chrome enterprise

Chrome Browser privacy guide for enterprises: Understanding your privacy mode options

Introduction

Thanks to the everywhere access to key apps and data accessed through the browser, the most connected business users are spending more than half of their day working in the browser. However, organizations also face growing security, privacy, and compliance requirements, while balancing giving users fast, reliable, and secure access to their web apps around the clock.

You expect a reliable and secure browser that your organization can trust and that provides options to help protect your organization's and employees' data efficiently. Depending on your organization's privacy and compliance requirements, you may also choose to utilize Chrome Browser's different policies to meet these requirements. We will detail ways your admins may deploy privacy modes, policies that help separate your employees' work vs. user profiles, and--finally--tools you can use to help your employees understand how their browser is being managed.

chrome enterprise

Chrome Browser privacy modes

As an IT administrator, you have the ability to apply policies to the browser 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, you won't see or change any other Chrome profile's info. When you exit Guest mode, your browsing activity is deleted from the computer. 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, Google Chrome will enable guest sessions. Guest sessions are an Ephemeral session that starts with a blank slate and leaves nothing from that session behind. When this policy is set to false, Google Chrome will not allow guest profiles to be started.

There is also BrowerGuestModeEnforced, which forces Chrome Browser to always start in Guest mode. When enabled, Google Chrome will enforce guest sessions and prevents opening Chrome Browser in existing profiles. Guest sessions are Google Chrome profiles where all windows are in incognito mode. If this policy is set to disabled, not set, or browser guest mode is disabled by BrowserGuestModeEnabled policy, Google Chrome will allow using new and existing profiles.

Ephemeral Mode: To enable your employees to work from their personal laptop or a shared device that they trust, you can force the Chrome profile to be ephemeral by policy. Forcing Ephemeral mode reduces the chances of any browsing information being left behind on their device. During the ephemeral session, the user has access to the full extent of a browser session including: signing in for Chrome sync, Cloud print, Cloud policy, Password storage, Bookmarks, autofill and other data normally present in the user profile, any corporate assets that are enabled in Ephemeral mode, which may include corporate webmail, documents, and intranet pages. If you use Ephemeral mode, we strongly recommend that 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 session will be saved for future sessions. The settings are saved in the user's Google account in the cloud. If Chrome sync is not enabled, any changes are lost when the user exits the browser.

When the ForceEphemeralProfiles 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 Google Chrome to remember a user's activity, consider enabling Incognito mode to allow private web browsing on their own device. They'll see their info and settings without saving any browsing history. Incognito mode is an organization's user's choice to browse in Incognito mode, whereas Ephemeral mode is a policy that is enforced by the organization's administrator. The below policy is for an admin to decide whether or not they want to allow their users to browse in Incognito mode. In Incognito mode, the user can't sign in and have the benefits of Chrome sync, such as corporate bookmarks.

Apps and extensions are not enabled by default in Incognito mode, but the user can enable them. Apps and extensions are enabled by default though in Ephemeral mode. Ephemeral mode gives the employee productivity benefits while reducing the risk of leaving data behind. When Ephemeral mode is set at the user level in the Admin console, it relies on the user to sign in to Chrome for sync benefits and for the policy to take effect. The policy should be used only on devices that the user trusts and that are compliant with other corporate policies. The profile is marked for deletion only after the user signs out or manually closes every window associated with the profile. The profile is deleted the next time Chrome starts. 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 whether and how Chrome retains certain types of data.

The IncognitoModeAvailability policy specifies whether the user may open pages in Incognito mode. If enabled or the policy is left unset, pages may be opened in Incognito mode. If disabled, pages may not be opened in Incognito mode. If forced, pages may be opened ONLY in Incognito mode.

You can enable any of these modes via a policy in any managed browsers via 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 Browser for the settings to take effect. Check users' devices to make sure the policy was applied correctly.

Using Incognito mode or Guest mode you can limit the information Chrome stores on your system when in these modes. Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit.
- Snapshots of pages that you visit.
- Records of your downloads, although the files you download will still be locally stored elsewhere on your computer or device.

chrome enterprise

How Chrome handles your Incognito or Guest information

Chrome won't share existing cookies with sites you visit in Incognito or Guest mode. When in Guest or Incognito mode, there will be no existing cookies since it is a clean slate. For the duration of the ephemeral session, sites may read and write cookies. The session is terminated when the last tab or window is closed, upon which all cookies are permanently removed. When you make changes to your browser configuration in Incognito mode, like bookmarking a webpage, or changing some settings, such as accessibility settings, this information is saved. This is only true for Incognito mode, not in Guest mode. Permissions you grant in Incognito mode are not saved to your existing profile. In Incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords while you are browsing. 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 can help separate between employee work and 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 Browser. If there's a conflict between a user policy set in the Admin console and a device policy set, for example, using Chrome Browser Cloud Management or Windows Group Policy, the device policy takes precedence.

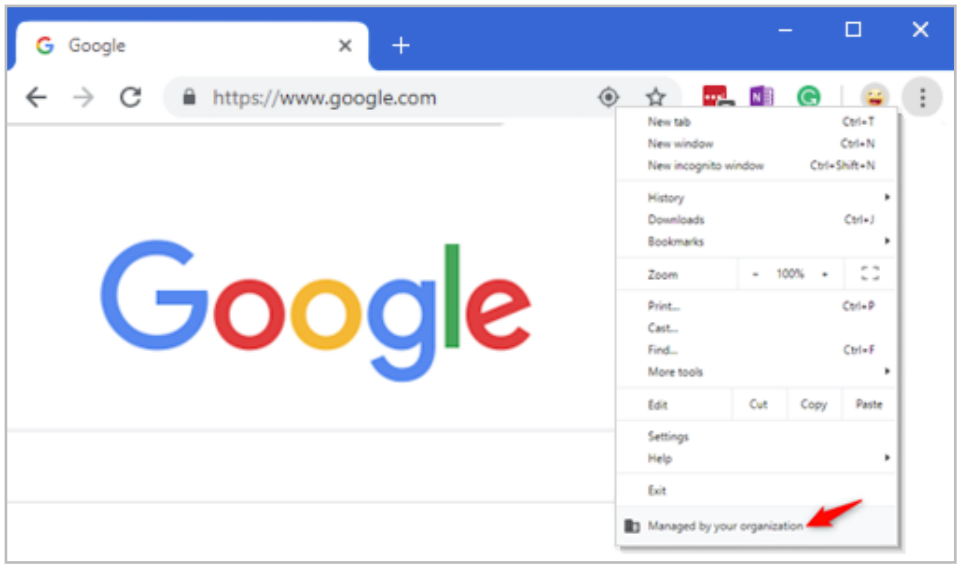
BrowserSignin
Specifies whether users can sign in to Chrome Browser and sync browser information to their Google Account. Choose one of these options:
0 — Disable browser sign-in: Users can't sign in to Chrome Browser or sync browser information to their Google Account.
1 — Enable browser sign-in: Users can sign in to Chrome Browser and sync browser information to their Google Account. Chrome Browser 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 Browser before they can use it. Chrome Browser 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 Browser. When users sign in to a Google service, such as Gmail, Chrome Browser automatically signs them in. Users can change it.
RestrictSigninToPattern
Restricts which Google Accounts can be signed in to as primary users in Chrome Browser.
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 Browser.

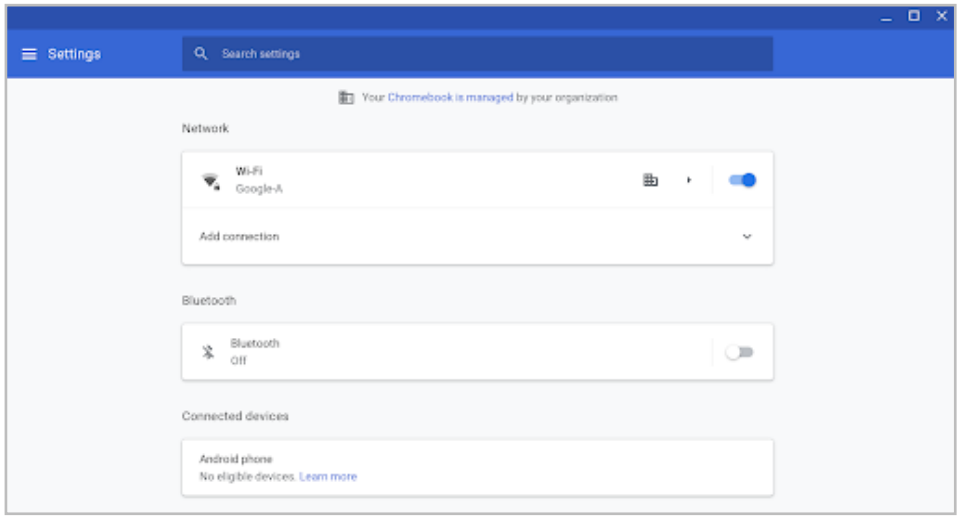
chrome enterprise

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 four ways to find information about what is being managed in their browsers.

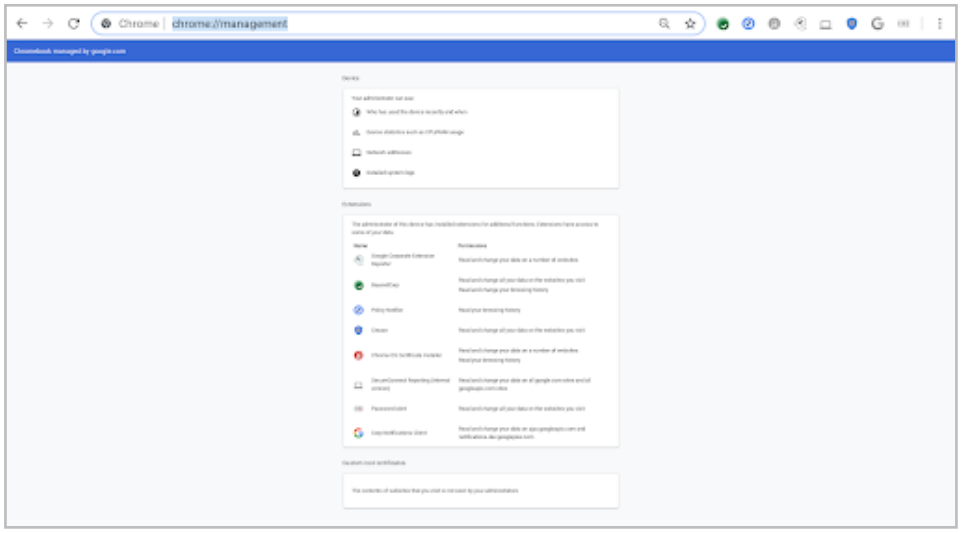
1. Managed By: Your users can gain visibility into knowing that IT is managing their device by their organization and that they can contact you with any questions. Users can see this by either seeing a "(Chrome is) Managed by Your Organization" message at the very bottom of the menu, under the "Exit" option, or if they click into "Settings."





chrome enterprise

2. By directing users to "chrome://management," they are able to see the extensions you as an admin have implemented, as well as provide visibility to them in what you are able to see from an admin perspective. Similarly, if users want to search "chrome://policy," they can get visibility into which policies you as an admin have enabled on their device.



chrome enterprise

Conclusion

To help your organization better meet their privacy and compliance standards, or help your users better understand how their browser is being managed, please consider these management options. This guide is intended to help administrators who manage Chrome Browser for a business or school customize Chrome Browser policies and settings to help meet their organization's privacy, data protection, or compliance needs. We recommend you consult with a legal expert to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

To deepen your understanding of Chrome Browser private browsing modes, **consider the following resources:**

Learn more about Ephemeral mode

Discover more about browsing in private

Explore how to browse Chrome as a guest

Learn more about how to allow private browsing

Explore Chrome Browser Cloud Management options

Check out Chrome Browser downloads for your enterprise

Learn more about Chrome Browser Enterprise Support

Explore the Chrome Browser Policy List

Read the latest Chrome Browser Enterprise 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 Browser Enterprise Help Center and Chrome Browser Help Forum

Review the Chrome Browser Public Bug Tracker