GAT LABS TRAINING RESOURCES

Drive File Ownership, Access Control & Compliance Reporting In Google Workspace

GAT labs

Training Resources

Drive File Ownership, Access Control & Compliance Reporting in Google Workspace

This guide explains how to audit Drive activity, manage file ownership, and control file access using GAT Labs tools. It is designed to help Google Workspace administrators gain better visibility, reduce data exposure risks, and ensure compliance across their domain.

With GAT+ you can:

- Gain full visibility into every file across your domain, including My Drive and Shared Drives.
- Efficiently manage file ownership, including transferring files from suspended users.
- Perform bulk actions to enforce security policies and remediate issues across thousands of files at once.
- Create custom scheduled reports to automate your compliance and security monitoring.

With GAT Shield you can:

- Set up real-time alerts for potential data leaks and policy violations.
- Control access to resources based on a user's location.
- Enforce restrictions on file downloads, printing, and sharing.

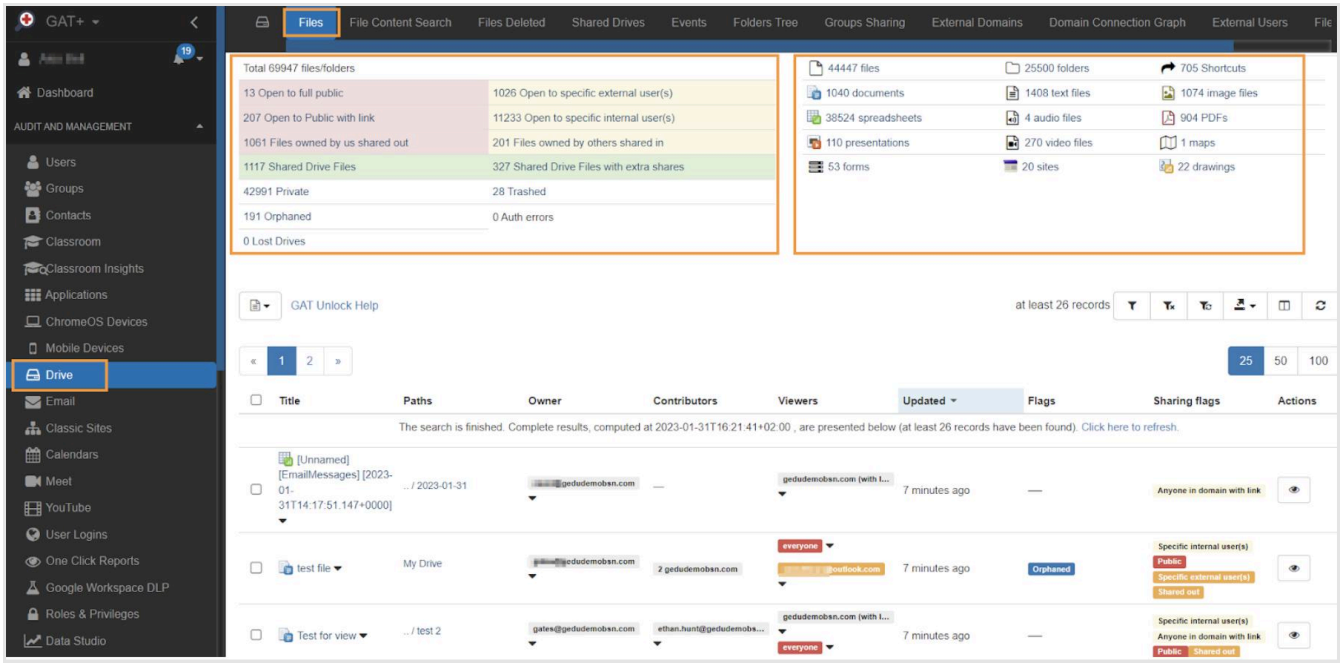
Section 1. Drive File Ownership

Why is Drive File Ownership Important?

Managing file ownership is a critical administrative task for maintaining data security and continuity. When an employee leaves the organization, their files can become "orphaned," leading to data loss and a lack of accountability. By proactively managing ownership, you can ensure that important files remain accessible and controlled by the company, reducing risk and improving long-term data governance.

1. Finding and Transferring Ownership of Files

Get full visibility into all Drive files across My Drive and Shared Drives. Use filters to narrow your scope and surface high-risk content. This is especially useful for managing files owned by departing employees.

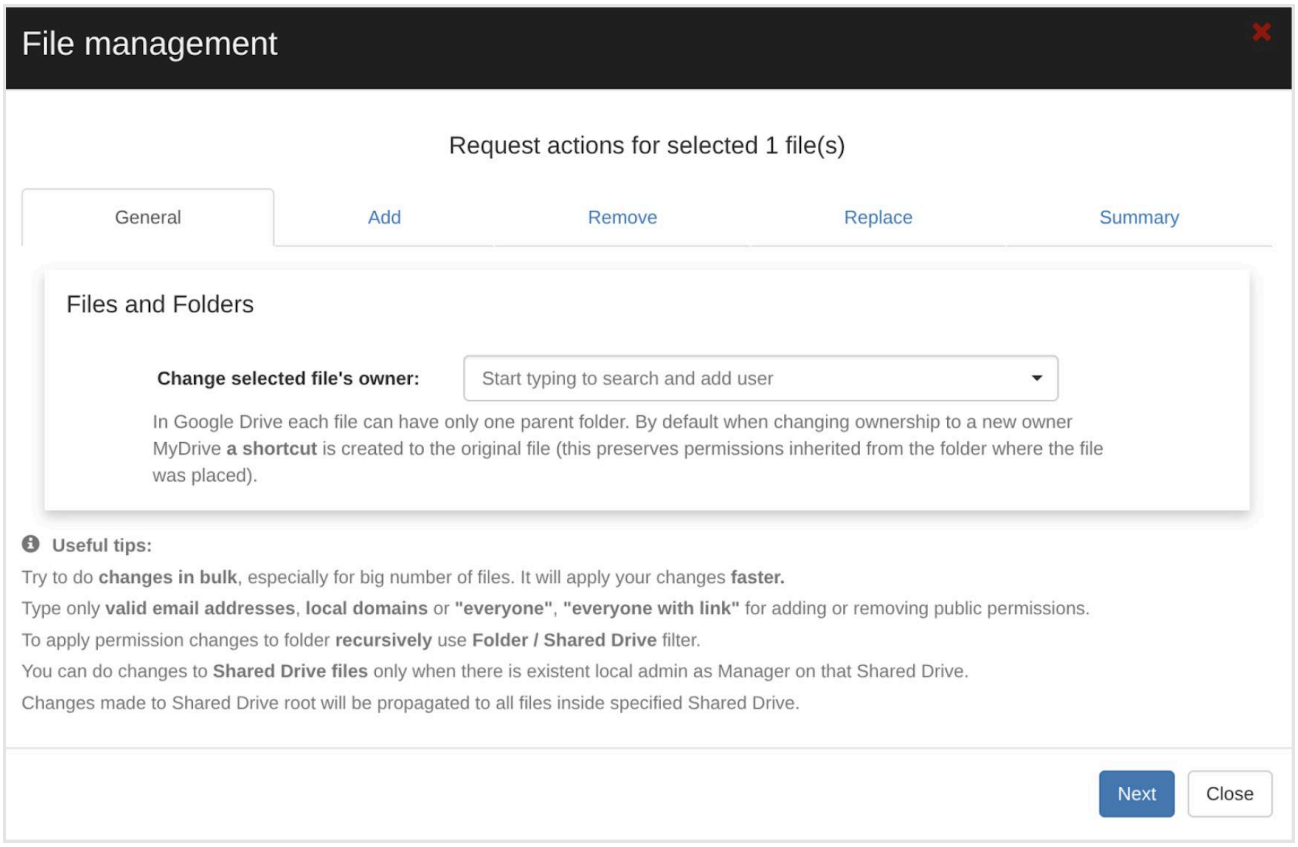


Training Resources: Drive File Ownership

In the Drive Audit Dashboard you can view the files across your entire domain. This table will allow you to see all the files sharing permissions on all files touching the domain and apply filters to find exactly what you need.
How to find a user's files and transfer ownership:

Navigate: *GAT+ > Drive > Files*

- Click the 'Filter' icon - ▼ - near the right hand side of the page
- Use the filter menu to search for all files owned by a specific user
- From the results, you can select individual files from the check box on the left
- Use the 'File operations' icon - 🗎 - and select the 'File management' option
- In the menu that appears choose who the new owner should be
- Click Next until you see the Send Request option, and click that too.
- The request will be sent to the security officer for approval
- Once approved by the another security officer, the job will run and the ownership change will be made
- **Don't worry, this process works even when the user is suspended.** GAT handles the ownership transfer in the backend regardless of the user's status.



2. Remove Access for the Previous Owner After Ownership Change

By default, when you transfer ownership of a file, the original owner's role is automatically downgraded to an editor. However, you can manually adjust their permissions and completely remove their access to the file.

Navigate: *GAT+ > Drive > Files*

- Locate the file you are wish to change permissions on, using the filter icon - ⏷
- View the file's permissions by clicking the eye icon beside the file - 👁
- From the permission list, locate the previous owner (they should be found in the 'Contributors' section), and click the down arrow by their email address
- Use the '***Remove permission for only this file***' option to remove the users access

Related Articles:

- Change ownership of Google Drive Folder and its content
- How to Transfer Ownership of Google Drive Files
- Transfer Files Ownership of a Suspended User
- Transfer Ownership of My Drive Folder with GAT Flow
- Identify Externally Owned Files Shared into the Domain with GAT+
- Transfer Drive Files and Folders to a Shared Drive

Section 2: Drive Access Control & Compliance

Controlling who can access, edit, and share your company's data is fundamental to a strong security posture. Unauthorized sharing, especially with external parties, can lead to data breaches and compliance violations. By implementing strict access controls and continuous auditing, you can protect sensitive information, meet regulatory requirements, and maintain the integrity of your data.

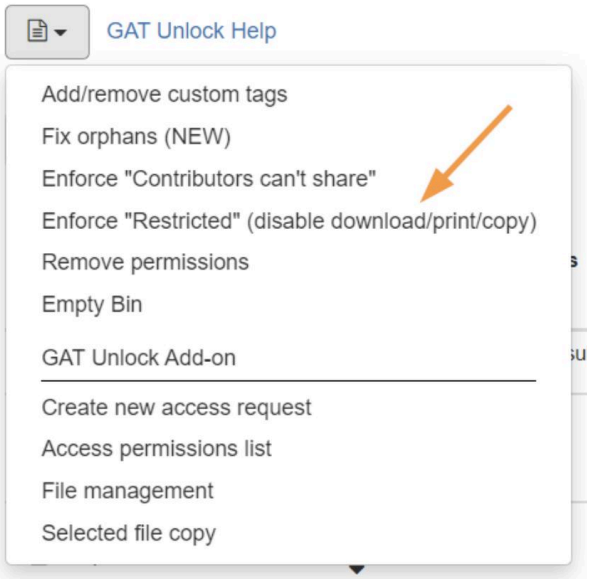
Moving beyond simple one-time audits is key to maintaining a secure and compliant Google Workspace. Advanced reporting allows you to create highly specific and scheduled reports that surface high-risk data without constant manual effort. Automation takes this a step further by allowing you to take immediate action on your findings, ensuring that security policies are enforced automatically.

1. Enforce extra restrictions on files for permission holders

Prevent users from downloading, copying, or printing files. This is a critical security measure to protect sensitive documents from being exfiltrated. GAT provides two specific actions for this: ***"Enforce (contributors can't share)"*** and ***"Enforce 'Restricted' (disable download/print/copy).***

Navigate: *GAT+ > Drive > Files*

- Locate the file, using the filter icon - ▼
- Click on the checkbox beside the file's title to select it, select multiple file if desired
- Click on the File operations menu icon - 🗎
- Select *'Enforce "Restricted" (disable download/print/copy)'*, which prevents viewers and commenters only from downloading, printing, or copying the file.
- Select *"Contributors can't share"*, so the file cannot be re-shared by the contributors with access



2. Remove Public or Link-Sharing

Easily find and remove files that are shared publicly with a link, or are published on the web which can be a major source of data leakage.

Navigate: *GAT+ > Drive > Files*

- From the file sharing dashboard on the top left, click on the ***"Open to Public"*** or ***"Open to public with link"*** categories.
- This will automatically filter your file list to show all the files with these permissions.
- Select the dropdown arrow beside any one of the Everyone (with link) tags and chose 'Remove permission for only this file' to remove the permission from a single file
- Or choose 'Remove everyone (with link) as Contributor and Viewer from files in current filter' to remove the permission from every file in the domain at once.

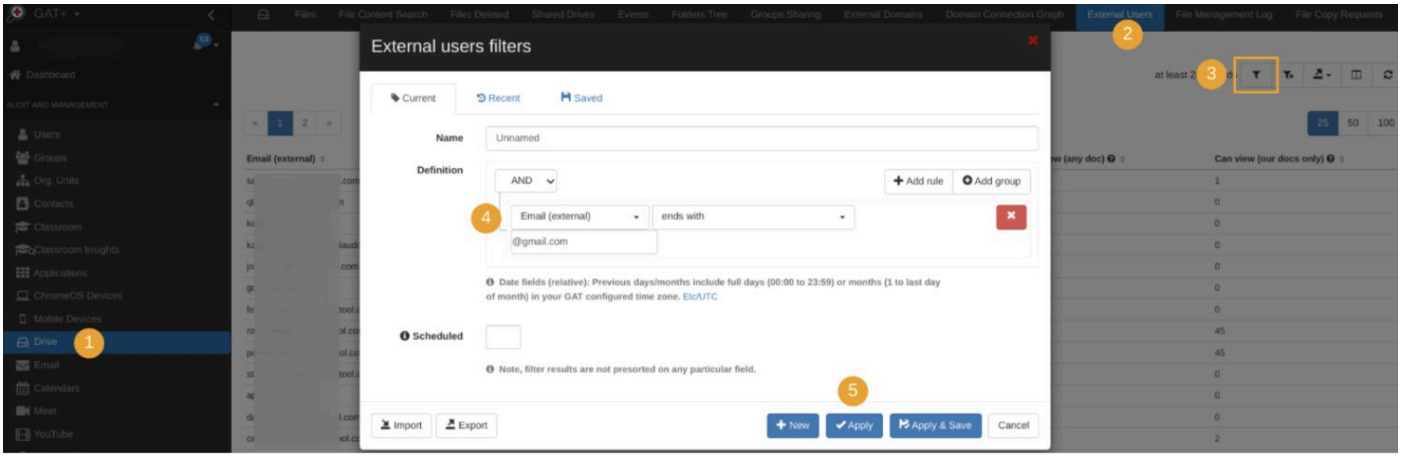
3. Audit and Restrict External File Access

Get a clear view of all files shared outside your domain and remove access to ensure data is not exposed to unauthorized parties.

Navigate: *GAT+ > Drive > External users*

- This shows all the accounts that are not from your domain, that either have access to, or own a file that is touching your domain
- This could be somebody's personal account, or an account from another organization
- You can click the column titles to sort in ascending order, to see the accounts that own, have viewer access, or have contributor access to the most files.
- Choose one of the numbers on screen to see all details on the files
- Use the ***"Remove Shares"*** or ***"Change Permissions"*** option to restrict access.

Alternatively, you could use the filter icon in the External users section, to filter for all the accounts that end in gmail.com or outlook.com.
This can surface the personal accounts with access to a lot of files, or bring to light users that are creating files for work purposes with their personal accounts, and sharing them into the domain (and retaining the files once they leave).



4. Creating and Scheduling Custom Reports

Automate your compliance and security monitoring by setting up scheduled reports, and even removing the file access. This helps you consistently audit for sharing policy violations, data loss prevention (DLP) alerts, and other high-risk activities.

Navigate: *GAT+ > Drive > Files*

How to set up a scheduled report:

- From whatever file filter you had set in the previous step.
- Instead of clicking 'Apply,' click the 'Scheduled' checkbox.
- Name your report, configure the frequency (daily, weekly, monthly) and choose the recipients that should receive the report.
- The report will automatically be generated and delivered to the specified recipients, and should provide you with continuous oversight without further manual work.

Tip: Set a time factor in your filter eg. ***'Shared out (relative)' 'in the last x days'*** - this way you will get different results in your report each day / week / month, and will not have to read data from the previous report.

5. Automated Remediation

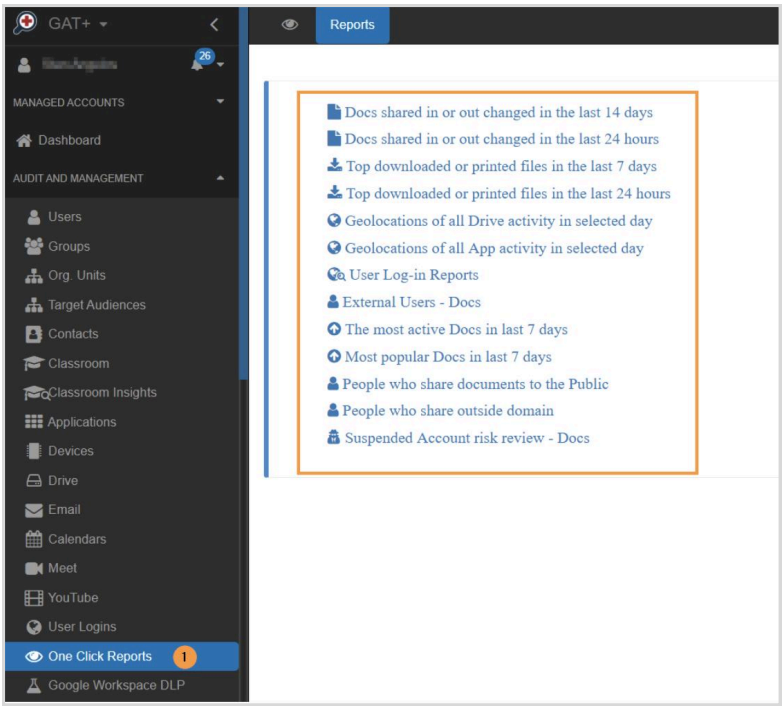
You can then automate the removal of permissions from files that your scheduled report contains. This ensures that any publicly shared files are automatically secured without manual intervention.

Navigate: *GAT+ > Scheduled report section*

How to automate the removal of shares:

1. In the Scheduled report section, find the report you created and click the icon beside it
2. Under "Actions," select External and choose Remove only the following External Shared.
3. Enter "everyone with link" and "everyone" to target these specific shares or enter *@gmail.com to remove shares to those personal accounts
4. Select the Enabled checkbox and click the Save Settings button to finish. The shares will be automatically removed according to your schedule.

Tip: Navigate to the One Click Reports section for some more inspiration on other reports you might schedule.



6. Secure Entire Folders with Access Controls

Apply uniform access controls across an entire folder and its sub-folders to ensure consistent security policies.

Navigate: *GAT+ > Drive > Files*

- Locate the folder you are wish to change permissions on, using the filter icon - ⏷
- Find the folder you want to secure, and in the Title column, click the dropdown arrow beside the folder's title
- Choose the option 'Apply permission change to this folder (recursive)' to open up the 'File management' menu
- Any changes you apply will propagate to the contents of this folder its subfolders

7. Control Chrome Access Based on Location

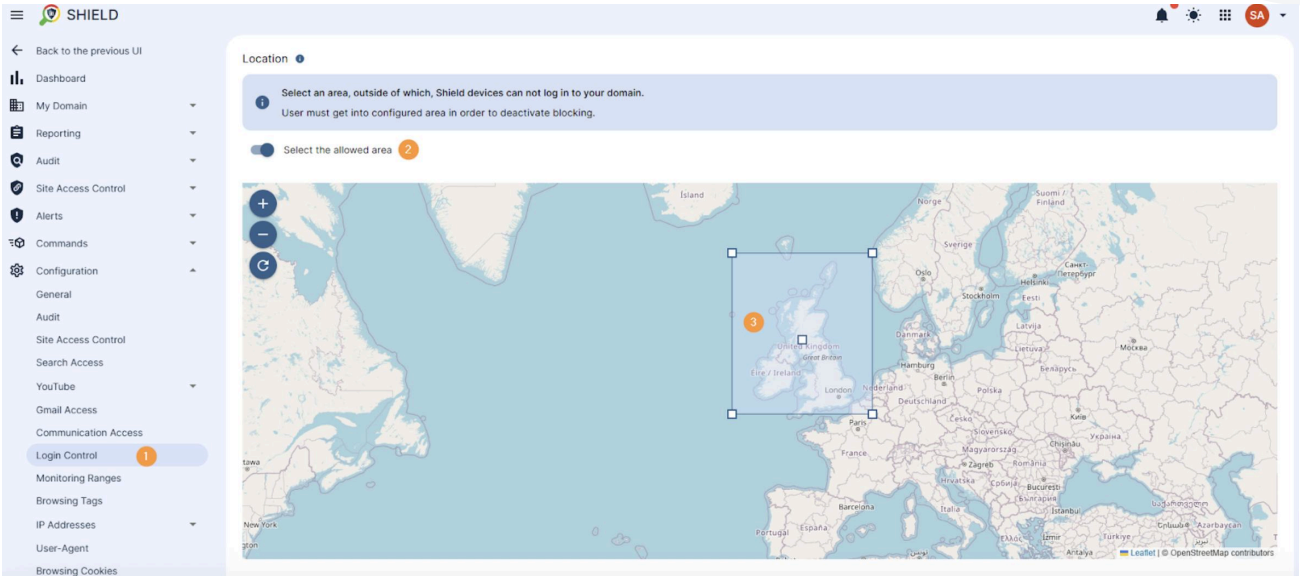
You can set up location-based security policies for Chrome access. GAT Shield allows you to create policies that will alert administrators about, or block a user's login, based on their location.

Navigate: *GAT Shield > Alerts > Rules*

- **For alerts:** Define trusted locations and create a location alert rule that sends an alert to administrators and a notification to the user when a Chromebook is used from an untrusted location.

Navigate: *GAT Shield > Configuration > Login Control*

- **For blocking logins:** Use the ***"Login Control"*** feature to actively prevent users from logging into a chrome profile with their domain account from an unauthorized location.



Related Articles:

- Create Scheduled Reports in Drive Audit
- Daily Removal of Drive Files Set as Public with Link via a Scheduled Report
- Scheduled Report to Replace Public with Public with Link Permissions in Google Drive
- Daily Removal of Drive Files Set as Public with Link via a Scheduled Report
- One-Click Reports
- GAT Shield Login Control
- Find Publicly Shared Google Drive Files
- Remove Public and Public with Link Permissions from Google Drive Files
- How to Find All Files Shared to a Specific External User and Remove Their Access
- Location-Based Alerts and Access Control for Chromebooks

Section 3: Compliance Reporting

Why is Compliance Reporting Important?

Proactive compliance reporting and auditing are essential for a healthy and secure Google Workspace environment. They allow you to identify and address security risks, ensure adherence to company policies, and easily produce the necessary reports for internal and external audits. By automating these processes, you can maintain continuous oversight without manual effort, saving time and reducing the potential for human error.

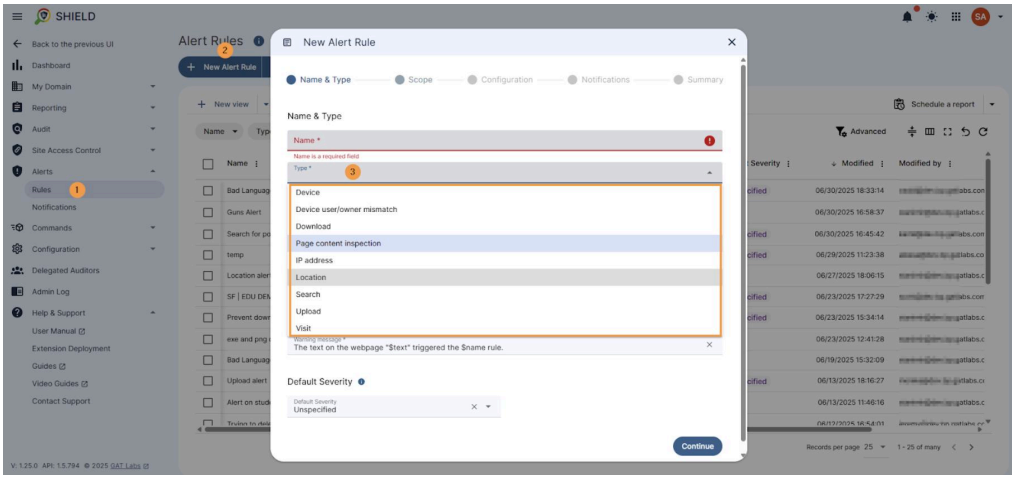
1. Set Up Data Loss Prevention (DLP) Alerts

Set up real-time alerts to detect, respond and even remind your end users in advance of potential data leaks. GAT Shield allows you to monitor for specific details in specific scenarios, like Personally Identifiable Information on an email being composed, or block a download if it's on a specific site, or if the file is of a certain type.

Navigate: *GAT Shield > Alerts > Rules*

How to set up a DLP alert:

- On the Rules page, click the pill shaped button labeled *'+ New Alert Rule'* to begin, or click the drop down arrow on the + New Alert Rule button to choose from one of our templates.
- The alert rule creation wizard will guide you through the configuration, you can choose who the alert should run on, or if it should be excluded from triggering on certain websites, and even what the alert will look like from the end user perspective.



Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

GAT labs