GAT LABS TRAINING RESOURCES

Auditing Apps And Extensions In Google Workspace With GAT+ And GAT Shield

GAT labs

Training Resources

Auditing Apps and Extensions in Google Workspace

Third-party apps and Chrome extensions are common blind spots in Google Workspace environments. Without proper oversight, users can connect risky apps or install unsafe extensions that expose your domain to data leaks and compliance issues.

This guide helps Google Admins:

- Identify which apps users have connected
- Spot risky OAuth scopes
- Monitor Chrome extension activity across devices
- Take action to audit or remove apps/extensions

With GAT+ and GAT Shield, you can:

- Gain full visibility into apps and extensions
- Monitor OAuth scopes and permissions
- Set rules to trust, block, or auto-remove apps/extensions
- Act quickly on policy violations

Let's walk through how to audit and control apps and extensions across your Google Workspace domain.

1. Why App and Extension Auditing Matters

Google Workspace Admins face a growing challenge: users connecting third-party apps or installing Chrome extensions without oversight. This can expose your domain to serious security and compliance threats, from OAuth abuse to silent data leaks. Without proper visibility, even well-meaning users can unintentionally put sensitive data at risk.

Common pain points include:

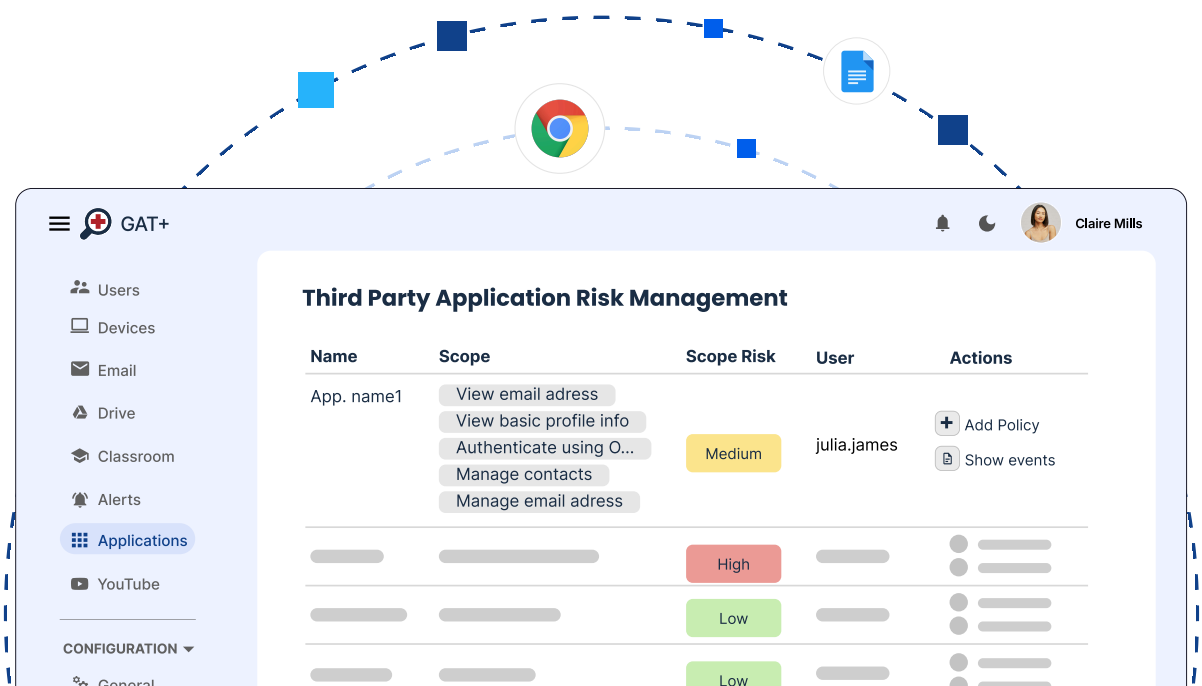
- Shadow IT from unapproved SaaS apps
- Apps requesting excessive OAuth permissions like full access to Gmail, Drive, or Contacts
- Malicious Chrome extensions installed from the web store
- Difficulty identifying which tools are being used across the domain

GAT Labs provides a dual solution:

- GAT+ audits and manages all third-party apps connected to Google Workspace accounts, with full visibility into OAuth scopes and usage.
- GAT Shield audits Chrome browser extensions installed on managed devices, with alerts and policy enforcement.

With both tools, Admins can reduce risk exposure, enforce security standards, and answer one of the most critical IT questions:

"What's connected to our domain, and is it safe?"



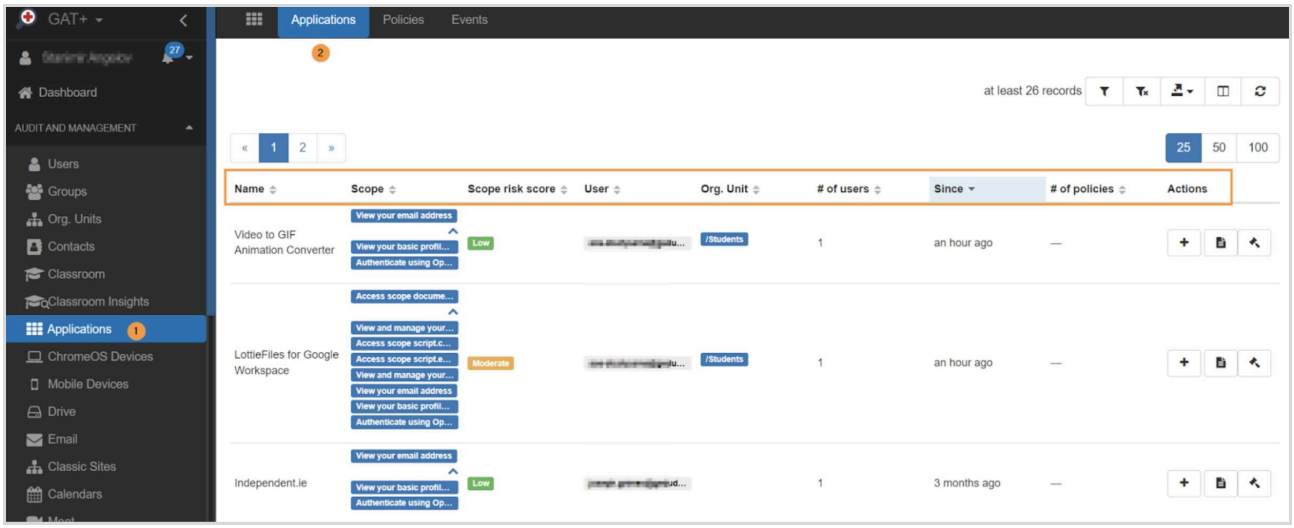
2. Auditing Google Workspace Apps with GAT+

Many Admins are surprised by how many third-party apps are connected to user accounts, some of which were never reviewed or approved. These apps can request powerful OAuth scopes, like full access to Gmail or Drive, without users fully understanding the impact.
Without auditing, domains face unnecessary exposure to data exfiltration, compliance violations, and shadow IT.

How to do it:

Navigate: *GAT+ > Applications*

The Applications section in GAT+ lists all third-party apps users have connected to their Google Workspace accounts, current and historical.



Key Actions for Admins:

- View all third-party applications connected to user accounts
- Identify apps by user, risk score, and scopes requested
- Block or trust apps across the domain, OUs, or users
- Generate audit reports for compliance reviews

Related Articles:

- Audit And Manage Third-Party Applications
- Google Workspace Apps Risk Assessment

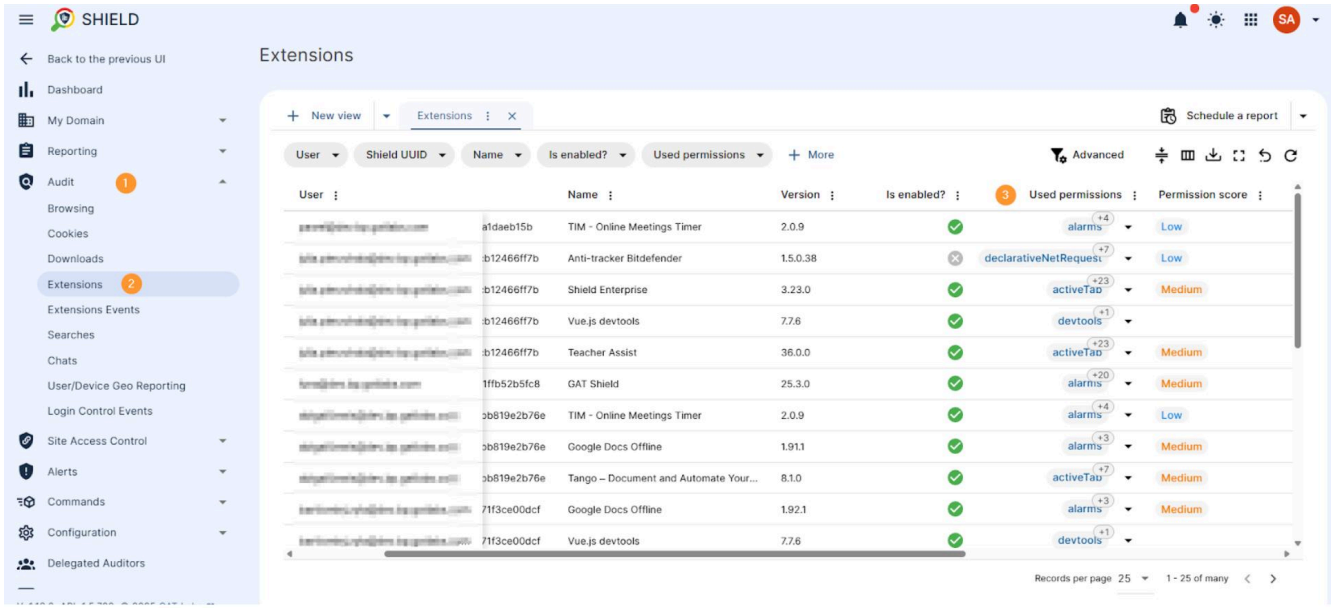
3. Auditing Chrome Extensions with GAT Shield

Chrome extensions can pose serious risks if not monitored properly. Admins need full oversight of what's installed across managed browsers to prevent data leaks or policy violations.

GAT Shield allows Google Admins to audit Chrome extensions on Chromebooks across their domain. You can track installation and removal activity, assess permission risks, and gain a full picture of extension behavior on managed ChromeOS devices.

How to do it:

Navigate: *GAT Shield > Audit > Extensions*



You'll have a detailed view of every Chrome extension installed on a user's browser, including:

- **Name:** The extension's name as listed in the Chrome Web Store
- **Version:** The currently installed version
- **Used permissions:** A breakdown of permissions the extension requires
- **Permission score:** A GAT-calculated score based on the type and scope of permissions:

  Low – minimal access

  Medium – moderate access to services like tabs or web requests

  High – full access to sensitive data (e.g. Gmail, Drive, browsing history)

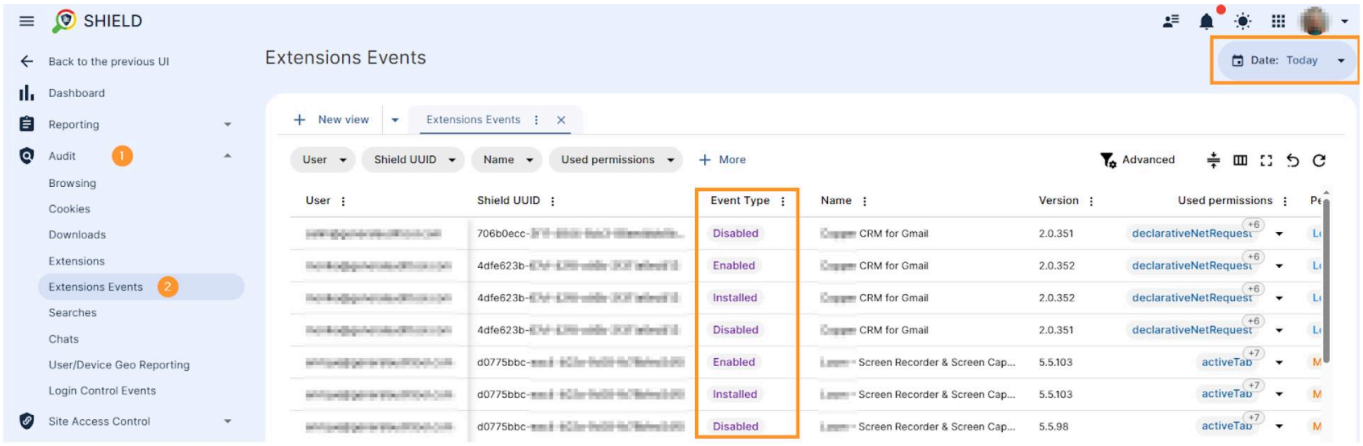
- **Enabled:** Indicates if the extension is currently active
- **Installed:** Timestamp of when the extension was installed
- **Removed:** If uninstalled, the removal date
- **Users:** Lists which users have the extension installed

Types of Extension Events Tracked by Shield

The following event types are recorded:

- **Installed:** An extension has been added to a user's Chrome account.
- **Enabled:** An extension that was previously installed or disabled has been activated for a user.
- **Disabled:** An extension has been deactivated by or for a user.

This level of visibility helps Admins maintain tighter control over Chrome usage and reduce risks.



Related Articles:

- Chrome Extensions Audit In GAT Shield
- Audit Chrome Extension Events In GAT Shield

4. Policy Enforcement and Automation

In addition to app and extension control, GAT+ also allows policy enforcement across Drive file sharing, app access, and user behavior. Here's how to automate actions based on what your audits uncover:

Create custom sharing policies

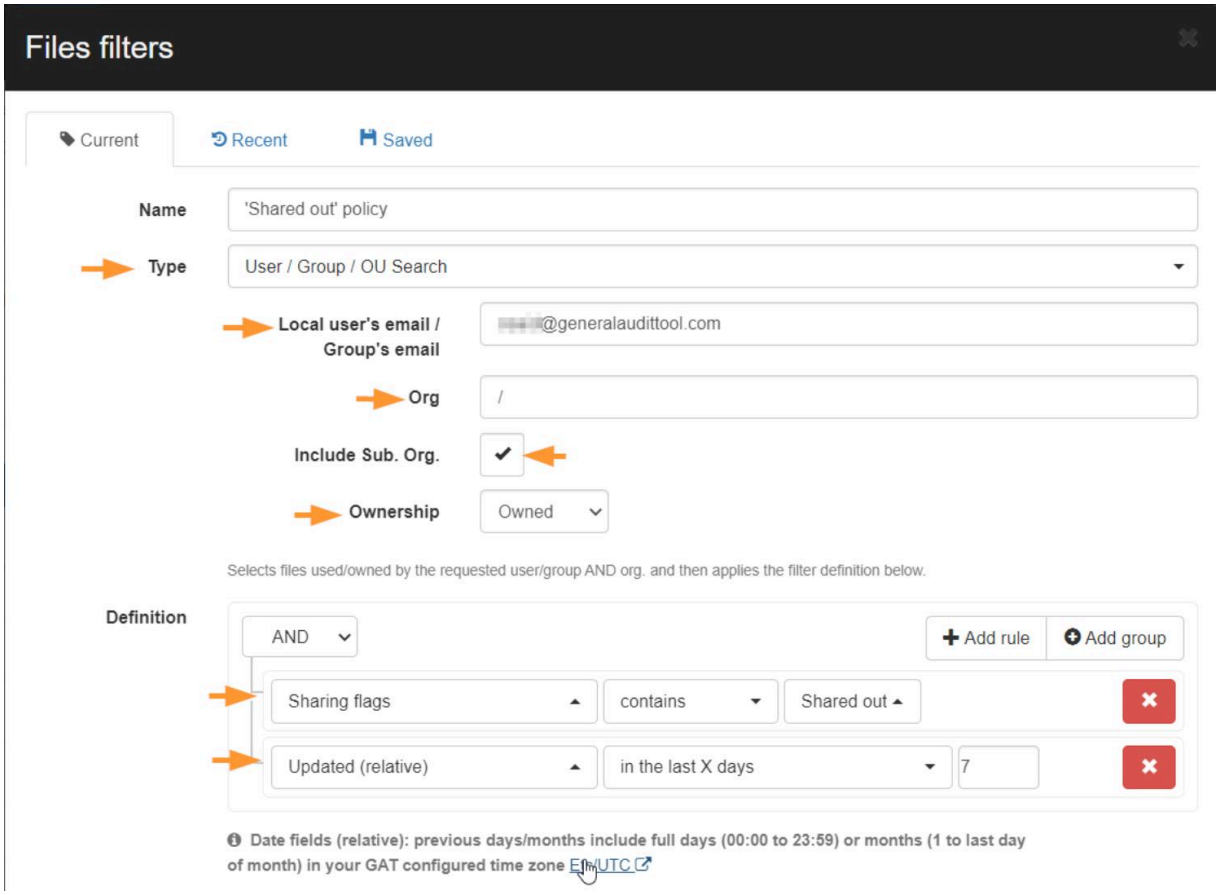
Detect violations based on Drive file type, ownership, or exposure (e.g. shared externally or publicly).

Set and Detect policy violations

Search for Sharing violations on Users, File, Folder, or any filter option.

How to do it:

Navigate: *Drive > Files >Apply custom filter*



Scheduled report

When the result is found, this can be set as “Scheduled report”.
Click "Scheduled" and complete the setup:

- **Occurrence** – select the time needed.
- **Enabled** – enable the report.
- **Apply & Schedule**

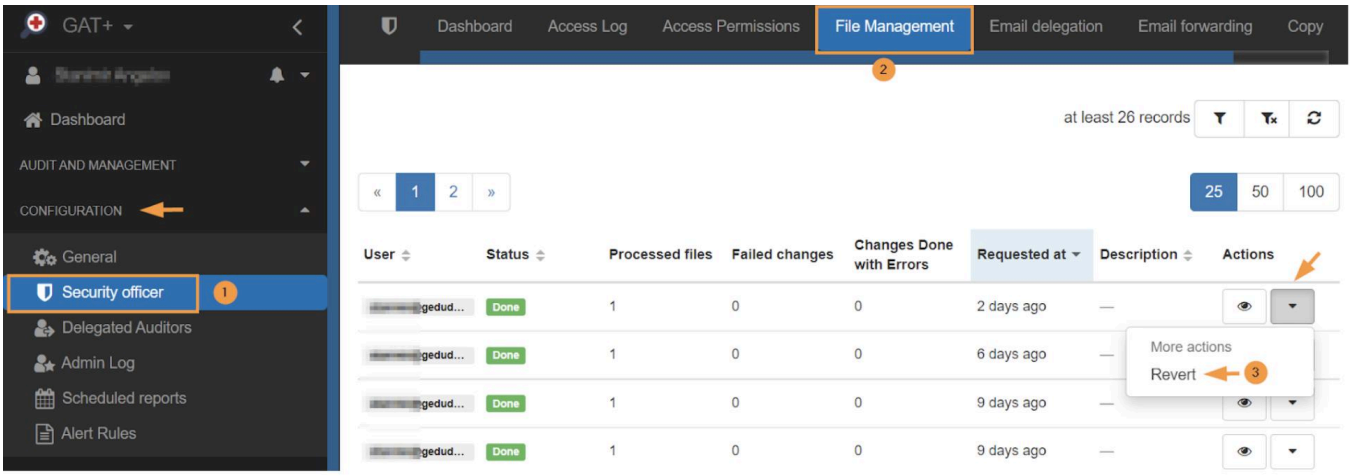
The policy report will run on your chosen schedule and show users and files involved in policy violations.

Restore permissions automatically

The Security Officer can revert the changes made by the Admin.
When a policy has been enforced, you will receive an email containing the details of the policy changes and a requested time, which you can then search for.

How to do it:

Navigate: *GAT+ > Configuration > Security officer > File management tab.*



Related Articles:

- Create A Policy For Any File Or Folder
- How To Detect A Sharing Policy Violation
- Restore Permissions Removed By A Policy
- Audit And Policy For Google Workspace Apps

5. Best Practices for Auditing Apps and Extensions

Securing your Google Workspace environment is not just about visibility, it's about taking action on what you uncover. The following best practices will help you maintain control, reduce risks, and respond proactively to potential threats:

- Review third-party app access monthly in GAT+ under Applications, with a focus on high OAuth scope scores and unused applications.
- Revoke or block unused, suspicious, or overly permissioned apps across OUs or the entire domain.
- Use trust/block policies and tags to pre-approve or ban apps/extensions based on scope or behaviour.
- Set alerts in GAT+ and GAT Shield to detect high-risk authorizations or new extension installations.
- Export and archive audit logs regularly for incident review, compliance, and reporting.
- Educate users on approved apps, how permissions work, and how to recognise risky authorisation prompts.

With GAT+ and GAT Shield, Google Admins can take proactive control over apps and extensions before they become a problem.

Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

GAT labs