IMTLazarus extension installation in Google Workspace and security measures

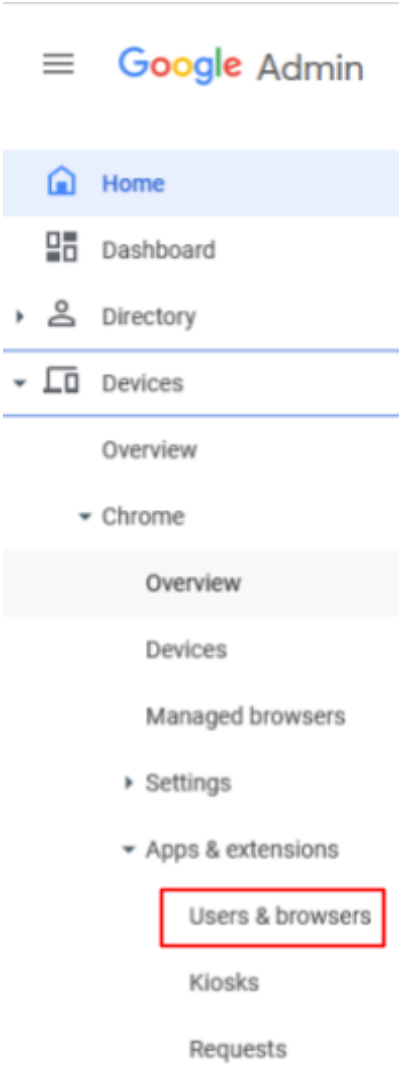
Index

Introduction

For IMTLazarus to work properly on Chrome devices, IMTLazarus recommends performing the following actions within the Google Workspace Management Console. The first point is mandatory for IMTLazarus to work; the following are recommended so that users cannot skip filtering:

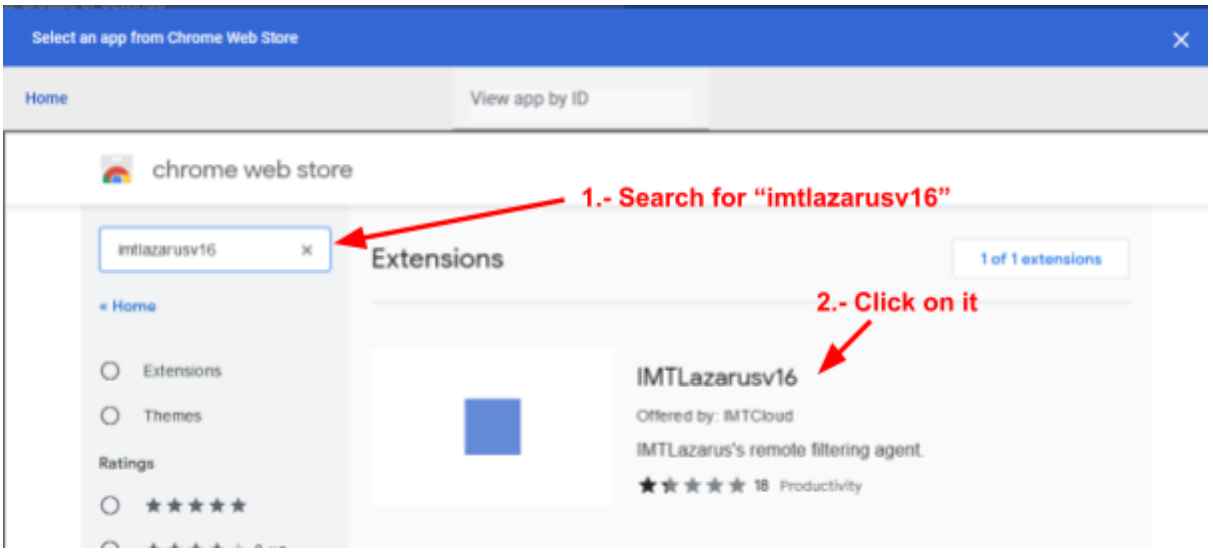
1. Installation of the IMTLazarus extension:

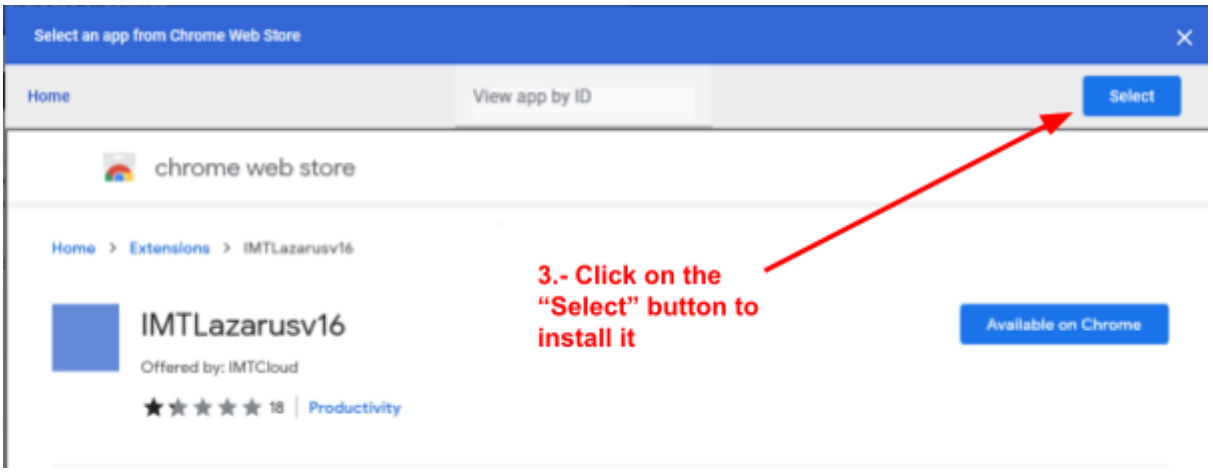
From the Google Workspace Management Console, in the menu on the left, we display the menu Devices > Chrome > Chrome Devices Apps and Extensions and click on Users and browsers:



Once on this screen, **in the left part of the screen, we will select the Organizational Unit on which we want to work** and, within the tab USERS AND BROWSERS, we will give the button "+" yellow we'll find down to the right and then the Chrome icon:

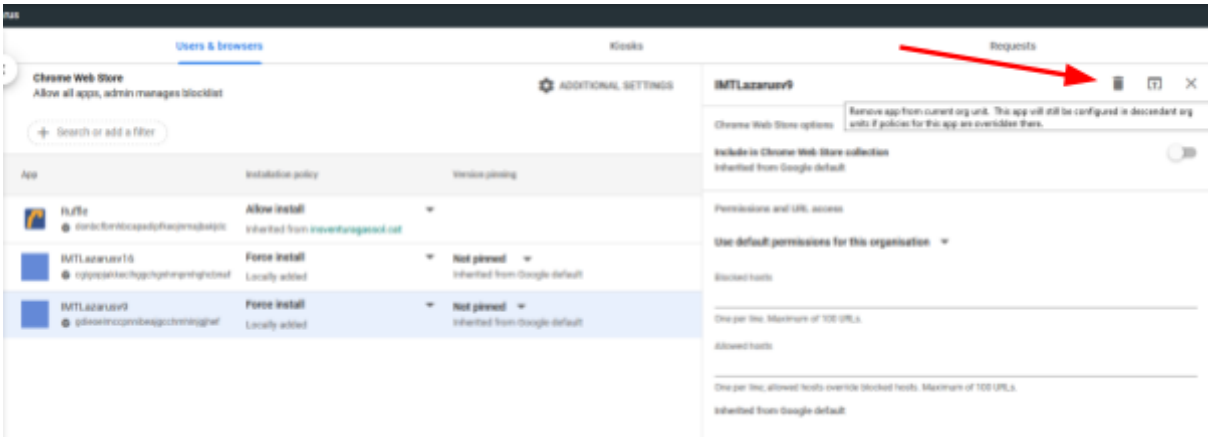
This will make us open a new window called **"Select a Chrome Web Store App"** from which we will have to look for the extension **"IMTLazarusv16"**, click on it and then on the blue button "Select":





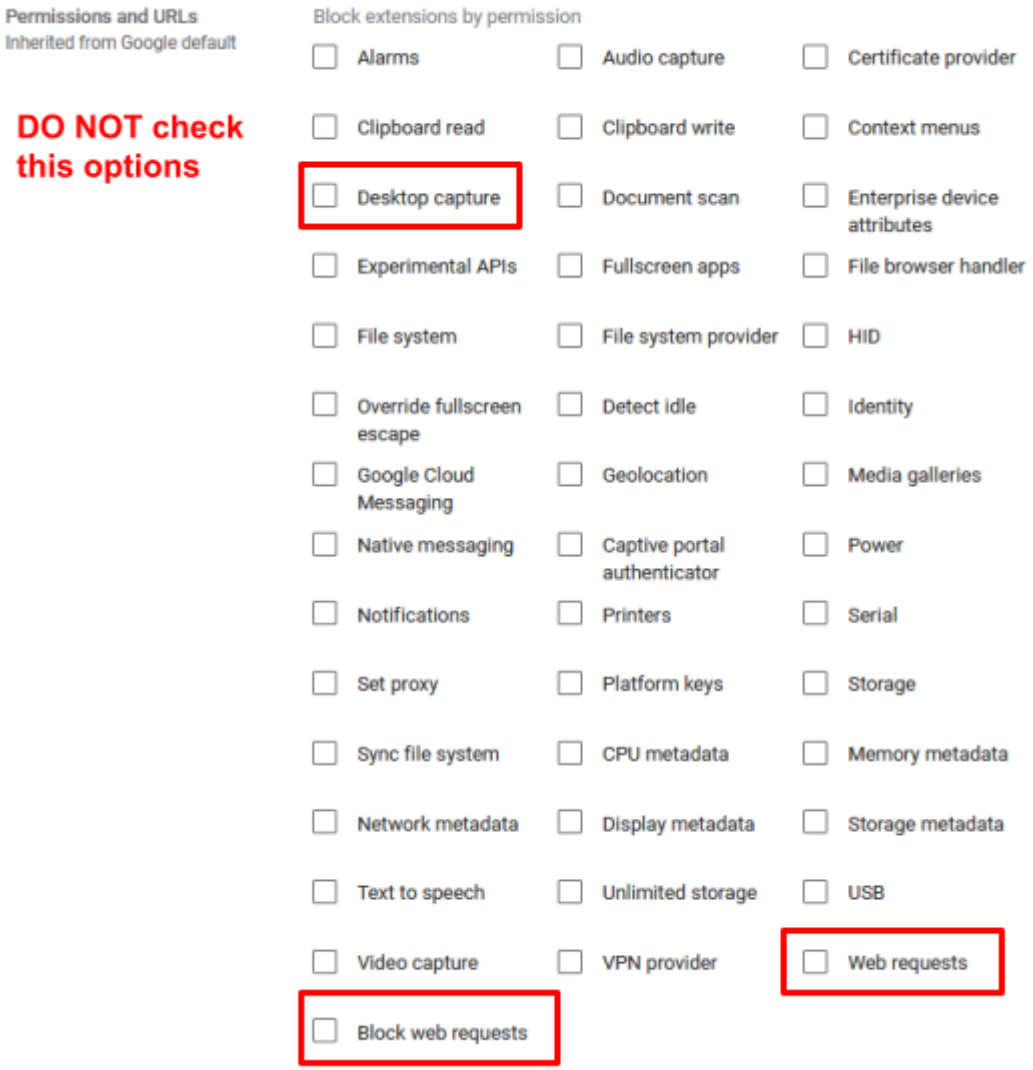
Once the extension is available, we will verify that we have selected the correct Organizational Unit and select as Installation Policy "Force Installation" and hit the "SAVE" button that will appear at the top right of the screen.

If you have an older version of the IMTLazarus extension installed, remove it from this screen by clicking on the previous version of IMTLazarus and then on the bin icon and on the "Save" button on the top right:



Without leaving that screen, click on the "Additional Settings" wheel:

Within the "Additional Settings" section, under "Permissions and URLs", we check that **the following parameters are NOT blocked:**

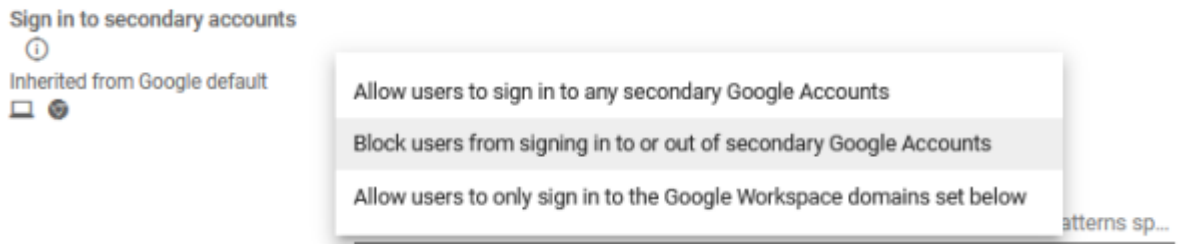


2. Prevent logging in with other accounts outside the domain and incognito mode:

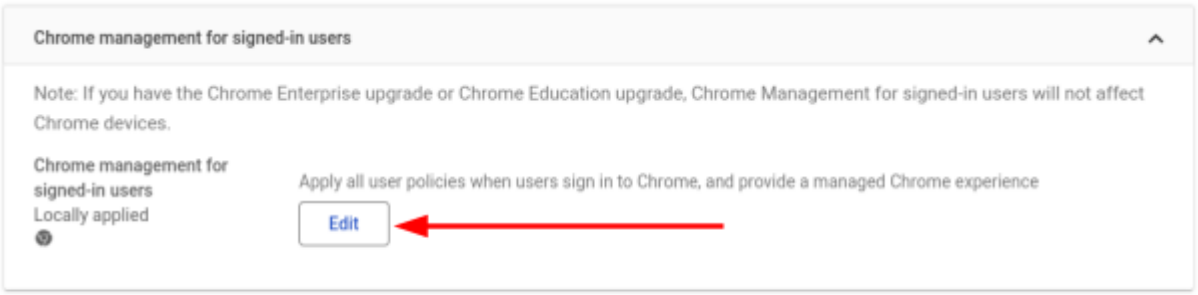
From the Google Workspace Management Console, in the menu on the left, drop down the menu Devices > Chrome > Settings and click on Users and browsers.

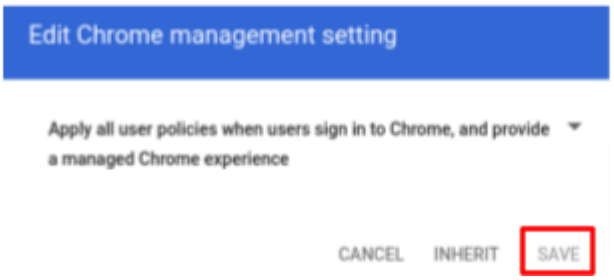
Once on this screen, on the left side of the screen, we will select the Organizational Unit we want to work on

Within this USER SETTINGS AND BROWSER tab, we will go to the User Experience section and in Sign in to secondary accounts we will have to click and select the option "Prevent users from logging in or out of secondary Google accounts". To apply the changes, we will click the "SAVE" button that will appear at the top right of the screen.

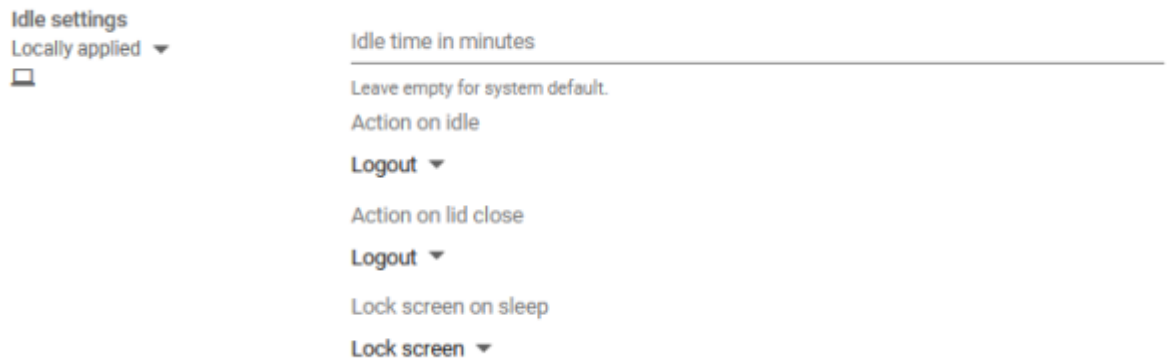


Without leaving that screen, in the "Chrome management for signed-in users" section, within Chrome management for signed-in users section, click on the Edit button and select the option "Apply all user policies when users sign in to Chrome, and provide a managed Chrome experience".





In the "Security" section and in Idle settings, under "Lock screen on sleep" we will select the option "Lock screen":

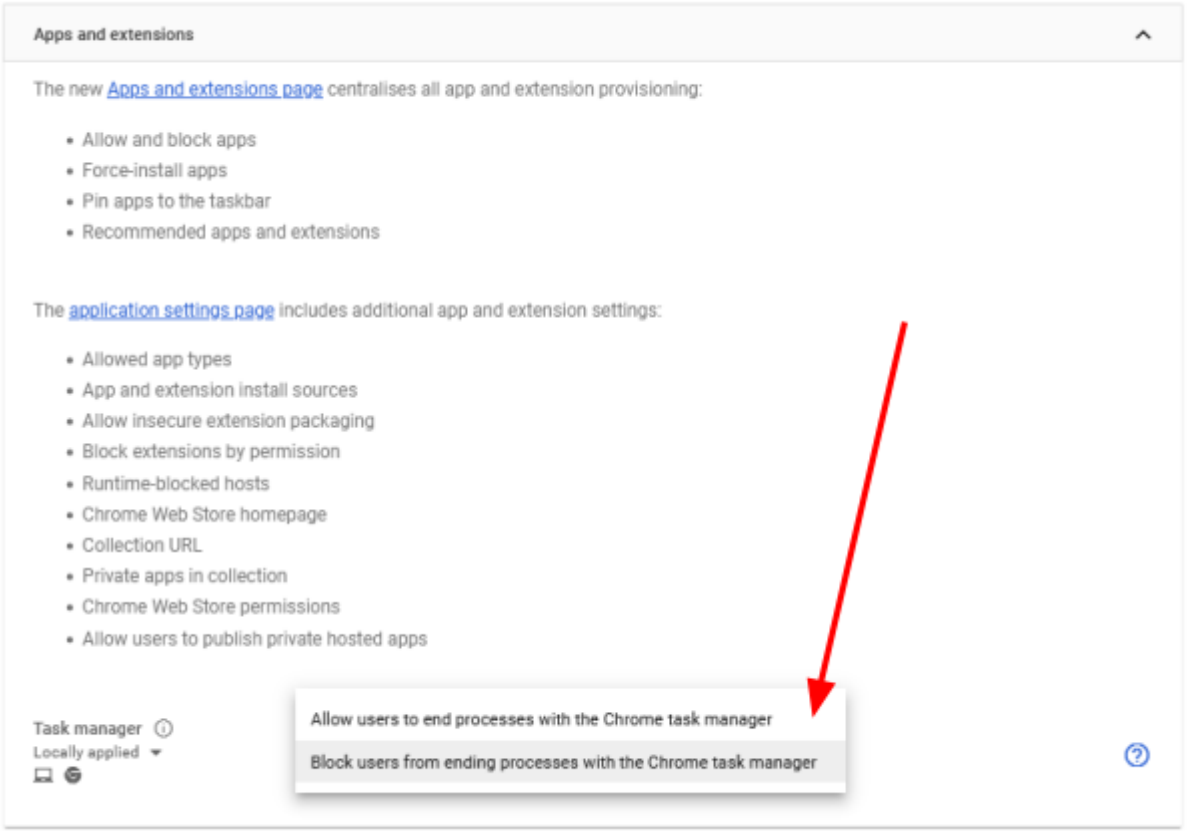


Just below that parameter and within that same Security section, in Incognito Mode we will select the option "Do not allow incognito mode" and we will click the "SAVE" button that will appear at the top right of the screen.

Without leaving where we are in the USER AND BROWSER SETTINGS tab, we will go to the User Experience section and in Access by multiple login we will select the option "Block access by means of multiple login for this organization's user" and we will click the "SAVE" button that will appear at the top right of the screen.

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

Without leaving the USER AND BROWSER SETTINGS tab, we will go to the Applications and Extensions section and in Task Manager we will select the option "Prevent users from completing processes with the Chrome Task Manager" and we will click the “SAVE" button that will appear at the top right of the screen.



4. Device registration permissions:

To prevent users from restoring the devices to the factory state and, therefore, uninstalling IMTLazarus and any other application, we need to enable mandatory computer registration, so that, if this happens (the reset or "powerwash" of the Chrome device), force you to enroll in the Administration Console to be able to use it.

To do this, in the Google Workspace Management Console, in the menu on the left, we display the menu Devices > Chrome > Settings and click on Users and browsers.

Once on this screen, on the left side of the screen, we will select the Organizational Unit we want to work on.

Within this USER AND BROWSER SETTINGS tab, we will go to the Registration Controls section, configure the Registration Permissions setting as: Do not allow users of this organization to register new or previously registered devices.
We will hit the "Save" button that will appear at the top right of the screen.

Without leaving where we are, in the DEVICE SETTINGS tab, we will go to the Registration and access section and mark the following:

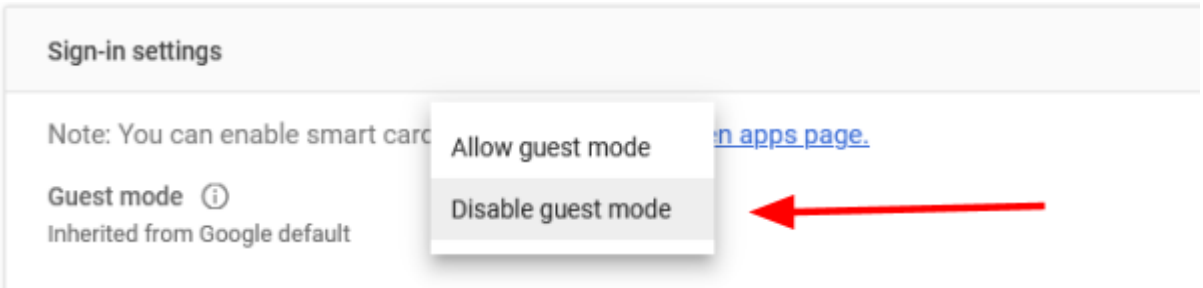
- **Obligation to re-register:** Force replay of device registration with user credentials when their data is deleted
- **Powerwash:** Do not allow Powerwash function to activate

We will hit the "Save" button that will appear at the top right of the screen.

This way, if a user resets the factory values, they will have to return the device to us so that we can re-register it manually with an Administrator account.

5. Disabling Guest Mode:

From the same window, click on the DEVICE SETTINGS tab, go to the Login Settings section and in Guest Mode select the "Disable Guest Mode" option and hit the "SAVE" button which will appear at the top right of the screen.



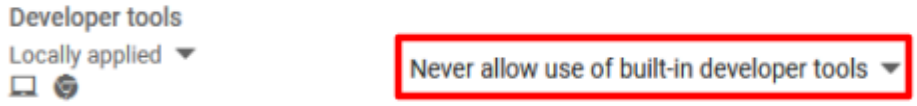
If we have left the screen, we will be able to return to the main screen of the Administration Console and, in the menu on the left, we will display the menu Devices > Chrome > Settings and click on Device.
We will select the Organizational Unit where we want to apply the changes. We looked for the section called Login Settings and in the parameter "Guest Mode" we marked "Disable Guest Mode". To save the changes, we will click the Save button that will appear at the top right of the screen.

6. Disable developer mode:

From the Google Workspace Management Console, in the menu on the left, drop down the menu Devices > Chrome > Settings and click on Users and browsers.

Once on this screen, on the left side of the screen, we will select the Organizational Unit we want to work on.

We look for the section called User Experience and in the parameter "Development tools" select "Never allow the use of integrated development tools". To save the changes, we will click the Save button that will appear at the top right of the screen:



7. Disable the camera app to control camera usage in Google Meet sessions:

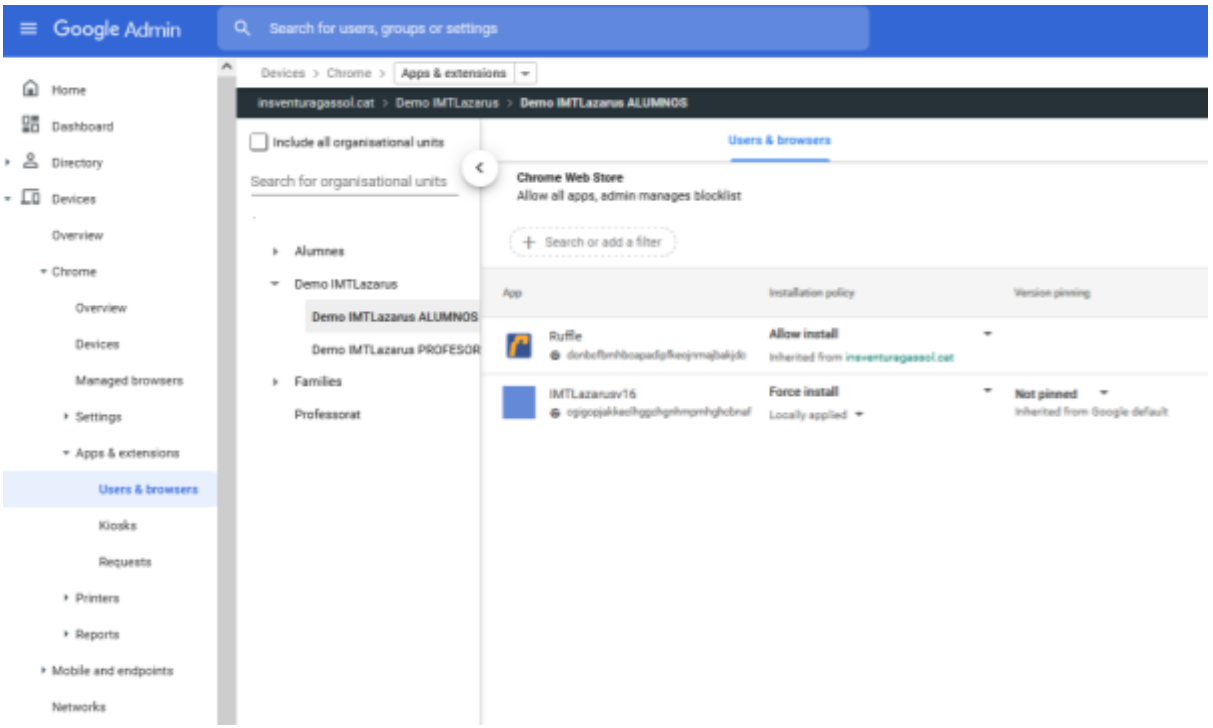
From the Google Workspace Management Console, we can either disable the camera resource at the hardware level (it is completely disabled) or restrict the camera's native application, but in turn allow its use in Google Meet sessions and allow supervisors to control it from IMTLazarus with the functionality "Google Meet - Inside!".

To restrict the camera from the Console, we will need to know the ID of the camera application. From the Chrome Web Store we locate it in the following URL:

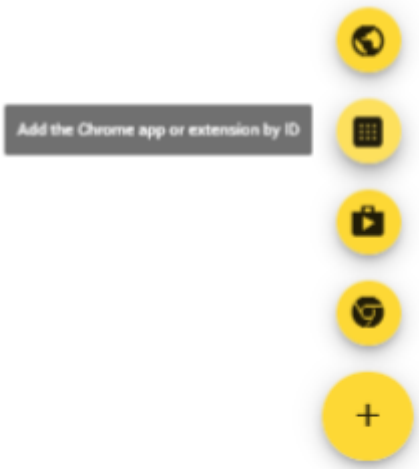
https://chrome.google.com/webstore/detail/camera/**hfhhnacclhffhdffklopdkcgdhifgngh**

We keep the final part of the ID: **hfhhnacclhffhdffklopdkcgdhifgngh**

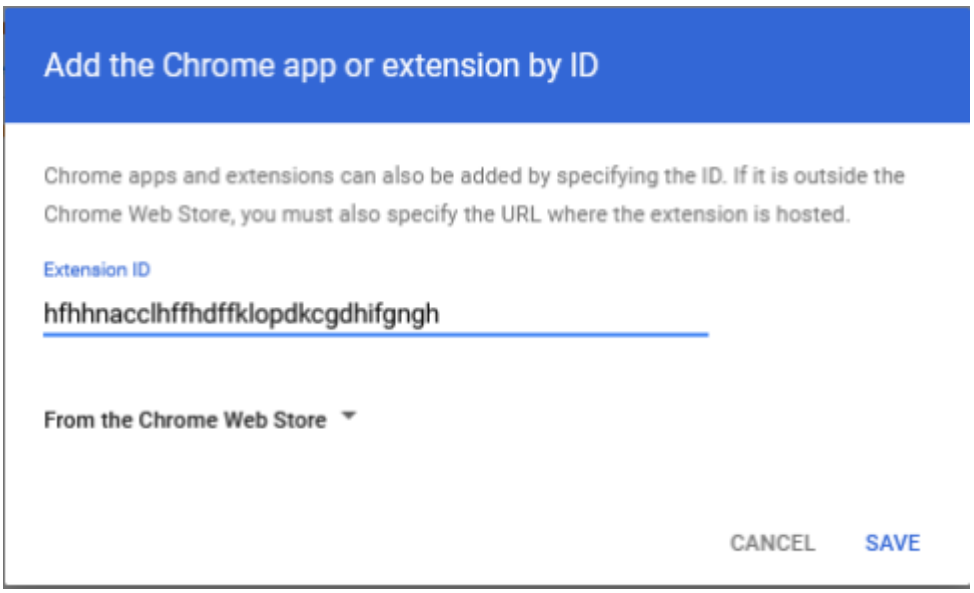
From the Google Workspace Management Console, in the menu on the left, we display the menu **Devices > Chrome > Applications and Extensions > Users and Browsers**. We select the **Organizational Unit** where we want to apply the restriction to:



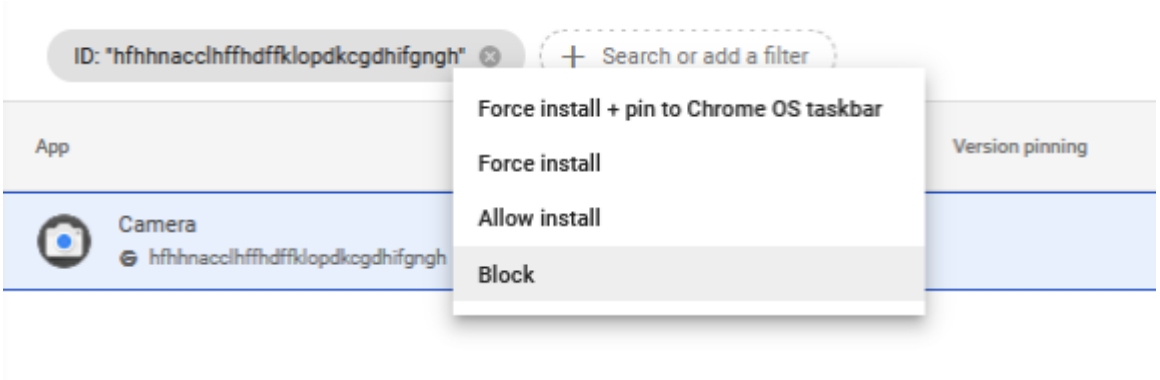
Click the Button + Yellow > Add Chrome App or Extension by ID:



In the window that opens, we enter the ID of the camera application that we have obtained previously: **hfhhnacclhffhdffklopdkcgdhifgngh** and press **SAVE**



Once added, the following screen will appear so you will have to click on the dropdown and select **"Block"**:



And finally press **SAVE** at the **top right of the screen.**

8. Disable javascript execution in the browser bar:

To prevent students from making use of javascript expressions to try to bypass the lock, we must add an additional configuration.

From the Google Workspace Management Console, in the menu on the left, drop down the menu **Devices > Chrome > Settings** and click on **Users and browsers**. We select the Organizational Unit where we want to apply the restriction.

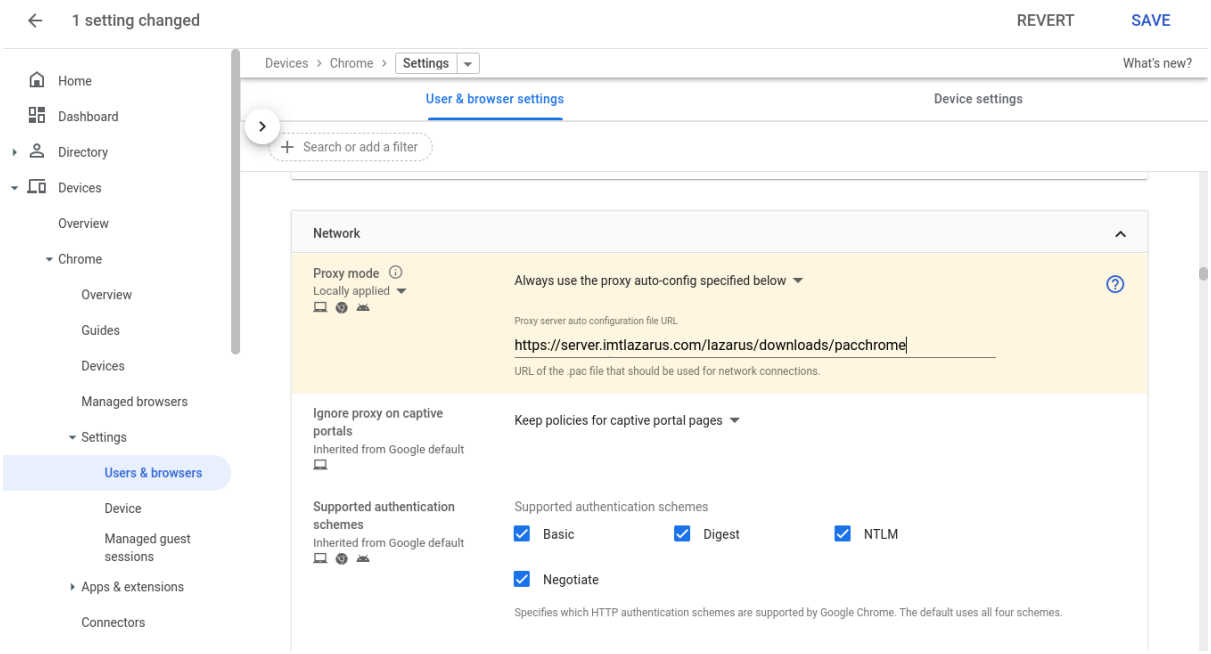
In **Locking URLs** we add **javascript://*** and press **SAVE** at the top right:

9. PAC para seguridad en el acceso a Play Store:

To ensure the security of devices when accessing the Play Store, we must configure the following parameter in the Admin Console:

From the Google Workspace Management Console, in the menu on the left, drop down the menu **Devices > Chrome > Settings** and click on **Users and browsers**. We select the Organizational Unit where we want to apply the restriction.

In the section “Network”, inside the parameter “Proxy mode”, select the dropdown menu to choose the option “Always use the proxy auto-config specified below” and add the following URL: https://server.imtlazarus.com/lazarus/downloads/pacchrome



Press **SAVE** at the **top right of the screen** to save the changes.