chrome enterprise

Understanding your Chrome Browser update options in Windows environments

Introduction

Many people working in enterprise environments use the 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 business effectiveness.

While the browser has become a mission-critical enterprise application, it also poses challenges for IT professionals managing Windows environments.

These challenges include:

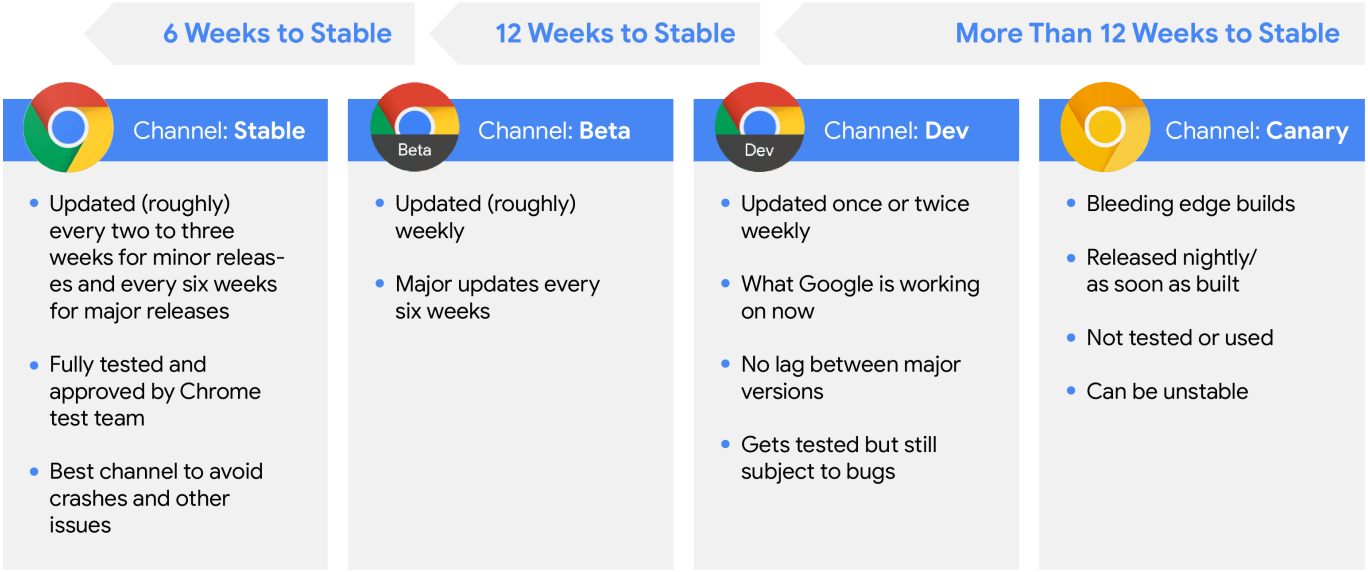
- Many enterprises have not standardized on a single browser.
- IT teams are challenged to keep all browsers up to date for optimal security.
- App compatibility across browsers may differ, especially between legacy and modern browsers.

chrome enterprise

Chrome Browser 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 Chrome Browser and policy updates on managed 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 Browser.

Getting to know Chrome Browser update channels



Chrome has four update channels: Stable, Beta, Dev, and Canary. The Beta, Dev, and Canary channels can run side by side with the Stable channel on the same machine, making testing easier for enterprises.

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 roughly every two to three weeks for minor releases and every six 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.

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 list, crbug.com. Minor updates occur roughly every week, with major updates every six 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 six-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 12 weeks before the next Stable channel release. Because it's an early release of Chrome Browser, the Dev channel is not 100 percent 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 or 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

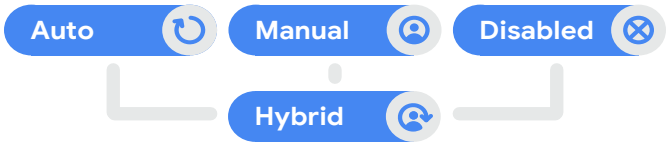
may uniquely impact your environment. By having a few IT and developer staff on the Dev channel, you can quickly identify and report any changes that may impact your environment before they reach the Beta or Stable channels.

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 12 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-updates

Provide fast-paced protection for known vulnerabilities. Your users only need to refresh Chrome Browser 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 Browser.

Recommendation:
Users who mostly use cloud 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 manual updates. Then, develop a plan to move as many users and devices as possible to auto-updates.

Manual updates

Allow you to push periodic updates that 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 manual updates 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:
Issue manual updates regularly and try to keep as many users as possible on the same version.

Disabled updates

Are only appropriate for users who have to stay on a browser version longer or need to pin indefinitely to a specific version for app compatibility or compliance. For example, certain organizations cannot update their browser without significant approvals and review cycles.

Healthcare companies, financial services firms, and defense firms often fall into this category. In these organizations, the IT administrator is essentially pinning users to a specific browser version and disallowing users to update their browser. Since Chrome 65, admins can use a specific policy for version pinning.

Recommendation:
Google does not recommend you disable updates unless you have a clear mandate to do so. Out-of-date versions of Chrome have known security vulnerabilities and are susceptible to attack. If you operate in a highly regulated industry and need to pin users on a mandated version of Chrome Browser, you should periodically reevaluate update options. Google recommends updating at least twice a year. You might still benefit from keeping some IT staff on the Beta channel so that you'll be well-positioned to update if your regulatory environment changes. If needed, you can set up a policy for version pinning. For details, see Manage Chrome updates (Windows).

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 manual-update 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 Browser on your managed Windows devices. After Chrome Browser 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 Browser:

- Enables management of third-party extensions.
- Provides legacy browser support.
- Manages Adobe Flash Player.

Managing updates to third-party extensions
Extension management is part of the Chrome Browser enterprise bundle. The bundle 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 Browser 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 Browser 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 Browser 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.

Adobe Flash Player updates
Although many enterprises are on their journey to move away from Flash by Adobe's deprecation date of December 2020, your organization may still require some use of Flash. By default, Chrome installs Adobe Flash Player in the background or the first time that a user encounters Flash content. Also by default, and as a recommended best practice, Chrome will continue to update Flash Player via the Chrome Component Updater. However, some IT admins may want to manage their users' Flash experience by disabling the Component Updater through policy. If your organization decides to disable the updater, you should stay on top of issuing Flash updates manually in order to avoid potential vulnerabilities.

chrome enterprise

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 Browser 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 manual or hybrid updating.
- 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 Browser 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 Browser 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