# IMTLazarus extension deployment in Google Workspace and security measures

## IMTLazarus Administrators

C Arteagabeitia 41, Barakaldo
48902, Vizcaya, Basque Country (Spain)

(+34) 94 437 78 01

www.imtlazarus.com

# IMTLazarus extension deployment in Google Workspace and security measures

IMTLazarus Administrators

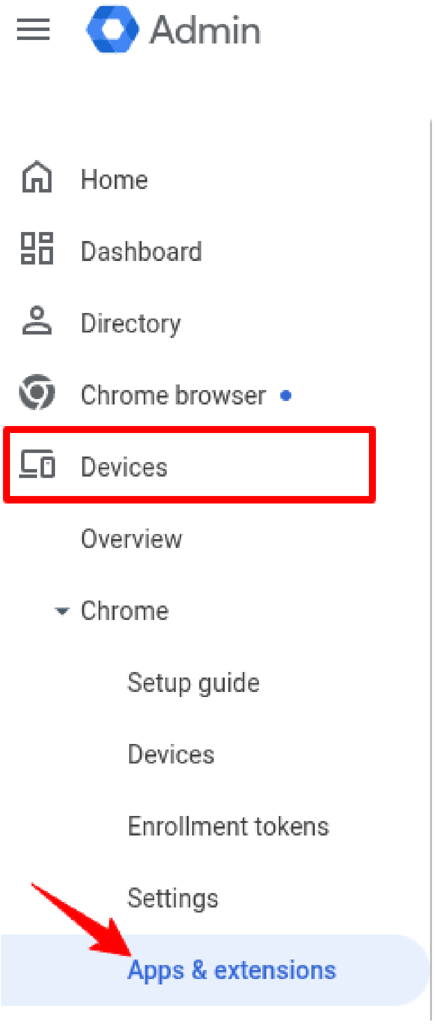
## Index

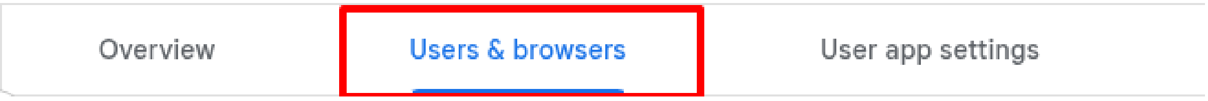
## Introduction

For IMTLazarus to work correctly on Chrome devices, IMTLazarus recommends performing the following actions within the Google Workspace Admin Console. The first step is mandatory. The following steps are recommended to prevent users from bypassing the security and for IMTLazarus to work properly.

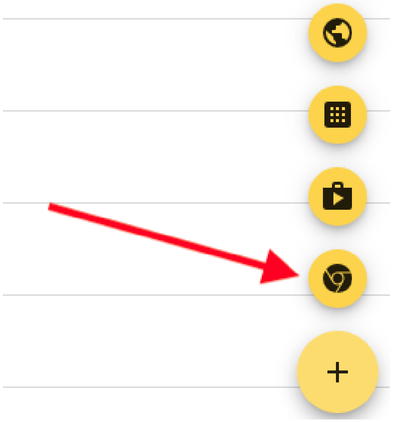
# 1. Deploy the IMTLazarus extension:

From the Google Workspace Admin Console, in the left-hand menu, expand the Devices menu > Chrome > Chrome Devices Apps and extensions and click on Users and browsers:

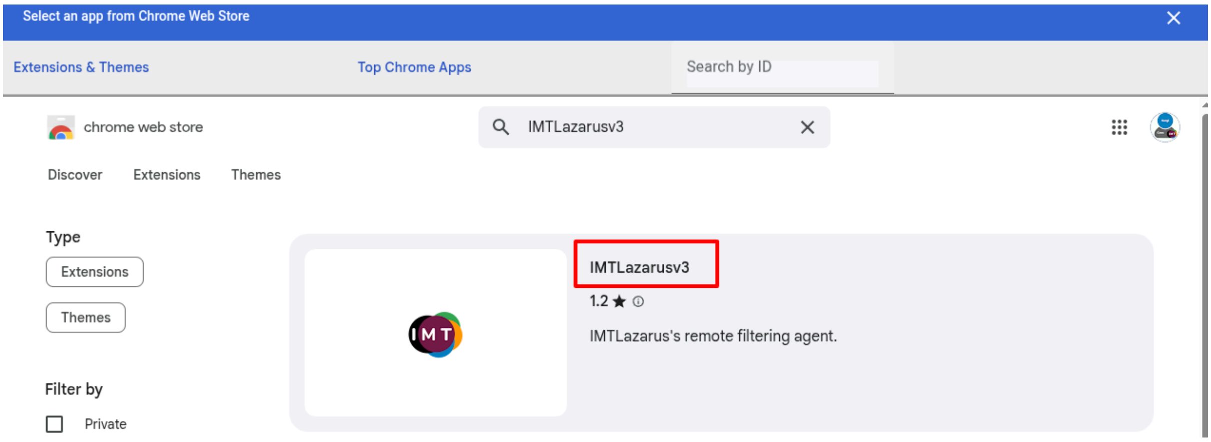


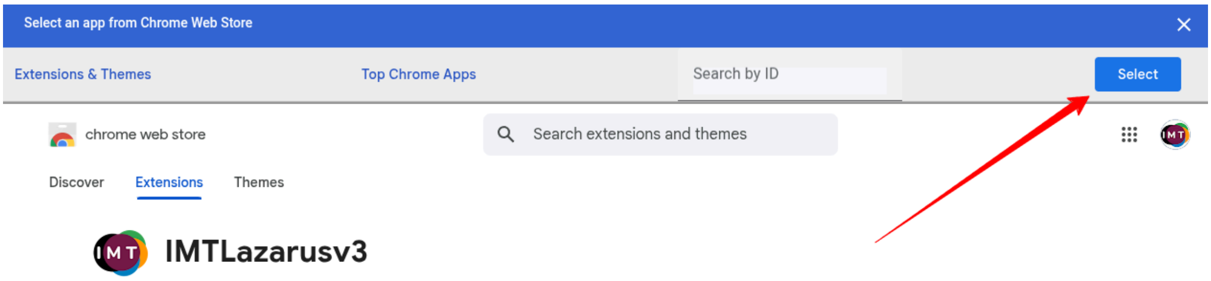


Once on this screen, in the left side of the screen you will select the Organizational Unit that you want to work on. Then, within the USERS & BROWSERS tab, click on the yellow “+” button that you will find at the bottom right of the screen and then click on the Chrome icon:

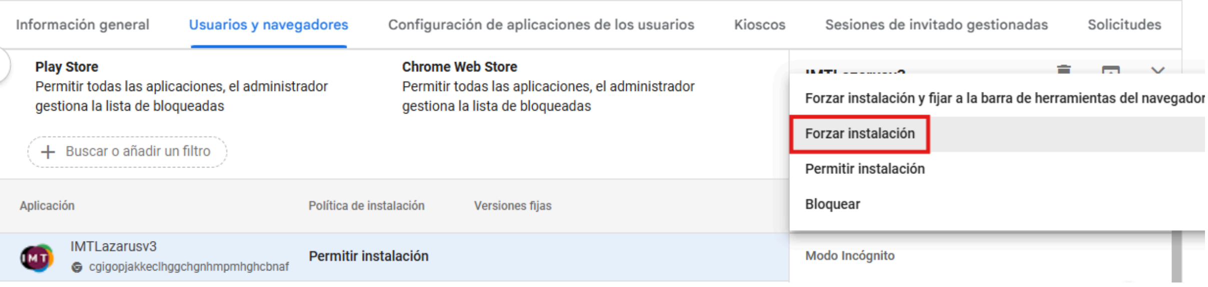


This will open a new window called “Select an app from the Chrome Web Store” from which you will have to search for the extension “IMTLazarusv3”, click on it and then on the “Select” button at the top right of the window:





Once the extension is available, verify that you have selected the correct Organizational Unit and select the Installation Policy “Force installation” and click on the "SAVE” button that will appear at the top right of the screen to save the changes.



Información general | Usuarios y navegadores | Configuración de aplicaciones de los usuarios | Kioscos | Sesiones de invitado gestionadas | Solicitudes

**Play Store**
Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas

**Chrome Web Store**
Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas

+ Buscar o añadir un filtro

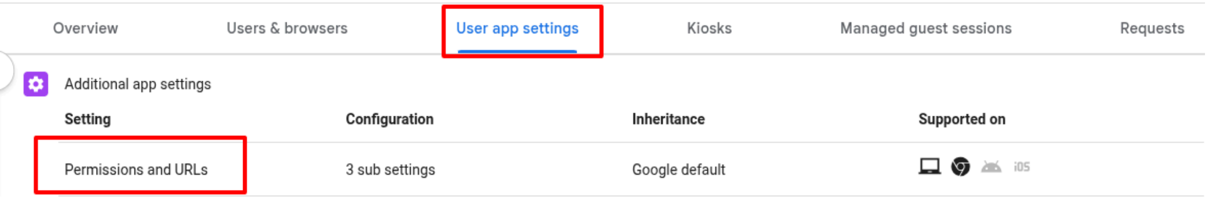
| Aplicación | Política de instalación | Versiones fijas |
|---|---|---|
| IMTLazarusv3<br>cgigopjakkeclhggchgnhmpmhghcbnaf | Permitir instalación | |

Forzar instalación y fijar a la barra de herramientas del navegador
Forzar instalación
Permitir instalación
Bloquear

Modo Incógnito

If you have an older version of the IMTLazarus extension installed, remove that version from this screen:

Without leaving that screen, click on the “User app settings” tab and in the “Additional app settings” section click on the setting“ Permissions and URLs”:



Overview | Users & browsers | User app settings | Kiosks | Managed guest sessions | Requests

Additional app settings

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Permissions and URLs | 3 sub settings | Google default | iOS |

Verified that <u>you DO NOT have the following parameters checked.</u>:

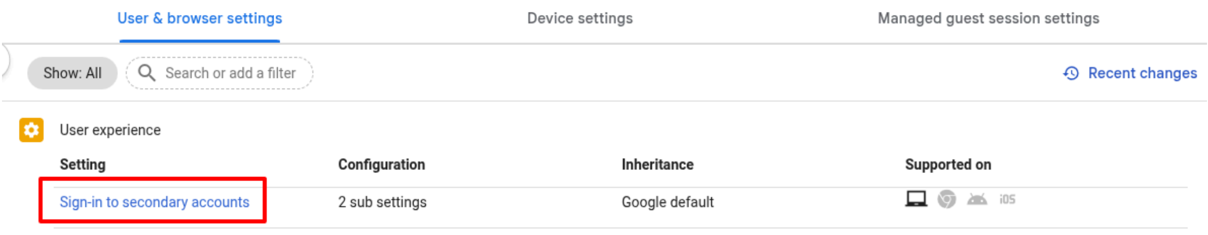
- Desktop capture
- Block Web requests
- Web requests

## 2. Prevent login with accounts outside the domain and incognito mode:

From the Google Workspace Admin Console, expand the Devices menu > Chrome > Settings and click on the “Users & browsers settings” tab.

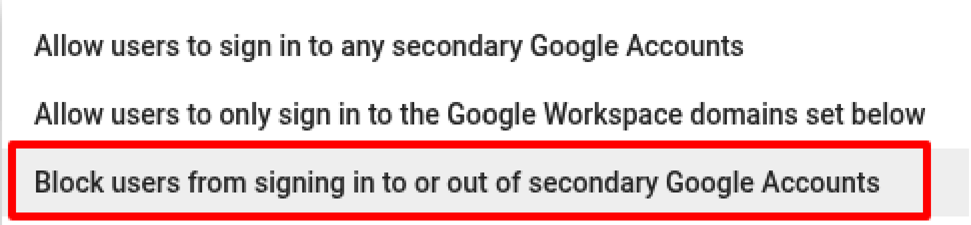
Once in this screen, on the left side of the screen select the Organizational Unit on which you want to work.

Go to the section “User experience” and click in the “Sign-in to secondary accounts” settings select the option “Block users from signing in or out of secondary Google accounts”. To apply the changes, click the “SAVE" button at the top right of the screen.



User experience

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Sign-in to secondary accounts | 2 sub settings | Google default | iOS |

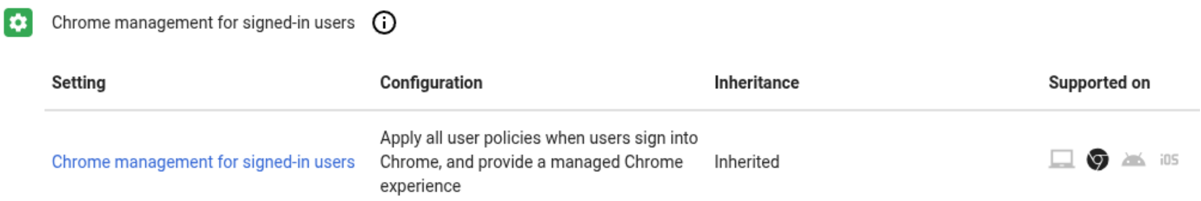


Allow users to sign in to any secondary Google Accounts

Allow users to only sign in to the Google Workspace domains set below

Block users from signing in to or out of secondary Google Accounts

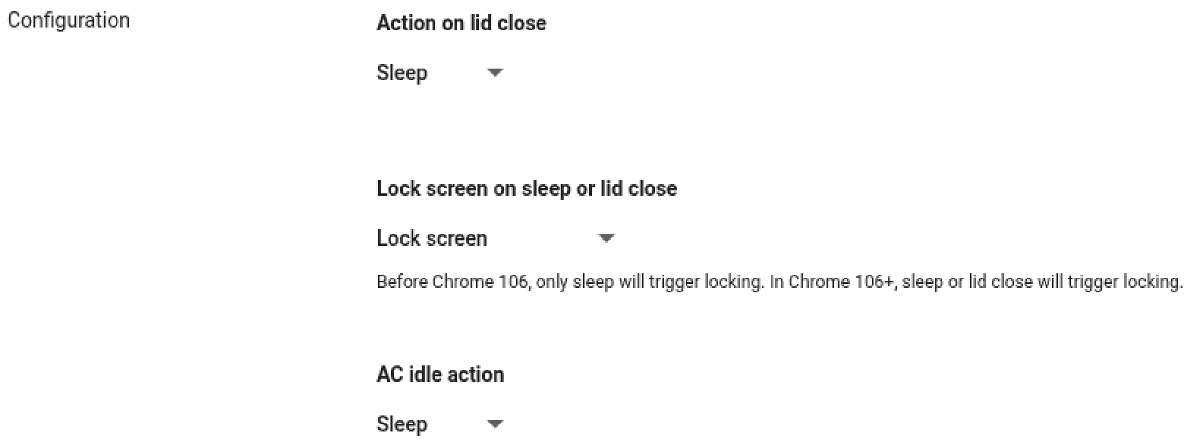
Without leaving that screen, in the section “Chrome management for signed-in users” select the option “Apply all user policies when users sign in to Chrome and provide a managed Chrome experience”.



Chrome management for signed-in users

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Chrome management for signed-in users | Apply all user policies when users sign into Chrome, and provide a managed Chrome experience | Inherited | iOS |

In the "Power and shutdown" section, select the "Idle settings" and within the setting "Lock screen on sleep or lid close" select the option "Lock screen":



Configuration

Action on lid close

Sleep

Lock screen on sleep or lid close

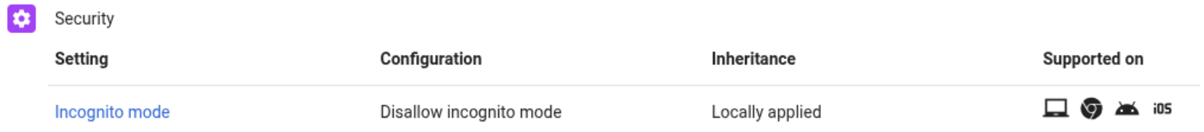
Lock screen

Before Chrome 106, only sleep will trigger locking. In Chrome 106+, sleep or lid close will trigger locking.

AC idle action

Sleep

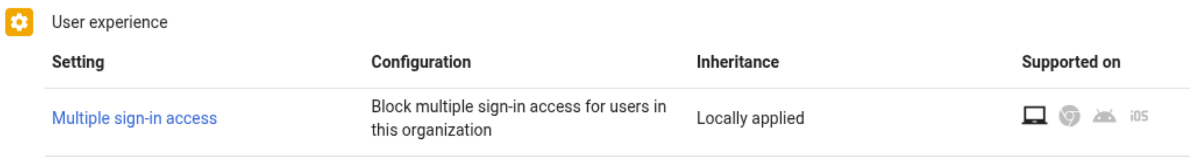
In the "Security" section, click on the setting "Incognito mode" and select the option "Disallow incognito mode":



Security

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Incognito mode | Disallow incognito mode | Locally applied | iOS |

Without leaving where you are in the USER & BROWSER SETTINGS tab, go to the section "User experience" and in the setting "Multiple sign-in access" select the option "Block access via multiple logins for users of this organization".

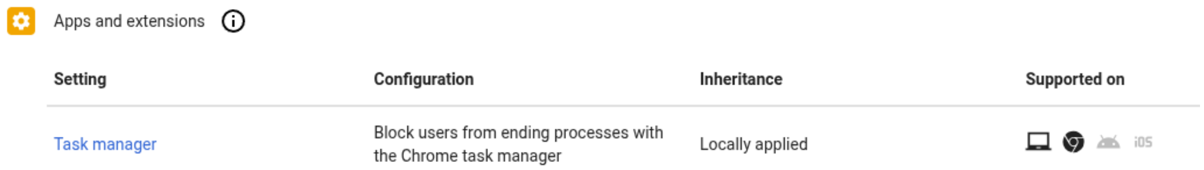


User experience

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Multiple sign-in access | Block multiple sign-in access for users in this organization | Locally applied | iOS |

## 3. Prevent users from ending processes with the Chrome task manager:

Without leaving the USER & BROWSER SETTINGS tab, go to the section “Apps and extensions”, select the option “Block users from ending processes with the Chrome task manager” and click on the "Save" button to save the changes.



Apps and extensions ⓘ

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Task manager | Block users from ending processes with the Chrome task manager | Locally applied | 💻 ◉ 🤖 iOS |

## 4. Equipment registration permissions:

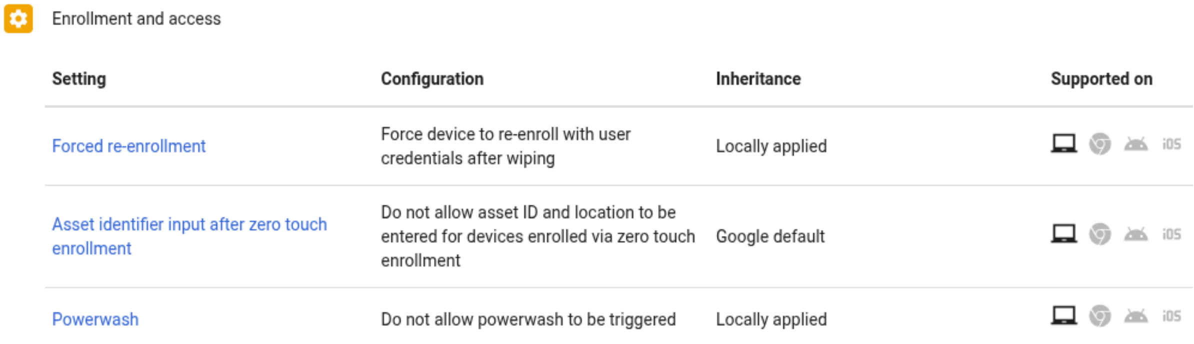
To prevent users from resetting devices to factory settings and thus uninstalling IMTLazarus and any other application, it is necessary to enable mandatory device registration. This way, if this were to happen (a reset or "powerwash" of the Chrome device), it would force the user to enroll in the Admin Console in order to use it.
To do this, in the Google Workspace Admin Console, in the left-hand menu, expand the Devices menu > Chrome > Settings and click on the Users & browsers tab.

Once on this screen, on the left side of the screen select the Organizational Unit that you want to work with.

Within this USER & BROWSER SETTINGS tab, go to the section “Enrollment controls” and click on the setting “Enrollment permissions” to set it to “Do not allow users of this organization to enroll new or re-enroll existing devices”.
Click on the “Save” button to save the changes.

Without leaving the screen, go to the DEVICE SETTINGS tab and then to the section “Enrollment and access” and mark the following:

- Forced re-enrollment: Force device to re-enroll with user credentials after wiping.
- Powerwash: Do not allow Powerwash to be triggered.



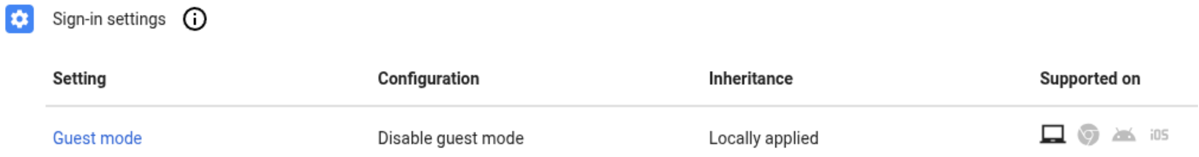
Enrollment and access

| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Forced re-enrollment | Force device to re-enroll with user credentials after wiping | Locally applied | 💻 ◎ 🤖 iOS |
| Asset identifier input after zero touch enrollment | Do not allow asset ID and location to be entered for devices enrolled via zero touch enrollment | Google default | 💻 ◎ 🤖 iOS |
| Powerwash | Do not allow powerwash to be triggered | Locally applied | 💻 ◎ 🤖 iOS |

This way, if a user performs a factory reset, they will have to return the device to the IT Admins so they can manually re-enroll it with an Administrator account.

## 5. Prevent logging in as a guest:

From the same window, click on the DEVICE SETTINGS tab, and go to the section “Sign-in settings” and then on the “Guest mode” setting select the option “Disable guest mode”and click on the save button at the bottom of the screen to save the changes.



Sign-in settings ⓘ

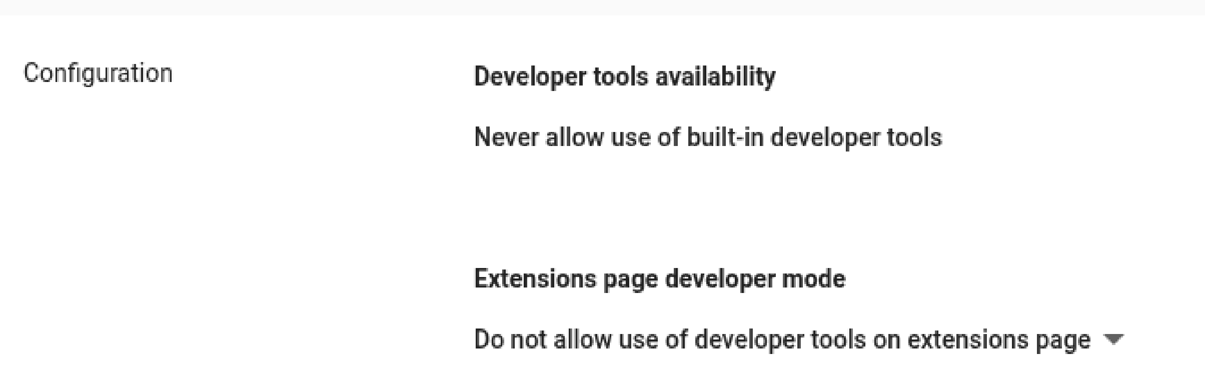
| Setting | Configuration | Inheritance | Supported on |
|---|---|---|---|
| Guest mode | Disable guest mode | Locally applied | 💻 ◎ 🤖 iOS |

# 6. Prevent developer mode:

From the Google Workspace Admin Console, in the left-hand menu, expand the Devices menu > Chrome > Settings and click on Users & browsers.

Once on this screen, on the left side of the screen select the Organizational Unit that you want to work with.

Go to the section "User experience" and in the setting "Developer tools" configure the option "Developer Tools availability" to "Never allow use of built-in developer tools" and the option "Extensions page developer mode" to "Do not allow use of developer tools on extensions page":



Configuration

Developer tools availability

Never allow use of built-in developer tools

Extensions page developer mode

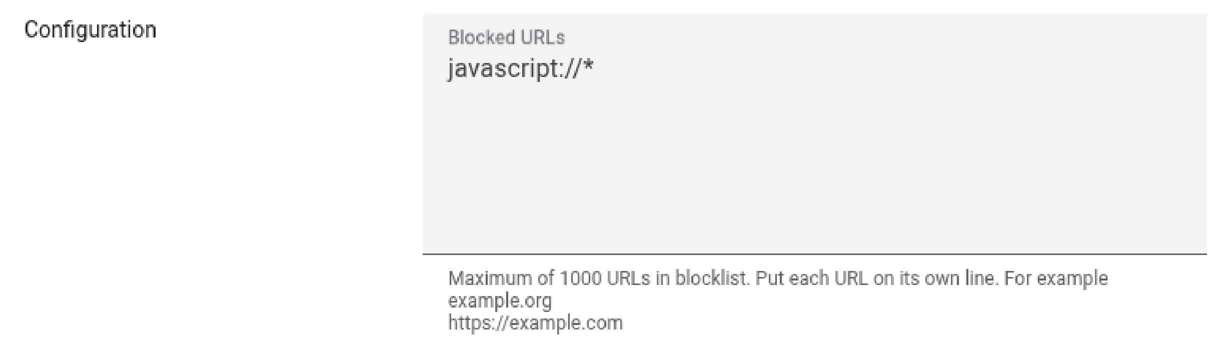
Do not allow use of developer tools on extensions page

## 7. Disable the execution of JavaScript in the browser toolbar:

To prevent students from using JavaScript code to try to bypass the security, we need to add an additional configuration.

From the Google Workspace Admin Console, in the left-hand menu, expand the Devices menu > Chrome > Settings and click on the Users & browsers tab. Select the Organizational Unit that you want to apply the restriction to.

Go to the “Content” section and click on the “URL blocking” setting. In the configuration section add “javascript//*” (withouth the inverted commas) in the “Blocked URLs” box.



Configuration

Blocked URLs
javascript://*

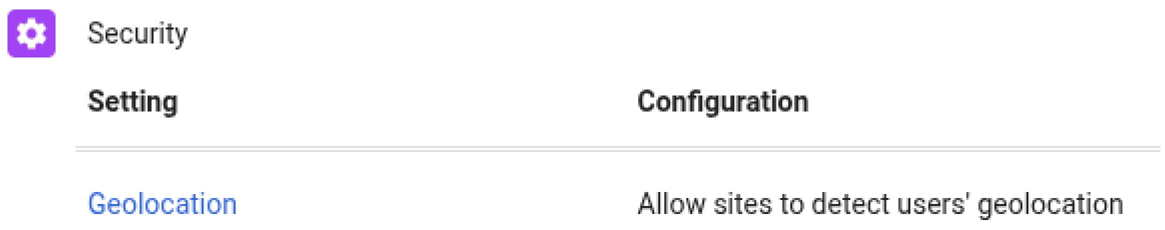
Maximum of 1000 URLs in blocklist. Put each URL on its own line. For example
example.org
https://example.com

Don’t forget to click on the Save button to register the changes.

# 8. Configure the Geolocation in Google Workspace:

To ensure the geolocation of the devices is enabled, we must configure the following setting in the Google Workspace Admin Console. From the menu on the left, expand the Devices menu > Chrome > Settings and click on the “Users & browsers” tab. Select the Organizational Unit that you would like to work with.

In the Security section, click on the setting “Geolocation” and select the option “Allow sites to detect users’ geolocation”.



Security

| Setting | Configuration |
|---|---|
| Geolocation | Allow sites to detect users' geolocation |

Finally, click the “Save” button to register the changes.