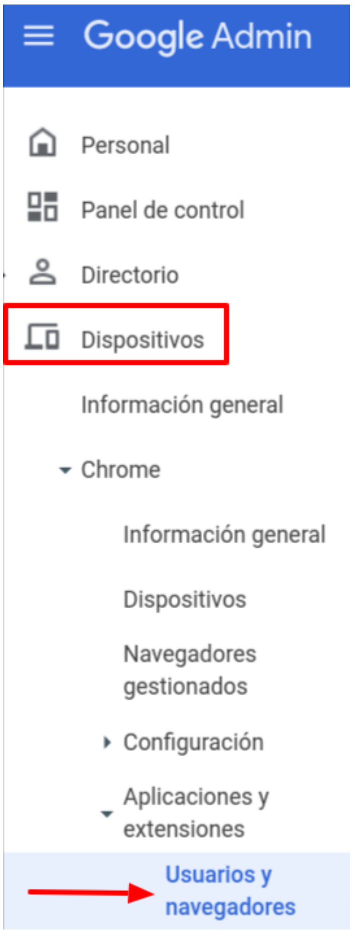
Index

Introduction

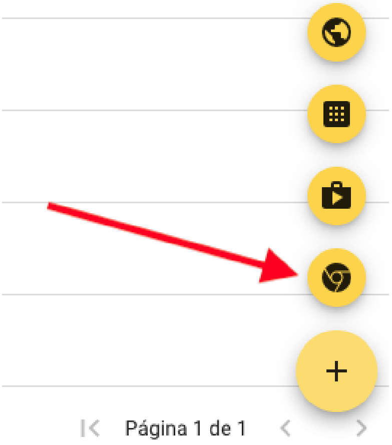
So that IMTLazarus works correctly on Chrome devices, IMTLazarus recommends performing the following actions within the Google Workspace Admin Console. The first point is mandatory so that IMTLazarus work; The following are recommended so that users cannot bypass filtering:

1. Installation of the extension IMTLazarus:

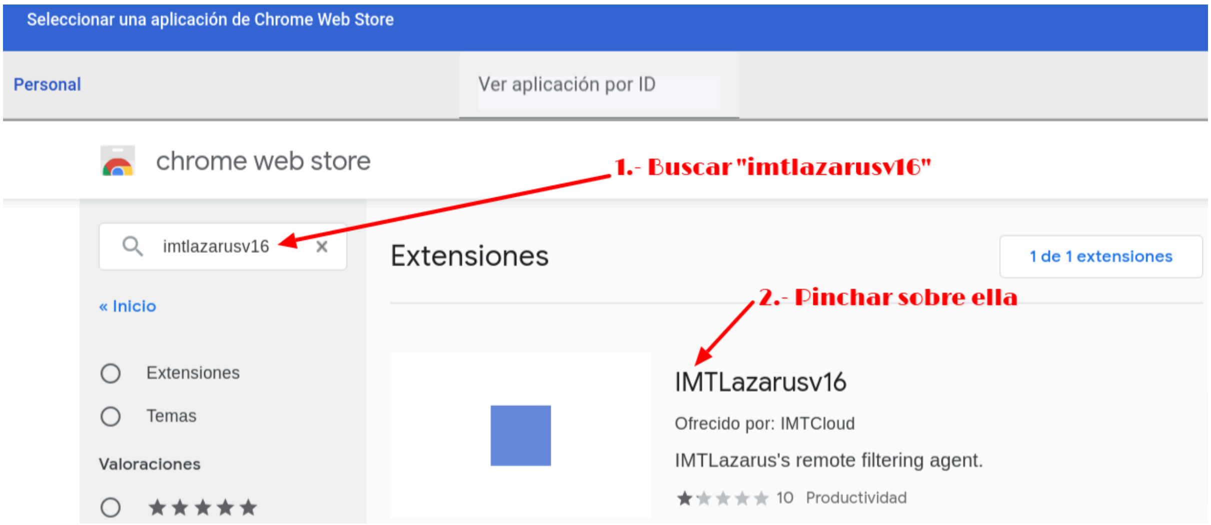
From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Chrome Devices Applications and extensions and click on Users and browsers:**



Once on this screen, on the left side of the screen, We will select the Organizational Unit on which we want to work and, within the USERS AND BROWSERS tab, we will click on the yellow "+" button that we will find at the bottom right and then on the Chrome icon:



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


Seleccionar una aplicación de Chrome Web Store

Personal

Ver aplicación por ID

chrome web store

1.- Buscar "imtlazarusv16"

imtlazarusv16

Extensiones

1 de 1 extensiones

2.- Pinchar sobre ella

« Inicio

○ Extensiones

○ Temas

Valoraciones

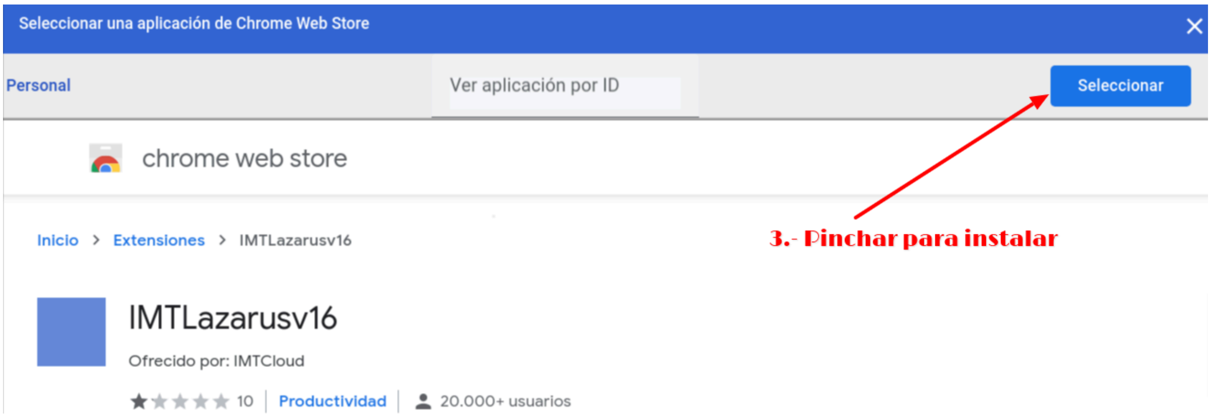
○ ★★★★★

IMTLazarusv16

Ofrecido por: IMTCloud

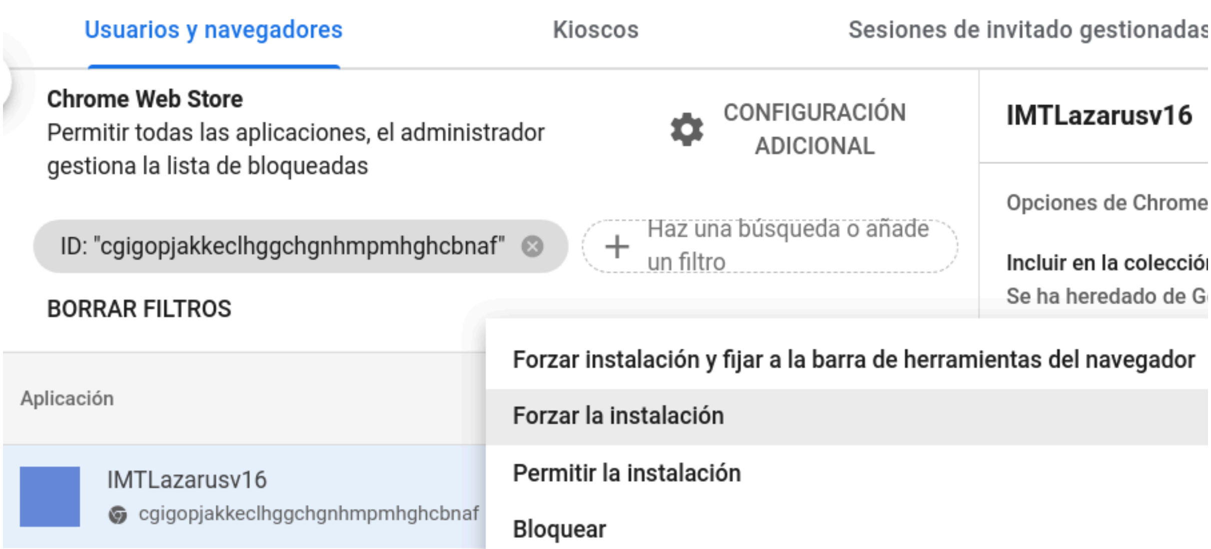
IMTLazarus's remote filtering agent.

★★★★★ 10 Productividad


Seleccionar una aplicación de Chrome Web Store
Personal
Ver aplicación por ID
Seleccionar
chrome web store
Inicio > Extensiones > IMTLazarusv16
IMTLazarusv16
Ofrecido por: IMTCloud
10 | Productividad | 20.000+ usuarios

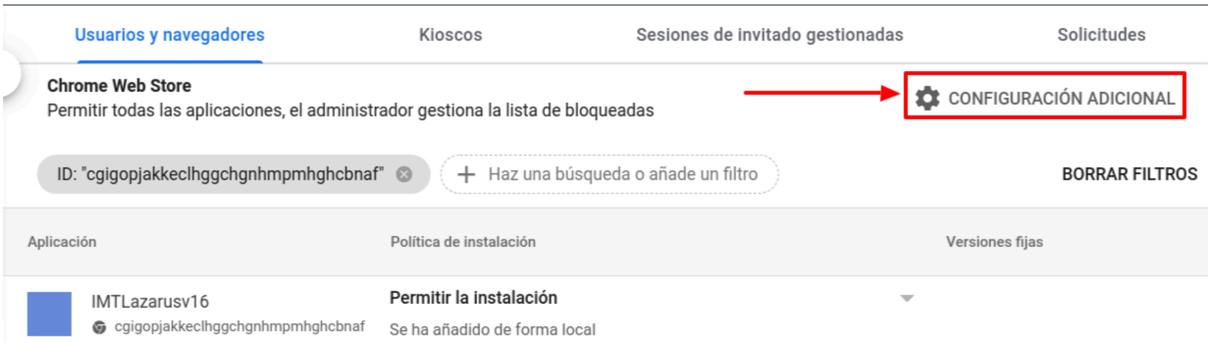
3.- Pinchar para instalar

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

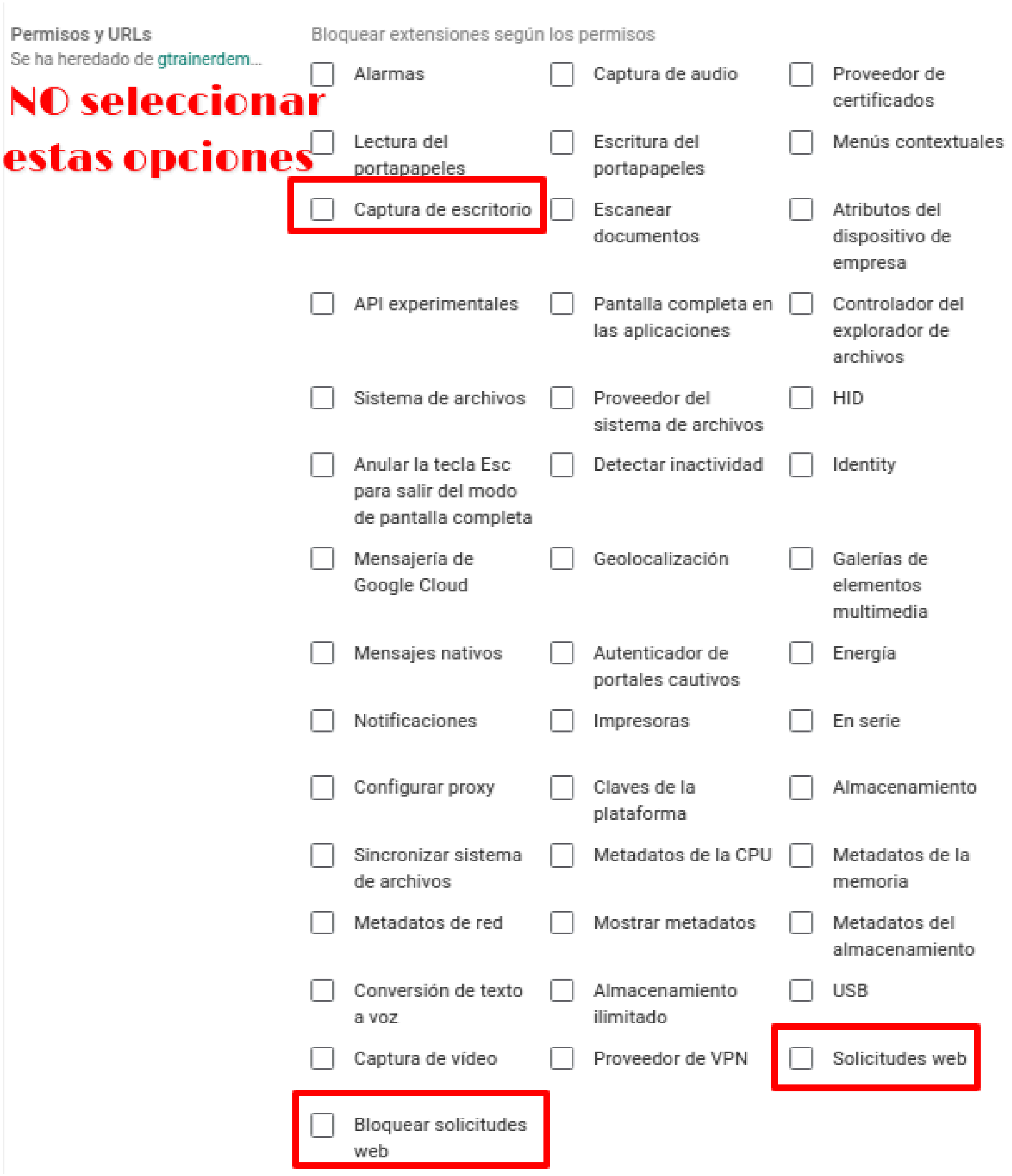

Usuarios y navegadores
Kioscos
Sesiones de invitado gestionadas
Chrome Web Store
Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas
CONFIGURACIÓN ADICIONAL
IMTLazarusv16
Opciones de Chrome
Incluir en la colecció
Se ha heredado de G
ID: "cgigopjakkeclhggchgnhmpmhghcbnaf"
Haz una búsqueda o añade un filtro
BORRAR FILTROS
Aplicación
IMTLazarusv16
cgigopjakkeclhggchgnhmpmhghcbnaf
Forzar instalación y fijar a la barra de herramientas del navegador
Forzar la instalación
Permitir la instalación
Bloquear

If you have a previous version of the IMTLazarus extension installed, delete said version from this same screen:

Without leaving that screen, click on the "Additional Configuration" gear:


Usuarios y navegadores
Kioscos
Sesiones de invitado gestionadas
Solicitudes
Chrome Web Store
Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas
CONFIGURACIÓN ADICIONAL
ID: "cgigopjakkeclhggchgnhmpmhghcbnaf"
Haz una búsqueda o añade un filtro
BORRAR FILTROS
Aplicación
Política de instalación
Versiones fijas
IMTLazarusv16
cgigopjakkeclhggchgnhmpmhghcbnaf
Permitir la instalación
Se ha añadido de forma local

Inside the section **“Additional application settings”**, within “Permissions and URLs”, we check that we DO NOT have the following parameters blocked:



Permisos y URLs

Se ha heredado de gtrainerdem...

NO seleccionar estas opciones

Bloquear extensiones según los permisos

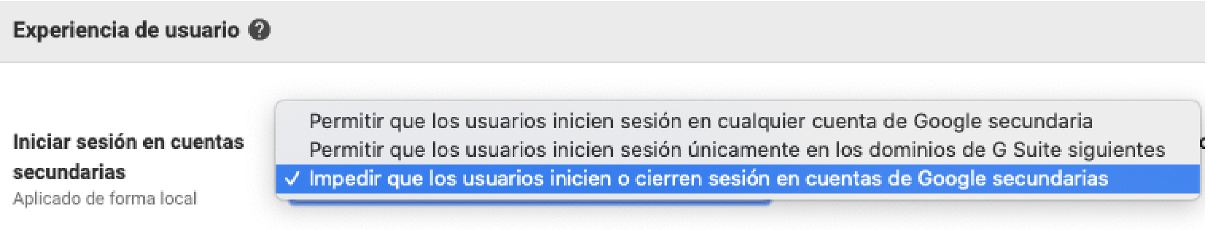
- □ Alarmas
- □ Captura de audio
- □ Proveedor de certificados
- □ Lectura del portapapeles
- □ Escritura del portapapeles
- □ Menús contextuales
- □ Captura de escritorio
- □ Escanear documentos
- □ Atributos del dispositivo de empresa
- □ API experimentales
- □ Pantalla completa en las aplicaciones
- □ Controlador del explorador de archivos
- □ Sistema de archivos
- □ Proveedor del sistema de archivos
- □ HID
- □ Anular la tecla Esc para salir del modo de pantalla completa
- □ Detectar inactividad
- □ Identity
- □ Mensajería de Google Cloud
- □ Geolocalización
- □ Galerías de elementos multimedia
- □ Mensajes nativos
- □ Autenticador de portales cautivos
- □ Energía
- □ Notificaciones
- □ Impresoras
- □ En serie
- □ Configurar proxy
- □ Claves de la plataforma
- □ Almacenamiento
- □ Sincronizar sistema de archivos
- □ Metadatos de la CPU
- □ Metadatos de la memoria
- □ Metadatos de red
- □ Mostrar metadatos
- □ Metadatos del almacenamiento
- □ Conversión de texto a voz
- □ Almacenamiento ilimitado
- □ USB
- □ Captura de vídeo
- □ Proveedor de VPN
- □ Solicitudes web
- □ Bloquear solicitudes web

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

From the Google Workspace Administration 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 on which we want to work.

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

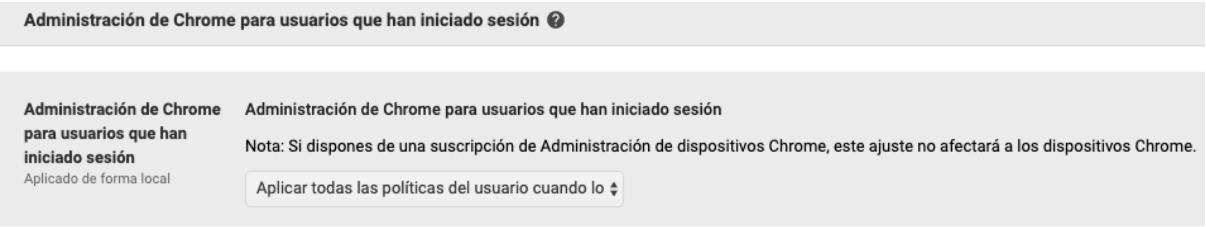


Experiencia de usuario

Iniciar sesión en cuentas secundarias
Aplicado de forma local

Permitir que los usuarios inicien sesión en cualquier cuenta de Google secundaria
Permitir que los usuarios inicien sesión únicamente en los dominios de G Suite siguientes
✓ Impedir que los usuarios inicien o cierren sesión en cuentas de Google secundarias

Without leaving that screen, in the section **"Chrome administration for users who are logged in"**, within **Chrome administration for users who are logged in** we will select the option **"Enforce all user policies when users sign in to Chrome and provide a managed Chrome experience"**.



Administración de Chrome para usuarios que han iniciado sesión

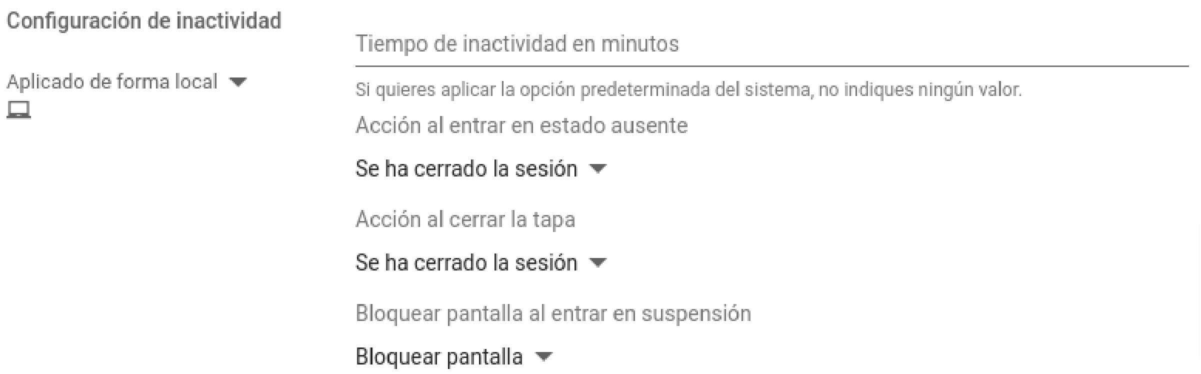
Administración de Chrome para usuarios que han iniciado sesión
Aplicado de forma local

Administración de Chrome para usuarios que han iniciado sesión

Nota: Si dispones de una suscripción de Administración de dispositivos Chrome, este ajuste no afectará a los dispositivos Chrome.

Aplicar todas las políticas del usuario cuando lo

In the section of **"Security"** and in **Idle Settings**, within **"Lock screen when it goes to sleep"** We will select the option **"Lock screen":**



Configuración de inactividad

Aplicado de forma local

Tiempo de inactividad en minutos

Si quieres aplicar la opción predeterminada del sistema, no indiques ningún valor.

Acción al entrar en estado ausente

Se ha cerrado la sesión

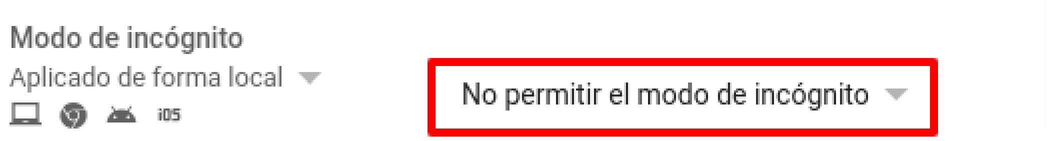
Acción al cerrar la tapa

Se ha cerrado la sesión

Bloquear pantalla al entrar en suspensión

Bloquear pantalla

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 hit the button **"KEEP"** that will appear at the top right of the screen.

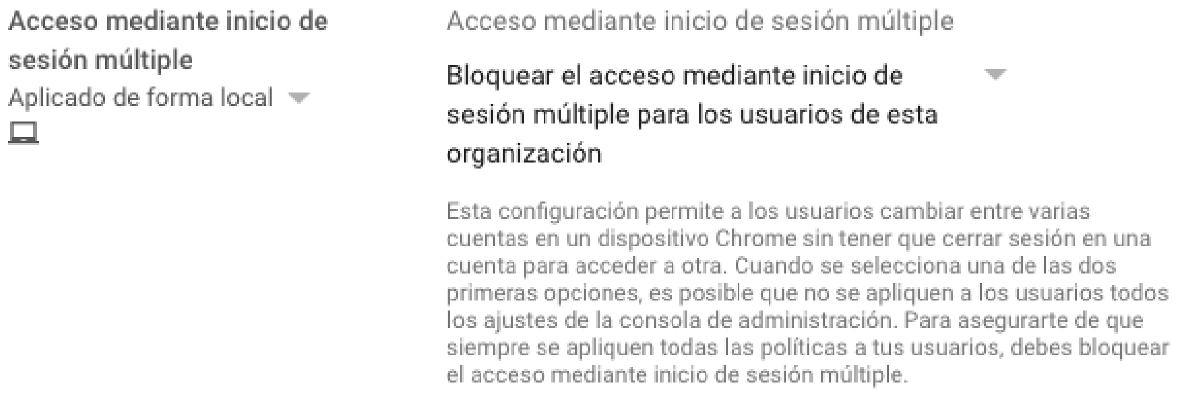


Modo de incógnito

Aplicado de forma local

No permitir el modo de incógnito

Without leaving where we are in the USER AND BROWSER SETTINGS tab, we will go to the section **User experience** and in **Multiple login access** we will select the option **"Block multiple sign-in access for a user in this organization"** and we will hit the button **"KEEP"** that will appear at the top right of the screen.



Acceso mediante inicio de sesión múltiple

Aplicado de forma local

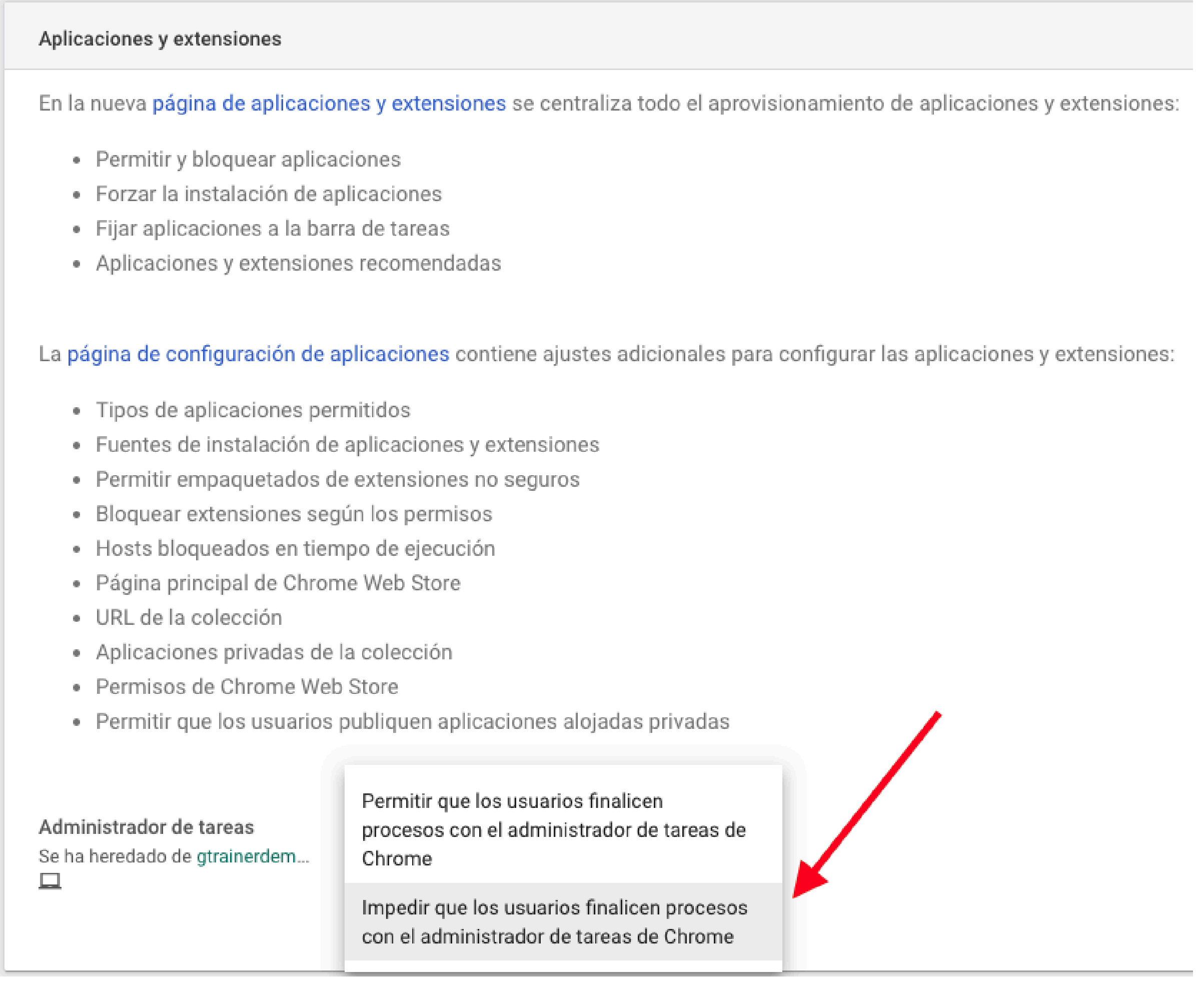
Acceso mediante inicio de sesión múltiple

Bloquear el acceso mediante inicio de sesión múltiple para los usuarios de esta organización

Esta configuración permite a los usuarios cambiar entre varias cuentas en un dispositivo Chrome sin tener que cerrar sesión en una cuenta para acceder a otra. Cuando se selecciona una de las dos primeras opciones, es posible que no se apliquen a los usuarios todos los ajustes de la consola de administración. Para asegurarte de que siempre se apliquen todas las políticas a tus usuarios, debes bloquear el acceso mediante inicio de sesión múltiple.

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

Without leaving the USER AND BROWSER SETTINGS tab, we will go to the section **Apps and extensions** and in **Task Manager** we will select the option **“Prevent users from ending processes with the Chrome task manager”** and we will hit the button **"KEEP"** that will appear at the top right of the screen.



Aplicaciones y extensiones

En la nueva página de aplicaciones y extensiones se centraliza todo el aprovisionamiento de aplicaciones y extensiones:

- Permitir y bloquear aplicaciones
- Forzar la instalación de aplicaciones
- Fijar aplicaciones a la barra de tareas
- Aplicaciones y extensiones recomendadas

La página de configuración de aplicaciones contiene ajustes adicionales para configurar las aplicaciones y extensiones:

- Tipos de aplicaciones permitidos
- Fuentes de instalación de aplicaciones y extensiones
- Permitir empaquetados de extensiones no seguros
- Bloquear extensiones según los permisos
- Hosts bloqueados en tiempo de ejecución
- Página principal de Chrome Web Store
- URL de la colección
- Aplicaciones privadas de la colección
- Permisos de Chrome Web Store
- Permitir que los usuarios publiquen aplicaciones alojadas privadas

Administrador de tareas
Se ha heredado de gtrainerdem...

Permitir que los usuarios finalicen procesos con el administrador de tareas de Chrome

Impedir que los usuarios finalicen procesos con el administrador de tareas de Chrome

4. Equipment registration permissions:

To prevent users from resetting the devices to the factory state and, therefore, uninstalling IMTLazarus and any other application, it is necessary that we activate the mandatory registration of the device, so that if this occurs (the reset or "powerwash" of the Chrome device), force you to enroll it in the Administration Console in order to use it.
To do this, in the Google Workspace Administration 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 on which we want to work.

Within this USER AND BROWSER SETTINGS tab, we will go to the section **Registration controls**, configure the setting **Registration permissions** as: **Do not allow users in this organization to register new or previously registered devices.**
We will click on the "Save" button that will appear in the upper right part of the screen.

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

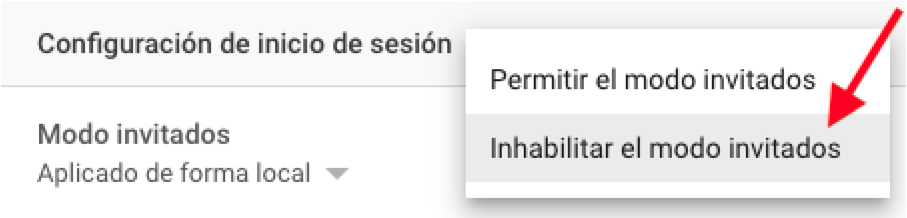
- **Obligation to re-register:** Force device re-registration with user credentials when user data is wiped
- **Powerwash:** Do not allow the Powerwash function to activate

We will click on the "Save" button that will appear in the upper right part of the screen.

This way, if a user performs a factory reset, they will need to return the device to us for manual re-enrollment with an Administrator account.

5. Prevent logging in as a guest:

From the same window, we will click on the DEVICE SETTINGS tab, we will go to the section **Login settings** and in **Guest mode** we will select the option **“Disable guest mode”** and we will hit the button **"KEEP"** that will appear at the top right of the screen.



Configuración de inicio de sesión

Modo invitados
Aplicado de forma local

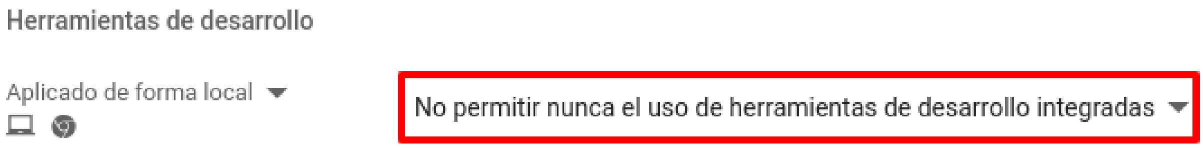
If we have left the screen, we can return to the main screen of the Administration Console and, in the menu on the left, we display the menu **Devices > Chrome > Settings and click on Device.**
We will select the Organizational Unit where we want to apply the changes. We look for the section called **Login settings** and in the parameter **“Guest mode”** we mark **“Disable guest mode”**. To save the changes, we will click on the Save button that will appear at the top right of the screen.

6. Prevent developer mode:

From the Google Workspace Administration 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, <u>We will select the Organizational Unit on which we want to work</u>.

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



Herramientas de desarrollo

Aplicado de forma local

No permitir nunca el uso de herramientas de desarrollo integradas

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

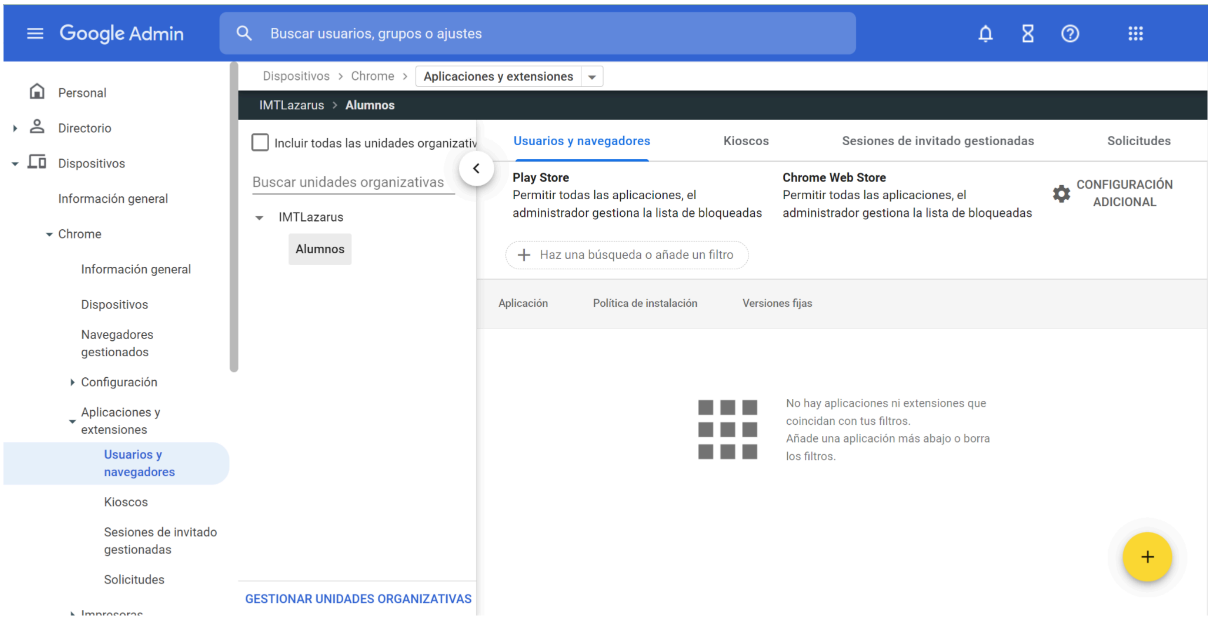
From the Google Workspace Administration Console, we can disable both the camera resource at the Hardware level (it is completely disabled) or restrict the native camera application, but at the same time allow its use in Google Meet sessions and allow supervisors can control it from IMTLazarus with the “Google Meet - Inside!” functionality.

To restrict the camera from the Console, we will need to know the camera app ID. From the Chrome Web Store we find it at the following URL:

[https://chrome.google.com/webstore/detail/camera/**hfhhnacclhffhdffklopdkcgdhifgngh**](https://chrome.google.com/webstore/detail/camera/hfhhnacclhffhdffklopdkcgdhifgngh)

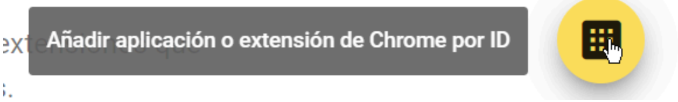
We are left with the final part of the ID: **hfhhnacclhffhdffklopdkcgdhifgngh**

From the Google Workspace Administration Console, in the menu on the left, we display the menu **Devices > Chrome > Apps and extensions > Users and browsers.** We select the **Organizational Unit** where we want to apply the restriction.

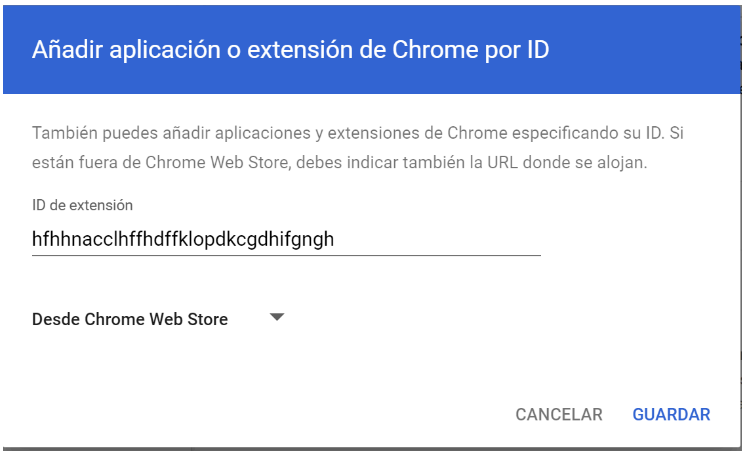

Google Admin
Buscar usuarios, grupos o ajustes
Personal
Directorio
Dispositivos
Información general
Chrome
Información general
Dispositivos
Navegadores gestionados
Configuración
Aplicaciones y extensiones
Usuarios y navegadores
Kioscos
Sesiones de invitado gestionadas
Solicitudes
Impresoras
Dispositivos › Chrome › Aplicaciones y extensiones
IMTLazarus › Alumnos
Incluir todas las unidades organizativ
Buscar unidades organizativas
IMTLazarus
Alumnos
GESTIONAR UNIDADES ORGANIZATIVAS
Usuarios y navegadores
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
CONFIGURACIÓN ADICIONAL
Haz una búsqueda o añade un filtro
Aplicación
Política de instalación
Versiones fijas
+

No hay aplicaciones ni extensiones que coincidan con tus filtros.
Añade una aplicación más abajo o borra los filtros.

We click on the **Yellow + button > Add Chrome app or extension by ID**



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



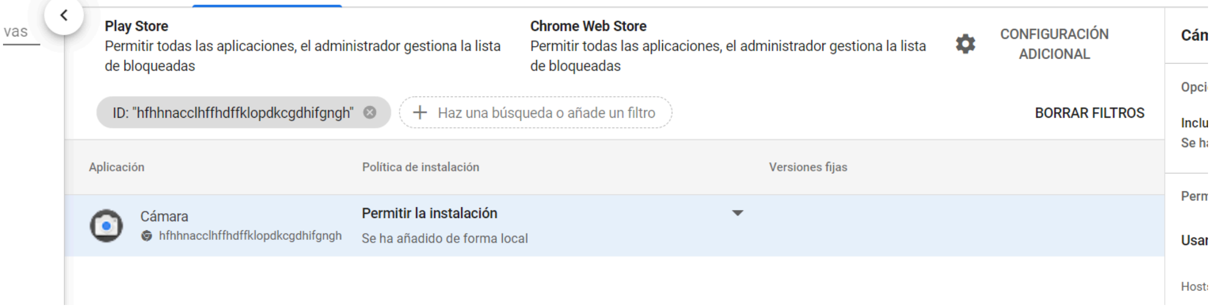
Añadir aplicación o extensión de Chrome por ID

También puedes añadir aplicaciones y extensiones de Chrome especificando su ID. Si están fuera de Chrome Web Store, debes indicar también la URL donde se alojan.

ID de extensión: hfhhnacclhffhdffklopdkcgdhifgngh

Desde Chrome Web Store

Once added:



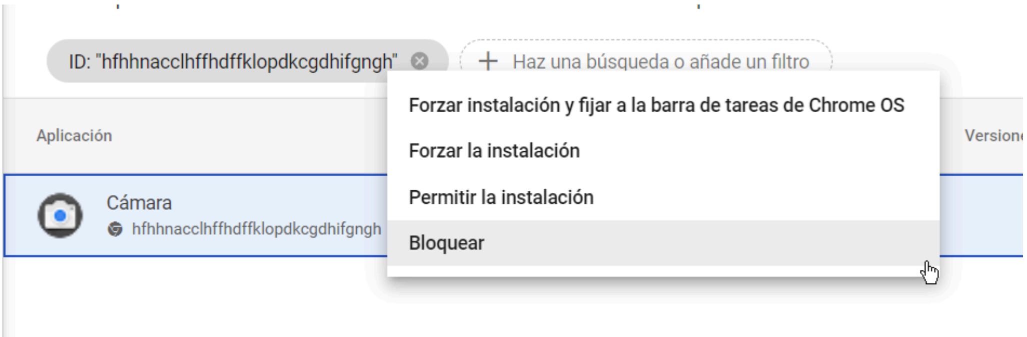
Play Store: Permitir todas las aplicaciones, el administrador gestiona la lista de bloqueadas

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

ID: "hfhhnacclhffhdffklopdkcgdhifgngh"

Aplicación	Política de instalación	Versiones fijas
Cámara hfhhnacclhffhdffklopdkcgdhifgngh	Permitir la instalación Se ha añadido de forma local	

We click on the drop-down menu and select **"Block"**

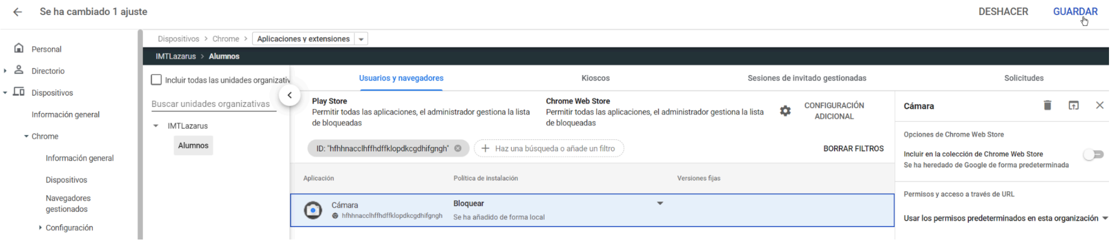


ID: "hfhhnacclhffhdffklopdkcgdhifgngh"

Cámara
hfhhnacclhffhdffklopdkcgdhifgngh

Haz una búsqueda o añade un filtro
Aplicación
Version
Forzar instalación y fijar a la barra de tareas de Chrome OS
Forzar la instalación
Permitir la instalación
Bloquear

And finally we press **KEEP** at the top right of the screen.



Se ha cambiado 1 ajuste

Dispositivos > Chrome > Aplicaciones y extensiones

IMTLazarus > Alumnos

☐ Incluir todas las unidades organizativ

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

ID: "hfhhnacclhffhdffklopdkcgdhifgngh"

Aplicación	Política de instalación	Versiones fijas
Cámara hfhhnacclhffhdffklopdkcgdhifgngh	Bloquear Se ha añadido de forma local	

Cámara

Opciones de Chrome Web Store

Incluir en la colección de Chrome Web Store
Se ha heredado de Google de forma predeterminada

Permisos y acceso a través de URL

Usar los permisos predeterminados en esta organización

8. Disable javascript execution in the browser bar:

To prevent students from using javascript expressions to try to bypass the block, we must add an additional configuration.

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

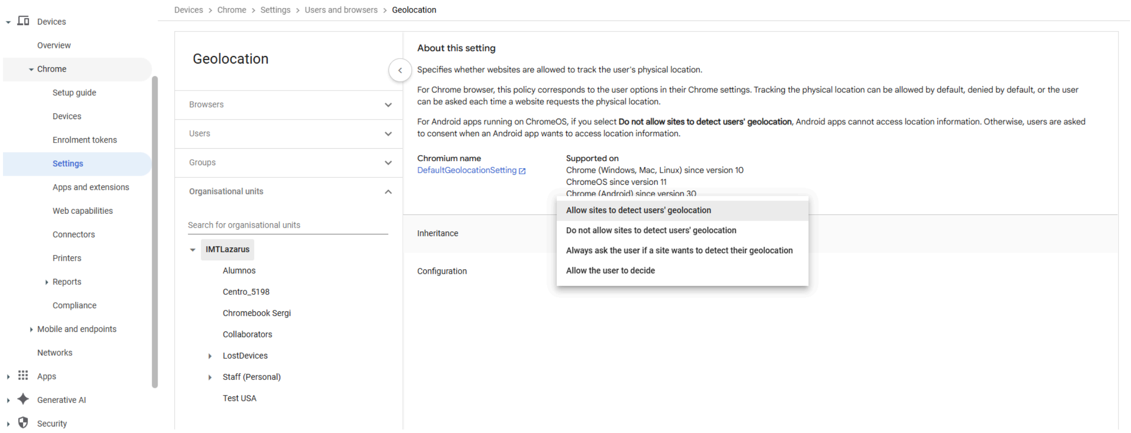
In **URL blocking** we add **javascript://*** and we press **KEEP** on top.

9. Configure Geolocation in Google Workspace

To ensure the geolocation of the devices, we must configure the following parameter in Google Workspace:

From the left-hand menu, expand **Devices > Chrome > Settings**, and click on **Users and Browsers**. Select the **Organizational Unit** where you want to apply the configuration.

In the **Security** section, under the **Geolocation** setting, select the option **"Allow websites to detect users' geolocation."**



About this setting

Specifies whether websites are allowed to track the user's physical location.

For Chrome browser, this policy corresponds to the user options in their Chrome settings. Tracking the physical location can be allowed by default, denied by default, or the user can be asked each time a website requests the physical location.

For Android apps running on ChromeOS, if you select **Do not allow sites to detect users' geolocation**, Android apps cannot access location information. Otherwise, users are asked to consent when an Android app wants to access location information.

Chromium name: DefaultGeolocationSetting

Supported on: Chrome (Windows, Mac, Linux) since version 10
ChromeOS since version 11
Chrome (Android) since version 30

Inheritance

Configuration

Allow sites to detect users' geolocation
Do not allow sites to detect users' geolocation
Always ask the user if a site wants to detect their geolocation
Allow the user to decide

And finally, click **SAVE**.