chrome enterprise

Cómo administrar las extensiones en su empresa

Administre las extensiones de Chrome a gran escala y de forma segura

Enterprise y Education

chrome enterprise

Índice

chrome enterprise

Objetivo de esta guía

Hay muchas extensiones útiles compiladas para el navegador Chrome que empoderan a los trabajadores y hacen que los lugares de trabajo sean más eficientes. Sin embargo, dada la gran cantidad de extensiones que pueden ejecutarse en las computadoras de los usuarios en un momento dado, supervisar y controlar esas extensiones puede ser una tarea abrumadora para los administradores de TI.

Esta guía está dirigida a los administradores de TI que buscan las prácticas recomendadas para administrar las extensiones del navegador Chrome en sus organizaciones. Proporciona pasos para administrar extensiones mediante la Consola del administrador de Google y las Directivas de grupo de Windows.

Esta guía está organizada según los métodos que puede usar para administrar extensiones. Puede hacer lo siguiente:

1. Bloquear extensiones en función de sus permisos
2. Administrar extensiones por política
3. Permitir o bloquear extensiones en la Consola del administrador de Google o la Directiva de grupo de Windows
4. Crear su propia tienda web local (no es una práctica recomendada)
5. Administrar extensiones mediante la Administración en la nube para el navegador Chrome (opción nueva introducida en abril de 2019)

Qué se aborda	Instrucciones, recomendaciones y consideraciones fundamentales para administrar las extensiones del navegador Chrome en una empresa
Público principal	Administradores de Microsoft® Windows® y el navegador Chrome
Entorno de TI	Microsoft Windows 7 y versiones posteriores
Contenido	Prácticas recomendadas para administrar extensiones con el navegador Chrome

Última actualización: *7 de abril de 2019*

Lugar de publicación: *https://support.google.com/chrome/a/answer/9296680*

Introducción

Las organizaciones necesitan proteger los datos de sus usuarios y evaluar más fácilmente las extensiones del navegador que son seguras y relevantes para su empresa. Los administradores de TI necesitan:

1. Evitar que se instalen aplicaciones y extensiones nocivas
2. Mantener las extensiones que los usuarios necesitan
3. Proporcionar acceso limitado a los datos de los usuarios y de la empresa

El objetivo de esta guía es aclarar qué pueden hacer los administradores de TI para gestionar las extensiones en su empresa y ofrecerles una experiencia productiva y segura a sus usuarios. Hay varios métodos para administrar extensiones. Esta guía presenta las diferentes opciones y lo ayuda a elegir el método correcto para su empresa.

Consideraciones sobre la administración de extensiones de Chrome

Los usuarios necesitan acceder a determinadas aplicaciones, sitios y extensiones para hacer su trabajo. Como administrador de TI, debe proteger los datos de los usuarios y de la empresa. Una estrategia de seguridad efectiva implica hacer las preguntas correctas para su empresa y ver cómo Chrome puede satisfacer sus necesidades. Estas son las preguntas clave:

- ¿Con qué reglamentaciones y medidas tengo que cumplir?
- ¿Hay extensiones que soliciten permisos demasiado amplios que podrían ir en contra de las políticas de seguridad de datos de mi empresa?
- ¿Cuántos datos corporativos o de usuarios se almacenan en las máquinas de mis usuarios?

Mientras responde estas preguntas, el navegador Chrome ofrece políticas detalladas que le permiten lo siguiente:

- Bloquear o permitir extensiones en las computadoras de los usuarios en función de sus políticas de protección de datos
- Instalar extensiones de manera automática en las máquinas de los usuarios a fin de que tengan las herramientas que necesitan para ser productivos
- Incluir en la lista blanca o en la lista negra extensiones para permitir la mínima cantidad de derechos necesarios para que trabajen los usuarios

El modelo tradicional para administrar extensiones ha sido incluir extensiones específicas en la lista blanca y en la lista negra. Sin embargo, Chrome también le permite administrar los permisos solicitados por las

extensiones. Con este otro modelo, puede decidir qué derechos y permisos quiere dejar que usen las extensiones en sus máquinas, y luego aplicar una política global que permita o bloquee las extensiones que cumplan con sus requisitos.

¿Qué son los permisos de las extensiones?

Las extensiones pueden requerir derechos para hacer cambios en una máquina o una página web a fin de ejecutarse correctamente. Esos derechos se denominan permisos. Los desarrolladores deben indicar qué derechos y accesos requieren sus extensiones. Hay 2 categorías principales, pero muchas extensiones tienen ambas:

- Los permisos de sitios requieren que la extensión indique los sitios que puede ver o modificar.
  Ejemplos: modificar una página web, acceder a cookies o modificar pestañas
- Los permisos del dispositivo son los derechos que necesita una extensión en la máquina en la que se ejecuta.
  Ejemplos: acceso al puerto USB, al almacenamiento o para ver la pantalla; comunicarse con programas nativos

Cómo decidir qué extensiones permitir

Para ayudarlo a decidir qué extensiones permitir en su organización, haga lo siguiente:

1. Arme una lista de las extensiones que los empleados necesiten en sus computadoras.
2. Examine las extensiones en un entorno de prueba para diagnosticar cualquier problema de compatibilidad con aplicaciones internas.
3. Determine qué permisos se necesitan para que se ejecuten esas extensiones.

Proceso de prueba: Antes de otorgar permisos específicos (como acceso a un sitio) en organizaciones preocupadas por la seguridad, puede consultar el archivo JSON de manifiesto de la aplicación web en el código de la extensión web de Chrome. Otras organizaciones pueden esperar a que los usuarios soliciten instalar extensiones específicas y validarlas antes de aprobarlas en toda la organización. Siga estos pasos para ver qué derechos necesita la extensión:

1. Instale la extensión desde Chrome Web Store.
2. Pruebe la extensión y averigüe cómo funciona en su empresa.
3. Revise los permisos que requiere la extensión en **chrome://extensions**.

Después de seguir estos pasos, decida si va a permitir o bloquear la extensión. Por ejemplo, la extensión Compatibilidad con navegadores heredados de chrome://extensions solicita los permisos “Leer el historial de navegación” y “Comunicarse con aplicaciones nativas en cooperación”. Compare la utilidad de esta extensión con respecto al nivel de permisos que solicita. Después de aprobar una extensión para su organización, adminístrela con las siguientes herramientas.

Cómo administrar extensiones

La mayoría de las organizaciones deberían administrar las extensiones según sus permisos y los sitios web a los que tienen acceso. Este método es más seguro y fácil de administrar, y es escalable para grandes organizaciones. Debe usar 3 o 4 de las siguientes políticas. Siga el vínculo directamente a la sección relevante de esta guía:

- Cómo bloquear o permitir permisos
- Hosts bloqueados en tiempo de ejecución
- Extensiones instaladas de manera automática
- Cómo incluir en la lista blanca o la lista negra (si es necesario)

Con este método, ahorrará tiempo porque solo tiene que configurarlo una vez. La administración de largas listas blancas y negras quedó en el pasado. De todos modos, puede incluir una pequeña lista negra de extensiones que no deban instalarse. Y con la política de hosts en tiempo de ejecución, los sitios más importantes estarán protegidos. Para administrar extensiones en su organización, haga lo siguiente:

1. Averigüe qué extensiones tienen instaladas los usuarios en sus computadoras.
   - **Método 1: Encuesta.** Pregúnteles a sus compañeros de trabajo y a sus gerentes qué extensiones usan con regularidad. Haga una lista de las extensiones que los usuarios necesiten para sus trabajos.
   - **Método 2: Consola del administrador.** Con Administración en la nube para el navegador Chrome, consulte qué extensiones descargaron los usuarios. Vaya a la sección de extensiones del navegador. En computadoras de escritorio, aparece la versión, si la instaló el usuario o el administrador, los permisos requeridos, la cantidad de instalaciones y el estado (activa o inhabilitada).

2. Elija los sitios que necesite que estén más seguros:
   - Averigüe en qué dominios o sitios web internos sensibles tiene que impedir que las extensiones hagan cambios o lean datos.
   - Evite el acceso a esos sitios bloqueando las llamadas a la API cuando se ejecute la extensión. Esto incluye bloquear solicitudes web, lectura de cookies, inyección de JavaScript, XHR, etcétera.

3. Identifique qué permisos representan riesgos potenciales para sus usuarios:
   - Audite las extensiones que hayan instalado los usuarios y consulte qué permisos requieren.
   - Algunos de los permisos que usan las extensiones pueden resultar confusos. En el caso de aplicaciones fundamentales para la empresa, puede comunicarse directamente con el desarrollador o proveedor de la aplicación para obtener más datos sobre la extensión o consultar el código. Estas personas deberían estar en condiciones de detallar los cambios que la extensión puede hacer en máquinas y sitios web.
   - Revise la lista de permisos declarados, que incluye todos los permisos que puede usar una extensión. A partir de esta lista, puede decidir qué permisos quiere aprobar en su organización.

4. Utilice los datos que haya recopilado para crear una lista principal que incluya lo siguiente:
   - **Extensiones requeridas:** Esta lista puede desglosarse por departamento, ubicación de la oficina o algún otro dato relevante.
   - **Lista blanca:** Extensiones requeridas con permisos que se bloquearían, pero que se dejarán ejecutar. Son extensiones que los usuarios necesitan o que, tras conversar con el proveedor, se determina que no representan un riesgo.
   - **Lista negra:** Extensiones que no se permite instalar. Esta lista incluye los permisos que no se deja que se ejecuten. También hay que incluir los sitios y los dominios principales que se deben mantener seguros y a los que no se permitirá que accedan las extensiones. Después, puede comparar esta lista negra con otras que ya tenga. Posiblemente descubra que puede relajar sus políticas actuales de lista negra.

5. Presente su lista principal a los interesados y al equipo de TI para que la acepten.
6. Aplique la nueva política en su lab o en una pequeña prueba piloto en su organización.
7. Implemente estos nuevos conjuntos de políticas entre los empleados por etapas.
8. Revise los comentarios de los usuarios.
9. Repita y ajuste el proceso de forma mensual, trimestral o anual.

Con una base de permisos aprobados y sitios corporativos sensibles protegidos, puede brindar más seguridad a su empresa y una mejor experiencia a los usuarios. Los empleados podrían instalar extensiones que antes no tenían disponibles, pero no ejecutarlas en sitios sensibles de la empresa.

Opción 1: Bloquear extensiones en función de sus permisos

Puede controlar las extensiones que pueden instalar los usuarios por medio de los permisos. Si una extensión instalada necesita un permiso que está bloqueado, simplemente no se ejecutará. La extensión no se quita, solo se inhabilita. Estos pasos son exclusivos de Windows. Para otras plataformas, consulte: DISPOSITIVOS CON SISTEMA OPERATIVO CHROME | MAC | LINUX

Cómo administrar las extensiones según sus permisos en la Consola del administrador de Google

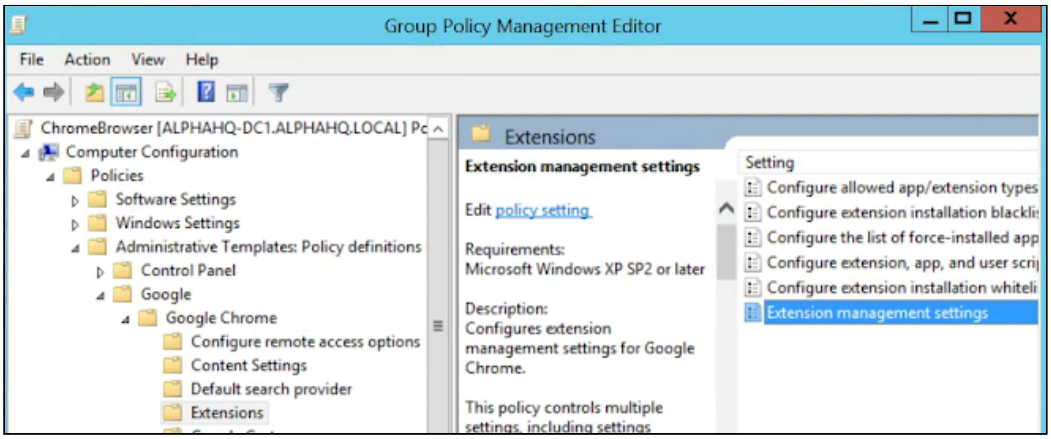
Puede impedir que sus usuarios ejecuten extensiones que necesiten permisos no admitidos. Por ejemplo, podría bloquear una extensión que se conecte a los dispositivos USB de sus usuarios o que impida el acceso para leer cookies.

1. En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome > Configuración del usuario**.
2. Selecciona la unidad organizacional con los usuarios a los que quiera permitirles las extensiones. Para conocer detalles, consulte Cómo definir una política de Chrome en varias aplicaciones.
3. Junto a "Bloquear las extensiones en función de los permisos", seleccione la opción de bloquear o permitir las extensiones que necesiten los permisos que eligió.

4. Marque cada permiso para bloquearlo o aprobarlo.
   Para conocer todos los detalles, consulte esta lista de permisos.
5. Haga clic en **Guardar**.

Cómo administrar extensiones según sus permisos en Directiva de grupo

1. Navegue al Objeto de directiva de grupo (creado en la sección Antes de empezar: Cómo configurar políticas de Google Chrome en GPO) en Microsoft Management Console.
2. Haga clic con el botón derecho > y elija **Editar**.
3. En el Editor de administración de directivas de grupo, vaya a **Directivas > Plantillas administrativas > Google Chrome > Extensiones > Configuración de la administración de extensiones**.
   Defina la ruta de configuración de la administración de extensiones



4. Habilite la directiva; luego ingrese los permisos que quiera aprobar o bloquear, comprimiéndolos en una sola string JSON.

Use el formato de este ejemplo de datos JSON. (Así bloquea cualquier extensión que necesite usar USB).

```
{
        "*": {
                "blocked_permissions": ["usb"]
        }
}
```

Datos JSON compactos:

```
{"*":{"blocked_permissions":["usb"]}}
```

Nota:

- Si puede especificar el ID de una extensión, la directiva solo se aplicará a esa extensión. Puede bloquear más de una, pero deben estar separadas en sus propias entradas.

- Para bloquear todas las extensiones que usen un permiso en particular, agregue un asterisco en el ID de la extensión.

Opción 2: Administrar extensiones por política

Windows ofrece varias formas de administrar extensiones. Una forma común es establecer varias políticas en un mismo lugar con una string JSON o en el Registro de Windows con la política de configuración de extensiones.

Esta política puede controlar parámetros de configuración como la URL de actualización, desde donde se descargará la extensión para instalarla por primera vez, y los Permisos bloqueados (aquellos que no se pueden ejecutar). Lea la Descripción completa de la configuración de extensiones.

Usted decide si quiere establecer todos los parámetros de administración de extensiones aquí o configurar estos controles a través de otras políticas individuales.

- La configuración de Hosts permitidos/bloqueados en tiempo de ejecución solo puede establecerse en la política de configuración de extensiones.
- La política de configuración de extensiones puede reemplazar otras políticas que tenga en otra parte de la directiva de grupo, por ejemplo:
  - ExtensionAllowedTypes
  - ExtensionInstallBlacklist
  - ExtensionInstallForcelist
  - ExtensionInstallSources
  - ExtensionInstallWhitelist

El parámetro se configura con uno de estos 2 métodos:

- Registro de Windows
- String JSON en el Editor de directivas de grupo de Windows

Sugerencia: Darle el formato correcto a una string JSON puede ser complicado. Antes de implementar la política, use el comprobador de JSON.

Cómo configurar la política de extensiones con el Registro de Windows

La política ExtensionSettings se debe escribir en el registro de la siguiente manera:
`HKLM\Software\Policies\Google\Chrome\ExtensionSettings\`

- Se puede usar HKCU en lugar de HKLM. Se puede configurar la ruta equivalente con GPO.
- Puede crear las claves con el método que elija en la máquina del usuario.

Para Chrome, todos los parámetros de configuración comenzarán con esta clave:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\`

La siguiente clave que creará es el ID de extensión para el alcance individual o un asterisco para el alcance predeterminado. Por ejemplo, use la siguiente ubicación para la configuración que se aplique a Hangouts de Google:

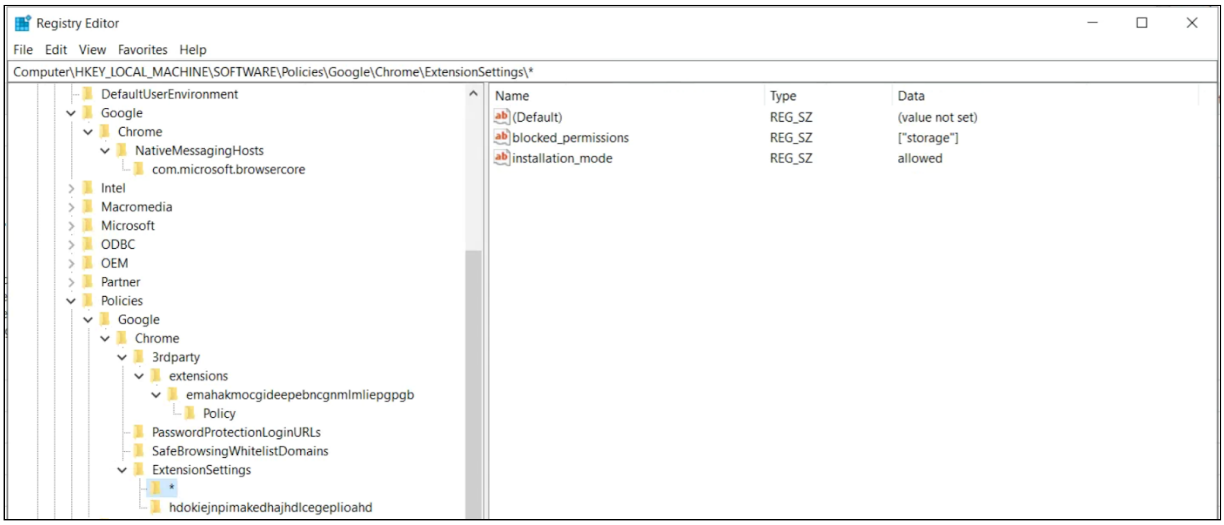
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\nckgahadagoaajjgafhacjanaoiihapd`

Para la configuración que se aplique al alcance predeterminado, use esta ubicación:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*`

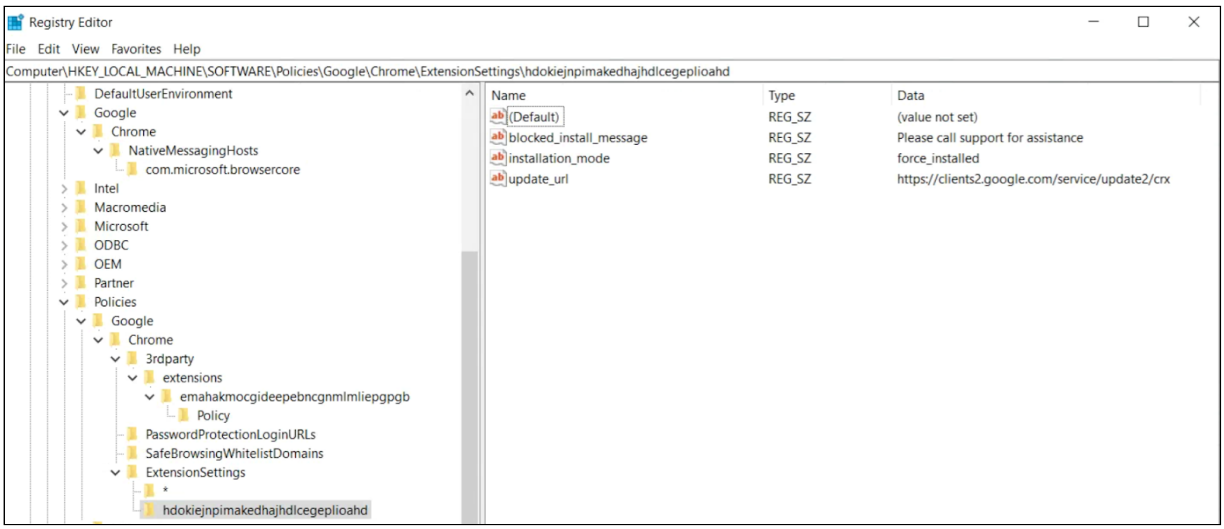
Los diferentes parámetros de configuración requerirán distintos formatos, según se trate de una string o un arreglo de strings. Los valores de arreglos requieren [" value "]. Los valores de strings se pueden introducir sin cambios. En esta lista se indica qué parámetros de configuración son arreglos y cuáles son strings:

- Installation_mode = String
- update_url = String
- blocked_permissions = Arreglo de strings
- allowed_permissions = Arreglo de strings
- minimum_version_required = String
- runtime_blocked_hosts = Arreglo de strings
- runtime_allowed_hosts = Arreglo de strings
- blocked_install_message = String

Ejemplos de cómo se ven las claves dentro del registro:



La clave de alcance predeterminado (*) y sus valores



Un alcance individual y sus valores

Aquí, las claves establecidas en el registro se convierten a JSON con la política:

Chrome policies

Applies to	Level	Source	Policy name
Machine	Mandatory	Platform	DefaultBrowserSettingEnabled
Machine	Mandatory	Platform	ExtensionSettings


```
{
  "*": {
    "blocked_permissions": [ "storage" ],
    "installation_mode": "allowed"
  },
  "hdokiejnpimakedhajhdlcegeplioahd": {
    "blocked_install_message": "Please call support for assistance",
    "installation_mode": "force_installed",
    "update_url": "https://clients2.google.com/service/update2/crx"
  }
}
```


Cómo configurar mediante una string JSON en el Editor de directivas de grupo de Windows

En los pasos para usar la política de configuración de extensiones con GPO, se presupone que ya importó las Políticas ADM/ADMX para Chrome.

Para otras plataformas de SO, consulte: Mac | Linux

1. En el editor de administración de GPO, vaya a la política **Google Chrome > Extensiones > Configuración de la administración de extensiones**.
2. Habilite la política y luego ingrese sus datos compactos de Notación de objetos JavaScript (JSON) en el cuadro de texto como una sola línea (sin saltos de línea).

Para validar las políticas y compactarlas en una sola línea (a continuación, hay un ejemplo de datos JSON), use esta herramienta de compresión JSON de terceros.

JSON con el formato correcto para la política de configuración de extensiones. Para usar este método, tiene que entender las 2 partes de esta política: el alcance **predeterminado** y el **individual**. El alcance predeterminado es el genérico para extensiones sin alcance propio. El alcance individual se aplica solo a una extensión en particular.

El alcance predeterminado se identifica con un asterisco (*). Este ejemplo define un alcance predeterminado y el alcance individual de una extensión:

```
{
   "*": {},
   "nckgahadagoaajjgafhacjanaoiihapd": {}
}
```

Las extensiones se configuran con un solo alcance. Si una extensión tiene un alcance individual, este será el que se aplique. Si no tiene alcance individual, se usará el alcance predeterminado.

Aquí hay un ejemplo de JSON que impide que cualquier extensión se ejecute en .example.com y bloquea cualquier extensión que requiera el permiso "USB":

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.example.com"],
    "blocked_permissions": ["usb"]
  }
}
```

Datos JSON compactos:

```
{"*":{"runtime_blocked_hosts":["*://*.example.com"],"blocked_permissions":["usb"]}}
```

Ejemplos de referencia con valores:

- "allowed" (predeterminado)
  El usuario puede instalar la extensión desde Chrome Web Store.
  Ejemplo de JSON:

```
{ "*": {"installation_mode": "allowed" }}
```

- "blocked"
  El usuario no puede instalar la extensión desde Chrome Web Store.
  Ejemplo de JSON:

```
{ "*": {"installation_mode": "blocked" }}
```

- "Blocked_install_message"
  Aquí se puede especificar un mensaje personalizado para mostrar cuando se bloquea la

instalación.
Ejemplo de JSON: blocked_install_message:
`{"*": {"blocked_install_message": ["Call IT(408 - 555 - 1234) for an exception"]}}`

- "force_installed"
  - La extensión se instala automáticamente sin que interactúe el usuario.
  - El usuario no puede inhabilitar ni quitar la extensión.
- "Normal_installed"
  La extensión se instala automáticamente sin que interactúe el usuario, pero este puede inhabilitarla.

Si una extensión se instala de manera "normal" o "automática", también hay que definir otro campo "update_url", que apunte al lugar desde el que se puede instalar la extensión.

- Si la extensión que va a descargar está alojada en Chrome Web Store, use "https://clients2.google.com/service/update2/crx".
- Si aloja la extensión en su propio servidor, ingrese la URL de la que Chrome puede descargar la extensión empaquetada (.crx file).
  Ejemplo de JSON: force_installed extension with update_url:
  `{"nckgahadagoaajjgafhacjanaoiihapd": {"installation_mode": "force_installed","update_url": "https://clients2.google.com/service/update2/crx"}}`

Configuración adicional: Evitar que las extensiones modifiquen páginas web

Este parámetro evita que las extensiones cambien y lean datos de sus sitios web y dominios más sensibles.

Para eso, bloquee la inyección de secuencias de comandos en sus sitios web, la lectura de cookies o las modificaciones en las solicitudes web. Este parámetro de configuración no impide que los usuarios instalen o quiten extensiones. Solo evita que esas extensiones alteren los sitios web que usted especifica en la política. Estas instrucciones son para administrar este GPO en máquinas con Windows. Para otras plataformas, consulte: Consola del administrador | Mac | Linux

En la política de Configuración de extensiones, puede establecer los siguientes parámetros para evitar (o permitir) que se modifiquen sitios web o dominios:

- Runtime_blocked_hosts
  Este parámetro de configuración impide que las extensiones hagan cambios o lean datos en los sitios web que elija.
- Runtime_allowed_hosts
  Este parámetro de configuración permite que las extensiones hagan cambios o lean datos en los sitios web que elija. El formato para especificar los sitios en la string JSON de la política es el siguiente:

  ```
  [http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*]
  [http|https|ftp|*],
  ```

Nota: Las secciones [hostname|*] y [eTLD|*] son obligatorias; en cambio, la sección [subdomain|*] es opcional.

Ejemplos de patrones de host válidos y patrones de coincidencia:

Patrones de host válidos	Coinciden	No coinciden
://.example.*	http://example.com https://test.example.co.uk	https://example.google.com http://example.google.co.uk
http://example.*	http://example.com http://example.ly	https://example.com http://test.example.com
http://example.com	http://example.com	https://example.com http://test.example.co.uk
://	Todas las URL	

Este es un ejemplo de una string JSON que le bloquea el acceso a una sola extensión. Esta string evita que una extensión aumente un sitio específico:

```
{
              "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
                            "runtime_blocked_hosts":
["*://*.importantwebsite"]
              }
}
```

Datos JSON compactos:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb":
{"runtime_blocked_hosts":["*://*.importantwebsite"]}}
```

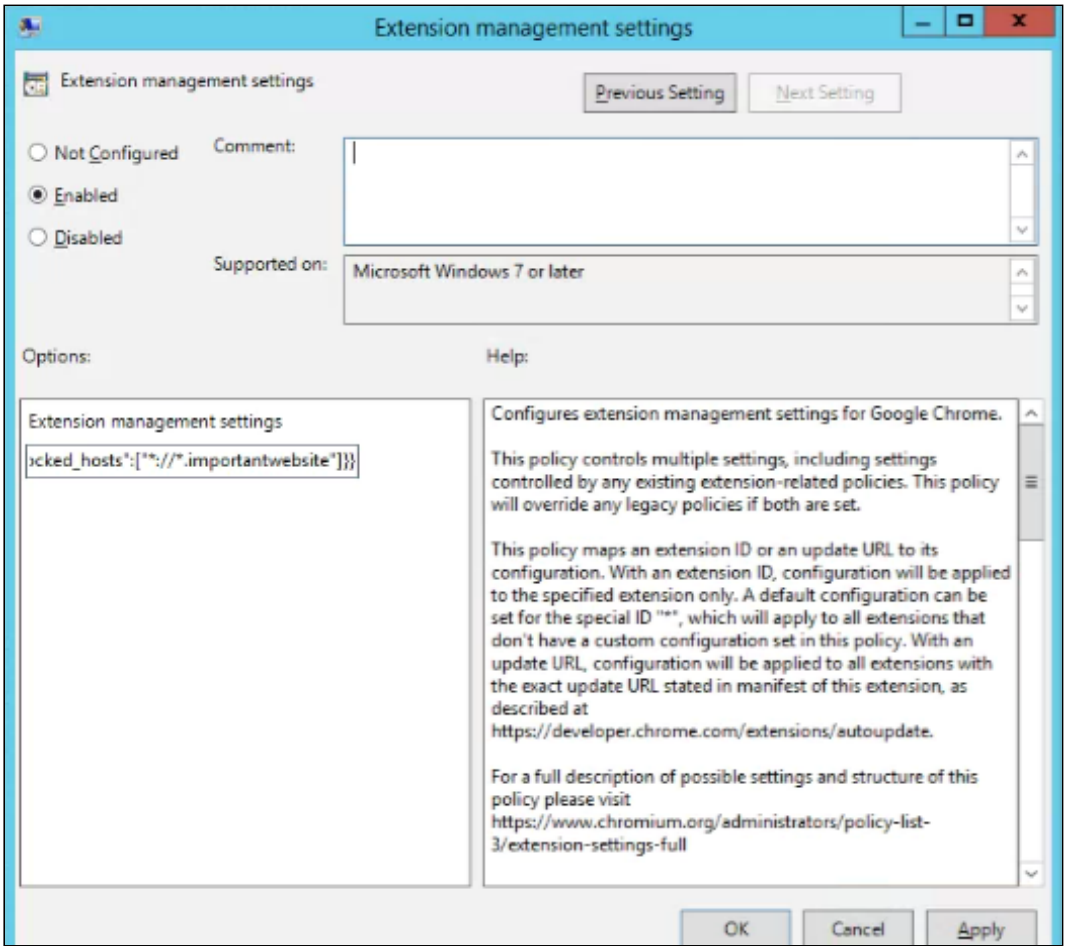
Use una entrada para cada ID de aplicación que quiera bloquear. Este es un ejemplo de cómo impedir que 2 extensiones se ejecuten en el mismo dominio:

```
{
              "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
                            "runtime_blocked_hosts":
["*://*.importantwebsite"]
              },
              "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {
                            "runtime_blocked_hosts":
["*://*.importantwebsite"]
              }
}
```

Datos JSON compactos:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":
["*://,*.importantwebsite"]},"bfbmjmiodbnnpllbbbfblcplfjjepjdn":
{"runtime_blocked_hosts": ["*://*.importantwebsite"]}}
```

Y esta es la string JSON ingresada en la política **Google Chrome > Extensiones > Configuración de la administración de extensiones**:



Opción 3A: Permitir o bloquear extensiones en la Consola del administrador de Google

Además de los métodos descritos anteriormente, puede controlar qué extensiones pueden instalar los usuarios en sus dispositivos mediante listas blancas y negras. Puede permitir que los usuarios instalen cualquier aplicación o extensión. O bien, puede establecer políticas que bloqueen o permitan aplicaciones para toda su organización o ciertos grupos de empleados.

Antes de empezar: Para administrar las extensiones de los usuarios, tiene que activarles el servicio de Chrome Web Store en la Consola del administrador. Puedes encontrar Servicios adicionales de Google en la sección Aplicaciones de la Consola del administrador. Para averiguar los pasos, consulte Cómo activar o desactivar servicios adicionales de Google.

En los siguientes pasos, se presupone que sabe cómo cambiar la configuración en la Consola del administrador.

Cómo permitir todas las extensiones excepto las que quiera bloquear

1. En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome > Configuración del usuario**.
2. Seleccione la organización de los usuarios a los que les quiera bloquear extensiones.
3. Junto a "Permitir o bloquear todas las aplicaciones y extensiones", seleccione la opción de permitir todas las aplicaciones y extensiones, excepto las que bloquee.
4. Junto a "Aplicaciones y extensiones permitidas", haga clic en **Administrar**.
5. Seleccione cada extensión que quiera bloquear.
6. Haga clic en **Guardar**.

Cómo bloquear todas las extensiones excepto las que quiera permitir

1. En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome > Configuración del usuario**.
2. Seleccione la organización de los usuarios a los que les quiera permitir extensiones.
   Para averiguar todos los detalles, consulte Cómo definir una política de Chrome en varias aplicaciones.
3. Junto a "Permitir o bloquear todas las aplicaciones y extensiones", seleccione la opción de bloquear todas las aplicaciones y extensiones, excepto las que permita.
4. Junto a "Aplicaciones y extensiones permitidas", haga clic en **Administrar**.
5. Seleccione cada extensión que quiera permitir.
6. Haga clic en **Guardar**.

Cómo bloquear o permitir una extensión

1. En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome > Administración de aplicaciones**.
2. Seleccione la extensión que quiera bloquear o permitir.
3. Seleccione el tipo de configuración, por ejemplo, "Configuración del usuario" o "Configuración de las sesiones públicas".
4. Seleccione la organización con los usuarios a los que les quiera permitir o bloquear la extensión.
   Para averiguar todos los detalles, consulte Cómo definir políticas de Chrome en aplicaciones concretas.
5. En "Permitir la instalación", haga clic en bloquear o permitir la extensión.
   Al principio, las organizaciones heredan la configuración de su organización superior.
6. Si va a cambiarle un parámetro de configuración a una organización secundaria:
   - Para anular el valor heredado, haga clic en **Anular** y luego cambie el parámetro.
   - Para restablecer el valor heredado de un parámetro de configuración, haga clic en **Heredar**.

7. Haga clic en **Guardar**.

Cómo instalar una extensión de manera automática

Si sabe que un usuario necesita una extensión para su trabajo, puede instalársela de manera automática. Tenga en cuenta que, si lo hace, otorgará automáticamente todos los permisos que necesita la extensión para ejecutarse.

Cómo instalar varias extensiones de manera automática

1. En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome > Configuración del usuario**.
2. Seleccione la organización de los usuarios para los que quiera instalar extensiones de manera automática.
   Para averiguar todos los detalles, consulte Cómo definir una política de Chrome en varias aplicaciones.
3. En la sección "Extensiones y aplicaciones instaladas de manera automática", haga clic en **Administrar las aplicaciones instaladas de manera automática**.
   Sugerencia: Use la barra de búsqueda para encontrar rápido la sección.
4. Seleccione la extensión que quiera instalar de manera automática y haga clic en **Guardar.**

Cómo instalar una sola extensión de manera automática

1. 1.En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome > Administración de aplicaciones**.
2. 2.Seleccione la extensión que quiera bloquear o permitir.
3. 3.Seleccione el tipo de configuración, por ejemplo, "Configuración del usuario" o "Configuración de las sesiones públicas".
4. 4.Seleccione la organización de los usuarios para los que quiera permitir o bloquear la extensión.
   Para averiguar todos los detalles, consulte Cómo definir políticas de Chrome en aplicaciones concretas.
5. 5.En "Instalación automática", active el parámetro de configuración.
   Al principio, las organizaciones heredan la configuración de su organización superior.
6. 6.Si va a cambiarle un parámetro de configuración a una organización secundaria:
   - Para anular el valor heredado, haga clic en **Anular** y luego cambie el parámetro.
   - Para restablecer el valor heredado de un parámetro de configuración, haga clic en **Heredar**.
7. 7.Haga clic en **Guardar**.

Opción 3B: Permitir o bloquear extensiones en Directiva de grupo

Antes de empezar: En los siguientes pasos, se presupone que ya administra Chrome para sus usuarios. Para obtener más información sobre cómo implementar Chrome en Windows, consulte la Guía de implementación del navegador Chrome (Windows). Para averiguar sobre implementación y administración de políticas en Mac®, vaya a Cómo configurar el navegador Chrome en Mac.

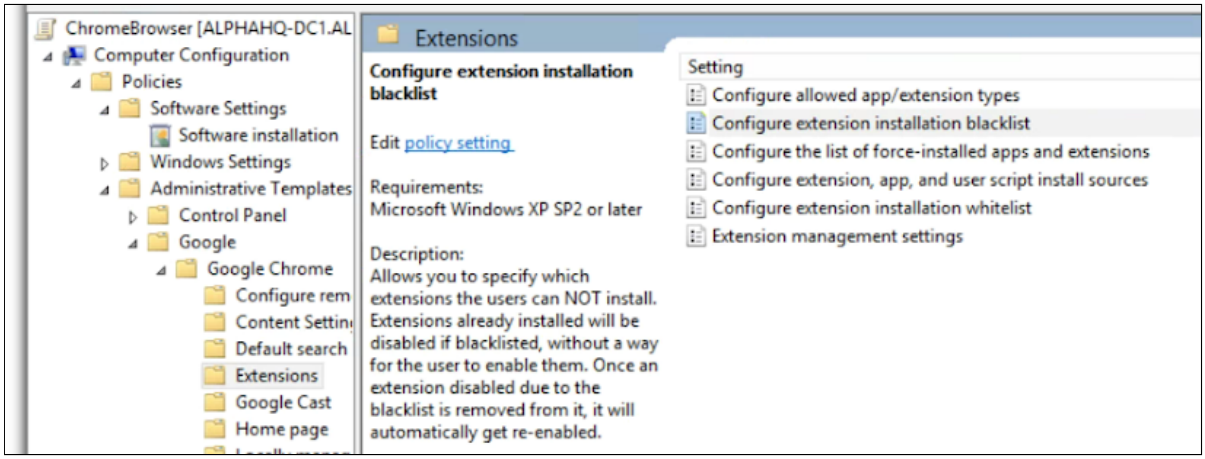
Para Windows, hay 2 tipos de plantillas de políticas: ADM y ADMX. Asegúrese de verificar qué tipo puede usar en su red. Las plantillas muestran qué claves de registro puede establecer para configurar Chrome y cuáles son los valores aceptables. Chrome examina los valores establecidos en estas claves de registro para determinar cómo actuar.

1. Descargue las plantillas de políticas de Chrome.
   Las plantillas de Windows, así como la documentación de políticas comunes de todos los sistemas operativos, se pueden encontrar en este archivo zip de plantillas y documentación de Google Chrome.
2. Abra la plantilla ADM o ADMX que descargó:
   a. Vaya a **Inicio > Ejecutar: gpedit.msc**. (O ejecute gpedit.msc en su terminal).
   b. Vaya a **Directiva de equipo local > Configuración del equipo > Plantillas administrativas**.
   c. Haga clic con el botón derecho en **Plantillas administrativas** y seleccione **Agregar o quitar plantillas**.
   d. Agregue la plantilla chrome.adm a través del diálogo.

Luego, si aún no está allí, aparecerá una carpeta de Google o Google Chrome en "Plantillas administrativas". Si agregó la plantilla ADM en Windows 7 o 10, aparecerá en Plantillas administrativas clásicas / Google / Google Chrome.

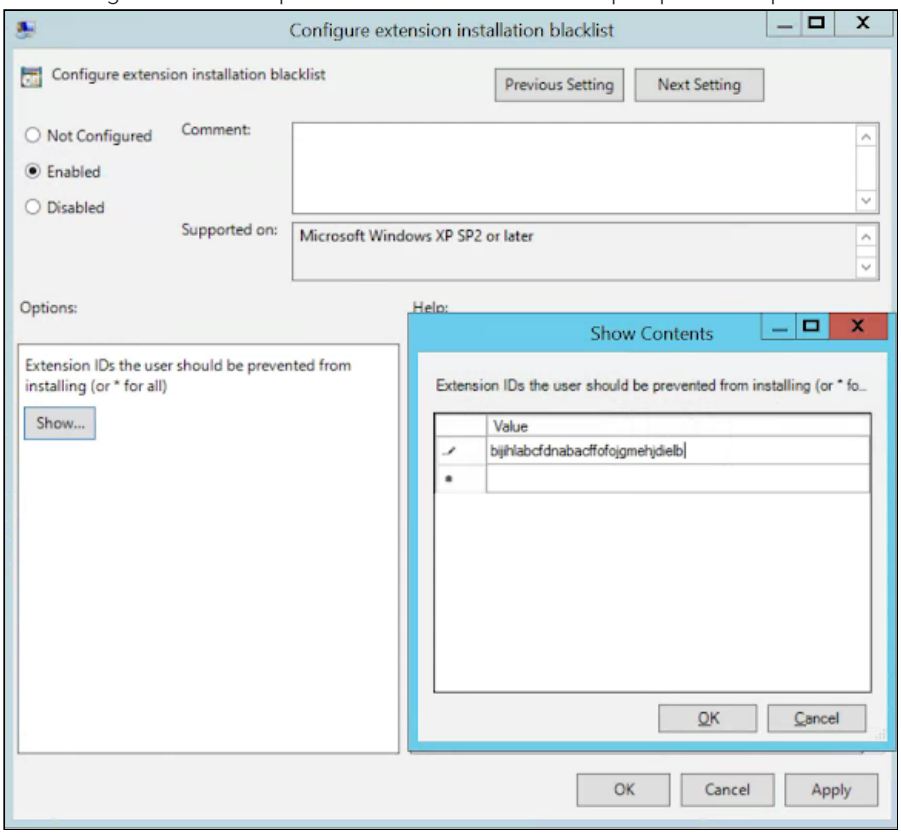
Cómo permitir todas las extensiones excepto las que quiera bloquear

1. En el Editor de directivas de grupo, abra la plantilla que acaba de agregar.
2. Navegue a **Google > Google Chrome > Extensiones > Configurar la lista negra de instalación de extensiones**.



Ruta a las políticas de administración de extensiones

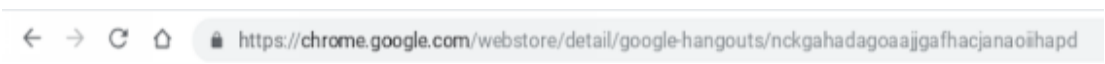
2. En el parámetro de configuración, seleccione **Habilitado**.
3. Haga clic en **Mostrar**.
4. Ingrese el ID de aplicación de las extensiones que quiera bloquear.



Configurar la lista negra de instalación de extensiones

Notas:

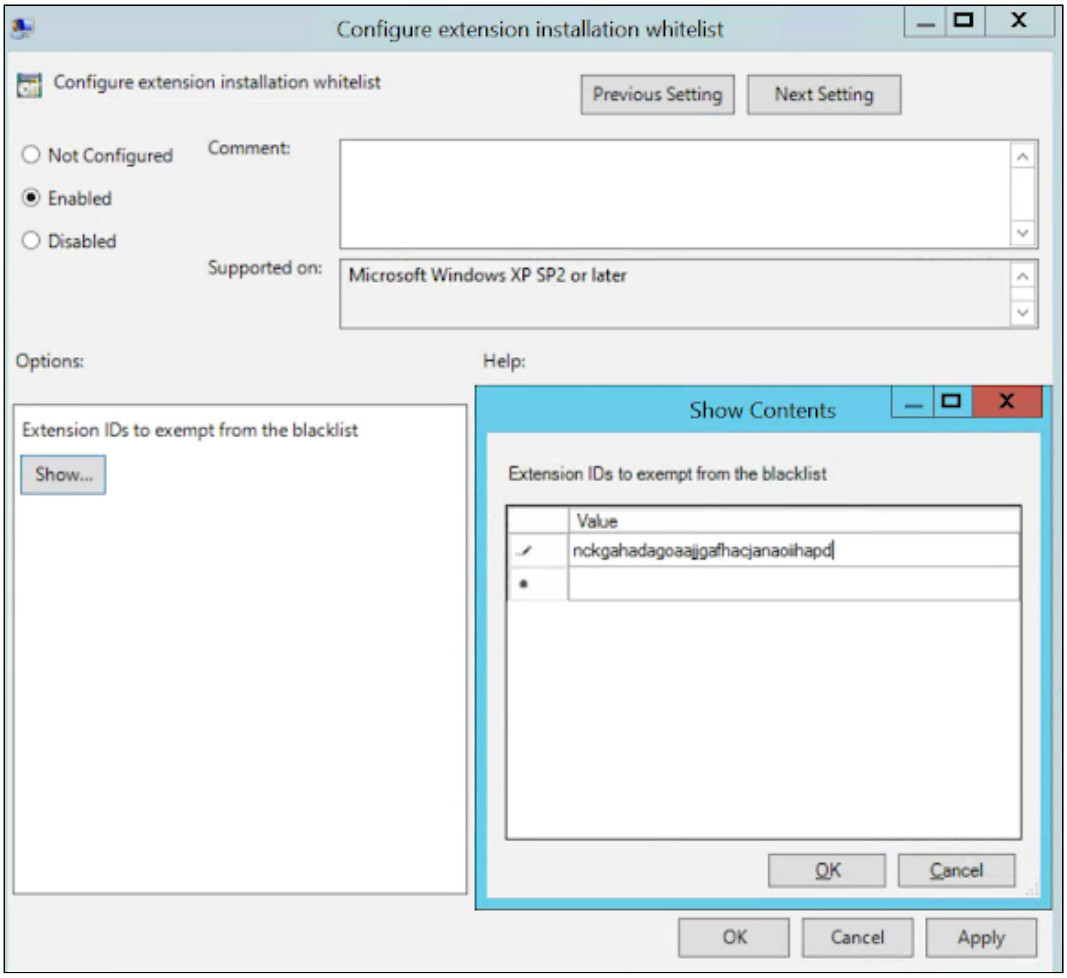
- Si no encuentra el ID de aplicación de una extensión, podrá verlo en Chrome Web Store. Allí, busque la extensión específica y verá el ID de aplicación al final de la URL en el cuadro multifunción de Chrome:



Ejemplo de ID de aplicación ubicado después de google-hangouts/

- Ingrese * en la política para evitar que se instale cualquier extensión. Puedes usar esto con la política Configurar lista blanca de instalación de extensiones. De esta manera, solo permite que sus usuarios instalen determinadas extensiones.

- Puede agregar a la lista negra una extensión que ya esté instalada en la máquina de un usuario. Así inhabilitará la extensión y le impedirá al usuario volver a habilitarla. No se desinstalará, solo quedará inhabilitada.



Configurar la lista blanca de instalación de extensiones

Cómo bloquear o permitir una extensión

Para bloquear una sola extensión, agregue el ID de aplicación de la extensión que quiera bloquear a la política "Configurar la lista negra de instalación de extensiones". Todas las demás extensiones podrán instalarse.

Para permitir una sola extensión:

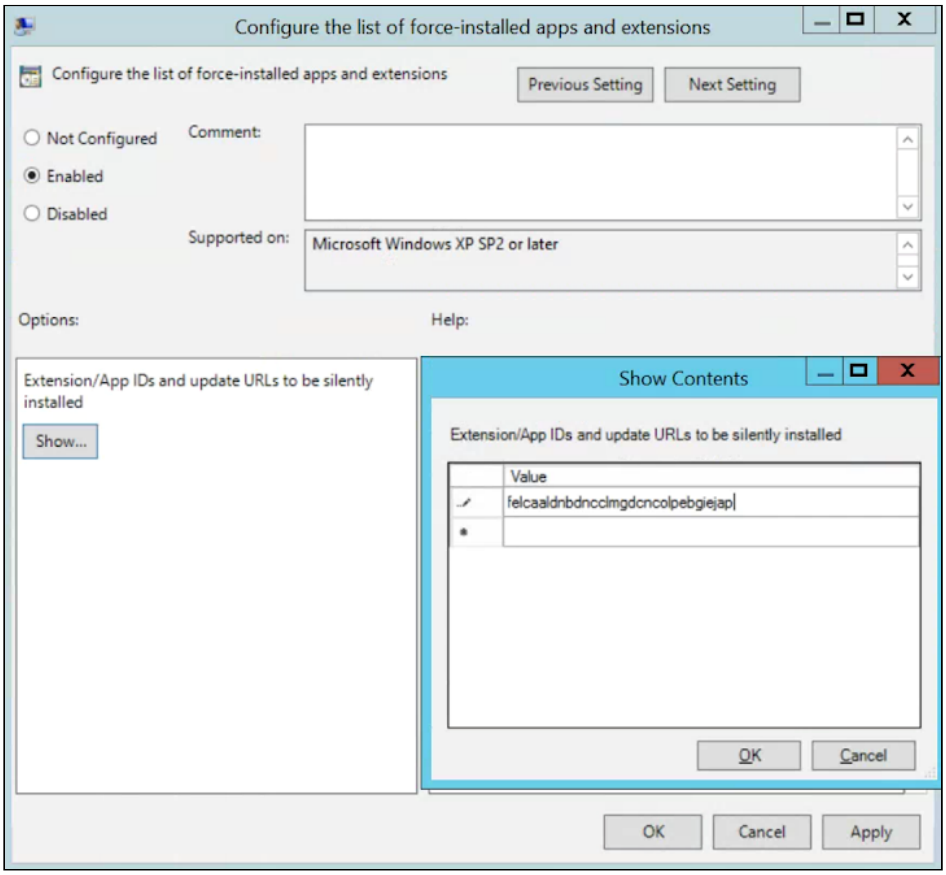
1. En la sección de contenido en la política "Configurar la lista negra de instalación de extensiones", ingrese *****.
   Así incluirá en la lista negra todas las extensiones, por lo que no podrán instalarse.

2. Agregue el ID de aplicación de la extensión permitida a la política "Configurar la lista blanca de instalación de extensiones".

Cómo instalar una extensión de manera automática

1. En el Editor de directivas de grupo, navegue a **Google > Google Chrome > Extensiones > Configurar la lista de extensiones y aplicaciones que se instalarán obligatoriamente**.
2. Seleccione **Habilitada**.
3. Haga clic en **Mostrar**.
4. Ingrese los ID de aplicación de las extensiones que quiera instalar de manera automática.

La extensión se instalará de forma silenciosa sin necesidad de que interactúe el usuario. El usuario tampoco podrá desinstalar ni inhabilitar la extensión. Este parámetro de configuración reemplazará cualquier política de lista negra que hayas habilitado.



Configurar la lista de extensiones y aplicaciones que se instalarán obligatoriamente

Cómo crear su propia tienda web local

Chrome Web Store aloja extensiones y ofrece una serie de funciones de seguridad, como escaneo automático y manual de códigos para evitar que se les envíe código malicioso a los usuarios. Existe la opción de alojar sus extensiones en su propia tienda web, pero no se recomienda. El método de hosting

propio requiere una cantidad significativa de trabajo para validar la seguridad de sus extensiones y mantenerlas actualizadas.

Si decide alojar su propia tienda, esta sección le explica cómo hacerlo. Abarca cómo empaquetar una extensión y alojarla sin usar Chrome Web Store. También incluye instrucciones sobre cómo implementar esas extensiones en sus dispositivos y usuarios.

Como alternativa a crear su propia tienda web, considere la posibilidad de marcar las extensiones internas como privadas en Chrome Web Store. Aquí se explican las diferentes opciones para publicar en Chrome Web Store.

Requisitos

Para alojar su propia extensión, deberá proporcionarle su archivo de manifiesto y sus propios servicios de hosting web. Esta ubicación de hosting no debe requerir autenticación. Debe ser accesible para los dispositivos, independientemente de dónde se usen. Tenga esto en cuenta si quiere alojar el archivo en su repositorio interno.

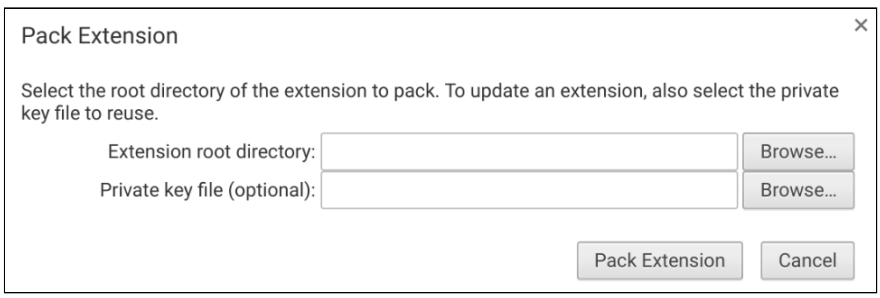
En estos pasos, se presupone que ya creó su extensión, tiene cierta experiencia con archivos XML y tiene algún conocimiento sobre directiva de grupo y el uso del Registro de Windows.

Cómo publicar su extensión

Primero, hay que empaquetar las extensiones en un archivo CRX. Si la extensión no está empaquetada como archivo CRX, siga estos pasos:

1. Vaya a **chrome://extensions** en la barra de dirección de Chrome y marque la casilla de **Modo de desarrollador**.

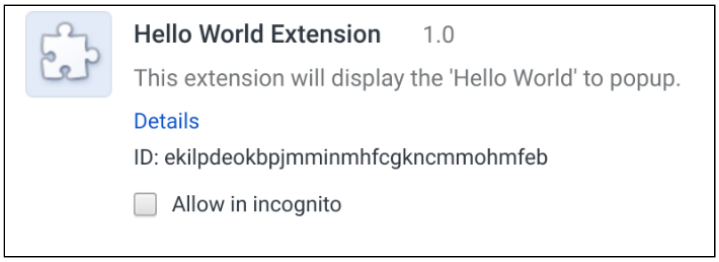
2. Una vez que estén en modo de desarrollador, cree el archivo CRX haciendo clic en **Empaquetar extensión**.
3. Seleccione el directorio donde está su fuente.
   Así se creará el archivo CRX, junto con un archivo PEM.



Selector del directorio raíz para empaquetar la extensión

Sugerencia: Mantenga el archivo PEM guardado de forma segura, ya que es la clave de su extensión. Lo necesitará para realizar actualizaciones en el futuro.

4. Arrastre el archivo CRX a su ventana de extensiones y asegúrese de que se cargue.
5. Pruebe la extensión y tome nota del campo de ID y el número de versión.
   Serán importantes más adelante.



Detalles de la extensión

5. Coloque el archivo CRX en la ubicación del host desde donde lo descargarán los usuarios o dispositivos.
6. Tenga en cuenta la URL de donde se carga el archivo.
   Será importante para el archivo XML del manifiesto.
7. Para crear un archivo XML de manifiesto con el ID de aplicación/extensión, la URL de descarga y la versión, defina estos 3 campos:

- **aplicaciónid** (el ID de la extensión del paso 3)
- **codebase** (la ubicación de descarga del archivo CRX del paso 4)
- **version** (la versión de la aplicación/extensión, que debe coincidir con la del paso 3)

Ejemplo de archivo XML de manifiesto:

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='ekilpdeokbpjmminmhfcgkncmmohmfeb'>
    <updatecheck codebase='https://app.somecompany.com/chrome/helloworld.crx'
      version='1.0' />
  </app>
</gupdate>
```

8. Suba el archivo XML completo a una ubicación desde donde sus usuarios o dispositivos puedan descargarlo y tome nota de la URL.

Cómo publicar las actualizaciones de su extensión

Asegúrese de haber hecho los cambios necesarios en su extensión y de haberlos probado. Para publicar actualizaciones, haga lo siguiente:

1. Cambie el número de versión del archivo JSON de manifiesto de su extensión por uno superior.
   Ejemplo:
   `"version": "versionString"`
   Si tiene `"version":"1.0"`, puede actualizarla a `"version":"1.1"` o cualquier número superior a `"1.0"`.

2. Actualice la `"version"` de `<updatecheck>` en el archivo XML para que coincida con el número que ingresó en el archivo de manifiesto en el último paso.
   Otro ejemplo:
   ```
   <updatecheck
   codebase='https://app.somecompany.com/chrome/helloworld.crx'
   version='1.1' />
   ```

3. Vuelva a crear un archivo CRX que incluya los nuevos cambios:
   a. Vaya a **chrome://extensions** en la barra de dirección de Chrome.
   b. Marque la casilla **Modo de desarrollador**.

4. Para crear el archivo CRX, haga clic en **Empaquetar extensión** y seleccione el directorio donde está su fuente.
   Nota: Para el archivo PEM, use el mismo archivo que se generó y guardó la primera vez que se creó el archivo CRX.
5. Arrastre el archivo CRX a su ventana de extensiones y asegúrese de que se cargue.
6. Pruebe la extensión.
7. Reemplace los archivos CRX y XML anteriores por el nuevo archivo.
   Este debe estar en la misma ubicación de host desde donde los usuarios o dispositivos descargaron los archivos anteriormente.

Los cambios se recogerán en el próximo ciclo de sincronización de políticas**.**

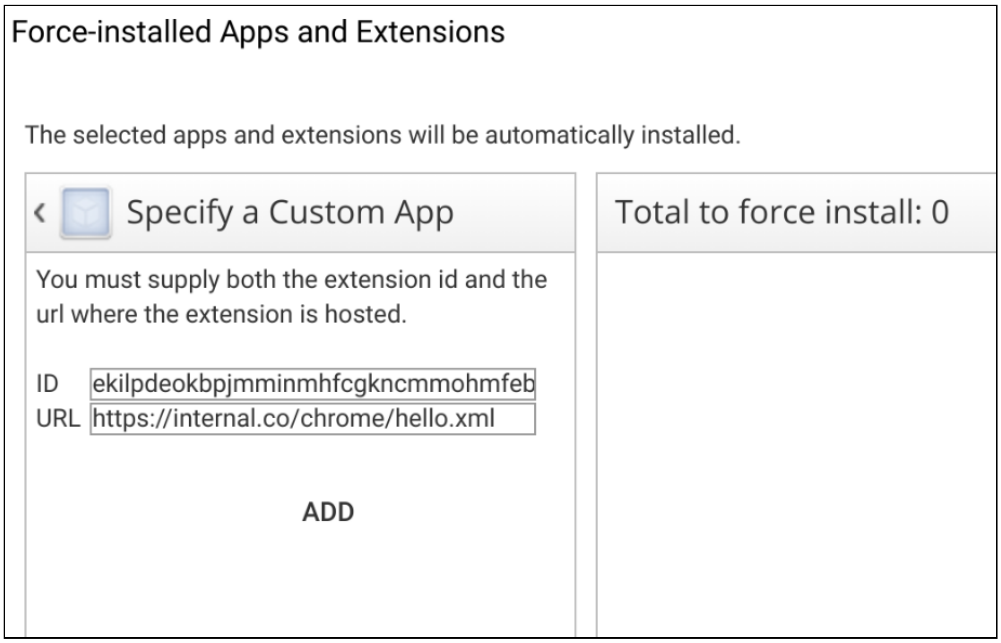
URL de referencia:

- Actualización automática
- URL de actualización
- Manifiesto de actualización

Cómo distribuir extensiones alojadas de forma privada

En la Consola del administrador de Google: Para que Chrome descargue su extensión alojada, puede seguir estos pasos.

1. Abra la Consola del administrador en admin.google.com.
2. Vaya a la sección "Administración de dispositivos" y luego a "Administración de Chrome".
3. Según el caso práctico de su extensión, seleccione uno de estos grupos de Configuración:
   - **Configuración del usuario: para extensiones que utilizarán los usuarios administrados en ese dominio que hayan accedido a su cuenta**
   - **Configuración de las sesiones públicas: para extensiones que se utilizarán en kioscos de sesión pública**
4. Asegúrese de seleccionar la unidad organizacional que corresponda para limitar el alcance de la instalación.
5. Seleccione **Especificar una aplicación personalizada**.
6. Llena el ID de sus extensiones y la URL del manifiesto XML, y haga clic en **Agregar**.



Instalar aplicaciones y extensiones de manera automática

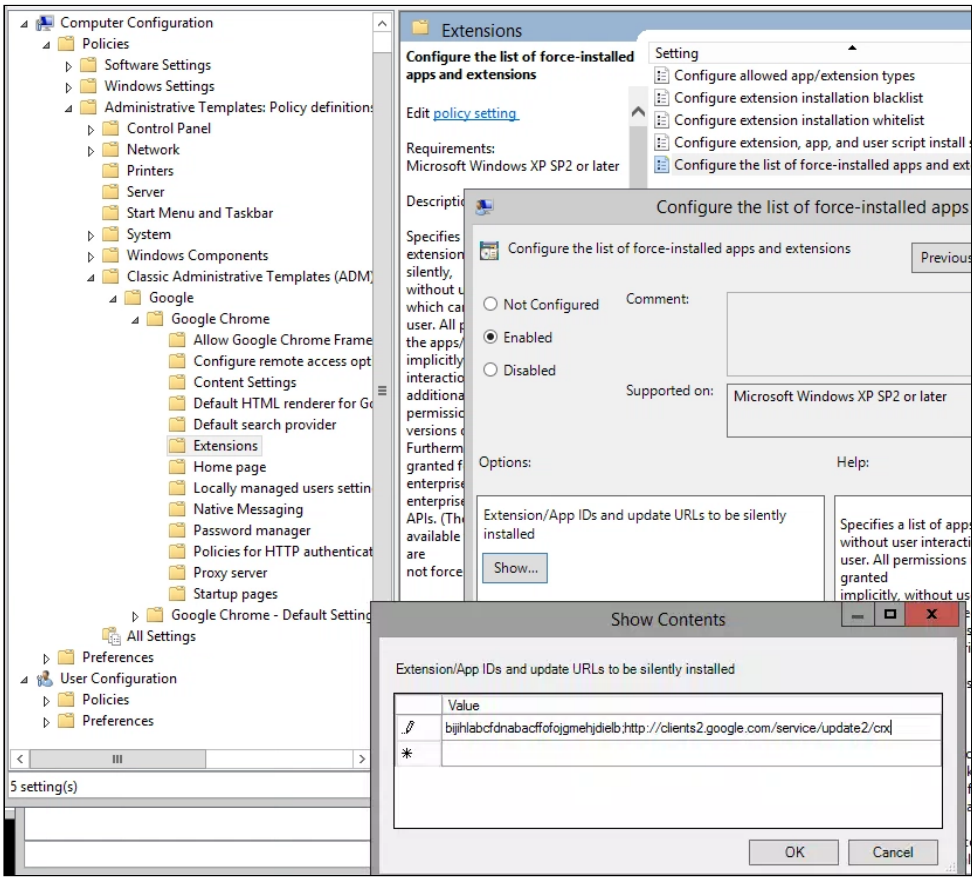
7. Asegúrese de hacer clic en **Guardar**.

Durante la próxima actualización de políticas del usuario, la extensión se instalará en los dispositivos seleccionados.

En Directiva de grupo: Si no usa la Consola del administrador, puede usar la política llamada "Configurar la lista de extensiones y aplicaciones que se instalarán obligatoriamente" para instalar una extensión de manera automática en el dispositivo del usuario.

Para aplicaciones alojadas de forma privada (que no se encuentren en Chrome Web Store), use una string como esta:
`pckdojakecnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml`

La URL se especifica en el **archivo update.xml de la aplicación interna**, en lugar de la URL `clients2.google.com`, que verá el público.



Directiva de GPO "Configurar la lista de extensiones y aplicaciones que se instalarán obligatoriamente" (Mostrar contenido)

Luego las políticas se pueden aplicar a las máquinas o a los usuarios elegidos, o a ambos. Es posible que demoren algún tiempo en surtir efecto. Para acelerar el proceso, ejecute "gpupdate" en la máquina del usuario.

Cómo gestionar extensiones mediante la Administración en la nube para el navegador Chrome

Administre el navegador Chrome en máquinas Windows, Mac y Linux desde un solo lugar, y obtenga una vista detallada del estado del navegador Chrome en su entorno. La Administración en la nube para el navegador Chrome es una nueva consola para administrar la configuración del navegador Chrome. Con ella, puede obtener rápidamente información valiosa sobre lo siguiente:

- Las versiones del navegador Chrome que tiene actualmente instaladas en sus equipos
- Las extensiones instaladas en cada navegador
- Las políticas que se aplican a cada navegador

También puede realizar acciones rápidas en la consola, como bloquear una extensión sospechosa en todas las máquinas. Administre extensiones desde cualquiera de las 3 subpáginas de la Consola del administrador. Para acceder a ellas, haga lo siguiente:

1. En la Consola del administrador, vaya a **Dispositivos > Administración de Chrome**.
2. Haga clic en **Navegadores administrados**.
3. Haga clic en cualquiera de las siguientes subpáginas para administrar extensiones:

- **Aplicaciones y extensiones instaladas:** En esta página, puede ver las extensiones instaladas, sus estadísticas, cómo se instalaron, la versión y el canal de versiones, y en qué perfil de usuario está instalada. Esta consola le da más control para administrar extensiones y ver qué aplicaciones hay instaladas. Si hace clic en Más  en cada extensión, verá 2 acciones:
  - **Bloquear:** Impide que se ejecute la extensión.
  - **Instalar de manera automática:** Exige la extensión seleccionada y la instala automáticamente.
- **Detalles del dispositivo:** En esta página, puede ver el nombre, la versión de SO, los detalles de usuarios, la arquitectura (32 o 64 bits), la fecha de inscripción y cuántas políticas se aplican en una máquina administrada.
- **Navegador y perfiles:** Aquí puede ver la versión del navegador y el canal de versiones (Estable, Para desarrolladores, Beta o Canary), así como a qué perfiles está vinculado el navegador Chrome.

Recursos adicionales

A continuación, le ofrecemos más recursos para ayudarlo a administrar el navegador Chrome en su organización:

- Guía de implementación del navegador Chrome (Windows)
- Lista de políticas de Chrome
- Notas de la versión de Chrome Enterprise
- Centro de ayuda de Chrome Enterprise
- Configure Chrome como navegador predeterminado (Windows 10)