chrome enterprise

Chrome Browser Cloud Management

Securely manage Chrome Browser from the Admin console

Enterprise & Education

Table of contents

Purpose of this guide

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

What is Chrome Browser Cloud Management?

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

With Chrome Browser Cloud Management, you can quickly see reports on:

- Chrome Browser versions deployed across your fleet
- Device information
- Apps and extensions installed
- The 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.

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, and Chrome Browser administrators
IT environment	Microsoft® Windows 7 and later, Mac OSX, and Linux
Takeaways	Best practices for managing Chrome Browser from the cloud

Last updated: July 22, 2019

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

Get started

Chrome Browser Cloud Management groups your devices by a domain (such as example.com). If you're already a G Suite customer or if you manage Chrome devices, you're set. You can use the same domain (or domains) you use when managing Chrome Browser. G Suite isn't required to use this feature.
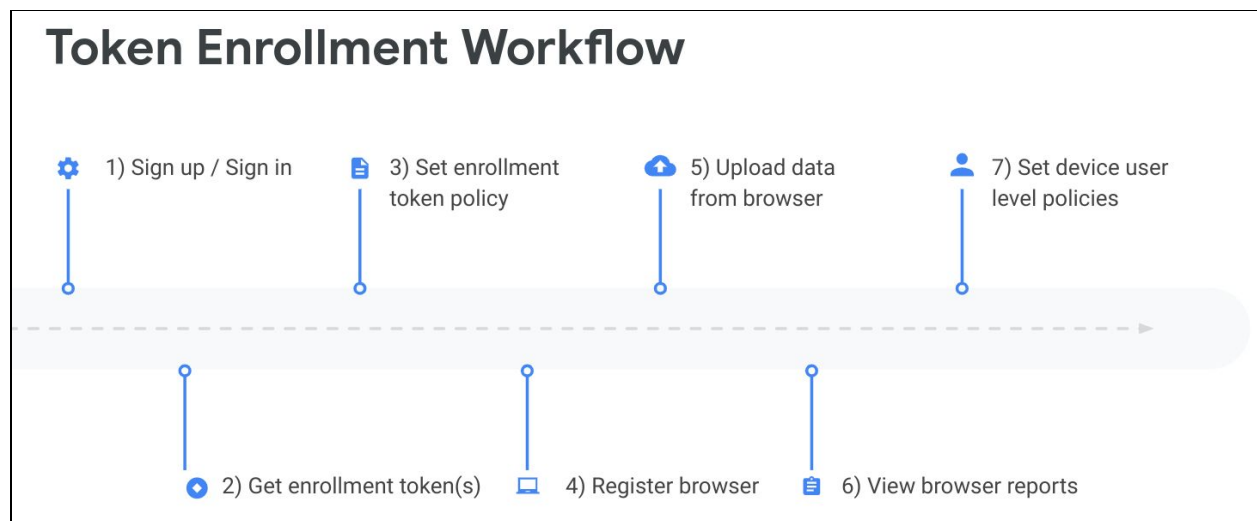
If you don't have G Suite or Chrome Enterprise licenses, set up a [provided domain](#). This gives you a Google-owned domain to use. This option has the same functionality as what you'd get with a verified domain, except that you're limited to one admin account.

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

How are devices enrolled?

Cloud management doesn't require your users to be signed in to Google. You will manage the devices by enrollment tokens.

The tokens are only used once to add your devices to the console. The token 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:

Token Enrollment Workflow

1) Sign up / Sign in

2) Get enrollment token(s)

3) Set enrollment token policy

4) Register browser

5) Upload data from browser

6) View browser reports

7) Set device user level policies

Enrollment tokens are associated with one organizational unit. When a device registers, it gets placed in that token's organizational unit. You can move the device from one organizational unit to another.

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 **Device management > Chrome > Managed Browsers**, then clicking **Download**. The data is exported in JSON file format.

You can delete enrolled browsers from the Admin console by clicking the menu ⋮ on the right and **Delete**. 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. See below to learn more.

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 Browser management is located under **Admin roles > Privileges > Chrome Management**. A user also might need to have read/write rights if they are also going to create organizational units for the browsers.

Auditing admin actions

You can view changes made in the console for auditing purposes. See Admin audit log.

Chrome Browser Cloud Management feature overview

Navigate directly to the Chrome Management section in the Admin console.
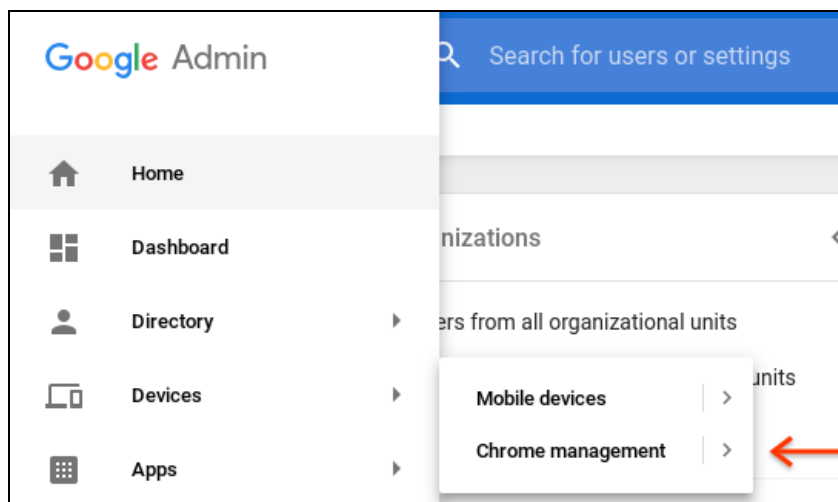
You can also find the console under **Devices > Chrome management**. The main features of the console are in the following sections:

- **Managed browsers:** View the details of the managed machines, and organize the devices into organization units for granular management.
- **User & browser settings:** Find the central location for managing user & browser based settings for Chrome Browsers.
- **App management:** Manage applications and Chrome extensions.
- **Browser extensions list:** View what extensions are installed, how they were installed, their status, and required permissions.

Browsers page
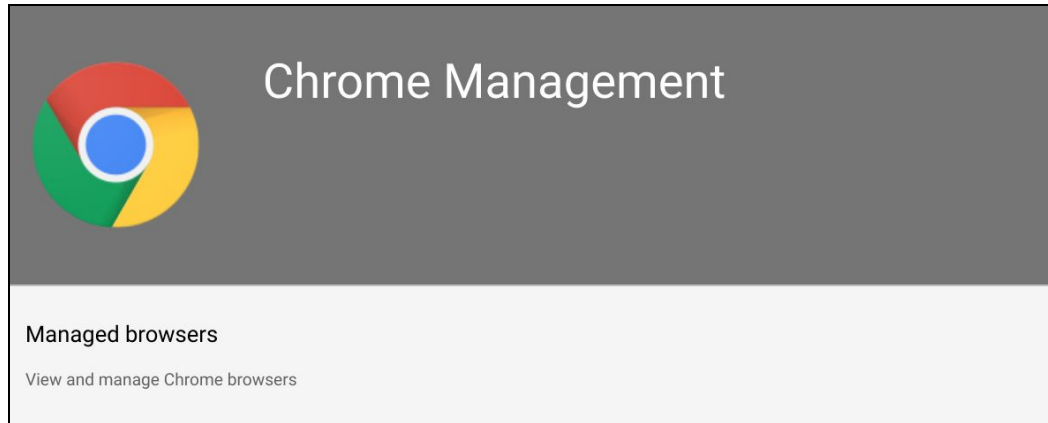
In this section of the console, you can see a list of the machines that have managed browsers. Click on a device for details.

- **Device details:** View managed machine's name, OS version, user details, architecture (32 or 64 bit), enrollment date, and applied Chrome Browser policies.
- **Browser & Profiles:** View the browsers that are installed, what version or release channel (Stable, Dev, Beta, or Canary), and which profiles the installation is linked to.
- **Installed apps & extensions:** View the installed applications and extensions, their stats, how it was installed, version or release channel, and what user profile it's installed on.

 Through More ⋮ on each application or extension, there are 2 actions:
    - Block—Restrict the application or extension from being run.
    - Force-install—Require and autoinstall the selected application or extension.
- **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 is the device policy first, then the OS user policy, and then the cloud Policy. For additional details, review the image below and 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.

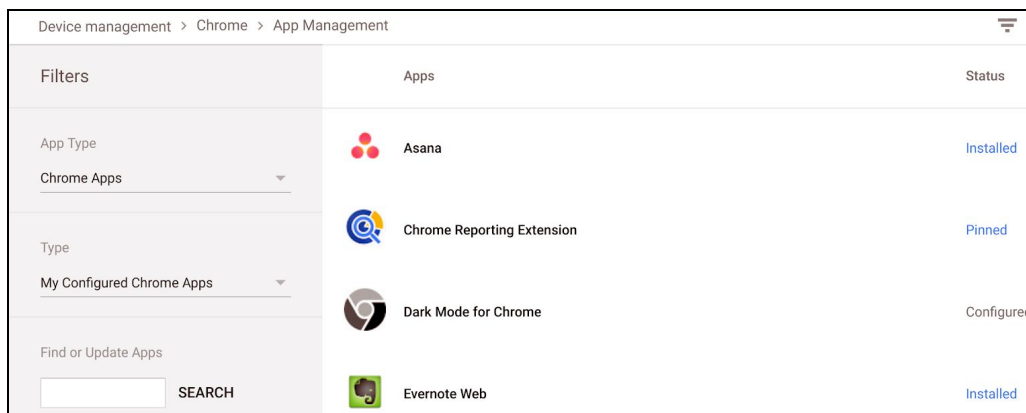## User & browser settings section
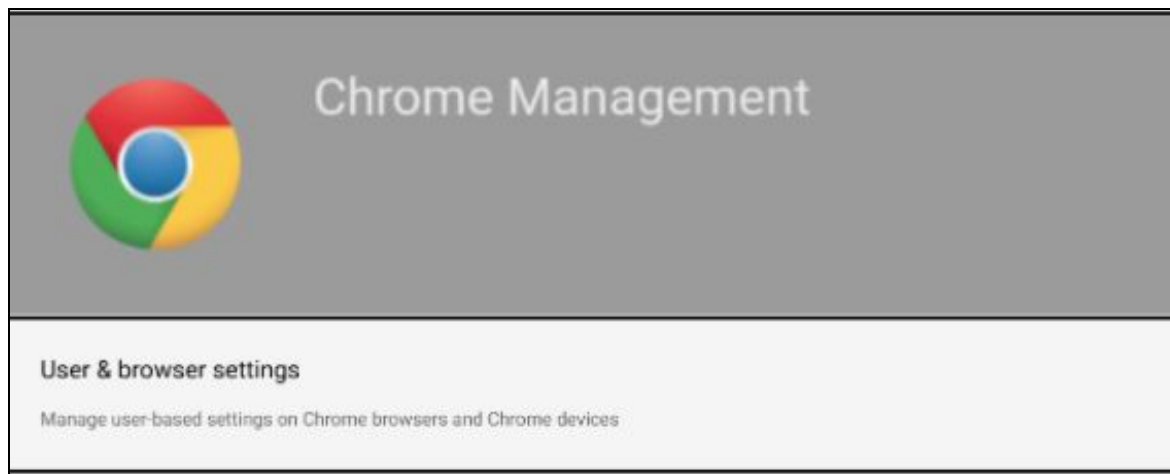
In this section, you can set various policies and settings for your managed devices. Some fields might not be relevant if your enterprise is only managing Chrome Browser and you aren't a G Suite customer. To learn more, see Set Chrome policies for users or browsers.

App Management section
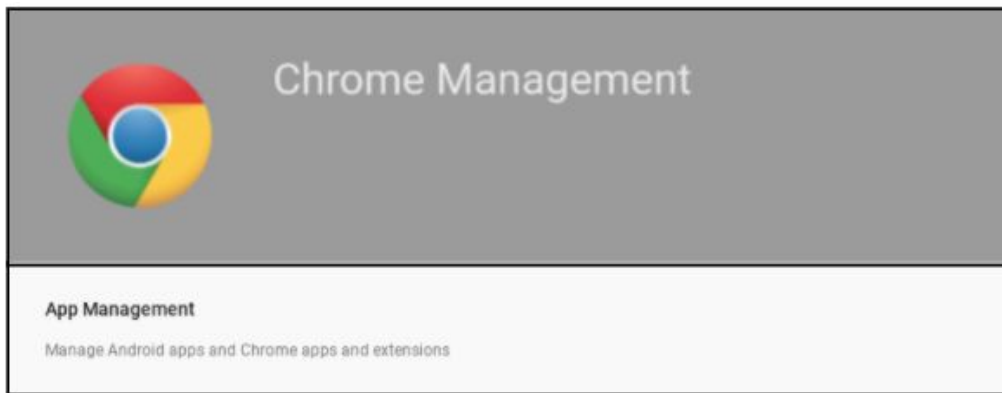
In this section, you can set permissions and policies for a single app and apply them to a specific organizational unit or the entire enterprise. On the left side of the console, specific apps can be searched by name or by type.

Clicking on the extension will expand to the setting for that specific extension or application through the user settings and public session settings. This can apply for signed-in users on any device, or enrolled browsers on Windows, Mac, or Linux. Find more information and a quick overview of each setting:

- **Allow installation:** 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 installation:** Force-install the extension or application on to users' machines.
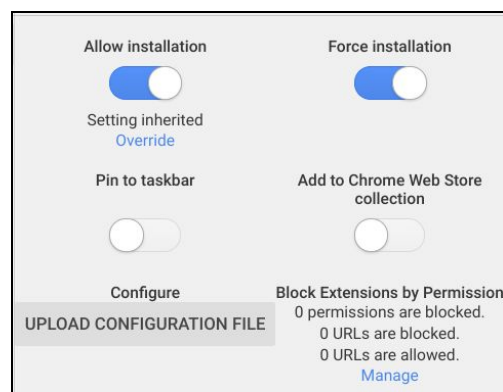
- **Pin to taskbar:** Pins the application or extension to the taskbar (Chrome OS only).
- **Add to the Chrome Web Store:** Adds to CWS as a recommended extension or application.
- **Configure:**
  - Uploads a configuration file for customized policies or settings supported by the app.
  - Details about the creation of configuration files are located using this link.
- **Block Extensions by Permission:** Allows for blocking extensions or applications by permissions.

Browser extensions list
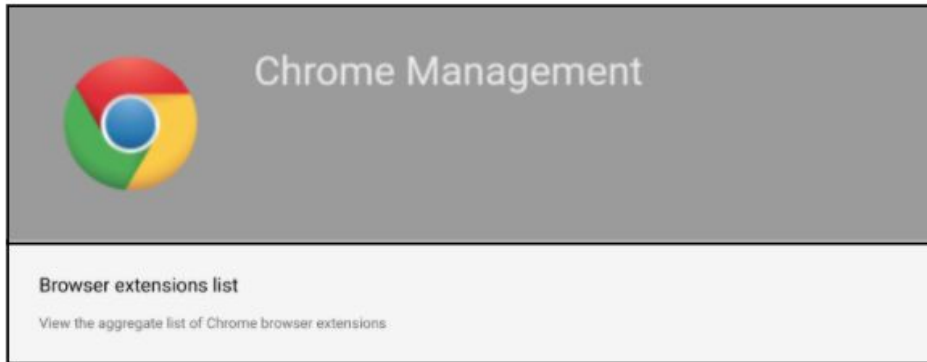
The browser extensions list provides the administrator an overview of the status of extensions in their enterprise. The view can also be filtered by selecting an organizational unit using the field to the left.

Within the view, you can see:

- **Extension name:** Clicking on the name will link to that extensions page in the Chrome Web Store.
- **Version:** This is the version of the installed extension.
- **Install Type:** The options are normal (by user), admin (by policy), sideload (installed outside of Chrome Web Store) or multiple (install types).
- **Installed:** Refers to how many instances are installed within your enterprise.
- **Disabled:** This is the number of instances of that extension that are disabled on a user's machine.
- **Forced:** Lists how many instances of this extension were force-installed (either through GPO or Cloud Policy) onto users' machines.
- **Permissions:** Refers to the number of permissions required to run the selected extension.

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 also search for a specific permission type, install type, name, or app ID. Multiple items can be entered separated by a space. Here is the syntax to use and an example image of searching multiple items:

- id
- version

- name
- permission
- install_type

Setting up Chrome Browser Cloud Management

Follow the steps for [Chrome Browser Cloud Management setup](#).

Best Practices for Chrome Browser Cloud Management

Cloud Reporting

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

- Your company devices and operating systems running Chrome Browser
- 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](#).

Extension Management

Protect your users from potentially harmful software by only allowing them to install extensions you have tested and approved. Block all apps and extensions. Then create an allow list of approved extensions in User Settings.

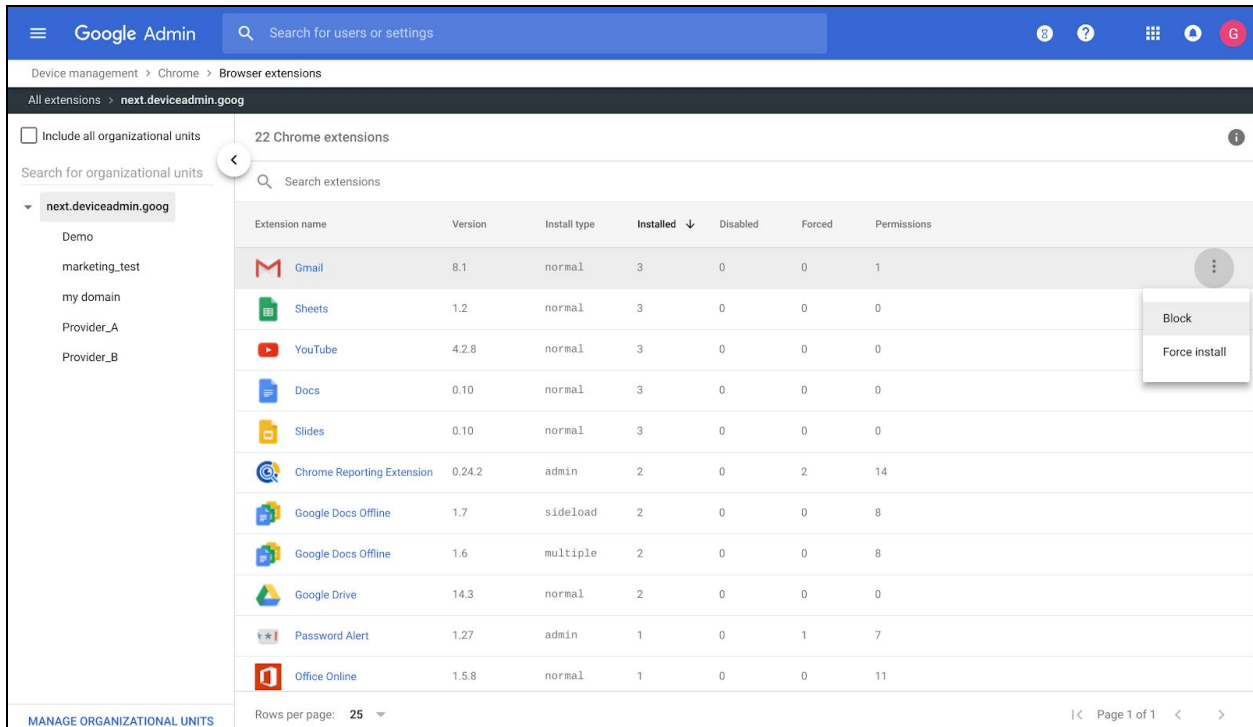| Block Extensions by Permission | Permissions and URLs 💡 |
| Locally applied | Block extensions by permissions and URLs. Learn more |

If the extension uses one of the selected permissions, block users from installing or using it

☐ Alarms	☐ Audio Capture	☐ Certificate Provider	☐ Clipboard Read
☐ Clipboard Write	☐ Context Menus	☐ Desktop Capture	☐ Document Scan
☐ Enterprise Device Attributes	☐ Experimental APIs	☐ Fullscreen Apps	☐ File Browser Handler
☐ File System	☐ File System Provider	☐ HID	☐ Override Fullscreen Escape
☐ Detect Idle	☐ Identity	☐ Google Cloud Messaging	☐ Geo Location
☐ Media Galleries	☐ Native Messaging	☐ Captive Portal	☐ Power
☐ Notifications	☐ Printers	☐ Authenticator Serial	☐ Set Proxy
☐ Platform Keys	☐ Storage	☐ Sync File System	☐ CPU Metadata
☐ Memory Metadata	☐ Network Metadata	☐ Display Metadata	☐ Storage Metadata
☐ 2-Factor Devices	☐ Text to Speech	☐ Unlimited Storage	☐ USB
☑ Video Capture	☐ VPN Provider	☐ Web Requests	☐ Block Web Requests

If you would like to give your users more freedom while preventing them from installing extensions that, for instance, rely on video capture, you can block extensions by permission. You'll prevent any extensions that use that permission in User Settings. For more information, see Allow or block apps and extensions.

Also, you can block extensions from accessing sensitive sites through the console. By entering the URLs of the sites you never want extensions to run (to prevent the reading of data or cookies, for example), you can specify them under the Blocked URL section. They will function on other sites, so your users can use extensions that they want—just not on sensitive sites. To learn more about this feature and the URL syntax, see Prevent Chrome extensions from altering webpages.

If an extension already installed by your users is found to be harmful or unwanted, you can block it directly from the Browser extensions page.

See [Browser extensions list](#) for more details.

Extensions that are mandatory for all users can be force-installed from the Extensions List page (as above) or from User Settings. This saves users from having to install those extensions themselves, ensuring that they all have access to essential tools they need to stay productive.

For more information on force-installing extensions, see [Automatically install apps and extensions](#).

Safe browsing

A major security concern for many enterprises is exposure to malware and phishing. Users might unintentionally navigate to unsafe webpages, which could then cause a costly loss of data and damage to reputation. Enable Safe Browsing in User Settings to show users a warning message before they visit a dangerous site or download a harmful app. For added security, you can also prevent users from proceeding anyway to potentially malicious sites after they have been shown a warning.

URL blocking

In addition to the sites that are flagged by safe browsing, there might be sites that you don't want your users to visit—whether because of privacy concerns, or to ensure they stay productive. Use the URL Blacklist to specify URLs that should be blocked. You can use wildcards to block a broader set of URLs that match a pattern.

The URL Blacklist Exception list specifies URLs that will always be allowed. If a URL appears or matches a pattern in both lists, the exception list will take precedence and the URL will be allowed.

URL Blocking
Locally applied

URL Blacklist
Any URL in the URL blacklist will be blocked, unless it also appears in the URL blacklist exception list. Put each URL on its own line. For example:
example.org
http://example.com
[Google Chrome Build 15.0.874.12+]

URL Blacklist Exception
Any URL in the blacklist exception list will be allowed, even if it appears in the URL blacklist. Wildcards ("*") are allowed when appended to a URL, but cannot be entered alone. Put each URL on its own line. For example,
sites.example.org
http://mail.example.com
file://*
[Google Chrome Build 15.0.874.12+]

Bookmark management

Make it simple for your users to find the tools they need to do their jobs by creating Managed Bookmarks. In this folder, curated by you and your team, users will find everything they need in one place. Create different lists in different organizational units to customize Managed Bookmarks for different sets of browsers. Users won't be able to change or delete any of these bookmarks, so they won't get lost or overwritten.

Managed Bookmarks
Locally applied

Managed Bookmarks Folder Name

Managed Bookmarks

URL	Name	Count: 0
www.example.com	Name	+

Enrollment token details

The enrollment token is used to tie the device 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.
4. For Windows computers, this device token is stored in the registry.

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:
- 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).

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:
- 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.

Conclusion: The future of Chrome Browser Cloud Management

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 G Suite users and applications, Chrome devices, Jamboards, and mobile devices. While platform-specific policy management (such as GPO) remain available, Cloud Management gives you control of all your Chrome Browser instances. In the future, we plan to:

- Update controls, such as the ability to roll back to a previous version of Chrome and to only relaunch Chrome at specific times of day after an update.
- Enable Legacy Browser Support from the Admin console.
- Allow admins to protect passwords by configuring Password Alert in the Admin console. This helps prevent password reuse and gives the admin visibility into if their users type their password into a non-corporate site.

Chrome Browser Cloud Management in the Google Admin console is just getting started. We're continuing to work on improvements to make it even more powerful.