

Chrome Enterprise Core

Securely manage Chrome browser from the Admin console

Table of contents

Purpose of this guide

What is Chrome Enterprise Core?

Get started

How are devices enrolled?

Enrollment token details

Device token details

Security and auditing

- Chrome Enterprise Core Data Export

- Role-based administration

- Auditing admin actions

- Using APIs

Chrome Enterprise Core feature overview

- Managed browsers page

- User & browser settings section

- Browser versions report

- Apps and extensions section

- Apps and extensions report

Setting up Chrome Enterprise Core

Best Practices for Chrome Enterprise Core

- Turning on Cloud Reporting

- Extension Management

- Managing Updates in Chrome

Conclusion: The future of Chrome Enterprise Core

Purpose of this guide

This document describes how to manage Chrome browser from a central cloud-based console. In this document, we discuss the value of having a central location for managing Chrome. We also cover the Google Admin console's features and best practices for managing browsers in the cloud.

What is Chrome Enterprise Core?

The Google Admin console makes it easy for you to manage and see the status of Chrome across your business. Chrome Enterprise Core supports Windows®, Mac®, and Linux® and iOS and Android platforms.

With Chrome Enterprise Core, you can quickly see reports on:

- Chrome versions deployed across your fleet
- Device information
- Apps and extensions installed
- Management policies applied

You can also take quick action with this information. You can block or force-install an extension across your entire company with just the click of a button. For a quick overview of Chrome Enterprise Core, check out this [YouTube overview video](#).

What's covered in this guide	Instructions, recommendations, and critical considerations for enrolling browsers and managing browsers from the Google Admin console
Primary audience	Microsoft® Windows, Mac, Linux, mobile and Chrome Browser administrators
IT environment	Microsoft® Windows 7 and later, MacOS, Linux and mobile
Takeaways	Best practices for managing Chrome browser from the cloud

Last updated: June 2022

Published location: <https://support.google.com/chrome/a/answer/9116814>

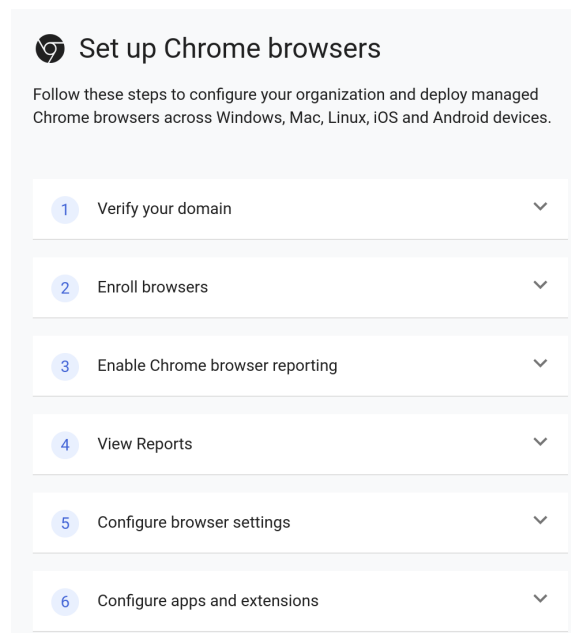
Third-party products: This document describes how Google products work with the Microsoft Windows operating systems and configurations that Google recommends. Google does not provide technical support for configuring third-party products. Google accepts no responsibility for third-party products. Please consult the product's website for the latest configuration and support information. You may also contact Google Solutions Providers for consulting services.

©2022 Google LLC All rights reserved. Google and the Google logo are registered trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.

Get started

Chrome Enterprise Core has two options for domain based management. Option one is to bring your own domain and verify it in the admin console. Option two is to have a Google provided domain account. Check out this link for more information on [domains and Chrome Enterprise Core](#).

If you're already a Google Workspace customer or if you manage Chrome devices, you're set. You can use the same domain (or domains) you use to manage Chrome. Having your own domain isn't required to use this feature, but is highly recommended. Step by step instructions of how to get started with Chrome Enterprise Core are located via [this setup guide](#). There is also a new section in the admin console under Device>Chrome>Guides that provides step by step instructions on how to set up Chrome Enterprise Core.



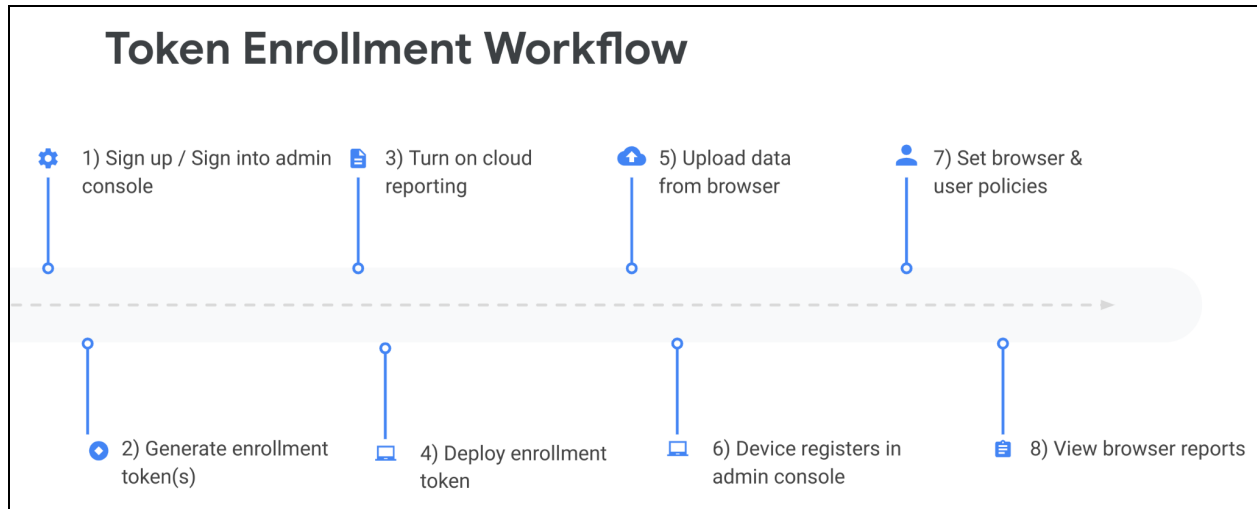
If you don't have Google Workspace or Chrome Enterprise licenses, you can set up a [provided domain](#). This gives you a Google-owned domain to use. This option has the same functionality as what you'd get with a verified domain, except that you're limited to one admin user account. With this account, you can bring your own domain and once you verify the domain then you will be given an additional 9 admin accounts for a total of ten. Note that if you choose the Google-provided domain, there is not currently any method of migrating the data to a different admin console. For more information on access options, please refer to [this section in the Best Practices for using Chrome Enterprise Core](#) technical paper.

Note: You must be running Chrome 71 or later on the devices you're going to manage. Dev, Beta, and Stable channels of Chrome are supported.

How are devices enrolled?

Cloud management of the browser doesn't require your users to be signed in to Google websites and it does not require your users to sign into the browser. You will manage the Chrome browser by enrollment tokens that are generated directly from the Google Admin console.

The tokens are only used once to enroll your browser to the console. The token's Globally Unique Identifiers (GUID) are randomly generated in the Admin console. They can be used for many devices or just one. Here is a workflow of the enrollment process:



Enrollment tokens are associated with the organizational unit that they are generated from. When a browser registers, it gets placed in that token's organizational unit. If you want to enroll multiple browsers into the same organizational unit, you can use the same token for multiple machines. You can also move the browser from one organizational unit to another directly within the console or via API. It is not recommended (or needed) to manually update the token deployed to your users' machines. If you do need to manually update the token via the registry, [follow these steps](#) for unenrolling a device (deleting the machine first in the admin console, then removing the three registry locations).

Note that the enrollment process is handled through the Google update service. Due to this, the device needs to communicate with certain URLs in order for the enrollment process to succeed. Please review this section and make sure that you have the [URLs needed for Google update](#) open (under the section What URLs are used for Chrome browser updates) to function on your network.

Enrollment token details

The enrollment token is used to tie the browser to a specific organizational unit at the time of registration. It's only used when registering and enrolling the device.

Chrome uses the enrollment token like this:

1. The enrollment token is used to register the device.
2. Once registered with Google, Google sends a device token.
3. This device token is stored on the computer.

The enrollment token can be revoked in the Admin console.

Enrollment token installation location:

- **Windows**
RegKey: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
String value name: CloudManagementEnrollmentToken
- **Mac**
Deployed through this policy: /Library/Managed Preferences/com.google.Google.plist
Can be deployed with a plain text file: /Library/Google/Chrome/CloudManagementEnrollmentToken
- **Linux**
Enrollment token is stored at: /etc/opt/chrome/policies/enrollment.

Server-side effects if the token is removed:

- The device will continue to report and update data and fetch policy to and from the Admin console as long as the device token is present.
- If the device token is already present, policies will still be applied and data will be uploaded to the Admin console. If both the enrollment and device tokens are deleted, this clears all the machine-level cloud policies on the next policy refresh (about every 3 hours or immediately once a policy change occurs in the admin console that is applied to the target machine). The data is still present in the admin console, until the browser entry is deleted manually by the admin. This is done via selecting the device in the managed browsers section and hitting the trash icon to remove it.

Device token details

The device token is used as the unique identifier of the device, and it's applied during registration and enrollment. On Windows computers, it's saved in a read-only section of the registry. For other platforms, it's saved on disk. If the device token is already on a machine, the enrollment token is ignored.

Device token installation location:

- **Windows**
RegKey: HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Enrollment
String value name: dmtoken

Note: If you have multiple Windows instances imaged using the same image, please make sure each machine gets a unique identifier (SID) [using Sysprep](#). Otherwise, Cloud Management may not work correctly.

- **Mac**
Device token is stored in the home directory: ~/Library/Application Support/Google/Chrome Cloud Enrollment/{device-id}
- **Linux**
Device token is stored in user data directory: {user_data_dir}/Policies/Enrollment/{device-id}
File name is different on every device for both Mac and Linux.

Server-side effects if the token is removed:

- Reports and status won't be uploaded to the Admin console. The managed browser will remain listed in the Admin console, but the data will be out of date because the managed browser will no longer be reporting to the Admin console.
- Cloud policies won't load and reports won't be uploaded to the Admin console. If the enrollment token is still present, the next time Chrome restarts, the device token will be readded. Policies and reports will then resume. If the enrollment and device tokens are deleted, this clears all the machine-level cloud policies the next time Chrome restarts.

Security and auditing

Chrome Enterprise Core Data Export

Enterprises that want to see all of the data that is within the Admin console can download data from enrolled machines by navigating to **Devices > Chrome > Managed Browsers** ([direct link here](#)), then clicking the  button.

The data is exported in JSON file format. You can also export a CSV file but it will only include data that can be formatted into a flat CSV table. For more information about what data is sent to Google's servers, please refer to [this link on what gets uploaded from users' devices](#). Additional information can be pulled from the console [using the API](#).

You can delete enrolled browsers from the Admin console by clicking the menu  on the right and **Delete** or selecting the check box next to the machine name and hitting the trash icon. Policies that have already been downloaded continue to apply. In order to remove cloud policies from a device entirely, delete both enrollment token and device token from that device. For more information see this link on [un-enrolling a device](#). You can also do this at scale via the [Chrome Enterprise Core API](#).

Role-based administration

By using role-based administration, you can control which of your users can access specific features. For more information, see [Administrator privilege definitions](#). The rights needed to administrator Chrome management is located under **Admin roles > Privileges > Chrome Management**. Checking the settings box

by the Chrome Management box, will automatically add all of the Chrome Management features. An admin also will need to at least have read/write rights for Organizational Units. Full organizational Unit access (read/write/delete) is recommended as a best practice. If they are also going to manage organizational units for the browsers. For more information on what rights are required for browser management, refer to [this link on setting up role based access control](#).

Auditing admin actions

You can view changes made in the console for auditing purposes under **Reporting>Audit and investigation>Admin log events** ([direct link here](#)). For more information see [Admin audit log](#) for the event types captured and [Data retention and lag times](#). Admins will require the reports privilege in order to view these logs found under Security>Reports in the custom role creator.

Using APIs

Chrome Enterprise Core has many different APIs that can be used to pull information from the console as well as setting controls in the console. Here are some resources with more information:

[Use the Chrome Enterprise Core API](#)

[Use the Chrome Browser Enrollment Token API](#)

[How to use Chrome Enterprise Core's Takeout API Service Script](#)

[YouTube on API setup in Chrome Enterprise Core](#)

[Getting started with CBCM's Postman integration](#)

[Chrome browser enterprise Github](#)

Chrome Enterprise Core feature overview

Navigate directly to the Chrome Management section ([direct link here](#)) in the Admin console.

You can also find the browser section under **Devices > Chrome > Overview**. The main features of the console that are relevant to the browser are in the following sections:

- **Managed browsers:** View the details of the managed machines, and organize the devices into organization units for granular management.
- **Enrollment tokens:** Manage enrollment tokens for Chrome
- **User & browser settings:** Find the central location for managing user & browser based settings for Chrome.
- **Apps and extensions:** Manage applications and Chrome extensions.
- **Apps and extensions usage report:** View what extensions are installed, how they were installed, their status, and required permissions.
- **Version report:** View summary of Chrome versions in active devices.

Managed browsers page

In this section of the console ([direct link here](#)), you can see a list of the machines that have managed browsers. Click on a device for details.

- **Machine info:** View managed machine's name, OS version, user details, architecture (32 or 64 bit), enrollment date, and number of Chrome policies.
- **Browser & Profiles:** View profiles that are installed, their installed version, pending install and release channel
 - Expanding profile also provides remote actions such as clearing the cache and cookies by clicking on the  that appears when you hover over the profile row.

- **Installed apps & extensions:** View the installed applications and extensions, their status, how it was installed, version or release channel, and what user profile it's installed on. You can also click on the hyperlink for Apps and extensions usage report to see data on extensions installed across multiple enrolled devices.

Clicking on the  on each app or extension, there are 2 actions:

- Block—Restrict the application or extension from being run to all devices in the selected Organizational unit.
- Force-install—Require and autoinstall the selected application or extension to all devices in the selected Organizational unit.
- **Applied Browser Policies:**
 - View the applied browser policies, where they are being applied from (Local machine or Cloud policy), their status, and the applied value to the policy.
 - The precedence that will be applied in case of a policy conflict is:
 - Device policy first, then the OS user policy, and then the cloud Policy. For additional details, review the [policy precedence help article](#).

Remember that policies applied in the top-level organizational unit will also apply to the child units. They can be overwritten through the various options in the console for different organizational unit configurations.

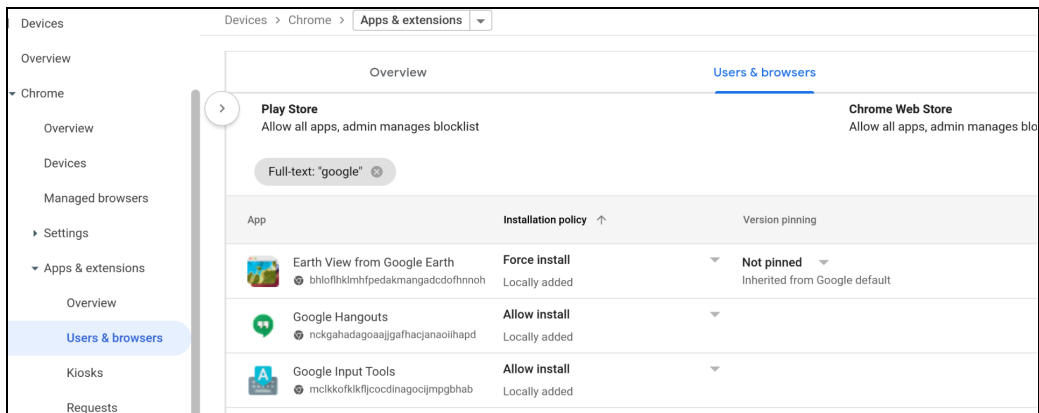
- **Plugins:** View plugins on select machines' browser instances.
- **Custom Fields:** Edit or enter reference information about the device, like asset ID, location, and any notes.

User & browser settings section

In this section ([direct link here](#)), you can set various policies and settings for your managed devices. Some fields might not be relevant if your enterprise is only managing Chrome and you aren't a Google Workspace customer. To learn more, see [Set Chrome policies for users or browsers](#).

Apps and extensions section

In this section ([direct link here](#)), you can set permissions and policies for all or a single extension and apply them to a specific organizational unit or the entire enterprise.



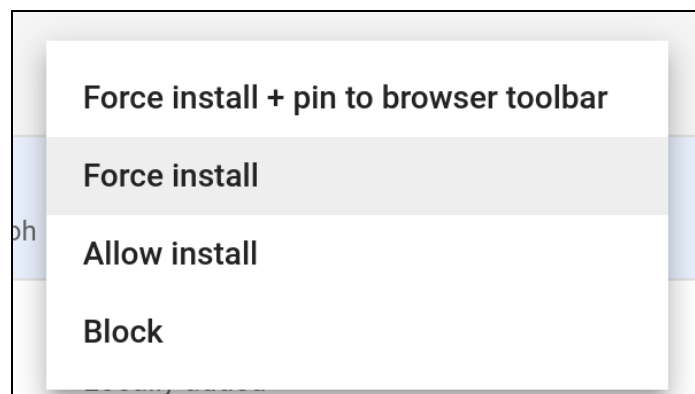
To add extensions to the list you can click on the  on the lower right side of the screen.

- It provides the ability to browse to the extension directly within the Chrome web store or add it via App ID or URL.

Clicking on the extension will expand to the setting for that specific extension or application. This can apply for signed-in users on any device, or enrolled browsers on Windows, Mac, or Linux.

More information and a quick overview of each setting:

- **Allow install:** Allow the user to choose if the extension can be installed. Setting Inherited (from a parent organizational unit) can be overridden by clicking **Override**.
- **Force install:** Force-install the extension or application onto users' machines.
 - If you force install an extension, you also have the option to pin that extension to a latest version that is present in the Chrome Web Store.
 - This is not recommended as a best practice as the extension will no longer receive important security and feature updates.
- **Force install + pin to browser toolbar:** Pins the extension to the toolbar in Chrome
- **Block:** Blocks the extension from being installed and disables existing installs



⚙️ ADDITIONAL SETTINGS

- For more information about managing extensions within Chrome Enterprise Core, please refer to this [YouTube video](#) and the [Managing extensions in your enterprise guide](#).

You can also have your users request extensions and approve them within the admin console via the Extensions Workflow. For more information about this feature, please review [the help center article for Extension Workflows](#) or this [YouTube video on extension workflow](#).

Browser versions report

The browser version report provides a view of all of the different versions of Chrome that are present in your enrolled browsers. Each entry under the version is clickable which will take you to a filtered list of those machines in the managed browser view. With this information, you can view all of the device information for those machines with that version of Chrome and if needed take action through applying update controls in the Users & browsers section of the admin console. For more information about managing updates, check out this [update strategies guide](#).

Chrome Versions

All managed devices and browsers

Organizational Units

Search for organizational units

Global Organization

APAC

BCE

Browsers Test

Chrome

Default settings

EMEA

Chrome versions

Export

Version

Windows

macOS

Linux

ChromeOS

Android

iPhones and iPads

Total

^

M105

1

1



105.0.5116.0 (Canary)

1

1

^

M103

3

1

4



103.0.5060.114 (Stable)

2

1

3



103.0.5060.42 (Beta)

1

1

^

M100

1

1



100.0.4867.0 (Dev)

1

1

Apps and extensions report

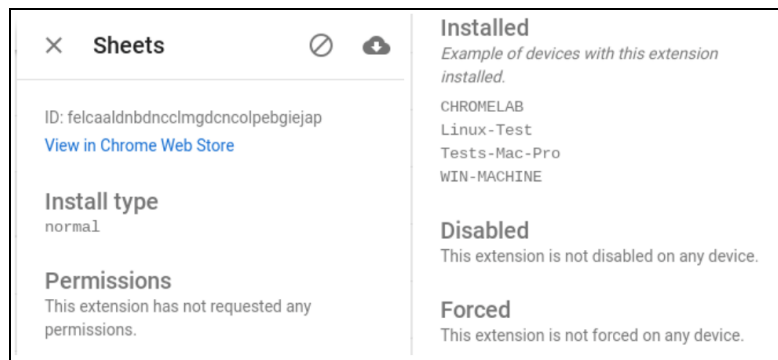
The Apps and extensions report ([direct link here](#)) provides the administrator an overview of the status of extensions in their enterprise. The view can also be filtered by selecting an organizational unit using the field to the left.

App name	App type	Install type	Installs ↓	Permissions
 Google Play Music	Unknown	Unknown	191	0
 Google Docs Offline	Unknown	Unknown	155	0
 Google Voice Search Hotword 	Unknown	Unknown	132	0
 Google Docs Offline	Chrome Extension	Sideload	9	3

Within the view, you can see:

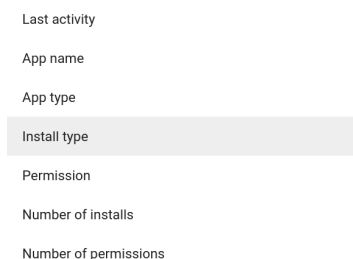
- **App name:** Clicking on the name will link to that extensions page in the Chrome Web Store.
- **App Type:** Shows if the entry is a theme, Chrome Extension or Chrome App
- **Install Type:** The options are normal (by user), admin (by policy), sideload (installed outside of Chrome Web Store) or multiple (install types).
- **Installs:** Refers to how many instances are installed within your enterprise.
- **Permissions:** Refers to the number of permissions required to run the selected extension.
- **Manifest versions:** Shows if the extension is developed using Manifest version 2 or 3. More information about the [EOL of Manifest version 2 located here](#).

Clicking on these fields opens a more detailed view on the left side of the console.



In this section, an administrator can view more details about install type, permissions required, where the extension is installed, and if it's disabled or force-installed on any device.

- Clicking Install  will trigger a prompt to force-install this extension, and you can select the organizational unit to target.
- Clicking Clear  will trigger a prompt to block this extension, and you can select the organizational unit to target.
- You can filter the extension list by the following:



- You can also use the Takeout API from Chrome Enterprise Core to export all extension data from enrolled browsers into a CSV file.
 - For more information see : [Step by step guide](#) | [Blog entry](#) | [Demo Video](#)

Coming in late 2022, when you click on an extension it will take you to the extensions details page

- Here you can get more insights about the extension including the permissions required and information directly from the Chrome Web Store listing.



Devices > Chrome > App details

Google Docs Offline

All users in this account

Organizational Units

Search for organizational units

- Global Organization
 - APAC
 - BCE
 - Dev
 - EMEA
 - Mac devices
 - North America
 - UK

Details

ID	ghlmmgpoekgpmocmndebdofhki
Type	Chrome app, extension or theme
Chrome Web Store listing	View
Listed since	Jun 26, 2015
Last updated	1 week ago
Developer	google.com
Privacy policy	View
Reviews	2.7/5 (3,852 reviews)
Number of active users	10,000,000+
Is a theme	No
Developed by Google	Yes
Hosted in the Chrome Web Store	Yes

Requested permissions (9)

This app or extension requests these permissions.

Name	Access to user data
------	---------------------

Setting up Chrome Enterprise Core

Follow the steps for [Chrome Enterprise Core setup](#).

Here are the steps for setting up Chrome browser management [for iOS](#) and [Android](#).

For help on deploying the enrollment token check out this resource for [enrolling browsers with various deployment methods](#).

Best Practices for Chrome Enterprise Core

For tips and tricks on how best to manage browsers within Chrome Enterprise Core please refer to [Best Practices for using Chrome Enterprise Core tech guide](#).

Organizational unit structure

Organizational units in the Google admin console act as a parent/child relationship. So any policies that you set at the top level will be inherited by the sub-organizational units. It is recommended as a best practice to not enroll browsers or set any policies at the root level (or top level) organizational unit. Instead create one under the top level organizational unit. This will make sure that there is always an organizational unit that has no policies or browsers enrolled in it. This is important so you are able to easily create new units without having policies already been applied.

Turning on Cloud Reporting

Visibility into browser activity can help you better secure and manage your enterprise environments. Enabling reporting is highly recommended and can help you better understand:

- Your company devices and operating systems running Chrome
- The different channels and versions of Chrome
- The extensions installed in their environment and whether policies are applied as expected

To get additional reporting data on your organization's browsers within the Admin console, see [Enable Chrome browser reporting](#). This link also details the data that is sent to the console from your user's machine.

Extension Management

For more information about managing extensions please refer to the [Managing extensions in your enterprise tech paper](#) and this YouTube video for [Managing extensions in Chrome Enterprise Core](#).

Managing Updates in Chrome

For more information about managing how Chrome updates, please refer to the [Chrome update management strategies tech paper](#).

Conclusion: The future of Chrome Enterprise Core

Chrome Enterprise Core provides a single location from which to manage the Chrome Browser across platforms, along with centralized reporting for your fleet. It's part of the Google Admin console, where you can also manage your Google Workspace users and other Google services.. While platform-specific policy management (such as GPO) remains available, Cloud Management gives you control of all your Chrome browser instances.

Google and related marks and logos are trademarks of Google LLC. All other company and product names are trademarks of the companies with which they are associated.