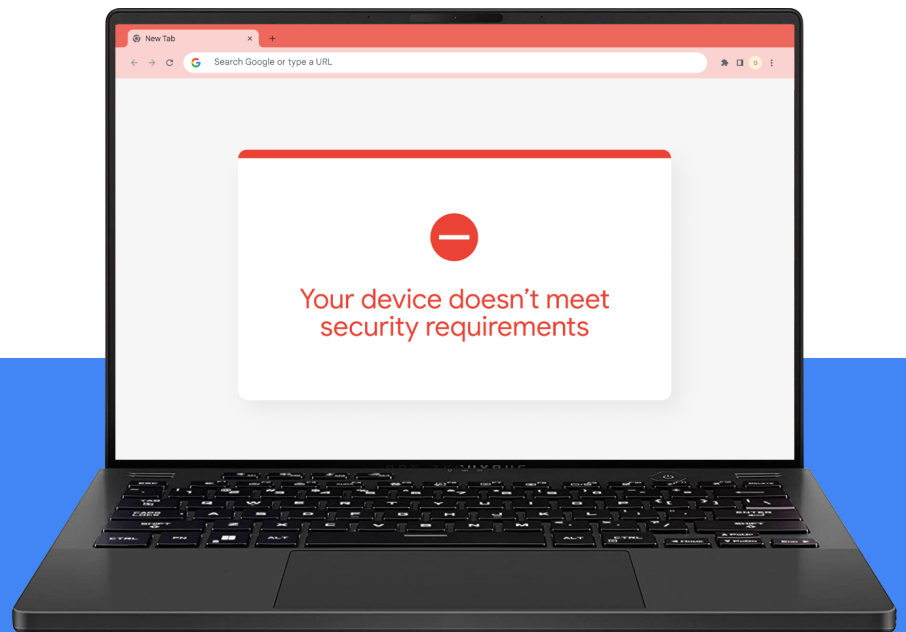


Understanding your **Privacy Mode** Options in Chrome Browser

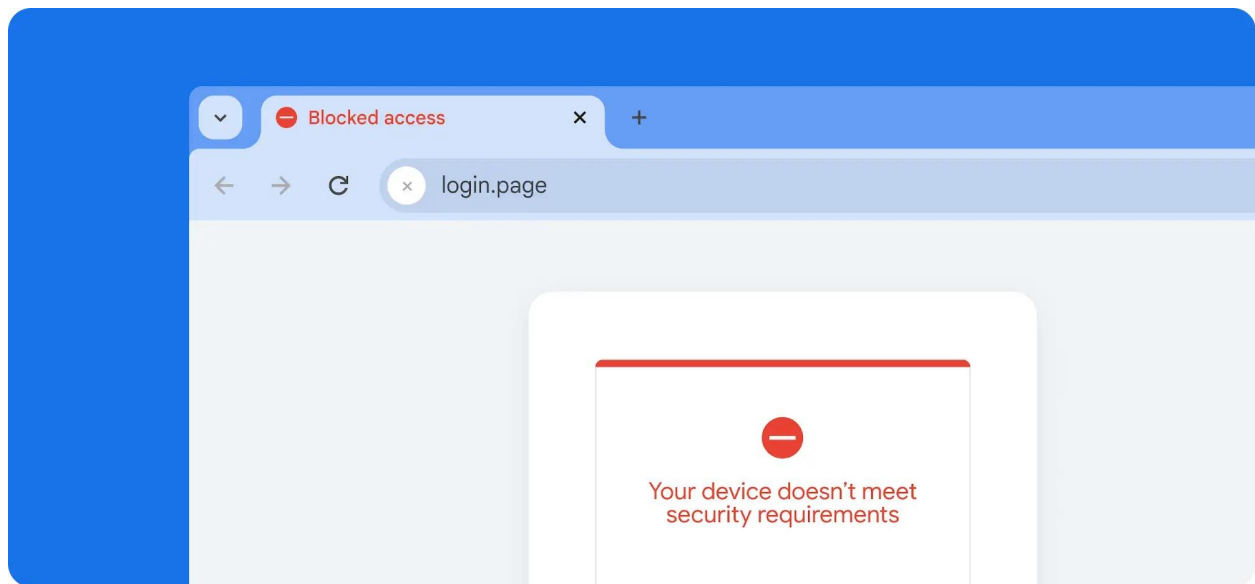
How Chrome can play a central role
in your enterprise security strategy



Introduction

With employees spending more time on the web than ever before, the browser has become the heart of the modern workday. IT and security teams are under pressure to secure this critical endpoint without disrupting productivity, but traditional security solutions are no longer sufficient and can negatively impact the user experience.

With automatic, built-in security features that detect over 40,000 phishing attacks and more than 1,000 malware sites daily, Chrome browser makes it safe and easy for users to access the web content they need from anywhere, with any device. In this paper, we will detail the ways you can deploy privacy modes, work profile policies, and other tools you can use to help your employees understand how their browser is being managed.



Chrome Browser Privacy Modes

As an IT administrator, you have the ability to apply policies to the browsers you manage. Chrome checks periodically for updates to your environment's policies. To implement private browsing across your enterprise, consider the following Chrome browser privacy modes, which are recommended for shared or public terminals that are used by multiple employees.

Guest mode: In Guest mode, users start with a blank slate, with no bookmarks or enabled apps and extensions. At the end of the session, the browser erases browsing history information such as URLs visited, cached page text, snapshots of pages visited, records of downloaded files, and IP addresses of pages linked from the websites visited. Guest mode is ideal for letting others borrow your device, borrowing someone else's device, or using a public device.

When the [BrowserGuestModeEnabled](#) policy is set to true or not configured, Chrome will enable guest sessions. When this policy is set to false, Chrome will not allow guest sessions.

There is also [BrowserGuestModeEnforced](#), which forces Chrome to always start in Guest mode. When enabled, Chrome will enforce guest sessions and prevent opening Chrome in existing profiles. All guest session browsing takes place in Incognito windows, and activity isn't attributed to a specific user. If this policy is set to disabled or not set, or browser guest mode is disabled by the [BrowserGuestModeEnabled](#) policy, Chrome will allow the use of new and existing profiles.

Ephemeral mode: When Ephemeral mode is set at the user level in the Google Admin console, the user signs into Chrome Sync to access their bookmarks (including corporate bookmarks), browsing history, apps and extensions, corporate intranet pages, and corporate webmail, as well as features such as Cloud policy and password storage. You can force a user's Chrome profile to open in Ephemeral mode when working from a trusted personal or shared device that meets corporate policies.

Forcing Ephemeral mode reduces the chance of any browsing information being left behind on the device. At the end of the session, all records of browsing activity are erased, just as in Guest mode. Do not use Ephemeral mode if you are using the [Chrome Roaming Profile Support](#) feature on Windows. There are also more granular policies that control how Chrome retains certain types of data.

If you use Ephemeral mode, we strongly recommend you also use Chrome Sync. If Chrome Sync is enabled, any changes that the user makes to the browser's settings or to their Chrome data (such as bookmarks, history, apps, etc.) during an Ephemeral mode session will be saved for future sessions in their Google account in the cloud. If Chrome sync is not enabled, any changes are lost when the user exits the browser.

When the [ForceEphemeralProfiles](#) policy is enabled, it forces the profile to be switched to Ephemeral mode. If this policy is specified as an OS policy (e.g., GPO on Windows), it will apply to every profile on the system. If the policy is set as a Cloud policy, it will apply only to a profile signed in with a managed account.

Incognito mode: If you don't want Chrome to remember a user's activity, consider enabling Incognito mode to allow private web browsing on their device. They'll see their info and settings without saving any browsing history. Chrome Sync is unavailable in Incognito mode. Users can elect to browse in Incognito mode, whereas Ephemeral mode is a policy enforced by the organization's administrator. Apps and extensions are not enabled by default in Incognito mode, but the user can enable them.

The [IncognitoModeAvailability](#) policy enables admins to decide whether or not they want to allow their users to browse in Incognito mode. If enabled or the policy is left unset, users may open pages in Incognito mode. If disabled, users cannot open pages in Incognito mode. If forced, pages will be opened only in Incognito mode.

These modes can all be enabled in managed browsers with the Google Admin Console, Group Policy, JSON file editor, or in your Chrome configuration profile depending on the operating systems you are configuring. After you apply any Chrome policies, users must restart Chrome for the settings to take effect. Check users' devices to make sure the policy was applied correctly.

How Chrome Handles Your Incognito or Guest Information

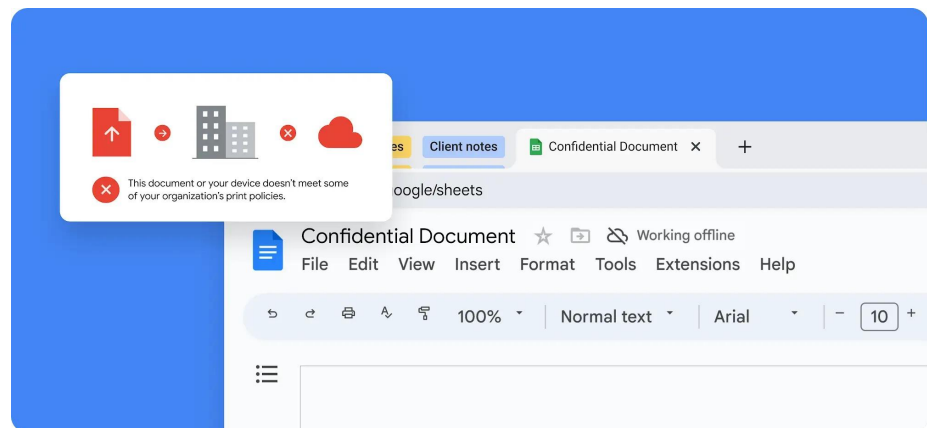
Chrome won't share existing cookies with sites you visit in Incognito mode or Guest mode. However, sites may read and write cookies during an Ephemeral mode session. All cookies are permanently removed when the session is terminated.

In Incognito mode, users have access to information from their existing profile, such as suggestions based on browsing history or saved passwords. Changes made to the browser configuration, like bookmarking a site or updating settings, are saved while permissions granted are not.

In Guest mode, you can browse without seeing information from any existing profiles. Guest mode is always an entirely new session and does not have any existing user data.

Profiles Help Separate Employee Work From Personal Data

Policies can be set that force users on corporate Windows, Mac, or Linux computers to sign in to their managed account to use Chrome. If there's a conflict between a user policy set in the Google Admin console and a device policy, the device policy takes precedence.



BrowserSignin

Specifies whether users can sign in to Chrome and sync browser information to their Google Account. Choose one of these options:

0 — Disable browser sign-in: Users can't sign in to Chrome or sync browser information to their Google Account.

1 — Enable browser sign-in: Users can sign in to Chrome and sync browser information to their Google Account. Chrome automatically signs in users when they sign in to a Google service, such as Gmail.

2 — Force browser sign-in: Forces users to sign in to Chrome before they can use it. Chrome does not let secondary users sign in. Sync is turned on by default and users can't change it. To turn off sync, use the [SyncDisabled](#) policy.

Unset: Users can sign in to Chrome. When users sign in to a Google service such as Gmail, Chrome automatically signs them in. Users can sign out or switch to different profiles as needed.

RestrictSigninToPattern

Restricts which Google Accounts can be signed in to as primary users in Chrome.

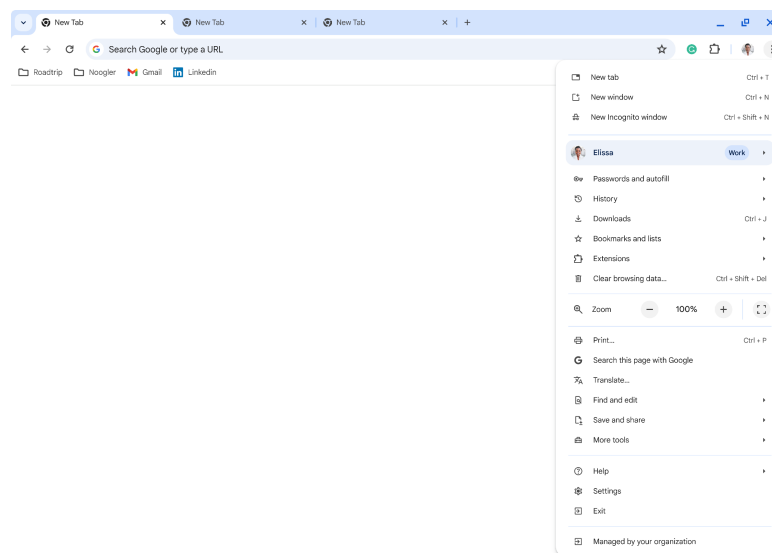
Use it with BrowserSignin to force users with multiple Chrome profiles to sign in to a specific profile before using Chrome. Users can only sign in with profiles that match the patterns you specify.

Unset: Users can sign in to any Google Account as a primary user in Chrome.

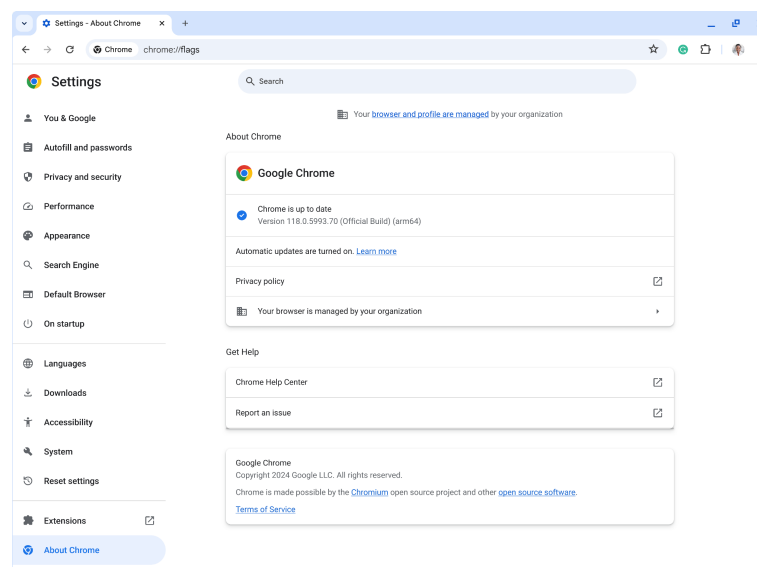
Help Your Organization's Users Understand How Their Browser is Being Managed

Privacy and transparency go hand-in-hand. Chrome is committed to giving users visibility into settings and configurations, even at the enterprise level. Google provides users with 4 ways to find information about what is being managed in their browsers:

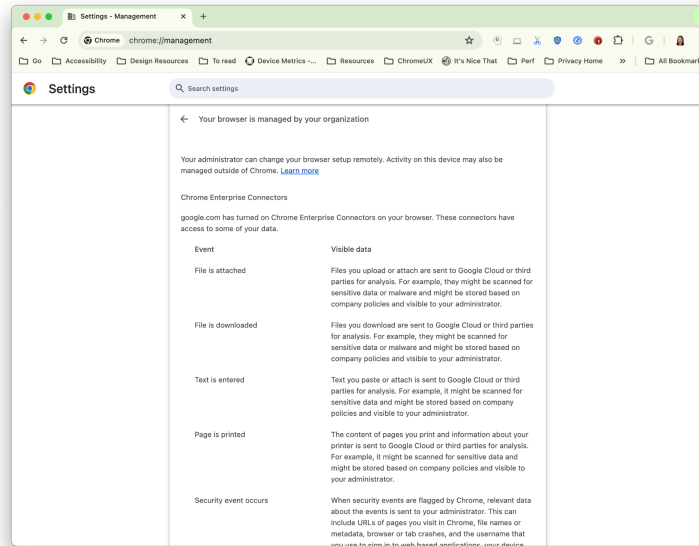
1. Users can see if their browser is managed by clicking on the three dot menu in the top right corner of their Chrome window. If their browser is managed, a message will display at the bottom of the dropdown menu.



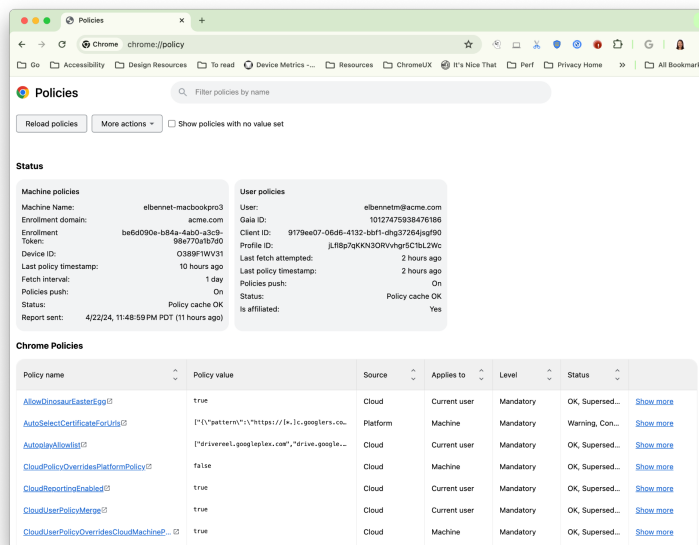
2. If a user clicks Settings in the three dot menu dropdown, a new window will open. If their browser is managed, a message will display at the top of the window.



- By directing users to **chrome://management**, they can see the extensions you have implemented. Users have visibility into what you are able to see from an admin perspective.



- By directing users to **chrome://policy**, they can see which policies you have enabled on their browser. Users have visibility into what you are able to see from an admin perspective.



Conclusion

To help your organization better meet its privacy and compliance standards, or help your users better understand how their browser is being managed, please consider these management options.

This guide does not constitute legal advice. We recommend you consult a legal expert to obtain guidance on the specific requirements applicable to your organization.

To deepen your understanding of Chrome's private browsing modes, consider the following resources:

Learn more about [Ephemeral mode](#)

Discover more about [browsing in Incognito mode](#)

Learn how to [allow private browsing](#)

Explore [Chrome Enterprise Core](#)

Download [Chrome](#) for your enterprise

Learn more about [Chrome Enterprise support](#)

Explore the [Chrome Enterprise policy list](#)

Read the latest [Chrome Enterprise and Education release notes](#)

Stay up to date on the latest Chrome browser release updates via the [Chrome Releases blog](#)

Explore [Google's official Safety & Security blog](#)

Visit the [Chrome Enterprise and Education Help Center](#) and [Google Chrome Help Community](#)

Review the [Chromium Public Bug Tracker](#)