

**STEP BY STEP GUIDE**

# **10 Essential Steps to Audit your Google Workspace Domain with GAT Labs**



# Table of Contents

|  |    |
|--|----|
| 1. Access Management Audit .....           | 04 |
| 2. Administrator Role Audit .....          | 07 |
| 3. Security Audit .....                    | 09 |
| 4. Application Audit .....                 | 13 |
| 5. Drive and Shared Drives Audit .....     | 16 |
| 6. Email Compliance and Security Audit ... | 23 |
| 7. Compliance Audit .....                  | 28 |
| 8. Training and Policy Audit .....         | 37 |
| 9. Use Google Workspace Audit Logs .....   | 40 |
| 10. Regular Reviews .....                  | 41 |

# How to Audit your Google Workspace Domain with GAT Labs

In this guide, we will take you through the steps you need to perform to ensure your Google Workspace environment is as **secure and well audited as possible**.

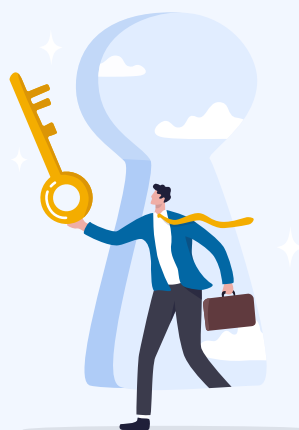
These steps are essential in their own right and an essential part of tasks such as **SOC II, HIPAA, FERPA or CIPA** compliance preparation or end of year security audits.

Our goal is to show you how to achieve these tasks quickly and efficiently with both the Workspace Admin console, GAT+ and other tools. Once proper audit and security is in place we will show you how to maintain that posture for your domain.

A prerequisite for performing most of these tasks is that you have installed and granted full access to GAT+ for the root OU and all sub-OU's in your domain. If you have not already done so, add GAT+ to your domain from [here](#). For certain additional browsing reporting, browser protection and compliance tasks GAT Shield may be required.

If you are unfamiliar with the changes you are making to your domain, it is always best to take a screenshot of the existing configuration and environment.

You can use these screenshots both as an audit path and an aid to revert in the event of unintended consequences to the changes that you make.



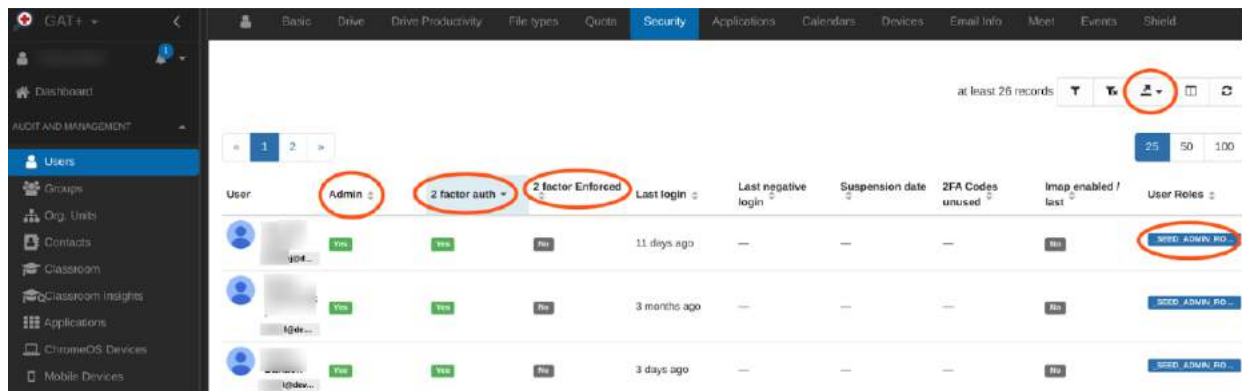
# Access Management Audit:

## 1.1 Review user accounts to ensure that only authorized personnel have access.

Understanding the security profile of each account and being able to see that information in a clear presentable way is the key to this review.

After the **GAT+ initial scan completes**, the first item on the Audit and Management menu is the Users audit. It covers many areas, from Basic user configuration to their Drive usage to their security profile.

Selecting the **Security table** is an essential first step and allows you to see which accounts have privilege or Admin rights, which have 2 factor authentication enabled, which accounts are idle for a long time (perhaps allowing for clean ups and saving license costs) and many other key fields



The screenshot shows the GAT+ interface with the 'Security' tab selected. The table displays user accounts with columns for User, Admin, 2 factor auth, 2 factor Enforced, Last login, Last negative login, Suspension date, 2FA Codes unused, Imap enabled / last, and User Roles. Several cells are circled in red to highlight specific features: the 'Admin' column, the '2 factor auth' and '2 factor Enforced' columns, and a 'User Roles' cell showing 'NONE: ADMIN, PO...'. The table also includes pagination controls and a filter icon.

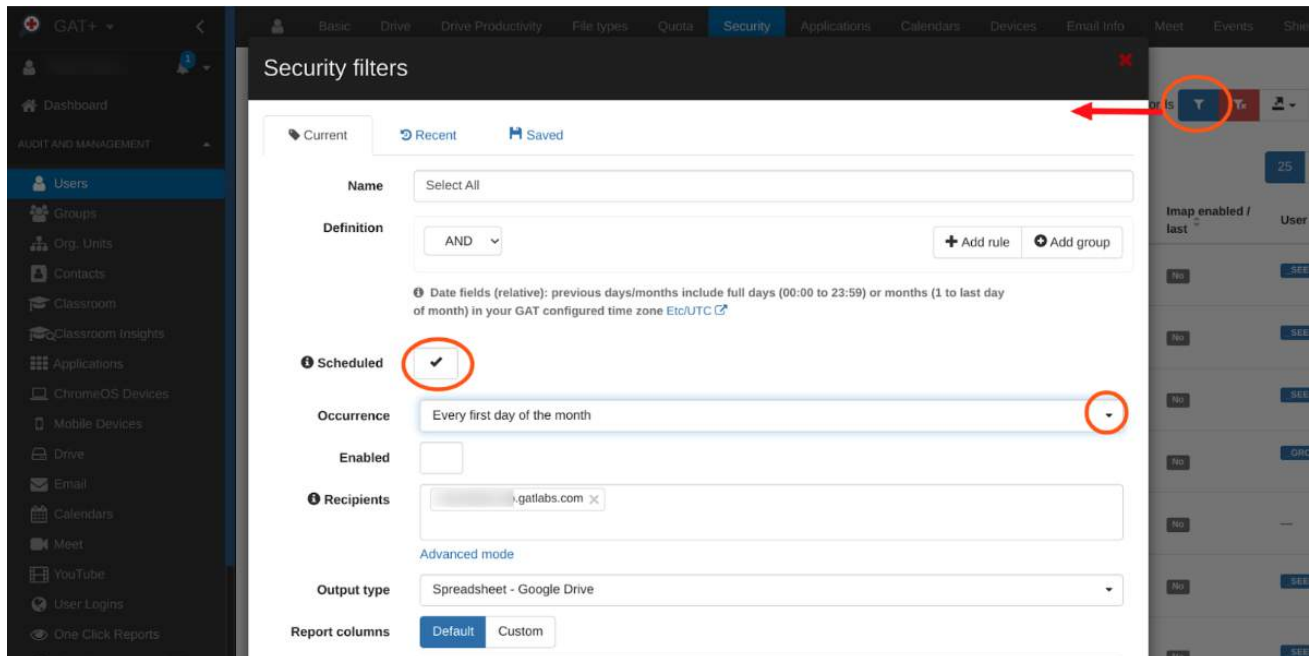
| User   | Admin | 2 factor auth | 2 factor Enforced | Last login   | Last negative login | Suspension date | 2FA Codes unused | Imap enabled / last | User Roles         |
|--------|-------|---------------|-------------------|--------------|---------------------|-----------------|------------------|---------------------|--------------------|
| id4... | Yes   | Yes           | No                | 11 days ago  | —                   | —               | —                | No                  | NONE: ADMIN, PO... |
| id4... | Yes   | Yes           | No                | 3 months ago | —                   | —               | —                | No                  | SECO: ADMIN, PO... |
| id4... | Yes   | Yes           | No                | 3 days ago   | —                   | —               | —                | No                  | SECO: ADMIN, PO... |

As with most tables you can select from multiple columns and all data can be exported to a spreadsheet (a Google sheet or a CSV file).

Not only that, but as with most tables, the output can be turned into a scheduled report, helping you meet your audit tracking and reporting requirements. In the security table simply click on the Filter icon to generate a report configuration table. To report on all fields in the report, delete the filter definition. To make it a scheduled report, check the scheduled box and complete the remaining fields as appropriate.



# 1 Access Management Audit:



**Note the above step**, as you will be able to do this again and again with reports that you deem critical. To get the full report we removed the filter selector, thus selecting everything.

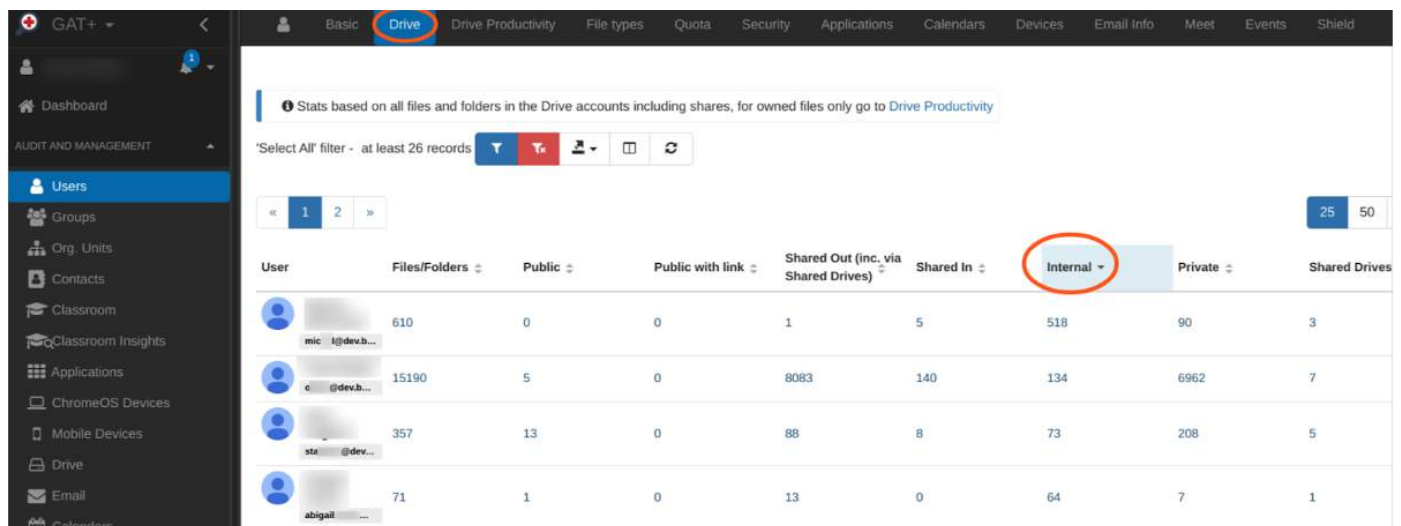
## 1.2 Verify that former employees or non-active users are suspended, archived or deleted.

From the first table and selecting the sort function on columns you can see how easy it is to report on inactive or suspended accounts.

# Access Management Audit:

## 1.3 Check for any external sharing of internal documents and ensure it complies with company policies.

To verify the status here for each user we select a different table in the Users report. Under the Drive table you can find statistics and nearly every aspect of a user's Drive behavior. Each of the columns can be sorted to identify such concerns as excessive sharing.



The screenshot shows the GAT+ interface with the 'Drive' report selected. The report displays statistics for four users across various sharing categories. The 'Internal' column is circled in red.

| User           | Files/Folders | Public | Public with link | Shared Out (inc. via Shared Drives) | Shared In | Internal | Private | Shared Drives |
|----------------|---------------|--------|------------------|-------------------------------------|-----------|----------|---------|---------------|
| mic l@dev.b... | 610           | 0      | 0                | 1                                   | 5         | 518      | 90      | 3             |
| e @dev.b...    | 15190         | 5      | 0                | 8083                                | 140       | 134      | 6962    | 7             |
| sta @dev...    | 357           | 13     | 0                | 88                                  | 8         | 73       | 208     | 5             |
| abigail        | 71            | 1      | 0                | 13                                  | 0         | 64       | 7       | 1             |

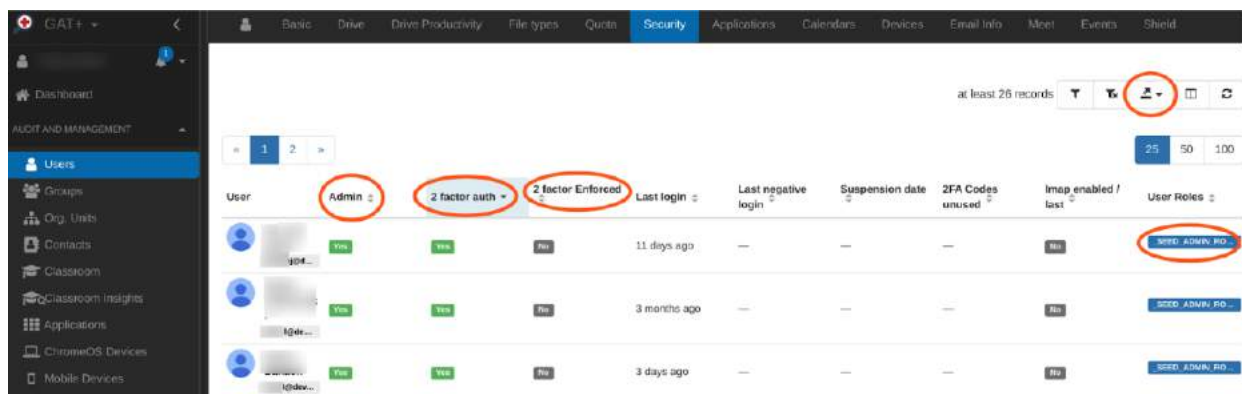
Reports can again be [exported or scheduled for export](#), thus providing input for other reports or keeping a permanent record.

[Every number is clickable](#) to see the exact detail for each file including exactly who it is shared with. In later sections we will discuss how to revoke sharing and how to automate the sharing revocation process.

# 2. Administrator Role Audit:

## 2.1 Ensure that only a few trusted individuals have administrative access.

This is a repeat of the first step in the Access Management Audit.



| User   | Admin | 2 factor auth | 2 factor Enforced | Last login   | Last negative login | Suspension date | 2FA Codes unused | Imap enabled / last | User Roles      |
|--------|-------|---------------|-------------------|--------------|---------------------|-----------------|------------------|---------------------|-----------------|
| [User] | Yes   | Yes           | No                | 11 days ago  | —                   | —               | —                | No                  | SUPER ADMIN, PO |
| [User] | Yes   | Yes           | No                | 3 months ago | —                   | —               | —                | No                  | SUPER ADMIN, PO |
| [User] | Yes   | Yes           | No                | 3 days ago   | —                   | —               | —                | No                  | SUPER ADMIN, PO |

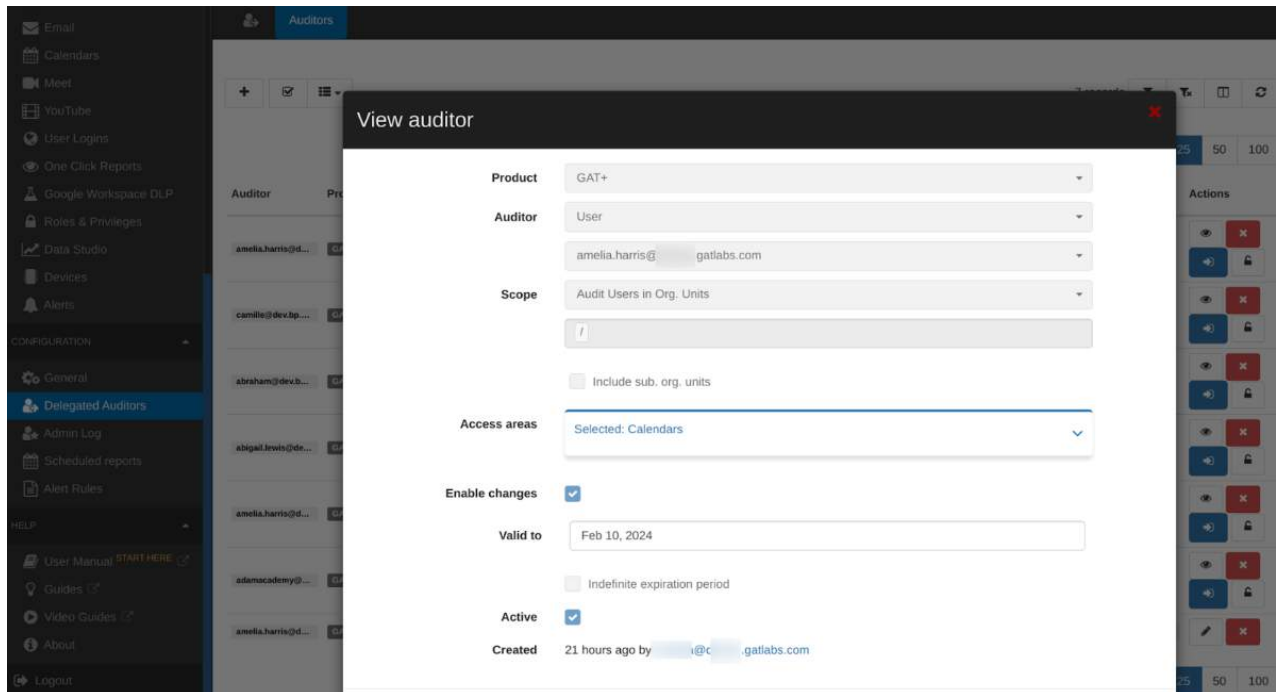
However in this case we are focusing on sorting on the Admin column and also paying attention to the User Roles column.

Best practice here is to ensure as few Admins as possible and that all Admins have 2 FA in place and enforced. Many time consuming tasks require Admin privilege with under normal use tends to lead to expansion of the Admin accounts.

With GAT+ features such as **‘Delegated Auditors’** and tools such as **GAT Flow**, nearly all Admin tasks can be defined as specific actions and carried out by non-Admin users who are ‘sandboxed’ to perform just that task.

This greatly enhances security and ensures tight control over Super Admin accounts.

# 2. Administrator Role Audit:



In the above screenshot we can see how a Google Workspace Admin using GAT+ can elevate an ordinary user to have **audit and management control** over Google Calendars (selected as an example from a long list of areas from Drive to Devices to mention just 2 more) for a particular OU or set of OUs in the domain.

In this way a mundane admin task that would normally fall to a Super Admin account to do can be done by a help desk employee for example.

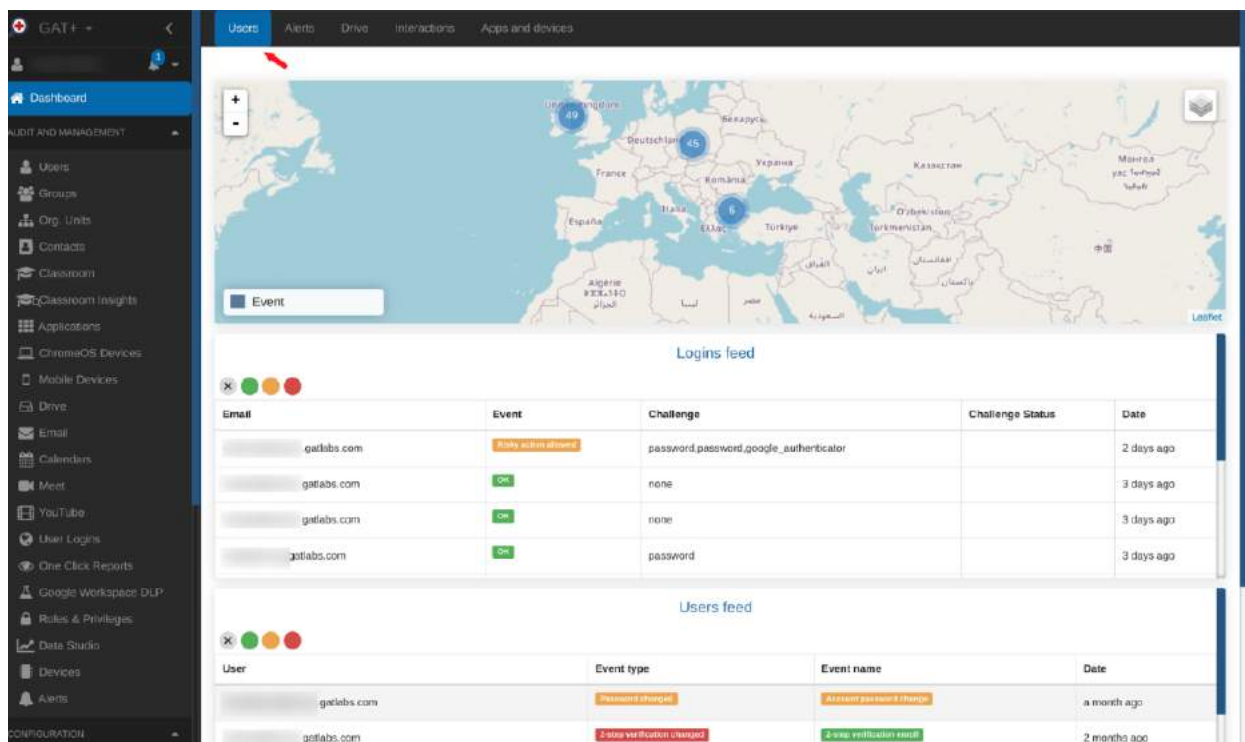
## 2.2 Review the list of admins periodically and adjust their permissions according to their job requirements.

As outlined in the Access Management Audit, this is a repeat of Step 1 with just Admin accounts selected and the report automatically generated on a monthly recurring basis. The report **can be emailed automatically** to the existing Admins, Auditors or Security officers, for confirmation and review.

# 3. Security Audit:

## 3.1 Check the security dashboard for any suspicious activity.

The GAT+ security dashboard is the first thing you see when you enter the tool.



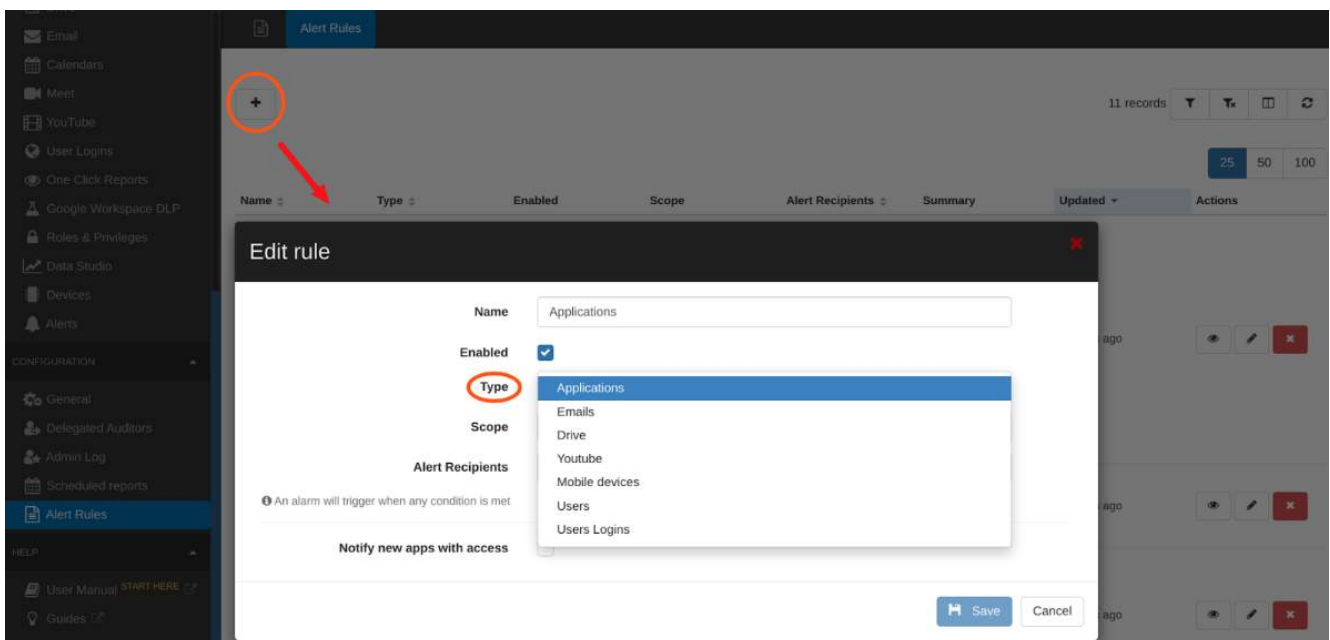
Starting with a '**Users' dashboard**, it is designed to show Admins quickly and clearly any unusual activity on their domain. Where applicable it categorizes activity and events using a color code system where green is normal behavior and red is either dangerous, a major event, or requires particular attention.

This is designed to **quickly surface issues of interest** for the Admins attention. There are **5 separate dashboards** for the Admin to scan across, each dashboard allows you to dive deeper into the alerts reported on that dashboard. Apart from being tracked and recorded here, major security events can also be reported via other channels in realtime.

# 3. Security Audit:

## 3.2 Set up alerts for unusual activities, like an unexpected increase in file sharing or login attempts from unusual locations.

Enabling detailed alerting is critical for on-going security and timely reporting. GAT+ has a detailed alerting configuration area, allowing you to create real time alerts, many with actionable outcomes causing automatic remediation, covering a wide range of Workspace areas.



Actions cover alerts for a huge range of situations and can include steps like revoking shares for inappropriate or not allowed file shares based on recipients or RegEx. Examination of the content.

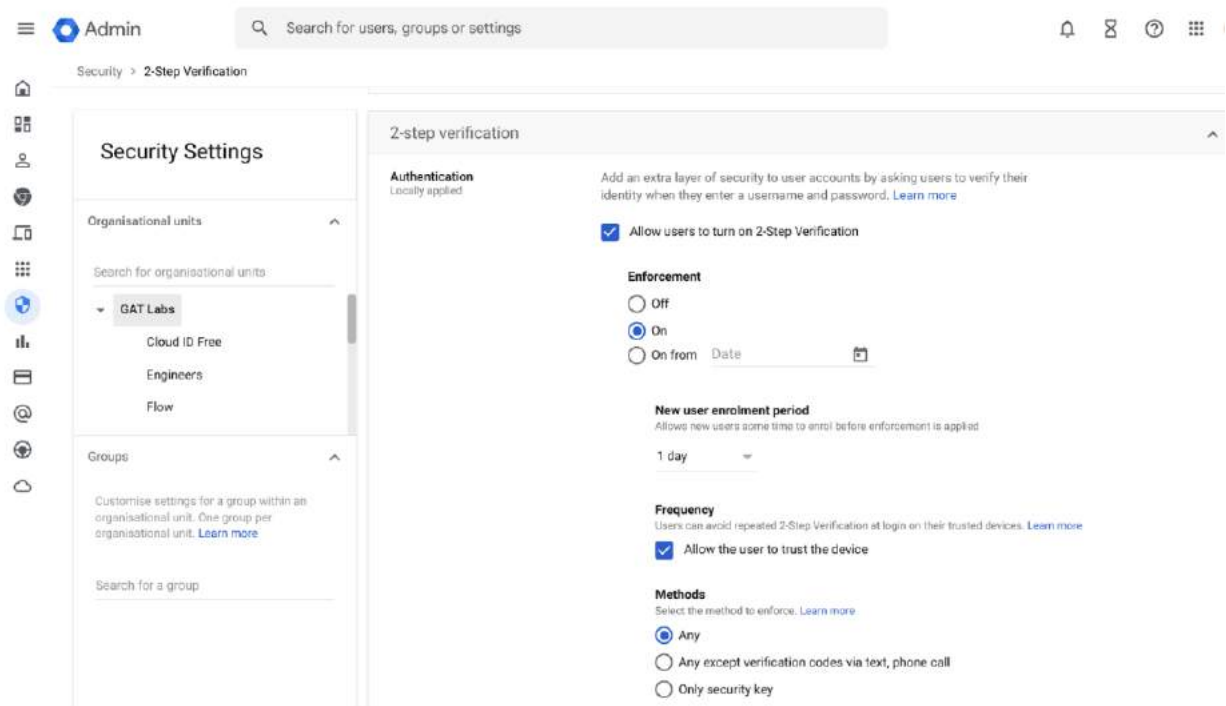
## 3.3 Ensure 2-factor authentication is enabled for all users.

This is a feature configured from the Workspace Admin console.

# 3. Security Audit:

## 3.3 Ensure 2-factor authentication is enabled for all users.

This is a feature configured from the Workspace Admin console.



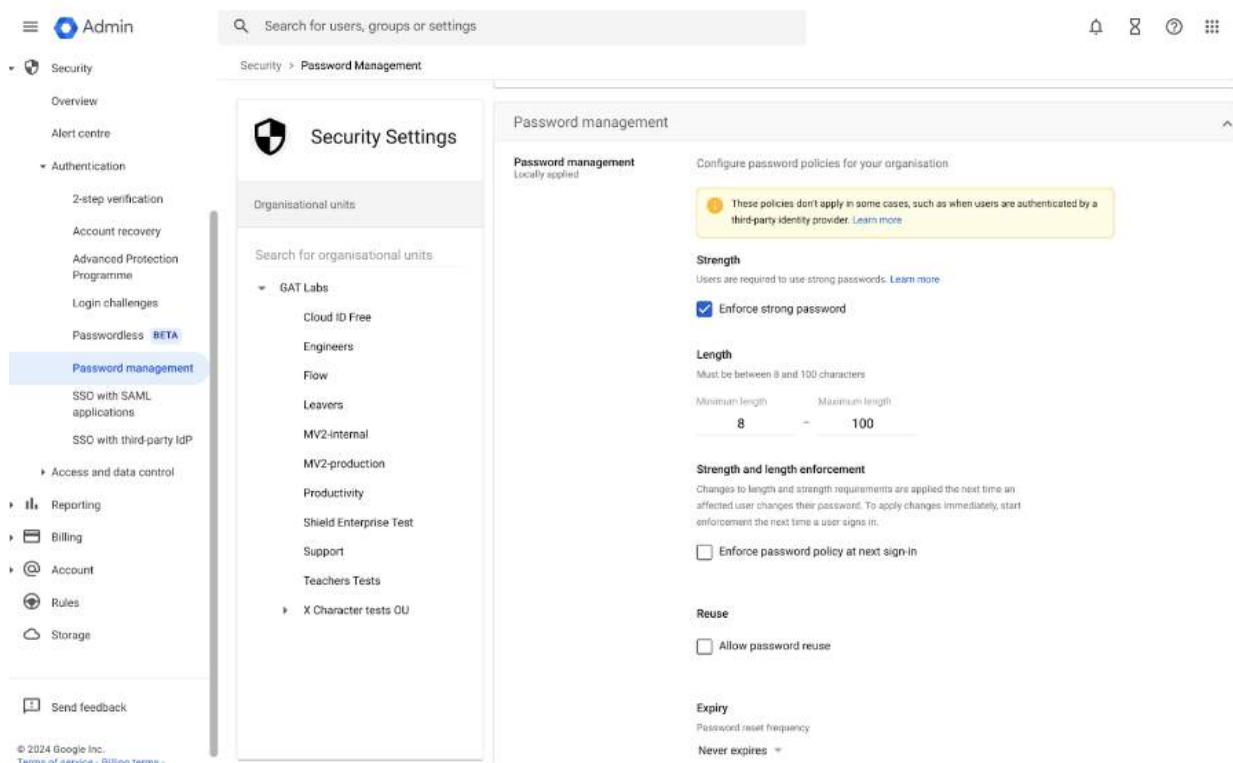
As a super Admin, in the Admin console, under Security settings, select 2-step verification.

**A useful tech tip** here is to set an enrollment period, but set it short. This will allow the new user time to log in and set up their 2-step environment, including perhaps downloading the Google authenticator to their phone. See more about this really powerful security utility [here](#).

# 3. Security Audit:

## 3.4 Regularly update the password policies and enforce strong password requirements.

Password management for the domain is also done in this area.



This section allows for the setting of password characteristics, the most important of which is probably length, **12 being a good minimum length, but longer is better.**

There is an open debate on the utility of forcing regular password changes. It is something best considered in the absence of 2-step verification, but we would consider **2-step verification an essential part of the login process.**

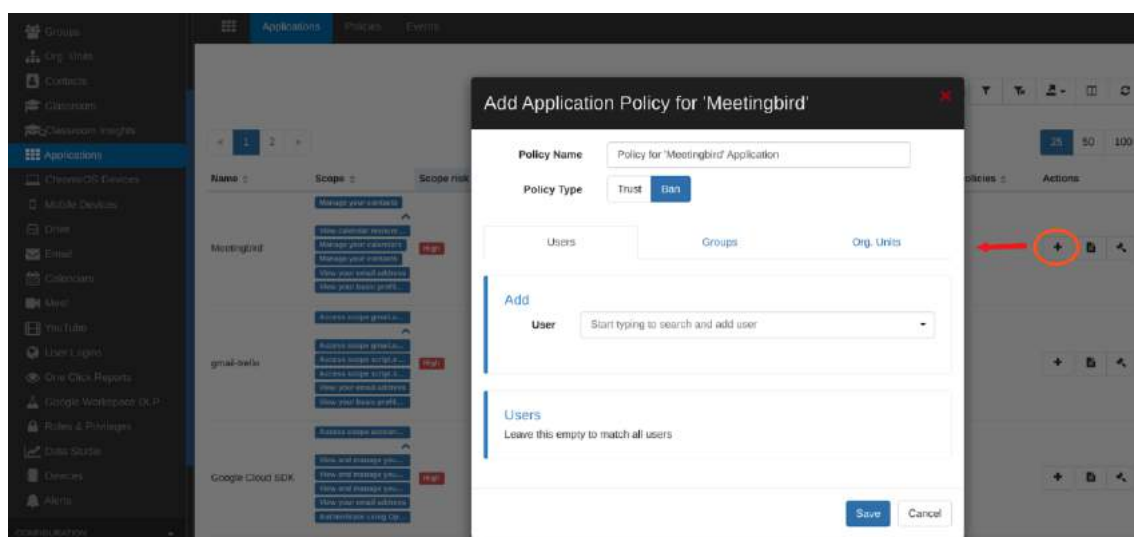


# 4. Application Audit:

## 4.1 Assess third-party apps connected to your Google Workspace and revoke any that are unnecessary or not compliant with your security standards.

Third party apps gain access to your domain either through Admin installs (like how you added GAT+) or through user based installs.

**GAT+ reports on all third party apps** via the Applications reporting section. Your entire third party app installed base is assessed by GAT+ and graded based on the extent of the API scopes they request. Sorting on this column allows you to see which apps have the most access to your files, emails and other potentially sensitive information.



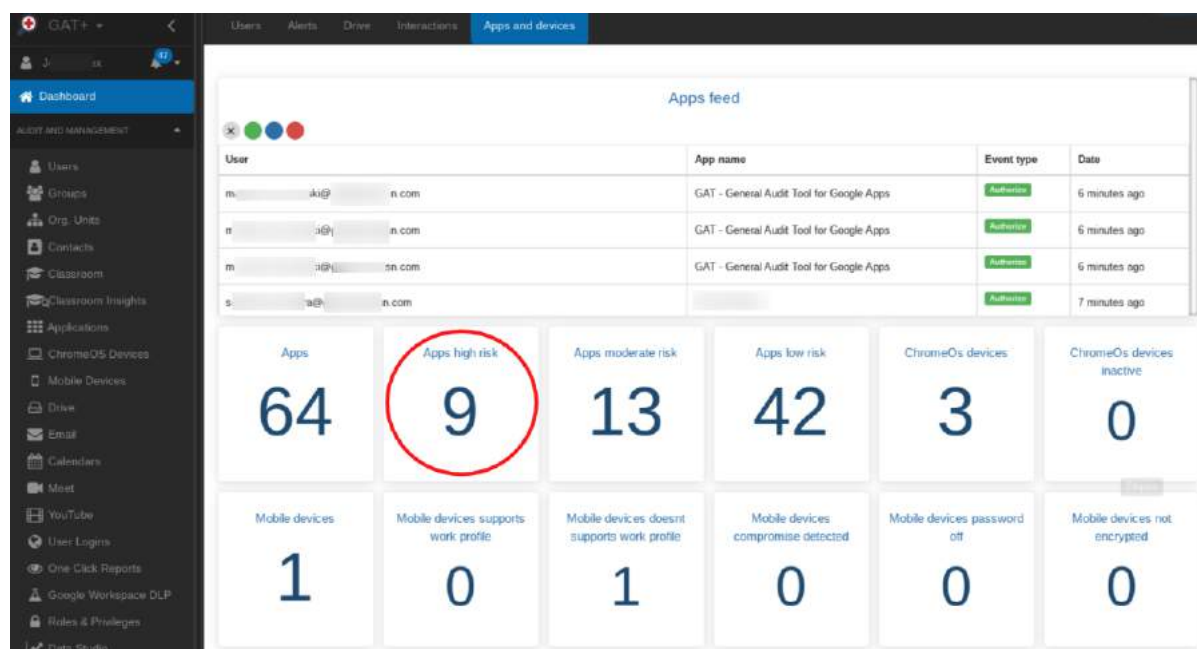
You can also enforce Third Party App policy from this area, allowing an app or banning an app for a particular user, group or org unit.

Referring back to section 3 (previously mention) and the configuration of **alerts for unusual activity** you can also use this to cover real time alerting when a third party app is installed on your domain.

# 4 Application Audit:

## 4.2 Regularly review API permissions for any unusual or unauthorized access.

This is really about reviewing the third party app table to identify risky apps in terms of scopes requested. We try to make this process easier for the Admin by doing a bulk categorisation in the dashboard.

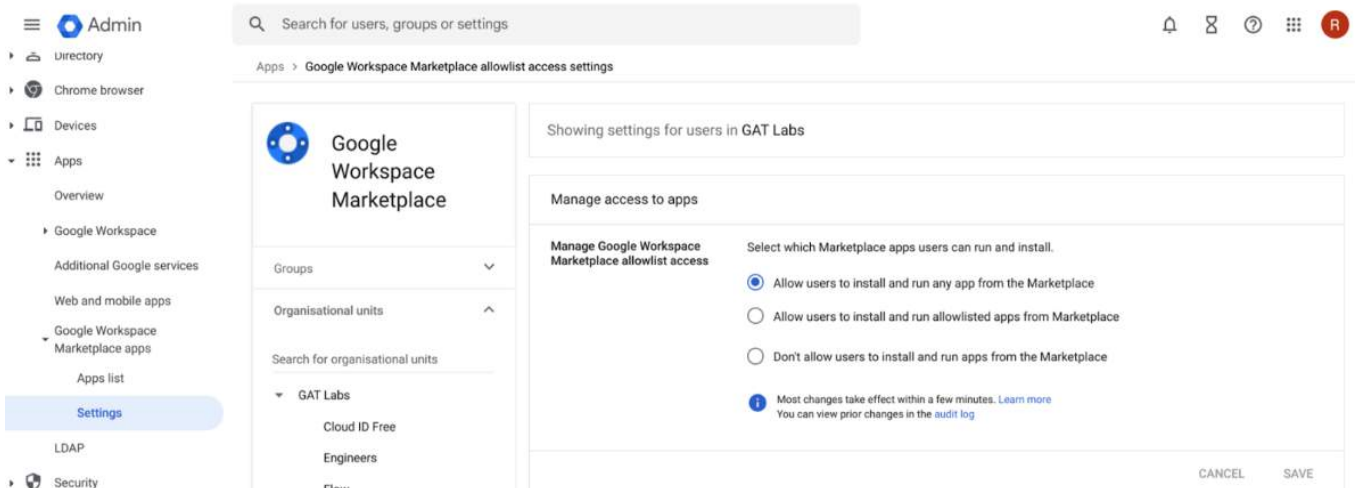


This table is basically a summary of the Apps and Devices that have access to the domain. All the numbers in the table are clickable, and clicking on one will take you to a summary of the information behind it.

While reviewing after the event is useful as you come to grips with what is on your domain, alerting on each new install is essential to ensure you can allow users access to useful new apps while staying alert to the scopes and information those apps request.

# 4. Application Audit:

Again, the Workspace Admin console has some very useful configuration options in this area.



**Remember**, third party apps are often very useful productivity tools and blocking them completely can take away a huge amount of the utility of the Workspace environment.

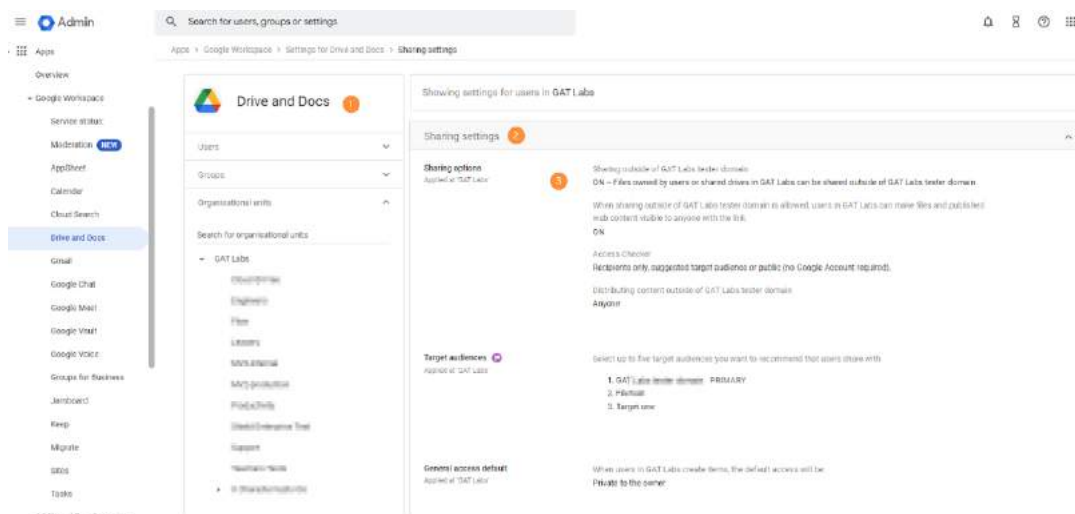
The best we can suggest is to **find the correct balance for your own domain**.



# 5. Drive and Shared Drives Audit:

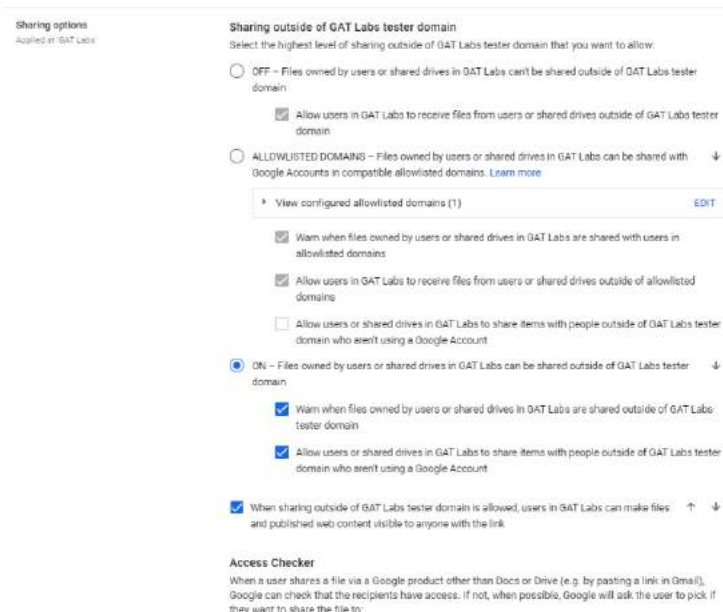
## 5.1 Review sharing settings to ensure sensitive information is not shared with the wrong people or groups.

Review the Sharing settings for your domain in Google Admin console.



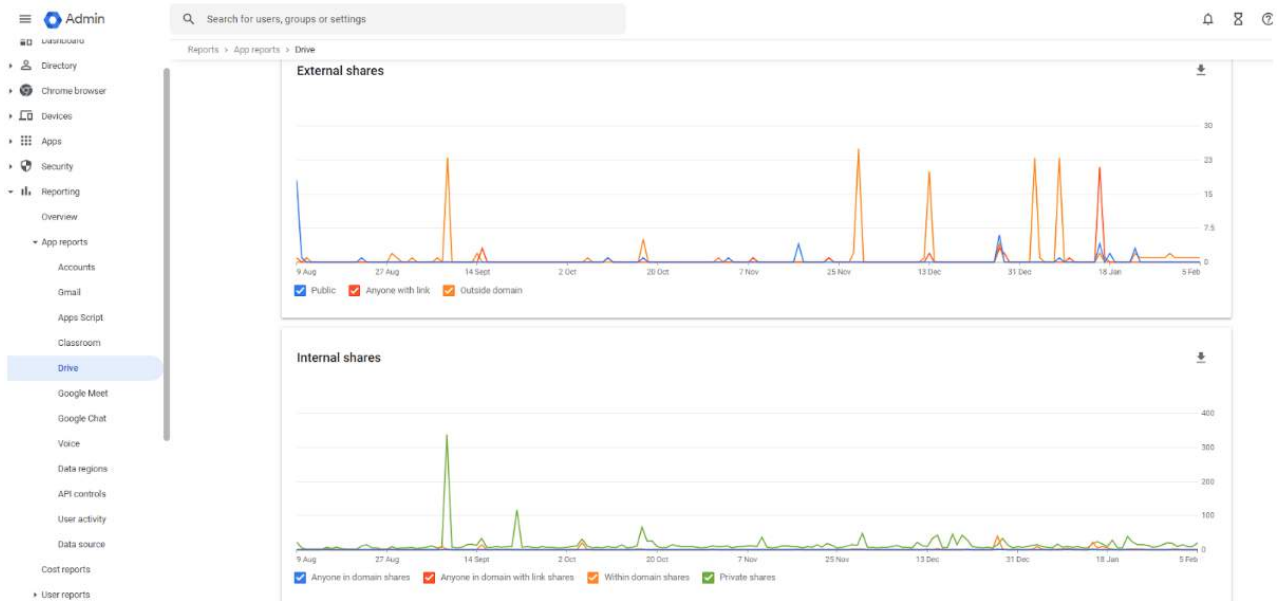
You can **audit the Sharing options** - to see if Sharing outside of the domain is possible. Set global policies for sharing files outside your organization, and define the default link sharing visibility of new files.

**The Admins can set up** what sharing permissions to be allowed on the domain.



# 5. Drive and Shared Drives Audit:

In regards to the report of the Drive shares - can be audited in the **Admin console > Reporting > App reports > Drive**

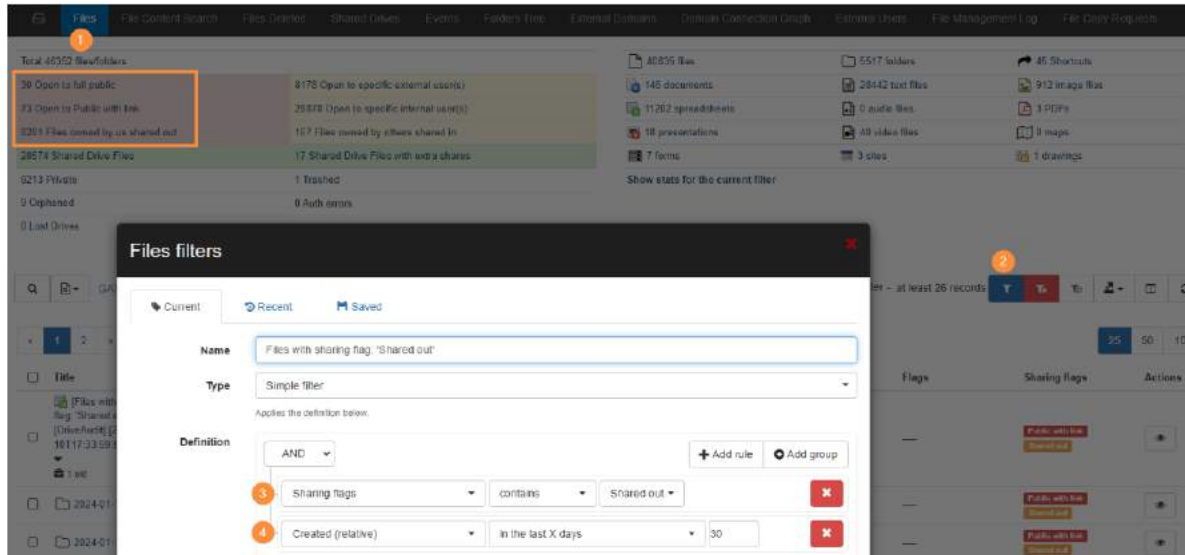


This chart is useful to see if there was a sudden spike in external sharing. Unfortunately the exact files being shared or their significance can't be seen from here.

Use the **many filter features of GAT+**, including by date and sharing direction to see what caused the spike in sharing:

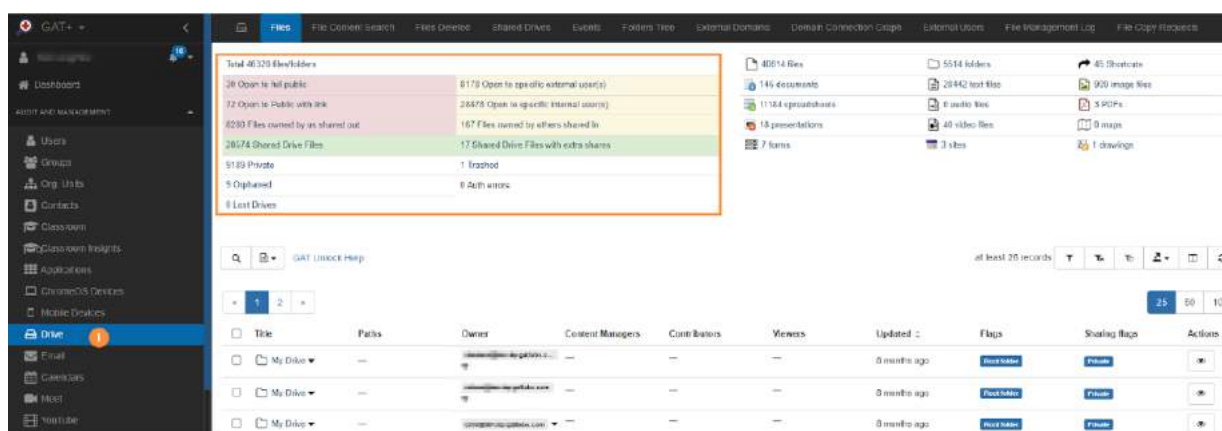
- **Search for Shared Out** (all externally shared out files) that are created in the last X days.
- **Search for Public files** - that are updated in the last X days.

# 5. Drive and Shared Drives Audit:



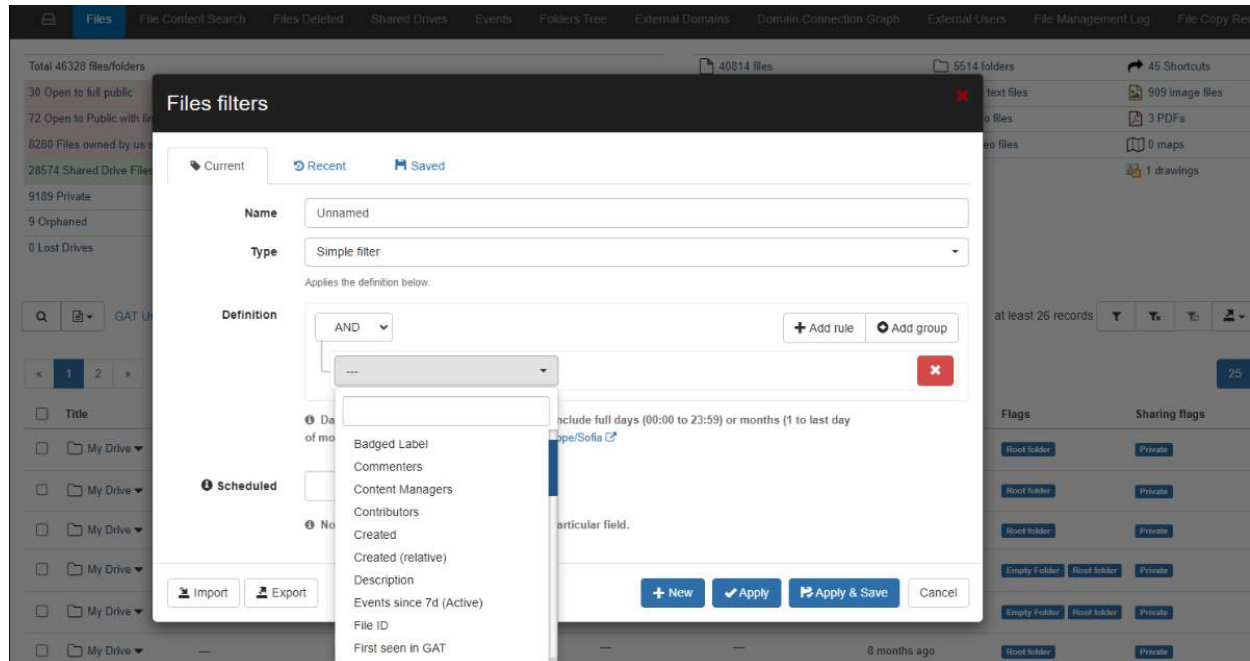
In Google's GAT+, administrators have comprehensive visibility into and control over all Google Drive files within their domain. This includes detailed access to the actual files and their metadata, enabling the Admins to take necessary actions with ease.

Navigate to **GAT+ > Drive > Files >** table view on the top will show all files of the domain and divided by the Sharing permissions all Drive and Shared Drive files and folders have.



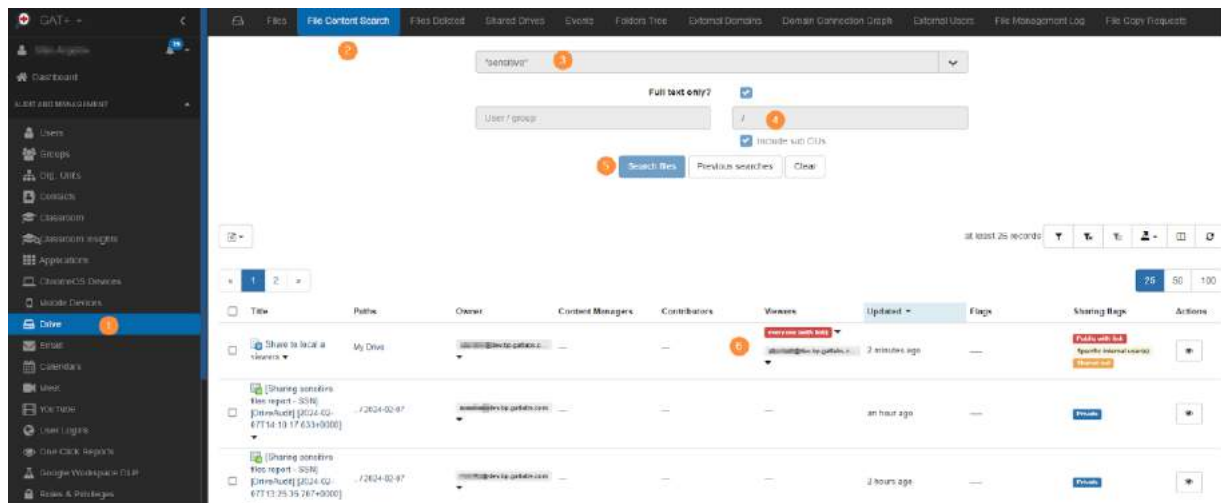
# 5. Drive and Shared Drives Audit:

Filters can be applied to search for specific files based on any criteria you can think of.



Using File Content Search - you can use the Google Drive search operators and search the contents of files. See the Google Drive search operators [here](#).

Navigate to **GAT+ > Drive > File Content Search > Apply query** to search for file content.





# 5.

## Drive and Shared Drives Audit:

Using the Unlock feature the Admins can gain access to view the file and its contents. The admins can also change ownership of the files to different local users.

In GAT+ **1 click filters** can be very useful for getting the big picture very quickly.

**Files owned by External users where your users have access to.**

Files

File Content Search

Files Deleted

Shared Drives

Events

Folders Tree

Groups Sharing

External Domains

Domain Connection Graph

Total 183295 files/folders

92 Open to full public

20163 Open to specific external user(s)

1784 Open to Public with link

62819 Open to specific internal user(s)

21520 Files owned by us shared out

2434 Files owned by others shared in

51098 Shared Drive Files

1523 Shared Drive Files with extra shares

111352 Private

83 Trashed

60 Orphaned

0 Auth errors

3 Lost Drives

120146 files

63149 folders

3337 Shortcuts

5880 documents

1256 text files

22782 image files

55043 spreadsheets

275 audio files

24180 PDFs

818 presentations

1657 video files

17 maps

100 forms

32 sites

61 drawings

One of the most important 1 click filters is **Files shared in**. This information is available nowhere else and in no other tool. What is critical about this information is that you need it to see the complete picture of file usage on your domain.

Having applied the filter, further filters can be added and each file can be examined in detail to see who the local users are.

### 5.2 Audit files in Drive to check for proper ownership, especially for users who have left the organization.

In the Drive audit section of GAT+, admins can access comprehensive information about files and their metadata in Google Drive. This includes details such as the file owner, who it's shared with, when it was last updated or accessed, and other metadata.



# 5. Drive and Shared Drives Audit:

Additionally, **the audit will highlight** if Google Drive files and folders are owned by users within your organization and if they are shared with external users. It will also indicate if files and folders are shared into your domain from external domains.

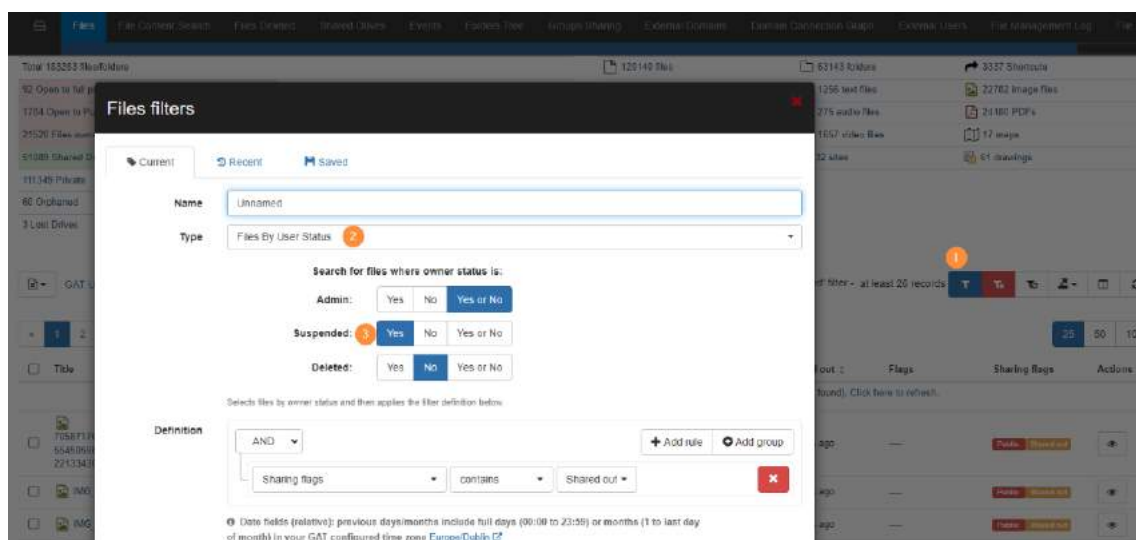
Files where your users have access but aren't the owners will be flagged as **"Shared In."** These are files owned by external users but shared within your domain.

| Title                                   | Paths       | Owner         | Content Managers | Contributors  | Viewers | Updated      | Flags                    | Sharing flags                       | Actions  |
|---|-------------|---------------|------------------|---------------|---------|--------------|--------------------------|-------------------------------------|----------|
| GAT Unlocks Help                        | 512x512     | External user | —                | —             | —       | 13 days ago  | Contributors can't share | Specific internal user(s) Shared in | Eye icon |
| Doc for testing to see docx             | —           | External user | —                | External user | —       | a month ago  | —                        | Specific internal user(s) Shared in | Eye icon |
| A new video to keep away from the clock | —           | External user | —                | External user | —       | 14 days ago  | —                        | Specific internal user(s) Shared in | Eye icon |
| Slide that really has access to         | —           | External user | —                | External user | —       | a month ago  | Contributors can't share | Specific internal user(s) Shared in | Eye icon |
| Complicated and Fungible                | Hyphen test | External user | —                | External user | —       | 9 months ago | —                        | Specific internal user(s) Shared in | Eye icon |

Files owned by external users will be visually shown with an orange background.

## Audit files of people who left the organization

The Admins can also see all Drive files that are owned by users who are suspended and all the users who the files are shared with.



# 5. Drive and Shared Drives Audit:

All the suspended users will be shown visually and easily recognizable via black background.

The screenshot shows the 'Drive and Shared Drives Audit' interface. At the top, there's a search bar with 'GAT Unlock Help' and a filter dropdown set to 'Unnamed' with 'at least 26 records'. Below the search bar, there are pagination controls showing '1' of 2 pages and a table view icon. The main table has columns: Title, Paths, Owner, Contributors, Viewers, Commenters, Updated, Shared out, Flags, Sharing flags, and Actions. The table contains several rows of data, each representing a file or folder. The first row is highlighted with a red background, indicating a suspended user. The table also includes a 'The search is finished. Complete results, computed at 2024-02-07T17:13:31+02:00, are presented below (at least 26 records have been found). Click here to refresh.' message.

| Title                         | Paths      | Owner | Contributors | Viewers  | Commenters | Updated     | Shared out  | Flags | Sharing flags     | Actions |
|-------------------------------|------------|-------|--------------|----------|------------|-------------|-------------|-------|-------------------|---------|
| 7058...<br>5548...<br>2213... | .../Images | ...   | ...          | everyone | —          | 4 years ago | 4 years ago | —     | Public Shared out | ...     |
| 7058...<br>5548...<br>2213... | .../Images | ...   | ...          | everyone | —          | 4 years ago | 4 years ago | —     | Public Shared out | ...     |
| 7058...<br>5548...<br>2213... | .../Images | ...   | ...          | everyone | —          | 4 years ago | 4 years ago | —     | Public Shared out | ...     |
| 7058...<br>5548...<br>2213... | .../Images | ...   | ...          | everyone | —          | 4 years ago | 4 years ago | —     | Public Shared out | ...     |
| 7058...<br>5548...<br>2213... | .../Images | ...   | ...          | everyone | —          | 4 years ago | 4 years ago | —     | Public Shared out | ...     |

## Shared Drives audit

In the Shared Drive audit of GAT+, admins get **a complete view of all Shared Drives within the domain**. They can see metadata detailing which users have access to the files and folders within these Shared Drives. This section displays all the root Shared Drives in the domain, allowing Workspace Admins to efficiently update and manage their data.

The Shared Drive audit in GAT+ offers various filters to **help locate specific Shared Drives quickly**. Additionally, admins can take actions like adding or removing user access directly from this interface. This makes it easy to manage Shared Drives efficiently.

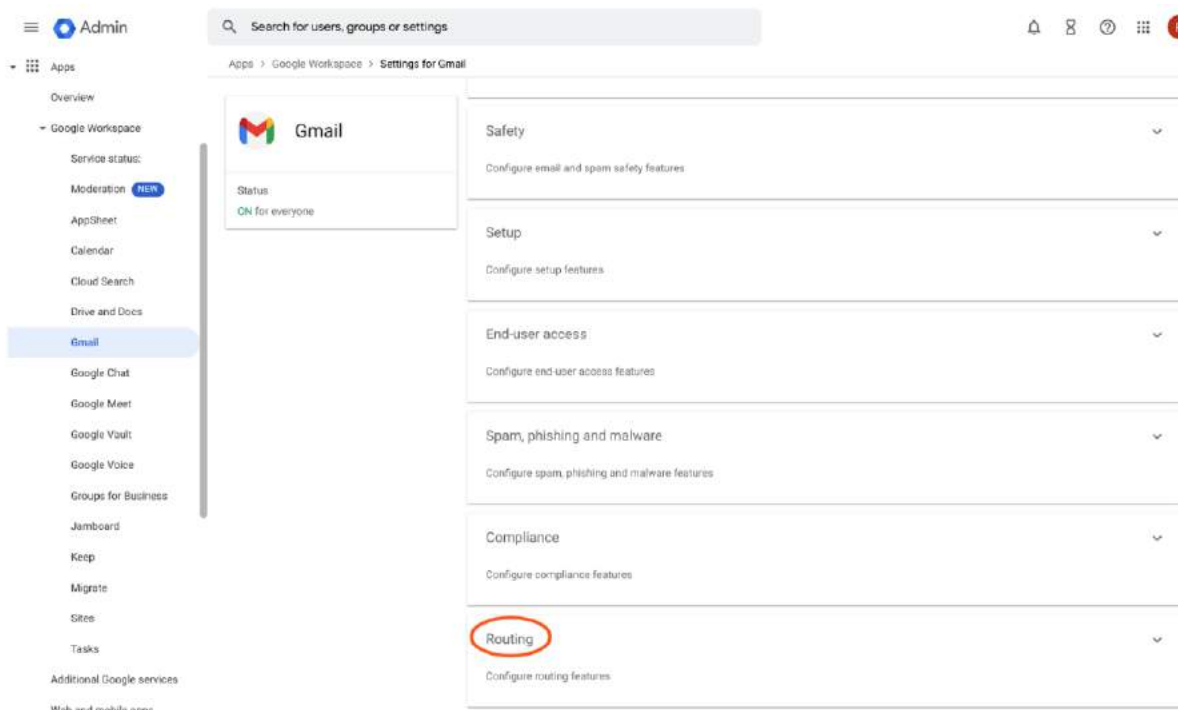
The screenshot shows the 'Shared Drives' audit interface. The left sidebar has a menu with 'Drive' selected. The main table has columns: Title, Managers, Content Managers, Contributors, Viewers, Commenters, Updated, Admin privileges, Sharing only, Sharing only with drive members, Only Contributors can download, copy and print, Sharing flags, and Number of items. The table contains several rows of data, each representing a shared drive. The first row is highlighted with a red background, indicating a suspended user. The table also includes a 'The search is finished. Complete results, computed at 2024-02-07T17:13:31+02:00, are presented below (at least 26 records have been found). Click here to refresh.' message.

| Title                  | Managers | Content Managers | Contributors | Viewers | Commenters | Updated      | Admin privileges | Sharing only | Sharing only with drive members | Only Contributors can download, copy and print | Sharing flags                                   | Number of items |
|------------------------|----------|------------------|--------------|---------|------------|--------------|------------------|--------------|---------------------------------|--|---|-----------------|
| Shared drive Marketing | ...      | ...              | ...          | ...     | ...        | 4 years ago  | unknown          | unknown      | unknown                         | unknown  | Shared Drive external Specific internal user(s) | 7               |
| Test mailbox created   | ...      | ...              | ...          | ...     | ...        | 2 years ago  | unknown          | unknown      | unknown                         | unknown  | Shared Drive external Specific internal user(s) | 96              |
| Shared Drive Support   | ...      | ...              | ...          | ...     | ...        | 7 months ago | Disabled         | Disabled     | Disabled                        | Enabled  | Specific internal user(s)                       | 0               |
| Budget 2022 March      | ...      | ...              | ...          | ...     | ...        | 7 months ago | Disabled         | Disabled     | Disabled                        | Enabled  | Specific internal user(s)                       | 2               |
| Flag: number of files  | ...      | ...              | ...          | ...     | ...        | 7 months ago | Disabled         | Disabled     | Disabled                        | Enabled  | Specific internal user(s)                       | 2352            |

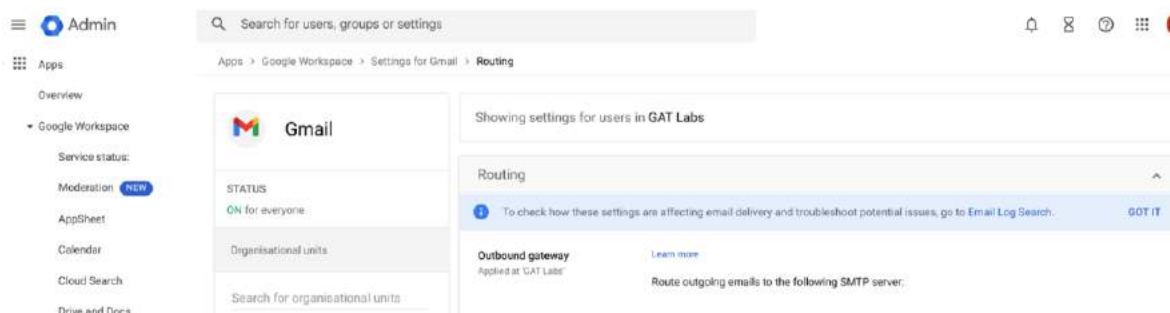
# 6. Email Compliance and Security Audit:

## 6.1 Review email routing and delivery settings to ensure compliance with data protection laws.

These settings are actually part of the gmail configuration found in the **Workspace Admin console**.



The default for most of the routing values is that nothing is set. However, you should look through them to make sure that nothing is suspicious, or if changed that the settings are what you want.



# 6. Email Compliance and Security Audit:

One important thing to verify is that you **have no outbound gateway set**, or if one is set, it is the gateway you expect. If your Admin account had been compromised in the past, hackers could use this value to route all email through their servers before onward delivery.

## 6.2 Check for proper email authentication with SPF, DKIM, and DMARC records to prevent email spoofing.

If you have not already configured SPF, DKIM and DMARC then the steps to follow are outlined [here](#).

To novice domain Admins these sound intimidating but they are actually quite easy to set up. Just make sure you have edit access to your domains DNS records and that you know how to change them. You can usually access these through your Google Admin console if you also used google to create your domain name. If not, you may manage your own DNS or have an external DNS provider, like Hover or Amazon.

SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) are email authentication methods that help protect email senders and recipients from spam, phishing, and email spoofing. Here are the advantages of each:

### SPF (Sender Policy Framework):

- **Prevents Spoofing:** SPF allows domain owners to specify which mail servers are permitted to send email on behalf of their domain. This prevents unauthorized servers from sending emails pretending to be from that domain.
- **Easy to Implement:** Adding an SPF record to your DNS settings is relatively straightforward.

# 6. Email Compliance and Security Audit:

---

- **Reduces Spam:** By verifying sender IP addresses, SPF reduces the amount of spam and phishing emails received.
- **Improves Deliverability:** Emails from domains with an SPF record are less likely to be marked as spam by receiving mail servers, improving deliverability.

## DKIM (DomainKeys Identified Mail):

- **Ensures Message Integrity:** DKIM provides a digital signature that verifies that the content of the emails has not been tampered with during transit.
- **Domain Reputation:** Helps build a good sending reputation for your domain, as email providers can verify the signature against your domain's public key published in the DNS.
- **Complements SPF:** DKIM complements SPF by adding an additional layer of trust, ensuring that not only the sender IP is authorized but also that the message content is trustworthy.

## DMARC (Domain-based Message Authentication, Reporting & Conformance):

- **Combines SPF and DKIM:** DMARC uses both SPF and DKIM to provide a robust defense against email spoofing and phishing attacks.
- **Policy Enforcement:** DMARC allows domain owners to specify how receiving mail servers should handle emails that fail SPF and DKIM checks. This could include reporting the failure, sending the email to spam, or outright rejecting the message.
- **Reporting Capabilities:** DMARC provides reports back to the domain owner about emails (both legitimate and fraudulent) that are claiming to be from their domain. This allows domain owners to identify and address potential issues.

# 6. Email Compliance and Security Audit:

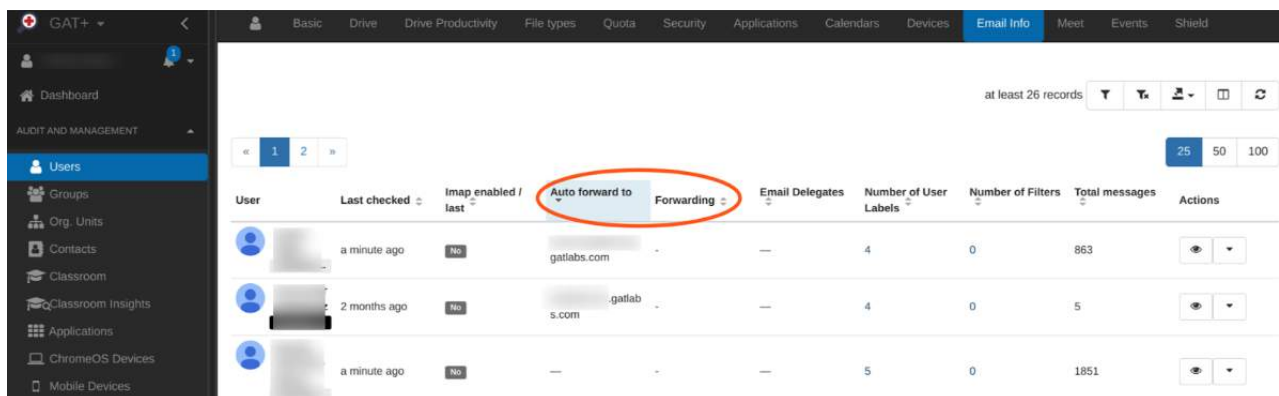
- **Increases Email Trust:** Implementing DMARC can increase the trust recipients have in emails from your domain, as they know that the emails have passed strict authentication checks.
- **Protects Brand Reputation:** Helps protect your brand from being used in phishing scams, which can otherwise lead to a loss of customer trust.

By implementing **SPF, DKIM, and DMARC** in conjunction, organizations can significantly improve the security and reliability of their email communications. These protocols are part of a layered defense strategy that helps to authenticate the source of emails, preserve the integrity of the messages, and build trust with email recipients that the communications are truly from the claimed sender.

To ensure the integrity and trustworthiness of your domain's emails it is important that you follow these steps and configure these controls.

## 6.3 Audit any email forwarding rules to prevent data leakage.

These are user settings and if a user account was compromised it is a likely setting for a hacker to change. Once in place the user often is not aware of its existence and their emails will be forwarded in the background.



| User        | Last checked | Imap enabled / last | Auto forward to | Forwarding | Email Delegates | Number of User Labels | Number of Filters | Total messages | Actions               |
|-------------|--------------|---------------------|-----------------|------------|-----------------|-----------------------|-------------------|----------------|-----------------------|
| [User Icon] | a minute ago | Yes                 | gatlabs.com     | -          | —               | 4                     | 0                 | 863            | [Eye Icon] [Dropdown] |
| [User Icon] | 2 months ago | Yes                 | .gatlabs.com    | -          | —               | 4                     | 0                 | 5              | [Eye Icon] [Dropdown] |
| [User Icon] | a minute ago | Yes                 | —               | -          | —               | 5                     | 0                 | 1851           | [Eye Icon] [Dropdown] |

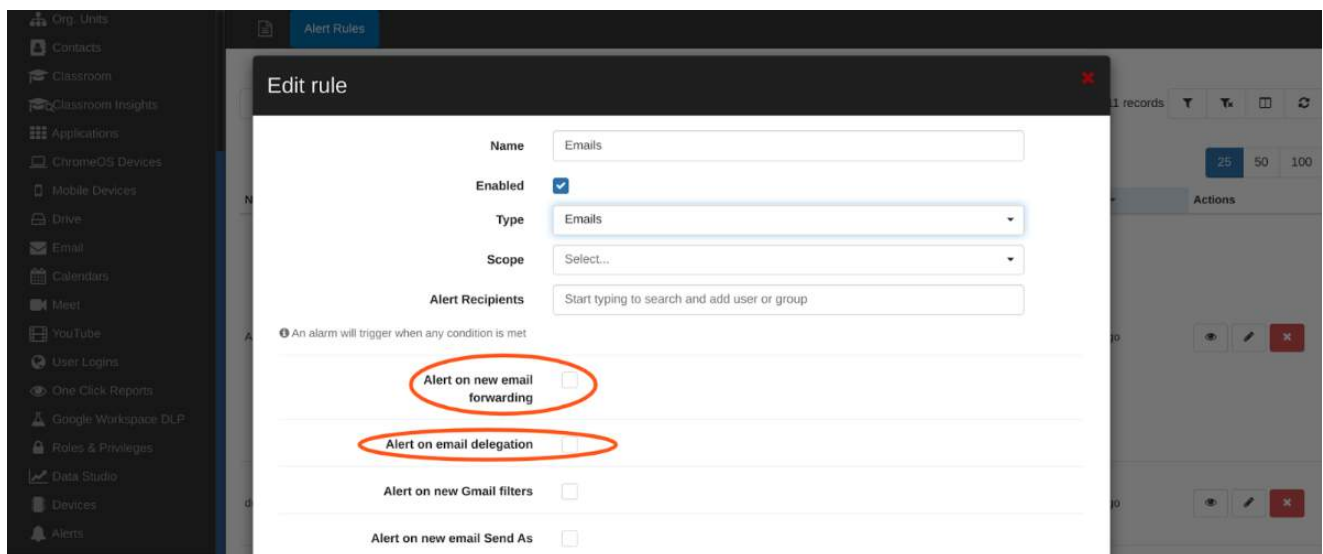


# 6. Email Compliance and Security Audit:

Using the **GAT+ user audit**, under the Email Info table, the Admin can quickly see which accounts have forwarding enabled. You can see if there are any suspicious forward destinations and alert or confirm with the end user if this is what they intended.

**Email delegation** is also a potential backdoor to a user's mailbox and email delegates should also be verified (see next column over).

Of course **email forwarding** from a user account can be set up at any time. GAT+ supports real time alerting for Admins when this happens.



Again the configuration for this is found under Alert Rules in the GAT+ configuration menu, Emails being the selected type.

**Another important alert** to receive is if email delegation to an account has been enabled. This will allow an impersonator to send and receive emails on the users behalf and grant full access to their mailbox.

# 7 Compliance Audit:

## 7.1 If your organization is subject to regulations like GDPR, HIPAA, CIPA etc., ensure that your Google Workspace settings comply with these standards.

Ensuring compliance with **GDPR (General Data Protection Regulation)** and **HIPAA (Health Insurance Portability and Accountability Act)** within Google Workspace requires configuring several settings and adopting best practices.

These settings focus on securing personal data, controlling access, and ensuring data integrity. Here's a general guide:

### 7.1.1 For GDPR and HIPPA Compliance:

Whilst logged in as a Super Admin, navigate to **Account settings > Legal & compliance**. Scroll to the “**Security and Privacy Additional Terms**” section to review and accept the following terms if applicable:

#### **Cloud Data Processing Addendum (CDPA)**

- Make sure you've reviewed and accepted Google's DPA, this is essential for GDPR compliance.

#### **Indicate if the EU data protection law applies to you**

- Review and certify if applicable to your organization

#### **HIPAA business associate amendment**

- Review and accept if applicable to your organization

Additionally, review your Google contract and consider the following



# 7 Compliance Audit:

## EU Model Contract Clauses:

- Incorporate **EU Model Contract Clauses** in your contract with Google if processing data of EU citizens.

## Data Access and Control:

- Regularly review who has access to personal data.
- Use Google's advanced protection settings to control access to sensitive data.

## Data Export and Deletion:

- Ensure you can export or delete user data in compliance with **GDPR's "right to be forgotten."** GAT+ powerful search tools will help you identify this data across Calendar, Drive and Email.

Security and Privacy Additional Terms

Review and agree to the amendment(s) below if applicable to your compliance needs. [Learn more](#)

Cloud Data Processing Addendum (CDPA)

REVIEW AND ACCEPT

Indicate that the EU data protection law applies to you

Please click the button below if your use of Workspace is subject to the EU GDPR, UK GDPR or the Swiss FDPA, and your billing address is outside Europe, the Middle East and Africa. This selection will apply the appropriate version(s) of the standard contractual clauses, as described in the [Cloud Data Processing Addendum](#). [Learn more](#)

CERTIFY IF APPLICABLE

Google Workspace/Cloud Identity HIPAA business associate amendment

REVIEW AND ACCEPT

DONE

# 7 Compliance Audit:

## Secure Email Practices:

- If using Gmail to transmit PHI, ensure emails are encrypted and secure.
- Consider additional email security measures or third-party encryption services.

## Data Backup:

- Ensure regular backups of PHI to prevent data loss.

## Data Retention and Deletion:

- Implement policies for retaining and securely deleting PHI as per HIPAA requirements.

## Employee Training:

- Train staff on HIPAA compliance, particularly regarding handling PHI.

## Incident Management:

- Have an incident response plan in place for potential data breaches.

## 7.1.3 For CIPA Compliance:

To ensure compliance with the Children's Internet Protection Act (CIPA), which requires schools and libraries that receive certain federal funds to implement internet safety measures, Google Workspace for Education (formerly G Suite for Education) administrators should configure a variety of settings. These settings are focused on filtering harmful content, monitoring usage, and educating users about safe internet practices.

Here's a guide to configure Google Workspace for CIPA compliance:

## Content Filtering:

- Utilize [Google SafeSearch](#) to filter explicit search results on Google Search. GAT Shield can help you do this.
- In Google Workspace for Education, enforce SafeSearch for all users.

# 7 Compliance Audit:

- Consider enabling **YouTube Restricted Mode** to limit access to age-inappropriate content.
- For schools using **Workspace and Chrome**, GAT Shield offers a single checkbox to enable all of the above recommendations and apply a special URL filtering category to block sites not CIPA compliant.

The screenshot displays the GAT Labs web interface. On the left is a dark sidebar with a navigation menu. The top of the sidebar lists 'Shield Alerts' and 'Site Access Events'. Below these are 'Login Control Events', 'User Activity', and 'YouTube'. A 'CONFIGURATION' section follows, with 'General & CIPA' selected and highlighted in blue. Other options in this section include 'Modules', 'Alert Rules', 'Browsing Tags', 'Browsing Cookies', 'Site Access Control' (marked with a 'NEW' badge), 'Search Access', 'YouTube Access', 'Gmail access', 'Chat Access', 'Porn image block' (marked with a 'BETA' badge), 'Monitoring Ranges', 'Login Control', 'Scheduled reports', 'Delegated auditors', and 'Admin Log'. At the bottom of the sidebar is a 'MANAGEMENT' section with 'Template Alert Rules' and 'Template Browsing Tags'.

The main content area has a top navigation bar with 'General', 'CIPA Compliance' (active), and 'Webhooks'. Below this is a 'Quick help' box with a question mark icon. The text inside explains that enabling CIPA compliance requires being CIPA (Children's Internet Protection Act) compliant and that clicking the box will enable CIPA compliance over the entire domain or a selected OU and its SUB OUs. It lists three enabled features: a special URL filtering category called CIPA-Compliant-Category, Strict Safe Search for both words and images on Google, and Restricted Youtube access. It also notes that access to web sites via IP addresses is blocked. Below the quick help box, there is a section titled 'Enable CIPA compliant features' with a checked checkbox. A 'Scope' dropdown menu is set to 'Select...'. Below this, there is a note about rule recipients. At the bottom of the main content area, there are three status messages: 'Safe Search is not enabled - check Search Access section', 'YouTube Strict mode is not enabled - check YouTube Access section', and 'IP Blocking is not enabled - check URL Access Config section'. A blue 'Save' button is located at the bottom right of the main content area.

## Supervised User Accounts:

- Create supervised accounts for students using Google Workspace, which allows for monitoring and controlling their activities.

# 7 Compliance Audit:

---

## Monitoring and Reporting:

- Regularly review audit logs and reports in Google Workspace Admin Console to monitor user activities and ensure compliance with internet safety policies.
- Use Google Workspace's reporting features to track and record online activities, which is essential for CIPA compliance.

## Email and Chat Controls:

- Implement Gmail and Google Chat restrictions, especially for younger users, to prevent exposure to harmful communications.
- Utilize moderation tools and consider implementing content compliance rules to limit email exchange outside the school's domain. [Steps to configure content compliance rules here.](#)

## Application Control:

- Manage the applications that users can access in Google Workspace. Disable or limit access to applications that are not appropriate or necessary for educational purposes.

## Educational Programs and Policies:

- Implement educational programs for students about responsible and safe internet use.
- Develop and enforce an internet safety policy as required by CIPA. Both GAT+ and Shield can help with enforcement of this policy

## Customizable User Settings:

- Customize user settings based on age groups or grades. Different restrictions might be appropriate for different age levels.

# 7 Compliance Audit:

## Google Classroom:

- Use Google Classroom to create a controlled environment where teachers can share content, assignments, and communications with students. GAT Teacher Assist supports the live monitoring of students in Chrome by both teachers and principles.

## Parental Notification and Involvement:

- Keep parents informed about the internet safety measures and policies in place. With GAT Shield parents can monitor their own child's browsing usage and activity.
- Involve parents in monitoring their children's internet use where appropriate.

## Regular Audits and Reviews:

- Conduct regular audits of your CIPA compliance measures and update them as necessary.

## Device Management:

- If using Chromebooks or other devices managed through Google Workspace, utilize the Chrome Management tools to enforce safe browsing standards and GAT Shield to track device usage.

Remember, while Google Workspace provides tools that can help in achieving CIPA compliance, the ultimate responsibility lies with the institution to ensure these tools are correctly implemented and used.

Always **[tailor the settings to the specific needs and circumstances](#)** of your institution, and regularly review your compliance status, especially as technology and regulations evolve.

# 7 Compliance Audit:

## 7.2 General Best Practices:

- Implement **strong password policies** and **enforce two-factor authentication**.
- Limit the use of **third-party apps** and add-ons. Use GAT+ Apps monitoring to assist you tracking and audit log preservation.
- Conduct **regular** security assessments and compliance audits.

### Note:

- Consult a Legal Expert: Always consult with a legal professional or a compliance expert to ensure that all your practices are in line with GDPR and HIPAA requirements.
- Customize According to Need: The exact requirements may vary based on the nature of your organization and the data you handle.

## 7.3 Use Google Vault to set up retention policies and legal holds appropriately.

Google Vault is an information governance and eDiscovery tool for Google Workspace. With Vault, you can **retain, hold, search, and export** users' Google Workspace data. This helps organizations comply with legal and regulatory requirements by retaining important information for a specified period. Google Vault has a select few key features:

### Keep data for as long as you need it.

- If your organization is required to preserve data for a set time, you can configure Vault to retain it. Data remains available to Vault even when users delete it and empty their trash.

# 7 Compliance Audit:

## Remove data when you no longer need it.

- If your organization is required to delete sensitive data after a set time, you can configure Vault to remove it from user accounts and purge it from all Google systems.

## Search through all a users Google Workspace data

- Using keywords and dates within a specific range you can bring up data that may be required at some point for regulatory purposes.



If your domain has [Google Vault license add-ons](#), a GAT admin can use GAT Flow to create a Vault export as part of your offboarding process.

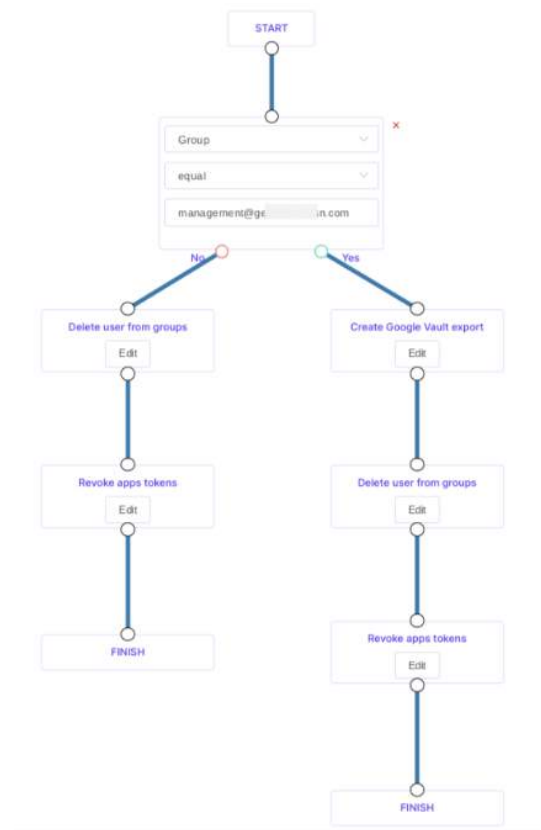
GAT Flow allows an admin to create an export for a matter, if and when certain conditions are met, when configured by admins.

# 7. Compliance Audit:

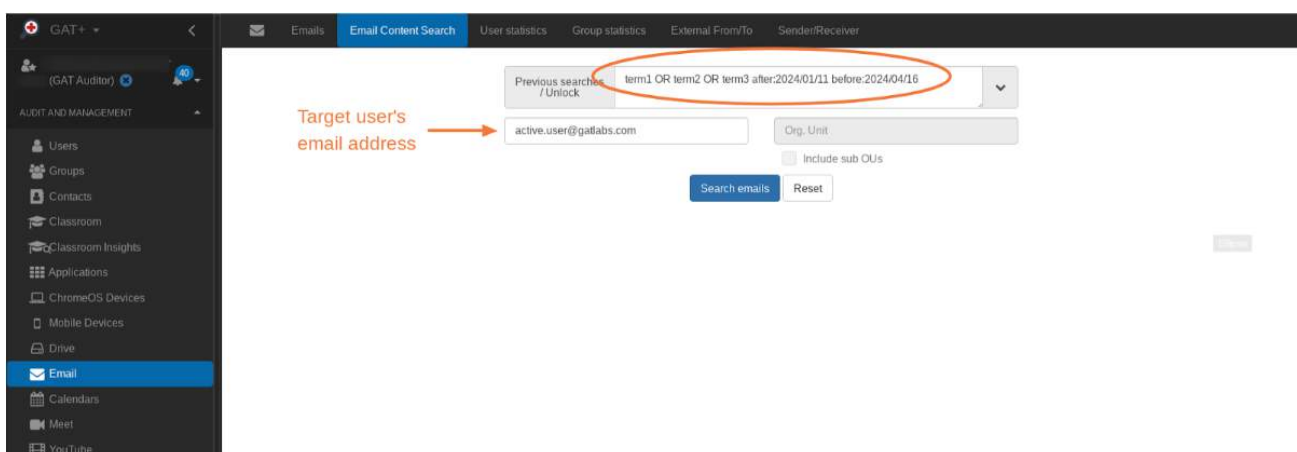
For example, with **GAT Flow**, an export could be created as part of a conditional case, offboarding process.

With this setup, **an export will be created** on account depending on a certain condition being met for that account, for example the departing user could be moved to a 'departing manager' group as part of the exit flow.

This would automatically trigger your Vault export Flow stream. In this way you never need to worry about visiting a separate app, or the cost involved if you were creating the export for every user.



If you are not paying for Google Vault licenses, you can still use the '**Email content search**' in GAT+ to search for specific terms, between any dates, for any active user on your domain.





# 8. Training and Policy Audit:

## 8.1 Ensure that all users are trained on how to use Google Workspace securely.

**Training** is an essential part of ensuring that users can use Google Workspace safely. While GAT Labs do not provide user training, with GAT Flow used in the onboarding process, the user environment can be extensively prepared for each new user.

This can include sending appropriate onboarding emails, adding appropriate training material to their drives, adding users to their correct calendars and groups and much more.

In particular we recommend using Security Awareness training tools such as [Knowbe4](#) and conduct regular training for all staff, on at least an annual basis.

## 8.2 Make sure your organization's policies for data handling are up-to-date and aligned with features and services provided by Google Workspace.

Creating appropriate corporate policies for data handling is crucial to ensure the security, integrity, and confidentiality of data, as well as to comply with legal and regulatory requirements. Here's a guide to developing effective data handling policies:

### 8.2.1 Data Classification:

- Define categories for data based on sensitivity and confidentiality (e.g. public, internal use, confidential, highly confidential).
- Establish handling protocols for each category.

### 8.2.2 Data Access and Authorization:

- Implement strict access control policies. Only authorized personnel should have access to sensitive data.
- Use the principle of least privilege, granting employees access only to the data necessary for their job functions.

# 8. Training and Policy Audit:

---

## 8.2.3 Data Collection and Storage:

- Define what data can be collected, and ensure it's in line with privacy laws (like GDPR, CCPA).
- Determine secure storage solutions, whether on-premises or in the cloud, and ensure they comply with regulatory standards.

## 8.2.4 Data Transfer and Sharing:

- Establish protocols for secure data transfer, both internally and externally.
- Set guidelines for data sharing with third parties, including requirements for encryption and secure transmission methods.

## 8.2.5 Data Encryption:

- Encrypt sensitive data both at rest and in transit. Thankfully this is a native feature of Google Workspace but consider implementing strong encryption for any legacy systems to protect your data.

## 8.2.6 Data Retention and Disposal:

- Define how long different types of data should be retained, in accordance with legal and business requirements.

## 8.2.7 Data Breach Response:

- Develop a data breach response plan outlining steps to take in the event of a data breach, including notification procedures as per legal requirements.

## 8.2.8 Employee Training and Awareness:

- Regularly train employees on data handling policies and the importance of data security.
- Keep staff updated on new data protection practices and policies.

## 8.2.9 Monitoring and Auditing:

- Regularly audit data handling practices to ensure compliance with policies.
- Use monitoring tools to detect unauthorized access or handling of data.

# 8. Training and Policy Audit:

---

## 8.2.10 Regulatory Compliance:

- Ensure that data handling policies are in compliance with all relevant laws and regulations, adjusting as these evolve.

## 8.1.11 Policy Review and Update:

- Regularly review and update the data handling policies to reflect new technologies, business practices, and legal requirements.

## 8.1.12 Incident Reporting:

- Establish clear procedures for employees to report security incidents or policy violations.

## 8.1.13 Vendor Management:

- If using third-party vendors for data processing, ensure they adhere to your data handling standards and are compliant with relevant regulations. Both Google and GAT Labs are SOC II compliant and certified.

These policies should be documented, easily accessible to employees, and enforced through regular audits and disciplinary actions for non-compliance.

**Remember**, effective data handling policies are not static; they should evolve as the business grows and as new threats and technologies emerge. Some versions of Google Workspace support the addition of 'Drive Labels' for document classification. GAT+ on all versions of Google Workspace supports the addition of 'tags' to documents for classification, reporting and security management.

While all of the above looks like a huge task, remember there are only going to be a limited number of data categories (see point one above) and everything else follows from that. Many of the items such as encryption are just checkboxes. **Both Google and GAT metadata** is encrypted at rest and in transit.

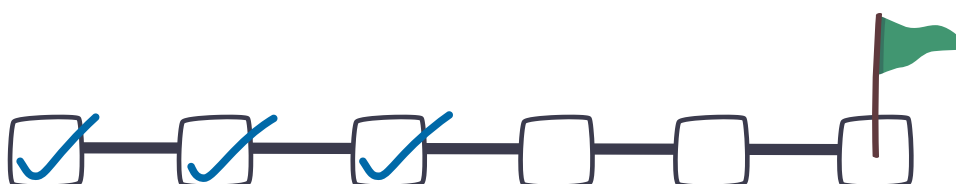
# 9.

## Use Google Workspace Audit :

### 9.1 Utilize the reports and audit logs provided by Google Workspace to get insights into various aspects of your environment, such as login activity, Admin activity, OAuth Token activity, etc.

Google provides very **detailed health checks** for your environment, they provide recommended steps and check boxes for medium and large domains (more than 100 users by their count) which can be found [here](#) and for smaller domains (less than 100 users) which can be found [here](#).

You will see that these steps are complementary to the steps and processes you enable in GAT+.



In most cases GAT+ is designed to ensure active compliance with rules and standards you set up using the Google checklists. GAT+ is also designed to provide detailed and scheduled reporting on a level that meets audit and compliance standards.

# 10. Regular Reviews:

## 10.1 Conduct regular audits to ensure ongoing compliance and security—quarterly or biannually, depending on the size and nature of your organization.

GAT+ reports can be scheduled to be **monthly, quarterly, biannual or even weekly basis** depending on your requirements.

These reports provide a written record of, and health check for your Google workspace environment.



# Dive Deeper Into GAT Labs

---

[EXPLORE MORE](#)

[VISIT OUR WEBSITE](#)

[SCHEDULE A DEMO](#)

[15 DAY FREE TRIAL](#)

