

IMTLazarus extension installation in Google Workspace and security measures

Index

1. Installation of the IMTLazarus extension:	2
2. Prevent logging in with other accounts outside the domain and incognito mode:	6
3. Prevent users from completing processes with the Chrome task manager:	8
4. Device registration permissions:	9
5. Disabling Guest Mode:	9
6. Disable developer mode:	10
7. Disable the camera app to control camera usage in Google Meet sessions:	10
8. Disable javascript execution in the browser bar:	13
9. PAC para seguridad en el acceso a Play Store:	13





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:

≡	Google Admin
â	Home
	Dashboard
, °	Directory
- [0	Devices
	Overview
	Chrome
	Overview
	Devices
	Managed browsers
	 Settings
	✓ Apps & extensions
	Users & browsers
	Kiosks
	Requests





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":

Select an app from Chrome Web Store		×
Home	View app by ID	
🚡 chrome web store	1 Secret f	er "imtlezerveu16"
	1 Search fo	or "imtlazarusv16"
imtlazarusv16 ×	Extensions	1 of 1 extensions
« Home		2 Click on it
O Extensions	IMTLaza	arusv16
O Themes	Offered by:	IMTCloud
Ratings	IMTLazaru	s's remote filtering agent.
Ratings	****	★ 18 Productivity
○ ★★★★★		-
0 ++++++		





Select an app) from Chrome Web Store		×
Home		View app by ID	Select
~	chrome web store		
Home >	Extensions > IMTLazarusv16	3 Click on the	
	IMTLazarusv16	"Select" button to install it	Available on Chrome
	Offered by: IMTCloud		
	★★★★ 18 Productivity		

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.

				REVERT	SAVE
sie	65 v				What's new?
en	•				
	Users & browsers		Kizaka Reque	ata	
í	Chrome Web Store Allow all apps, admin manages blocklist				AL SETTINGS
	10: "cgigopjakkechiggshgnhmpminghcbnal" ()	+ Search or add a filter			CLEAR FILTERS
	Ano Porce in	sstall + pin to browser toolbar	Tersion pinning		
ſ	MTLazarusv16 Force in	votall	Not piesed *		
l	6 oppspäkkentopchommennightbraf	liater	Inheritad from Ouogle default		
	Block				

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:

l	Users & brow	rsets		Kiosks		Requests
	Chrame Web Store Allow all apps, admin manages blocklist			ADOUTIONAL SETTINGS	IMTLazaruov9	i a ×
	+ Search or add a filter				Chrome Web Store options	Remove app from current org unit. This app will still be carefigured in descendent org units if policies for this app are oversidates there.
	hea	instalization policy		Version pitning	Include in Chrome Web Stare Inherited from Geogle default	
	Puffe o toráctor/Acapado/Sacjorsajasáját	Allow install Interted from investuragesocilitat	*		Permissions and URL access	
	MTLatarum/16 © oppopalitachgechgehmenteglebeat	Force install Locally added	*	Not pieved v Inherited from Google default	Use default permissions fo	r this organisation 👻
	MTLazarusv0 g pšivosincoprvibesjochrningjiať	Force install Locally added	•	Not pived v inherted from toogle default	One per Inc. Maximum of 100 (R.L.
					Allowed horts	
					One per line, allowed hosts over	ilde blocked hooks. Maximum of 100 URLs.
					Inherited from Google default	1





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

	Users & browser	rs.		Kioska	Requests
1	Chrome Web Store Allow all opps, admin manages blocklist				ADDITIONAL SETTINGS
	Full-text: 'cgigopjakkechggchgnhmpmlight	0			CLEAR FILTERS
1	10 in	stallation policy	Version planing		
	MTLazaruav16 Fa		Not pixzed 🗢 Inherited from Google default		

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

Permissions and URLs	Bloc	k extensions by permis	sion		
Inherited from Google default		Alarms		Audio capture	Certificate provider
DO NOT check		Clipboard read		Clipboard write	Context menus
this options		Desktop capture		Document scan	Enterprise device attributes
		Experimental APIs		Fullscreen apps	File browser handler
		File system		File system provider	HID
		Override fullscreen escape		Detect idle	Identity
		Google Cloud Messaging		Geolocation	Media galleries
		Native messaging		Captive portal authenticator	Power
		Notifications		Printers	Serial
		Set proxy		Platform keys	Storage
		Sync file system		CPU metadata	Memory metadata
		Network metadata		Display metadata	Storage metadata
		Text to speech		Unlimited storage	USB
		Video capture		VPN provider	Web requests
		Block web requests			

IMTLazarus

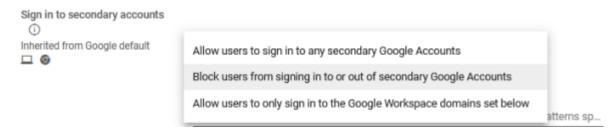


2. Prevent logging in with other accounts outside the domain and incognito mode:

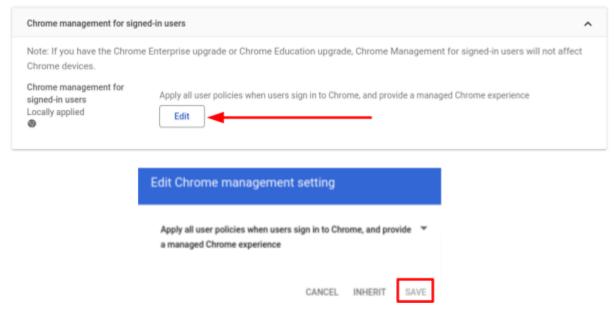
From the Google Workspace Management Console, in the menu on the left, drop down the menu Devices > Chrome > Settings and click on Users and browsers.

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".

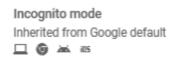




In the "Security" section and in Idle settings, under "Lock screen on sleep" we will select the option "Lock screen":

Idle settings Locally applied 👻	Idle time in minutes
	Leave empty for system default. Action on idle
	Logout 👻
	Action on lid close
	Logout 👻
	Lock screen on sleep
	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.



Disallow incognito mode 🔻

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.

Multiple sign-in access Locally applied 🔻	Multiple sign-in access Block multiple sign-in access for users in this organisation 🔻
	This setting allows users to switch between multiple accounts on a Chrome device without having to sign out of their account and sign back in to another. When either of the first two options are selected, not all settings in the Admin console may apply to users. To ensure that all policies always apply to your users, you need to block multiple sign-in access.





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.

Apps and extensions		^
The new Apps and extension	ns page centralises all app and extension provisioning:	
 Allow and block apps 		
 Force-install apps 		
 Pin apps to the taskba 	ar	
 Recommended apps a 	and extensions	
The application settings page	g includes additional app and extension settings:	
 Allowed app types 		
 App and extension ins 	stall sources	
 Allow insecure extens 	ion packaging	
 Block extensions by p 	ermission	
 Runtime-blocked host 	s	
 Chrome Web Store ho 	mepage	
 Collection URL 		
 Private apps in collect 	lion	
 Chrome Web Store pe 	rmissions	
 Allow users to publish 	private hosted apps	
Task manager ①	Allow users to end processes with the Chrome task manager	
Locally applied 👻	Block users from ending processes with the Chrome task manager	0





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:

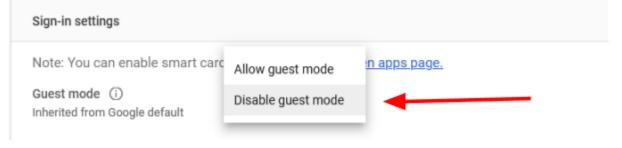
- **Obligation to re-register:** Force replay of device registration with user credentials when their data is deleted
- Powerwash: Do not allow Powerwash function to activate

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:

Developer tools Locally applied ▼

Never allow use of built-in developer tools

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!".

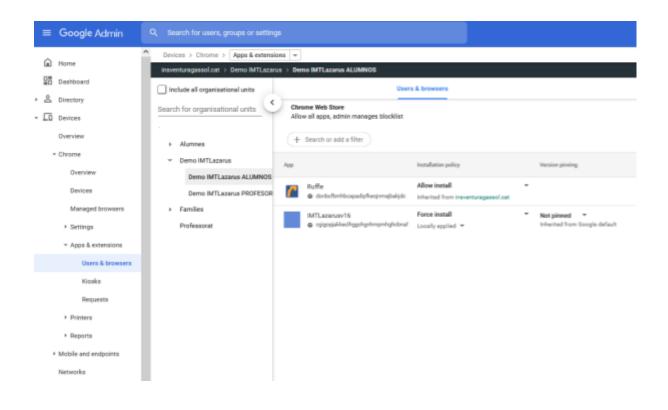
To restrict the camera from the Console, we will need to know the ID of the camera application. From the Chrome Web Store we locate it in the following URL:

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**



Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted. Extension ID hfhhnacclhffhdffklopdkcgdhifgngh	Add the Chrome app or extension by ID		
hfhhnacclhffhdffklopdkcgdhifgngh			
	Extension ID		
From the Chrome Web Store 👻	nfhhnacclhffhdffklopdkcgdhifgngh		
	in in account of the part of the gain in gright	_	
	From the Chrome Web Store 🔻		

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

ID: "hfhhnacclhffhdffklopdkcgdhifgngh	🛚 🛞 🤇 🕂 Search or add a filter	
	Force install + pin to Chrome OS taskbar	
Арр	Force install	Version pinning
Camera	Allow install	
G hfhhnacclhffhdffklopdkogdhifgngh	Block	

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



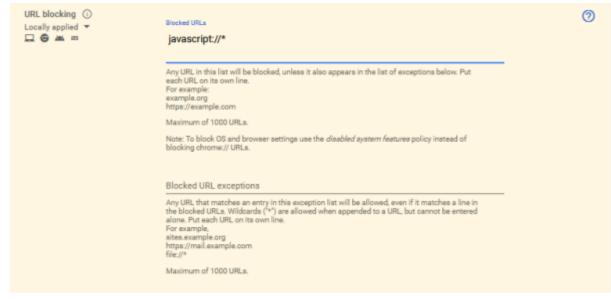


8. Disable javascript execution in the browser bar:

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





\leftarrow	1 setting changed				REVERT	SAV	/E			
<u> </u>		Devi	ces > Chrome > Settings -			What's	s new?			
🖬 Ho 🖬 Da:	me shboard		User & bro	wser settings Device setting	S					
) 💪 Dir	ectory		+ Search or add a filter							
✓ □ Dev	vices									
Ove	erview		Network			^				
- Chi	rome		Proxy mode 🛈	Always use the proxy auto-config specified below 🔻						
	Overview			Locally applied 🔻 🛄 🥘 🛎			0			
	Guides			Proxy server auto configuration file URL https://server.imtlazarus.com/lazarus/downloads/pacchrome						
	Devices			URL of the .pac file that should be used for network connections.						
	Managed browsers		Ignore proxy on captive	Keep policies for captive portal pages 💌						
-	 Settings 		portals Inherited from Google default							
	Users & browsers									
	Device		Supported authentication schemes	Supported authentication schemes						
	Managed guest sessions		schemes Inherited from Google default 🖵 🎯 🗯	Gest Gest MTLM						
•	Apps & extensions			✓ Negotiate						
	Connectors			Specifies which HTTP authentication schemes are supported by Google Chrome. The default uses all four	schemes.					

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

