

# Drive Auditing + File Access Control



# Drive Auditing + File Access Control



This guide explains how to audit Drive activity and control file access using GAT Labs tools. It's designed to help Google Workspace Admins gain better visibility, reduce data exposure risks, and take action on file permissions across their domain.

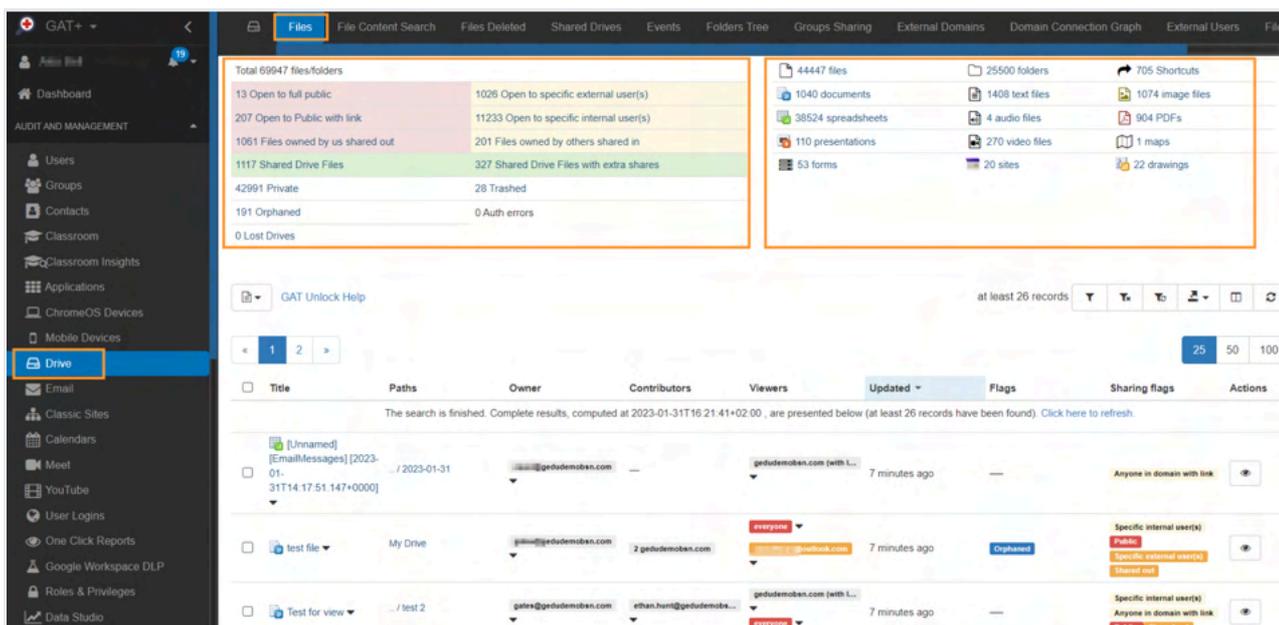
## 1. Access the Drive Audit Dashboard

Get full visibility into all Drive files across My Drive and Shared Drives. Use filters to narrow your scope and surface high-risk content.

If you've ever encountered the problem: "I can't see who's accessing what, especially in Shared Drives," this section is for you.

**Navigate:** *GAT+ > Drive > Files*

Here you can view the **one-click summary table**. This table will allow you to see all the files across your entire domain.



## Training Resources: Drive Auditing + File Access Control

From the dashboard summary table, you can instantly view the total number of Drive files across your domain, grouped by:

- **File exposure** (public, internal, external)
- **File type** (Docs, Sheets, PDFs, etc.)

All the files will be divided based on the **Sharing permissions** they have:

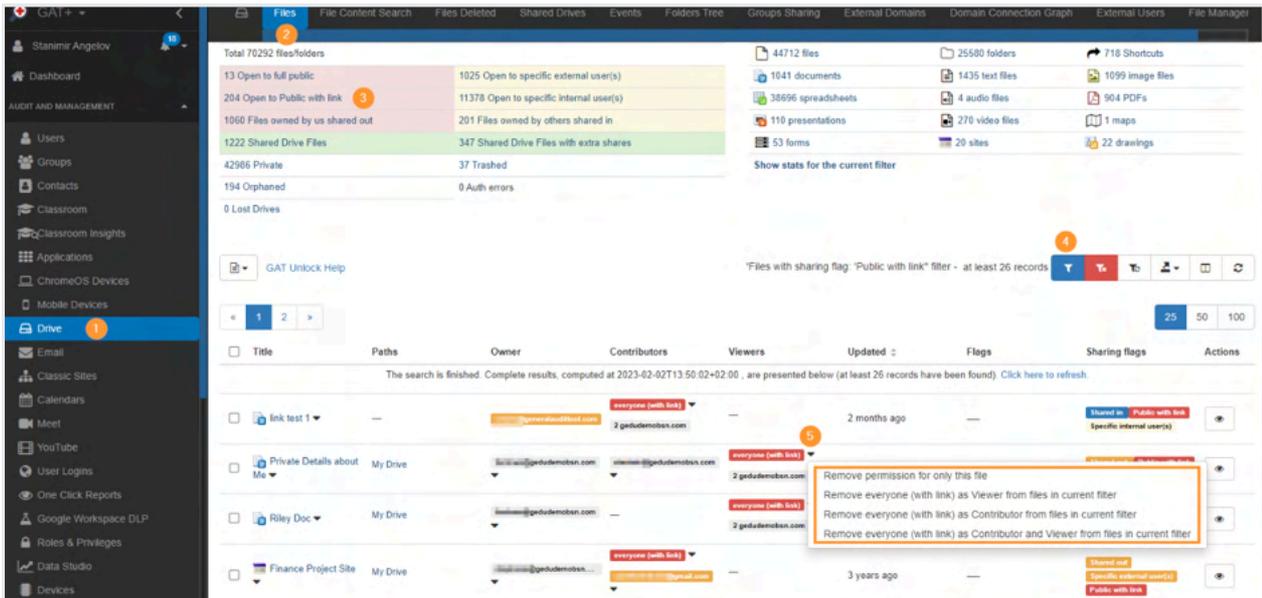
- **Open to public:** all files with public permission
- **Open to public with link:** all files with public with link permission
- **Files owned by us shared out:** all files shared out to external users
- **Shared Drive Files:** all files from the Shared Drives
- **Private:** all private files on the domain ( not shared to anyone)
- **Orphaned:** orphaned when the parent folder is missing
- **Lost Drives:** a local Shared Drive that cannot be audited because it has no local members
- **Open to specific external user(s):** all files that are shared to specific external users (no public or public with link permissions)
- **Open to specific internal user(s):** all files shared to specific internal users
- **Files owned by others shared in:** externally owned file shared into the domain
- **Shared Drive Files with extra shares:** all shared drive files with extra shares
- **Trashed:** all Google Drive files that are in the trash folder

Click any category to instantly apply a filter and view those files below.

# Training Resources: Drive Auditing + File Access Control

For example:

- Clicking on the *Open to Public with link*, will apply a filter for all the files (3)
- This filter can be seen by selecting the “funnel icon”, filter button (4)
- Additional filters can be applied to include or exclude certain data
- On the Permission itself, the sharing can be removed (5)



**Related Articles:** [Audit Google Drive](#)



## Training Resources: Drive Auditing + File Access Control

**Bonus Tip:** To see broader access patterns across entire external domains:

**Navigate:** *GAT+ > Drive > External Domians*

- Filter by Owner domain or Shared with domain to audit external access at scale.

### Result:

You'll see a breakdown of external file access across:

- **Individual external users:** including what files they can view or edit
- **External domains:** highlighting broader sharing trends into or out of your organisation

### Visual indicators in the results:

- Grey background = local (internal) users
- Amber background = external users outside your domain

Title	Paths	Owner	Contributors	Viewers	Commenters	Updated	Shared out	Flags	Sharing flags	Actions
Share with gmail	My Drive	external@generala...	external@gedade...	external@gedade...		20 days ago	3 months ago		Specific external user(s) Shared out	
[Report for daily Email activity]	My Drive / DailyEmailReport / April	external@generala...		external@gedade...		3 months ago	3 months ago		Specific external user(s) Shared out	
restricted test	My Drive	external@generala...		external@gedade...		3 months ago	3 months ago		Specific external user(s) Shared out	
Darren Hee	My Drive / Meet Recordings	external@generala...		everyone (with link)		5 months ago	5 months ago	Restricted	Specific internal user(s) Public with link Shared out	

### Related Articles:

[Identify Access by external user to any Google Drive file on your domain](#)

## 3. Find publicly shared Google Drive files

Navigate: **GAT+ > Drive > Audit table**

1. Select **"Full Public (everyone)"** or **"Public with link (everyone with link)"**
2. This will apply a filter where Sharing Flag contains **"Public"** or **"Public with link"**
3. **Add additional filter:** Sharing Flag does not contain **"Shared In"** to exclude externally shared-in files

Title	Paths	Owner	Contributors	Viewers	Updated	Flags	Sharing flags	Actions
testing	4 Replace Public on web	4 Replace Public on web	4 Replace Public on web	2 gatkdemoban.com	5 months ago	Shared Drive Shared Drive Extra ACLs	Public with link Shared out	
testing	~/ Public on the web	2 Remove ONLY the following External Shares	2 gatkdemoban.com	2 gatkdemoban.com	5 months ago	Shared Drive Shared Drive Extra ACLs	Public with link Shared out	
Admin console.webm	~/ Screencastify My Drive / Screencastify	carlos.gatkdemoban.com	2 gatkdemoban.com	nk.perry@gatkdemoban.c...	2 months ago		Public with link Shared out	
Testing	4 Replace Public on web	4 Replace Public on web		2 gatkdemoban.com	5 months ago	Shared Drive Shared Drive Extra ACLs	Public with link Shared out	
Master Chromebook List - Distribution Sheet	~/ Sel's ChromeOS Devices Exporte	andres@gatkdemoban.com		gammster@gatkdemoban.c...	4 months ago		Public with link Shared out	
Logs	My Drive	student.user@gatkdemoban.com		everyone (with link)	2 years ago		Public with link Shared out	

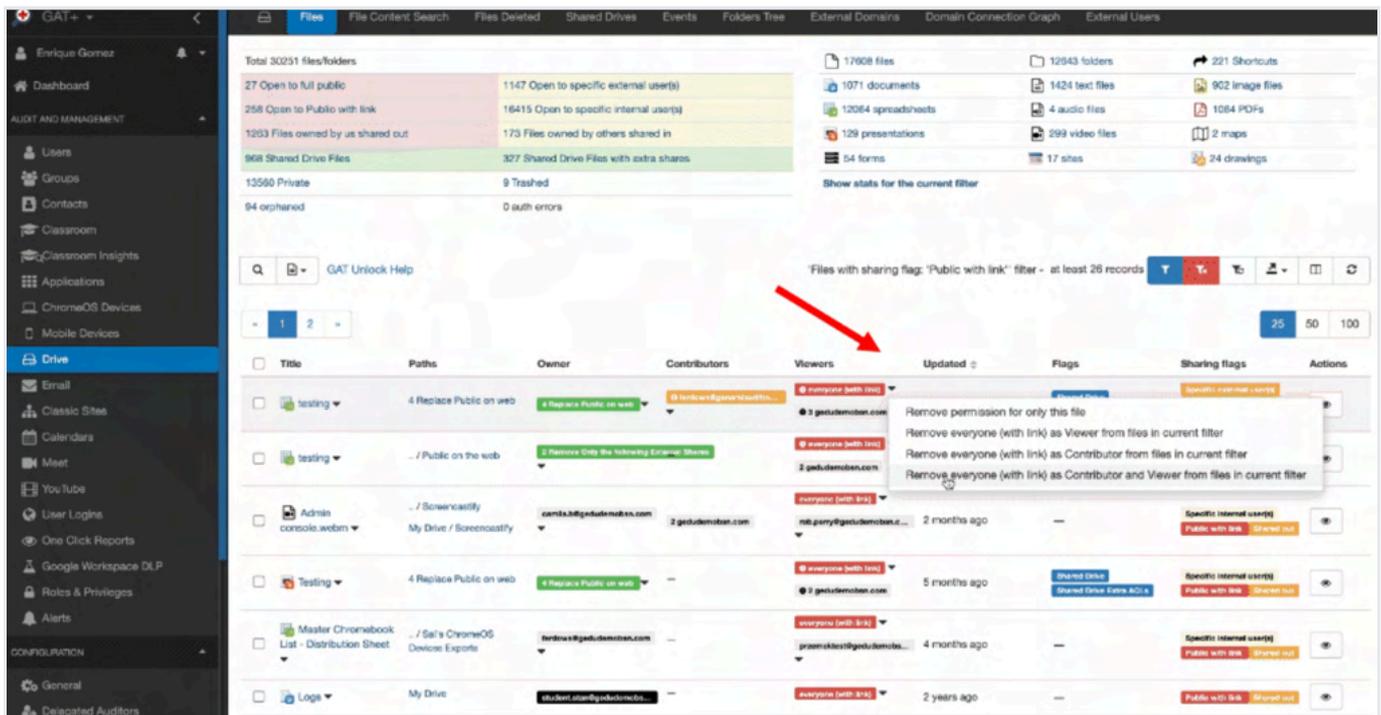
### Result:

You'll now see all files that have touched your domain, that are publicly accessible to anyone with an internet connection, and a navigation link to the file.

## Training Resources: Drive Auditing + File Access Control

Click on any of the **"Everyone (Public)"** permission label arrows to open some actionable options:

- **Remove this permission:** Removes the *public permission* from the selected file
- **Remove everyone as Viewer:** Removes 'Viewer' permission across all files in the current filter
- **Remove everyone as Contributor:** Removes 'Editor' permission across all files in the current filter
- **Remove everyone as Contributor and Viewer:** Fully revokes public permissions



The screenshot displays the Google Drive Admin console interface. On the left is a navigation sidebar with sections like 'AUDIT AND MANAGEMENT' and 'CONFIGURATION'. The main area shows a list of files with columns for Title, Paths, Owner, Contributors, Viewers, Updated, Flags, and Sharing flags. A red arrow points to the 'Viewers' column, where a dropdown menu is open. The menu options are: 'Remove permission for only this file', 'Remove everyone (with link) as Viewer from files in current filter', 'Remove everyone (with link) as Contributor from files in current filter', and 'Remove everyone (with link) as Contributor and Viewer from files in current filter'. The table lists several files, including 'testing', 'Admin console.webm', and 'Master Chromebook List - Distribution Sheet', each with its own set of permissions and sharing flags.

You can also generate a report and notify file owners of these permissions.

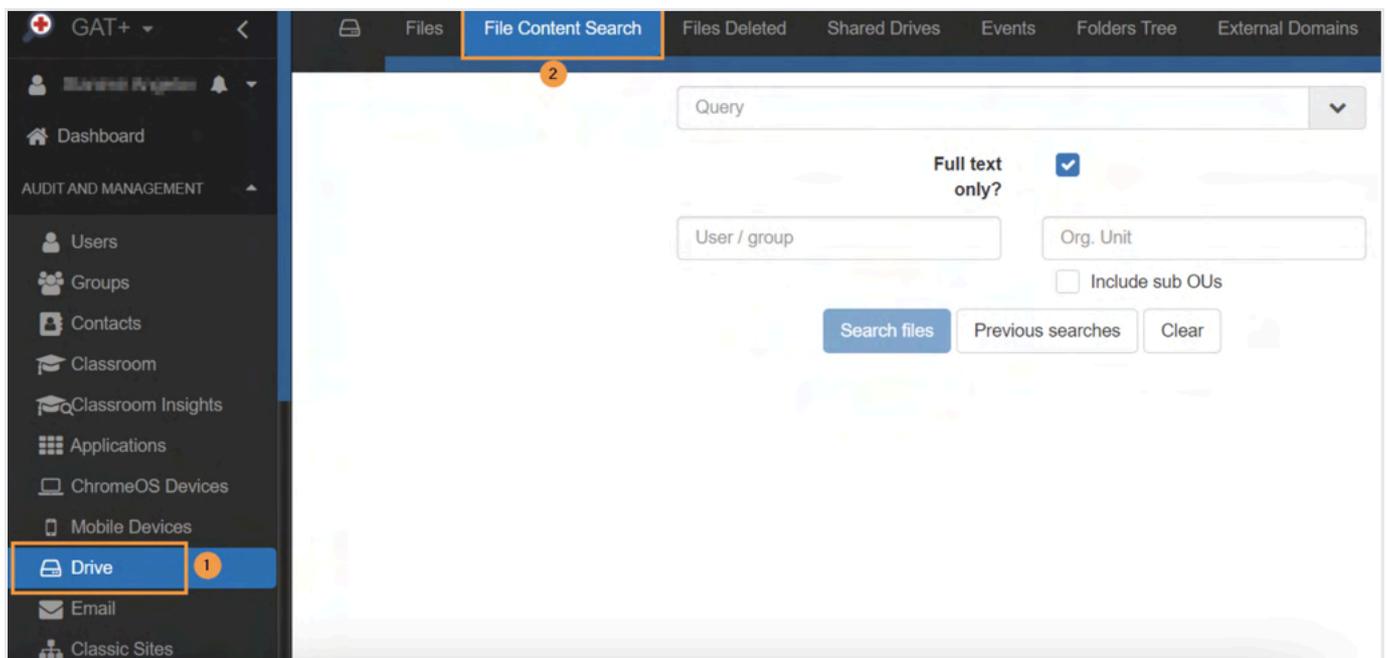
**Related Articles:** [Find Publicly Shared Files](#)

# 4. Search for Sensitive Content in Files

This section helps admins detect sensitive terms such as personal data, financial info, or confidential keywords.

Full context search is a direct (live) API call to search in Google Drive for any user of the domain.

**Navigate:** *GAT+ > Drive > File Content Search*



### Use Case Example:

A compliance officer wants to check if any documents in the Sales OU contain the term "SSN".

### Steps:

- 1. Query:** Enter the search term needed
  - Show more options: click on the drop-down arrow on the right side to see syntax query options to refine your search – [search queries](#)
- 2. Full text only:** When checked, your query will include searching text in the body of all files, as well as all other other metadata in the file. You would only uncheck this box if you wanted to target your search to a specific part of the file meta-data (eg. name = 'My Project Data')/

## Training Resources: Drive Auditing + File Access Control



### 3. Users: select on which users to apply the query filter

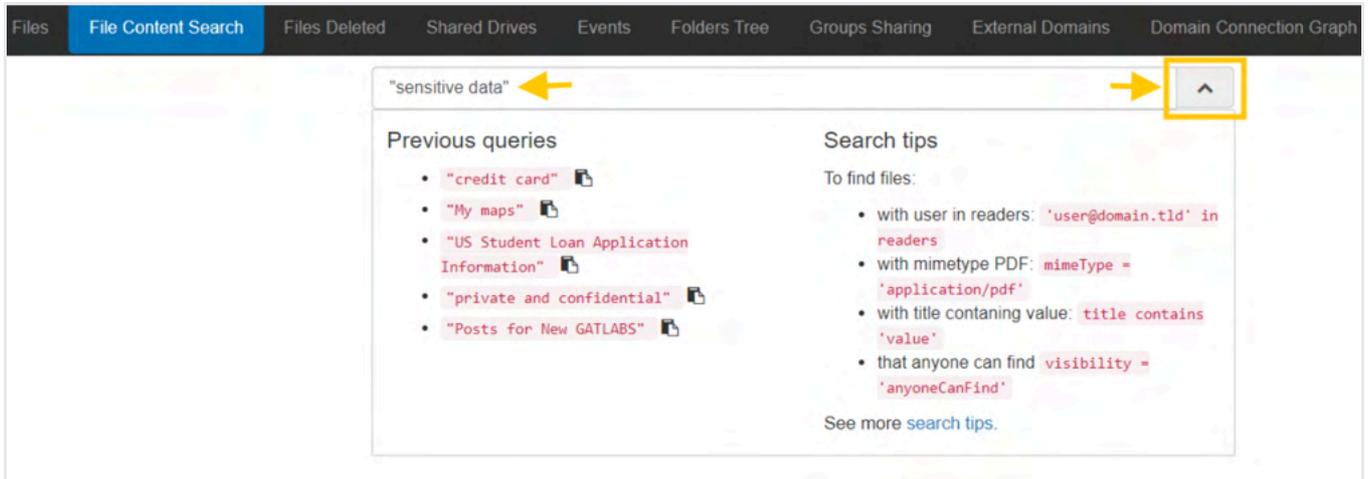
- User
- Group
- Org. Unit: enter “/” to search domain-wide
  - a. Include sub. ou

### 4. Search files: select when the query and users are selected

Depending on the query applied, different results will be displayed:

- **“sensitive data”**: means that any files containing both words in that exact order will be displayed as result.
- **sensitive data**: without quotes means any file that contains both words, doesn't have to be in any particular order. For example, the word “Sensitive” could be in the title and the word “data” can be in the content (body).

Show more options: click on the “arrow” on the right side to see options [\[search queries\]](#)



# Training Resources: Drive Auditing + File Access Control

## Result:

You'll see all files that match your search query.

The screenshot displays the 'File Content Search' interface. At the top, there's a navigation bar with tabs like 'Files', 'File Content Search', 'Files Deleted', etc. The search bar contains the query 'sensitive data'. Below it, there are checkboxes for 'Full text only?' (checked) and 'Include sub OUs' (checked). There are also buttons for 'Search files', 'Previous searches', and 'Clear'. Below the search bar, there are navigation controls including a dropdown menu, a page indicator showing '1' of '2' pages, and a record count of 'at least 26 records'. The main area is a table with the following columns: Title, Paths, Owner, Contributors, Viewers, Updated, Flags, and Sharing flags. The table contains four rows of search results:

Title	Paths	Owner	Contributors	Viewers	Updated	Flags	Sharing flags
How to secure	My Drive / Orphaned	generalaudittool.com	generalaudittool.com	—	34 minutes ago	—	Specific internal user(s)
SOC 2 Criteria and	My Drive / Orphaned	generalaudittool.com	generalaudittool.com	—	40 minutes ago	—	Specific internal user(s)
Copy of Security	My Drive / Orphaned	generalaudittool.com	generalaudittool.com	—	42 minutes ago	—	Specific internal user(s)
Video Production	My Drive	generalaudittool.com	4 generalaudittool.com	—	an hour ago	—	Specific internal user(s)

From here, the admin can remove the sharing permissions on the found files, if desired.

**Related Articles:** [Find documents that contain sensitive information in Google Drive](#)

# 5. See Who Viewed What and When

Use Case: “I need to know who accessed sensitive Drive files and when, especially before a potential data leak.”

Navigate: **GAT+ > Drive > Events**

### Steps to Track File Viewing Activity:

1. Click “Apply custom filter”
2. Fill in the details:
  - **Name:** (Optional) Give your search a name (this will also be used to name a scheduled report if you choose to generate one)
  - **Type:** Select Simple Filter
  - **Definition:**
    - Event Quality View
    - Email equal [\[user@example.com\]](#)
    - **Date (relative):** in the last [x] days
3. Click Apply to see all Drive view events by the selected user.

## Training Resources: Drive Auditing + File Access Control

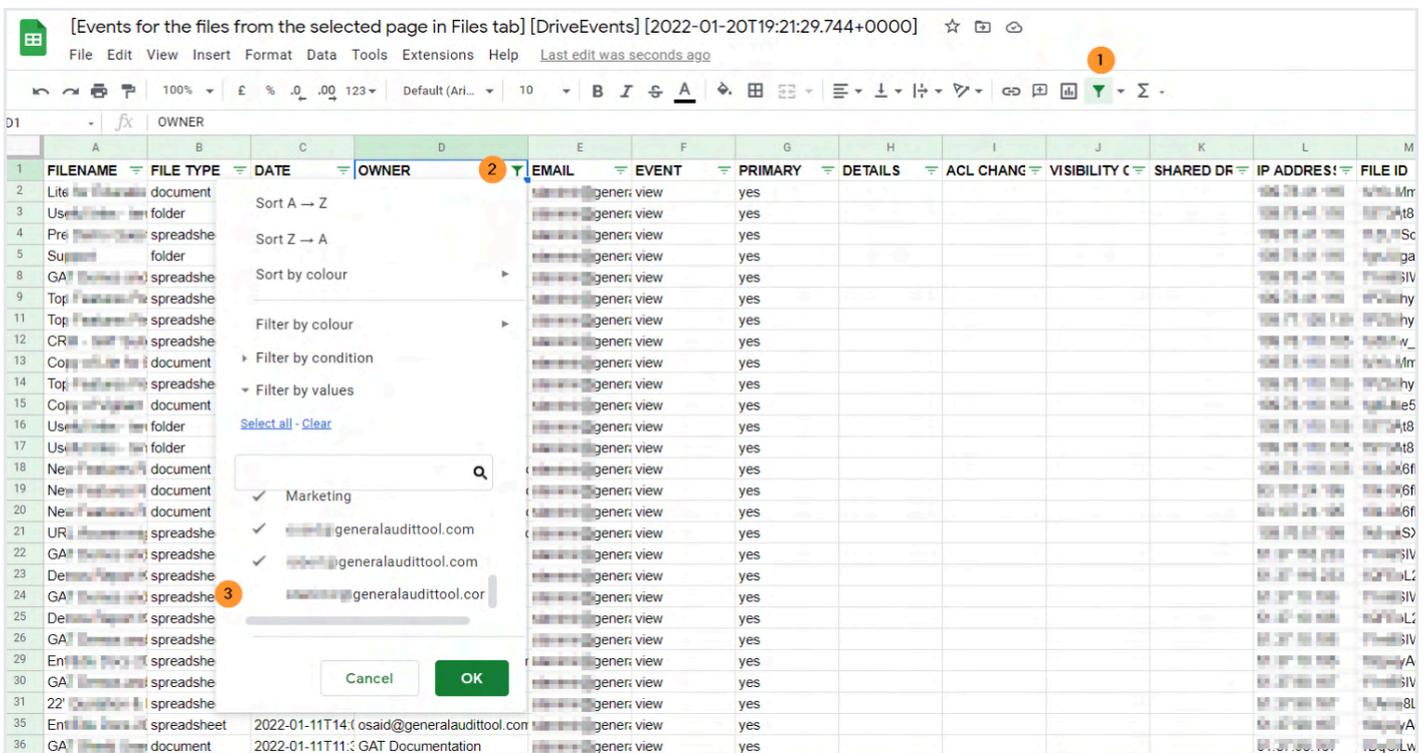
### Result:

The result will show all the 'view' events by the selected user in the past 30 days", corresponding to the user in the filter applied above.

### Pro Tip:

Want to exclude files the user owns?

- Export the results as a Google Sheet or CSV.
- In the Google Sheet, apply a filter and exclude the user from the Owner field.
- The result you'll get is all the documents visited by the subject, excluding the files that the person owns.



The screenshot shows a Google Sheet titled "[Events for the files from the selected page in Files tab] [DriveEvents] [2022-01-20T19:21:29.744+0000]". The sheet has columns for FILENAME, FILE TYPE, DATE, OWNER, EMAIL, EVENT, PRIMARY, DETAILS, ACL CHANG, VISIBILITY C, SHARED DR, IP ADDRESS, and FILE ID. A filter is applied to the OWNER column, showing a list of filters: Sort A → Z, Sort Z → A, Sort by colour, Filter by colour, Filter by condition, and Filter by values. The Filter by values filter is selected, and a list of values is shown: Marketing, generalaudittool.com, and generalaudittool.cor. The table contains 36 rows of data, with the first row being the header row. The data shows various file types (document, folder, spreadsheet) and events (generally 'view') for different users and files.

FILENAME	FILE TYPE	DATE	OWNER	EMAIL	EVENT	PRIMARY	DETAILS	ACL CHANG	VISIBILITY C	SHARED DR	IP ADDRESS	FILE ID
Lite for Education	document				gener: view	yes						
Useful for Education	folder				gener: view	yes						
Pre	spreadshe				gener: view	yes						
Support	folder				gener: view	yes						
GAT	spreadshe				gener: view	yes						
Top	spreadshe				gener: view	yes						
Top	spreadshe				gener: view	yes						
CR	spreadshe				gener: view	yes						
Copy	document				gener: view	yes						
Top	spreadshe				gener: view	yes						
Copy	document				gener: view	yes						
Useful for Education	folder				gener: view	yes						
Useful for Education	folder				gener: view	yes						
New	document				gener: view	yes						
New	document				gener: view	yes						
UR	spreadshe				gener: view	yes						
GAT	spreadshe				gener: view	yes						
De	spreadshe				gener: view	yes						
GAT	spreadshe				gener: view	yes						
En	spreadshe				gener: view	yes						
GAT	spreadshe				gener: view	yes						
22	spreadshe				gener: view	yes						
En	spreadsheet	2022-01-11T14:10:00	osaid@generalaudittool.com		gener: view	yes						
GAT	document	2022-01-11T11:11:00	GAT Documentation		gener: view	yes						

### Related Articles:

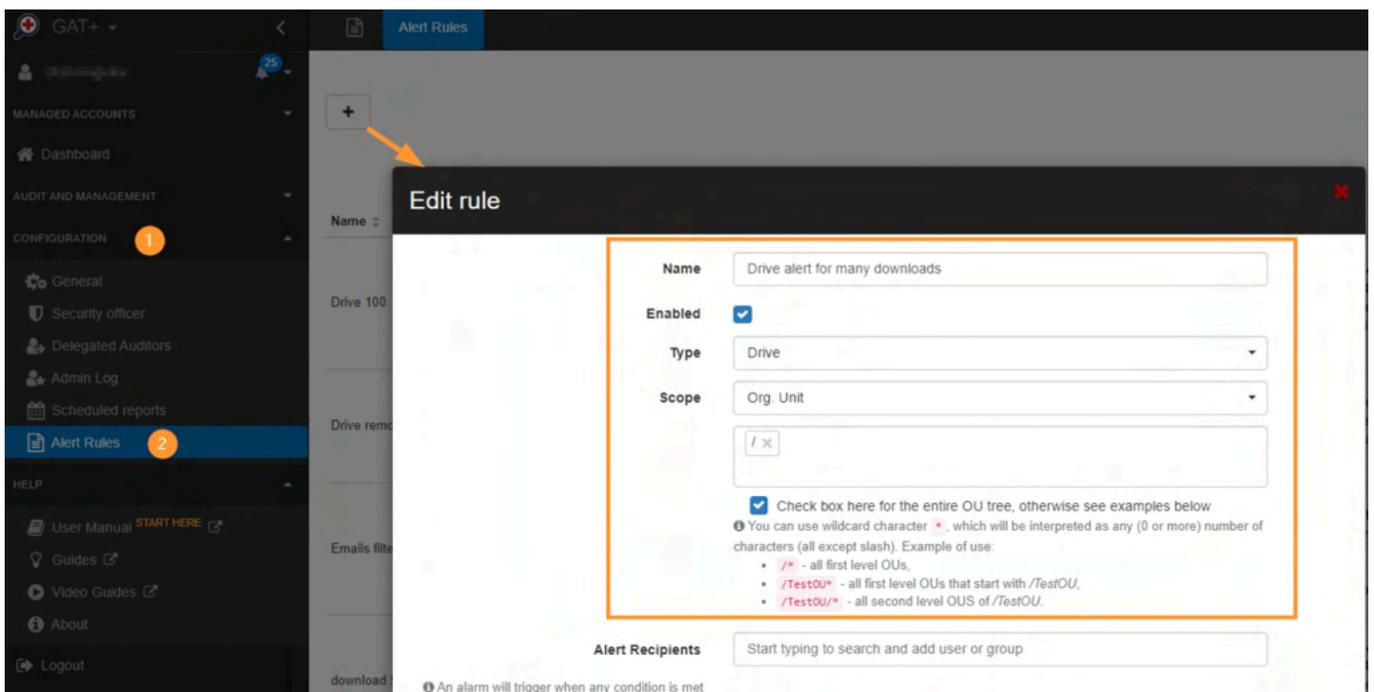
- [Who Read What Google Drive Document and When?](#)
- [How to Track Visitors and Editors of Specific Documents](#)

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

Navigate: **GAT+ > Configuration > Alert Rules**

Click on the '+' icon, and a new window will be displayed. Fill in the Name and select some of the details that are shown. Your options are as follows.

- **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 the 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.

## Training Resources: Drive Auditing + File Access Control

### 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.

Alert on number of files downloaded

Enter the number of files that will trigger the alert

50

files in a 24 hour period

Exclude the following applications from calculation

- Google Drive for desktop

Search for an application that should be excluded from the alert

Type in the application name

The alert will be triggered when 50 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.

Alert on number of files shared out

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

You can exclude certain applications from triggering this alert that may trigger it by downloading files on a users behalf (eg. a cloud backup solution).

### Result:

You'll be alerted when a user downloads a large volume of files in a short period, allowing you to investigate early signs of data leakage.

**Related Articles:** [Set Up Google Drive DLP Alert](#)

# 7. Create Scheduled Reports in Drive Audit

The scheduling mechanism is built into the query filter button. In any filter menu of GAT+ you can apply a filter condition, and have the results of the filter sent via email in export format, as a scheduled export.

### Creating a Schedule Report using Filter Conditions:

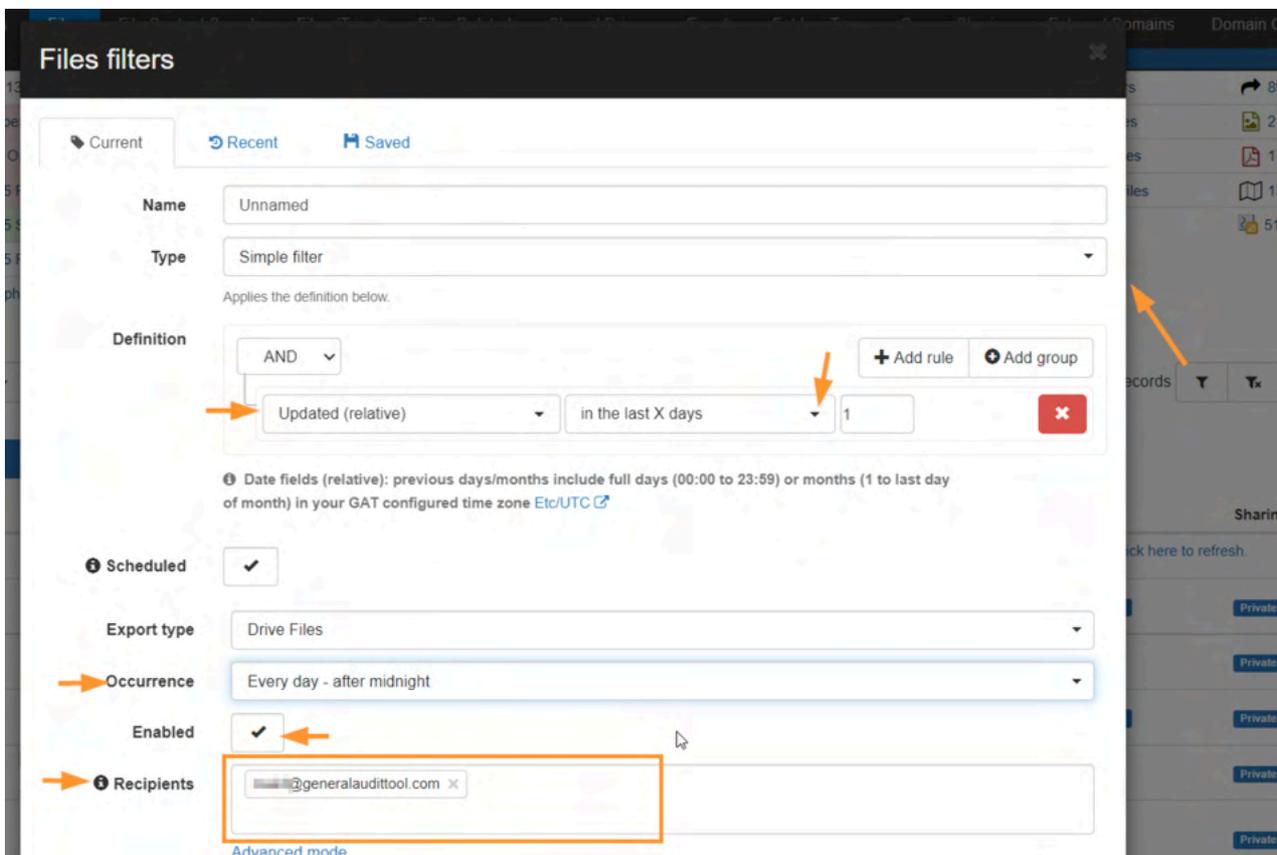
You can easily introduce the scheduling mechanism on any filter you have applied. You can the results of your filter emailed to your inbox (or another admin's inbox) on a regular basis. This normally works best when a time parameter is included in the filter.

The following example will be a report about files recently edited.

Navigate: Drive > Files

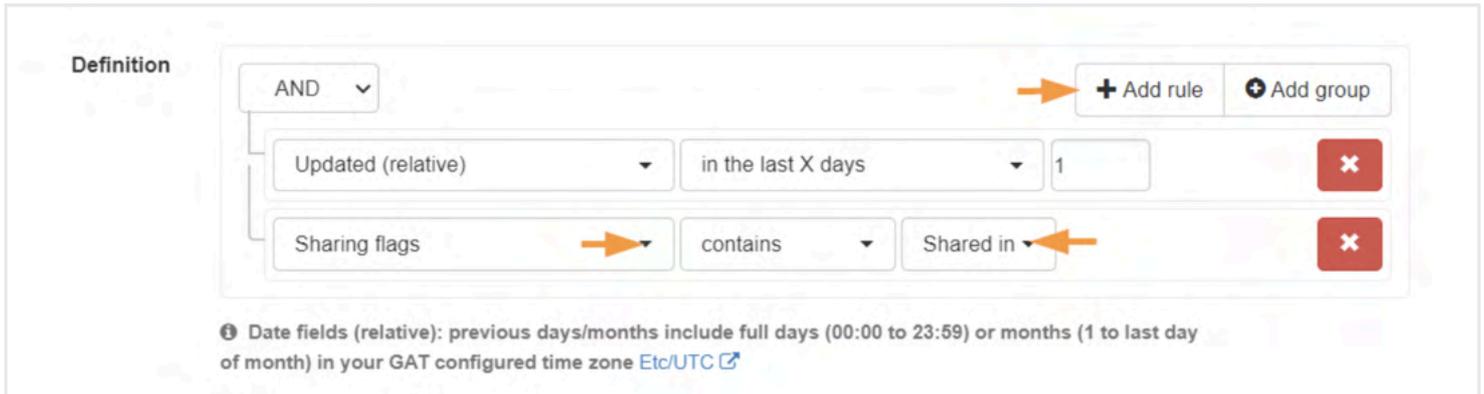
### Steps :

1. Create a filter condition (e.g., Updated (relative) in last x days). Creating scheduled reports is done by clicking on the 'Scheduled' checkbox on the drive file filter menu.



## Training Resources: Drive Auditing + File Access Control

2. You can share this report with multiple admins by adding their email addresses into the 'Recipients' field.
3. You may be interested in expanding the above filter condition, to report on files shared in and updated yesterday, or files shared out and updated in the last week etc. To do this, you can simply expand on the filter and add another rule. Click on 'Add rule' and select the 'Sharing Flags' filter option, and set it to 'Shared in'.



Definition

AND

+ Add rule + Add group

Updated (relative) in the last X days 1

Sharing flags contains Shared in

**i** Date fields (relative): previous days/months include full days (00:00 to 23:59) or months (1 to last day of month) in your GAT configured time zone [Etc/UTC](#)

This will report on files that are 'shared in' from external domains, and also, were 'updated' (edited, shared, renamed) in the last day.

4. When you have finalized your filter, go ahead and *Apply & Schedule*.

### Result:

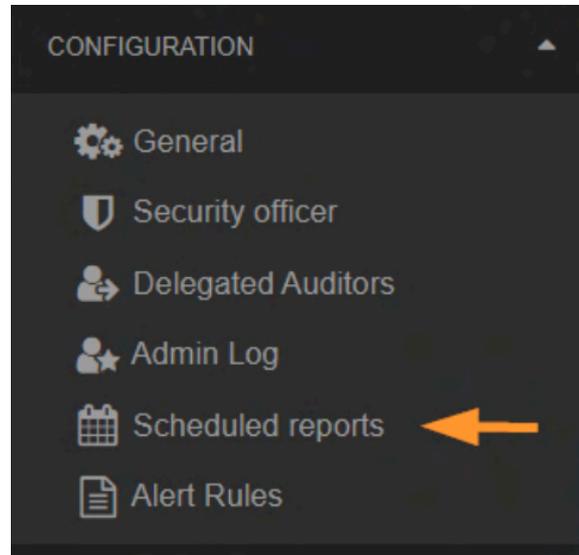
At the set time, you will receive an email with a link to your report in your email inbox, and the link will bring you to the export in Google Sheet spreadsheet format, with the relevant data, related to the filter you have set on that day. The file will be placed in the file path that GAT will have created on your behalf, under [GAT/<yourDomainName>/DriveAudit/<currentDate>/](#)

*Note: You can change the search operands to report back on all file types and or exposures. For more details, contact [support@generalaudittool.com](mailto:support@generalaudittool.com)*

## Training Resources: Drive Auditing + File Access Control

### Viewing your scheduled jobs:

Under the Configuration area of GAT+, you can view all the scheduled reports that have been created by super admins by clicking on '*Scheduled reports*':



**Related Articles:** [Create Scheduled Reports in Drive Audit](#)

## **Additional Resources for Drive Auditing & File Access Control**

- [Remove shares from owned files in Google Drive](#)
- [Remove and replace Google Drive sharing permissions based on Files not being accessed for X amount of days](#)
- [Domain Security Monitoring with GAT+ Activity Report](#)
- [Find and Take Action on Shared Files](#)
- [Report on Files Shared Out to Gmail Accounts](#)
- [Copy Externally Owned Folders and Retain Structure](#)
- [View Google Drive Quota and Set Storage Alerts with GAT+](#)

## Want To Learn More?

[VISIT OUR WEBSITE](#)

[VISIT OUR RESOURCES PAGE](#)

[TRAINING SESSIONS CALENDAR](#)