



Understanding your Chrome browser update options in Windows environments

Updated September 2021

Introduction

Many people working in enterprise environments use cloud- and browser-based business apps—often on a variety of devices—to conduct their daily work. In fact, some cloud workers would say their ability to access company resources from any location via their browser significantly enhances their effectiveness¹.

While the browser has become a mission-critical enterprise application, it also poses challenges for

IT professionals managing Windows environments.

These challenges include:

- Many enterprises have not standardized on a single browser.
- IT teams are challenged to keep all browsers up to date for optimal security.



- App compatibility across browsers may differ, especially between legacy and modern browsers.

Chrome is a common choice for enterprises, especially as users find it to be a familiar browsing experience. And as a modern browser for enterprises, Chrome uses an automatic update model to ensure fast and secure updates across enterprise environments.

Given the challenges facing IT teams, especially the complexity of Windows environments,

Chrome gives admins a variety of options for managing your browser on Microsoft™ Windows™ computers. You can use different update channels for different users. This technical paper will describe the different options available to you for updates and provide some recommendations as your enterprise evaluates how you manage Chrome.

Getting to know Chrome browser update channels

|  | | 4 weeks to stable | 8 weeks to stable | More than 8 weeks to stable |
|--|---|---|--|--|
| Extended Stable | Stable | Beta | Dev | Canary |
| <ul style="list-style-type: none"> • Update (roughly) every two weeks for minor releases and every eight weeks for major releases • Fully tested and approved by Chrome test team • More time to vet new features | <ul style="list-style-type: none"> • Update (roughly) every two weeks for minor releases and every four weeks for major releases • Fully tested and approved by Chrome test team • Most secure channel | <ul style="list-style-type: none"> • Update (roughly) weekly • Major updates every four weeks | <ul style="list-style-type: none"> • Update once or twice weekly • What Google is working on now • No lag between major versions • Gets tested but still subject to bugs | <ul style="list-style-type: none"> • Bleeding edge builds • Release nightly/ as soon as built • Not tested or used • Can be unstable |

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. Starting with 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 three early access update channels: Beta, Dev, and Canary. Stable channel installs can be moved between the Stable, Extended Stable, Beta, and Dev channels via the [TargetChannel](#) policy. In addition, the Beta, Dev, and Canary channels can be installed and run side-by-side one another and Stable Chrome.

Stable channel

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

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, since Extended Stable receives every other major milestone (for example, Stable goes from 94 to 95 to 96, whereas Extended Stable goes from 94 straight to 96). Major releases are every eight weeks and minor releases are every two weeks.

Recommendation:

Segments of your organization that need more time between releases can go on the Extended Stable channel. The longer cycle for milestone updates gives admins the ability to keep users on the same version of Chrome for longer, while reducing the need to pin to a specific version. It is a light touch update mechanism - set the policy once and you're done.

Beta channel

You can see what's next, with minimal risk, on the Beta channel. Google actively investigates issues on this channel that are reported to the Chrome release bug tracker, crbug.com. Minor updates occur roughly every week, with major updates every four 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 percent 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 percent of each type of hardware on the Beta channel. With this recommendation, you get a four-week lead time to engage multiple users and hardware types in testing.

There are two ways to do this. You can install Beta side-by-side with Stable, allowing users to run either at their discretion - if they discover a problem with Beta, they can report it and switch to Stable. Alternatively you can use TargetChannel to set those browsers to the Beta version. If a user discovers a problem, they can report it, but they will need an admin to modify their TargetChannel policy setting to move them back to Stable if there is a critical problem.

Dev channel

You can use the Dev channel to stay aware of upcoming updates and features. Releases to the Dev channel occur eight weeks before the next Stable channel release. Because it's an early release of Chrome, the Dev channel is not as stable as Beta and Stable. Your IT and developer staff can use it to ensure apps and systems are compatible with upcoming updates and feature changes. Updates are once or twice weekly. 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.

Recommendation:

You might want to keep a few people from your IT staff and some 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 may uniquely impact your environment. By having a few 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. Because Dev can be unstable, we recommend running it side-by-side with Stable, rather than using TargetChannel to make it the only available instance of Chrome for these users.

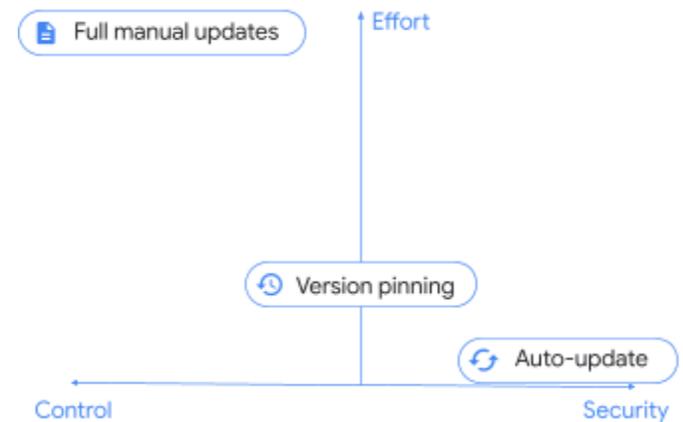
Canary channel

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

Recommendation:

Unless you have a business need for advanced testing, you will not need to 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 SaaS websites 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

Allows you to control when your users receive updates, to meet your software distribution requirements and align with the regular update process of your organization. Your IT department can govern the update process. Users are not allowed to update on their own. 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 where there is no internet access, and the browser is used for internal webapps only. In these sorts of scenarios, Google Update is not an option for keeping Chrome up to date, and you must do so manually by pushing a new MSI each time.

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 which 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 Browser 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 the Chrome browser enterprise bundle 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 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 browser 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 provides IT teams the ability to control extension access and management, both through on-prem policies and through cloud management. Note that the extensions themselves have their own update process. You can manage extensions using auto-updates, manual updates, disabled updates, or the hybrid approach. See the [Managing Extensions in your Enterprise](#) technical guide for more details.

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 is part of the enterprise bundle and can be enabled through Chrome Browser Cloud Management or Group Policy

Next steps and resources

Google understands you have complex policies and requirements governing the updating of software. 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 update 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 update channels to maximize testing opportunities.
- Have 5 percent 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. The Chrome team actively investigates reported issues.

You can also purchase Chrome Browser 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.

Finally, to deepen your understanding of Chrome capabilities for your enterprise, **consider the following resources:**

Download for your enterprise:

[Chrome Browser](#)

Learn more about:

[Chrome Browser Enterprise Support](#)
[Get in touch with Browser specialists](#)

Explore:

[Chrome Browser Policy List](#)

Read the latest:

[Chrome Browser Enterprise Release Notes](#)

Visit:

[Chrome Browser Enterprise Help Center](#)
[Chrome Browser Help Forum](#)

Review:

[Chrome Browser Public Bug Tracker](#)