



The Google Admin's Guide To Securing Files Shared Internally And Externally

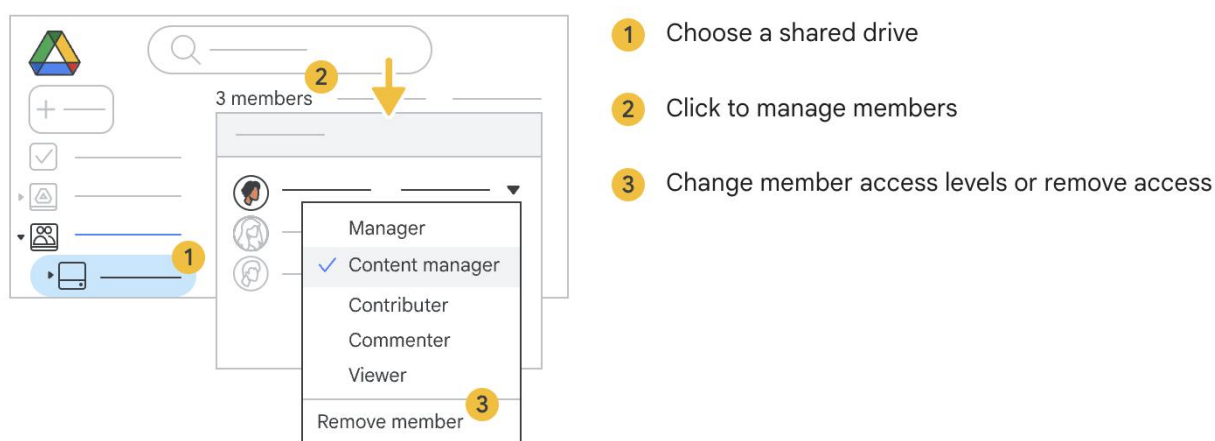
SECURE YOUR GOOGLE WORKSPACE

Google Drive powers collaboration, but managing files shared within and outside the organisation can be challenging, especially for Google Admins focused on security.

This guide provides actionable steps for **monitoring files shared in and files shared externally**, ensuring robust data security across your Google Workspace.

1. Understanding Google Drive Sharing Permissions

A well-organised permission structure is essential for managing data access. Drive permissions include Viewer, Commenter, and Editor levels, each allowing different degrees of access to information.



- 1 Choose a shared drive
- 2 Click to manage members
- 3 Change member access levels or remove access

It's crucial to:

- Review and assign permissions based on [user roles](#), avoiding unnecessary Editor permissions.
- Set default [internal and external sharing settings](#) in the Google Admin Console, restricting access to sensitive files.

Steps:

- Go to **Admin Console > Apps > Google Workspace > Drive and Docs > Sharing Settings**.
- Configure internal and external sharing defaults to limit unnecessary exposure.

2. Auditing Files Shared Externally

Regular audits of files shared externally can prevent unauthorised access. Use [Google's File Sharing Exposure report](#) to gain insight into shared files and ensure only authorised users retain access.

How to Conduct an Audit:

- Open the Admin Console, and navigate to **Reporting > Drive Audit**.
- Review shared files and their access levels, particularly for external shares.

Automate Audits with GAT+: Including Shared-in Files

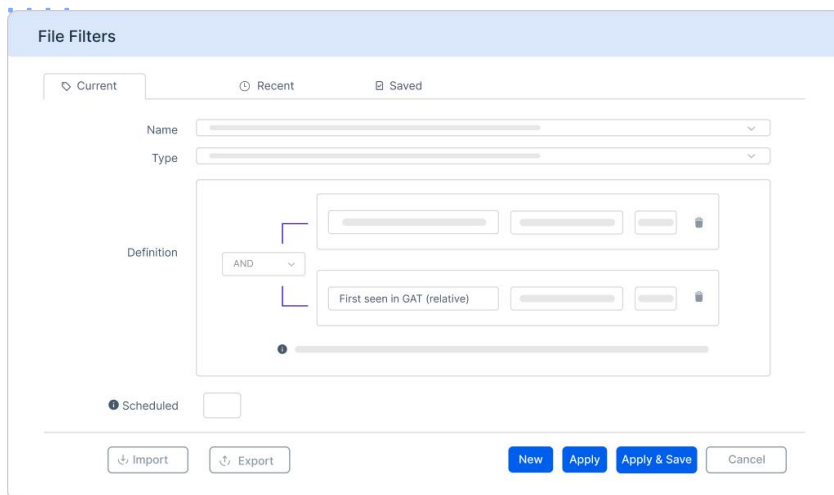
- Use GAT+ to create [automated reports of files shared externally](#), allowing you to detect any sharing anomalies quickly. This includes Shared-in files—files owned by an external user from another domain and shared with your organisation. GAT+ identifies these files uniquely, with external owners highlighted in orange for easy tracking under the “Owner” heading in the Drive audit.

Key Capabilities:

- **Scheduling Reports:** Set daily, weekly, or monthly reports for recently shared-in files, ensuring a regular audit of external shares.
- **Unique Search Operators:** GAT+'s “[First seen in GAT+](#)” search operator tracks when files were initially shared in, an advanced feature not available through Google's API.

Pro Tip:

Use GAT+'s alerts for files newly shared in to ensure admins have visibility over shared data in real time. For more details, view our [Knowledge Base article](#).



3. Structuring Files Shared in Google Drive

Organising files shared in Google Drive is crucial for data access control. A well-thought-out Shared Drive layout helps admins manage permissions and segment data access effectively.

Best Practices for Structure:

- Organise by department, function, or project to restrict access based on team needs.
- Set permissions at the folder level within Shared Drives, allowing each sub-folder to have more refined controls.

GAT Shield for Enhanced Control:

- [GAT Shield](#) enables admins to monitor permission changes across Shared Drives and ensure the structure remains secure. It offers real-time alerts for any modifications in file access, helping maintain control and compliance in Google Drive.

Best Practice

Regular audits minimise risks, especially for sensitive files. Schedule **monthly reviews** to stay proactive.

Practical Example:

- For a marketing department, create a **“Marketing” Shared Drive** with subfolders like **“Campaigns,” “Analytics,”** and **“Assets.”**
- Assign permissions so **only** relevant team members have access to specific subfolders.

4. Managing and Tracking External File Shares






Tracking external shares is essential to prevent sensitive data from leaving the organisation.

How to Find Files Shared Externally:

- Use GAT+ to [locate all files shared externally](#) in Google Drive. This can include any documents, spreadsheets, or presentations shared outside the company.

Steps to Manage External Sharing:

- In GAT+, use filters to display only externally shared files.
- Review permissions, especially for files shared publicly, and adjust as necessary.

Top 5 users sharing out files			
Name	Owned files	Public with link	Shared out
 Candice Wu candice@gat.com	25,223	7,300	19,556
 Natali Craig @natali@gat.com	24,473	1,647	245
 Drew Cano drew@gat.com	14,090	978	12,788
 Orlando Diggs orlando@gat.com	13,631	2,888	9,817
 Andi Lane andi@gat.com	10,450	653	1,425

Risk Mitigation Tip:

Restrict external sharing for sensitive documents like financial reports or project plans.

5. Proactive Data Loss Prevention for Shared Files

[Data Loss Prevention \(DLP\)](#) policies help Google Admins protect sensitive information proactively. [Configure DLP rules](#) for files shared externally to monitor activity that could lead to data leaks, such as unauthorised downloads or sharing.

Setting Up DLP Alerts:

- In the **Google Admin Console > Security > DLP**.
- Create rules that trigger alerts if sensitive data is shared externally, such as documents containing personal information or financial data.
- Use GAT+ to extend DLP to real-time monitoring for high-risk files.

Practical Steps for Protection:

- Set up alerts for printing, downloading, or copying sensitive data.
- Use [content detectors](#) to flag specific keywords like “*confidential*” or “*sensitive*” in documents shared externally.

6. Handling Files Shared In From External Parties

Managing files shared from external sources into your organisation is essential for data security. In the Google Admin Console, admins can monitor these files by navigating to **Reports > Drive audit log**. From there, filter by events like Incoming file shares or External sharing to view files shared from outside domains.

For more detailed tracking, GAT+ enhances visibility by allowing real-time alerts and in-depth insights on incoming files. This helps admins ensure only trusted sources are sharing sensitive data with your organisation.

FAQs on File Sharing in Google Drive

Q: How often should I audit files shared externally?

A: Monthly audits are ideal for high-security environments. Use GAT+ to automate this process and receive alerts on new external shares.

Q: How can I prevent sensitive files from being shared externally?

A: Configure DLP policies and enforce permissions in the Admin Console to control external sharing.

Q: How can GAT Labs tools help with managing shared files?

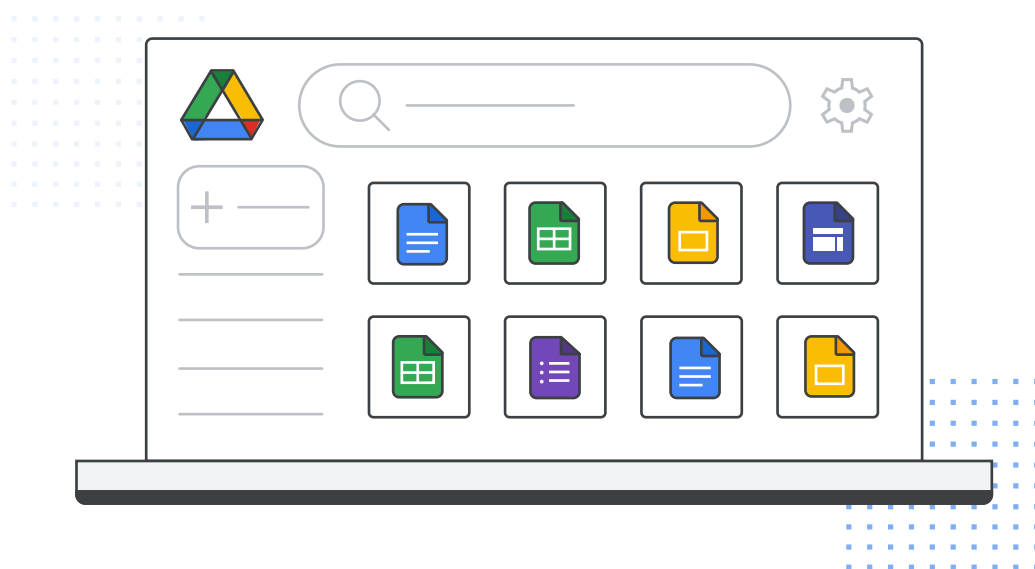
A: GAT+ and GAT Shield provide enhanced visibility, alerting, and reporting for files shared in and externally, streamlining Google Drive security.

Q: How can I restrict file-sharing settings for specific departments or teams?

A: In the Admin Console, customise sharing settings by organisational unit (OU). This allows you to limit external sharing permissions or disable sharing for sensitive teams, such as finance or HR, enhancing data security. GAT+ can help track and enforce these settings.

Q: What's the best way to handle file ownership transfers when offboarding employees?

A: Use GAT Unlock to securely transfer ownership of files from departing employees. This ensures no critical files are lost and prevents ex-employees from accessing shared data.



**For Enhanced
Google Drive Security,
Explore GAT Labs**

[DISCOVER MORE](#)

[VISIT OUR WEBSITE](#)

[SCHEDULE A DEMO](#)

[15 DAY FREE TRIAL](#)

