chrome enterprise

Chrome Browser Cloud Management

Securely manage Chrome Enterprise from the Google admin console

Table of Contents

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 the purpose of Browser Cloud Management?

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

With Chrome Browser Cloud Management, 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 Browser Cloud Management, check out this YouTube overview video.

What's covered

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

Get started

Access options for Chrome Browser Cloud Management

Following this guide for the setup of Chrome Browser Cloud Management is the best place to start. It covers all of the initial setup steps. Chrome Browser Cloud Management itself has no additional cost. Note that there are two options to get access to the admin console:

- Use your own domain (no existing Google services associated)
  - Provides 10 admins accounts total
  - Can be associated directly with your enterprise domain (once you verify your domain)
- Use your own domain (Google Services already associated)
  - Admin console is already set up and verified
  - Does not have any additional cost or use any of your Google licenses
  - Number of admins accounts allowed will be dependent on associated Google Service

If it is possible to use your company's existing Google admin console, that is the best option. If the console is already set up, Chrome Browser Cloud Management is already present. You just need to visit that section in the console and accept the terms of service.

Getting access to an existing Google Admin console

Check internally if your company has an existing Google Admin account before setting up your own. Many companies have accounts set up for various Google services like Chrome OS, Google Workspace or others.

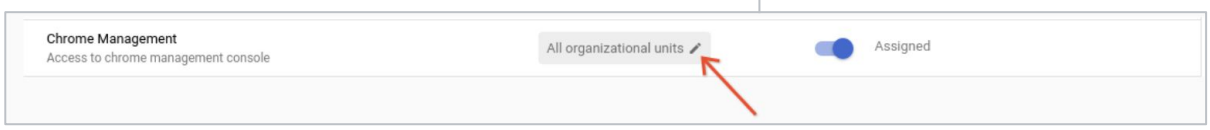
- The Super Admin at your company would need to set up your admin account to the console where Chrome Browser Cloud Management is located.
    - They also will be required to add the Chrome Browser Cloud Management license to the admin console which can be enabled through going to the Manage browser section and click the Get started button to add the no-cost license to your Google admin console.
- The console does provide role based administration so the Super Admin can provide you access just to what you need to manage Chrome Browser.
    - Note that a Super Admin account is required to generate additional admin accounts.
        - Consider asking for a Super Admin account for your team so you can generate your own in the future if needed.
        - If you can't find the original owner internally (like that person has left the company) here is a link for more information on domain reclamation.

If your company does have an existing account but you are not the Super Admin, here is the process of gaining access to Chrome Browser Cloud Management:

1. Have a Super Admin first log into admin.google.com and accept the terms of service agreements for Chrome Browser Cloud Management. This is required to use the service. The path do to do this within admin.google.com is:
    - Go to Devices>Chrome>Managed Browsers and click on the blue enroll link and accept the Terms of service that appear.
2. Have the Super Admin either create an account with super admin rights and assign it to you or if they just want to provide access just to Chrome Browser management, then they can provide the following rights in the admin console:
    1. Under Account>Admin roles click the create new role button and give it a name like "Chrome Browser Management".
    2. Check the box next to Organizational Units to give the following rights
        - Read, Create, Update, Delete
    3. Under Chrome Management check the Settings box to provide all rights to Chrome management.

Note: if your Super Admin wants to limit the rights even more on this admin account, they can create an organizational unit just for Chrome browser management and assign the custom role there. They can do this via the following steps:

1. In the admin console go to Directory>Users and select the user account that you want to assign the Chrome browser management role to.
2. Scroll down and click on the Admin roles and privileges section.
3. Select the Chrome browser management custom role that was created in the previous steps and click on the button to assign it to the user.
4. Once it is assigned you can click on the pencil icon on the button that says “All organizational units) and select the organizational unit(s) that you want to give the admin access to.
    - Once the admin logs in, they will not see any other organizational units aside from the ones that you have given them access to but will have full rights to do Chrome management and create new Organizational units under the assigned OU.
    - You can also view changes made in the console for auditing purposes. See Admin audit log.



Using your own domain

If you want to use your company's own domain but do not currently own any Google services, then you can sign up via this link and Google will provide you an admin console at no additional cost.

When the admin console is first launched, the initial admin will be the super admin with full rights to the console.

You will have the ability to invite other users to be admins (who also will be super admins) as well but you will not be able to create accounts for them, until you verify your domain. Here is a link for more information on verifying your domain.

- It is highly recommended to verify your domain to create custom roles to limit access to least rights and have the ability to create user accounts.
  - For more information checkout this link about email-verified vs domain-verified accounts.

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.

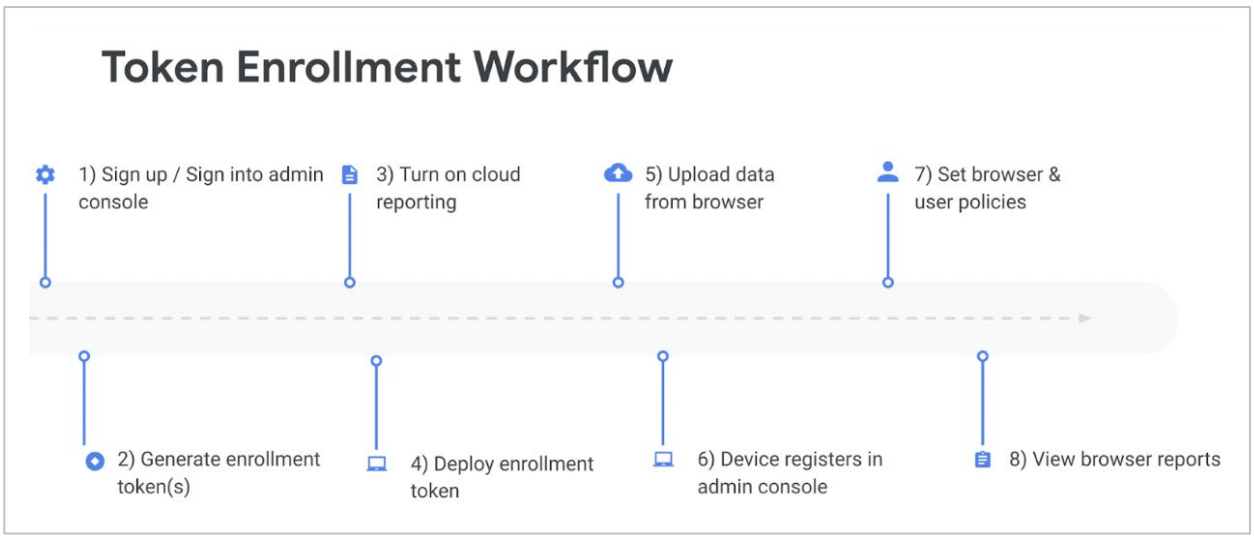
Note: You must be running Chrome 71 or later on the devices you're going to manage. Dev, Beta, and Stable channels of Chrome are supported.

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.

Here are the steps to enroll in browser (also detailed in this guide) into the console.

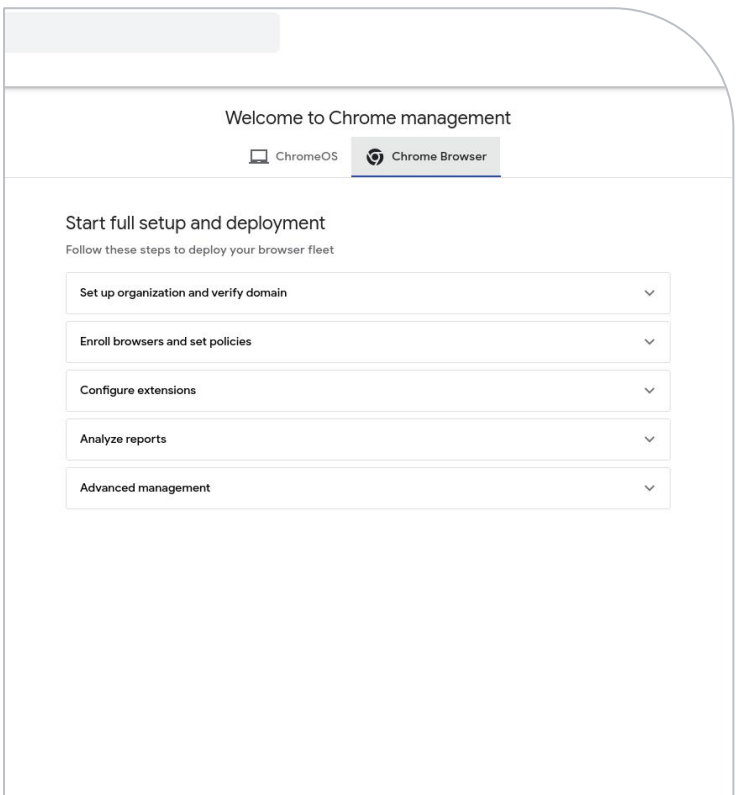
1. Go to Devices>Managed browsers.
2. Select the Organizational unit that you the device to be enrolled into.
3. Click on the blue Enroll link towards the top of the page.



4. You will be presented with a long GUID that is the token value for that selected Organizational Unit.
5. You can either download an App Config file for mobile enrollment, a reg. File for Windows, or a text file for Mac and Linux, or you can copy the value and set it in the Cloud management enrollment policy via your deployment method of choice.

Later on, if you need to, 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.

- You can invalidate or delete device tokens when you delete browsers from the Admin console via the Device Token Management policy located in the Other settings section in the admin console.
- When a device is enrolled in Chrome Browser Cloud Management (CBCM), a unique device token is added to the device. This device token is used to identify the browsers in the Admin console during policy refresh and report sync operations.
- If you select Invalidate token (default), the device token remains on the device when a browser is deleted from the Managed browsers list and it is marked as invalid. The device cannot be re-enrolled in CBCM and it remains unmanaged until the device token is manually deleted and a valid enrollment token is placed on the device.
- If you select Delete token, the device token is deleted from the device when a browser is deleted from the Managed browsers list. If the device has a valid enrollment token deployed, it can be re-enrolled in CBCM the next time the browser restarts.

Enrollment token details

The enrollment token is used to bind 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.

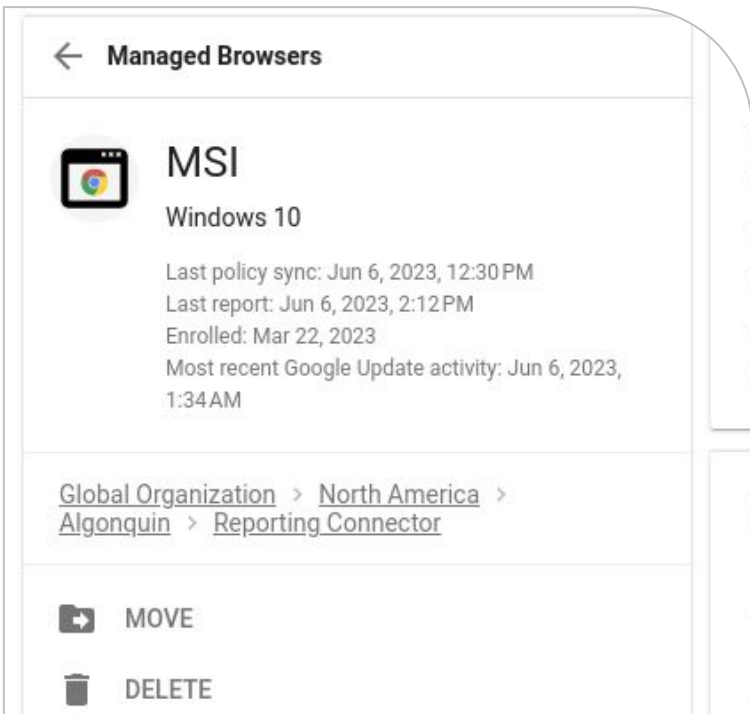
The enrollment token can be revoked in the Admin console.

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. Refer to the previous page if you want to change this behavior.



Device token details

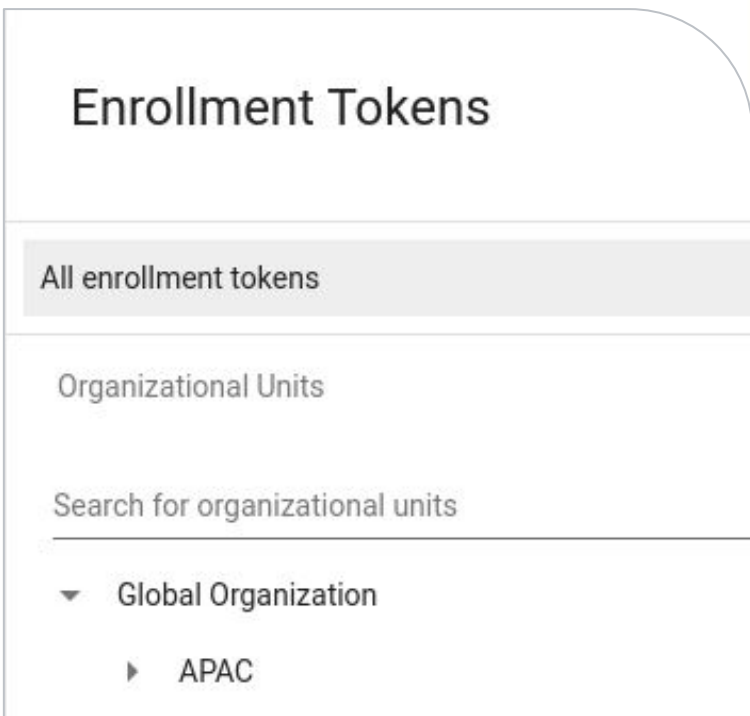
The device token is used as the unique identifier of the device, and it's applied during registration and enrollment. On Windows computers, it's saved in a read-only section of the registry. For other platforms, it's saved on disk. If the device token is already on a machine, the enrollment token is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

- The data is exported in JSON file format or as a CSV file.
    - 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 and large exports 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.
- To remove cloud policies from a device, delete both enrollment token and device token on the device. For more information, see this link on un-enrolling a device,
    - You can also do this at scale via the Chrome Browser Cloud Management 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 the section on Setting up role based administration in the Best Practices for using Chrome Browser Cloud Management guide or this Youtube video.

Auditing admin actions

You can view changes made in the console for auditing purposes under **Reporting>Audit and investigation>Admin log events.** 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 Browser Cloud Management 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 Browser Cloud Management API
- Use the Chrome Browser Enrollment Token API
- How to use Chrome Browser Cloud Management's Takeout API Service Script
- YouTube on API setup in Chrome Browser Cloud Management
- Getting started with CBCM's Postman integration
- Chrome browser enterprise Github

Chrome Browser Cloud Management feature overview

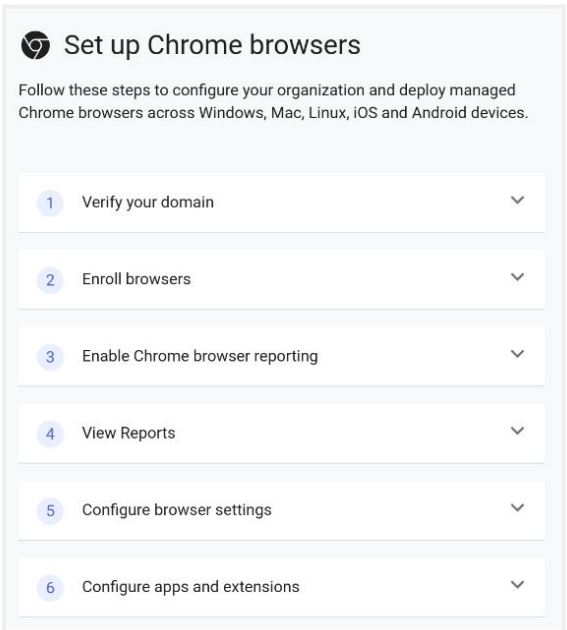
Navigate directly to the Chrome Management section in the Admin console.

The main features of the console that are relevant to the browser are in the following sections:

- **Guides:** Step- by- step walkthrough of how to set up Chrome Browser Cloud Management.
- **Managed browsers:** View the details of the managed machines, and organize the devices into organization units for granular management.
- **User & browser settings:** The central location for managing user and 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.

Guides

If you are just getting started in the admin console, check out the Guides section under Device>Chrome>Guides that provides step-by-step instructions on how to set up Chrome Browser Cloud Management.



Managed browsers page

In this section of the console, you can see a list of the machines that have managed browsers. This is where you can generate an enrollment token for a selected Organizational unit by clicking on the blue enroll link towards the top.

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 an apps and extensions usage report to see data on extensions installed across multiple enrolled devices. Clicking on the extension, will take you to that extension's app details page where you can view more information and set your extension install policy.

Applied Browser Policies: View profiles that are installed, their installed version, pending install and release channel.

- 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.

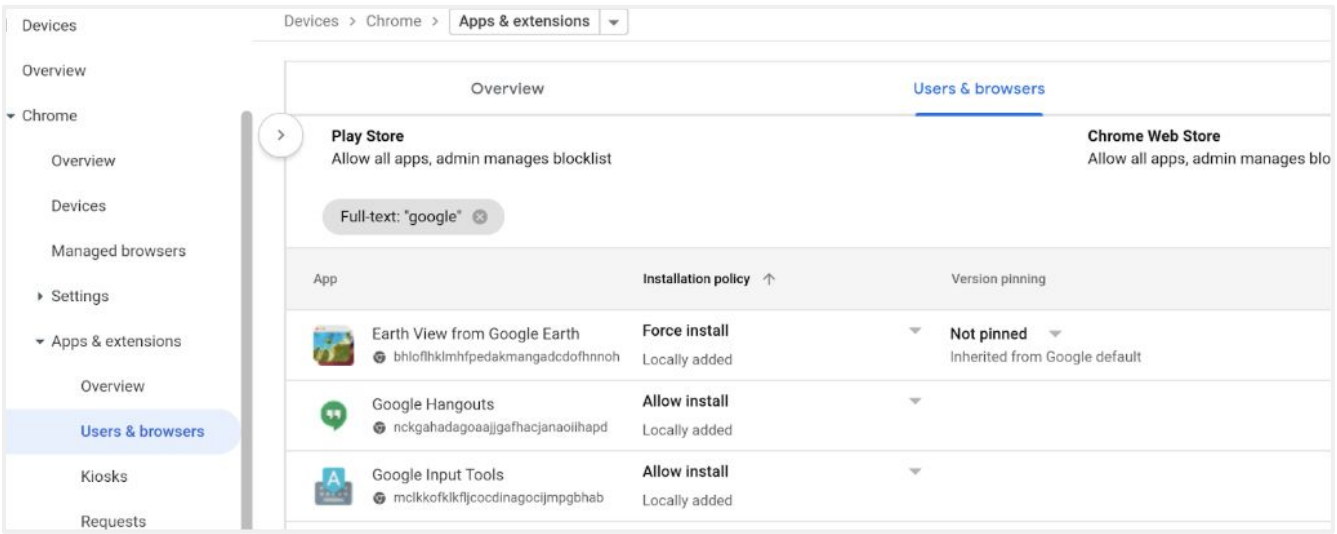
Custom Fields: Edit or enter reference information about the device, like asset ID, location, and any notes.

User & browser settings section

Found via Devices>Chrome>Settings> Users and browsers. In this section, 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

These are found via Devices>Chrome>Apps and extensions>Users and browsers. In this section, 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.

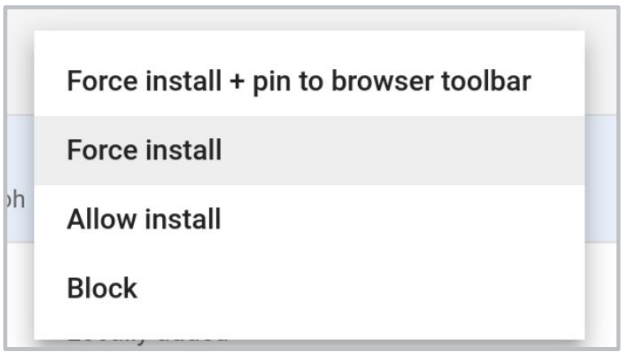
- It provides the ability to browse to the extension directly within the Chrome web store or add it via App ID or URL.

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:

1. **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.
2. **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.
3. **Force install + pin to browser toolbar:** Pins the extension to the toolbar in Chrome

Block: Blocks the extension from being installed and disables existing instal



There is also an additional setting section that can be reached by clicking the ADDITIONAL SETTINGS in the upper right corner of the section. This includes sections for setting allow/block lists, managing by extension permissions and website access and other settings.

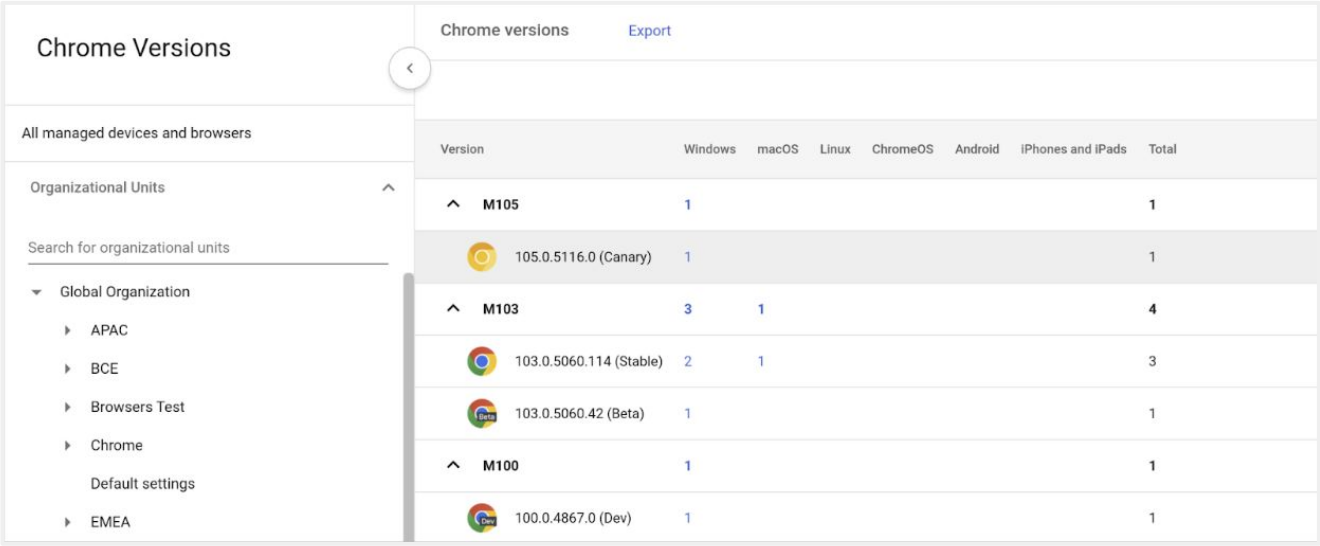
- For more information about managing extensions within Chrome Browser Cloud Management, please refer to this YouTube video and the Managing extensions in your enterprise guide.

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 version report

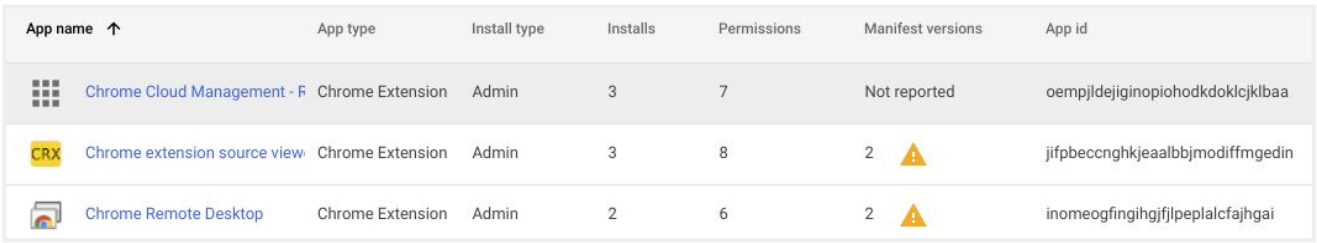
Found via Devices>Chrome>Reports>Versions. The browser version report provides a view of all of the different versions of Chrome that are present in your enrolled browsers. Each entry under the version is clickable which will take you to a filtered list of those machines in the managed browser view.

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.



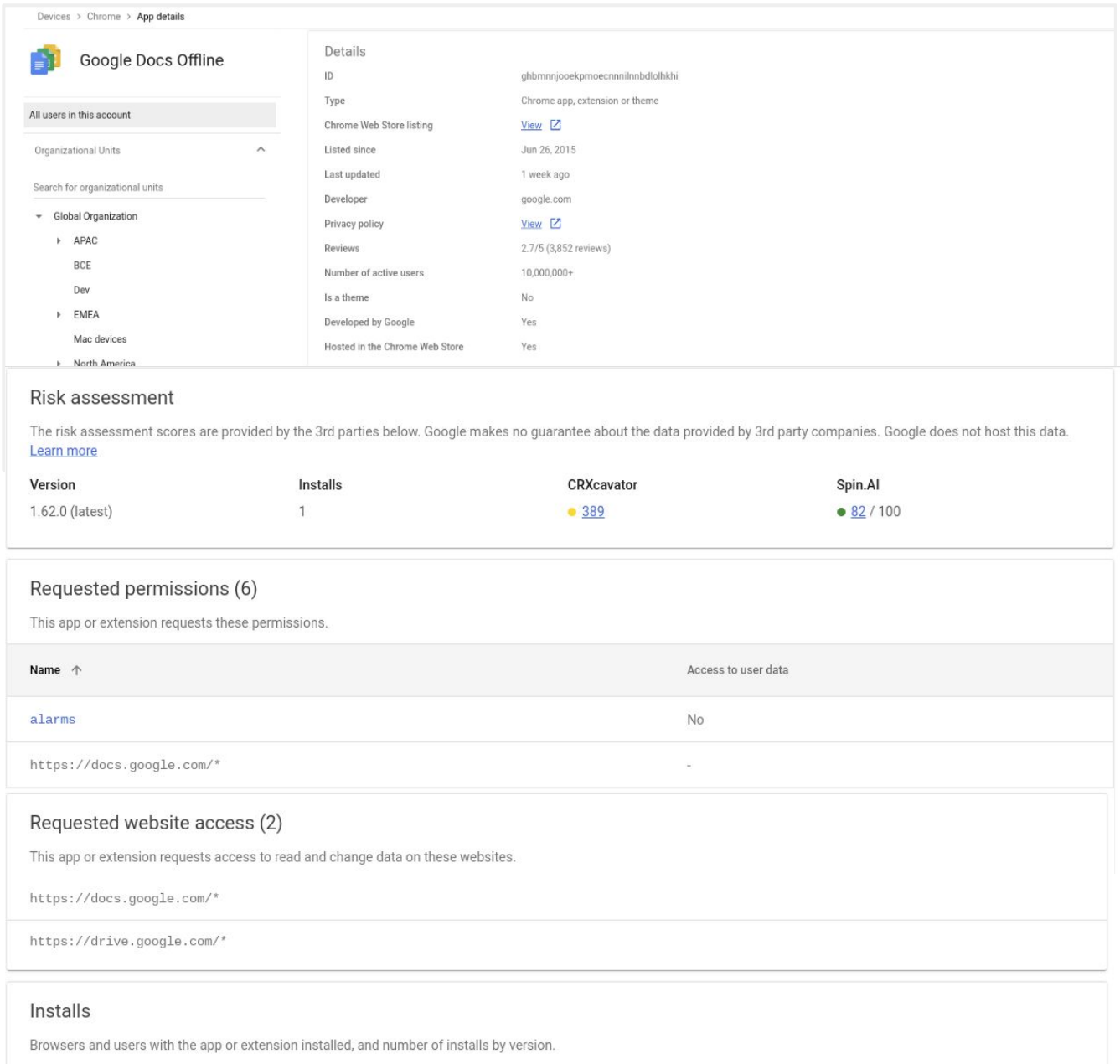
Apps and extensions usage report

Found via Devices>Chrome>Reports>Apps and extensions usage.The Apps and extensions report provides the administrator an overview of the status of extensions in their enterprise. Within the view, you can see:



App name	App type	Install type	Installs	Permissions	Manifest versions	App id
Chrome Cloud Management - F	Chrome Extension	Admin	3	7	Not reported	oempjldejiginopiohodkdoklcjklbaa
Chrome extension source view	Chrome Extension	Admin	3	8	2	jifpbeccnghkjeaalbbjmodiffmgedin
Chrome Remote Desktop	Chrome Extension	Admin	2	6	2	inomeogfingihgjfjlpeplalcfajhgai

- **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.
- **App** ID: the unique identifier of the extension
  - You can also use the Takeout API from Chrome Browser Cloud Management to export all extension data from enrolled browsers into a CSV file.
  - For more information see: Step by step guide | Blog entry | Demo Video

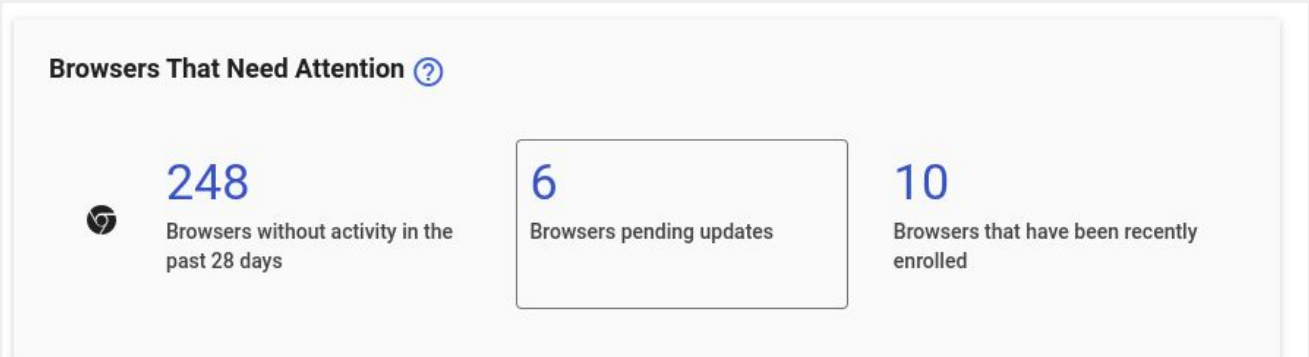


When you click on an extension it will take you to the extensions details page.

- Here you can get more insights about the extension including the permissions required and information directly from the Chrome Web Store listing, risk scores from 3rd parties, install footprint and more information about the functionality of the extension.

Chrome insights report

Found via Devices>Chrome>Reports>Chrome insights .The Chrome insights report provides the administrator an overview of the status of browsers that might need attention within their fleet. . Within the view, you can see:



- **Browsers that need attention:**

  The number of browsers that:

  1. Show no activity in the past 28 days.
     - Browsers that have not reported data or have not synced.
  2. Are with pending updates.
     - A new version of Chrome will be installed on browser restart.
  3. That have been recently enrolled.
     - Browsers that have enrolled in the past 28 days.

  You can navigate directly to a filtered browser list from the report to view all browsers that match the given criteria.

Chrome Enterprise Connectors Framework

Chrome Enterprise Connectors Framework offers a collection of connectors and APIs that simplify the steps needed to integrate Chrome browser with solution providers like Splunk, Crowdstrike, Chronicle, Google Cloud and more.

- Reporting Connectors provide the ability to send security related events (like malware downloads, malicious site visits and more) to various security solutions.
  - For more information, check out this link for how to set up reporting connectors.
- For more information about other connectors, check out the Enterprise Connectors Framework page.

Setting up Chrome Browser Cloud Management

Follow the steps for Chrome Browser Cloud Management 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 Browser Cloud Management

For tips and tricks on how best to manage browsers within Chrome Browser Cloud Management please refer to Best Practices for using Chrome Browser Cloud Management 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

Organizational unit structure

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:

1. Your company devices and operating systems running Chrome
2. The different channels and versions of Chrome
3. 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. You can also increase the frequency of the reports by changing Managed browser reporting upload frequency from uploading reports every 24 hours to the minimum of every 3 hours.

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 Browser Cloud Management.

Managing Updates in Chrome

For more information about managing how Chrome updates, please refer to the Chrome update management strategies tech paper.

Conclusion

Chrome Browser Cloud Management 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.

Want to learn more about Chrome Browser Cloud Management?

Visit our website →