GAT LABS TRAINING RESOURCES

Top 10 Security Alerts You Should Set Up In GAT

GAT labs

Training Resources

Top 10 Security Alerts You Should Set Up in GAT

For Google Workspace Admins, security threats don't come with warning signs; they come as overlooked file shares, inactive accounts, suspicious downloads, or missed login events.
While Google Workspace offers a strong foundation, it doesn't always give you the real-time visibility or control needed to catch the subtle signs of insider threats, data leaks, or compromised accounts.

Some of the most common challenges we hear from Admins include:

- "I had no idea that file was shared publicly."
- "We didn't catch the mass download until it was too late."
- "There's no way to know who accessed the file and when."
- "Too many inactive accounts, but no time to monitor them."

That's why proactive alerting matters.

This guide walks you through the 10 most important alerts you should configure right away to improve your Google Workspace security posture.

Each alert below includes:

- The risk you're solving
- Where to find it in GAT
- How to configure it
- Best practices
- Related articles from our Knowledge Base with a full step-by-step guide

Let's get started.

1. Files Shared Externally Without Owner Awareness

The risk: Sensitive internal files are shared with outside parties without oversight.

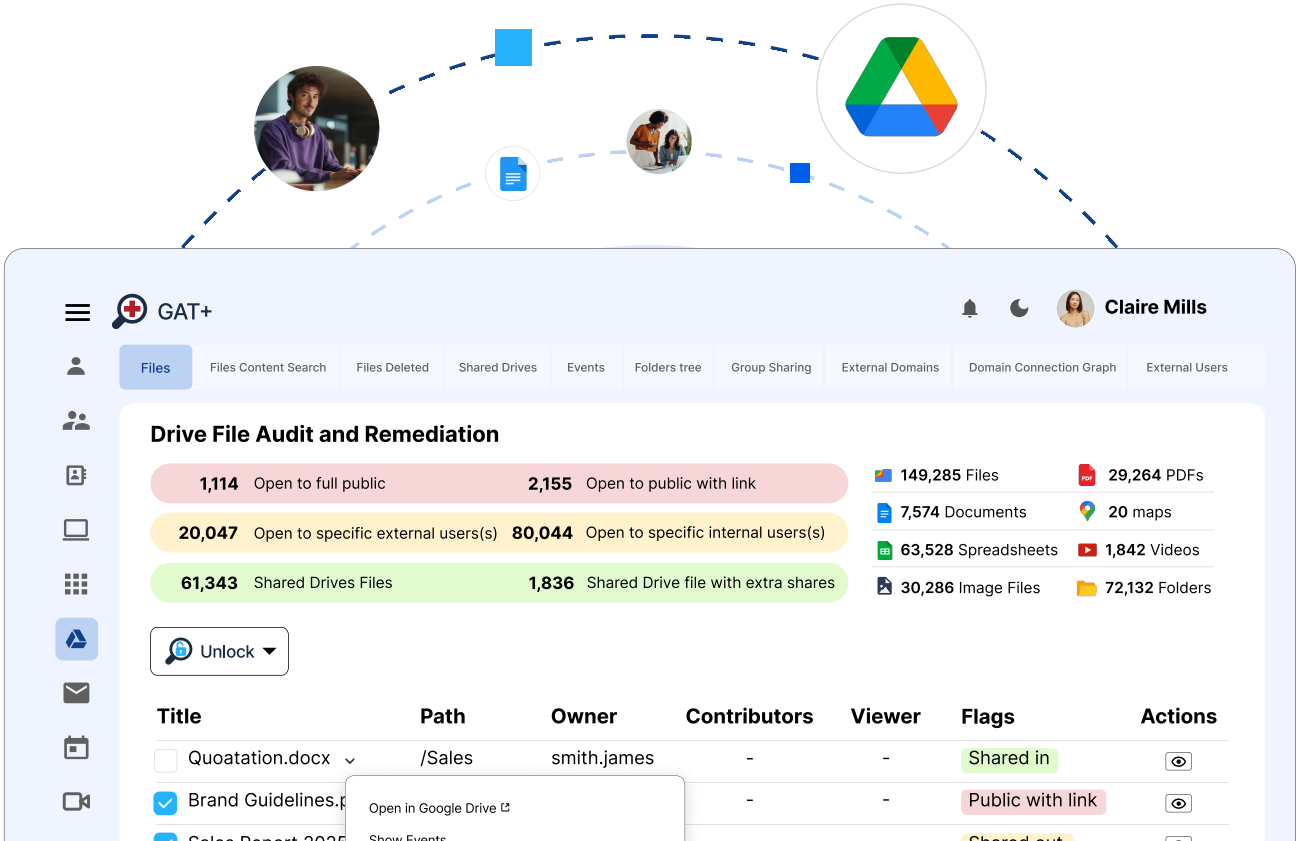
Our tool offers an alternative solution to Google Admin Console alerting, which we refer to as Alert Rules.

In GAT+, alerts are available across multiple areas:

- Applications
- Emails
- Drive
- YouTube
- Mobile devices
- Users
- User Logins

Drive Alert Rules support a range of activities, including:

- Number of files downloaded per day
- Number of files shared out per day
- Pattern-matching alerts (regex) for newly shared out files (Google-native, PDFs, TXT)
- Alerts based on "share to" email address patterns

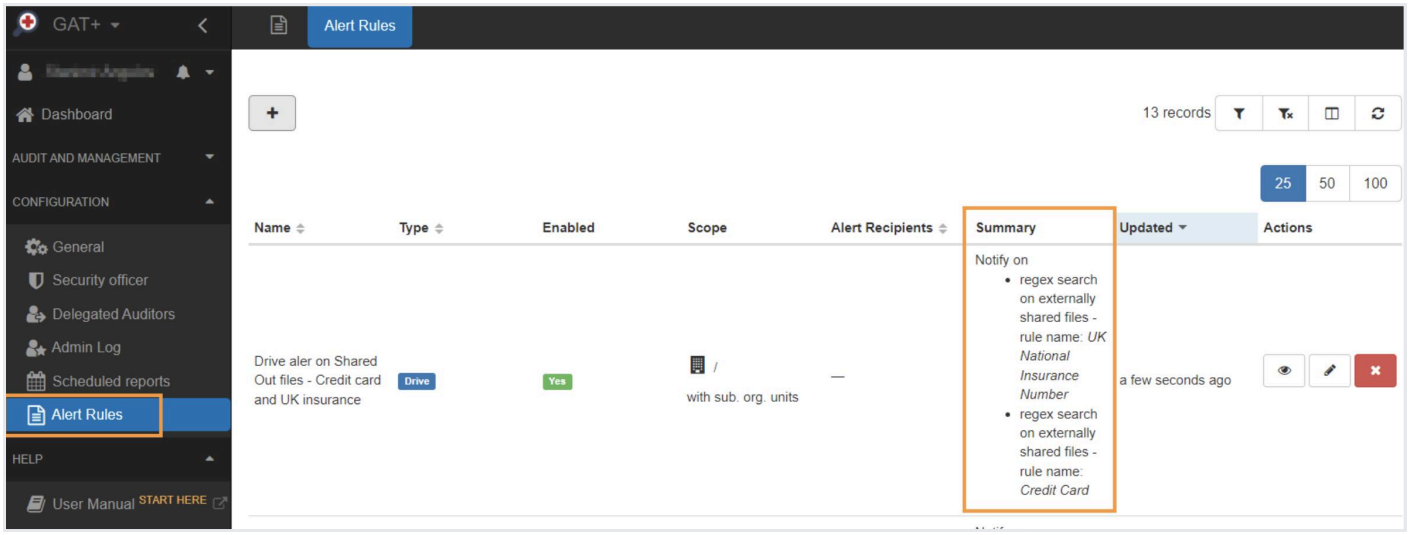


Training Resources: 10 Security Alerts You Should Set Up in GAT

How to set it up:

Navigate: *GAT+ > Configuration > Alert Rules*

- Create new alert
- Type: Drive
- Trigger: File shared externally
- Scope: Select Org Units, Groups or domain-wide
- Enable notification to file owners



Best practice: Notify both the admin and file owner for better accountability.

Related Articles: Set Up Google Drive DLP Alerts for Shared Out Files

2. Alert Logins from Users outside your City or Country

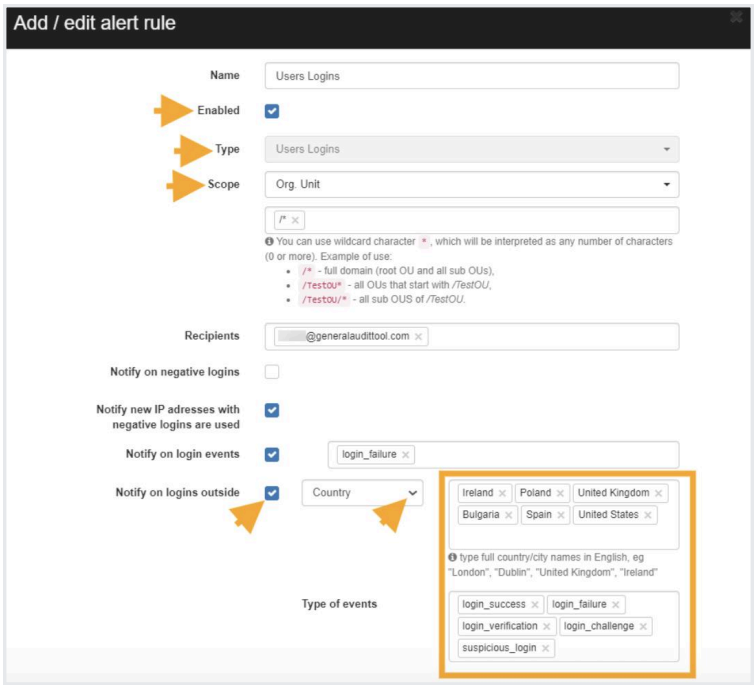
The risk: Suspicious logins from new or unexpected locations could indicate credential compromise, VPN tunneling, or unauthorized access attempts.

Without visibility into login geolocation, these incidents often go unnoticed until it's too late.

How to set it up:

Navigate: *GAT+ > Configuration > Alert Rules*

- **Add a name to the new rule and enable it.**
- **Type:** Select User Logins
- **Select Scope**
- **Trigger:**
  - A Failed login from a country or city not previously detected
  - Add a list of expected locations (e.g. countries) where login is permitted. If multiple boxes are selected it will trigger for any, so its best practice to have a separate alert rule for each trigger.
- **Start alert execution**

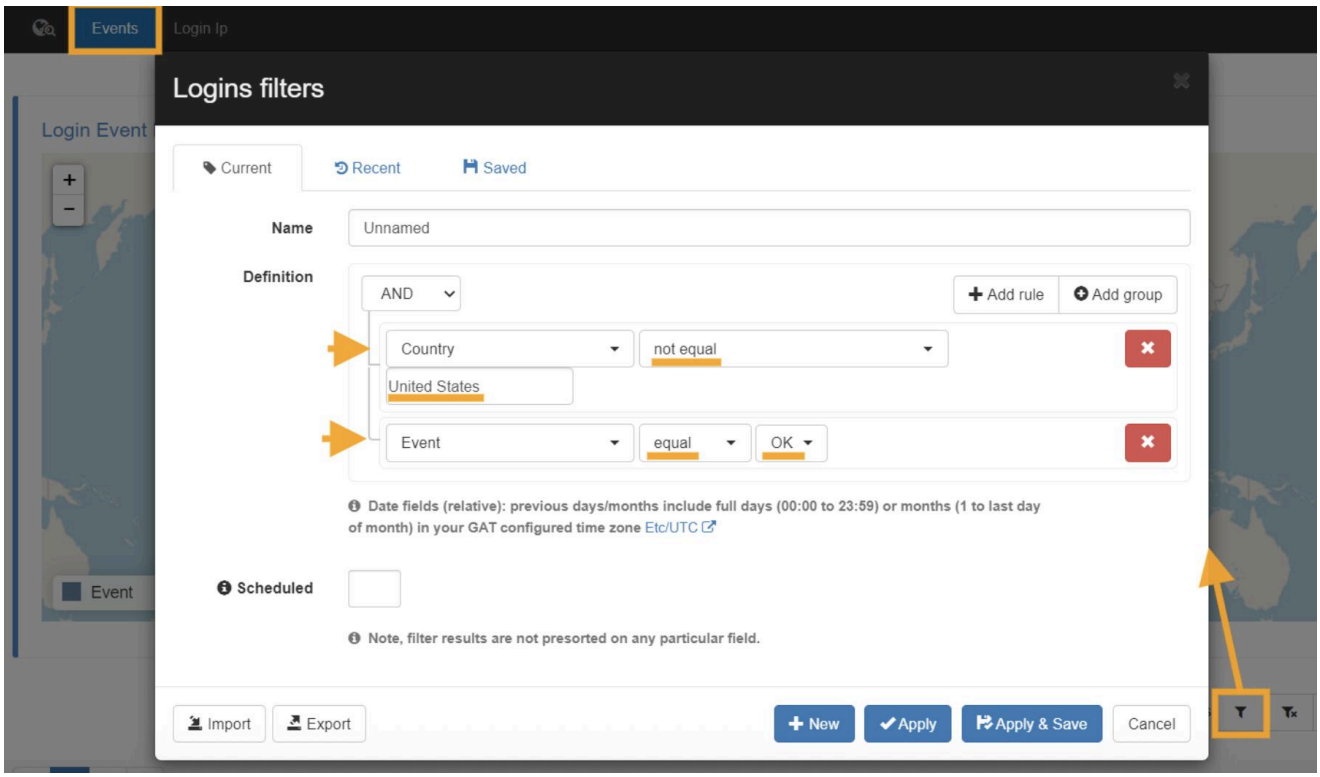


How to investigate user logins:

Navigate: *GAT+ > Audit & Management > Users Logins*

Use the **Events tab** to apply the following filters:

- Country not equal to expected country
- Event equal to “OK” (successful login)



Best practice: Always confirm with the user before taking action. Travel or legitimate remote work may explain the event.

Related Articles: Detect Suspicious Login Location

3. Privilege Misuse or Role Escalation

The risk: Admin privileges are among the most powerful tools in Google Workspace.

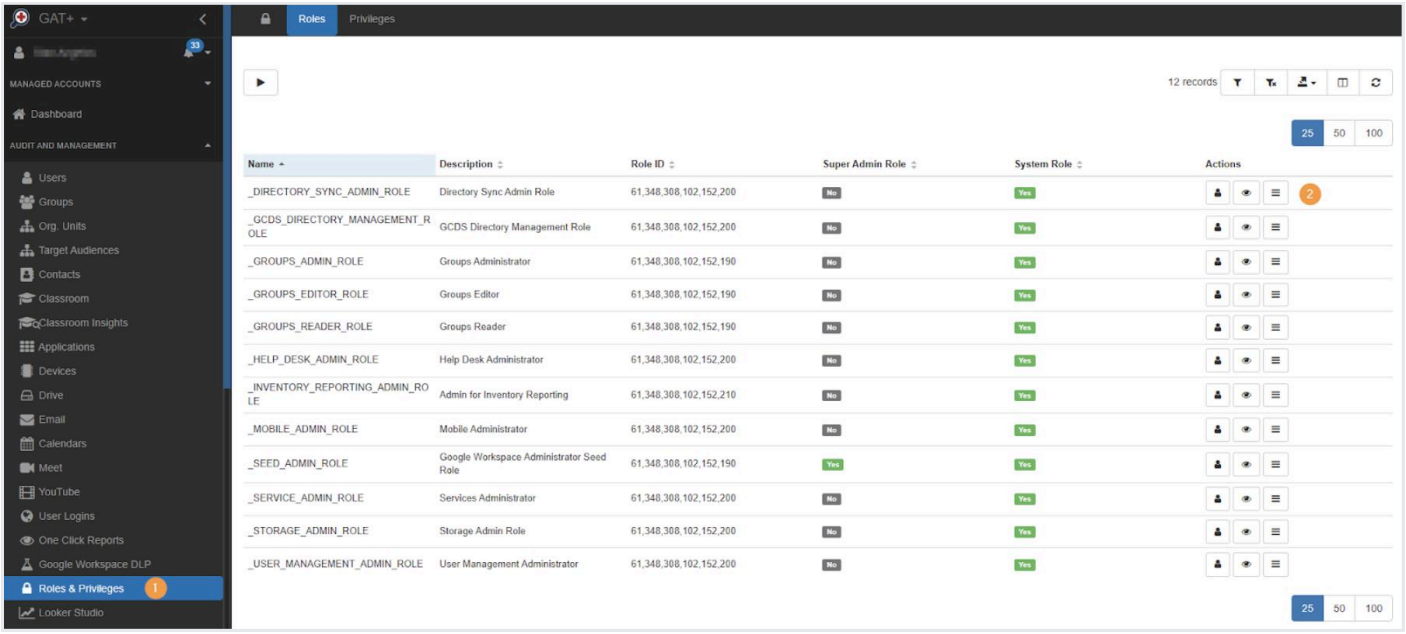
If a user is given elevated permissions by mistake or if an attacker gains access to a super admin account, the consequences can be severe.

How to monitor and audit admin roles:

Navigate: *GAT+ > Audit & Management > Roles & Privileges> Roles*

- Review which users hold elevated roles (Super Admin, Groups Admin, User Management, etc.)
- View role metadata and assigned privileges
- Export the list of users per role

GAT+ gives you a more readable breakdown of privileges than the native Google Admin Console, so you can quickly understand each role's risk level.



Best practice: Periodically review all user roles to eliminate dormant or unnecessary elevated permissions.

Related Articles: User Roles and Privileges within Google Workspace Admin Console

4. Detect Deleted Drive Files and Who Deleted Them

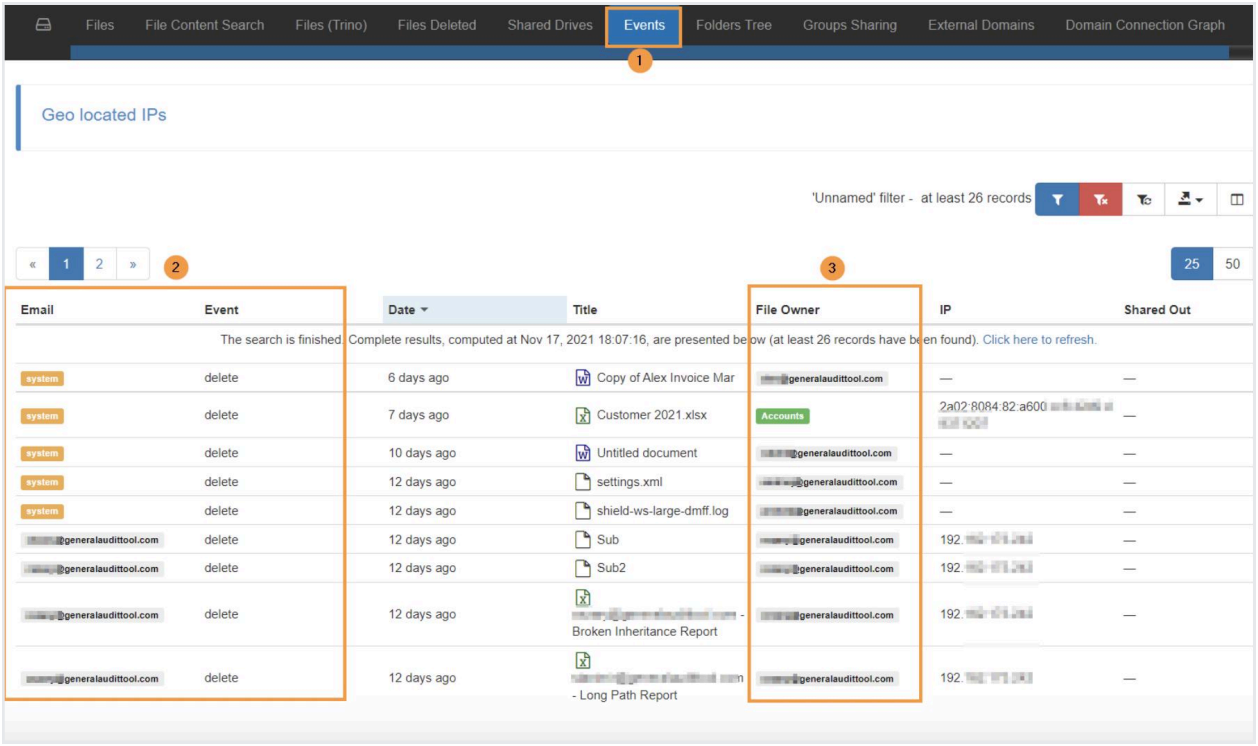
The risk: Files deleted without approval, especially from Shared Drives, can disrupt workflows or indicate insider threats.

How to investigate Drive deletions:

Navigate: *GAT+ > Drive > Events*

- Filter by Event = Delete
- Filter by File Owner = Shared Drive (for Shared Drive files)
- Use the Email column to identify who deleted the file

An Admin can combine the filters and search for Events equal to 'Delete' or 'Trash' to view all Deleted and Trashed files and who performed the Deletion.



Best practice: Combine this alert with a daily Drive activity report to spot suspicious behavior, especially around sensitive content.

Related Articles: How to Find Who Deleted a File in Google Drive

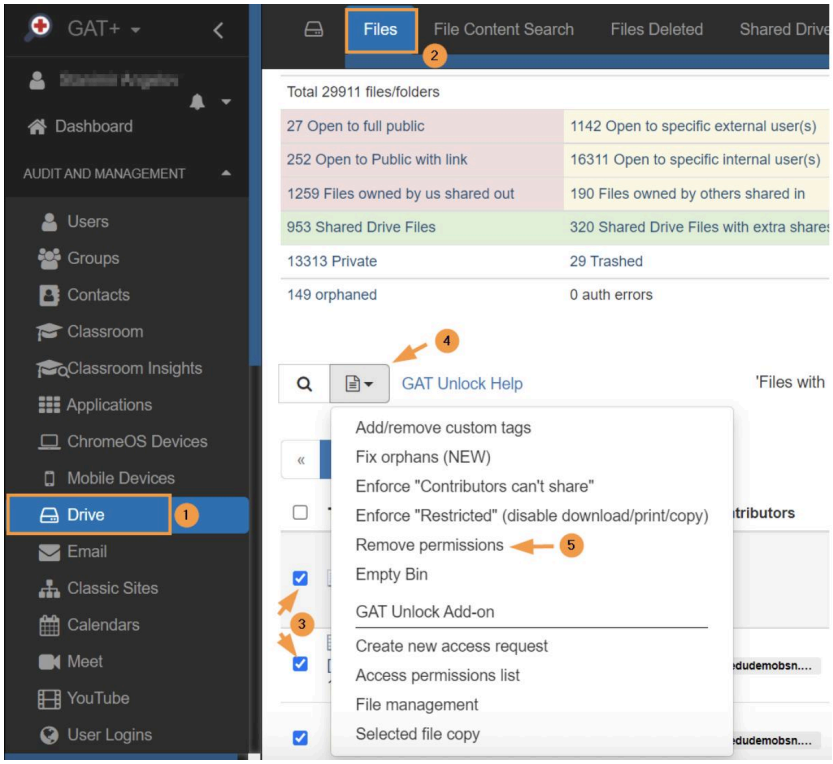
5. Detect and Remove Public or Public with Link File Shares

The risk: Public file sharing settings expose internal data to anyone with a link, or to everyone on the internet.

How to find and remove public links:

Navigate: *GAT+ > Drive > Files*

- Apply filter:
  - Sharing Flags contains Public OR Public with link
- Use File Operations > Remove Permissions to:
  - Remove “everyone” or “everyone with link” permissions
  - Apply scheduled cleanup
  - Optionally notify file owners



Best practice: Enable Report Only first to audit before taking action. Then automate remediation with scheduled reports.

Related Articles: Remove Public and Public with Link Permissions from Google Drive Files

6. Monitor Suspicious Gmail Forwarding and Calendar Events

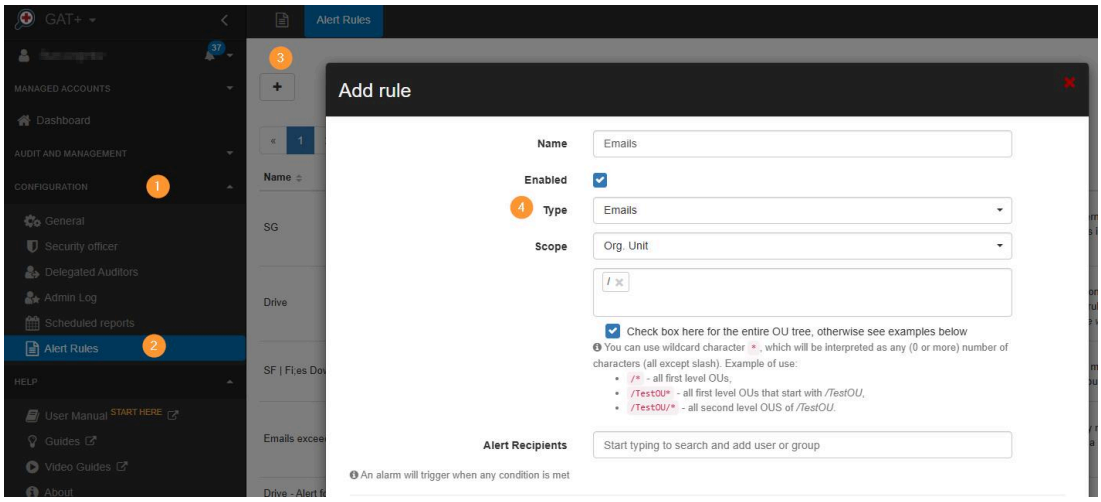
The risk: Gmail forwarding rules are a classic method for data exfiltration.

Likewise, calendar invites with sensitive data or recurring access can expose internal information without oversight.

How to monitor Gmail alert activity:

Navigate: *GAT+ > Configuration > Alert Rules*

- Create a new alert
- Type: Emails
- Scope: Choose user, group, or OU



- **Enable one or more of the following alert types:**
  - Alert on External email forwarding (when email forwarding is enabled)
  - Alert on Email delegation (when email delegation is set)
  - Alert on new Gmail filters (when a new Gmail filter is added)
  - Alert on new email Send as
  - Alert on number of external emails received (emails in a 24 hour period)
  - Alert on number of external emails sent (emails in a 24 hour period)
  - Alert on number of external emails sent (by number. of recipients)

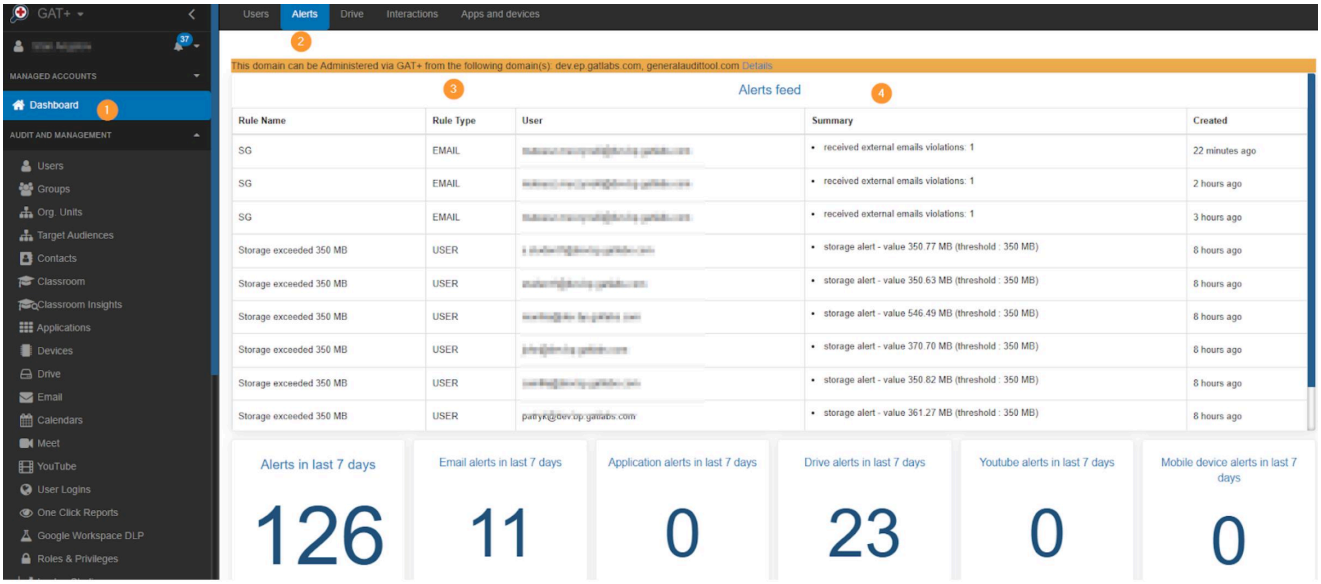
Note: It also includes the number of (external) members in groups

- Alert on number of internal emails received
- Alert on number of internal emails sent

How to investigate triggered alerts:

Navigate: *GAT+ > Dashboard> Alerts*

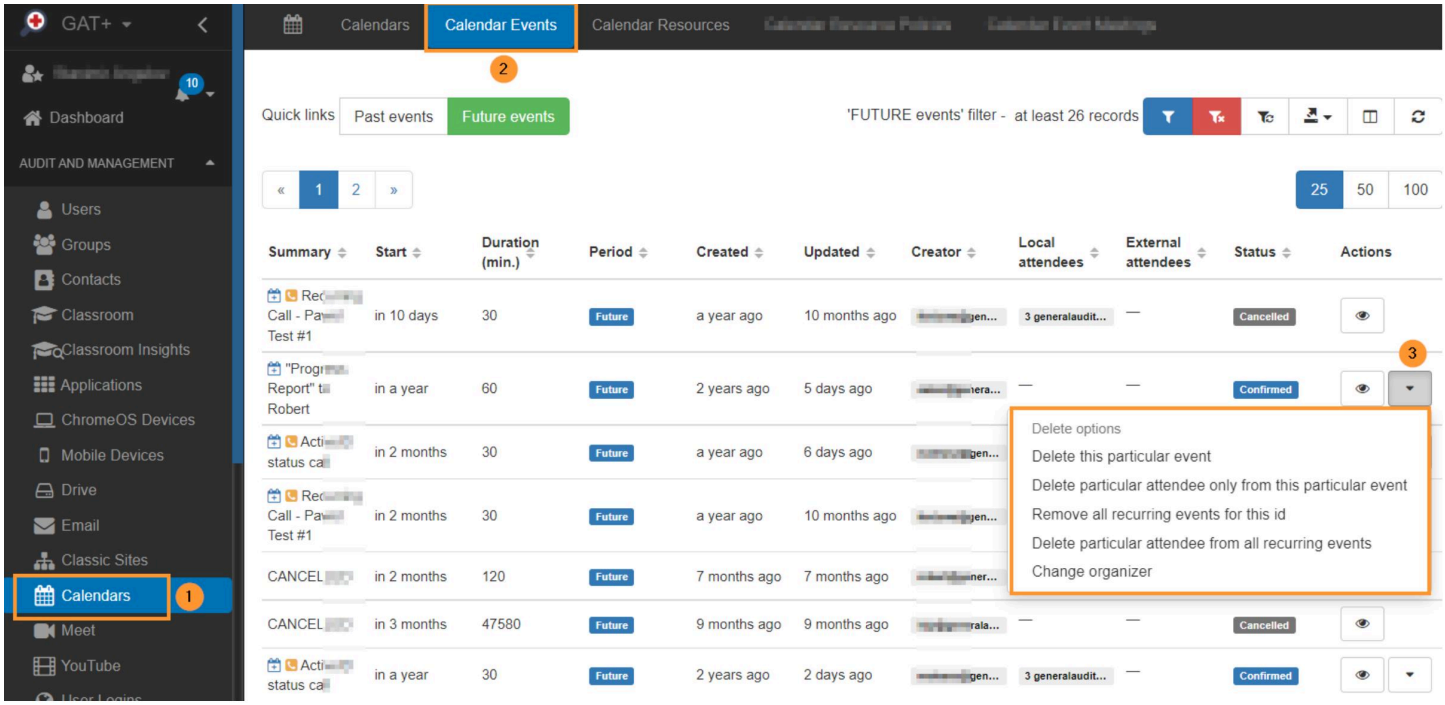
- View the alert log by user and type
- Click into alert to trace timeline and related actions



Bonus: How to Audit Calendar Events in Parallel

Navigate: *GAT+ > Calendars > Calendar Events*

- Filter for future events or sensitive subjects
- Use Actions to remove attendees or cancel events



Best practice: Combine Gmail forwarding alerts with calendar audits to catch coordinated misuse (e.g. external meetings with attachments + filter forwarding setup).

Related Articles:

- Set Up Gmail Alerts for Google Workspace Users with GAT+
- Google Calendar Audit and Event Management with GAT+

7. Use of Risky Chrome Extensions

The risk: Chrome extensions can introduce major vulnerabilities if they require sensitive permissions or are not vetted.

Some may access private user data, change browser settings, or even exfiltrate files, all without the user's full awareness. In schools and enterprise environments, it's critical to monitor and assess these extensions proactively.

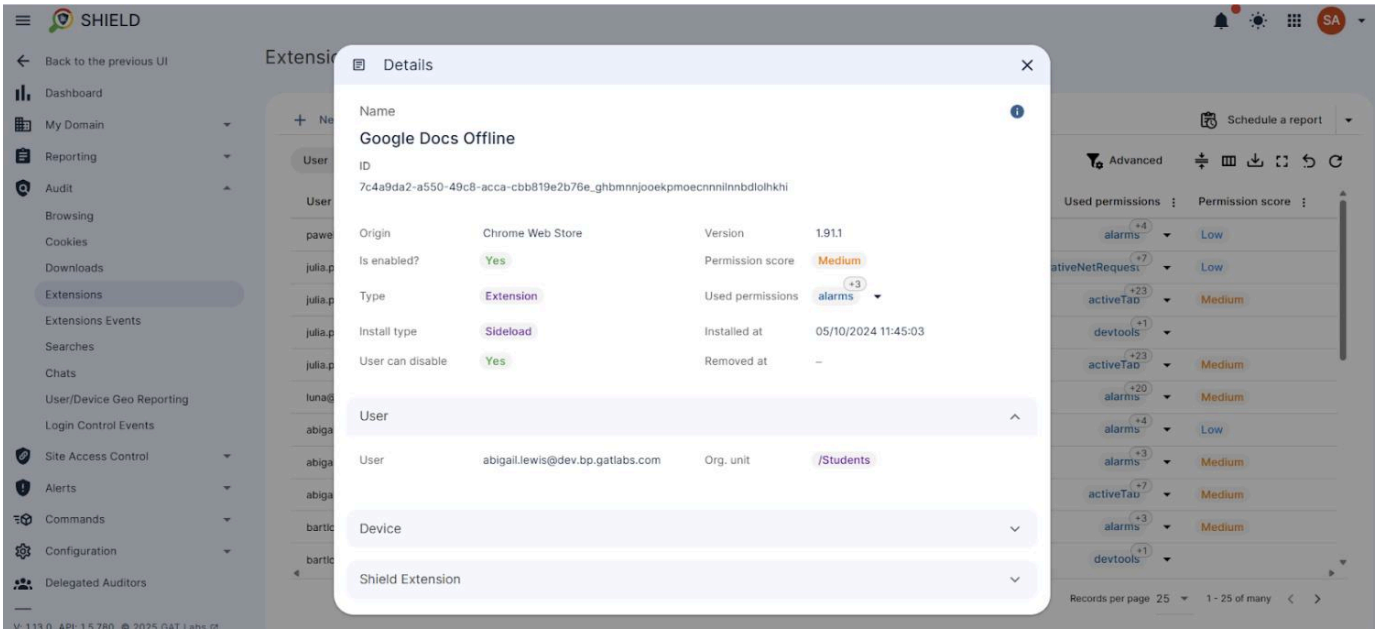
How to monitor extensions:

Navigate: *GAT Shield > Audit > Extensions*

View data on every extension installed across your domain:

- Extension name and version
- Permission list and permission score (Low, Medium, High)
- Whether enabled or disabled
- When installed or removed
- Who installed it

Use filters to audit by risk level or scope, click the “details” icon on the right end side to review deeper permissions.



Risk Assessment:

Navigate: *GAT Shield > Extensions > Extensions Explorer*

Permission scores are calculated based on Chrome's permission categories. A high score signals potentially risky behavior, like file system access, audio/video capture, or identity manipulation.

Tip: Use GAT Shield's Extension Control feature or set up Alert Rules to auto-block extensions based on permission scores or specific criteria.

Related Articles: Audit Chrome Extensions with GAT Shield

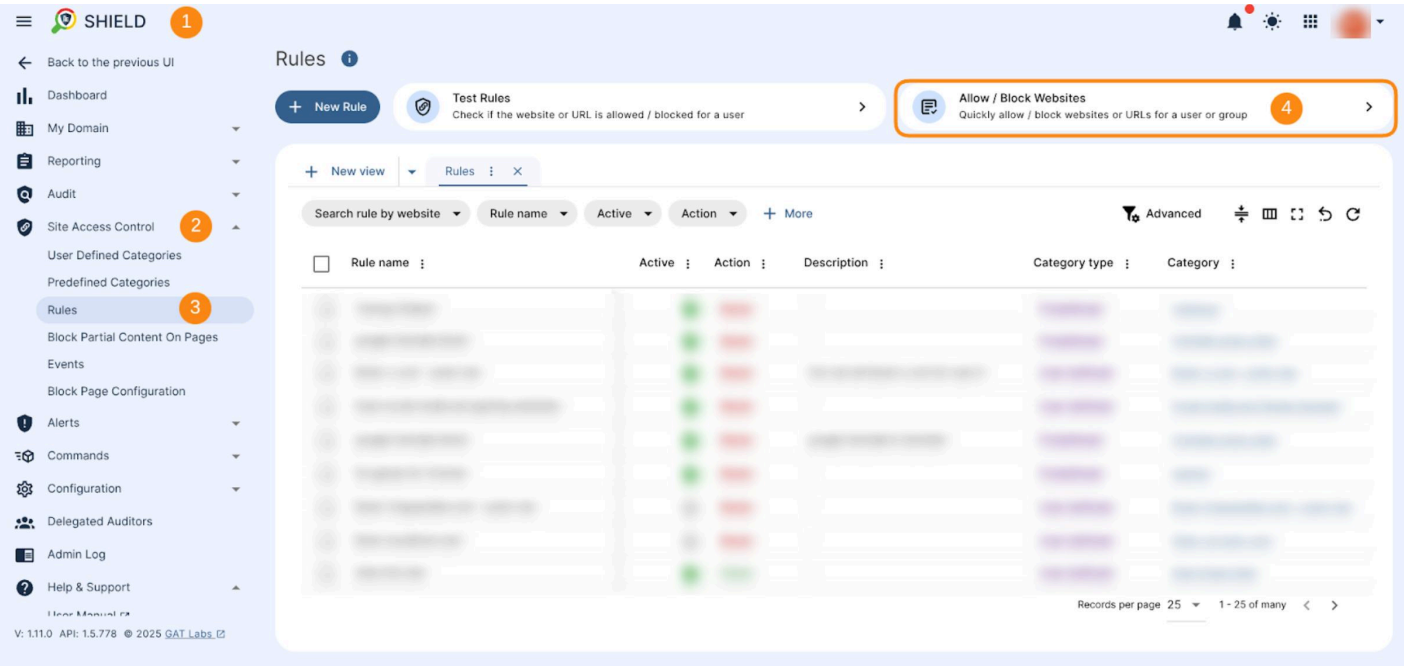
8. Block Risky or Inappropriate Websites for Users

The risk: Students or staff may visit dangerous or inappropriate sites, whether by accident or intent. This opens the door to malware, phishing, and productivity loss.

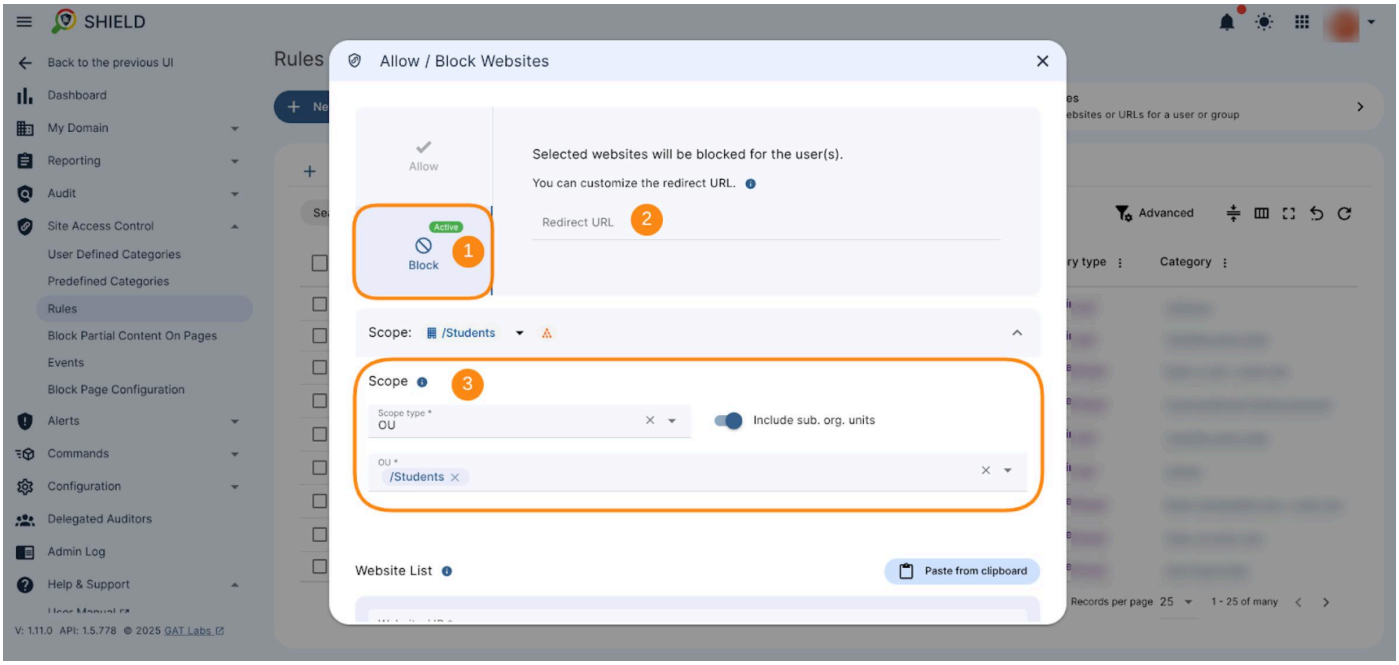
How to block websites:

Navigate: *GAT Shield > Site Access Control*

- Go to Rules > Allow/Block Websites



- Choose Block and define the website(s)
- Optionally set a redirect URL (e.g., company homepage)
- Define the Scope: user, group, OU, or all users
- Click Block to activate



Tip: You can batch paste website lists and apply rules by OU to support tiered browsing policies (e.g., students vs. staff).

Related Articles: Block Websites with Site Access Control in GAT Shield

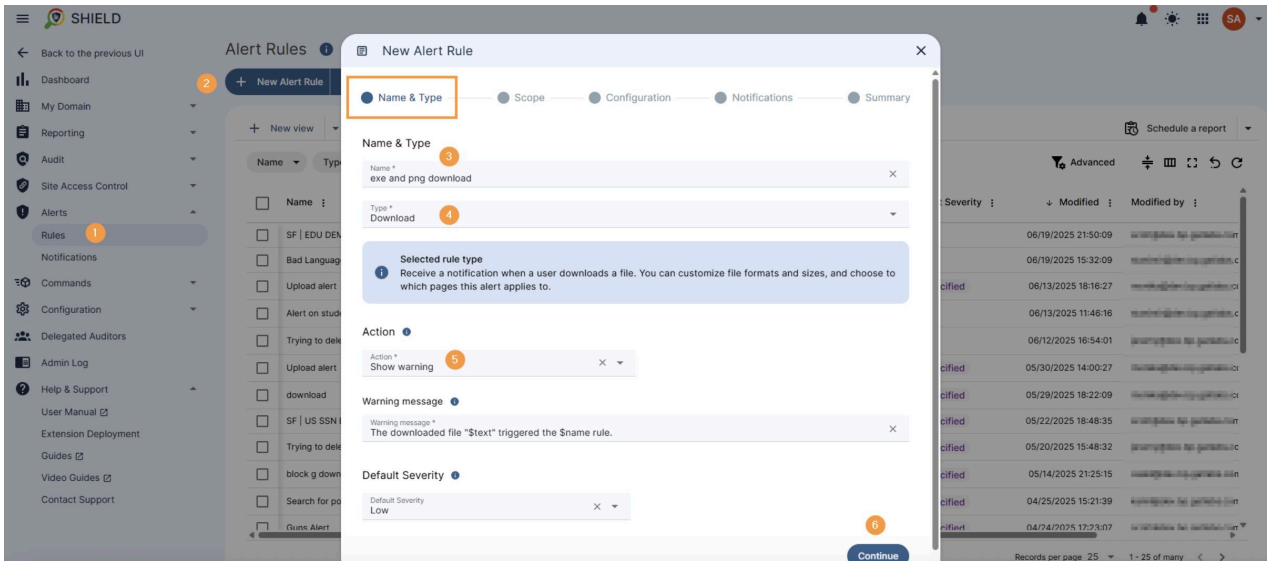
9. Block Risky File Downloads in Google Chrome

The risk: Users downloading executable or compressed files (like .exe, .zip, .mp3) through Chrome can introduce malware, bypass data controls, or hoard internal assets.

How to configure download blocking:

Navigate: *GAT Shield > Configuration > Alert Rules*

- Click to create a new rule
- **Rule Type:** Select Downloads
- **Scope:** Apply to Org Unit, Group, or entire domain
- **Trigger:** Download of specific file extensions (e.g., .exe, .zip, .mp3, .apk)
- **Select Actions:**
  - Block the download in real time
  - Notify the user and/or IT admin
  - Optionally, auto-remove the downloaded file using post-alert actions



Tip: You can also enable reporting-only mode first to observe behavior before enforcing blocks. Combine this rule with download thresholds or geolocation filters for additional context.

Related Articles:

- Block .EXE File Downloads in Google Chrome Using GAT Shield
- Prevent MP3 and Other Risky File Downloads

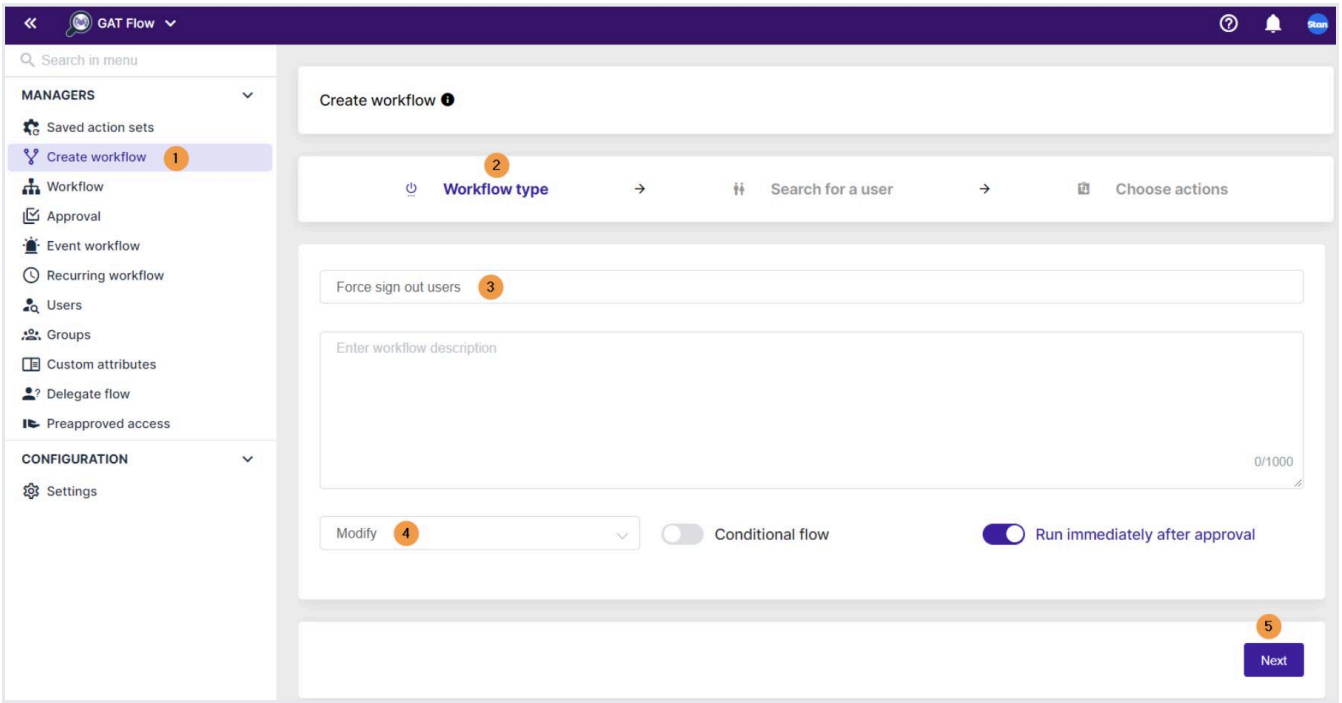
10. Force Sign Out Suspicious or Compromised Accounts

The risk: A user forgets to log out from a shared device, or a lost/stolen device remains logged into a corporate account, creating an open door to sensitive data.

How to force a logout of a user account:

Navigate: *GAT Flow > Create Workflow*

- Choose workflow type: Modify (for active users) or Offboard (for departing users)
- Select the user(s), group, or Org Unit
- Add the Force Sign Out action
- Submit for Security Officer approval
- Once approved, users will be signed out of all active sessions



Best practice: Combine with GAT+ login alerts to create a response workflow that auto-triggers a forced sign-out when suspicious login behavior is detected.

Related Articles: Force Sign Out Users in Google Workspace

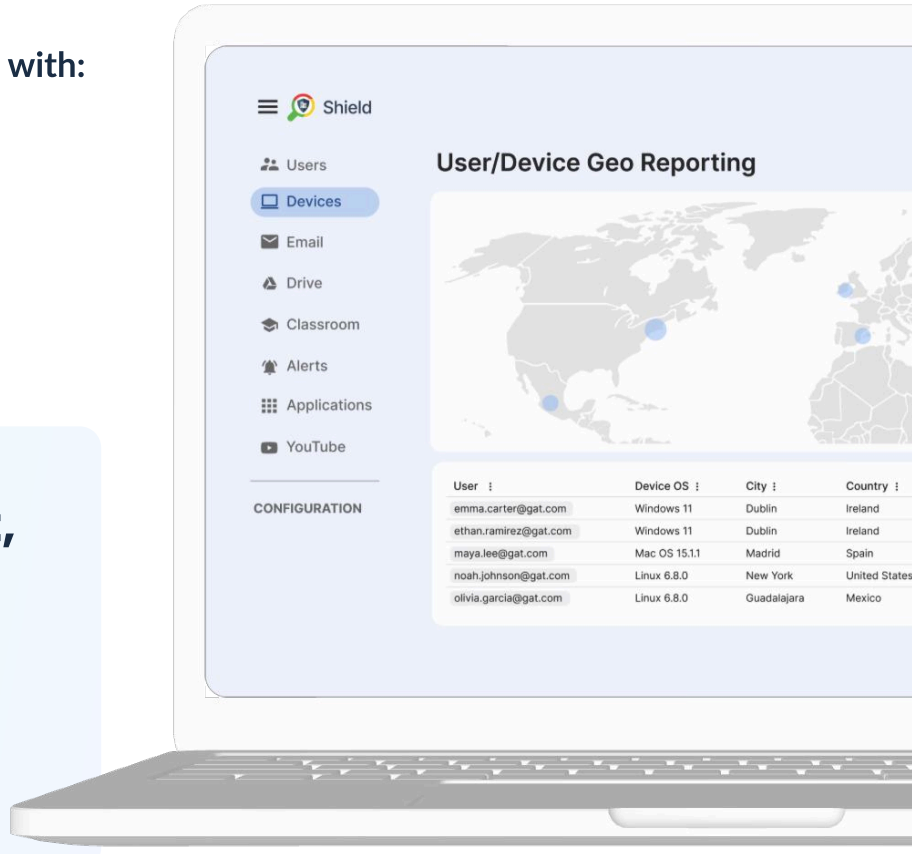
Final Tips for Admins

Security alerts are most effective when they're tied to action, not just awareness.
Here are some final tips to help you manage alerts more efficiently:

- Review alert rules quarterly to adapt to user, policy, or org structure changes
- Pair alerts with scheduled reports for ongoing visibility
- Use GAT Flow to trigger automatic actions based on alert conditions (like off boarding, password resets, or forced logouts)
- Keep a spreadsheet log of your current alert rules, scopes, and recipients to stay organized
- Use Report-Only mode to test rules before applying changes

If you're unsure where to start, begin with:

- Drive sharing alerts
- Gmail forwarding
- Login from new country



These are high-impact, low-effort wins.

From there, layer on Flow and Shield coverage as you grow.

Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

GAT labs