GAT Shield+ Overview

Products Overview · https://gatlabs.com/knowledge/tech-tips/gat-shield-plus-overview/

What is Shield+

Shield+ provides premium security for enterprises using Chrome. Built on GAT Shield, it combines a Chrome extension with a cloud-based service to provide advanced browser protection and real-time security monitoring.

With continuous identity verification, machine learning-based threat detection, and visibility into user activity, Shield+ helps IT and security teams detect suspicious behavior, protect active browser sessions, and respond to potential threats.

How it Works

Once deployed across your domain via Google Workspace or Chrome Enterprise management, Shield+ runs seamlessly on the user's Chrome browser. It works by continuously evaluating security telemetry without disrupting the user experience:

- **Continuous Identity Verification (ActiveID):** It analyzes the behavioral timing characteristics of a user's typing patterns (never the actual words) to ensure the person behind the keyboard is the legitimate account owner.
- **Proactive Policy Enforcement:** It monitors device performance, blocks phishing attempts via localized browser banners, and regulates copy/paste behavior based on organizational compliance rules.
- **Real-Time Visibility:** It feeds live browser data, alerts, and system health metrics directly back to the admin dashboard, allowing for instant incident response and session management.

Dashboard

Navigate to **Shield+ > Dashboard** (the default view). It presents a summary of security alerts raised by the system's Machine Learning models - the most important signal in the platform.

Time alerts - Three cards show alert counts; click on each to see more details

- Today - alerts from today
- Last 7 Days - alerts from the last 7 days
- All Time (Total) - overall total alerts

Alert types - Filter alert types

- All - all types of alerts combined
- ActiveID/TypingID - alerts for ActiveID/TypingID
- Inactivity Lock - Inactivity lock alerts
- Anti-Phishing - Anti-phishing alerts
- Device Performance - Device performance alerts

Scope - Used to select the users you want to view the dashboard for.

- Domain - select domain
- User - select a specific user
- Group - select a specific group
- Organization unit - select a specific org. unit

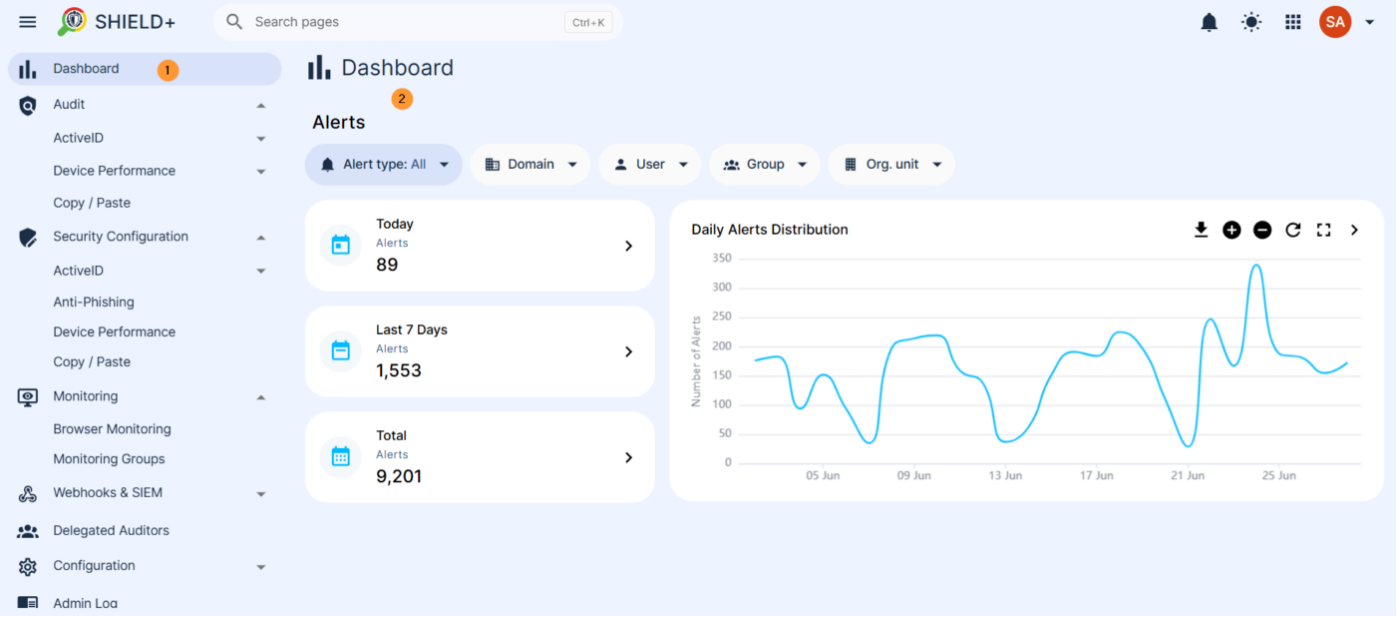
Daily Alerts Distribution

The daily alert distribution line chart shows alert volume over the past 30 days.

Clicking any point on the chart navigates directly to the matching filtered alerts list. It can be expanded by zooming in/out as well as downloaded as PNG, JPEG, or CSV.

It can also be expanded to full screen and downloaded as such

Navigate to **Shield+ > Dashboard**



Audit

The Audit section is a read-only section for logs and alert tables for every detection module for **ActiveID**, **Device performance, Anti-Phishing,** and **Copy and Paste**

ActiveID - TypingID

TypingID Alerts

TypingID Alerts - A paginated table of every TypingID alert - events where the Machine Learning model determined, with confidence above the rule's threshold, that the person typing is likely not the legitimate account owner. Each alert records the user, timestamp, confidence percentage, and current status.

- Severity can be updated, and alerts can be acknowledged individually or in bulk.
- Clicking an alert opens its details, which may include a screenshot, webcam capture, or the URL visited at the time, depending on the alert rule's attachment configuration.

TypingID Patterns

TypingID Patterns - The raw typing patterns collected from users and processed by the AI models. This view lets admins monitor how actively patterns are being generated per user, which directly reflects how well each user's identity model is trained.

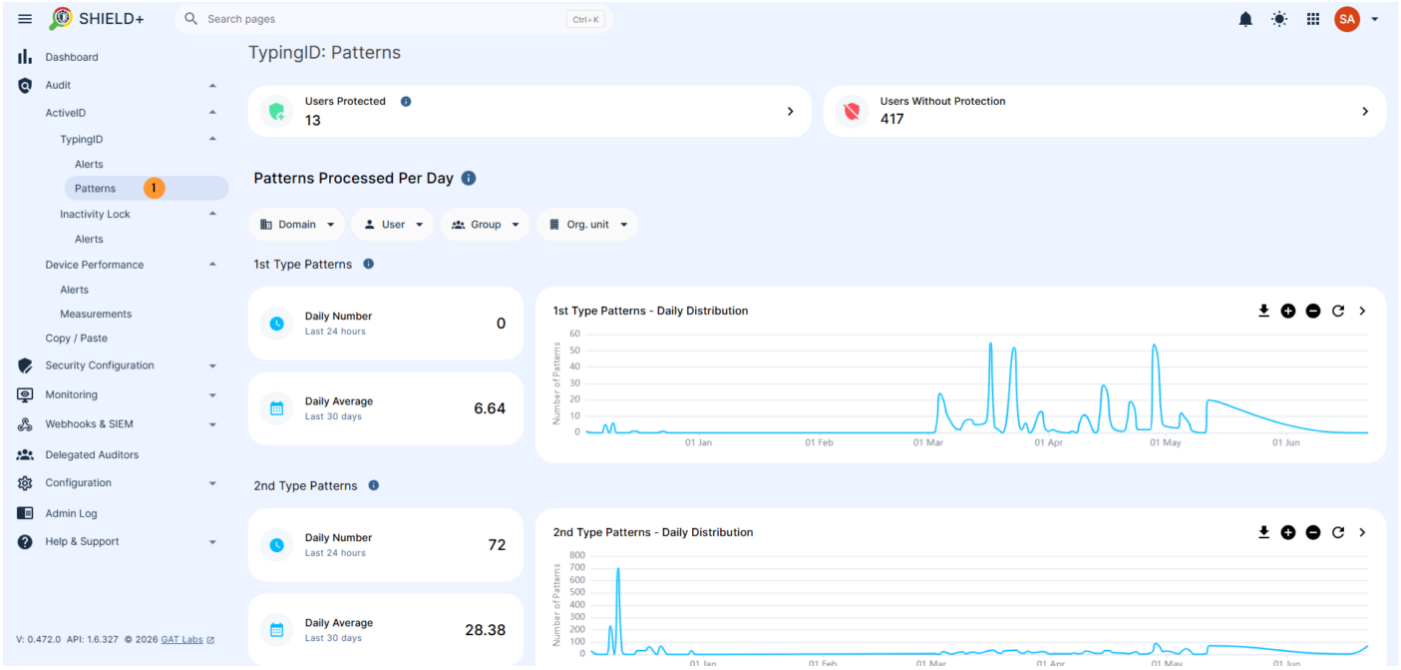
- We collect **2 types of typing patterns**. In this section, we present how many typing patterns were verified by our system on a daily basis.

- 1st type patterns - **Full Typing Pattern** - A detailed profile pattern of your typing style based on 100–150 keystrokes.
- View daily numbers - for the last 24 hrs
- View daily average - for the last 30 days
- 2nd type patterns - **Key-Pair Pattern** - faster profiles built from the timing of consecutive letter pairs like "TH" or "AE")
- View daily numbers - for the last 24 hrs
- View daily average - for the last 30 days

Scope - filter by user, domain, group, or org. unit.

- **Users protected** - a successfully built model means that the user is being actively protected. AI model checks if the generated text matches the user's previous typing behaviour
- **Users without protection** - list of users where this model is not built yet

Navigate to **Shield+ > Audit > ActiveID > TypingID > Alerts or Patterns**



Inactivity Lock

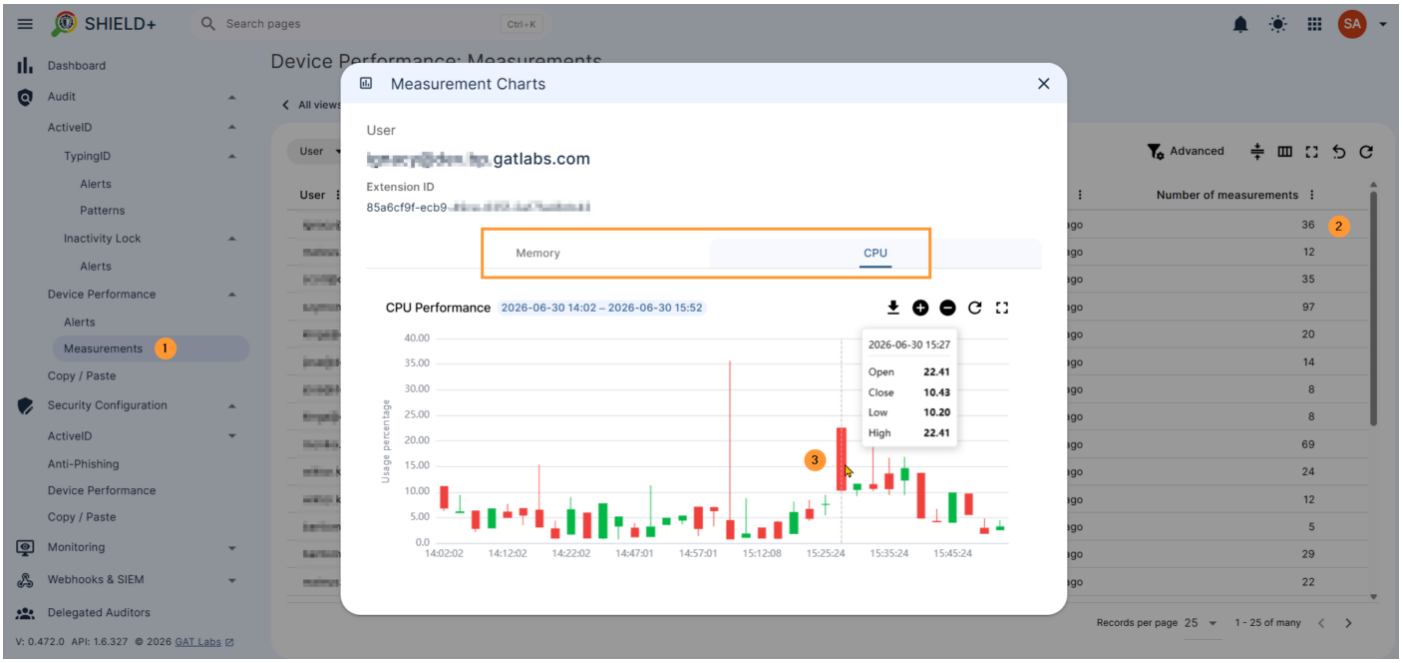
Inactivity lock - Alerts are raised when an inactivity lock challenge is triggered, but the user failed to respond, responded incorrectly, or let the request time out. Each record shows the user, trigger time, and the specific failure reason (e.g., verification failed, timed out, credential not found).

Device performance

Device performance is measured by the stats of alerts raised when a user's device CPU or memory usage exceeded a configured threshold for a sustained period. Each alert records the affected user, the resource (CPU or Memory), the metric (Maximum or Average), and the duration.

- **Alerts** - Alerts are raised when a user's device CPU or memory usage exceeds a configured threshold for a sustained period. Each alert records the affected user, the resource (CPU or Memory), the metric (Maximum or Average), and the duration.
- **Measurements** - Raw performance readings collected from user devices over time. Individual records can be expanded to view CPU and memory measurement charts for a detailed history of a device's resource usage.

Navigate to **Shield+ > Audit > Device performance > Alerts or Measurements**



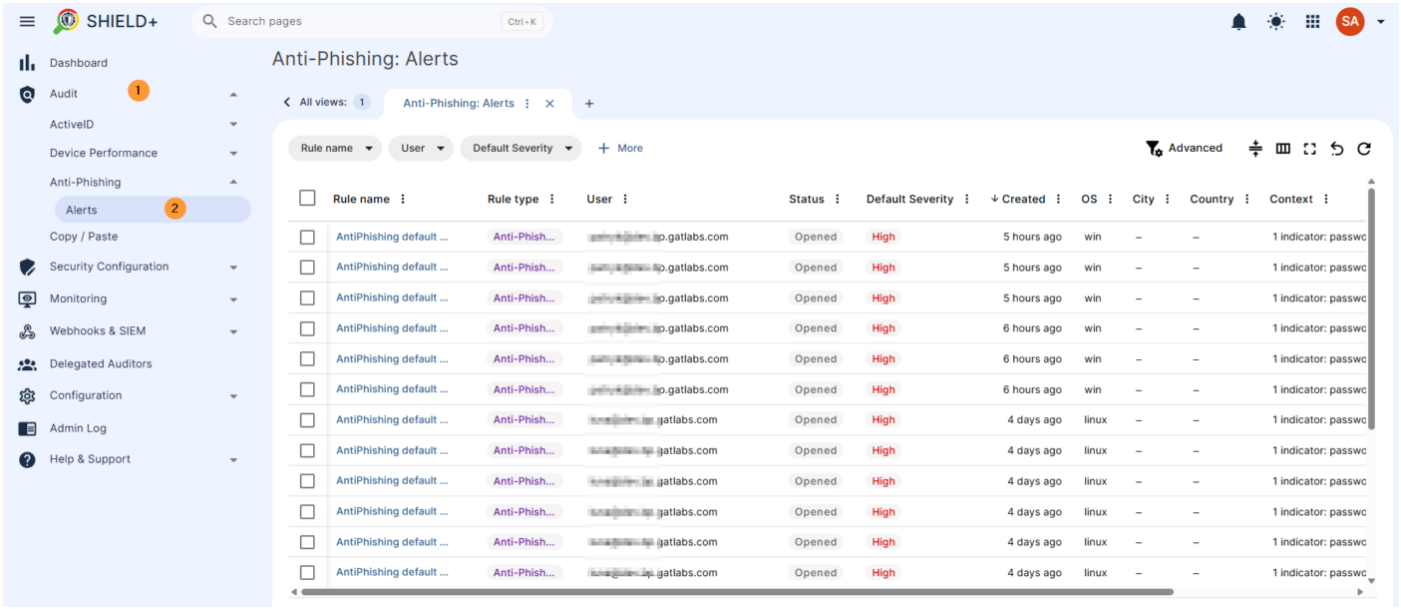
Anti-Phishing

Anti-Phishing Alerts – A paginated table of alerts generated by Anti-Phishing activity. Admins can review which user and URL were involved, when the event happened, which rule or policy applied, and the current alert status.

This view is used to inspect Anti-Phishing outcomes such as blocked access or warning/override events when browser enforcement is enabled. Admins can review alert details, update severity or status, acknowledge alerts, and decide whether a domain should be added to Allowed Websites or Blocked Websites.

Allowed and Blocked Websites are configured under Security Configuration. The Audit view is for reviewing Anti-Phishing alerts, not managing those lists.

Navigate to **Shield+ > Audit > Anti-Phishing > Alerts**

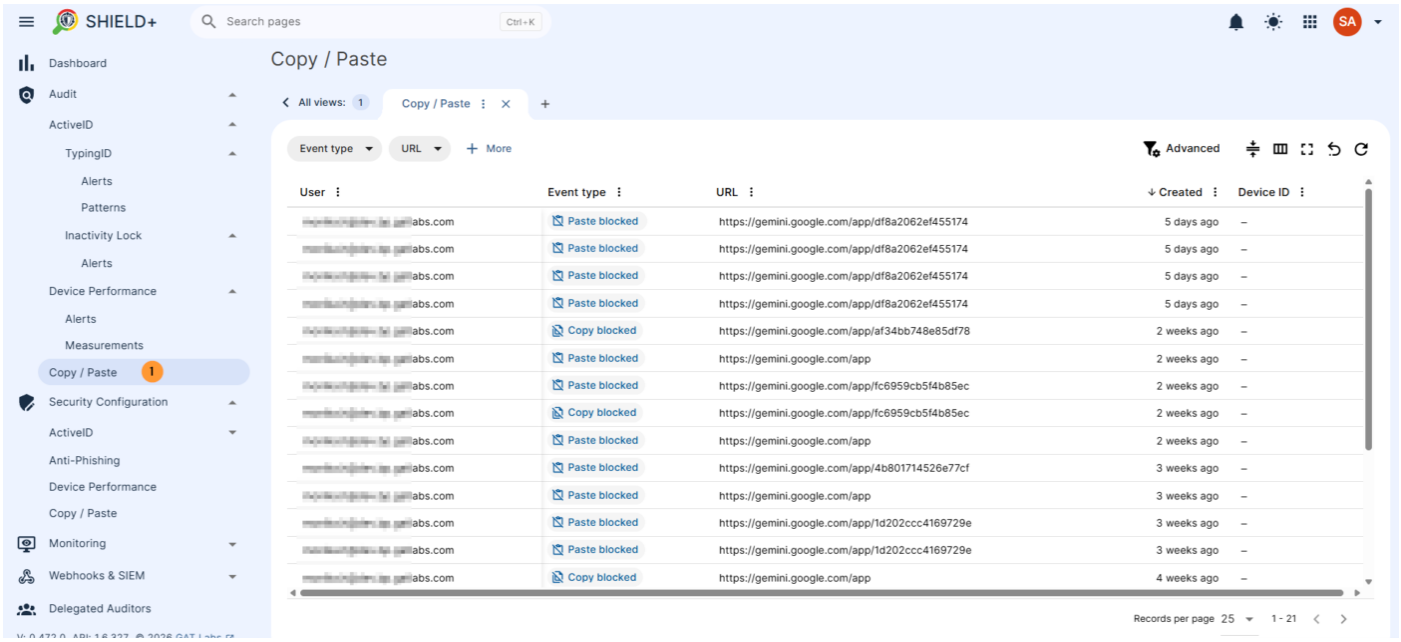


Copy / Paste

A log of all copy and paste events captured from users' browsers.

Each entry shows the URL where the event occurred, the event type (Copy Allowed, Copy Blocked, Paste Allowed, Paste Blocked), and the user who triggered it.

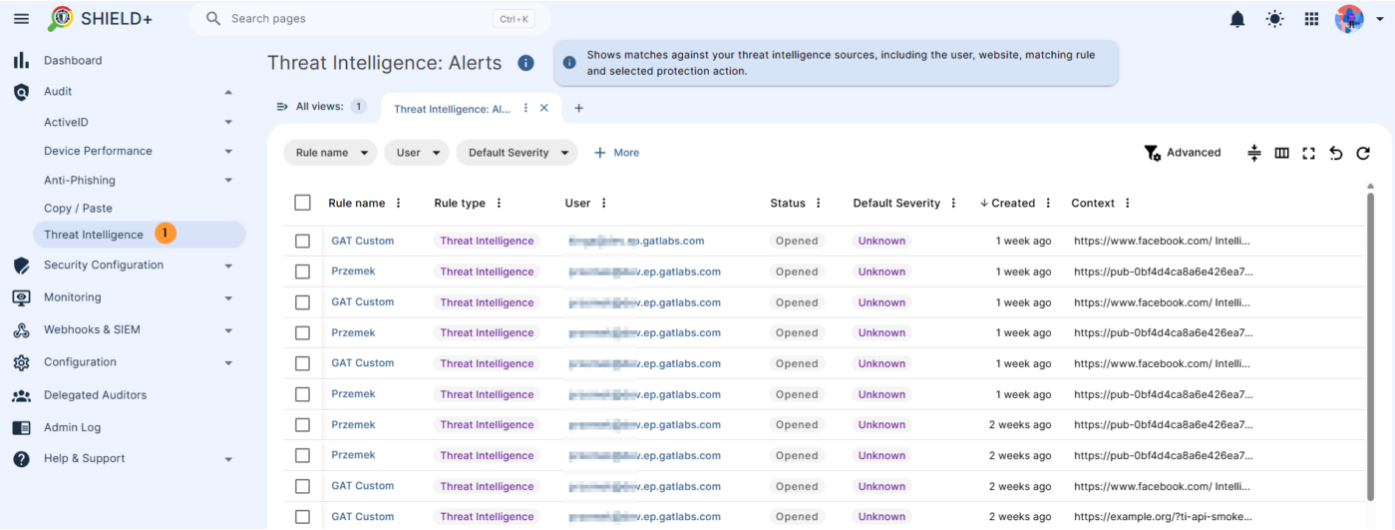
Navigate to **Shield+ > Audit > Copy/Paste**



The Admins can review flagged events, inspect details, and acknowledge alerts from these views.

Threat intelligence

Shows matches against your threat intelligence sources, including the user, website, matching rule, and selected protection action.



Security Configuration

The Admins create and manage rules, policies, and lists that control how Shield+ detects threats and enforces actions.

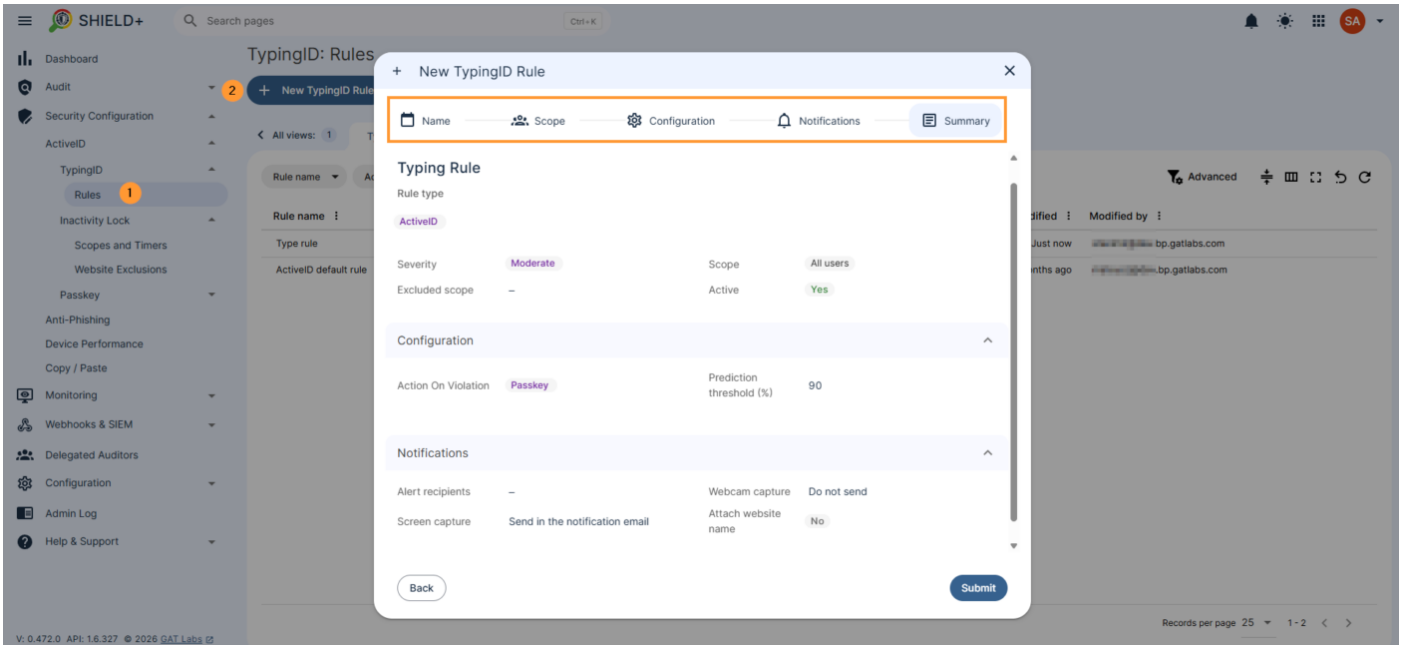
Changes here directly affect what gets flagged and what happens to users when a violation is detected.

ActiveID

ActiveID is a feature of continuous typing verification. It creates a profile of a user based on typing characteristics. In order to create a profile, it will have to record the user's typing patterns (but only timing characteristics; no actual words typed are recorded) for some time. Then it starts to verify every new pattern that comes to the app and decides whether it matches the profile or not. Based on the advanced logic of Machine Learning algorithms, it can decide whether the person who is typing is the actual user logged into their account or an imposter who gained unauthorised access to the account. In the latter case, the GAT Shield+ ActiveID feature will raise an alert, notifying the admin of the domain and (optionally) logging out the person who is typing from the account.

TypingID Rules

Create and manage the alert rules that govern when TypingID alerts fire. Each rule defines: the scope (which users it applies to), the prediction threshold (confidence level above which an alert is triggered), alert recipients and notification settings, optional alert attachments (screenshot, webcam capture, visited URL), and the action on violation - either no session action, a Passkey challenge (screen locked until the user verifies their identity), or clearing browser cookies (effectively ending all active sessions). Rules can be activated or deactivated without deleting them.



Create a typingID rule

Navigate to **Shield+ > Security configuration> ActiveID > TypingID > Rules > + New TypingID rule**

- **Name** - enter the name for the rule
  - Default severity - select severity for the rule
    - Unspecified
    - Low
    - Moderate
    - High
    - Critical

- **Scope** - pick and select the scope for the alert

    - Pick a user, group, or org. Unit of users
        - Excluded scope - Specify users, groups, or OUs that should be excluded from the scope of the defined rule.
            - Add: excluded scope

- **Configuration** - Confidence level at which ActiveID will send an alert.
    - **Enter the prediction threshold** (%) - add percentile
    - **Action on violation** - Select one of the user logout actions to be executed when a role is violated:
        - None - No user session action will be taken.
        - Passkey -Locks the screen. Success resumes access; cancel or failure keeps the screen locked.
        - Clear cookies -Clears browser cookies.

- **Notifications** - fill in the details
    - Alert recipients - enter alert recipients
    - Webhooks & SIEM - select option
        - Elastic Search
        - Generic receiver
        - Splunk
    - Webcam capture - select option
        - 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 with other alert recipients
    - Screen capture - select option
        - Do not send
        - Send in the notification email
        - Send in the notification email and save to the rule creator's Drive

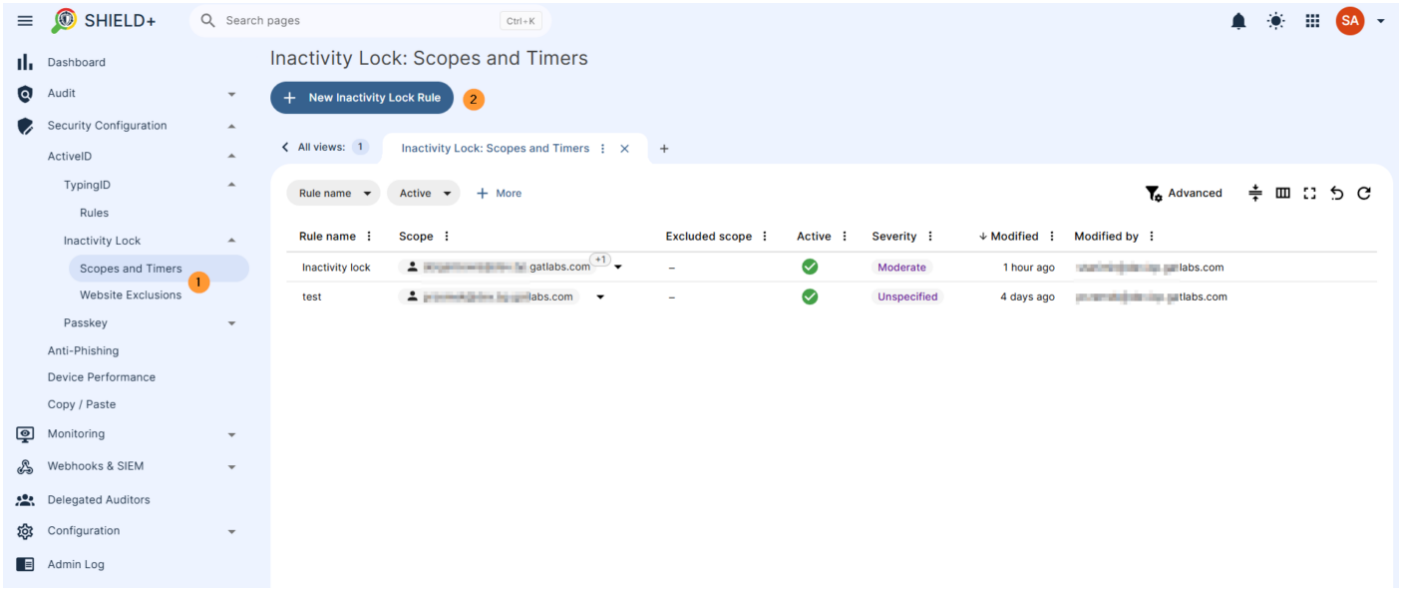
        - Send in the notification email, save to the rule creator's Drive, and share with other alert recipients
    - Attach website name - enable or disable the option
- **Summary** - view all the options that are selected

Inactivity Lock

Scopes and Timers

Configure policies that define how long a user can be inactive before Shield+ requires identity verification in the browser. Each policy specifies the inactivity period in minutes and the scope of users it covers. When the inactivity threshold is reached, Shield+ requires the user to verify with Passkey before continuing.

Navigate to **Shield+ > Security configuration > ActiveID > Inactivity Lock > Scopes and Timers > New inactivity lock rule**

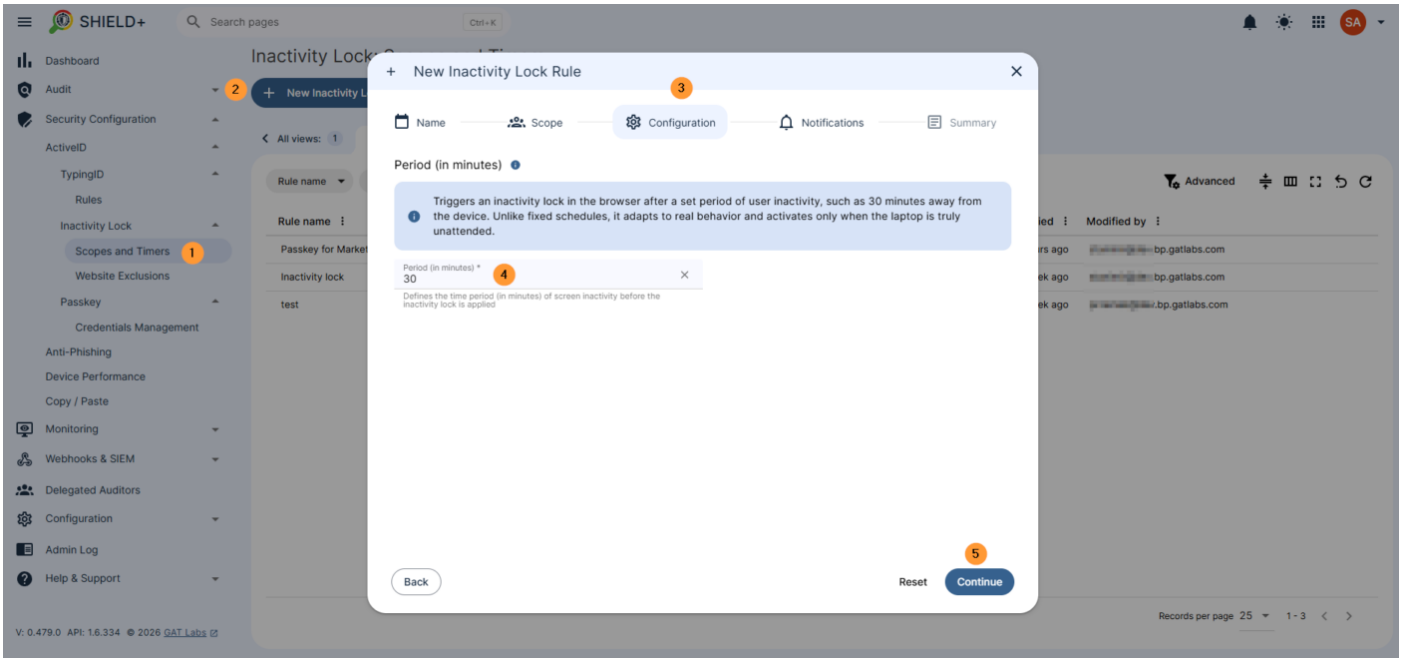


- **Name** - enter the name for the rule
    - Default severity - select severity for the rule
        - Unspecified
        - Low
        - Moderate
        - High

        - Critical

- **Scope** - pick and select the scope for the alert
    - Pick user, group, or org. Unit of users
        - Excluded scope - Specify users, groups, or OUs that should be excluded from the scope of the defined rule.
            - Add: excluded scope

- **Configuration** - **Triggers an inactivity lock in the browser after a set period of user inactivity**, such as 30 minutes away from the device. Unlike fixed schedules, it adapts to real behavior and activates only when the laptop is truly unattended.
    - **Defines the time period (in minutes) of screen inactivity before the inactivity lock is applied**



- **Notifications** - fill in the details
    - Alert recipients - enter alert recipients
    - Webhooks & SIEM - select option
        - Elastic Search
        - Generic receiver
        - Splunk

- Webcam capture - select option
  - 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 with other alert recipients
- Screen capture - select option
  - 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 with other alert recipients
- Attach website name - enable or disable the option

- **Summary** - view all the options that are selected

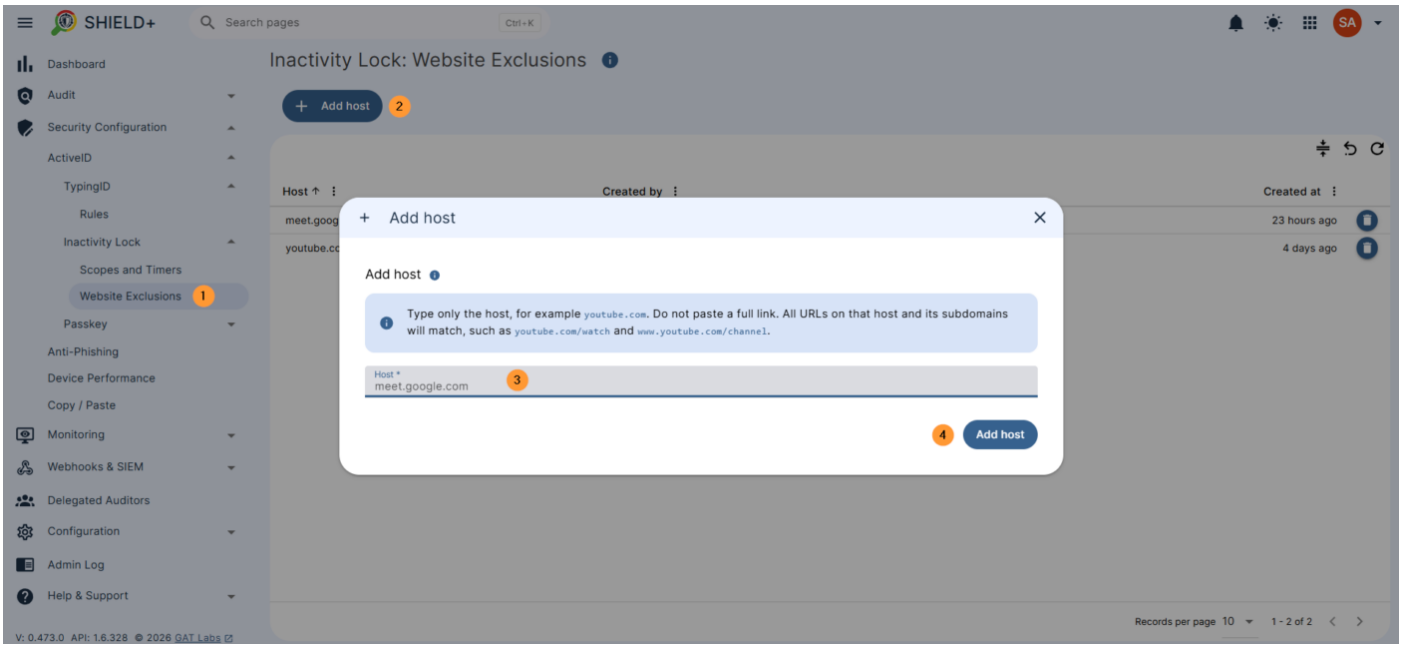
Website Exclusions

A list of website hosts excluded from immediate inactivity locking - intended for sites like video meetings, for example, **meet.google.com**, where users may be present without typing or moving the mouse.

Entries are hostnames only, not full URLs.

When a user on an excluded host reaches their inactivity period, Shield+ asks them to confirm they are still present before locking. If confirmed, the next inactivity check is deferred by the configured inactivity period, up to 30 minutes.

Navigate to **Shield+ > Security configuration > ActiveID > Inactivity Lock > Website exclusions > Add host**



Passkey - Credential management

View and manage "Passkey" credentials registered by users for identity verification challenges. Admins can see which users have registered credentials, how many credentials they have, and when they were last used. Revoking credentials for a user forces that user to register a Passkey again on their next verification prompt.

Passkey adds an extra identity check inside the Shield+ browser extension. It is used when the organization wants to make sure the person using the browser is still the correct user.

Works for the end-user.

- The user is asked to set up a passkey.
- They can create it on this device, with a phone, or with a hardware security key.
- When Shield+ needs confirmation, the browser opens a security check screen.
- The user verifies with their passkey, device PIN, fingerprint, face unlock, phone, or security key.
- After successful verification, Shield+ returns the user to the page they were using.

Shield+ does not store the user’s password or biometric data. The device keeps the private part of the passkey. GAT/Shield+ stores the registered credential information needed to check that future passkey responses are valid.

When Passkey Is Used

Passkey can be required in two main situations:

- **Inactivity Lock**

If the user has been inactive for a configured number of minutes, **Shield+ locks browsing** and **asks for passkey verification before the user can continue.**

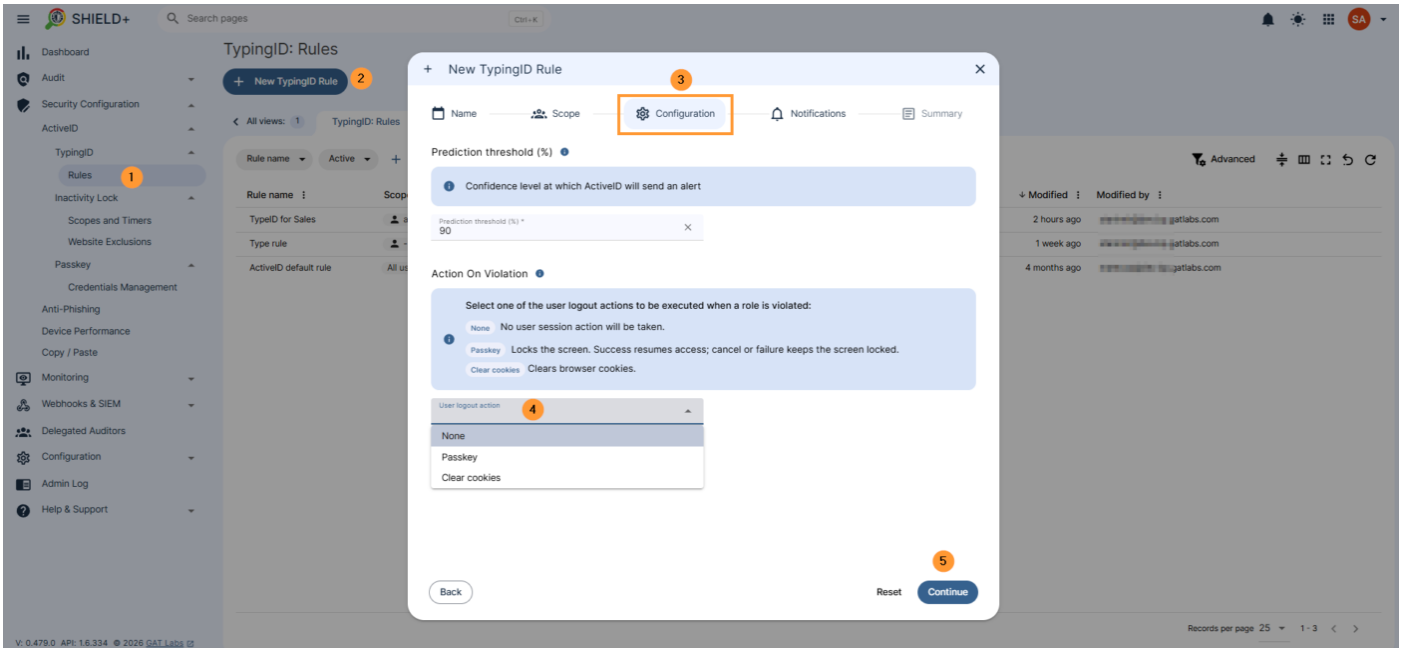
- **ActiveID Check**

If ActiveID detects unusual typing behavior, an administrator can configure the response to require passkey verification. This helps reduce false positives: instead of immediately treating the activity as unauthorized, the user can prove they are really present.

There is also an administrator-forced security check path in the extension, but the main user-facing configuration is Inactivity Lock and ActiveID Passkey action.

Administrator Configuration

Navigate to **Security configuration > ActiveID > TypingID > Rules > New TypingID rule**



Select one of the user logout actions to be executed when a role is violated:

- **None** -No user session action will be taken.
- **Passkey** - Locks the screen. Success resumes access; cancel or failure keeps the screen locked.
- **Clear cookies** - Clears browser cookies.

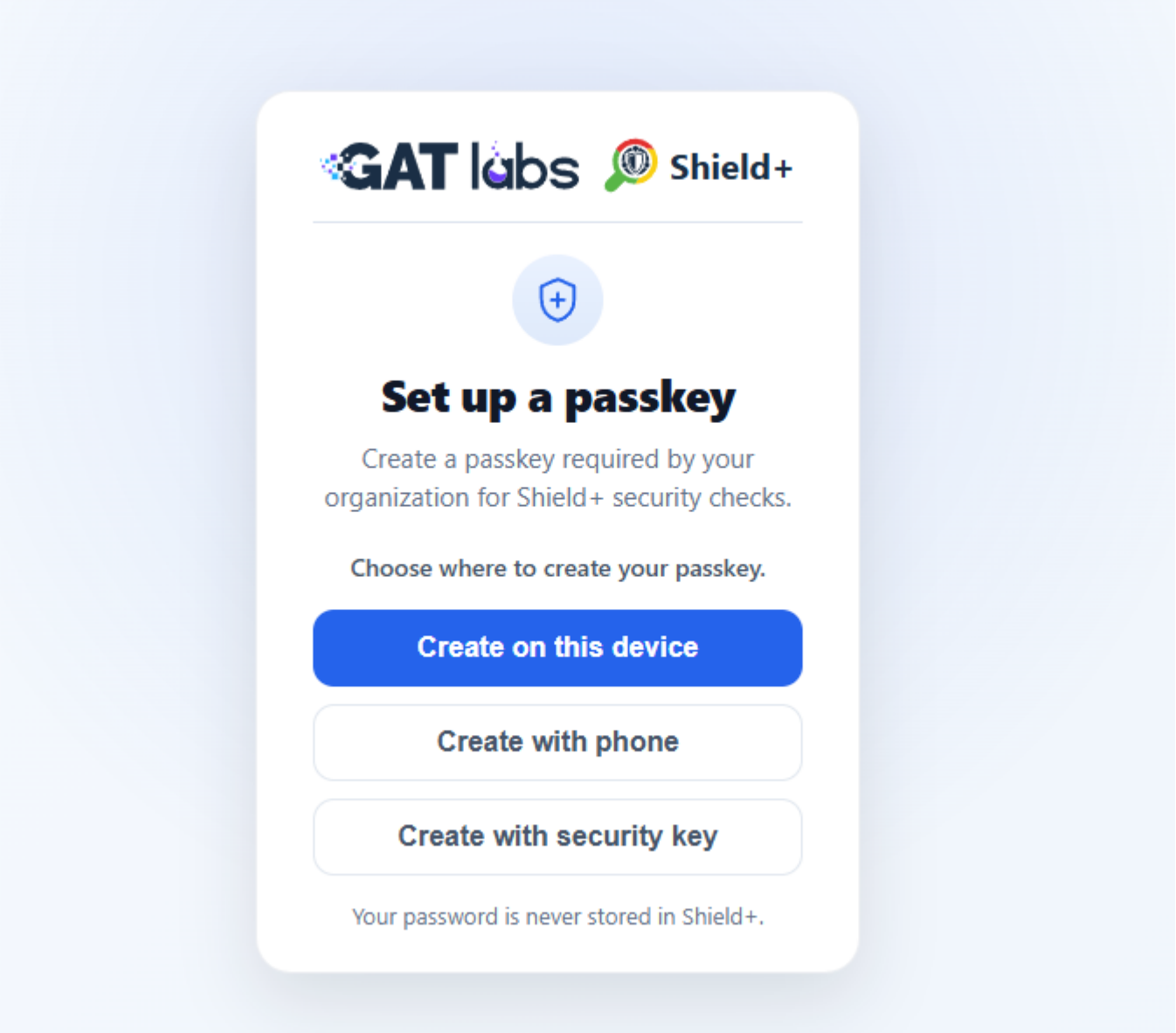
First-Time User Experience:

If a user is asked to verify but has no passkey yet, Shield+ sends them to the passkey setup page.

After setup, they can use the passkey for future security checks. If the user later adds another passkey, Shield+ may ask them to verify first.

Set up a **passkey** as follows.

- Create on this device - create for the device itself
- Create with phone - barcode will be generated, then scanned with mobile phone
- Create with security key - use USB to create passkey



What the Admin Controls

From the admin console, you manage the passkeys.

- **Visibility:** You can see a list of all Passkeys registered by your users, along with exactly when they were last used to unlock a browser.

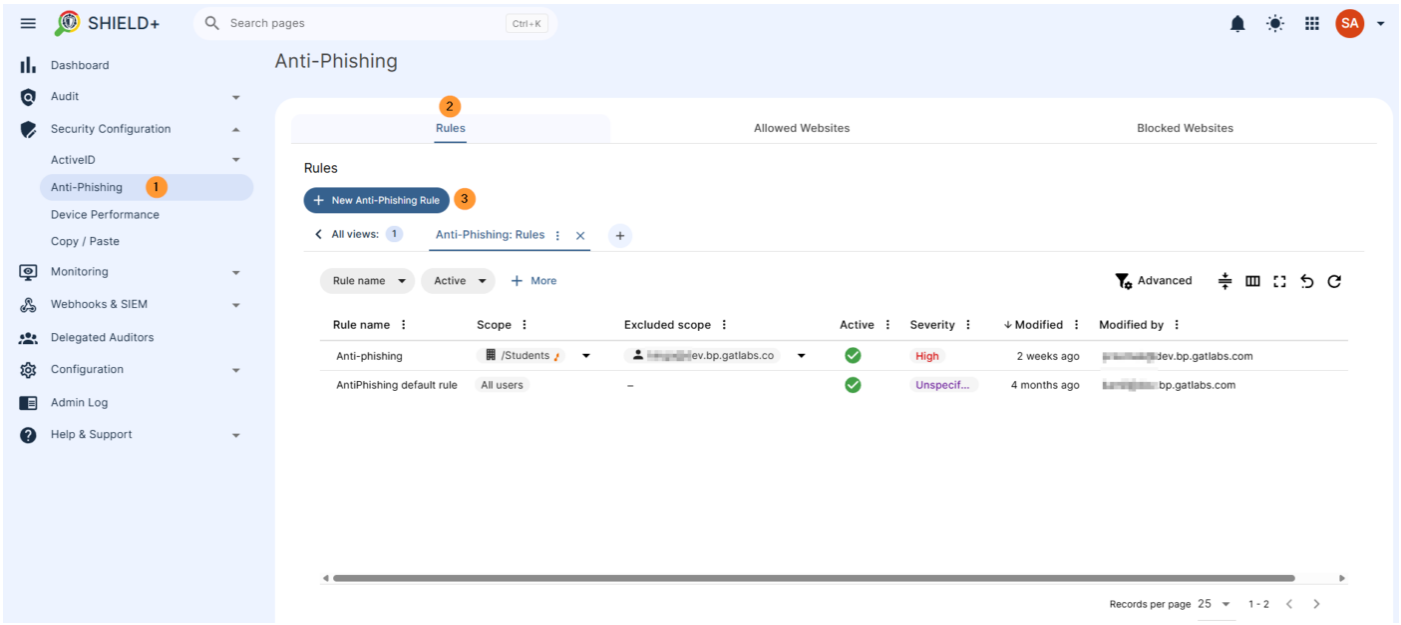
- **Revoking Access:** If a user loses a hardware key or if you suspect a security breach, you can instantly revoke an individual passkey or wipe all passkeys for that user.

Anti-Phishing

Create and manage Anti-Phishing alert rules. Each rule defines the scope, notification recipients, and browser action settings for detector results. Admins can choose whether detector warnings and blocking should interrupt the user in the browser, and can configure the severity threshold at which detector block results become hard blocks. Administrator-blocked websites are always blocked by policy.

Rules - Define and create new anti-phishing rules.

Navigate to **Shield+ > Security configuration > Anti-Phishing > New anti-phishing rule**

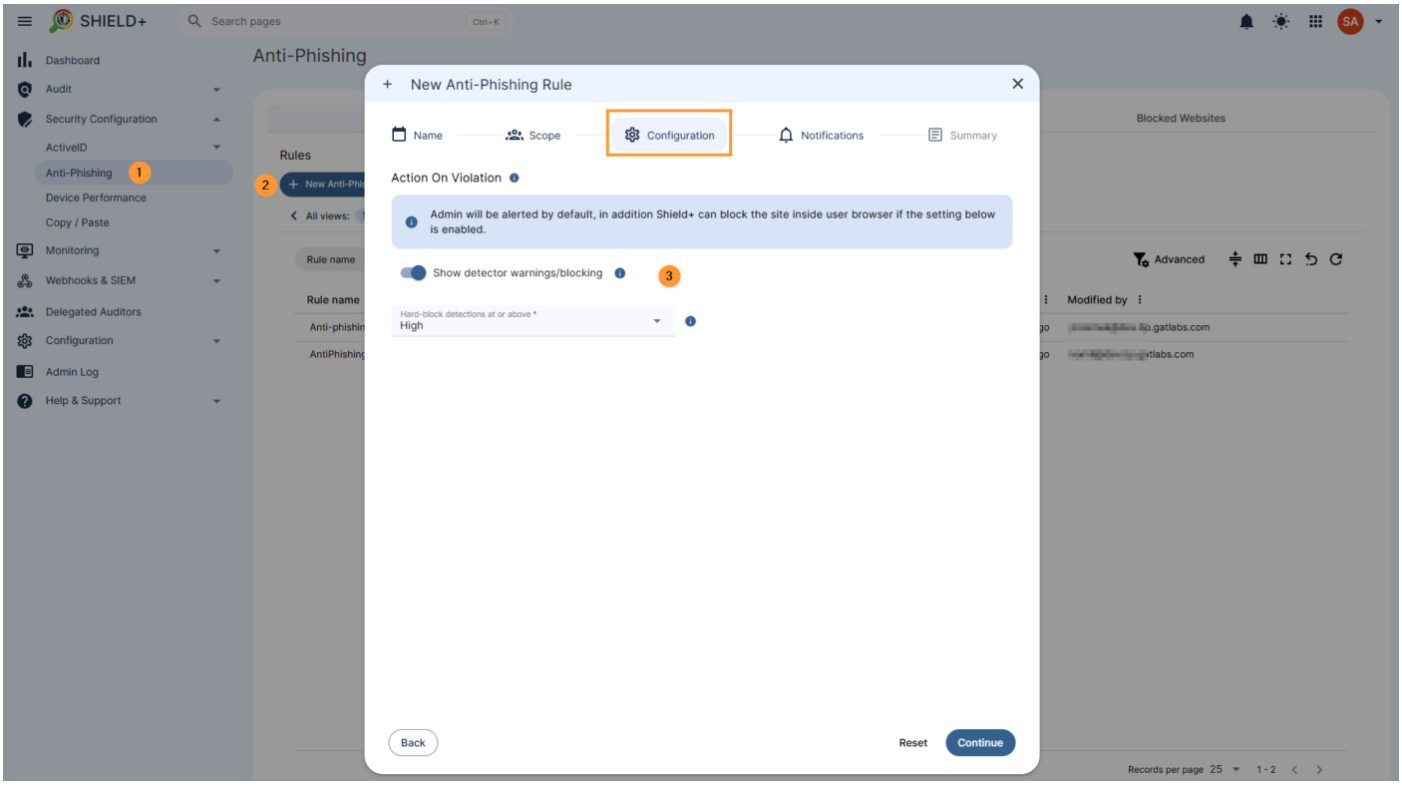


- **Name** - Enter the name for the rule
  - Default severity - When the Alert Rule is triggered, a notification is created. The severity of the notification is decided by the software and indicates its level of importance. The values are Low, Moderate, High, and Critical. "Alert Level Threshold" is the "notification threshold". If you set the default severity to "Low," it means that "all alerts with severity level Low and higher will be sent".
    - Unspecified
    - Low
    - Moderate

        - High
        - Critical

- **Scope** - pick and select the scope for the alert
    - Pick user, group, or org. unit of users
        - Excluded scope - Specify users, groups, or OUs that should be excluded from the scope of the defined rule.
            - Add: excluded scope

- **Configuration** - Admin will be alerted by default; in addition, Shield+ can block the site inside the user's browser if the setting below is enabled.
    - **Show detector warnings/blocking** – When enabled, detector results can interrupt the user in the browser. Warning results show a user-visible warning that can be overridden. Detector block results become hard blocks only at or above the configured hard-block threshold; below that threshold, they behave as overridable warnings. Administrator-blocked websites are always blocked.



- **Notifications** - fill in the details

    - Alert recipients - enter alert recipients
    - Webhooks & SIEM - select option
        - Elastic Search
        - Generic receiver
        - Splunk
    - Webcam capture - select option
        - 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 with other alert recipients
    - Screen capture - select option
        - 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 with other alert recipients
    - Attach website name - enable or disable the option
- **Summary** - view all the options that are selected

Allowed Websites / Blocked Websites

Domains manually added by admins to control Anti-Phishing behavior.

Allowed Websites are trusted domains where pages bypass Anti-Phishing checks and can override administrator-blocked domain entries. Blocked Websites are domains that are always treated as phishing threats and blocked for users by administrator policy.

Entries are saved as site domains. The current UI accepts domains only. Protocols, ports, paths, and wildcards are not accepted in these fields.

Allowed Websites: Add a domain that should be trusted by Anti-Phishing protection.

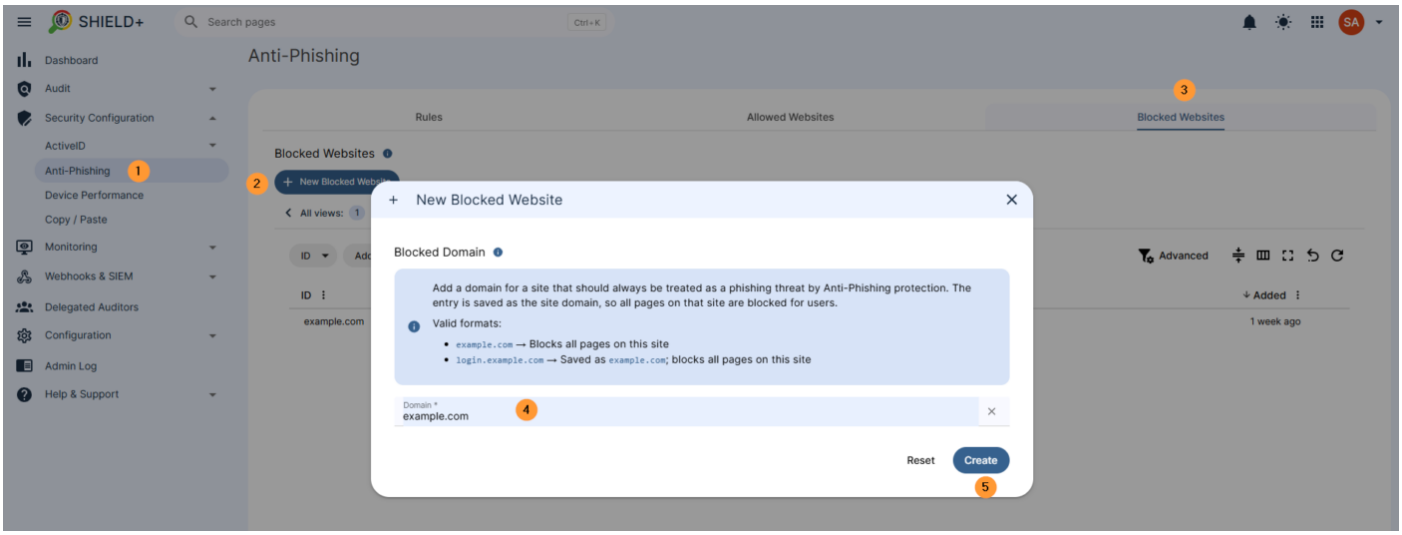
Valid format:

- example.com → Bypasses Anti-Phishing checks for pages on this site

Blocked Websites: Add a domain that should always be treated as a phishing threat by Anti-Phishing protection.

Valid format:

- example.com → Blocks pages on this site by administrator policy

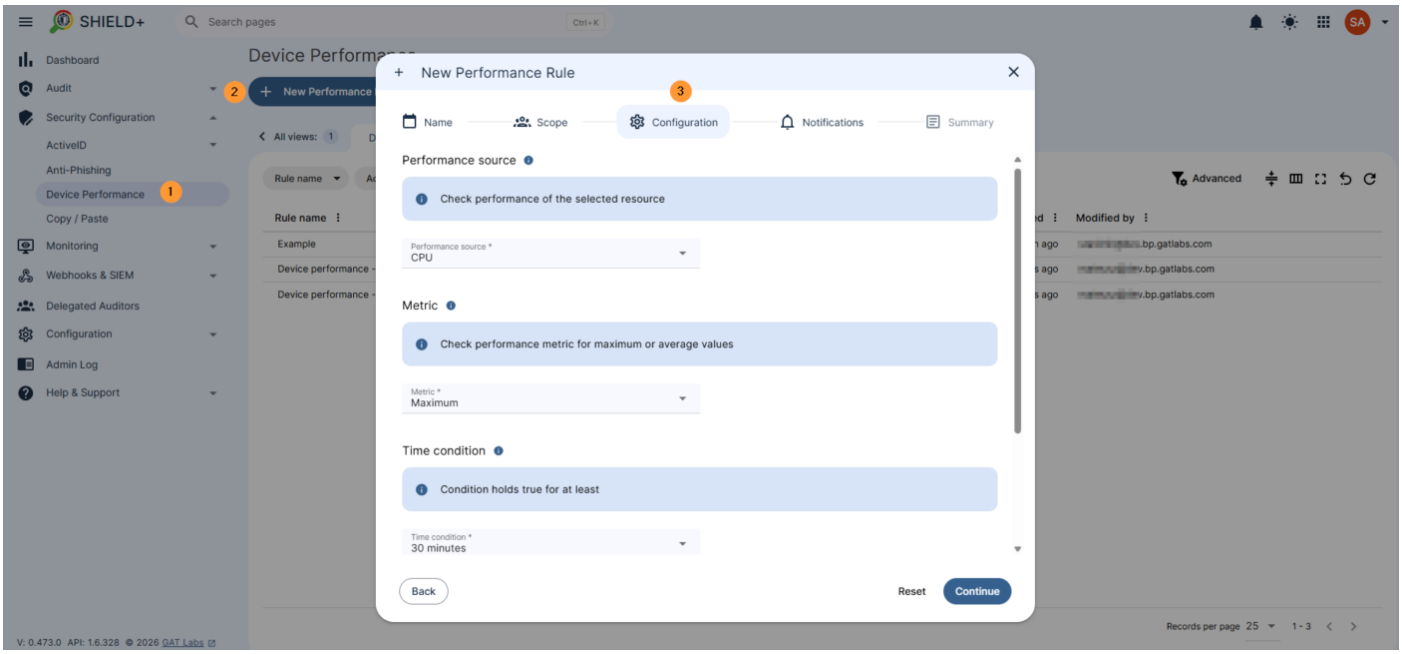


Device Performance - Performance Rules

Set up a performance rule for device resource monitoring. Each rule can specify a performance source; it can be CPU or Memory, the metric (Maximum or Average readings), the timeframe the condition must hold (15, 30, or 60 minutes), the threshold percentage, and notification recipients.

Navigate to **Shield+ > Security configuration > Device performance > New perormance rule**

Fill in the required details such as Source, Metric, and Time condition



Copy / Paste

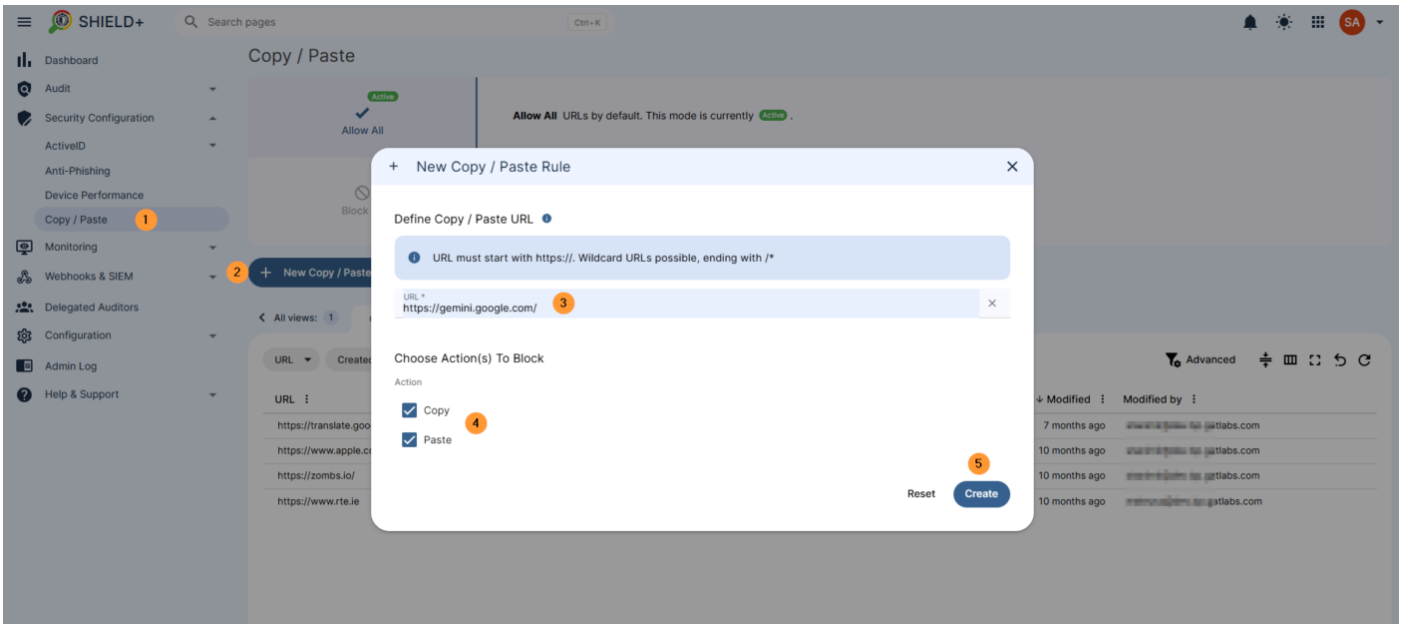
Configure copy and paste restrictions across the domain.

Two modes: Allow All (copy/paste permitted everywhere by default - specific URLs can be added to block) or Block All (copy/paste denied everywhere by default - specific URLs can be added to allow).

URL entries support wildcards ending with `/*` to cover child paths.

Navigate to **Shield+ > Security configuration > Copy / Paste > New copy/paste rule**

- Allow all - by default, all URLs are allowed by default
  - Add websites so the block of copy/paste is enabled only on those websites.
- Block all - you can block all and allow copy/paste on some sites

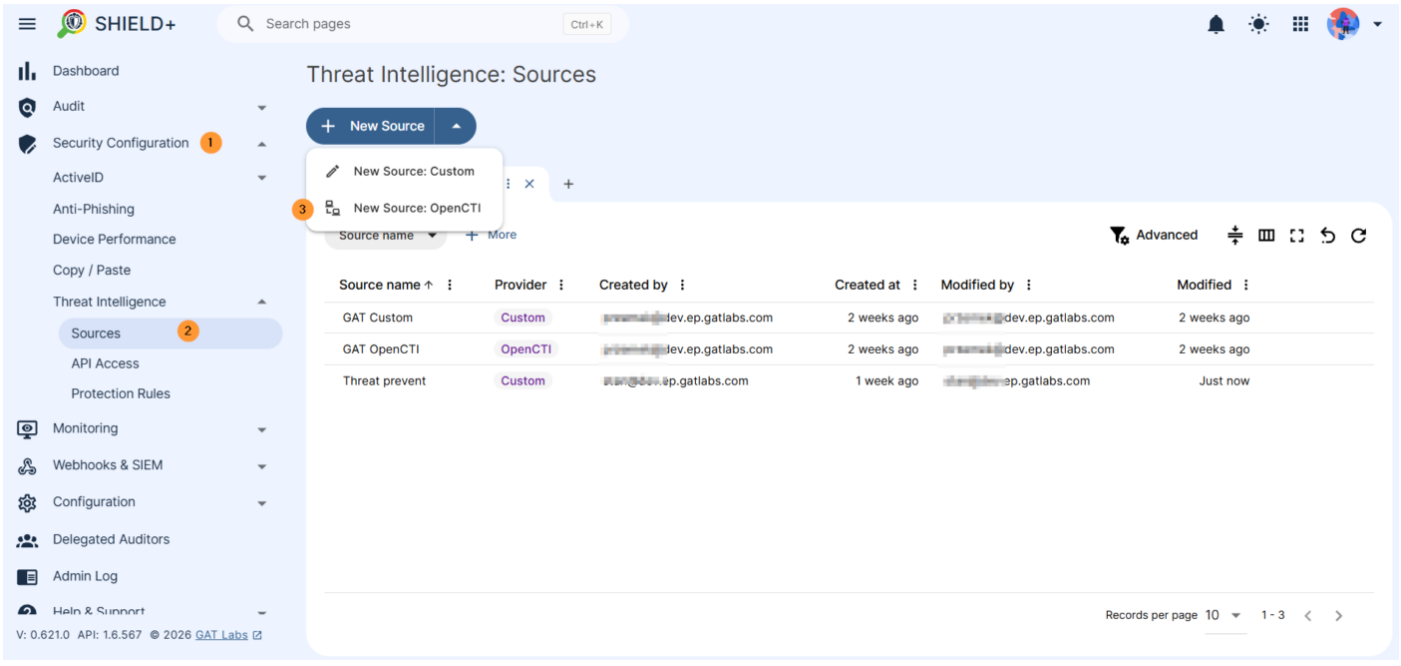


Threat Intelligence setup

Threat intelligence

OpenCTI Source

Navigate to **Shield+ > Security configuration > Threat Intelligence > Sources > New Source > New Source: OpenCTI**

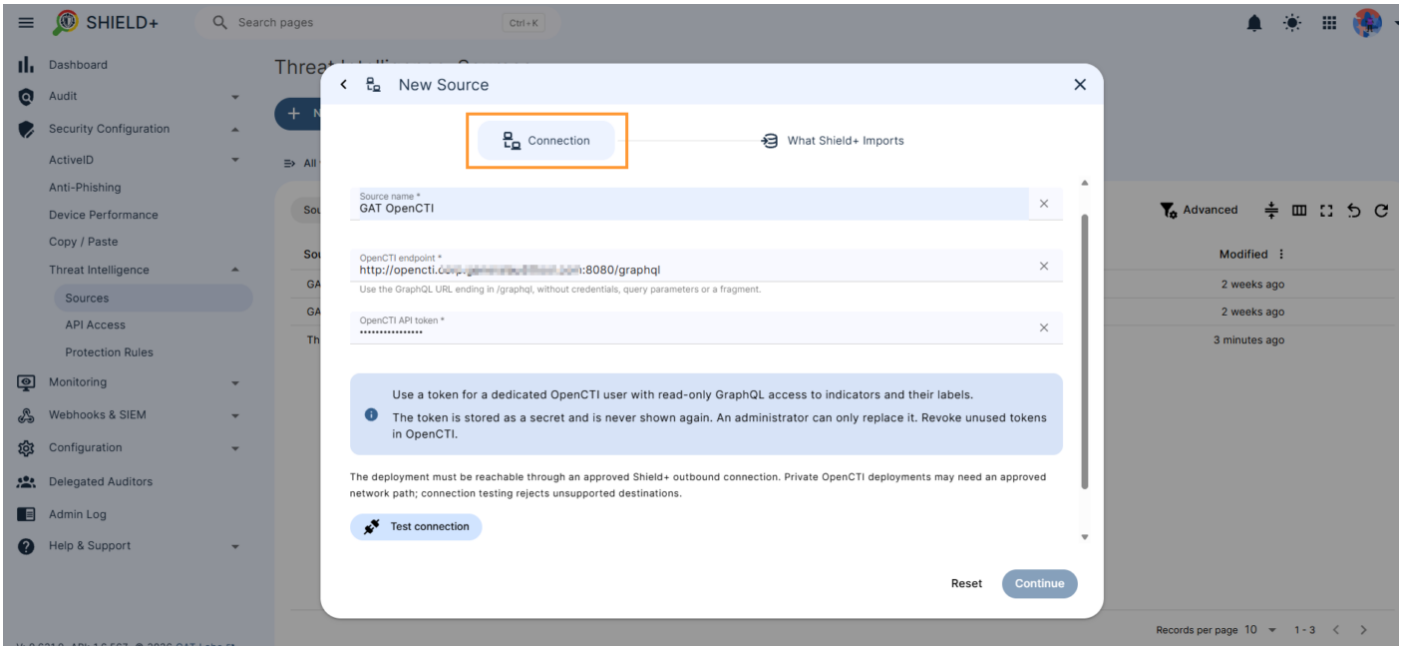


Fill in the required fields.

Use a dedicated read-only API user in this customer’s OpenCTI deployment. That user’s access rights determine which intelligence Shield+ can read.

Connection

- Source name - enter the name of the source
- OpenCTI endpoint - enter the URL
- OpenCTI API token - Use a token for a dedicated OpenCTI user with read-only GraphQL access to indicators and their labels.
  - The token is stored as a secret and is never shown again. An administrator can only replace it. Revoke unused tokens in OpenCTI.
- The deployment must be reachable through an approved Shield+ outbound connection. Private OpenCTI deployments may need an approved network path; connection testing rejects unsupported destinations.
- Test the connection and verify it.
- Click **Continue** to open **What Shield+ Imports**. If Continue is unavailable, check all required fields and repeat Test connection.



Choose labels and save the source

A **label** is a tag attached to an indicator in OpenCTI. An indicator is an address, such as a website URL or domain, supplied by a threat-intelligence feed. Labels help select which part of that feed Shield+ should import. They are managed in OpenCTI; you select existing labels here rather than inventing new ones.

- Read the short blue summary. Open the expandable help sections if you want more detail.

- Click **OpenCTI labels**.
  - Some suggestions appear.
  - If a label is not immediately visible, type abuse, then click the matching result to select it.
- In the same field, type clickfix and select that result too.
  - Both selected labels should remain visible as chips.
  - Typing text alone does not select a label.
- Click **Submit** to save the Source.
  - Return to Sources and find **OpenCTI training**.

What selecting both means: an indicator needs *at least one* selected label. An indicator labelled abuse, clickfix, or both can qualify.

- These are examples from this test instance; another customer may use different labels.

If either label is missing, check spelling and search separately.

- Do not substitute a different label just to continue.

Synchronize: bring the addresses into Shield+

- Open the saved Source's menu and choose **Synchronize**.
  - The menu may be available on the source row or in **Source Details → More** (three dots).
- Open **Source Details** and check the Synchronization section.
  - Refresh/reopen the details while the run is in progress.
- Continue only when the status is **Completed**, the last successful synchronization is recent, and **Active entries** are greater than zero.

Synchronization reads OpenCTI and prepares addresses for Shield+ to use. You do not add individual OpenCTI entries in Shield+.

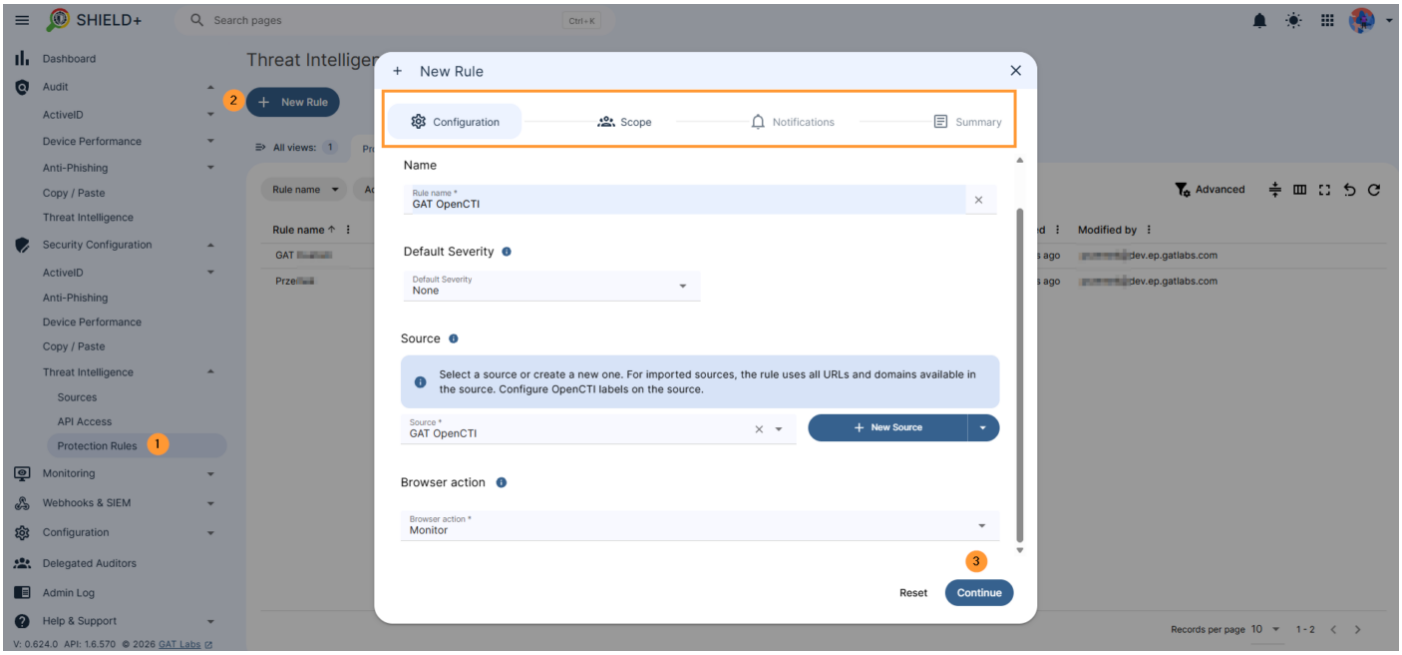
> A Source can import up to 1,000,000 accepted indicators.

Create a blocking Protection Rule

Navigate to **Security Configuration > Threat Intelligence > Protection rule > New Rule**

Fill in the required info

- Configuration - fill in the details
  - Name - enter a name
  - Default severity - select the severity needed
  - **Source** > select the saved **OpenCTI training source**
  - Set **Browser action** to **Block**.
    - The default is Monitor, which records matches but does not prevent the page from opening.
  - Click **Continue**.

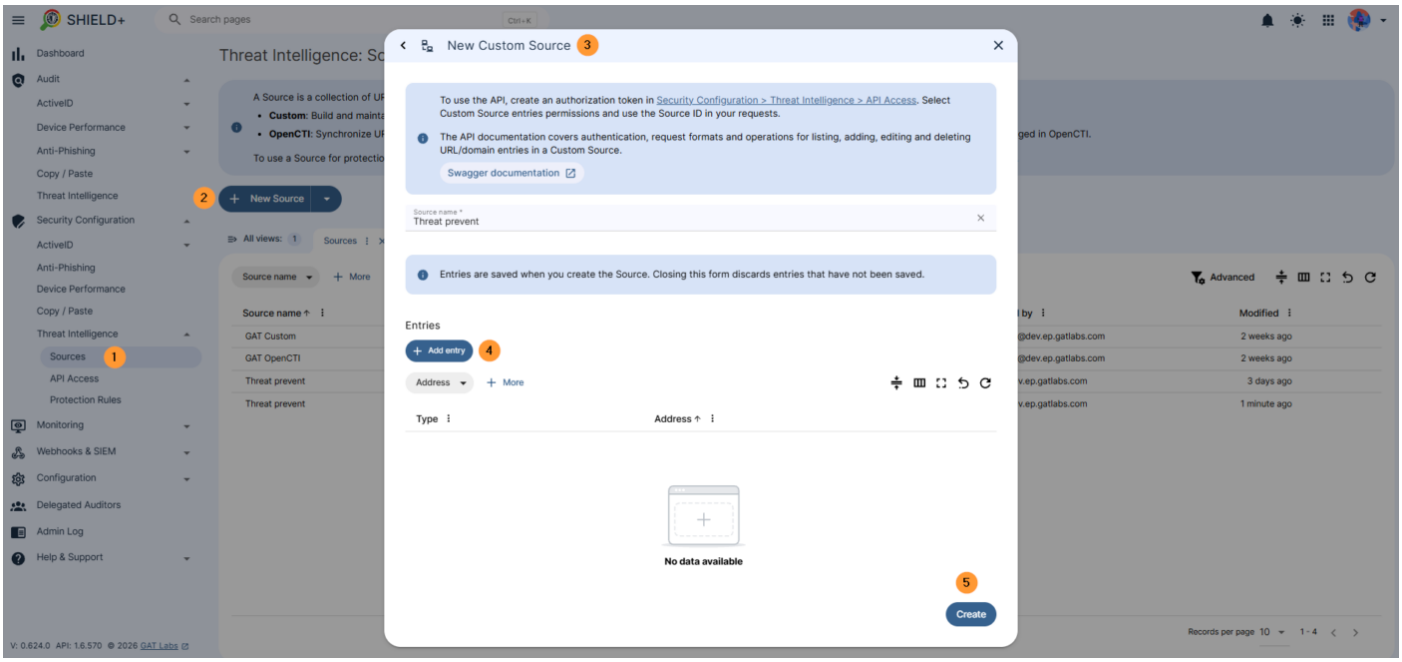


- Scope - select the users who will have the rule applied.
  - On **Scope**, change **Scope type** from All users to **User**. Search for and select the exact email of the test account used by the Shield+ browser extension.
    - Confirm it appears as a selected value. Leave Excluded scope empty. Click **Continue**.
  - **Scope matters:** the administrator who creates the rule and the browser user protected by the rule can be different people. The Scope must include the account actually browsing.
- Notifications - select alert recipients and webhook & SIEM if needed.
- Summary: review the summary of the Protection rule

Custom source

Create a Custom Source and add two entries in the UI

- Open **Security Configuration > Threat Intelligence > Sources**
- Click **New Source > Custom**.
  - Enter Custom training in the Source name.
- Click **Add entry**.
  - Change **Type** to **URL** (the initial choice may be Domain).
    - Paste the exact address below into Address, then click **Create** in the Add entry dialog.



Back in the Source form, click **Add entry** again.

- Choose **Domain**, paste the hostname below, and click **Create** in that entry dialog.
- Check that the Source form lists both entries with the correct types.
  - Click the main **Create** button to create the Source and save the draft entries. Closing the Source form before this step discards the drafts.
- Find **Custom training** in Sources and open its **Source Details > Entries**.
  - Verify that both entries are present.
- Use **Copy source ID** in Source Details (the copy icon/action beside the source actions).
  - Keep that ID private in your working notes; you will paste it into the API examples later.
    - The ID is a generated value, not the name “Custom training”.

After the Source exists: Add entry, edit, and delete operations on its Entries table save immediately. Updating the Source name is a separate action. Entries created through the API appear in this same table; refresh or reopen details if needed.

No synchronization step: Custom entries are maintained directly in Shield+. You do not select OpenCTI labels or run Synchronize for a Custom Source.

Create the Custom blocking rule

Navigate to **Security Configuration > Threat Intelligence > Protection rule > New Rule**

Fill in the required info.

- Configuration - fill in the details
  - Name - enter a name
  - Default severity - select the severity needed
  - **Source** > Enter Custom training > Block in Rule name.
  - Set **Browser action** to **Block**.
    - The default is Monitor and will not block pages
  - Click **Continue**.
- Scope - select the users who will have the rule applied.
  - On **Scope**, change **Scope type** from All users to **User**. Search for and select the exact email of the test account used by the Shield+ browser extension.
    - Confirm it appears as a selected value. Click **Continue**.
  - **Scope matters:** the administrator who creates the rule and the browser user protected by the rule can be different people. The Scope must include the account actually browsing.
- Notifications - select alert recipients and webhook & SIEM if needed.
- Summary: review the summary of the Protection rule

Create a GAT API token

The API is an alternative way to manage the same entries, for example, from a security automation tool. Swagger is an interactive documentation page where you can try those requests without writing a program.

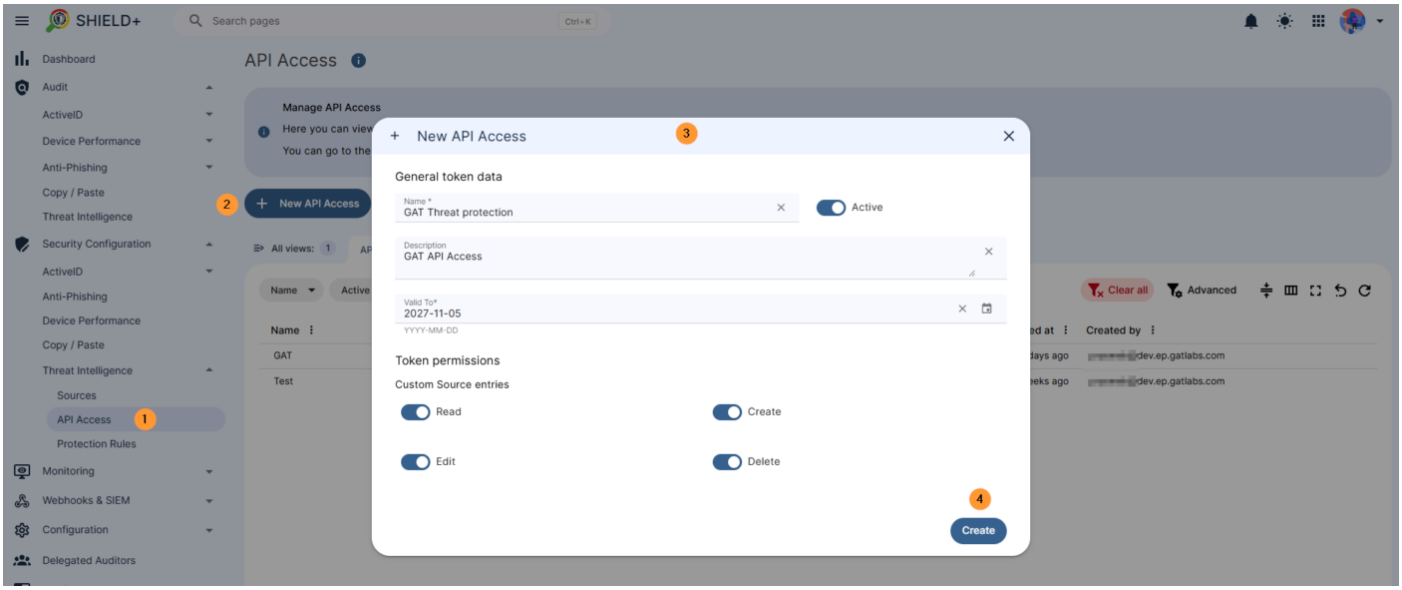
You first need a **GAT API token.**

- Open **Security Configuration > Threat Intelligence > API Access**
- Click **New API Access**.
  - Enter Custom training API as Name.
    - Leave **Active** switched on.

- Choose a future **Valid To** date, for example, seven days from today, using the date picker.
  - The date must be in the future and no more than one year away.
  - The blank date in the screenshot must be filled before creation.
- Under **Token permissions > Custom Source entries**, enable **Read, Create, Edit, and Delete** for this complete walkthrough.
  - For a real integration, give it only the permissions it needs.
- Click **Create**.

In the token preview, use the copy button to copy the generated token. Keep it in a private, secure place for the next steps, not in this document or a screenshot.

Note: The token belongs to you and its granted operations. Opening API Access from a Source does not restrict it to that Source alone. Always use the intended training Source ID in your requests.



Open Swagger, authorize, and list the entries

- Click **Swagger documentation** in API Access or Custom Source Details.
  - You can also open Swagger > Shield+ API directly.

- At the top, make sure to **select a definition = Shield+ API**.
  - Use the server offered by the production page, not a localhost server shown in these local screenshots.
- Click **Authorize**. Under **ApiTokenAuth**, confirm the header name is X-GatLabs-Token. Paste your GAT API token into **Value**.
  - Paste only the token: no Bearer prefix, quotation marks, or OpenCTI token.
- Click **Apply credentials** (some versions label this button Authorize), then **Close**.
- Find the section **Customer-managed TI entries**. Expand **POST /source_entry/v1/get_page** , labelled “List entries in a customer-managed Source”.
- Click **Try it out**.
- Replace the entire Request body with the JSON.
- Replace PASTE_YOUR_SOURCE_ID_HERE with the Source ID you copied in section
  - Keep the quotation marks around the ID.
  - Click **Execute**. Scroll to **Server response → Response body**. This is the real result.
  - The separate “Example Value” area is documentation, not the response to your request.
  - Confirm HTTP 200, success: true, and a pageData list containing the UI entries https://example.com/ and example.org.
  - Page numbering starts at zero.

Monitoring

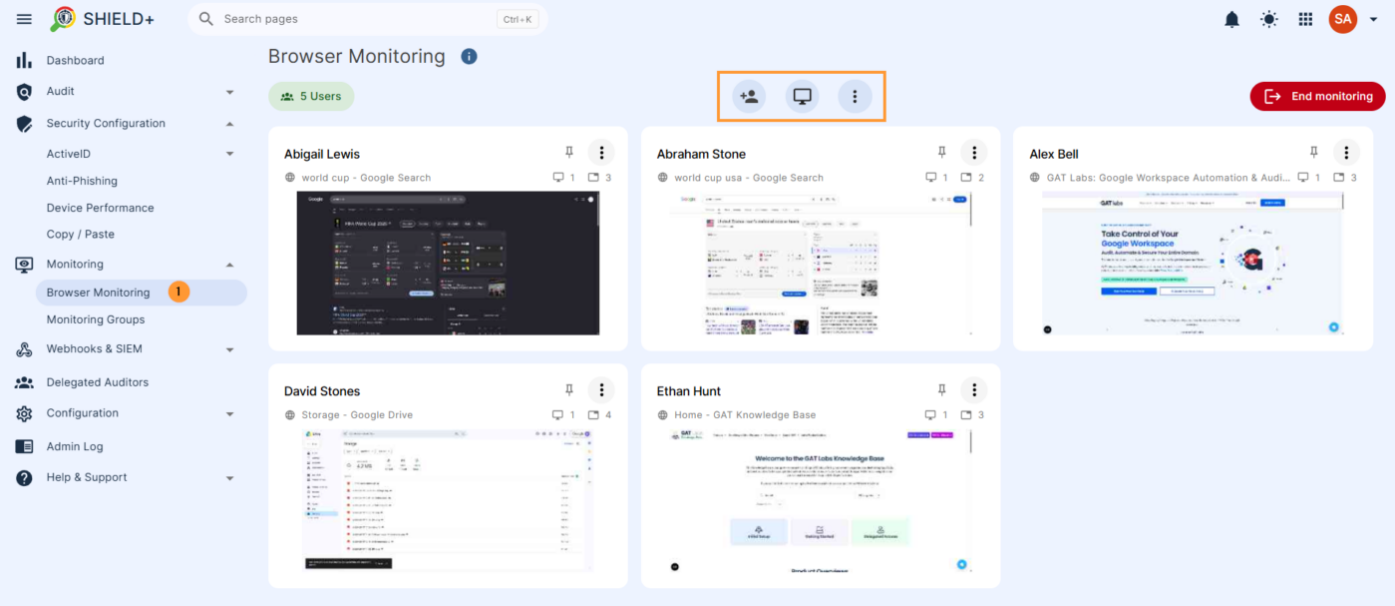
Real-time visibility into users' Chrome browser activity. The monitored user's browser always displays a visible indicator that monitoring is active.

> (Note, the user browser will indicate that it is being actively monitored.)

Browser Monitoring

The Admin can view one or more users' live browser screens in real time. After selecting a monitoring target (user, group, or OU), the admin sees thumbnails of all open tabs and windows. Available tab actions: switch the user to a specific tab, open a new tab for the user at a given URL, close a tab on the user's behalf, or open a copy of the tab in the admin's own browser.

Navigate to **Shield+ > Monitoring > Browser monitoring > Scope - select the scope of users to monitor**

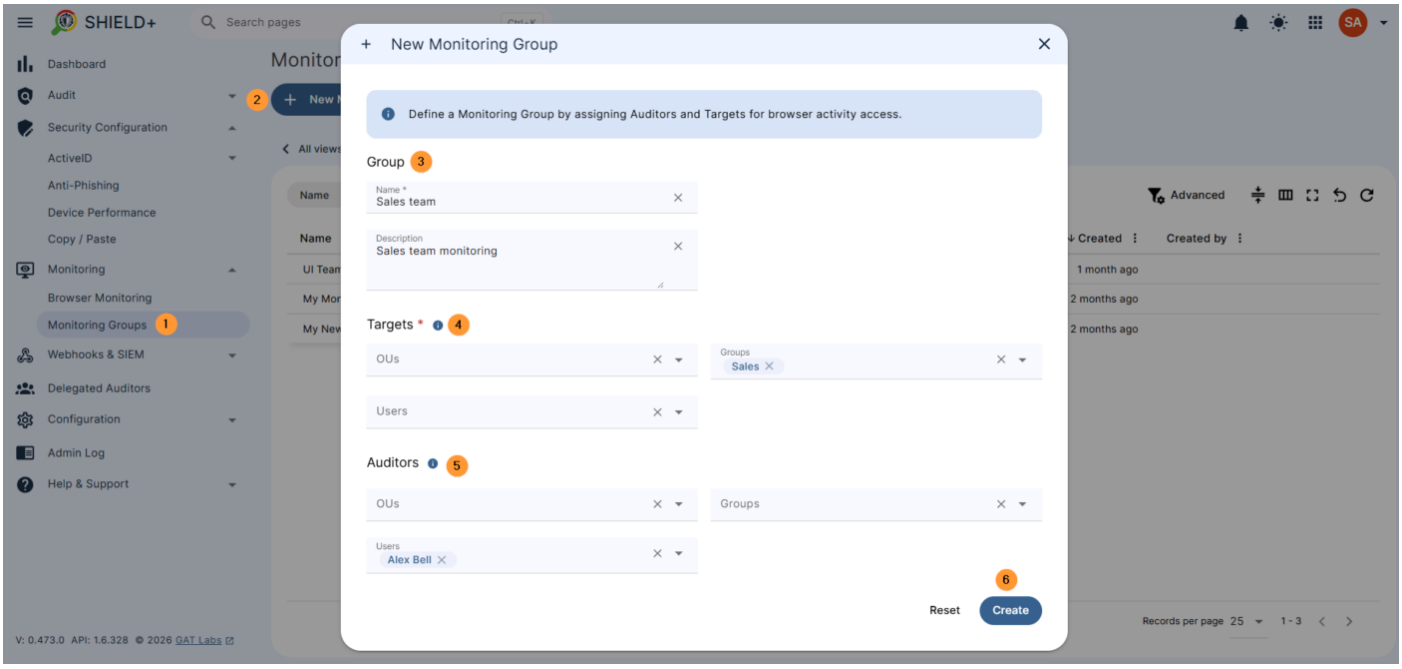


Monitoring Groups

Pre-configured groups that delegate browser monitoring authority to supervisors or managers without requiring admin involvement each time.

Each group defines Targets (users whose browsers can be monitored) and Auditors (people permitted to start monitoring sessions). Once a group is set up, any assigned auditor can initiate monitoring directly from the group's page.

Navigate to **Shield+ > Monitoring > Monitoring groups > New monitoring group**



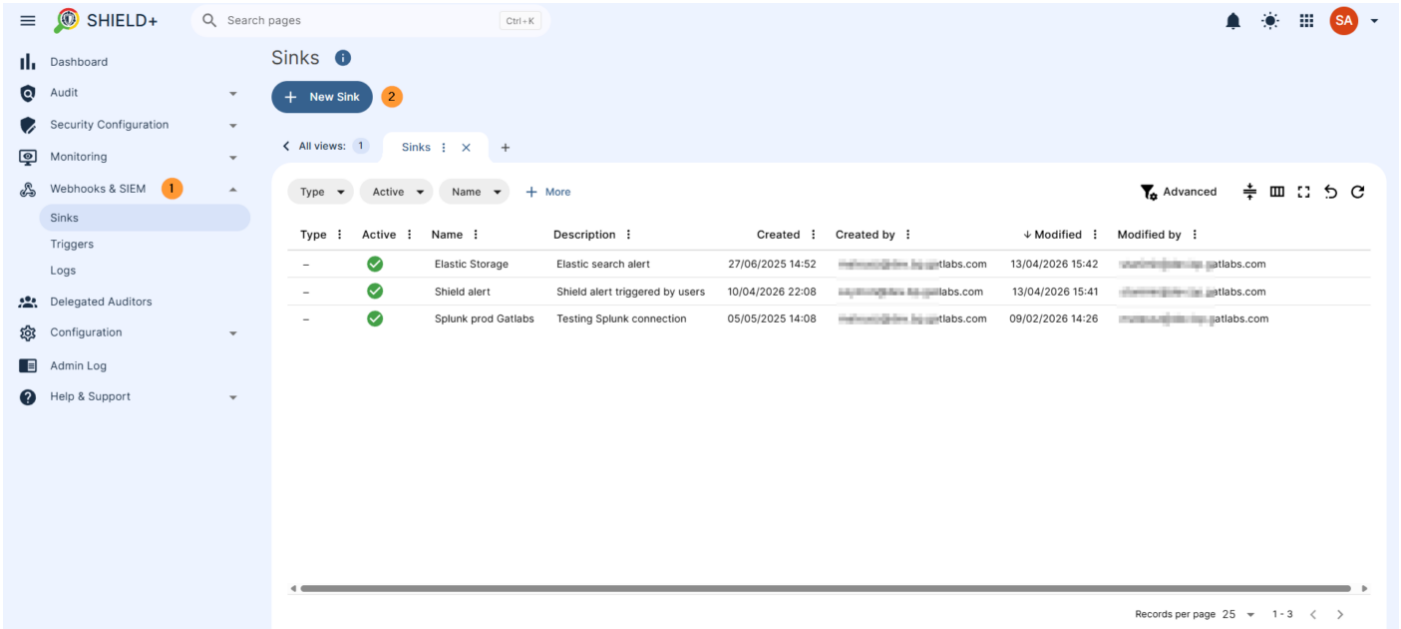
Webhooks & SIEM

Forwards Shield+ security events to external systems such as SIEM platforms, log aggregators, or custom webhook endpoints.

- **Sinks** - Configure the outbound destinations where Shield+ delivers event payloads. A Sink is a named endpoint (webhook URL or SIEM receiver) that accepts incoming events.
- **Triggers** -Rules that map specific Shield+ event types (e.g., TypingID alert, anti-phishing block, inactivity lock) to specific Sinks. Controls which events get forwarded where.
- **Logs** - A delivery log of all outbound SIEM and webhook events: what was sent, the destination Sink, and the timestamp.

Navigate to **Shield+ > Webhooks & SIEMs > New Sink > New Sink**

Fill in the details. Choose the receiving Sink system (e.g., SIEM) and configure credentials. Depending on the type of the receiver system, you need to provide the full URL and either an authorization token or a set of HTTP headers to be included in every request.

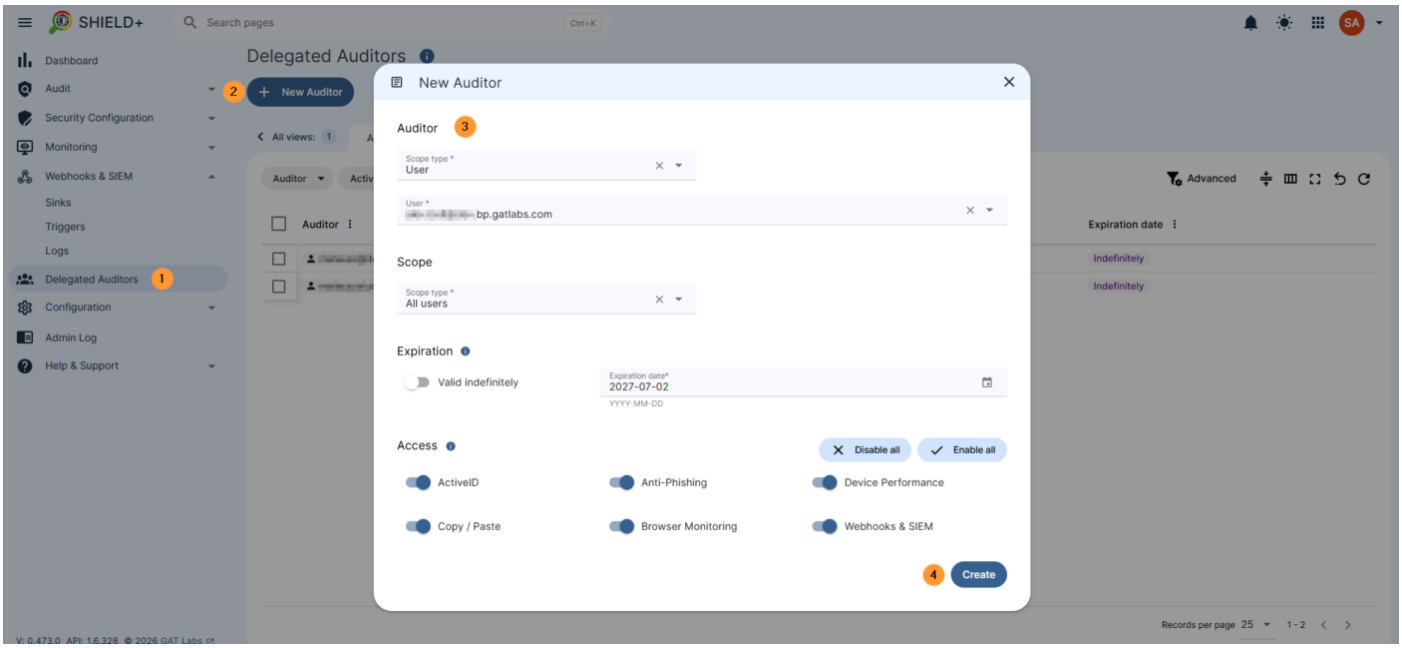


Delegated Auditors

Delegate Shield+ audit access to users who are not domain administrators. Auditors can be granted access to specific feature areas - ActiveID, Anti-Phishing, Device Performance, Copy/Paste, Browser Monitoring, or Webhooks & SIEM - and optionally scoped to a specific set of users, groups, or organizational units, so each auditor sees only the data relevant to their team.

Navigate to Shield+ > Delegated auditor

Fill in the details, select the scope type, who will be the auditor, and the scope - what users will be monitored



Configuration

Admin-only settings for the Shield+ deployment.

Manage the deployment of the Shield+ browser extension across the domain. The extension is installed on user machines and is the component that collects typing patterns, enforces copy/paste policies, enables browser monitoring, and displays anti-phishing blocking pages.

Admin Log

A complete audit trail of all administrative actions taken within Shield+: logins, creation, update, and deletion of alert rules and policies, browser monitoring session starts and stops, configuration changes, and data exports.

Each entry records the responsible administrator, the timestamp, and the full details of every change, including before-and-after comparisons where applicable.

Conclusion: Why Shield+ is Essential for Your Enterprise

Managing security across a distributed enterprise domain requires visibility that goes beyond static firewalls and standard login prompts. **Shield+** delivers this exact layer of deep, behavioral protection right at the edge - inside the browser where your users spend their workday.

Key Benefits for Enterprise Admins

- **Zero-Trust Identity Protection:** By utilizing Machine Learning to flag anomalous typing patterns and enforcing Passkey or session-termination challenges, Shield+ stops active session hijacking and insider threats in their tracks.
- **Granular Data & Compliance Control:** From blocking malicious URLs out-of-the-box to restricting copy/paste data leaks on sensitive websites, you have complete control over data movement.
- **Operational Efficiency:** The platform shifts your team from reactive auditing to proactive management. With real-time browser monitoring, automated alerts, delegated access for team managers, and seamless SIEM/Webhook integration (Splunk, Elasticsearch, etc.), security incidents are localized, logged, and mitigated instantly.

By deploying Shield+, you aren’t just monitoring your enterprise domain; you are actively hardening it against the modern threat landscape while maintaining full visibility and administrative control.

Related Posts

- How to install GAT Shield+