Chrome Login Control Events in GAT Shield

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

Chrome Login Control Events in GAT Shield

GAT Shield is an extension deployed on users' Chrome browsers. It allows the Google Workspace Admins to control the login activity of the end-users and manage the users' browsing activity while logged in the Chrome browser.

Embedded media:
https://www.youtube.com/embed/JXLt59a3QFg?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_loa

How to configure the Login Control module.

To set up Login Control, navigate to **GAT Shield > Configuration > Login Control**

Set up the fields as per your requirements and then click **Save.**

This module allows the Admins to block Google-related pages (except YouTube). As a result, the end user is redirected to a dedicated block page. Note: This does not prevent users from logging in and performing browsing activity on their device.

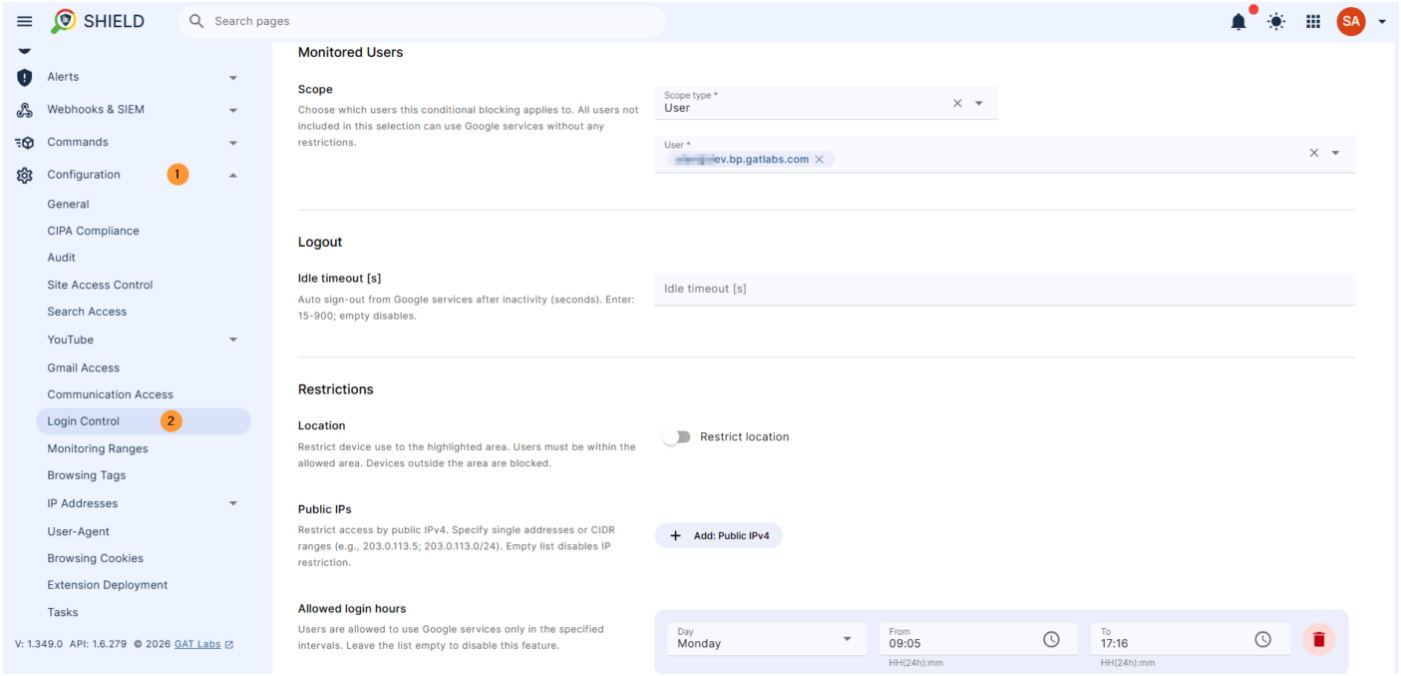
> Note that it may take a while for settings to propagate to extensions.

- **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

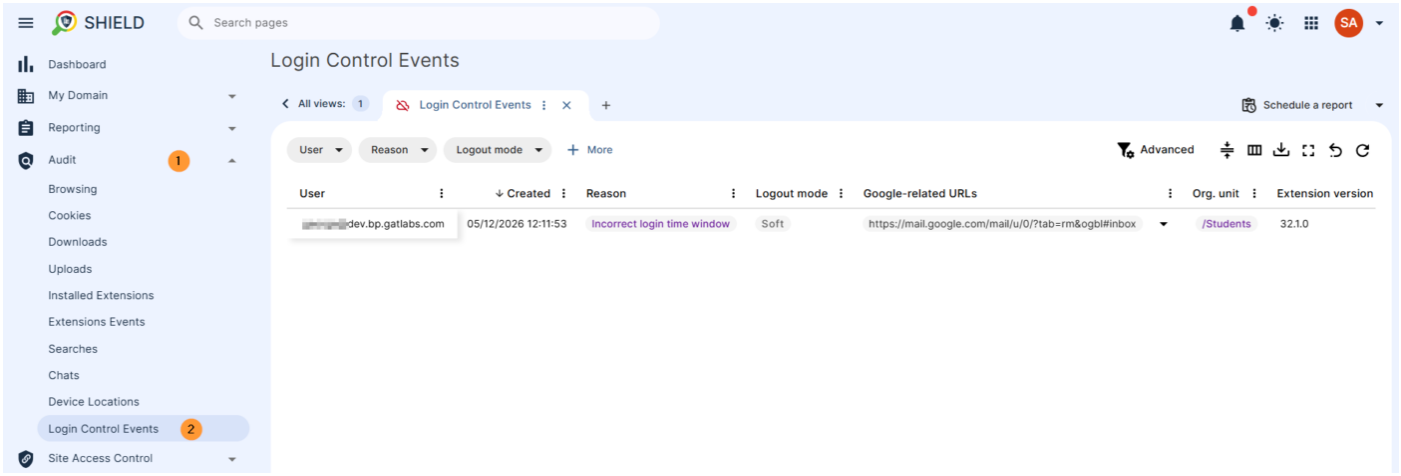
- **Update -** once the fields you want are filled in, click on **Update** to apply the rule



Login Control Events

The result of all the activities of users reported via **Login Control** can now be seen by Admins in the **Login Control Events** tab.

To access the reports, navigate to **GAT Shield > Audit > Login Control Events**



The following details of the user activity can be seen:

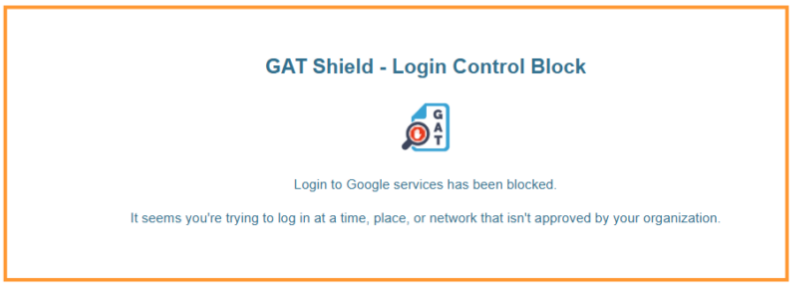
- **User** - view the user for whom the Login Control event was triggered
- **Created** - when the Login Control event was triggered
- **Reason** - the reason for the Login Control event
- **Logout mode** - view if the user was logged out from all of their accounts
- **Logout session URLs** - view the pages from which the user was logged out

- **Org. Unit** - the org. unit of the users
- **Usage groups** - view groups where the user is a member of
- **Actions** - view the details for the selected user
  - User info
  - Device info

Result for end user

The end-user will view this GAT+ default screen.





FAQ

Q1: Will enabling Login Control restrictions completely prevent users from browsing the internet or logging into their devices?

A1: No. The Login Control module only blocks access to Google-related pages (with the exception of YouTube), redirecting the end-user to a dedicated GAT+ block page. It does not prevent users from logging into their physical devices or conducting other non-Google browsing activities.

Q2: How should network addresses be formatted when restricting access to specific Public IPs?

A2: When configuring Public IPs, you must use IPv4 addresses only. You can enter direct addresses (e.g., `72.14.0.154`) or network addresses (e.g., `64.233.187.99/8`). Note that all network addresses must end with a CIDR notation. Leaving this list empty will allow users to log in from

any network.

Related Posts

- GAT Shield Extension – How to Deploy
- User Chrome Device History Explorer within GAT Shield console
- How to Locate and Track Devices with GAT Shield?