GAT Shield Login Control

Chrome Audit & Management · https://gatlabs.com/knowledge/tech-tips/gat-shield-login-control/

Control Google Workspace Logins with GAT Shield Login Control

GAT Shield allows admins to set up a **Login Control rule** for users of their domain. By setting up this rule, admins can control whether users can log in to their domain or not.

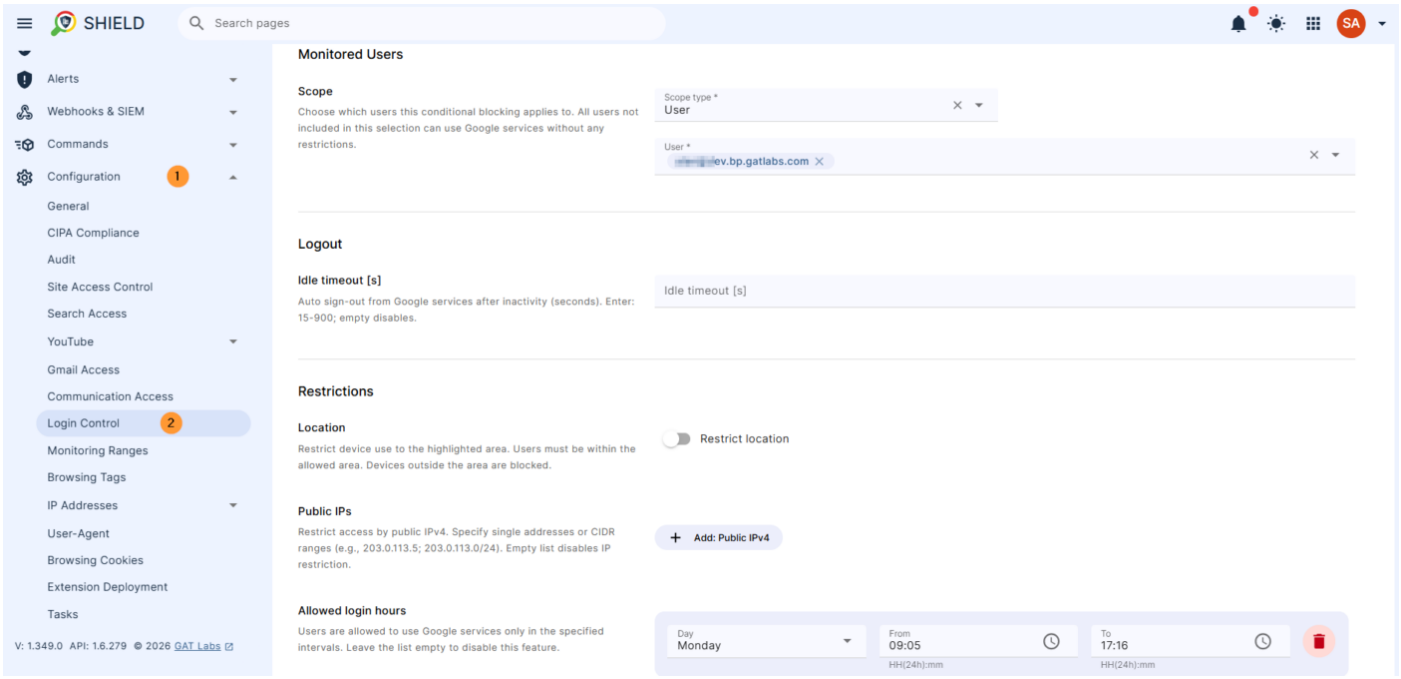
It works by disabling users from logging into your domain **based on different criteria.**

This type of Login control can be set up from the GAT Shield console.

Create a Login Control Rule in GAT Shield

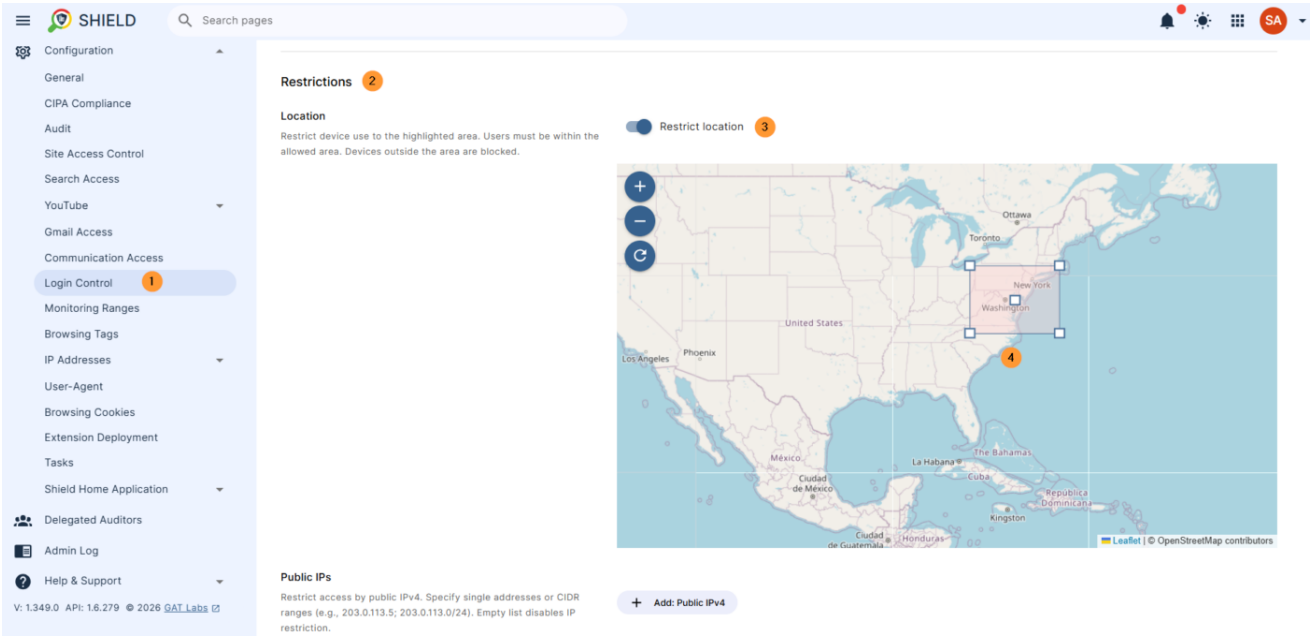
Open the dashboard

Navigate to **GAT Shield (1) → Configuration (2) → Login Control (3)**



In the Login Control window, fill in the rule details.

- **Scope** – Choose which users this conditional blocking applies to. All users not included in this selection can use Google services without any restrictions.
- **Logout** -Set the idle timeout (in seconds). After this time, Shield will log the user's device out of your domain. The entered value must be between 15 and 900 seconds, or empty to disable logout.
- **Restrictions –** set different restrictions such as Lication Public IPs and Allowed login hours.
  - **Location** – Restrict device use to the highlighted area. Users must be within the allowed area. Devices outside the area are blocked.



  - **Public IPs** – Allow only selected public IPs to log in to your domain.
    - An empty list means GAT Shield will allow all users to log in to your domain from any network.
    - Entered values should be IPv4 addresses only. Use direct (eg. 72.14.0.154) or network addresses (eg. 64.233.187.99/8). All network addresses should end with a CIDR.

- **Allowed login hours** – Users are allowed to use Google services only in the specified intervals. Leave the list empty to disable this feature.
  - Select when the configuration should be active.
  - By default, when no time restriction is added, the configuration will always be active.
  - To change it, select days and time ranges when the configuration will be active.
- **Timezone** – If enabled, the user's local time zone will override the time zone set in the General configuration.

- Toggle on/off the user of local time zone

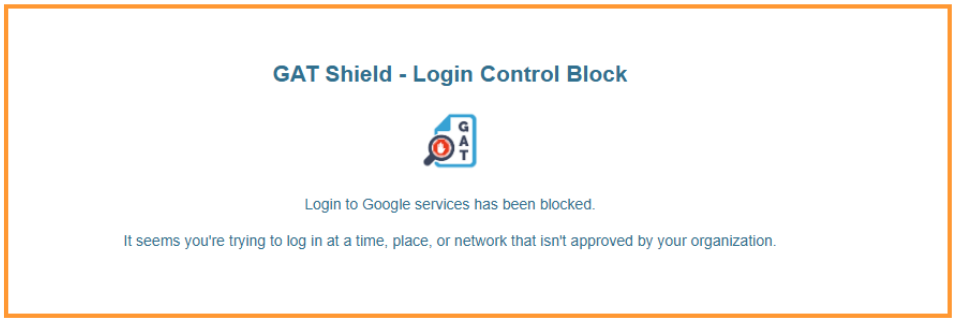
- **Update –** once the fields you want are filled in, click on **Update** to apply the rule

Result

When the Login control is enabled, the rule is applied. The users will be logged out if the rule is applied to them. The logout will happen from Google logins only, from different services where users is logged in with their Google workspace account

- Gmail
- Google Drive
- Google classrooms
- Google calendars
- All Google domain account services

The users will see a message as below.



Log in to Google services has been blocked at this time.

FAQ's: Login Control Rule

Q: How can I restrict Google Workspace logins by IP or location using GAT Shield?

A: You can use GAT Shield’s Login Control rule to block users from logging into your domain unless

they meet specific criteria, such as being within a geographic location or using an approved public IP. Admins can also configure logout timeouts and restrict access during certain hours.

Q: What happens when a GAT Shield login control rule is triggered?
A: When the rule is active and a user does not meet the login conditions (such as being outside the allowed IP range or time window), they will be automatically logged out of their Google Workspace account. This includes services like Gmail, Drive, Calendar, and Classroom.

Q: Can I apply GAT Shield login control rules to specific users or groups?
A: Yes. GAT Shield allows you to target login control rules by individual user, group, or organisational unit. This gives admins flexibility to apply different access policies across departments or user roles.

Related Posts

- Chrome Login Control Events in GAT Shield
- User logins IP/Location correction