Block websites visit with Alert rules

Users Audit & Management · https://gatlabs.com/knowledge/tech-tips/block-websites-visit-with-alert-rules/

Block website visits with Alert rules

GAT Shield offers two primary features for managing web access and data loss prevention:

Site Access Control

This feature allows administrators to **block users from visiting specified websites**. It's a direct web filtering mechanism to control what pages end-users can access.

Alert Rules

Acting as a real-time Data Loss Prevention (DLP) solution, **Alert Rules enable administrators to configure alerts based on end-user browsing activity**. These alerts are triggered instantly when a predefined Browse pattern or site visit occurs, providing immediate notification of potential policy violations.

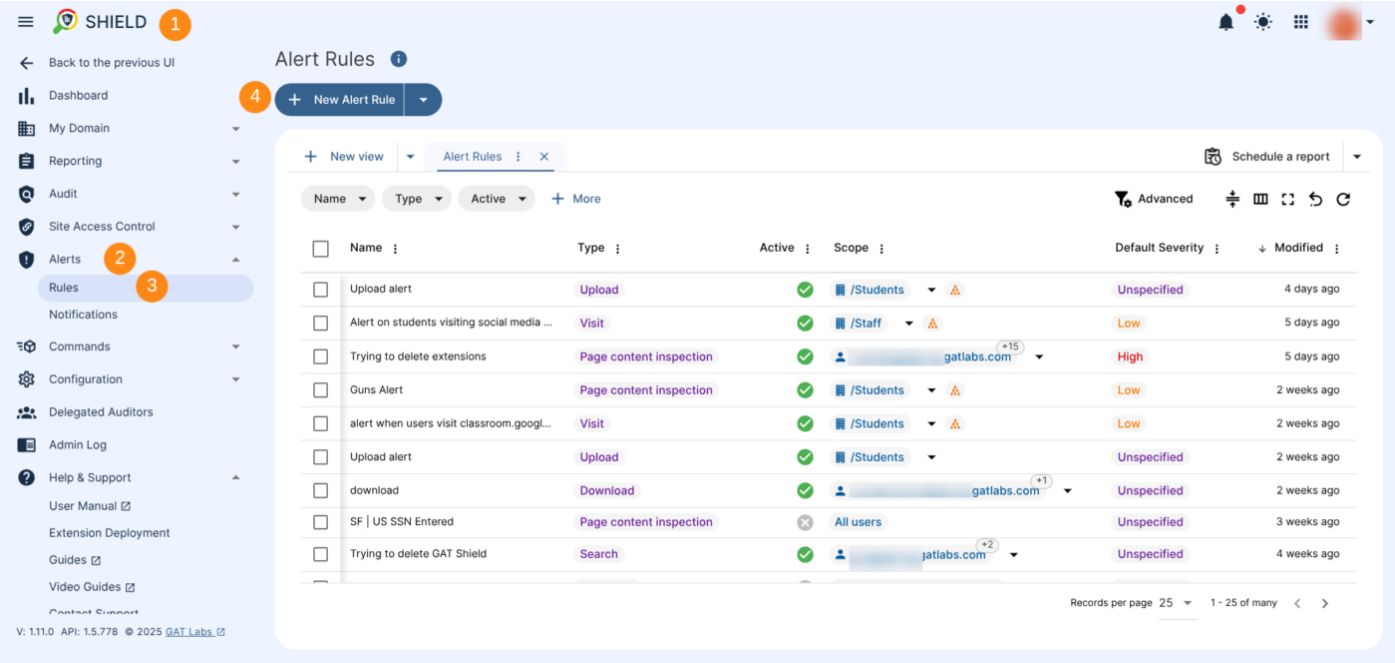
- Device
- Device user/owner mismatch
- Download
- Page content inspection
- IP Adress
- Location
- Search
- Upload
- Visit

"Visit" Alert rule

The "Visit" Alert Rule is a specialized alert type designed to **notify administrators when users access specific websites**.

This rule complements Site Access Control by offering an **alerting mechanism for web page visits**. While Site Access Control blocks access, the "Visit" Alert Rule provides real-time notifications when a user *attempts to visit* or *successfully visits* a designated webpage.

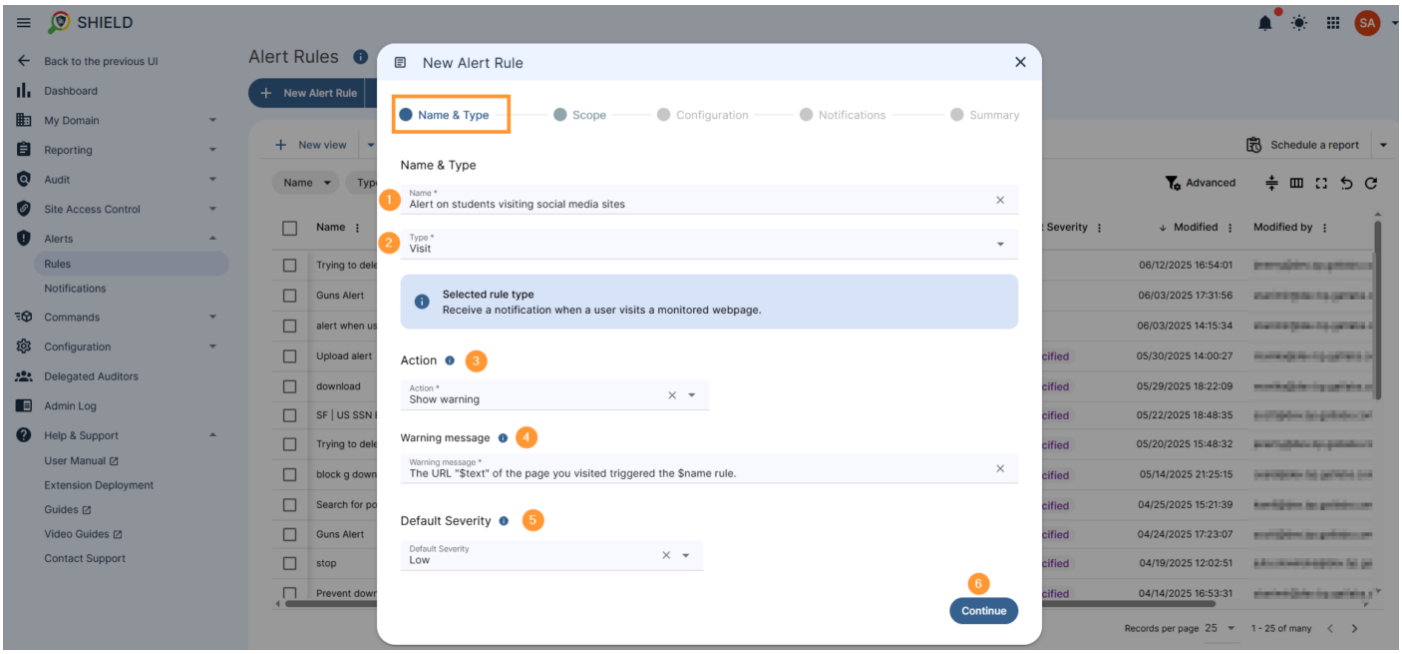
Configuration Path: GAT Shield > Alerts > Rules > + New Alert Rule



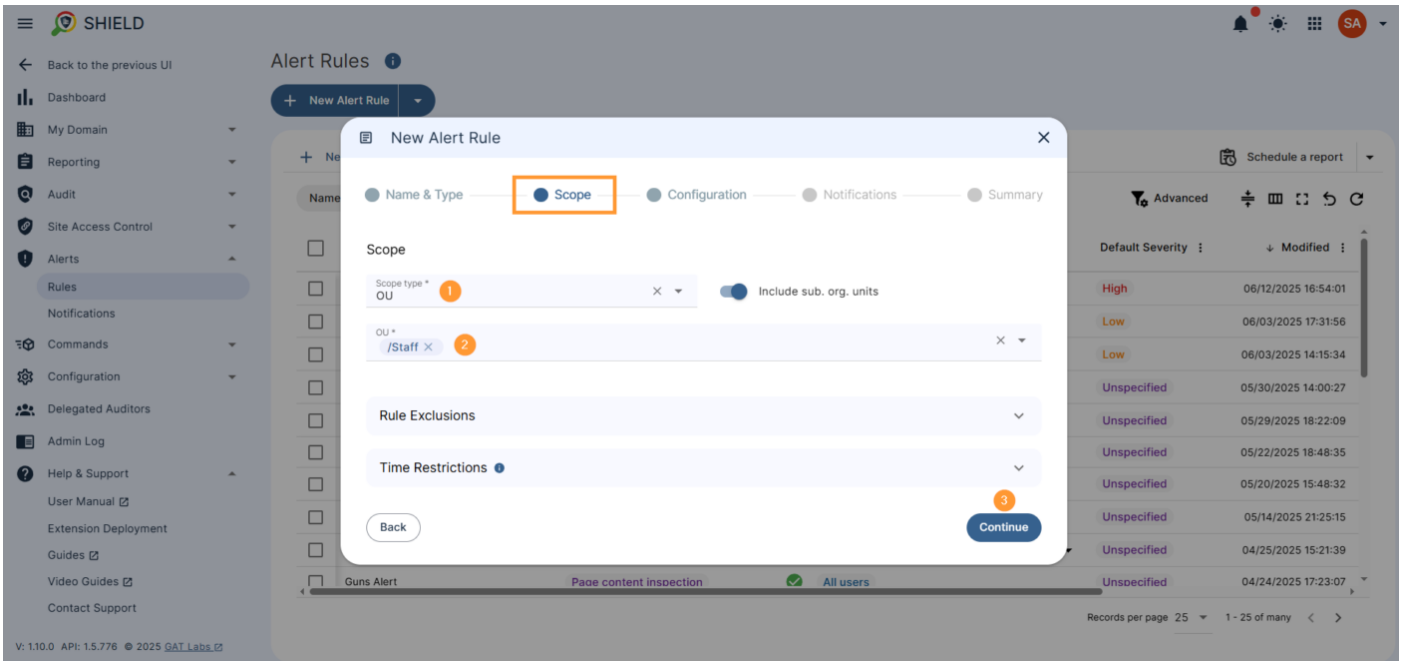
Enabling a "Visit" Alert Rule

When you enable a "Visit" Alert Rule, a pop-up window appears. Fill in the details.

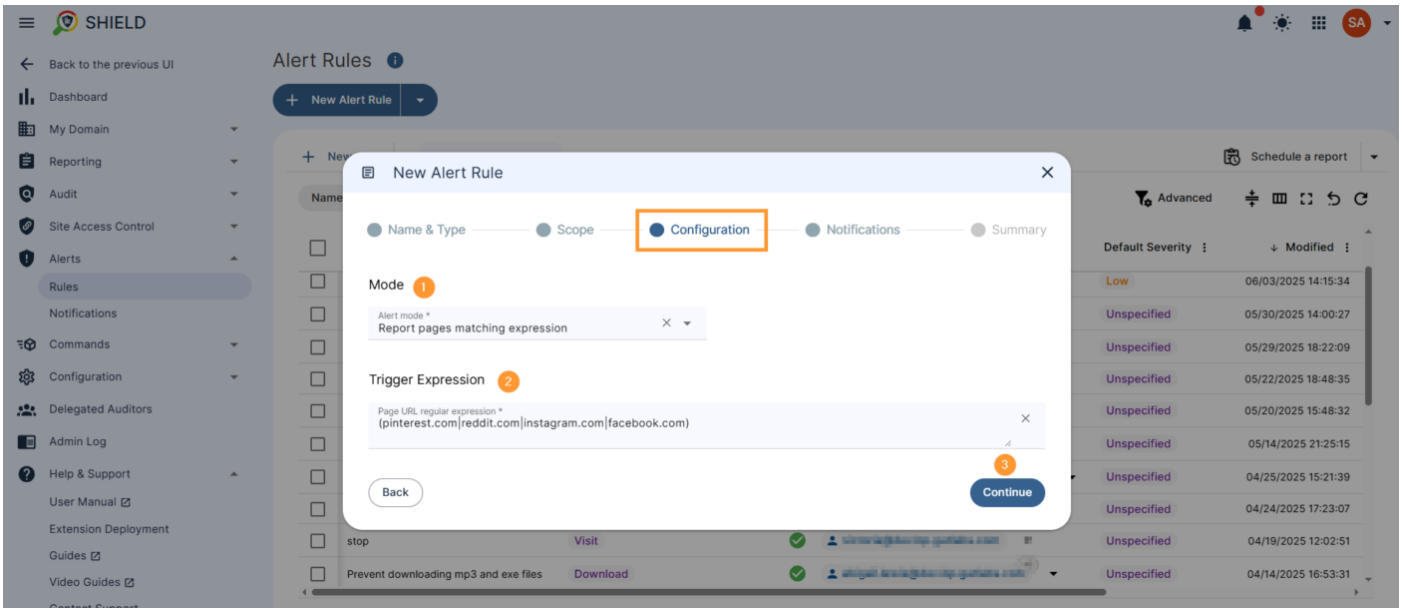
- **Name & Type**
  - **Alert rule name:** Give your rule a clear, descriptive name.
  - **Type:** Select the **Visit type** of alert
  - **Action:** Select **Show warning** or any other option from the menu
    - Close - close the tab for the user
    - Close without warning - close the tab without warning
    - Redirect - redirect the tab to another (added by the admin page)
    - Redirect without warning - redirect to another page without a warning message
    - No action - leave only the alert to be triggered without showing any notification to the end-user
  - **Default severity** - set up the severity for the alert to low, unspecified, or high



- **Scope**
  - Select the scope of affected users
  - Pick a user, a group of users, org. unit of users or all users



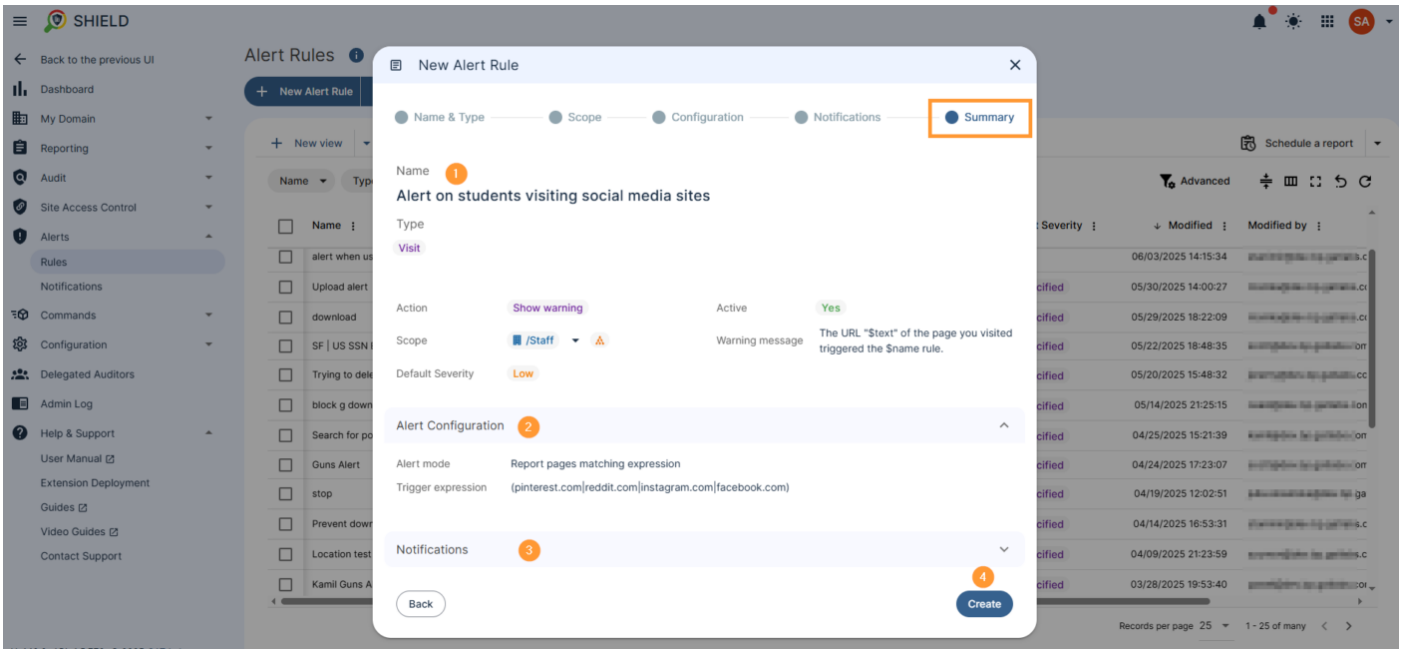
- **Configuration**
  - Mode - select alert mode
    - **Report pages matching expressions**
    - Click on to enable the "**regex mode**"
    - Enter the Trigger expression as a regex, from the examples above



- **Page URL regular expressions:** Here, you can enter the **specific site address or a Regular Expression (Regex) pattern** to match the URLs you want to monitor.
  - *Example 1 (Specific sites):* `(pinterest.com|reddit.com|instagram.com|facebook.com)` - This will trigger an alert for visits to any of these four social media sites.
  - *Example 2 (Blocking a domain, with exception):* `http(s|)?://(?!sketch)([-w].*.io)(?!sketch)S*` - This will trigger an alert for *all* `.io` sites, *except* `sketch.io`.
  - *Example 3 (Top-level domain):* `(\.io[\/\.])|(\.com\/io)` - This will trigger an alert for any site ending with `.io` **or** `.com/io`.
  - *Example 4 (Keyword in URL):* `games` - This will trigger an alert if the word "games" appears anywhere in the site's URL.

- **Notifications -** fill in the details for the notifications for the alerts
  - Alert recipients - enter the recipients of the alert
  - Notification interval - enter how many minutes to pass between the notifications
  - Full alert context - show the full context of the alert
    - Save website information and include it in the notifications
  - **Screen capture** - select any of the options
    - Do not report
    - Only send the picture as an attachment in the alert notification email
    - Send in the email and save it in the rule creator's Drive
    - Send in email, save in the rule creator's Drive, and share with other alert recipients.

- **Webcam capture** - this feature **must be enabled in the Admin console**
  - Do not report
  - Only send the picture as an attachment in the alert notification email
  - Send in the email and save it in the rule creator's Drive
  - Send in email, save in the rule creator's Drive, and share with other alert recipients

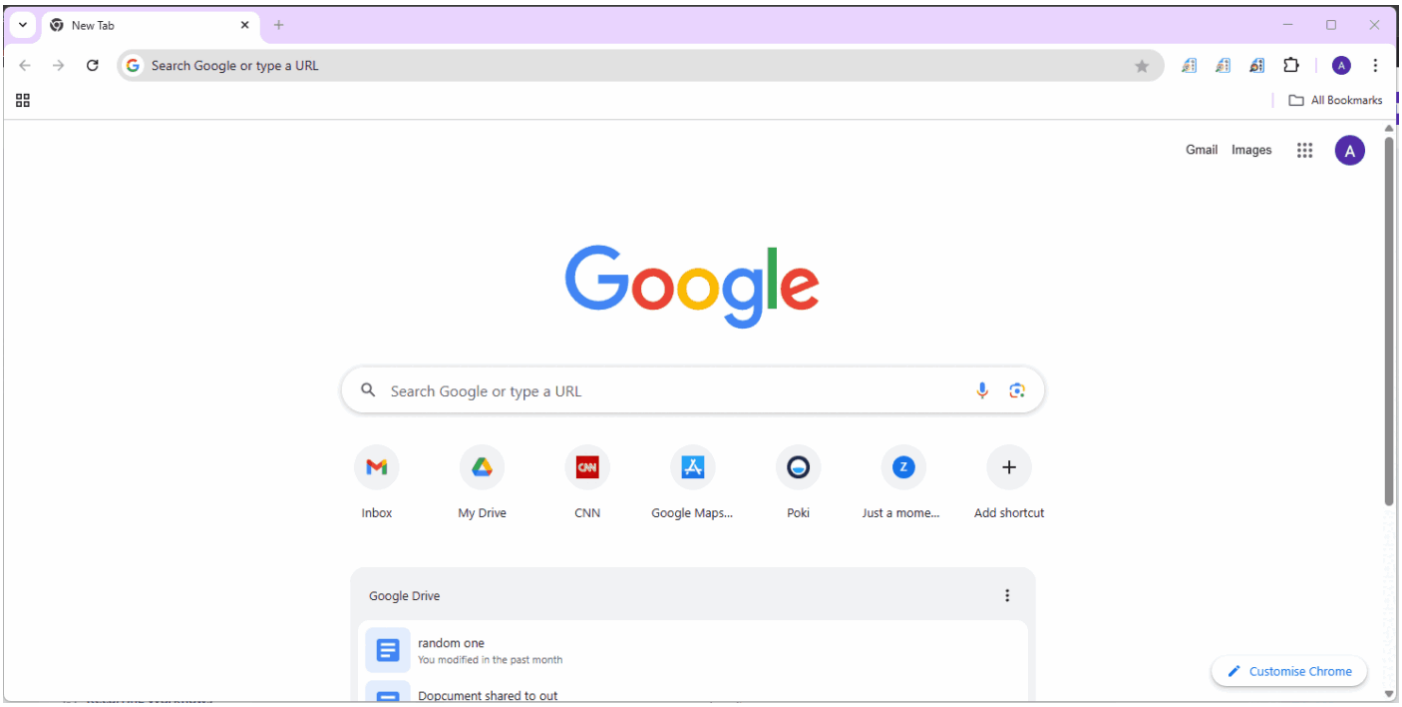


Click on the **Create** button to create the Visit alert rule

Result

When the alert is created, the end-users (under the Scope) will be affected by the rule.

When the user visits one of the specified sites in the **Page URL Regex** field, they **will see a warning message** and be **redirected** to the chosen page.


New Tab
Search Google or type a URL
All Bookmarks
Gmail
Images
Google
Search Google or type a URL
Inbox
My Drive
CNN
Google Maps...
Poki
Just a mome...
Add shortcut
Google Drive
random one
You modified in the past month
Dopcument shared to out
Customise Chrome