GAT LABS TRAINING RESOURCES

# DLP + Alerts Across Google Workspace

GAT labs

Training Resources

# DLP and Alerts Across Google Workspace

Learn how to proactively prevent data breaches, control sensitive data exposure, and receive alerts for critical activities using GAT+.

## Understanding DLP in GAT+

Data Loss Prevention (DLP) helps monitor and control sensitive data movement across Google Workspace to prevent accidental or intentional leaks.

### Key DLP Features in GAT+:

- Sensitive Content Search ( SSNs, financial data, keywords,etc)
- File Exposure Controls
- Automated Remediation Actions

### Types of Alerts in GAT+:

- Applications
- Emails
- Drive
- YouTube
- Mobile device
- Users
- Users Logins

**Related Articles:** Better reporting for Google Workspace DLP

# 1. Drive DLP Rules: Top 3 Actions You Can Take

Take immediate control over file sharing activities and prevent sensitive information from leaving your domain with these top DLP actions.

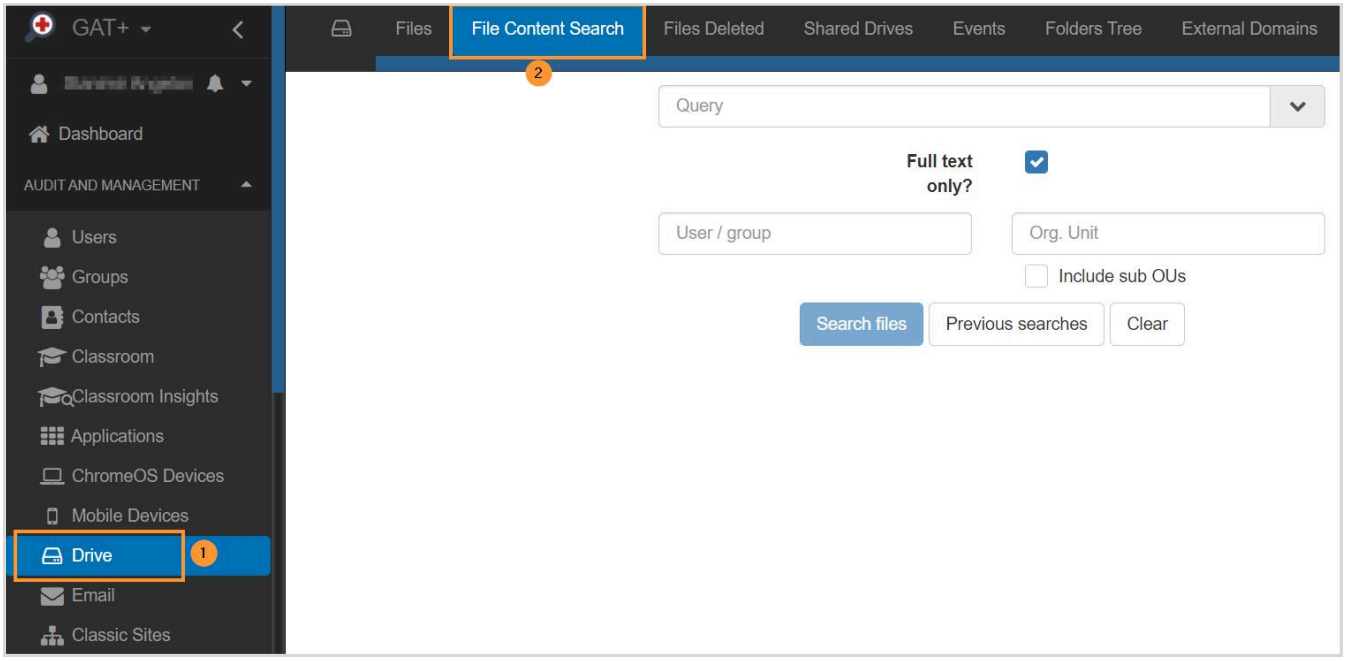
## 1.1. Identify and Remove External Sharing for Sensitive Files

GAT+ helps you detect and take corrective action on files that have been shared externally.

**Navigate:** *GAT+ > Drive > File Content Search*

**Steps:**

- Enter specific sensitive keywords or patterns (e.g., "SSN", "Confidential").
- Use advanced syntax for precise filtering.
- Select users, groups, or OUs to apply the search.
- Review results and take immediate action by adjusting sharing permissions.




**Related Articles:** Search for Sensitive Content in Files

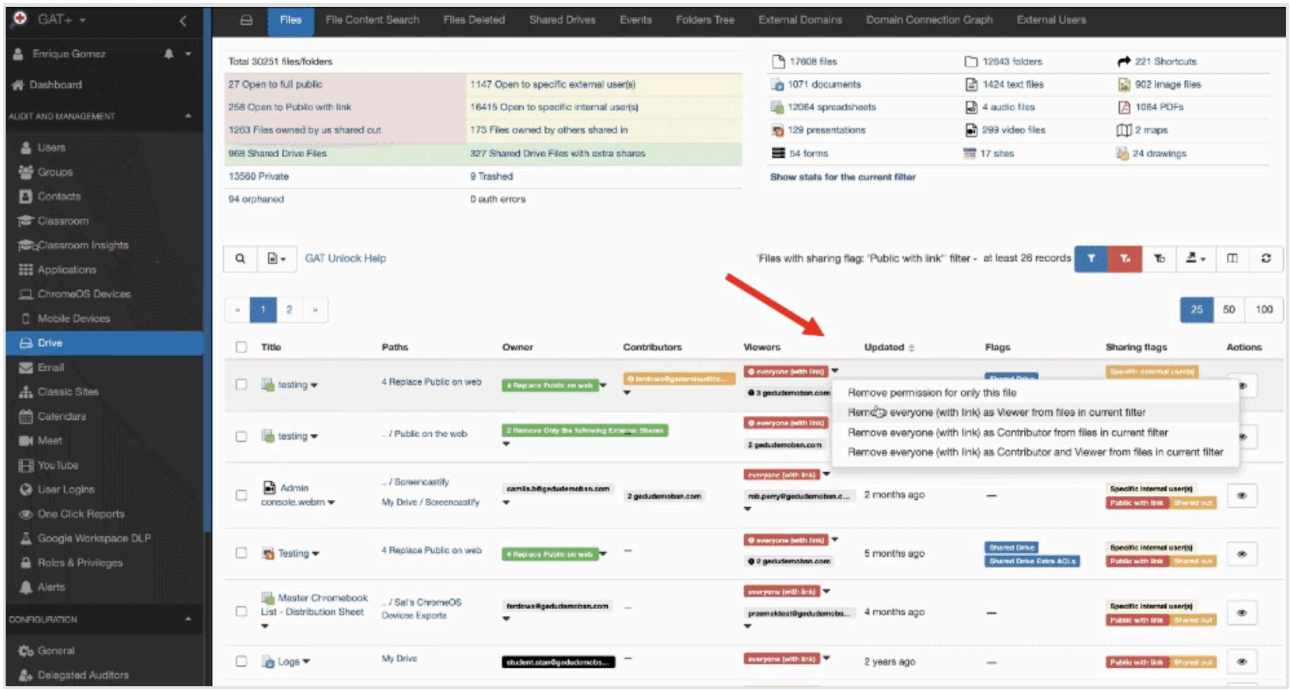
## 1.2. Auto-Remove Public Sharing Permissions

You may find that users from your domain have shared Google files publicly. Use this method to quickly restrict those files

**Navigate:** *GAT+ > Drive > Audit table > Select Full Public (everyone) or Public with link (everyone with link)*

**Steps:**

- Apply a filter where the Sharing Flag contains Public or Public with link.
- **Add an extra filter:** Sharing Flag does not contain Shared In to exclude files shared into your domain from external domains.
- Review the results and take corrective actions.




**Related Articles:** Find Publicly Shared Google Drive Files

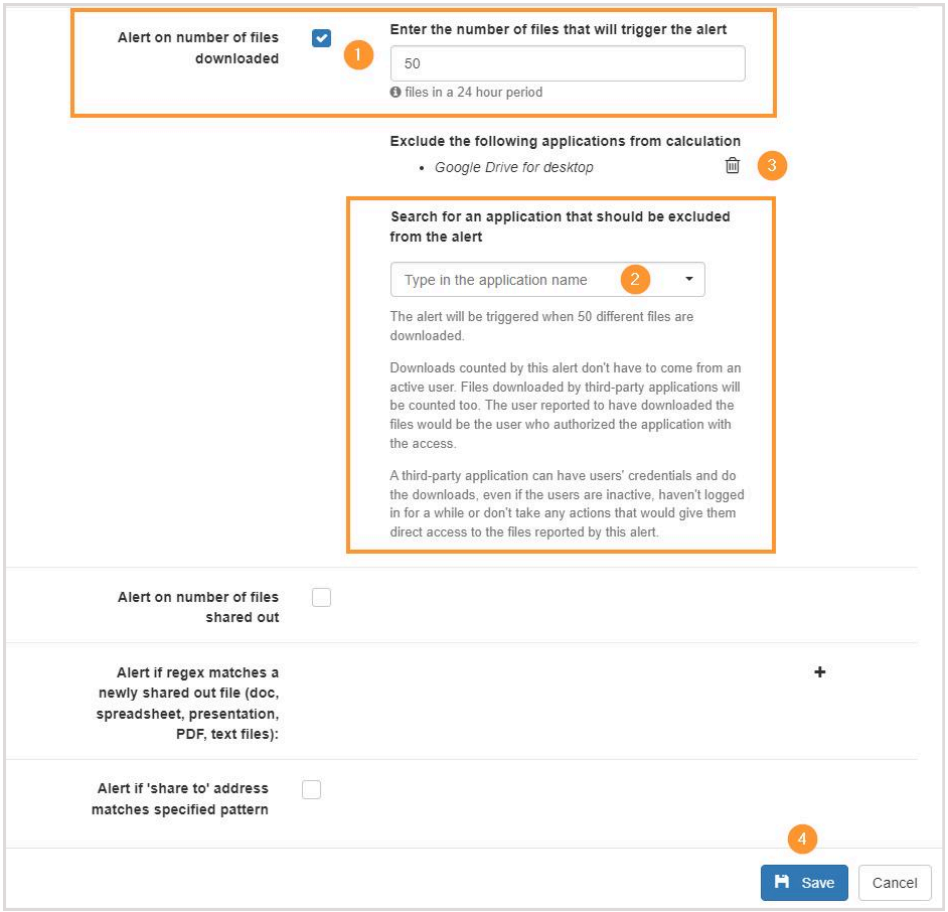
## 1.3. Enforce Download Limits to Prevent Data Exfiltration

Receive alerts when a user downloads more than X files in a short timeframe.

**Navigate:** *GAT+ > Configuration > Alert Rules*

**Steps:**

- Click on the + sign, and a new window will be displayed. Fill in the details.
- **Alert recipients:** Enter recipient emails who will receive an email for the alert (optional) By default, all alerts will be shown in *GAT+ > Alerts*
- Select *"Alert on a number of files downloaded."*
- Set the threshold to trigger the alert.




**Related Articles:** Set Up a Google Drive DLP Alert When the Number of Downloaded Files Exceeds X

# 2. Expanding DLP to Gmail and Mobile Devices

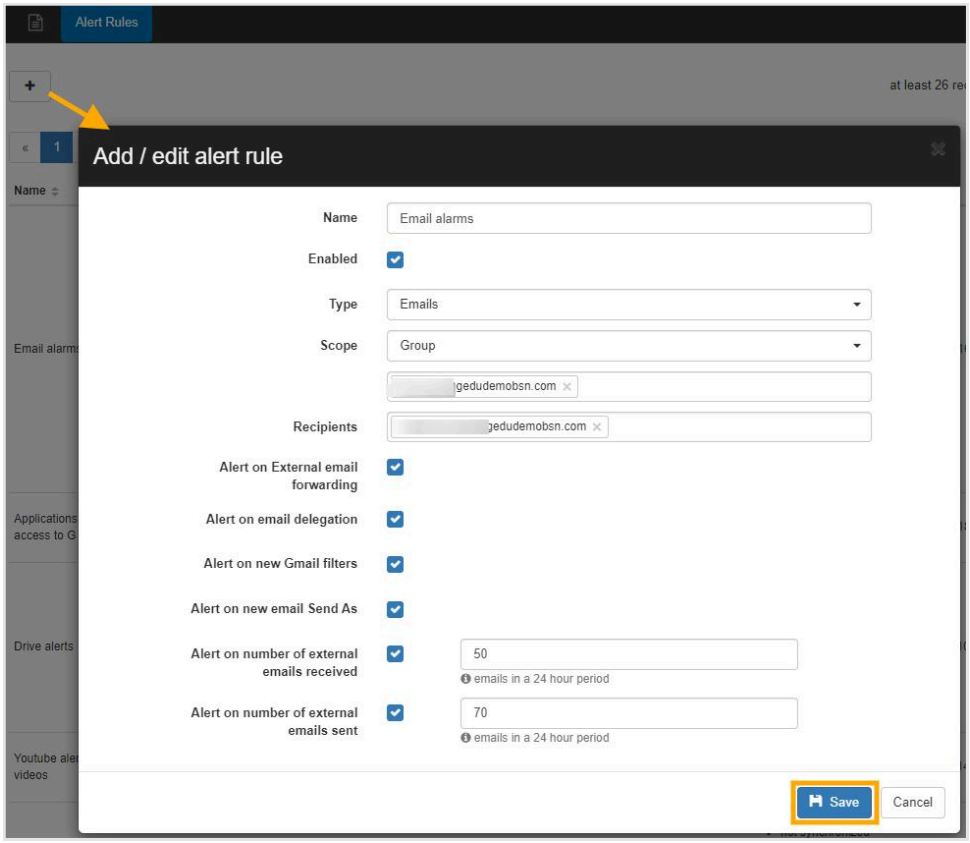
Take your DLP efforts beyond Drive to protect email and mobile environments.

**Navigate:** *GAT+ > Configuration > Alert Rules*

## 2.1. Gmail DLP Controls

**Choose any of the options available for the Email alert rules:**

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



**Related Articles:**

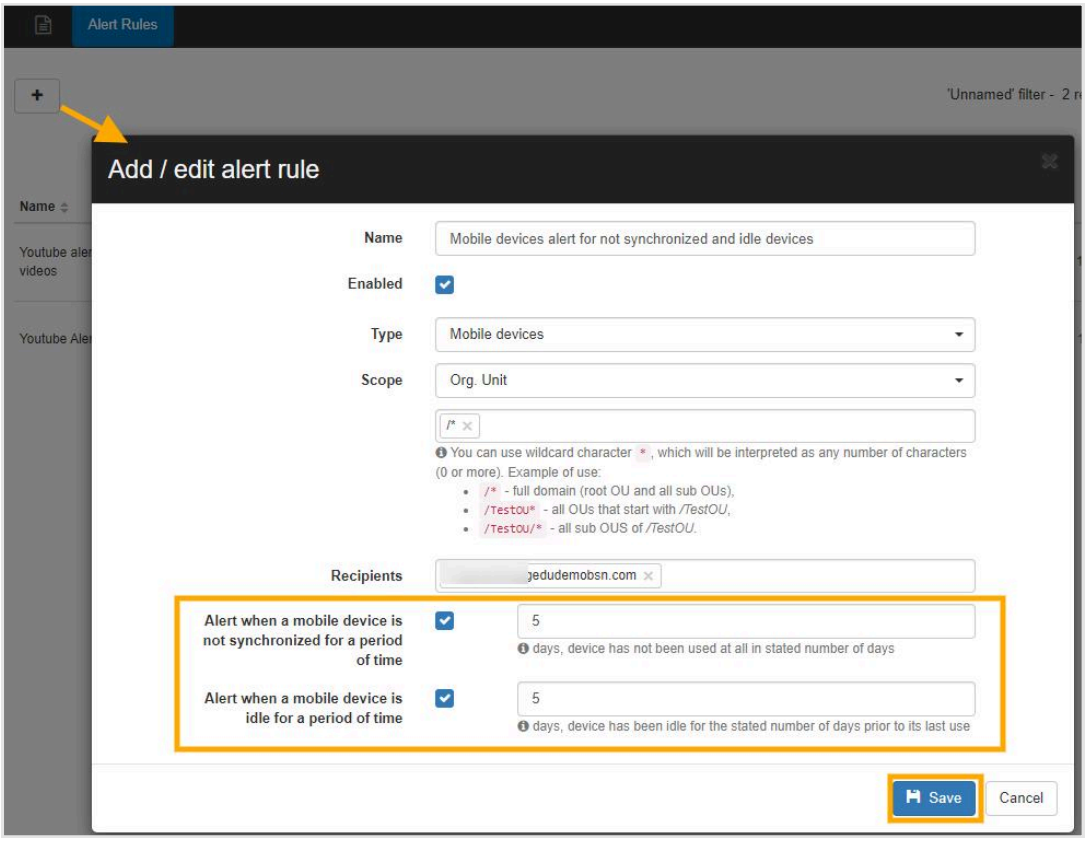
- Set Up a How to set up Gmail alerts for Google Workspace users
- Set up a Google Alert when a new filter is added in Gmail Drive DLP Alert When the Number of Downloaded Files Exceeds X

## 2.2. Mobile Device DLP Controls

Using the Alert Rule mechanism provided in GAT+, Super Admins or Delegated Auditors can alert on violations detected on corporate-enrolled mobile devices.

**Steps:**

- Set the Type to Mobile Device.
- Define the scope: User, Group, or Org. Unit.
- Select alert recipients to receive notifications.




**Related Articles:** Alert on Non-Synchronizing and Idle Mobile Devices

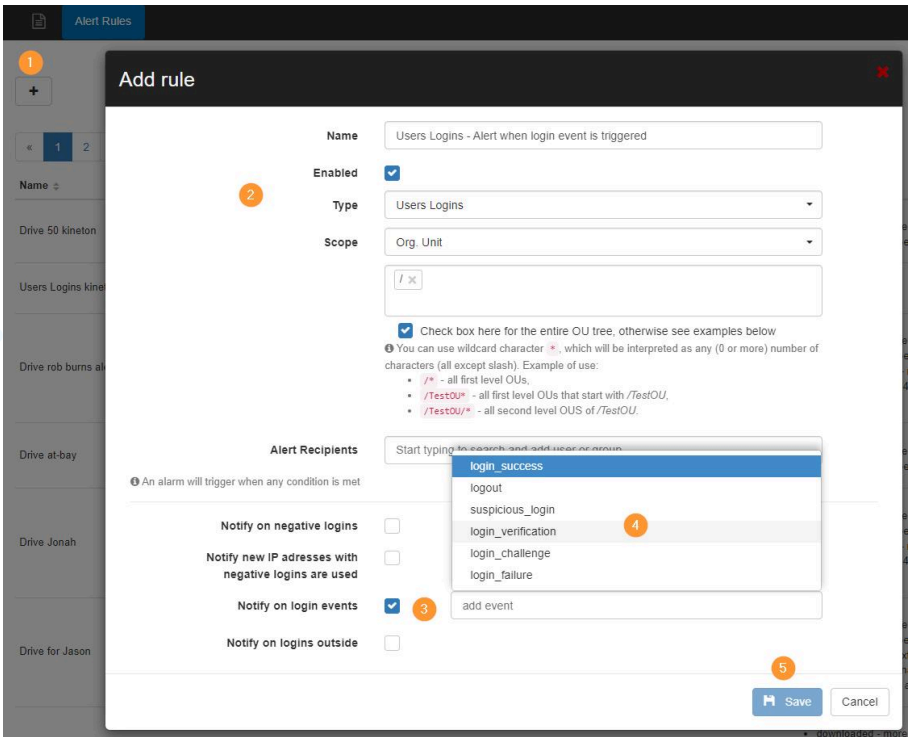
# 3. Setting Up User Login Alerts

Proactively monitor suspicious login activities to prevent unauthorised access and potential data leaks.

**Navigate:** *GAT+ > Configuration > Alert Rules*

**Steps:**

- Click the '+' icon to create a new alert.
- Enter a rule name and enable the rule.
- Set the Alert Type to Users.
- **Define the scope:** Individual user, group, or organizational unit.
- Add recipients to receive real-time notifications.
- Select the login events you want to monitor:
  - Login Success
  - Logout
  - Suspicious Login
  - Login Verification
  - Login Challenge
  - Login Failure
- Save the rule.

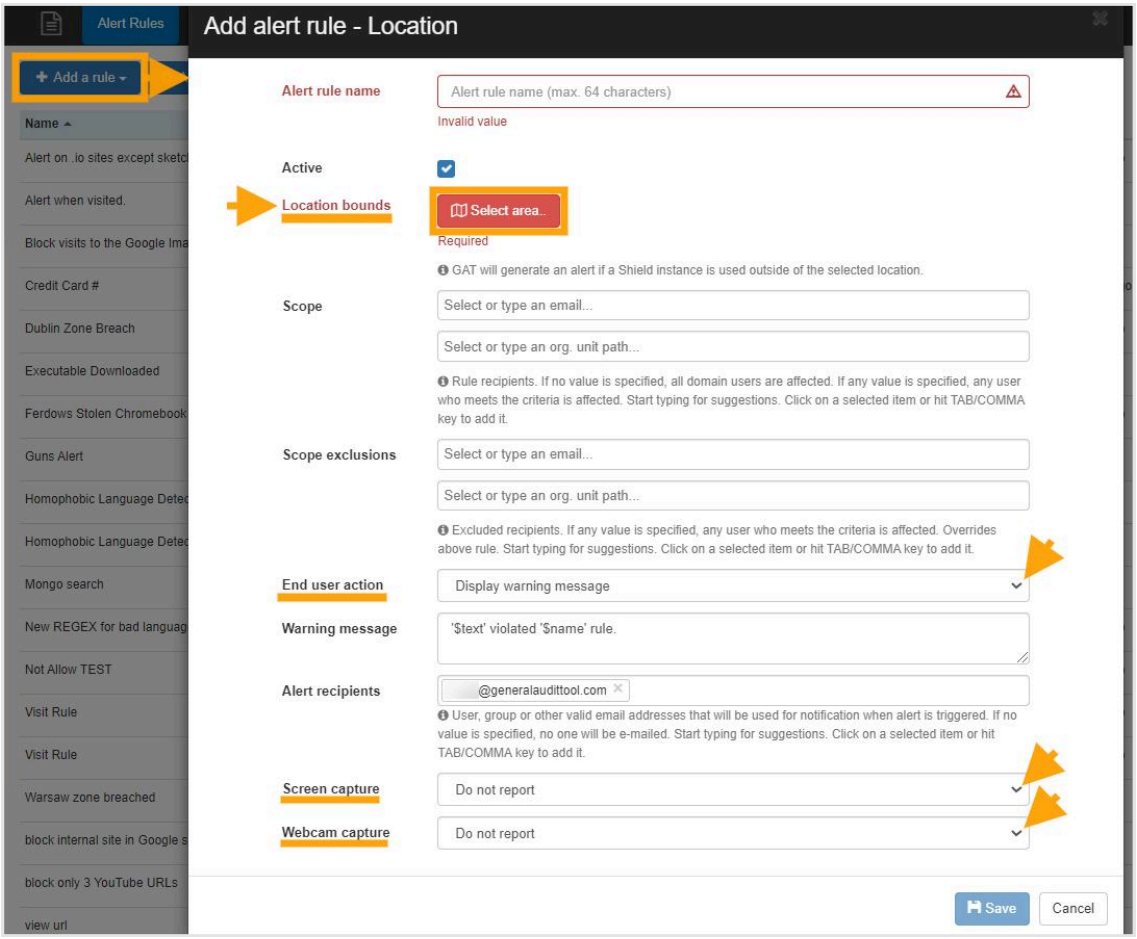



**Related Articles:** Setting Up User Login Alerts in GAT+

# 4. Location-Based Alerts and Access Control for Chromebooks

GAT Shield supports the use of Location maps to provide alerting and/or access control for Admins.

**Navigate:** *GAT+ > Configuration > Alert Rules*




**Tips:**

- If you don't want to alert end users outside the approved area, set the end-user action to No Action.
- You can enable webcam capture for security incidents.

**Related Articles:** Location-Based Alerts and Access Control for Chromebooks

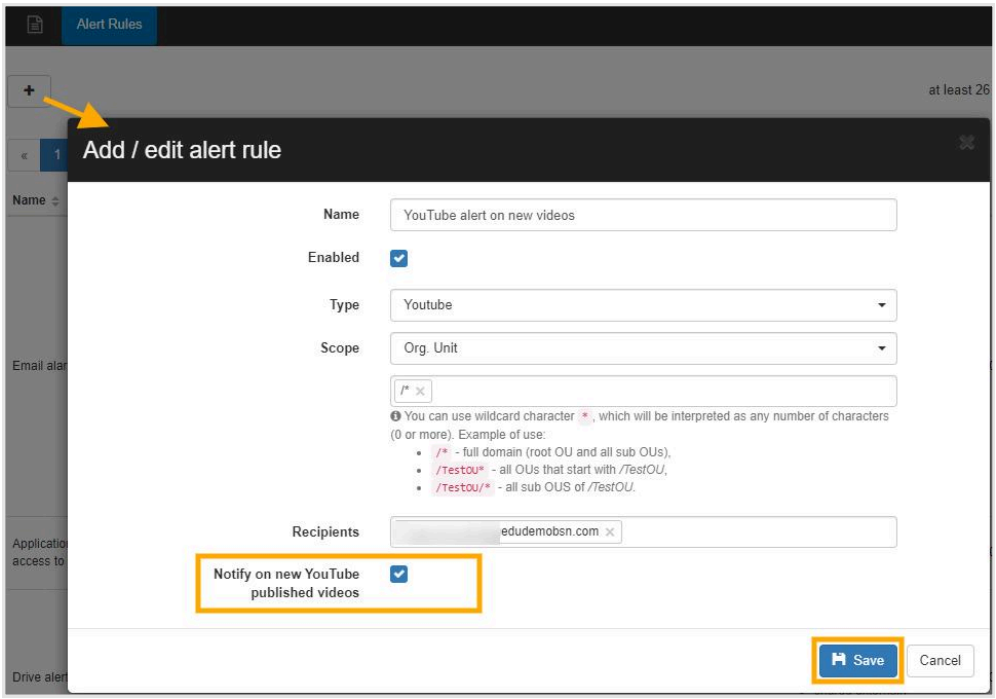
# 5. YouTube Content Monitoring Alerts

Prevent data exposure through public video content by monitoring when users publish videos to YouTube.

**Navigate:** *GAT+ > Configuration > Alert Rules*

**Steps:**

- Click the '+' icon to create a new alert.
- Enter a rule name and enable the rule.
- Set the Alert Type to YouTube.
- Define the scope: User, Group, or Organizational Unit.
- Select the recipients for real-time notifications.
- Enable the option Notify on new YouTube published videos.
- Save the rule.




**Use Cases:**

- Monitor users publishing potentially sensitive or unauthorized content.
- Audit brand reputation risks from public video posts.
- Ensure that corporate accounts are not used for personal content sharing.

**Tips:**

- You can also view and audit this activity in GAT Shield under the YouTube Audit section.

**Related Articles:** How to Set Up an Alert on New YouTube Published Videos

# DLP Best Practices for Google Admins

1. **Establish clear thresholds** for download and sharing alerts.
2. Combine **DLP scans with scheduled reports** for continuous monitoring.
3. Educate file owners to **remediate exposure risks directly.**
4. **Review and adjust DLP rules** quarterly based on emerging risks.
5. Leverage Shield for **endpoint-level controls** and download blocking.

# Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR

GAT labs