chrome enterprise

Updates technical document

chrome enterprise

Contents

Introduction

Keeping Chrome up to date is essential to keeping your users secure, and keeping them productive with the latest Chrome features. Chrome provides a range of update controls to help you get the best balance of security and control in your organisation.

This technical document explains the mechanisms through which Chrome is updated, and the controls available for those mechanisms, organised broadly into three update management strategies. Here you will also find additional tools for managing updates in your environment, including dealing with bugs and incompatibilities, and troubleshooting.

Please note that extensions are updated via a separate process, which is explained in our Extensions management technical document.

What is Google Update?

Google Update is the technology that Google uses to implement automatic updates in Chrome. Google Update supports software patching for Chrome (as well as other Google products) on Windows devices (the Mac equivalent is Google Software Update).

Using Google Update saves you the manual work of deploying new versions of Chrome, including security patches, managing them centrally and pushing them to your fleet of devices yourself.

Google Update can also be configured via policy to pin some users or devices to a specific version of Chrome, or to rollback to a previous version, all without manual intervention or deploying a new MSI. It is included in the Chrome installers, so there is no need to install it separately. You can set policies for Google Update via the Admin console (Chrome Stable channel only) or via GPO (all channels). Note that GPO policy will take precedence unless **CloudPolicyOverridesPlatformPolicy** is set for Google Update (this is separate from the Chrome policy with the same name). Download the latest Google Update administrative template here.

The initial Chrome Browser installation is approximately 56 MB.

- Subsequent updates from one version to the next are approximately 10–15 MB.
- Patch updates are typically 0.5–3 MB.

Updates from a major version to a later non-consecutive major version usually require a new complete installation.

What is the Chrome variations framework?

Features and fixes can also be gradually enabled (or if necessary, rapidly disabled) via the Chrome variations framework. The benefit of this approach is that it allows us to:

- Give a small group of users previews of new features and gather feedback.
- Safely roll out changes to a controlled percentage of users, to minimise the risk of incompatibilities.
- Provide security and other critical updates to you faster.
- Roll back features if needed, without you having to wait for a new version of Chrome. The user only needs to restart their computer to get a new configuration.

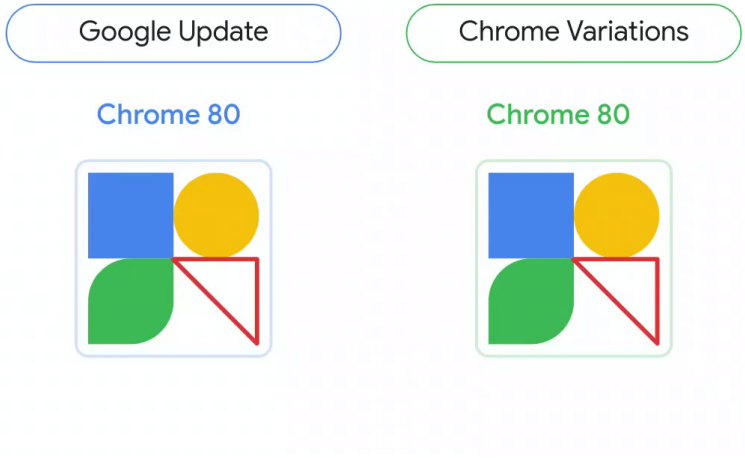

Fig. 1: Visual comparison of Google Update and the Chrome variations framework. The triangle represents a feature that is switched on and off by Chrome variations.

Optimise your testing with Chrome channels

A new major version of Chrome is released approximately every 4 weeks. Each of Chrome's channels gives you a window into a different stage in its release cycle, to help your organisation prepare for new releases.

- **Most users** should be using the **Stable channel**. Stable is fully vetted and supported by Google.

- Organisations that wish to keep some of their users on the same version of Chrome for longer than 4 weeks can use the **Extended Stable** channel. This channel extends every other milestone by four additional weeks with important security fixes. In other words, Extended Stable receives new features every 8 weeks, giving administrators a longer cycle to manage updates. Note that while security updates will still be released to Extended Stable roughly every two weeks to fix important issues, there may be some security positive changes and new features that are available earlier in the Stable channel - making it the more secure option. However, because Extended Stable is based on every other Stable milestone, the first 4 weeks of the cycle will be identical to Stable. Please read the sections below on Chrome variations and Component Updates to understand how those policies can also be useful for your Extended Stable or Stable configurations.

Tip: Provide your Beta users with a bookmark or other documentation that tells them how to contact IT if they find any issues.

- **5% of users** should be using the **Beta channel**. Beta is our release candidate and carries minimal risk of issues. It is fully supported by Google. Beta users should be spread across a range of functions, to maximise the chances that any issues or incompatibilities arising in Beta are caught before that version moves to Stable. Windows and Mac users can run Beta and Stable side by side, so users can easily switch to Stable Chrome in the unlikely event that a serious issue prevents them from continuing their work in Beta. It's also useful to enable MetricsReportingEnabled in order to collect usage statistics for these users, making it easier for Google to detect and fix crashes in Beta. This policy can be set as Recommended so that users can turn it off if they choose.

Admin console: User and browser settings page > Other settings section > Metrics reporting

GPO: Google > Google Chrome > Enable reporting of usage and crash-related data

Mac: MetricsReportingEnabled

- **IT staff and developers** may want to use the **Dev channel** for an even earlier preview of new features. These features are not guaranteed to make it to Beta or Stable, but this can be a good opportunity for testing what's coming down the pike. 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.

- **Developers** who want to test the bleeding edge of Chrome can use the **Canary channel**. Please note that Canary is not tested by Google and may be unstable (it's not even guaranteed to run!) – Canary is for testing purposes only.

	Channel	Release frequency	Supported	Testing by Google	Recommended for
	Stable	~ 2 weeks (minor) 4 weeks (major)	**Yes**	Fully vetted	Most users
	Extended Stable	~ 2 weeks (minor) 8 weeks (major)	**Yes**	Fully vetted	Users who require additional stability
	Beta	~ weekly (minor) 4 weeks (major)	**Yes**	Release candidate	5% of users
	Dev	Once or twice weekly		Minimally tested	IT staff only
	Canary	Daily/as soon as it's built		Not tested	Developers, for testing purposes only

If you've installed Chrome using the Stable binary, you can specify which channel Chrome follows on Windows or Mac by configuring **TargetChannel** to **stable**, **extended**, **beta** or **dev**. The Beta, Dev and Canary binaries are locked to their respective channels.

Update management strategies

The simplest and most secure update management strategy is to enable auto-update and allow Google Update to update Chrome for you every time that a new version is released. In some exceptional cases, however, you may need tighter control over which version of Chrome users in a specific organisational unit (OU) are using. Chrome provides several options to give you control and visibility of your environment. These fall broadly into three update management strategies:

1. Auto-update: Updates when they're available
2. Version pinning: Updates when you're ready
3. Full manual updates: Updates when you push them

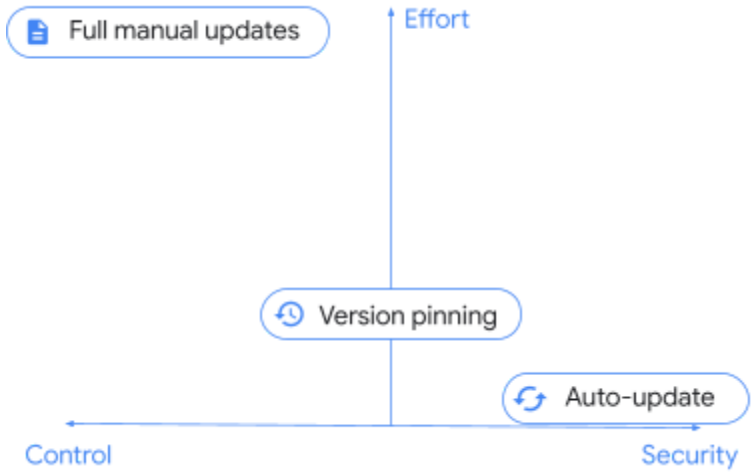

Fig. 2: Qualitative comparison of update management strategies.

Most organisations will rely on a combination of strategies, with most users falling into the auto-update category, and a small subset in another category as needed. The strategy that you choose for a specific set of users will depend on how strictly you need to control those users' browsers and the trade-offs that you are willing to make with the security of their environment.

Strategy 1: Auto-update (Updates when they're available)

Recommended best practice is to enable auto-update for the majority of your fleet and allow Google Update to update Chrome for you every time that a new version is released. This is the best way to make sure that all your users have received critical security fixes, as well as new features, as soon as they're available.

Pros	Cons
• Recommended best practice – this is what Google does internally • Users receive critical security fixes and new features as they become available • No need to manually deploy each release/security patch or centrally manage them; the browser will update itself • Reduces the risk of crashes and security vulnerabilities • Always on a supported version of Chrome • Test for up to 4 weeks before Stable release (using Beta) • (Optional) Get extra time for testing by using Extended Stable	• Does not accommodate change management vetting cycles longer than 8 weeks • Requires close collaboration between IT and app owners to ensure ongoing compatibility

Configuring Chrome to receive updates when they're available

To make sure that your users receive updates as soon as they're available, make sure that **Update policy override** is configured to **Always allow updates**. This gives your users two routes for automatic updates: when updates are found via the periodic update check and when the user does a manual update check by visiting chrome://settings/help.

Admin console
(Windows only): User and browser settings page > Chrome updates section > Chrome browser updates

GPO: Google > Google Update > Applications > Google Chrome > Update policy override

Mac: UpdateDefault

Other options include **Automatic silent updates only**, which *only* applies updates when they are found via a periodic update check, and **Manual updates only**, which *only* applies updates when the user does a manual update check by visiting chrome://settings/help. Manual updates only can be used on a test device which you want to receive updates, but not until the end user checks for them explicitly. Note that in either case, there is some risk that an update may be available but may not be applied in a timely manner, particularly if user intervention is required.

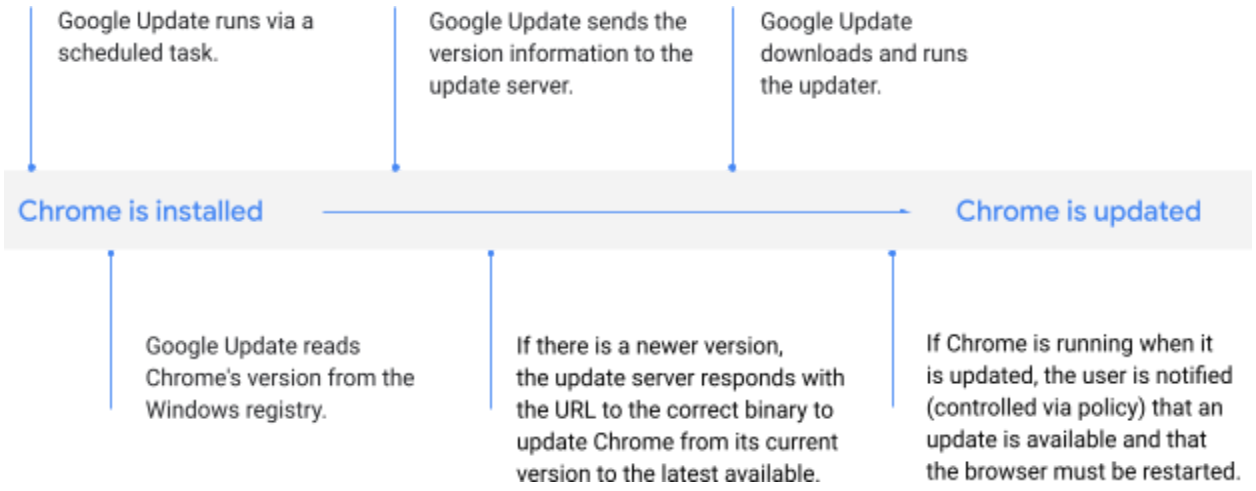

Fig. 3: How an existing Chrome install is auto-updated by Google Update.

Additional controls

For your users to benefit fully from all updates as soon as they're available, the Chrome variations framework must also be enabled so that Chrome can receive updates via variations in between versions. To do this, make sure that ChromeVariations is set to **Variations enabled**. Also consider using the relaunch notification policies to speed up version adoption.

Admin console
(Windows only): User and browser settings page > Chrome variations section > Variations

GPO: Google > Google Chrome > Determine the availability of variations

Mac: ChromeVariations

Strategy 2: Version pinning (Updates when you're ready)

Some organisations are bound to more controlled processes due to business or legacy requirements which require longer than 8 weeks to complete. Even if this is not the case in your workplace, you may have a subset of users who require a more predictable environment, where the features that they're using don't change for a set period of time. For these users, you may need to keep Chrome on a specific version until you're ready to receive a new one.

You can configure Google Update via policy to pin users in a particular organisational unit to a specific version of Chrome and to update when you're ready, without having to deploy Chrome manually.

Pros	Cons
• Accommodates change management vetting cycles that take longer than 8 weeks • Manual effort is minimal • Useful for exception users who need a specific version of Chrome	• Older versions may lack critical fixes and may not be supported

Configuring Chrome to receive updates when you're ready

To pin users in a particular organisational unit to a specific version of Chrome, configure **Target version prefix** to the major milestone that you've reviewed and tested. For example, if you want to keep users on version 80 of Chrome, configure this policy to **80**. (including the decimal point). Make sure that you subscribe to the Chrome Enterprise release notes as well.

Admin console (Windows only): User and browser settings page > Chrome updates section > Target version prefix

GPO: Google > Google Update > Applications > Google Chrome > Target version prefix override

Mac: TargetVersionPrefix

Note that pinning to a major version ensures that users continue to receive minor updates, including security fixes. You can also pin to a specific version (e.g. **80.0.3987.158**) but please note that these users *will not* continue to receive any updates or security fixes, so pinning to a specific version is not recommended.

Pinning to any version, even a major version, for extended periods of time is not recommended as those users may miss out on critical security fixes and may be on a version of Chrome that's not covered by Chrome Browser Enterprise Support.

When a new release is available, review the release notes to determine what testing is needed and begin your vetting process. Remember that you can also test the next major release in Beta up to 4 weeks before it's promoted to Stable. When you're ready for your users to update to the new version, change Target version prefix to the most recent version that you've vetted or remove it altogether to let users update to the latest version of Chrome.

If you decide to pin to a new version, note that new versions are rolled out gradually over a period of time, and your users may not receive that new version until it has rolled out fully. See Will all my browsers be updated at once? below.

Additional controls

If you need even finer-grained control of the specific version of Chrome that a subset of your users is using, you can configure **ChromeVariations** to **Critical fixes only**. This will allow those users to receive critical fixes that have been ramped up via the Chrome variations framework, but disable non-essential new features – users will receive those features when you unpin them or pin them to a newer version.

Admin console (Windows only): User and browser settings page > Chrome variations section > Variations

GPO: Google > Google Chrome > Determine the availability of variations

Mac: ChromeVariations

Note that there is also an option to disable Chrome variations altogether by setting **ChromeVariations** to **Variations disabled**. This option is **not recommended** and must only be used temporarily in environments where stability has been prioritised over security. Also consider using the relaunch notification policies to speed up version adoption.

Strategy 3: Full manual updates (Updates when you push them)

Some organisations run Chrome in extremely locked-down environments where there is no Internet access and the browser is used for internal web apps 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.

While this may be a necessary step for compliance in some organisations, it is worth bearing in mind the risks associated with a fully manual approach and minimising the number of users who are updated in this fashion. 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 labour intensive, as is rolling back if necessary. As with the previous section, older versions of Chrome may not be covered by Chrome Browser Enterprise Support if any issues arise.

Note that even with this approach, there is no need to uninstall Chrome before installing a new version - you can simply push the new MSI to all the machines that you wish to update.

Pros	Cons
• Accommodates change management vetting cycles that take longer than 8 weeks • Does not require Internet access	• Significant manual effort • Security and bug fixes won't be received automatically • Older versions may not be supported • Rollback subject to availability of older MSIs

Other considerations

Working with limited bandwidth

If some of your users work in an environment with limited bandwidth, having them all update their browsers at once may cause a heavy demand on the network that can impact their productivity. You can configure Google Update to update Chrome (and any other software that it manages) during scheduled maintenance windows, stagger updates over a period of time or cache updates locally to keep users with limited bandwidth productive while keeping their browsers up to date.

Set up maintenance windows

Maintenance windows ensure that Chrome updates only take place outside of designated hours, minimising disruption to your users in their busiest hours. You can specify hours during which Chrome *will not* auto-update by enabling **Time period in each day to suppress auto-update check** and specifying the **Hour** and **Min** of the time each day when you want updates to be suppressed and the **Duration** of time (in minutes) for which they will remain suppressed. Note that the times that you specify will be the local machine time and must be in 24-hour format.

Admin console (Windows only):
- User and browser settings page > Chrome updates section > Suppress auto-update check

GPO:
- Google > Google Update > Preferences > Time period in each day to suppress auto-update check

Mac:
- UpdatesSuppressedStartHour
- UpdatesSuppressedStartMin
- UpdatesSuppressedDurationMin

Stagger your updates

Another way to manage updates in a low bandwidth environment is to stagger them so that your entire fleet doesn't update all at the same time. You can do this by specifying a custom time period between update checks, which delays updates to reduce peak bandwidth use. Note, however, that while delaying updates can help reduce the peak bandwidth use, it may increase total bandwidth use.

To stagger updates, enable **Auto-update check period override** and specify a number between 1 and 43,200 (inclusive) in **Minutes between update checks**.

Admin console (Windows only):
- User and browser settings page > Chrome updates section > Auto-update check period

GPO:
- Google > Google Update > Preferences > Auto-update check period override

Mac: Not yet available

Cache updates

Chrome updates can also be cached locally using an intermediate proxy cache – most web-caching proxy servers should work. To tell the Google Update server to send Chrome updates via an URL that is more easily cached by proxy servers, set **Download URL class override** to **Cacheable download URLs**.

Admin console (Windows only):
- User and browser settings page > Chrome updates section > Cacheable URLs

GPO:
- Google > Google Update > Preferences > Download URL class override

Mac:
- DownloadPreference

If your proxy server is still having trouble caching Chrome updates, try configuring the following settings:

- **Maximum file object size** – At least 1 GB
- **Cache directory size** – Ensure that there is enough storage space either in memory (faster) or on disk
- **URL settings** - Give preference to **dl.google.com/*** and **www.google.com/dl/***
- **Maximum object size in memory** – E.g. 2,000 KB
- **Cache space on disk** - If you have a large hard drive (more than 30 GB), you can increase the value to cache more objects

Setting up a cache in environments with low bandwidth or slow connection speeds can give you better response times, as well as saving bandwidth for more important tasks.

Dealing with a bug or incompatibility

If you come across an issue with a specific version of Chrome, after raising a support case or a bug, you'll want to update your entire fleet to make sure that all your users receive the fix.

To be sure that all users have received the update, visit the **Versions report** page in the Admin console. The Versions report page allows you to see all Chrome Browser and Chrome OS versions across your fleet in one place, and you can filter by last active time.

Relaunch notification

If you spot a browser that should have received the update, but is still on an older version, it may need to relaunch. You can remind users to relaunch Chrome by setting RelaunchNotification to **Recommended** and configuring RelaunchNotificationPeriod to specify the time period for notifications (default is one week and the minimum is one hour).

To force a relaunch rather than merely recommending it, set RelaunchNotification to **Required** and specify the time period before relaunch using RelaunchNotificationPeriod. The minimum time period that you can specify is 1 hour (3600000 milliseconds) and the default is one week (168 hours, or 604800000 milliseconds). Note that in the Admin console, the relaunch notification period is specified in hours rather than milliseconds.

Admin console (Windows only):
- User and browser settings page > Chrome updates section > Relaunch notification
- User and browser settings page > Chrome updates section > Time period

GPO:
- Google > Google Chrome > Notify a user that a browser relaunch or device restart is recommended or required
- Google > Google Chrome > Set the time period for update notifications

Mac:
- RelaunchNotification
- RelaunchNotificationPeriod

Rollback

In some rare circumstances, you may find it necessary to roll back to a previous version of Chrome while you wait for a fix. To roll back to a previous version, configure **Target version prefix** to the version that you'd like to roll back to – this should be the most recent version that works as expected in your environment. You'll also need to enable **Roll back to target version** for the roll back to take effect.

To ensure that users' data is preserved, please refer to our Help Centre documentation on keeping data during version rollback. For older versions of Chrome (prior to 84), users will need **Chrome Sync** turned on to retain their browsing information.

Automatic rollback requires automatic updates through Google Update to be enabled, and the device must be domain-joined and/or the browser enrolled in Chrome Browser Cloud Management. You can only roll back to one of the last three versions of Chrome. For browsers that are updated manually, or that need to be rolled back to an older version, you will need to perform the rollback manually.

Admin console (Windows only):
- User and browser settings page > Chrome updates section > Target version prefix
- User and browser settings page > Chrome updates section > Roll back to target version

GPO:
- Google > Google Update > Applications > Google Chrome > Target version prefix override
- Google > Google Update > Applications > Google Chrome > Roll back to target version

Mac:
- TargetVersionPrefix
- RollbackToTargetVersion

Disabling variations

Admin console (Windows only): User and browser settings page > Chrome variations section > Variations

GPO: Google > Google

If an incompatibility is caused by a feature enabled through the Chrome variations framework, ChromeVariations can be set to **Critical fixes only** (or to **Variations disabled** to disable it entirely, though this is not recommended) as an emergency measure. Any features enabled via the variations framework will then be disabled after a relaunch of Chrome.

Disabling component updates

Chrome has components that are important pieces of code that may need to be updated dynamically. Usually components are updated (outside of the normal release cycle) only if a major issue is uncovered. ComponentUpdatesEnabled can be disabled to prevent changes from occurring as an emergency measure – though this is not a recommended practice.

Troubleshooting

Gather logs

If you run into unexpected issues with Google Update, it can be useful to gather logs to help troubleshoot. Logs are also valuable when raising a support case. Directions on how to gather logs are available in the Help Centre.

URL allowlist

Ensure that Google Update is able to reach the URLs it needs to update Chrome. The Help Centre contains a list of URLs to add to your allowlist.

Does Chrome get updates when it's not running?

As long as the machine is powered on, has network connectivity and Google Update has not been disabled by policy, Chrome will be updated silently in the background when a new update is available. The next launch of Chrome will be the new version. Note that the Admin console's version report may still report the old version until Chrome is launched. This can be mitigated by filtering the report on Last activity to remove stale browsers that have not been running for a long time. Third-party tools may not always report Chrome's version accurately, so check the Version Report or chrome://version on the target device for the most accurate information.

If Chrome is installed at the machine level (rather than at the user level), this will work even if no user is logged in to the device. In either case, the user logged in to the OS *does not* need to have administrator privileges in order for Chrome to update itself.

Will all my browsers be updated at once?

When a new version of Chrome is made available, it is initially released to a small percentage of browsers at random and then pushed progressively to more and more browsers until it is available to all browsers. It may take upwards of a week or more for machines in a fleet to get an update depending on how quickly we ramp up to 100% and whether or not it becomes necessary to pause the rollout. Note that if Chrome is pinned to the most recent milestone, your users may not receive that new version until it has rolled out fully. However, you can bypass the ramp by pinning to a fully-specified minor version. Please note that if you do pin to a minor version, you will need to remove or update Target version prefix before you can receive further updates. More details here. You can also view Chrome's version history programmatically using our VersionHistoryAPI.

Conclusion

These are some of the many ways that Chrome gives you control and visibility of your environment. Use these controls to get the best balance of security and stability for your users. For most scenarios, our recommendation is to:

- Enable automatic updates via Google Update
- Keep Chrome variations switched on
- Test in Beta for a preview of the next release
- Subscribe to the Chrome Enterprise release notes

Further information

- Chrome Browser Cloud Management technical document: Get started managing Chrome from the Google Admin console
- Extensions management technical document: Details on extension management, including extension updates
- Chrome Enterprise release notes
- Enterprise downloads: Installers and policy templates for Chrome (including the Beta channel) and Google Update
- Automated testing with headless Chrome for developers