

Chrome Enterprise Deployment Guide

Set up and deploy Chrome Enterprise on
Windows in your organization



About this guide

This guide focuses on the two critical steps required for a successful Chrome Browser deployment:

- **Configuration** - The considerations and decisions to build an installation package to deliver to each user/machine.
- **Deployment** - The timing and testing requirements for an installation package to deploy Chrome Browser.



What is Chrome Enterprise?

Chrome Enterprise lets you deploy and manage Chrome browser for your organization and it does not have any cost associated with it.

- It is a set of admin tools, resources, and installer packages which allow an IT administrator to deploy and manage Chrome Browser in an enterprise environment.

When deploying Chrome Enterprise, the administrator can control Chrome default settings and policies using the following methods:

- Policies can be used to enforce and maintain settings on client computers. For example, you can enable auto-updates, and set the update interval, the default search engine, and the default browser.

- Preferences can be used to set the default value for a particular setting, while still allowing the user flexibility to change the setting. For example, you can set the user's default homepage to the company intranet, set the home button to display in their toolbar, or allow the bookmarks bar to display in the toolbar.

For information about how to deploy initial preferences on users' computers, check out [this link for more information](#).

- Note: For Chrome browser 91 or later, the file named `initial_preferences` replaces the `master_preferences` file.
- To minimize disruption, Chrome continues to support both filenames, and any further change will be notified in the [Chrome Enterprise release notes](#).

Best Practices for Chrome management



Use Chrome Browser Cloud management and/or Group Policy Objects (GPOs) over preferences when possible. Unlike policies, preferences do not apply to previous installations of Chrome Browser and are only applied to a single profile.

- Policies also override any preferences settings for a feature. Also note that the initial_preferences file can be changed and not enforced like machine level policies.



We strongly recommend enabling Chrome Browser auto-updates (this is the default policy setting) to ensure that users have the latest features and security fixes.

- Using Autoupdate also removes the need to package and deploy Chrome regularly, removing additional management overhead.
- For more information on managing Chrome Updates, check out [this update strategy doc that covers all of the options](#).



Test your Chrome dependent applications with the Beta version of Chrome.

- Chrome updates ~every 4 weeks and testing with the Beta version will provide the most stable version (aside from the stable release) and will provide you with an extra 4 weeks of testing time to make sure that you address any breaking changes.
- For more information, check out this link on [testing with Chrome versions](#).



Review and subscribe to Chrome Enterprise release notes

- This provides a roadmap of upcoming features, depreciation and changes in Chrome browser, so reading it regularly will keep you up to date and informed.
- [Subscribing here to the release notes](#) will send the notes directly to your inbox on a monthly basis.

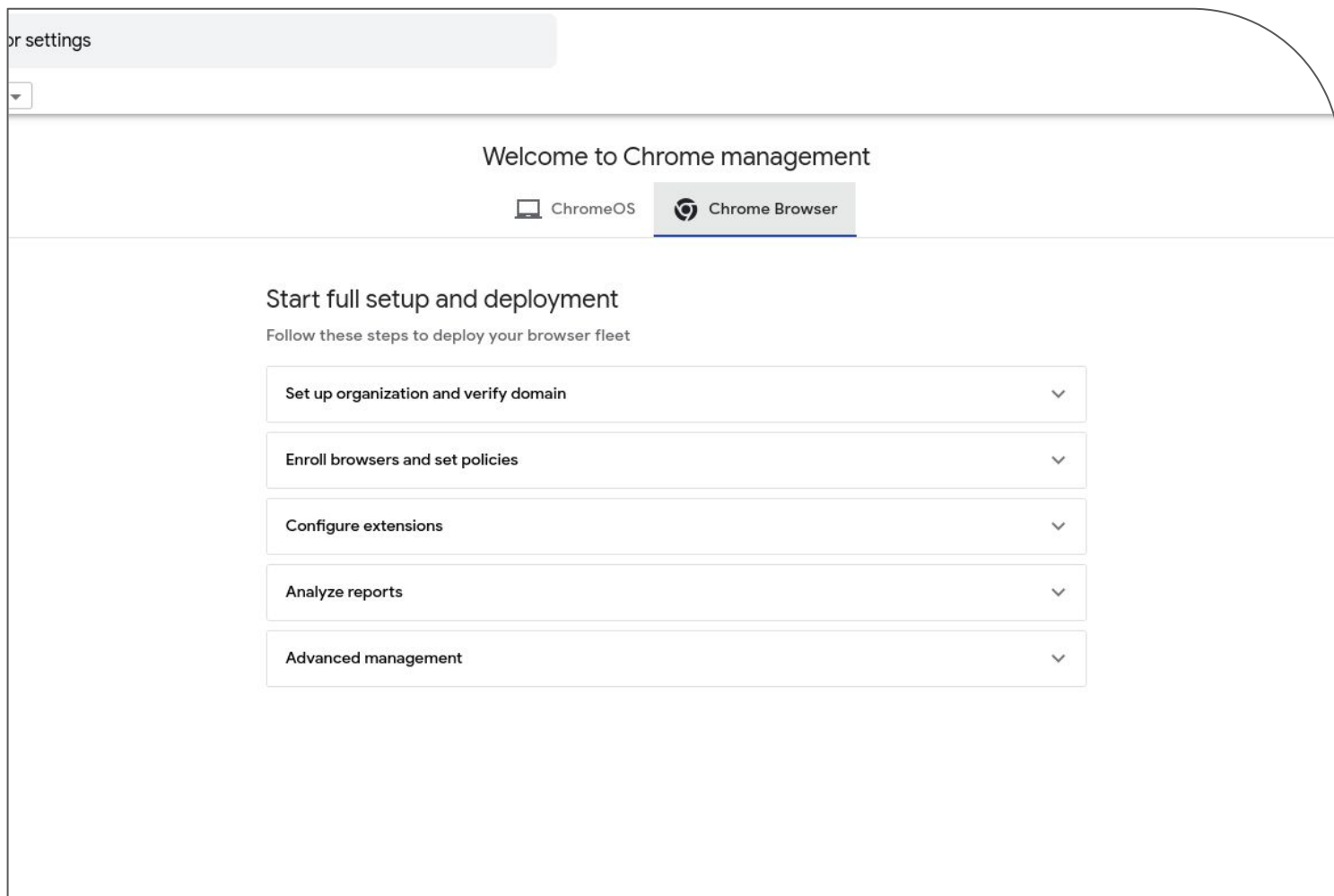


Chrome browser cloud management

You can use the Google Admin console at no additional cost to manage Chrome Browser on Windows, Mac, and Linux devices running Chrome Browser version 73 or later.

With [Chrome Browser Cloud Management](#), you can:

- Enforce 300+ Chrome policies for all users who open Chrome Browser on a managed device.
- Users don't have to sign in or have Google Accounts to receive policies.
- Block suspicious extensions across your organization and do other common IT tasks.
- View reports on Chrome Browsers deployed across your organization, including each browser's current version, installed apps and extensions, and enforced policies.
- For instructions on how to enroll devices and manage Chrome Browser, see [Set up Chrome Browser Cloud Management](#).



The screenshot shows the Chrome management console interface. At the top left, there is a search bar with the text "or settings" and a dropdown arrow. Below this is a navigation bar with two tabs: "ChromeOS" and "Chrome Browser", with "Chrome Browser" being the active tab. The main content area is titled "Welcome to Chrome management" and contains a section "Start full setup and deployment" with the instruction "Follow these steps to deploy your browser fleet". Below this are five expandable steps, each in a box with a downward arrow:

- Set up organization and verify domain
- Enroll browsers and set policies
- Configure extensions
- Analyze reports
- Advanced management

Choosing a management method

Google provides two different methods for managing Windows machines: group policy templates and Chrome Browser Cloud Management.

Here are instructions on managing Mac or Linux machines. [\[Mac\]](#) [\[Linux\]](#)

For managing multiple OSs, first consider Chrome Browser Cloud Management. This feature provides one location to manage Windows, Mac and Linux at no additional cost. You also get a view of installed extensions, plugins and versions of Chrome.



Here is a [link](#) to more information about that feature.

- Steps to setting up Chrome Browser Cloud Management are [found here](#).
 - A deep verbose guide is [located here](#).
- Steps to setting up Windows management via Group Policy are [located here](#).

The table below covers some tradeoffs with each solution; but note that both can work side by side.

	Pros	Cons
Chrome Browser Cloud Management	<ul style="list-style-type: none"> • No cost • Additional reporting <ul style="list-style-type: none"> • Extensions • Versions • Applied Policies • And more • Supports Windows, Mac, Linux, IOS and Android • New features arrive automatically • Ease of use 	<ul style="list-style-type: none"> • No on-prem option and must connect to the internet to fetch policy

Group Policy Objects or other local machine management

Pros

- does not require internet connection to apply policy
- Already in use for many enterprises

Cons

- Some policies are difficult to use (require JSON)
- Need to manually update templates when new policies are released
- No reporting/ visibility on chrome versions or installed extensions
- Platform Specific

- 1 If you are just starting it's recommended you pick a single method of management.
- 2 If you already have management via GPO and want to evaluate Chrome Browser Cloud Management, you can run both tools side by side and should there be a policy conflict your GPO policies will take precedence.
 - You can also swap this policy precedence should you wish. For more information about policy precedence and merging policies [check out this link](#).



Chrome Policy templates (Windows, Mac and Linux)

Chrome policies are applied differently depending on the client operating system.



After selecting the right template for the target environment, the administrator needs to define which Chrome policies will be enforced in the enterprise environment. [The Chrome enterprise policy page](#) lists the supported policies for Chrome Browser and can be applied via policy templates.

- For information about how to install and configure policy templates, see [Set Chrome Browser policies on managed PCs](#).



Windows

For managing Chrome on Windows devices, you have the choice of using [Chrome Browser Cloud Management](#) (recommended as a best practice) or use ADM or ADMX templates to manage Chrome Browser using Group Policy.

-  One of the downsides of using Group policy is that ADM and ADMX templates do not automatically update.
-  You need to download and install the latest administrative templates.
 - In Chrome Browser Cloud Management, new policies and features are automatically added.

There are three types of Chrome policy templates released: Stable, Beta, and Dev.

- 1 With Beta and Dev templates, you get access to policies that are scheduled for future releases.
- 2 This lets you test policies that are not yet available in the Stable template.
 - Whichever template channel you use, the policies that you configure apply to all Chrome Browser releases: Stable, Beta, Dev, and Canary.
- 3 There are also separate templates for Chrome Browser, Google Update, and LBS policies that you might need to manage your Chrome Browser deployment.

MacOS

Download the enterprise installer (offered in both a PKG or DMG format) via the [Chrome browser enterprise Mac download site](#).

- Use a .plist (property list) file to set Chrome policies or use tools like Jamf or Workspace One or preferred systems management tools to push the file to client Macs.
- For instructions on how to manage Chrome Browser on Mac computers, see the Mac Quick Start Guide.
- For information on managing updates on MacOS review this helpful [guide on update management on Macs](#).

Linux

Use a JavaScript Object Notation (JSON) configuration file to set Chrome policies. Use your preferred systems management tool to push the file to client PCs.

- For instructions on how to manage Chrome Browser on Linux Computers, see the [Linux Quick Start Guide](#).
- For information on managing updates on Linux, review this helpful guide on [update management on Linux](#).



Cloud user policy

In addition to machine-based policies, you can optionally provide users with the convenience of having their tabs, bookmarks, and themes synced with any PC where Chrome Browser is installed.

- Additionally, administrators can define pre-installation of Chrome extensions, and themes when users sign in to Chrome Browser.
- These cloud policies are defined by administrators in the Google Admin console and are set via the same method as device-based policy in [Chrome Browser Cloud Management](#).
 - Note that devices that are enrolled in Chrome Browser Cloud management do not require the user to sign into a Google account in the browser in order to be managed and receive policy.
- These policies apply to users on any platform where the user signs in to Chrome Browser with their Google Account.
 - If you're a Google Workspace customer or have Chrome OS licenses, you can use cloud user policies to manage Chrome Browser for your users.

- Cloud policies are deployed and updated anytime the client has internet connectivity.
 - Unlike the typical GPO policy push scenario which requires the PC to have LAN or VPN connectivity to the Active Directory controller, cloud policies can be pushed when the client PC has a connection to the public Internet.
 - For information about how to manage policies from the cloud, see [Cloud-managed Chrome Browser](#).



Note: By default Machine policies (GPO, Chrome Browser Cloud management policies) take precedence over cloud policies when there's a conflict.

- You can also swap this policy precedence should you wish. For more information about policy precedence and merging policies, [check out this link](#).



Chrome Browser Development

Introduction

Enterprise software deployments require a phased roll-out to capture and resolve any issues before deploying the software company-wide.

- We recommend you deploy Chrome Browser in a structured approach with the following phases: Development, Partial Deployment, and Full Deployment.
 - This multi-step approach allows you to evaluate the deployment at each stage and make necessary changes.
 - Below are some of the tasks that should be performed in each Chrome Browser.

Development

- Testing policies
- Incorporating Chrome browser into your base image
- Reviewing change management policies

Partial Development

- Identifying a subset of platforms, users and/or business groups to test the deployment

Full Development

- Deploy to the entire user-base

Preparing your environment for managed Chrome

Before applying policies, it's a good idea to see how your users use Chrome today. Once you have this information, plan to roll out policies slowly. This helps increase productivity and security, with minimal end-user disruption. Here are some steps to provide more visibility into user activity:

Using Chrome Browser

Cloud Management's Reporting

The best way to start managing extensions is to first get some data — data on extensions, policies, plugins and versions of Chrome that your users are utilizing. The easiest way to do this is through:

→ [Enrolling your browsers](#) into Chrome Browser Cloud Management

→ [Enabling cloud reporting](#) in Chrome Browser Cloud Management

Here are some features that can help you get insight into how Chrome is used in your enterprise:

Apps and Extensions usage report

This will provide you with insight into what extensions are installed and what rights they require to run.

- For additional information about extensions, you can use the console's new Takeout API to pull all of this information out of the console into a CSV file.
 - For more information on the Takeout API, [please visit this link](#).

Viewing Policy and applied Plugins

The console's device view is under Devices>Chrome Browser>Managed browsers> click on an enrolled browser.

This section provides details about:

- Versions of Chrome, profiles, extensions, applied policies and plugins
 - Try selecting a device in each geolocation, department, etc, and look at what policies and extensions are present.
 - This will provide a good idea on what users commonly use so you can set up policies per organization unit within the console.
 - For more information about setting up Organizational Units in the Google Admin Console, [refer to this link](#).

Preparing your installation package

Chrome Browser installations from an MSI package are installed at the system level and are available to all users. As a result, any user-level installation of Chrome Browser, (i.e. a user's own Chrome Browser installation), will be overridden. Here's where Chrome Browser is installed and linked for the two types of Chrome Browser installers:

- User Level: "%USER DATA%\Google\Chrome\Application"
- System Level: "Program Files\Google\Chrome\Application"

Note: Chrome Browser won't support an older version to be installed over a newer version. Any MSI of Chrome Browser needs to be newer than the version already deployed (for example, Chrome 68 cannot overwrite Chrome 69).

Test your Installation Process

Some users might have downloaded and installed Chrome Browser before your enterprise installation, and there will be a previous "user level" installation.

- In this case, Chrome Browser will install for all users and leave the user data (preferences, cache, etc.) untouched, unless you choose to have your distribution software uninstall any previous installations.
- It will also attempt to re-point all of the default shortcuts to point to the new system level installation.

Important: Test your Chrome Browser installation process to make sure it works correctly on your organization's Windows or Mac image and method of software distribution.

Logging

You can increase logging for Windows installation to troubleshoot problems and refer to the logs of your distribution software to log successful and failed installations. You can also use the logs created by the Chrome Browser installation to troubleshoot errors.



For more information about the different methods of logging, take a look at the [Chrome Browser Debug log guide](#).




Review these guides for [troubleshooting Chrome Crashes](#) and [performance issues](#) and some [tips on how to fix installation issues](#).



The Chrome MSI itself can also be configured to increase its logging verbosity to provide more clarity on the success or any failure. It's important to understand why a particular installation of the MSI failed.


- Separately, the logs created by the Chrome Browser installation are defaulted to the highest verbosity level and located here:
 - %TEMP%\chrome_installer.log
 - **Important:** %TEMP% should be the System temp directory and not the user-level system variable.


Chrome Updates

 The initial Chrome 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 requires a new complete installation (done automatically by Google Update).

It is recommended as a best practice to keep auto update on for all of your users to 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

 For less frequent updates, you don't need to disable updates altogether. Instead, you have two options:


- Put users on the Extended Stable channel to receive a new major version every 8 weeks. Here is a link for more information about the channels of Chrome.
- Pin to a specific version of Chrome until you have vetted a new version.
 - Allows for automatic rollback to a previous version
 - Reduces the risk of crashes and security vulnerabilities

 If you must turn off auto-updates, have a process to ensure timely updates throughout your network.

- Have a plan to re-enable auto-updates as soon as possible

The Google update engine

Chrome uses an update engine called Google Update. While you can configure the update frequency, it's important to understand what logging options are available when troubleshooting updates to Chrome Browser.

 For more information about logging Chrome Update issues, check out this [Chrome Update guide's](#) troubleshooting section.

Note: that if you are managing via local machine policy (like using GPO), that Google update has its own set of policies that are separate from the other Chrome browser policies. If you manage Chrome in the Google admin console then all of the policies are located together.

 Here is a link with more information about the Google [Update policies](#) template.

- For more information on managing Chrome Updates policies, check out [this update strategy doc that covers all of the options](#).

Getting started with Browser Policies

Regardless of the amount of management you want to apply, there are three common policy categories that most enterprises implement.



Making Chrome the Default browser (optional)

For more information on how to make Chrome the default browser on Windows 10 or higher, please refer to this [Chrome default browser guide](#).

Security

Chrome by default is one of the most secure browsers on the market. The best way to protect your users is to leave the default settings of Chrome on.

Need additional information about the security settings? Review the [Google Security Configuration Guide](#) for best practices.

- A 3rd party guide written by [Center for Internet Security](#) is also available.



Privacy Settings

The [Google Chrome Privacy Notice](#) describes how we treat personal information when you use Chrome Browser and associated services such as Safe Browsing.

- You can review the latest version via the link above, which outlines the data collected based on the feature being used.
- Note that in many cases, specific features can be disabled by the user or via policy to minimize the information sent to Google. These include but are not limited to:

- Chrome Sync with [SyncDisabled](#)
- Omnibox search suggestions with [SearchSuggestEnabled](#)
- Translate feature with [TranslateEnabled](#)
- Spellcheck feature with [SpellCheckServiceEnabled](#)
- Autofill feature with [AutoFillEnabled, AutofillCreditCardEnabled](#)
- Anonymous usage statistics and crash reports to Google with [MetricsReportingEnabled](#)

If you are concerned about personally identifying data remaining in Chrome, you might want to consider reviewing the [Browsing Data lifetime](#) and [ClearBrowsingDataOnExitList](#) policies that can automatically clear out data from the browser on exit or after a specified time period.

- You can also refer to the [Chrome Browser Enterprise Security Configuration guide](#) that advise on how to:
 - Manage settings to reduce security threats to your enterprise
 - Manage security for your users' personally identifiable information
 - Evaluate how security and privacy relate to Chrome management and performance

Unified end-user Experience

Want to provide the best experience for your users?
Consider applying some productivity policies.

You can find all of the policies that you can apply
in Chrome at [the policy page](#).

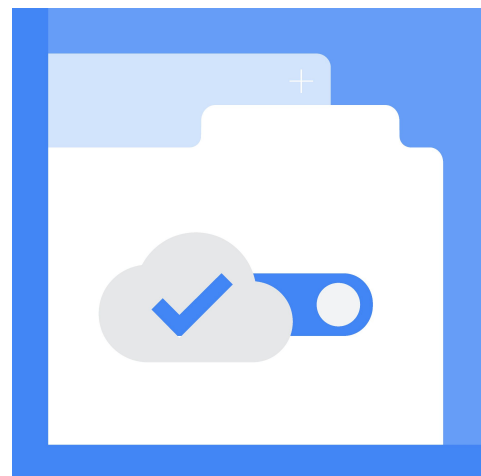
Initial Preferences for Chrome Browser

Administrators can use master preferences to
deploy default preferences to Chrome Browser
users on managed computers.

- 1 When users launch Chrome for the first time, the user's preference file is copied from the `initial_preferences` file.
- 2 We recommend you validate the `initial_preferences` file with a JSON validator and formatter before deploying.
- 3 After the `initial_preferences` file has been verified, package it with the Chrome installation for deployment.
 - For information about how to deploy initial preferences on users' computers, check out [this link for more information](#).

Note: For Chrome browser 91 or later, the file named `initial_preferences` replaces the `master_preferences` file.

- To minimize disruption, Chrome continues to support both filenames, and any further change will be notified in the [Chrome Enterprise release notes](#).



Legacy browser support

If your organization wants to take advantage of the Chrome Browser, but your users still need to access legacy websites and web apps that require Microsoft Internet Explorer (or Safari on Macs), you can use Legacy Browser Support to easily switch between browsers.

When users click a link in Chrome Browser that requires a legacy browser to open (such as a website with an embedded ActiveX control), the URL will automatically open in IE mode in Microsoft's Edge browser. Administrators can specify which URLs to launch into IE mode and deploy this Chrome policy for the organization.

- For information, see [Legacy Browser Support for Windows](#).
- For Mac support, see [Legacy Browser support on Mac](#).



Extension management

Extensions are popular with end users. Managing them can be a challenge. For a complete guide on managing extensions, check out [Managing Extensions in your Enterprise](#).

Get support

Chrome Browser Enterprise Support

Google offers a paid support offering called Chrome Browser Enterprise Support. It provides 24/7 phone, email and portal support for troubleshooting issues and assistance on management configuration questions. For more information, [please visit this site](#).

If you already have any Google Services like Google Cloud, Workspace or ChromeOS licenses, you might be entitled to support for Chrome browser as well.

- Check out [this blog on all of the support options available for Chrome browser](#).

Google Help Center

[The Help Center](#) is the primary source for all of the supporting documentation.

Chromium.org

[The Chromium Projects](#) is where you can submit possible bugs or feature requests to be included or fixed with upcoming versions of Chrome Browser.



Resources



[Setting up Chrome Browser Cloud Management](#)



[Chrome Browser Cloud Management Deployment Guide](#)



[Chrome Browser Policy List](#)



[Chrome update management strategies](#)



[Managing Extensions in your Enterprise Guide](#)