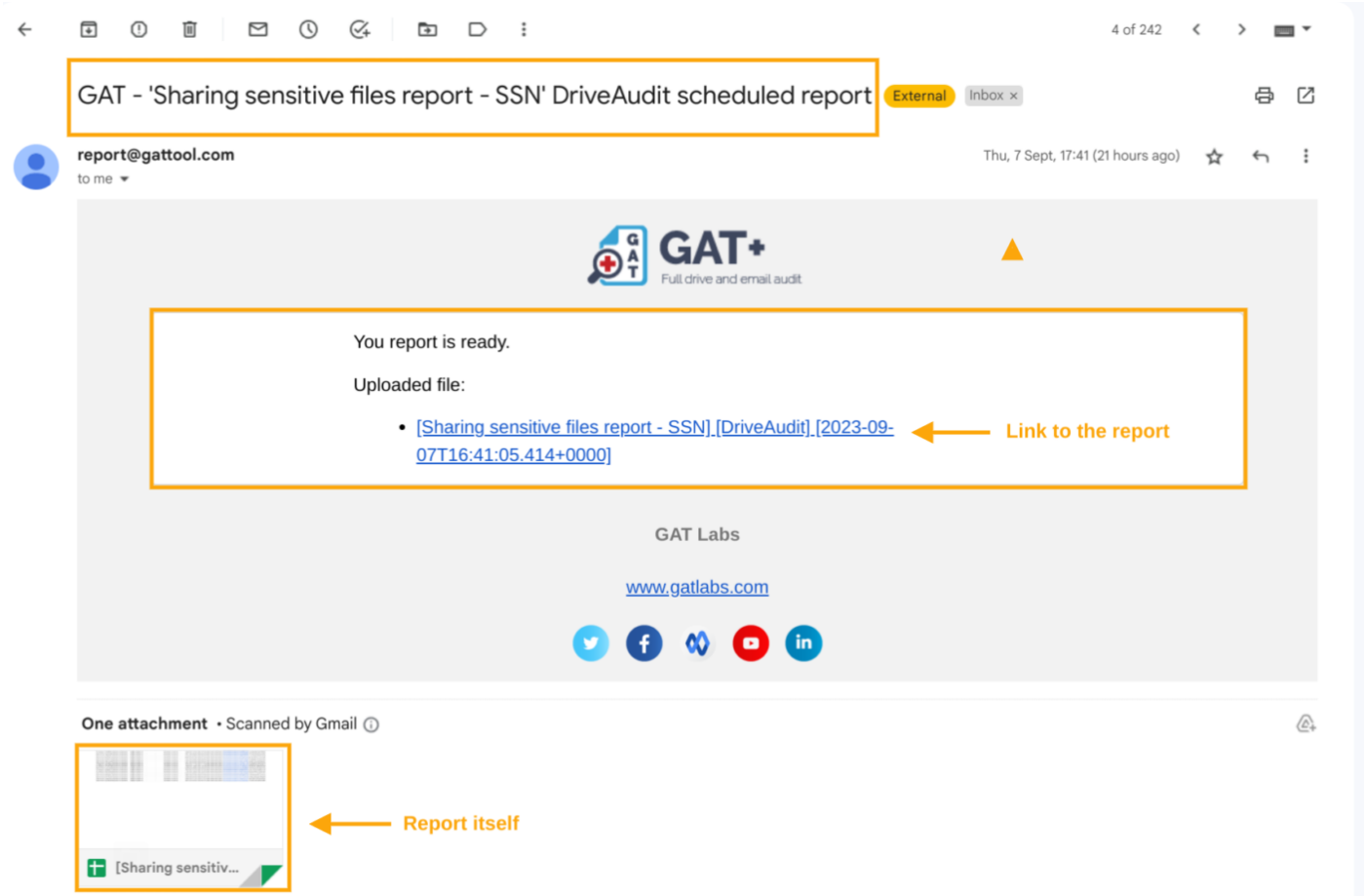
Once all is ready, apply for the job by clicking on the **Save settings** button **(4)**.




## Results

A scheduled report is configured to identify external file shares with "sensitive" content and notify the administrator of these events.

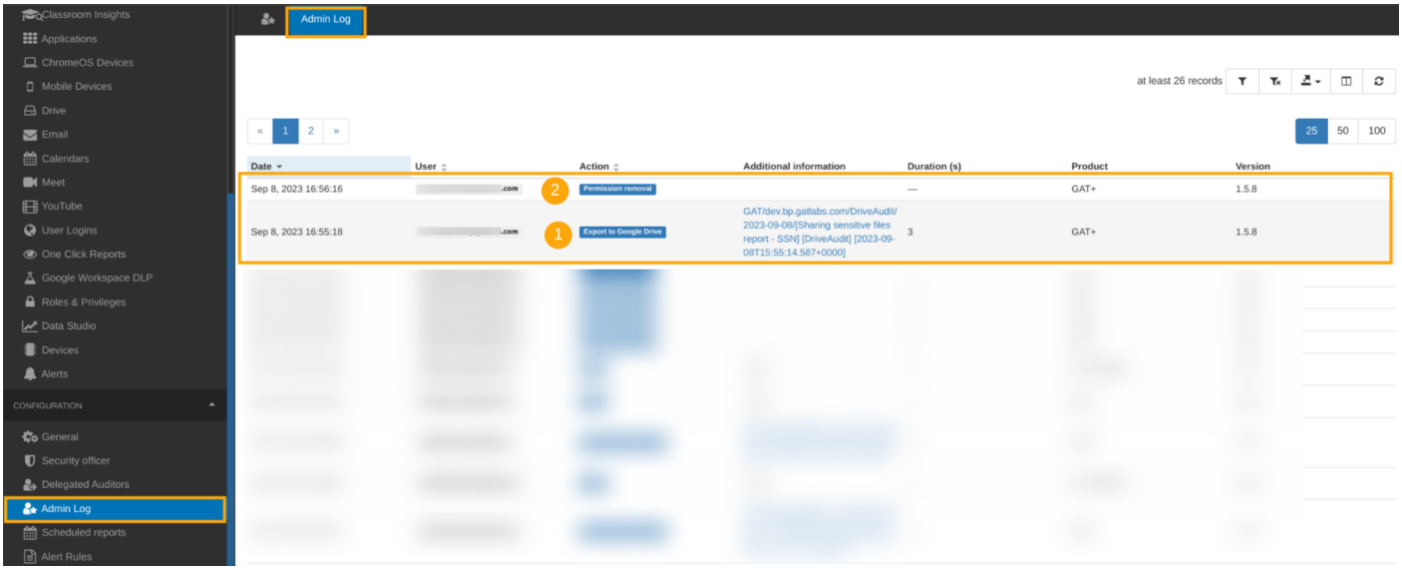
Additionally, depending on the settings enabled, the report will run automatically based on the Occurrence time selected.




Additionally, GAT+ configures a task to automatically delete these external shares once they are identified, providing protection against data leakage.

The filter setup identifies the files from which external shares will be automatically removed.

The record of the Drive report being generated **(1)**, as well as shares removal **(2)**, will be kept in the **Admin Log** in **GAT+.**

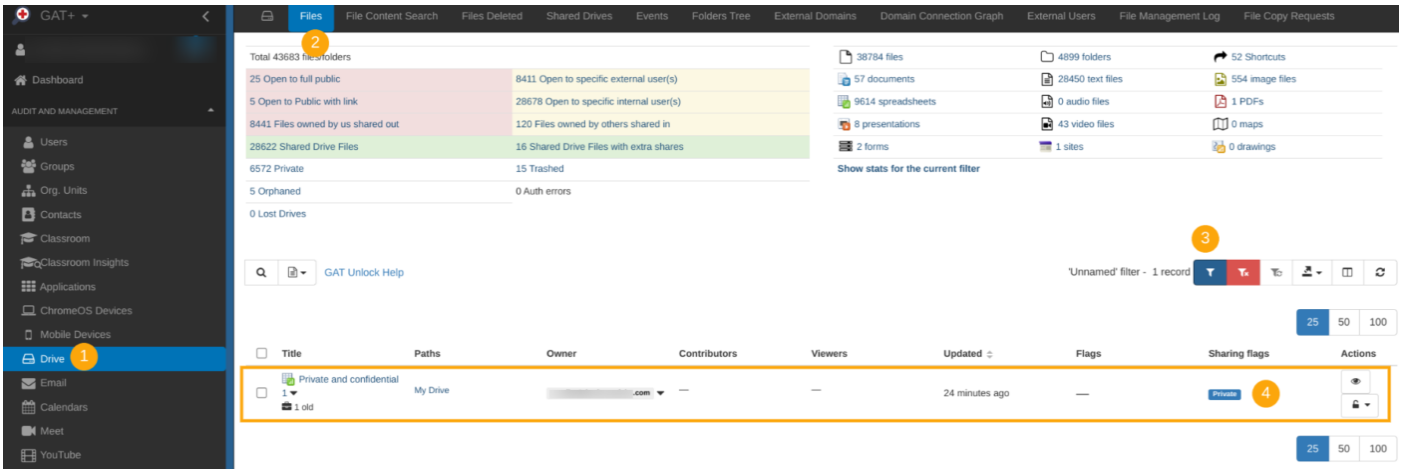


The result will be visible in the **GAT+ Drive** section when a new scan of the **Drive** metadata is completed.

To check, navigate to the Drive section of GAT+ **(1)**, under the Files tab **(2)** apply a filter **(3)** to find a file in question that was reported as shared out (you can use File Title, File ID, or any other metadata available from the report).

Subsequently, the file in question is returned by GAT+, and the privacy of the file can be confirmed under the **Sharing flag** section **(4)**.

This flag confirms that all existing external shares have been removed from the file and made it private again.




## Related posts

- Find documents that contain sensitive information in Google Drive
- Powerful SSN Detection Alert for your Enterprise
- How to apply and search for File content
- Remove all permissions to all ‘Sensitive’ folders and their sub-folders (in Google Drive)