chrome enterprise

Getting started: a guide to managing Chrome Browser Enterprise extensions

Introduction

There are thousands of Chrome Browser extensions available, and many of them do amazing things that save people time, improve business workflows, and enhance efficiency. From optimizing RAM utilization to increasing browser speeds and editing your grammar, extensions are built to improve our productivity at work – but it's important to remember that they can also introduce risk and vulnerabilities to an enterprise environment if they're not properly managed. For this reason, enterprise IT teams must balance users' productivity needs with the company's security needs.

When it comes to extension management, enterprise IT teams have three main priorities:

1. Protecting user and company data
2. Preventing the installation of malicious extensions
3. Ensuring users have access to the extensions they need to improve productivity and efficiency

chrome enterprise

With so many new and existing extensions and constant updates being made, it's crucial administrators follow best practices to monitor, manage, and secure their users' Chrome extensions.

This whitepaper will explain various extension management options and help you choose the method that best fits your needs.

Criteria to consider

Before you jump into managing extensions, you should first identify the parameters your organization will use to assess and approve them. To do this, you'll want to answer the following questions:

- What are the security regulations and compliance measures our organization needs to adhere to?
- What user and corporate data is being stored on users' devices?
- Which extension-requested permissions could potentially violate our data security policies?

Once you have your answers clearly defined, you're ready to consider your extension management options.

The traditional approach: whitelists and blacklists

For a long time, the only way to manage browser extensions was to manually evaluate each extension and then create whitelists and blacklists to dictate which extensions could and could not be installed on users' devices. Some organizations still use this approach today.

In the Google Admin console, you can choose to:

- Allow all extensions except those you want to block
- Block all extensions except those you want to allow
- Block or allow individual extensions
- Force-install one or several extensions

In Microsoft[1] Group Policy you can use templates to achieve similar protections that are applied to certain groups or the entire organization, including:

- Allow all extensions except those you want to block
- Block or allow one extension
- Force-install an extension

Both of these approaches work to a certain. They do have their limitations and they're very manual – which means they require a lot of human effort.

Their review times can negatively impact both user and admin productivity and you'll also need to security extensions that have already been whitelisted can be sold to and/or updated by entities that you have not vetted.

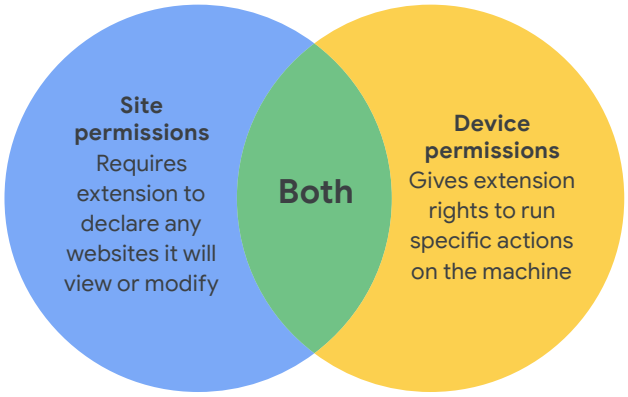
[1]Microsoft ®, Windows ®, and Internet Explorer ® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

A modern approach: managing extensions by permissions

To make enterprise extension management more efficient, scalable, and secure, Chrome also allows you to manage extensions requested by permission. Managing extensions by permissions make it possible for IT teams to give their users the extensions they want without putting corporate data at risk. It's the method Google's IT team uses and recommends for other enterprises.

Permissions give an extension the ability to make changes to website or device. For an extension to run properly, specific permissions are often required.

There are two main categories of extension permissions: site permissions and device permissions. Many extensions use both.



Some examples of site permissions include allowing an extension to block images or allowing an extension to control how much you can zoom into/out of a site. Examples of device permissions include accessing USB ports, viewing the screen, and interfacing with native programs.

To further mitigate risk, consider managing extensions with the following policies:

- **Blocked/allowed permissions:** Protects against already-whitelisted extensions updating with new permissions – and you can disable extensions post-install if they no longer meet your requirements
- **Runtime block hosts:** Specifies which sites extensions can run on
- **Force installed extensions:** Universally installs extensions on your users' machines so they have the tools they need to be productive
- **Whitelist/blacklist:** If required

This Chrome extension management method is more secure, easier to manage, and scales well for large organizations. It protects users from compromised extensions and saves IT time because they no longer have to manage excessively long whitelists/blacklists, review updates, or individually vet each extension. It's truly a win-win.

chrome enterprise

Get started: managing extensions by permission

To begin managing your enterprise extensions by permission, follow these steps:

1. Make a list of what extensions your users already have installed (use Chrome Browser Cloud Management reporting or survey your end users)
2. Identify what websites/hosts must be secure
3. Determine which permissions pose potential risks and need to be restricted
4. Build a master list of all of the data you've collected and share it with essential stakeholders to get buy-in
5. Test your new policies in a test environment or with a small pilot group, then roll the new sets of policies to employees in phases
6. Review feedback from users
7. Repeat and fine-tune the process on a monthly, quarterly, or annual basis (whatever is appropriate for your organization)

You only need to set the policies once to enforce a baseline of allowed permissions and protect sensitive corporate sites. Not only is your enterprise automatically more secure, your users also get a better experience.

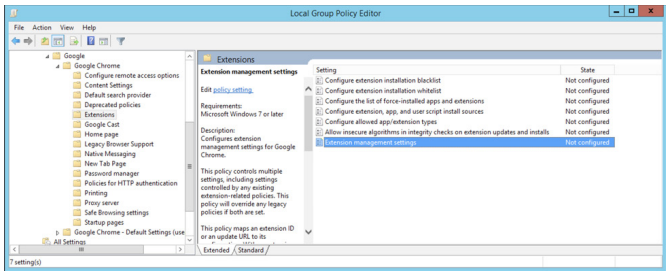
Employees may even be able to install extensions that they couldn't before, they just won't be able to run them on sensitive business sites.

Setting permissions

You can easily control which extensions your users are allowed to install. You simply have to designate which permissions are acceptable and flag the permissions that are not.

Google Admin console

In Windows, Chrome OS, Mac[2], and Linux environments you can use the Google Admin console to set these controls. If an extension requires access or permissions that violate your security policies, it won't be installed. For example, you can block an extension that connects to your users' USB devices or prevents access to reading cookies. If an installed extension needs permission that is blocked, it simply won't run. The extension isn't removed; it's disabled.



Group Policy

Another common way to manage extensions in Windows is to use the extensions settings policy. The group policy management editor allows you to set multiple policies in one place using a JSON string or in the Windows Registry. The extensions setting policy can control things like installation

[2] Mac and macOS are trademarks of Apple Inc., registered in the U.S. and other countries.

mode, update URL, blocked permissions, install sources, allowed types, blocked install, and runtime blocked and allowed hosts. You can decide if you want to set all extension management settings here, or you can set these controls through other individual policies. The setting is set using either Windows registry or JSON string in Windows Group Policy Editor.

Additional considerations

Some enterprise organizations prefer to launch their own site for downloading extensions. Google does not recommend this approach as it can be less secure than the Chrome Web Store, which has automated and manual code scans that prevent malicious code from being sent to users.

Chrome Browser Cloud Management is a new console that allows you to manage your Chrome Browser settings for your Windows, Mac, and Linux machines all in one place. The console offers an in-depth view of the state of Chrome Browser in your environment, providing instant insight into:

- Current Chrome Browser versions deployed across your fleet of desktops and laptops, regardless of desktop or laptop type
- Extensions installed on each browser
- Policies being applied to each browser

The console also allows you to block a suspicious extension on all of your machines with the click of a button.

Manage Chrome extensions like we do at Google

After using traditional blacklist and whitelist extension management method on its 300,000+ endpoints for years, Google's internal IT team knew they wanted to create a less cumbersome approach that balances the needs of enterprise IT and security with employee productivity. Their solution, managing extensions by permission, is a scalable, secure solution that greatly reduces overhead.

Like Google, you can make the switch from whitelists and blacklists to the more secure method described in this whitepaper. You'll get the security your enterprise needs while still allowing users to install safe, productivity-boosting extensions.

Start managing your extensions by permissions today.

To deepen your understanding of Chrome Browser extension management, **consider the following resources:**

Read the Managing Extensions in Your Enterprise guide

Watch Google Cloud Next '19 Breakout Session: How Google Cloud IT Manages Enterprise Extensions

Explore Chrome Browser Cloud Management options

View Chrome Browser downloads for your enterprise

Learn more about Chrome Browser Enterprise Support

Explore the Chrome Browser Policy List

Visit the Chrome Browser Enterprise Help Center and Chrome Browser Help Forum