How to Report and Remove Files Downloaded by Google Workspace Users with GAT Shield

Chrome Audit & Management · https://gatlabs.com/knowledge/tech-tips/how-to-report-and-remove-files-downloaded-by-users/

How to Report and Remove Files Downloaded by Google Workspace Users with GAT Shield

The GAT Shield extension allows admins to **track and view user behavior** while logged into their Google domain account.

Google Workspace Admins can set up real-time alerts based on the behavior of the end-users.

These GAT Shield Alert Rules allow admins to stop and report unsafe downloads by users across their domain.

Report and remove downloaded files GAT Shield

Set up a download rule

Navigate to **GAT Shield → Alerts → Rules > +New Alert Rule**

Fill in the details for the download alert rule

1. Name & Type

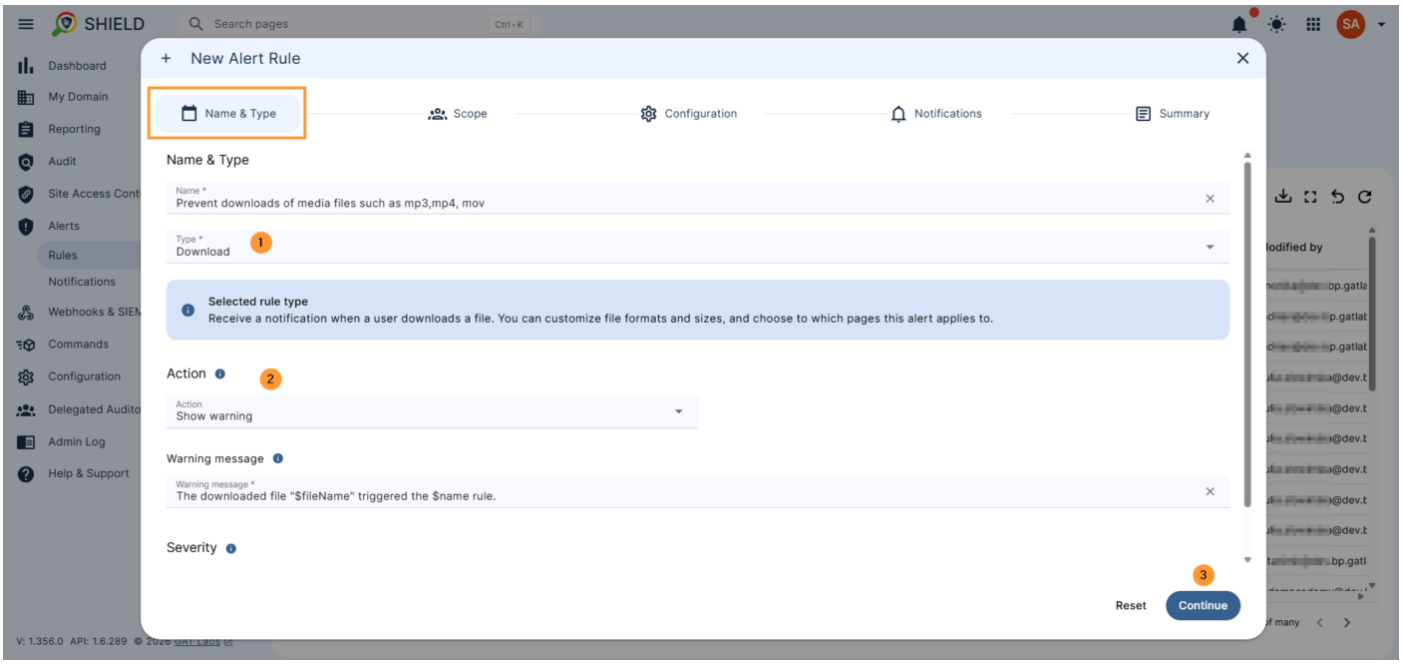
For each field, various options are displayed for selection.

- **Name**: Enter a descriptive name for the alert rule.
- **Type**: Select "**Download**" from the drop-down menu.
  - This option triggers a notification when a user downloads a file. You can customize the alert based on file formats, sizes, and specific web pages it applies to.

Action

When an alert rule is triggered, a pre-selected action will be executed on the user's device. Note that only tabs that trigger the rule will be affected if "Close" or "Redirect" actions are chosen.

- **Show a warning message**: Display a warning message to the end-user.
- **Close**: Close the Browse tab.
- **Close without warning**: Close the Browse tab directly, without any prior notification.
- **Redirect**: Redirect the user's browser tab. You must also enter a warning message to be displayed to the end-user.
- **Redirect without warning**: Redirect the user's Browse tab without displaying a warning message.
- **No action**: Select this option if no action should be performed on the end-user's device.
    - Default Severity
        - When an alert rule is triggered, a notification is generated. The severity of this notification indicates its level of importance. "Default Severity" is the value assigned to all notifications created by this specific rule.
            - Select **Low**, **Unspecified** (default), or **High** to set the notification's severity level.

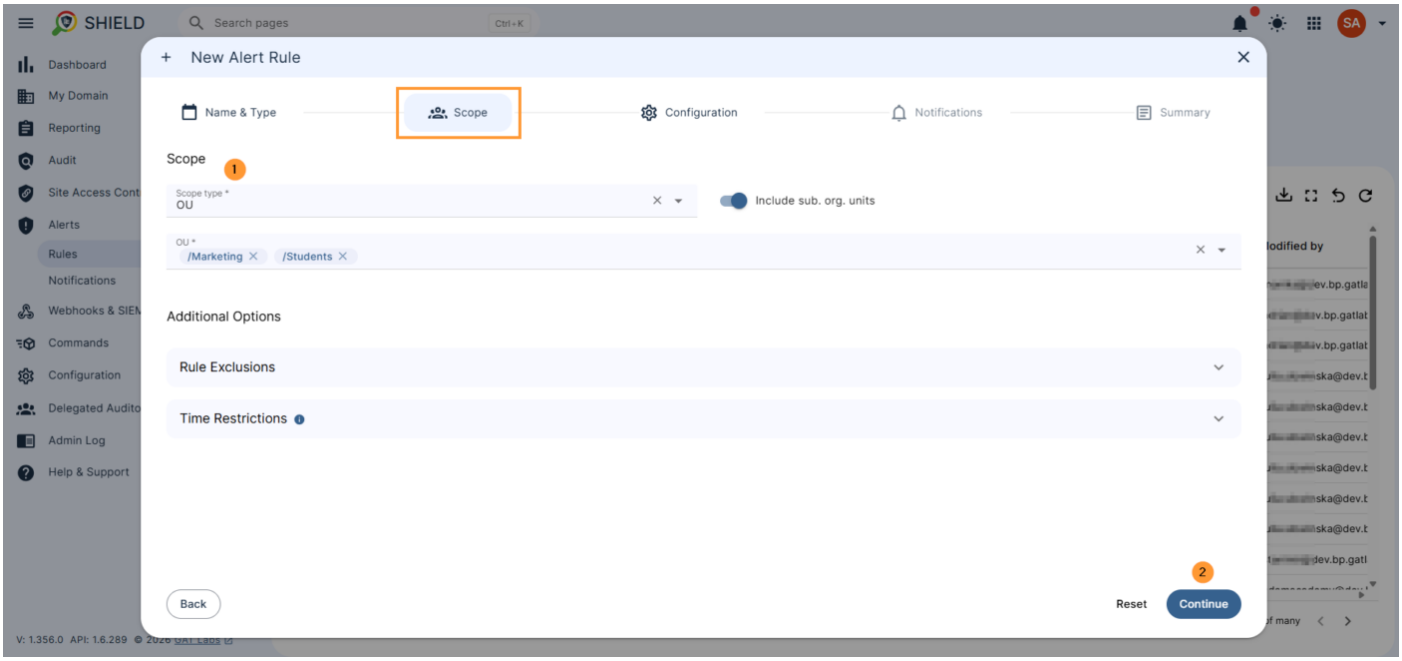


2. Scope of the New Alert Rule

In the Scope field, select all the users who will be affected by the alert rule

- **Scope** - add the users, group of users, or org. unit of users that will be affected by the rule

- **Rule exclusions**
  - Excluded Account - select a list of users to be excluded from the rule
  - Excluded OU - select an OU to be excluded from the rule
  - Excluded Websites - select a list of websites to be excluded from the rule
  - Active only on selected websites - select a list of websites that this rule will only run on
- **Time restriction** - select the times when the rules will be applied.
  - By default, when no time restriction is added, the rule will always be active. To change it, select days and time ranges when the rule will be active.
- **Continue** - click to continue to the next configuration

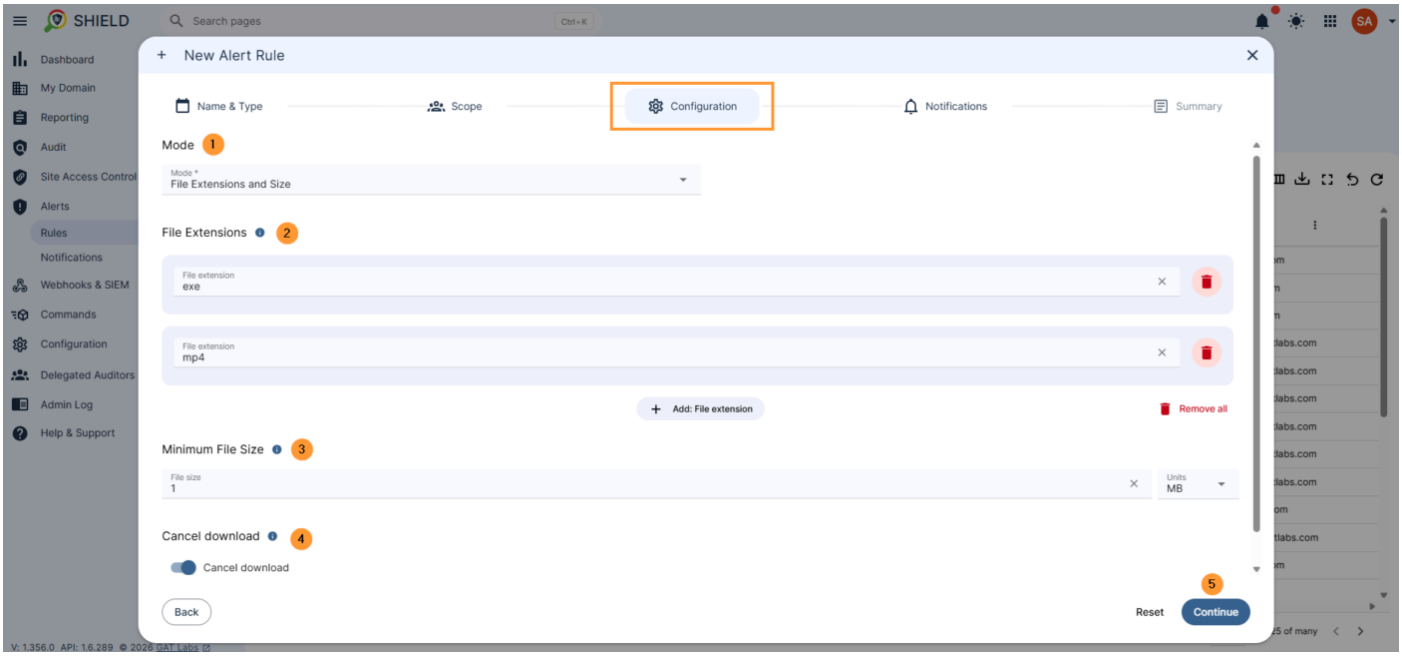


3. Configuration of the New Alert Rule

In the configuration, fill in the required information

- **Mode** - select what mode to be enabled.
  - **File Extensions**
  - **File Size**
  - **File Extensions and Size**
- **File extensions** - enter the file extensions for which the rule will be applied.
  - The alert rule will be triggered if the downloaded file has any of these extensions. If the minimum file size is set you can leave this list empty to trigger on any download.

- **Minimum File size** - Enter a minimum file size to trigger the alert.
- **Units** - Specify the file size unit you want to trigger the alert.
- **Cancel download** - Enabling this option cancels the download and removes local files
- **Continue** - click the button to continue



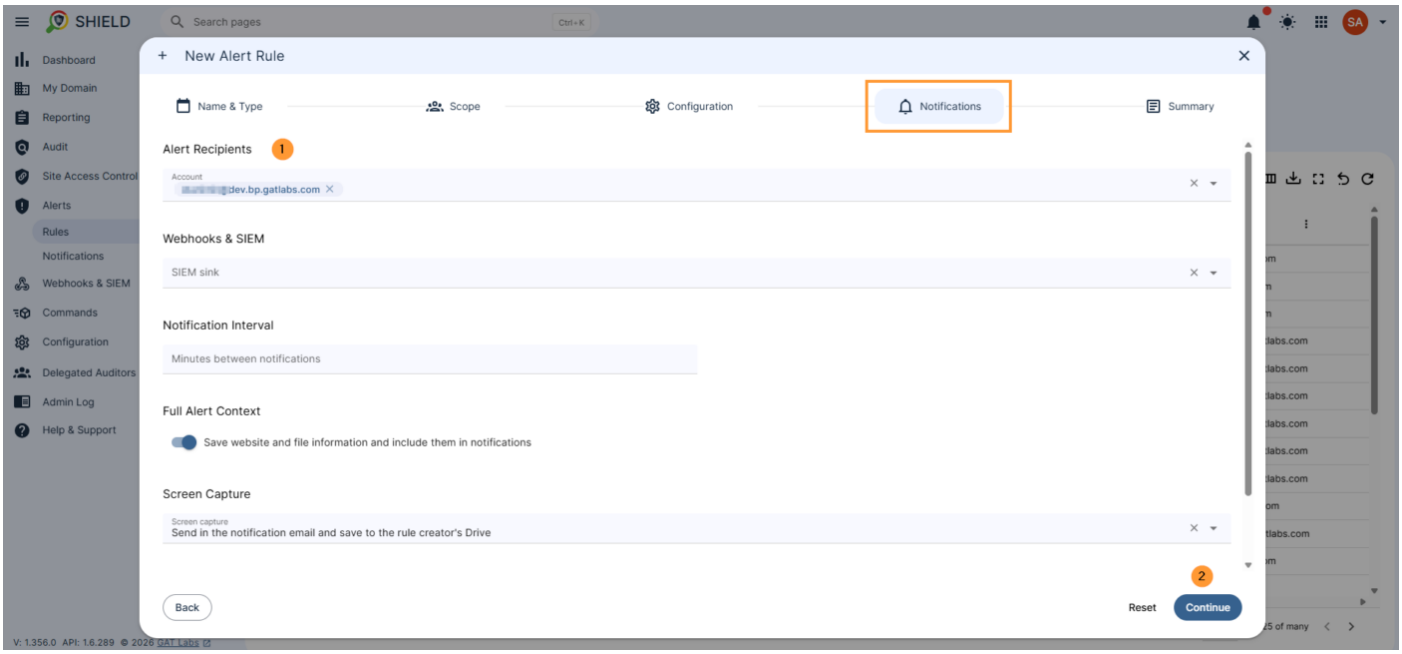
4. Notifications of the New Alert Rule

In the notifications,

- Recipients - Select the alert recipients
- Webhooks & SIEM - export alerts directly into a centralized external system such as Splunk, Elastic Search, or a Generic Webhook receiver
- Notification interval - select the time (in minutes) for which the alert notification will not be sent
- Full alert context by saving website and file information, and including them in the notifications
- Screen capture - select an option from the list
  - Do not send
  - Send in the notification email
  - Send in the notification email and save to the rule creator's Drive
  - Send in the notification email, save to the rule creator's Drive, and share it with other alert recipients
- Webcam capture - select an option from the list
  - Do not send

- Send in the notification email
- Send in the notification email and save to the rule creator's Drive
- Send in the notification email, save to the rule creator's Drive, and share it with other alert recipients

- **Continue** - click the button to continue



5. Summary of the New Alert Rule

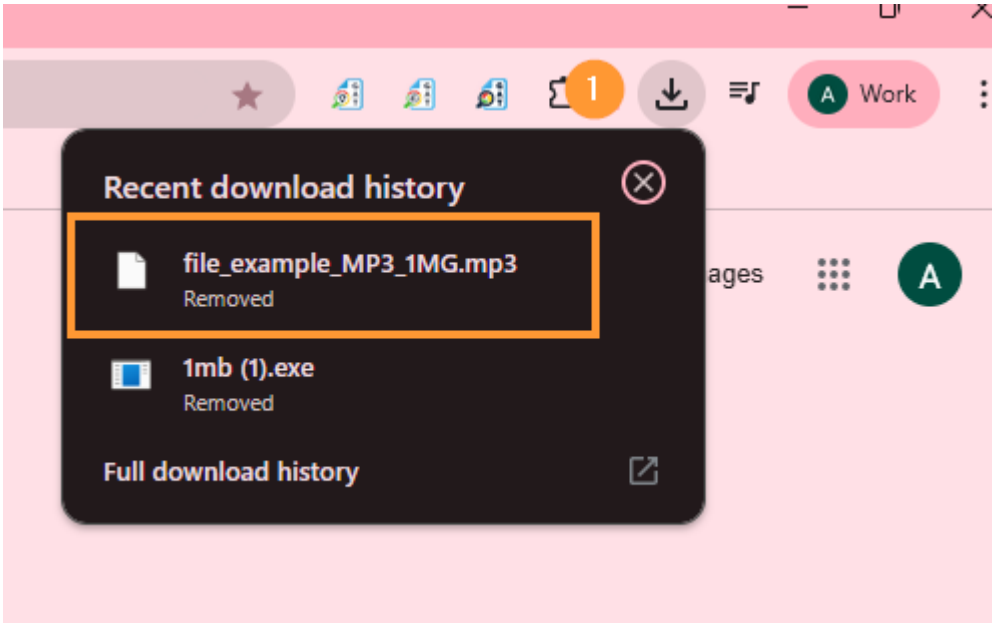
In the Summary, the Admin can view all the details for the rule that has been created

Click on the **Create** button to create the rule

Result for the end-user

The end-user where the rule is applied will receive a **notification** on their screen, depending on what "End-user" action is selected.

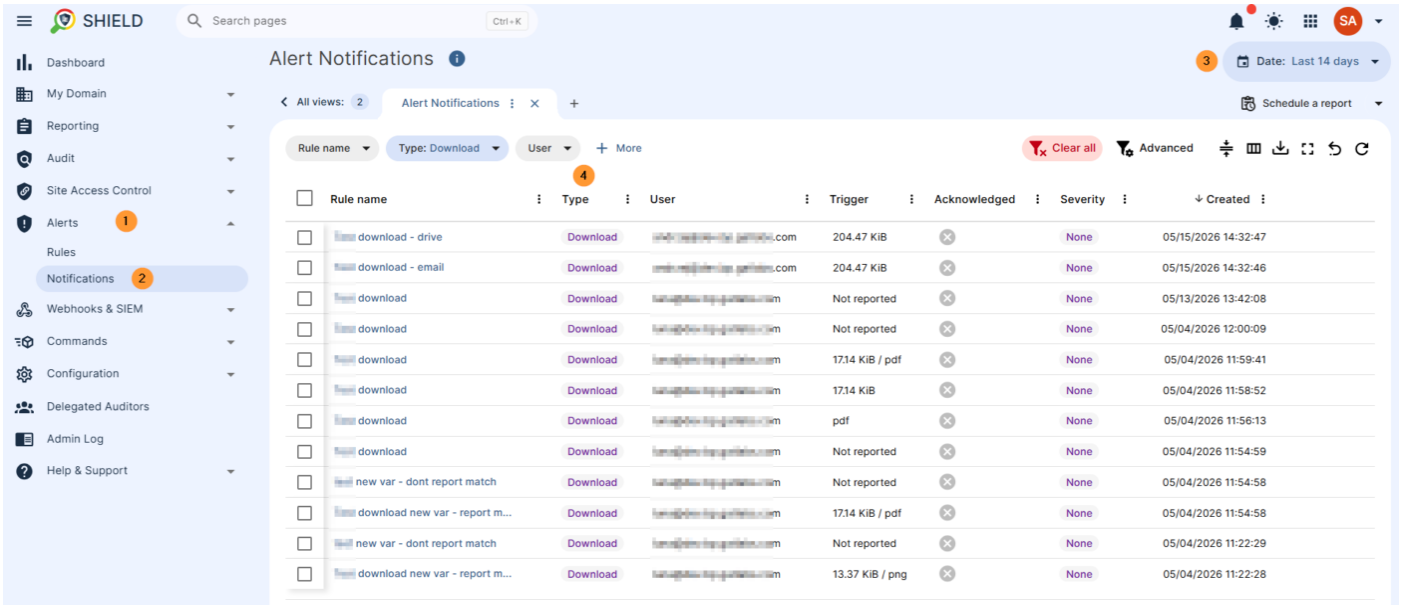
The download will **be removed, and** the user will see this message in the recent download history on their Chrome browser



Result for the Google Workspace Admin

All the results will be displayed in **GAT Shield > Alerts > Notifications**

Time frame, select the time frame (top right) for wich you want to see the notification for.



Frequently Asked Questions (FAQ)

Q1: Can I block specific file types from being downloaded without stopping all downloads?

A1: Yes**.** When configuring the **New Alert Rule**, you can set the mode to **"File extensions only"** or **"File extensions and Size."** By entering specific extensions (**e.g., `.exe`, `.zip`, or `.mp4`**), the rule will only trigger and cancel downloads for those specific file formats, leaving other downloads unaffected.

Q2: What happens to the file on the student's computer if a "**Cancel download**" rule is triggered?

A2: If the **"Cancel download"** option is enabled in the rule configuration, GAT Shield will actively terminate the download process and **remove the local file** from the user's device. The end user will see a "**Removed**" status in their **Chrome download history**, and depending on settings, they may also receive a warning message or have their tab closed/redirected.

How-to video:

Embedded media:
https://www.youtube.com/embed/1M8xNTbONZ8?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_