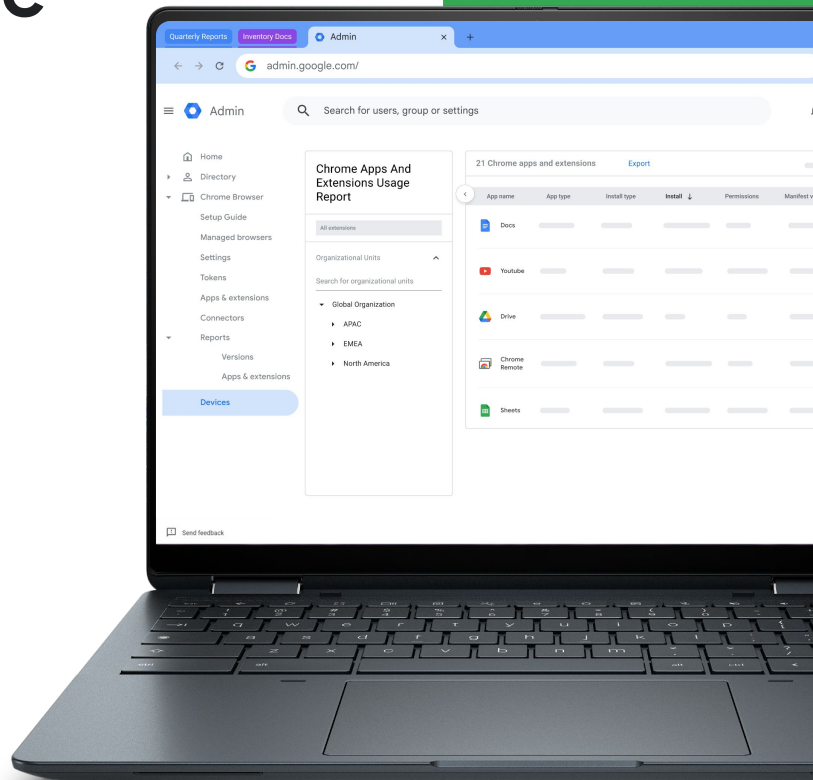




# Managing **Extensions** with Chrome Enterprise

Updated April 2024



## Introduction

There are thousands of Chrome browser extensions available that do amazing things. From optimizing RAM utilization to increasing browser speeds and editing your grammar, many extensions are built to improve our productivity at work. However, 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 and security teams must balance users' productivity needs with protections for the company.

### **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

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

## 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?
- What data is being requested by extensions?

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

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

## Managing Extensions Manually

For a long time, the only way to manage browser extensions was to manually evaluate each extension and then create allowlists and blocklists 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:

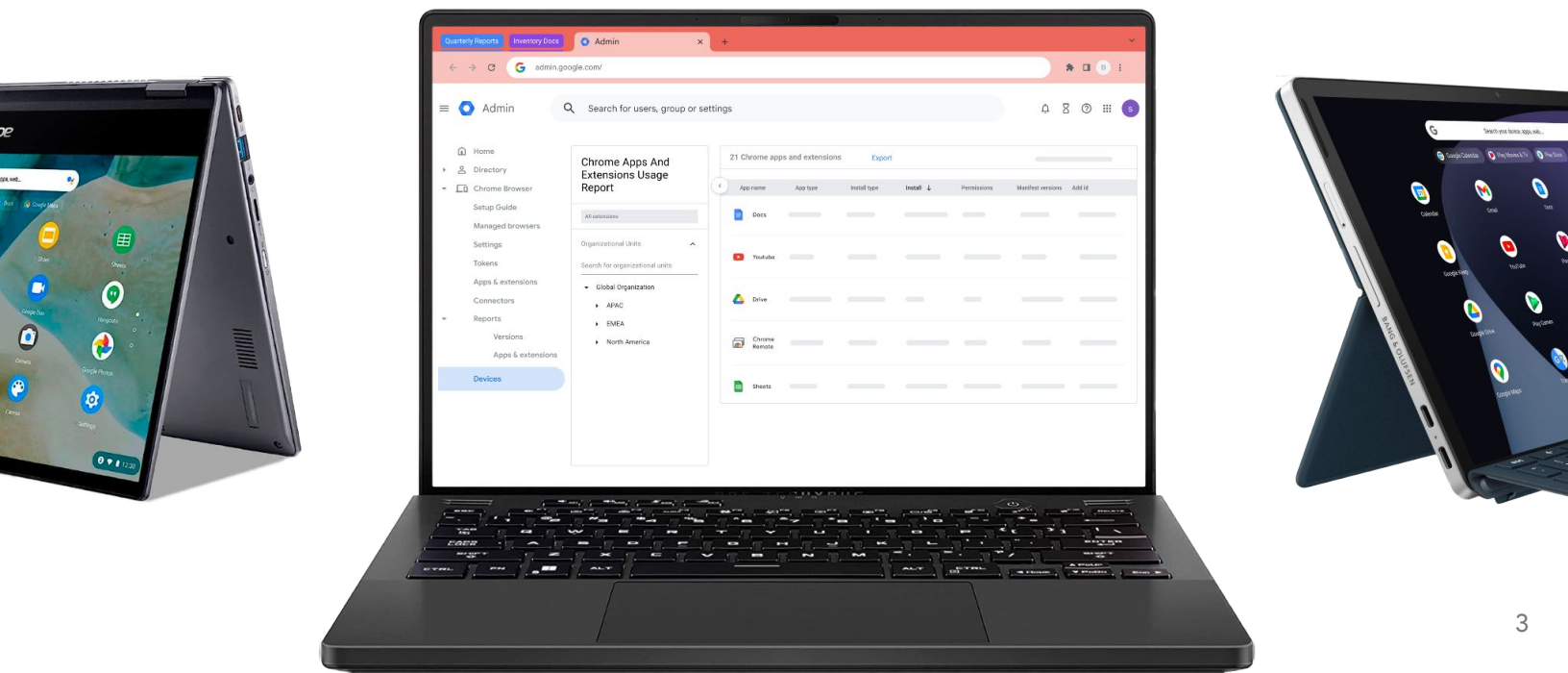
- Allow all extensions except those you want to block
- Block all extensions except those you want to allow
- Block or allow individual extensions
- Force install one or several extensions

In Microsoft's 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 degree. 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, perhaps most importantly from a security perspective, already allowlisted extensions can be sold to and/or updated by entities that you have not vetted.

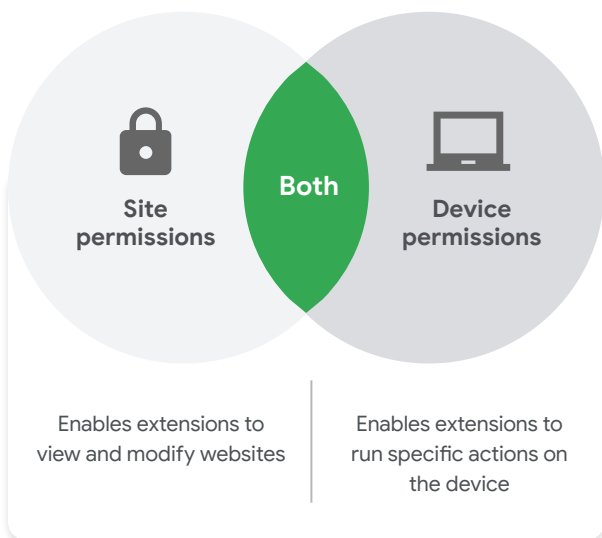


## Managing Extensions by Permissions

To make enterprise extension management more efficient, scalable, and secure, Chrome Enterprise also allows you to manage extensions based on permissions. Managing extensions by permissions makes 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 a 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 and out of a site. Examples of device permissions include accessing USB ports, viewing the screen, and interfacing with programs.

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

- **Blocked permissions:** Blocks extensions with permissions you don't want running in your environment and already installed extensions seeking update permissions that you don't allow
- **Runtime block hosts:** Blocks extensions from running on your most sensitive sites while allowing them to work elsewhere
- **Force-installed extensions:** Silently installs extensions on your users' machines so they have the tools they need to be productive
- **Allowlists and blocklists:** If required

The Chrome Enterprise approach to extension management 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 allowlists or blocklists, review updates, or individually vet each extension. It's truly a win-win.

## Getting Started

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

1. Make a list of the extensions your users already have installed (use reporting within [Chrome Enterprise Core cloud management](#) or survey your end users). Consider using an API to export your data directly into a spreadsheet. For more information, check out this [YouTube video](#).
2. Identify what websites/hosts must be secure. Determine which permissions pose potential risks and need to be restricted.
3. Build a list of all of the data you've collected and share it with essential stakeholders to get buy-in.
4. Trial your new policies in a test environment or with a small pilot group, then apply the new sets of policies to employees in phases.
5. Review feedback from users.
6. Repeat and fine-tune the process on a monthly, quarterly, or annual basis – whatever is appropriate for your organization.

With this strategy, not only is your enterprise automatically more secure, your users also get a better experience.

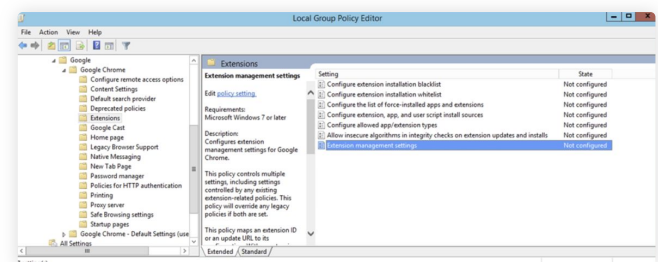
Employees may even be able to install extensions that they couldn't before – they just won't be able to run them on sensitive business sites.

## 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, ChromeOS, Mac, 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. For more information on managing extensions in the Google Admin console, check out this [YouTube video](#).



### Group Policy

Another common way to manage extensions in Windows is to use the [Extensions Settings policy](#). The Group Policy Management Console allows you to set multiple policies in one place using a JSON string or in the Windows Registry. The Extensions Settings policy can control things like installation 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

If you decide that managing an allowlist or blocklist is for you, you should consider using the Extension Workflow feature of Chrome's cloud management tool. This feature works with your existing allowlist and enables users to request extensions directly from the Chrome Web Store. Those requests show up in the Google Admin console, where you can review them for security and productivity requirements and allow or block them with a click of a button. For more information on this feature, check out this [YouTube video](#).

[Chrome Enterprise Core](#) allows you to manage and secure your entire browser fleet in one place, including your deployments on Windows, Mac, Linux, Android, and iOS machines. The Google Admin console offers an in-depth view of the state of Chrome in your environment, providing instant insight into:

- Current Chrome versions deployed across your fleet, regardless of device 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 Google

After using a traditional allowlist and blocklist 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 permissions and website access, is a scalable, secure approach that greatly reduces overhead.

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



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

- Read the [Managing Extensions in Your Enterprise guide](#)
- Watch [Managing Extensions in Chrome's cloud management tool](#) and the [Extension Workflow demo](#)
- Explore [Chrome Enterprise Core](#) options
- View [Chrome browser](#) downloads for your enterprise
- Learn more about [Chrome Enterprise support](#)
- Explore the [Chrome Enterprise policy list](#)
- Visit the [Chrome Enterprise and Education Help Center](#)