



# Understanding Your Chrome Browser Update Options in Windows Environments

Updated May 2024



## Introduction

IT and security professionals face new challenges as employees and third-party contractors increasingly rely on the browser to access business tools, collaborate with colleagues, and manage ever-evolving workflows. Providing stable, secure, and simple access to company resources from any location via the browser is a top priority.

Centrally managing the browser fleet is crucial to improving the security and productivity of browser deployments. Enterprises that don't manage their browser fleet may struggle with challenges like:

- Lack of visibility into what's happening with their browsers
- Inability to customize policies based on business needs
- Missed opportunities for added security controls that could be protecting their users

IT decision makers consistently emphasize the need for tools that can save time and enhance efficiency. [Chrome Enterprise Core cloud management](#) offers a centralized tool for configuring and managing browser policies, settings, apps, and extensions across Chrome – no matter the operating system, device, or location. Chrome Enterprise Core is available to all enterprises using Chrome at no cost.

The Chrome Enterprise Core cloud management tool can deliver significant benefits to businesses. A recent study found that enterprises using the cloud management tool experienced the following benefits<sup>1</sup>:

- Seventy-five percent of IT time saved on activities such as responding to tickets and packaging and confirming updates
- Improved user productivity through 30% fewer service desk tickets
- Twenty percent time savings for developers
- Avoiding \$2.6 million in breaches, compliance fines, and related security team tasks due to improved security

Chrome Enterprise Core offers access to a broad range of customizable controls, so you can configure Chrome to fit the unique needs of your organization. For example, keeping your fleet up to date with the newest security patches is simple with automatic updates. Users are prompted to relaunch Chrome to update to the latest version to ensure fast protections from zero-day vulnerabilities.

This technical paper will describe the different release channels and update options available to you and provide recommendations to consider as your enterprise evaluates how to manage Chrome.

<sup>1</sup>A commissioned study conducted by Forrester Consulting on behalf of Google, "The Total Economic Impact™ of Google Chrome Browser Cloud Management", 2023

# Getting to Know Chrome Browser Release Channels



4 weeks to stable	8 weeks to stable		9+ weeks to stable	
Channel: Stable	Channel: Extended	Channel: Beta	Channel: Dev	Channel: Canary
<ul style="list-style-type: none"> <li>Fully tested by the Chrome test team</li> <li>Should be used by most of your workers</li> <li>Updated every 2 to 3 weeks for minor releases and every 4 weeks for major releases</li> </ul>	<ul style="list-style-type: none"> <li>Feature updates occur less often than the Stable channel</li> <li>Fully tested and includes critical fixes</li> <li>May be preferred if you manually update to new releases of Chrome or want a slower release cadence</li> <li>Updated every 8 weeks</li> </ul>	<ul style="list-style-type: none"> <li>4 to 6 week preview of what's coming to the Stable version of Chrome</li> <li>Some features may require you to communicate additional information to users</li> <li>Gives you time to address issues before the release is rolled out to the full enterprise</li> <li>Updated (roughly) weekly</li> </ul>	<ul style="list-style-type: none"> <li>9 to 12 week preview of what's coming to the Stable version of Chrome</li> <li>Updated 1 to 2 times per week</li> <li>Your developers and IT staff can identify and report any changes that impact your environment on the Chromium site</li> </ul>	<ul style="list-style-type: none"> <li>Future version of Chrome still in development</li> <li>Unstable for everyday use as features appear and disappear</li> <li>Not recommended unless Google Cloud Support asks you to test it</li> </ul>

For more than a decade, Chrome has shipped a new milestone every 6 weeks, delivering security, stability, speed, and simplicity to our users and the web. Over time, we've improved our testing and release processes, which improved our patch gap and now allows us to shorten our release cycle to deliver new features more quickly. Since M94, Chrome now ships a new milestone every 4 weeks on the Stable channel, and every 8 weeks on the Extended Stable channel.

Chrome also has 3 more update channels: Beta, Dev, and Canary. The Beta, Dev, and Canary channels can run side-by-side with the Stable or Extended Stable channels on the same machine, making testing easier for enterprises.

To move your browsers between the Stable, Extended Stable, Beta, or Dev channels, you can use the [TargetChannel](#) policy.

## Stable Channel

The Stable channel has been fully tested by the Chrome test team and is the most secure version available. It features critical fixes to vulnerabilities and is the best bet to avoid crashes and other issues. It's updated roughly every 2 to 3 weeks for minor releases and every 4 weeks for major releases.

### **Recommendation:**

Other than the people you assign to the Beta and Dev channels (details below), the rest of your organization should be on the Stable channel for all mission-critical browser-centric activity. If you find a bug in the Stable release, you can report it at [crbug.com](https://crbug.com).

## Extended Stable Channel

Like the Stable channel, the Extended Stable channel has been fully tested and contains critical fixes to vulnerabilities and other issues. However, some security-positive changes and new features available with Stable may not be immediately included in Extended Stable. Minor releases are every 2 to 3 weeks and major releases are every 8 weeks.

### **Recommendation:**

Segments of your organization that need more stability can use the Extended Stable channel. The longer cycle for milestone updates gives admins more time to vet each new set of features before they're delivered to end users. This also reduces the need to pin to a particular milestone in order to ensure stability for those users.

## Beta Channel

On the Beta channel, you can see what's next with minimal risk. Google actively investigates issues on this channel that are reported to the Chrome release bug list, [crbug.com](https://crbug.com). Minor updates occur roughly every week, with major updates every 4 to 6 weeks before they're released to the Stable channel.

You might find some features aren't suitable for all your users. With the Beta channel, you can plan for a full rollout to your organization as well as investigate ways to control certain features through a policy. Uncovering issues on test devices gives you lead time to report issues. If Google can't resolve the issue prior to the next Stable release, you can decide to block the update before it reaches all your users.

### **Recommendation:**

Keep 5% of your organization (including IT staff, developer staff, and business users) on the Beta channel. If you have multiple types of hardware, Google also recommends that you keep 5% of each type of hardware on the Beta channel. With this recommendation, you get a 4-week lead time to engage multiple users and hardware types in testing.

## Dev Channel

You can use the Dev channel to stay aware of upcoming updates and features. Releases to the Dev channel occur 9 to 12 weeks before the next Stable channel release. Because it's an early release of Chrome, the Dev channel is not 100% stable. Your IT and developer staff can use it to ensure apps and systems are compatible with upcoming updates and feature changes. Updates are 1-2 times per week. There's no lag between major versions, so you get whatever code Google has. While the Dev channel build does get tested, bugs should be reported to the Chrome release bug list, [crbug.com](https://crbug.com).

### Recommendation:

You might want to keep a few IT staff members and developers on the Dev channel. They can identify and report any changes that could impact your environment before the changes reach your users on the Beta, Stable, or Extended Stable channels. While Google automatically fixes most issues before a release is marked as Stable, it may not be able to catch all the corner cases that could uniquely impact your environment. By having IT and developer staff on the Dev channel, you can quickly identify and report any changes that may impact your environment before they reach Beta or Stable.

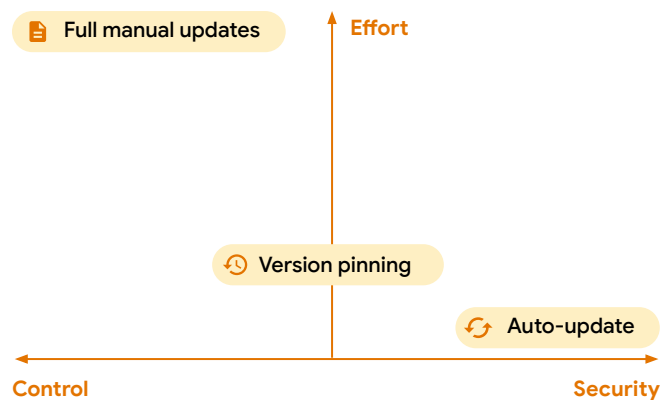
## Canary Channel

Builds for the Canary channel are released nightly and have not been tested or used. Releases to the Canary channel occur more than 8 weeks before the next release to the Stable channel. Bugs should be reported to the Chrome release bug list, [crbug.com](https://crbug.com).

### Recommendation:

Unless you have a business need for advanced testing, you shouldn't have any staff on the Canary channel, as it's the least stable.

## Identifying Chrome's Update Options



## Auto-Update

Provide fast-paced protection for known vulnerabilities. Your users only need to relaunch Chrome for the updates to take effect. Auto-updates eliminate the need for IT staff to manually fix problems, because users are all on the same version of Chrome.

### Recommendation:

Users who mostly use cloud-based apps are good candidates for auto-updates. Assess your IT environment, operational and security needs, and put users in two groups: those who can use auto-updates and those who cannot. For those who cannot, consider version pinning. Then, develop a plan to move as many users and devices as possible to auto-updates.

## Version Pinning

Version pinning allows you to control when your users receive updates, to meet your software distribution requirements, and to align with the regular update process of your organization. Your IT department can govern the update process. Users will not be able to update to an unpinned version. Your organization might need to pin to a particular version of Chrome for application compatibility, testing requirements, change management, security reviews, or regulatory requirements. If so, it's important to get your testing staff on the Beta and Dev channels as soon as possible. They can test early and keep up with the latest version of Chrome.

### Recommendation:

Pin to the most recent major Chrome version you've reviewed and tested, and [subscribe](#) to the [Chrome Enterprise release notes](#). Your users will continue to receive minor updates, including security fixes. When a new release is available, review the release notes to determine what testing is needed, and begin your vetting process. When you're ready, change your pin to the most recent version you've vetted, or remove it altogether to let users update to the latest version of Chrome.

## Full Manual Updates

Some organizations run Chrome in extremely locked-down environments without internet access, and the browser is used to access internal web apps only. Automatic updates are not an option for keeping Chrome up to date in this type of environment, and the browser must be updated manually.

### Recommendation:

Google does not recommend updating your browsers manually unless it is critical for compliance in your organization. Without access to automatic updates, browsers can miss critical fixes, leaving them susceptible to vulnerabilities that can compromise your secure environment. Applying updates in a timely manner is extremely labor-intensive, as is rolling back if necessary. Additionally, older versions of Chrome may not be covered by Chrome Enterprise support if any issues arise.

## A Hybrid Approach to Chrome Updates

Your organization may benefit from taking a hybrid approach to updating Chrome, where some users auto-update, some users are manually updated on a regular cadence, and some users have disabled updates and stay on a single version for a longer period of time.

This approach allows you to mix and match Chrome updates according to business needs while still getting some of the security and efficiency benefits from auto-updates. For example, you might set up Organizational Units (OUs) that roughly correspond to various business groups. For some of these groups, you might deploy an auto-update model, and on other groups, a version pinning model.

A segmentation approach is often required if you go this route, along with a solid understanding of the different application needs or requirements across multiple business groups.

## Chrome's Policy Template Capabilities

You can use the files in Chrome's cloud management tool to install and manage Chrome on your managed Windows devices. After Chrome is installed on your users' devices, you can use your preferred on-premise tools (such as Windows Group Policy) or the Google Admin console to enforce policies on the devices.

You can:

- Set device-level policies (not applied to a specific user)
- Set OS user-level policies that apply when specific users are signed in to the device
- Enforce policies that users cannot modify
- Deploy default preferences that users can change

To help with policy setup, Google provides policy templates (ADMX and ADM) that you can install and update. The templates are updated with new policies as they relate to new versions. In some cases, policies are deprecated. You need to download the new policy templates to use the latest policies, even if you are using auto-updates.

### **Recommendation:**

Use the [Chrome Enterprise and Education release notes](#) as a guide for new or changing policies. You can also download Dev and Beta channel policy templates to see changes ahead of time.

## Other Chrome Update Considerations

Enterprises should also be aware of updates related to how Chrome:

- Enables management of third-party extensions
- Provides Legacy Browser Support

### **Managing updates to third-party extensions**

Chrome's cloud management tool provides a variety of policies around extension access and management. But the extensions themselves have their own update process. You can manage extensions using auto-updates, manual updates, disabled updates, or the hybrid approach. For details regarding each extension, visit the [Chrome Web Store](#).

### **Legacy Browser Support**

If your organization wants to take advantage of Chrome but your users still need to access older websites and apps that require Microsoft Internet Explorer, you can use Chrome's [Legacy Browser Support](#) to automatically switch between Chrome and another browser. When one of your users clicks a link that requires a legacy browser, such as a site that requires ActiveX, the URL will automatically open in the legacy browser. They can seamlessly get back to Chrome when visiting other sites.

Legacy Browser Support can be enabled in Chrome's cloud management tool or Group Policy.

## Next Steps and Resources

Chrome Enterprise understands you have complex policies and requirements regarding software updates. You have to take into account software features and compatibility, security updates, internal application testing and policy administration, employee training, and many other critical factors. With the Stable, Beta, Dev, and Canary release channels and other options outlined in this technical paper, your enterprise can develop its preferred Chrome update strategy that maintains security and operational effectiveness.

As you develop your Chrome update strategy, keep the following in mind:

- Determine your bandwidth and tolerance for new updates in your organization
- Weigh the trade-off between security and your ability to control update timing
- Review Chrome's release notes and documentation early
- Familiarize yourself with Chrome's release channels to maximize testing opportunities
- Have 5% of your IT, dev, and business users testing on the Beta channel so you can report issues you find before code reaches the Stable channel
- See if there is an opportunity to segment users into OUs where some users can use auto-updates and others can use version pinning
- If you find a bug across any channel, you can report it at [crbug.com](https://crbug.com), where the Chrome Enterprise team actively investigates reported issues.

You can also purchase Chrome Enterprise support to get help configuring, deploying, and managing Chrome for users in your organization. You can get help from experts 24/7 for the Stable, Beta, and Dev channels. Some organizations that choose to manage updates manually can troubleshoot challenges quickly with 24/7 access to experts, making it easier to stay on track with rolling out their own updates.



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

- Download for your enterprise: [Chrome](#)
- Learn more about: [Chrome Enterprise support](#)  
[Get in touch with browser specialists](#)
- Explore: [Chrome Enterprise policy list](#)
- Read the latest: [Chrome Enterprise and Education release notes](#)
- Visit: [Chrome Enterprise Help Center](#)  
[Google Chrome Help Community](#)
- Review: [Chromium's public bug tracker](#)