

Chrome Enterprise

Security Configuration

Guide

Based on Chrome 130
Last updated: Dec 2024

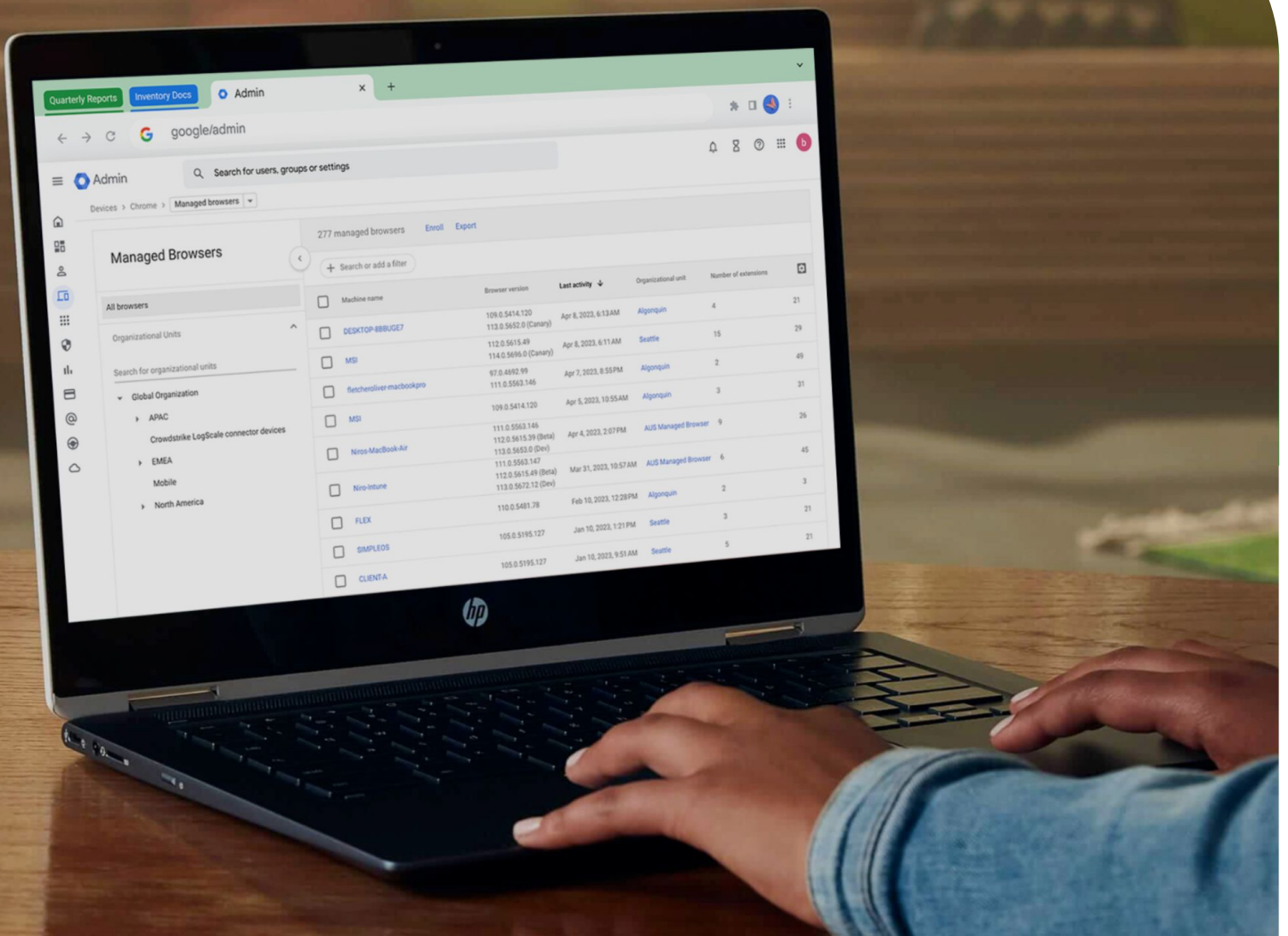


Table of Contents

Purpose of this guide	03
Introduction	04
Threat Prevention	06
Settings that enforce existing Chrome default behavior	07
Settings which degrade user functionality but reduce attack surface	11
Privacy	15
Settings relating to PII being stored on corporate devices	15
Settings relating to data flowing to the internet (data-loss)	18
Settings relating to data flowing to Google	20
User Journeys	23
Management and Performance	25
Managing Chrome	28
Chrome Enterprise Premium	28
Additional resources	30

Purpose of this guide

This document is focused on Chrome on Windows operating system, though most of the advice applies across all desktop platforms. There are trade-offs administrators need to consider when deciding between security for their organization and what technology and features their users want to access.

This document explores in detail the different security policies Chrome offers and the different compromises admins need to evaluate before enabling/disabling these policies.

What's covered

Recommendations and critical considerations for security-conscious organizations when enabling or disabling Chrome's security policies.

Primary audience

Microsoft® Windows® and Chrome browser administrators

IT environment

Microsoft Windows 10 and later

Takeaways

Considerations between enterprise security and its impact on users when setting security policies for Chrome browser.

Introduction

Chrome is designed to be a secure browser. The Chrome team takes security seriously, and we're proud of our reputation of pushing the browser industry forward in many areas, such as sandboxing, TLS standards, and usable security.

Out of the box, Chrome aims for a balance of security and usability that provides the best experience for all users. However, enterprises may have slightly different goals for using a secure browser in their organization. This document describes some options for configuring Chrome Enterprise to meet those goals.

Chrome's default behavior is to provide usability and security at the same time. In other cases, usability conflicts with security. In these cases, Chrome provides the option for you to choose, by offering a policy option. You, the IT administrator, decide what's the best policy to set in these specific cases.

This document describes some of the instances where you can choose between usability and security, and the pros and cons in each case. In each case, you should consider the security issues versus the usability issues, and decide the appropriate policy setting for your enterprise environment.



Introduction

This document looks at three distinct enterprise security needs:

Threat prevention

Privacy




User Journeys

Management and performance



Many of the recommendations here reference particular policy settings, full documentation for which can be found at <https://chromeenterprise.google/policies/>.

Threat prevention

Chrome already takes steps to eliminate threats from malicious websites, including:

-  **Site Isolation**, which keeps each website isolated into its own independent memory space (operating system process). For more info, see this [Help Center article](#).
-  **Sandboxes** are applied to these processes to reduce chances of the rest of the computer being affected by a vulnerability.
-  **Safe Browsing** finds malicious and deceptive content/software by constantly scanning the web and classifying the danger. Users are warned before reaching a site that has been flagged as potentially harmful.

Because Chrome is safe by design, you can further configure the browser for added threat prevention in two approaches:

-  **Enforcing standard default Chrome behavior**, so that users can't override it.
-  **Increasing security** still further, by making tradeoffs between ease of use and security.

The following two subsections discuss potential configurations in these areas.

Settings that enforce existing Chrome default behavior

Chrome is secure by default, but some settings can be changed by the user if they wish to change behavior. This can come at the expense of security. Admins can enforce some of the settings by policy.

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to ensure no previous administrators have set insecure policies within our organization.	None	None	<p>Ensure that the following policies are not already set, so that you get the benefit of the default (most secure) configuration:</p> <pre> EnableDeprecatedWebPlatformFeatures RunAllFlashInAllowMode SuppressUnsupportedOSWarning EnableOnlineRevocationChecks OverrideSecurityRestrictionsOnInsecureOrigin CertificateTransparencyEnforcementDisabledForC as CertificateTransparencyEnforcementDisabledForL egacyCas LegacySameSiteCookieBehaviorEnabled LegacySameSiteCookieBehaviorEnabledForDomainLi st ChromeVariations DnsOverHttpsMode LookalikeWarningAllowlistDomains SafeBrowsingAllowlistDomains RemoteAccessHostAllowRemoteAccessConnections PostQuantumKeyAgreementEnabled DevicePostQuantumKeyAgreementEnabled EnableDeprecatedWebBasedSignin InsecureContentAllowedForUrls EncryptedClientHelloEnabled InsecureFormsWarningsEnabled InsecureHashesInTLShandshakesEnabled UnsafelyTreatInsecureOriginAsSecure CertificateTransparencyEnforcementDisabledForU rls HttpsUpgradesEnabled SafeBrowsingDeepScanningEnabled </pre> <p>This is not an exhaustive list of security-related policies, but these particular policies are used by many enterprises. For more policy options, see our Chrome Enterprise policy list.</p>
I want to ensure users can't turn off fundamental security features.	None	None	<p>Explicitly set the policies:</p> <pre> AllowOutdatedPlugins, SitePerProcess, SafeBrowsingProtectionLevel and ThirdPartyBlockingEnabled. </pre> <p>There will be no user experience change except that users will be prevented from changing these settings.</p>

Threat prevention

Settings that enforce existing Chrome default behavior

Enterprise need	User impact	Potential adverse security impact	Options and notes
<p>I want to prevent users from downloading malware and avoid phishing, and ensure that these protections cannot be overridden by the user.</p>	<p>Low</p>	<p>None</p>	<p>Safe Browsing is the Chrome feature which aims to protect against malicious downloads and phishing. Read more about Chrome SafeBrowsing.</p> <p>Some enterprises are tempted to disable Safe Browsing because they feel that their existing security products (anti-virus, firewall) already fill these roles. Safe Browsing can work in tandem with your solution. For example, anti-virus products focus mostly on the content of downloads whereas Safe Browsing focuses more on the context - the chain of navigations which resulted in the user getting to the link. By disabling Safe Browsing, you lose the benefit of this knowledge.</p> <p>The Chrome security team recommends keeping Safe Browsing enabled. You can prevent the user turning off Safe Browsing with the policy <code>SafeBrowsingProtectionLevel</code> to 1 i.e. Safe Browsing is active in the standard mode. This should have no user-visible impact except that it prevents them from turning off Safe Browsing.</p> <p>In M79, we announced Enhanced protection in Chrome, a new option for users who require or want a more advanced level of security while browsing the web. Turning on Enhanced protection will substantially increase protection from dangerous websites and downloads. By sharing real-time data with Google Safe Browsing, Chrome can proactively protect users against dangerous sites, even ones Google didn't know about before. You can turn on Enhanced protection by setting <code>SafeBrowsingProtectionLevel</code> to 2.</p> <p>You can enforce Safe Browsing more aggressively by setting: <code>DisableSafeBrowsingProceedAnyway</code>. This may have user impact as it prevents a user continuing with their navigation if Safe Browsing has misclassified a website as malware or phishing.</p> <p>You may also wish to set <code>DownloadRestrictions</code> to 2 in order to enforce safe browsing decisions a little more strictly. For more info, see Prevent users from downloading harmful files.</p> <p>Some enterprises also decide to block printing because they see saved PDFs as another route that malware can be saved to disk. The Chrome security team does not think this is a useful step. In virtually all cases, format-conversion from a web page to a PDF file eliminates any malicious content, though we recommend using a safe PDF viewer for such saved files (such as Chrome itself).</p>

Threat prevention

Settings that enforce existing Chrome default behavior

Enterprise need	User impact	Potential adverse security impact	Options and notes
I'm planning to use a third-party software that requires injecting code into Chrome.	High	None	<p>Chrome blocks third-party software on the PC from injecting its own code into Chrome. Such third-party injection has proven to be a major source of crashes and bugs which could (in theory) be exploited by malicious websites. We recommend keeping the default set (<code>ThirdPartyBlockingEnabled False</code>).</p> <p>Other security products may advise you to unblock their code so that they can instrument Chrome or otherwise affect its behavior. If you choose to do this, you may get the benefit of their functionality, at the expense of more crashes and a higher risk of exploitable vulnerabilities.</p> <p>If you use a security product which injects executable code into Chrome, please contact the vendor to see if they offer this functionality through a Chrome extension instead. Also consider that Chrome Enterprise Premium's DLP features natively integrate into the browser without the need for third-party code injection, making it less disruptive to users and more stable. Also consider that there are robust DLP features in Chrome Enterprise Premium that are built directly into the browser. This eliminates the need for third-party code injection, leading to a more stable experience and less disruption for users.</p>

Settings which degrade user functionality but reduce attack surface

You can alter Chrome's functionality to reduce the attack surface available to malicious websites. With each item you block, users may experience degraded functionality.

Many of these changes disable Chrome features. We emphasize that each of these features has been designed and built to be secure out of the box, so disabling Chrome features should not be necessary. However, we know many enterprises wish to make changes or need to do so. Below are considerations to help you make those decisions.

Enterprise need	User impact	Potential adverse security impact	Options and notes
My organization has its own trusted root certificates on the endpoints which are used to trust enterprise servers. If attackers steal the private key for those trusted roots, I want to be able to revoke the certificates.	Low	None	<p>You can mark a root certificate as distrusted using the <code>CADistrustedCertificates</code> policy, or via Chrome Cloud Management.</p> <p>If you are additionally worried about leaf certificate keys being compromised, and you run an OCSP server for your private PKI, you can use the <code>RequireOnlineRevocationChecksForLocalAnchors</code> policy to force Chrome to check for revocation.</p> <p>Should the revocation be inaccessible, these certificates will not be usable (hard-fail), which could prevent websites from being accessible.</p>
Older versions of Chrome running in my environment may be exploitable by malicious websites.	Low	None	<p>You can force users to relaunch Chrome to take updates more rapidly using the policies <code>RelaunchNotification</code> and <code>RelaunchNotificationPeriod</code>.</p> <p>We strongly recommend this in an enterprise environment, as it will keep users on the latest version of Chrome with the latest security fixes.</p>
I want to avoid any risk that users' passwords will be intercepted when traveling across the internet using older authentication protocols (digest, basic auth).	Low	None	<p>You can disable these older schemes using <code>AuthSchemes</code>.</p> <p>Few modern legitimate websites use these schemes and disabling them in an enterprise context makes sense.</p> <p>As of Chrome 75 we recommend NTLM and Negotiate.</p> <p>Ensure your enterprise services also use modern authentication mechanisms.</p>

Threat prevention

Settings which degrade user functionality but reduce attack surface

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to stop documents from the cloud from compromising vulnerable printers.	Low	None	You can prevent your enterprise printers from receiving documents from Google cloud print by configuring <code>CloudPrintProxyEnabled</code> .
I'm concerned that attackers already in the network could compromise WPAD to move laterally.	Low	None	You can use <code>ProxySettings</code> to disable proxy auto-discovery.
I'm concerned that downloading files automatically might give attackers opportunities for unforeseen DLL planting attacks or to pass password hashes to malicious SMB servers. I want to disable automatic download.	Medium	None	To prompt the user for every download you can alter <code>PromptForDownloadLocation</code> .
I want to disable 3D graphics because I think it increases the attack surface and few websites used by our users require it.	Medium	None	<p>You can turn this off using <code>Disable3DAPIs</code>.</p> <p>Chrome already provides significant mitigations against 3D graphics attacks, including a layer called "ANGLE" whose job is to sanitise 3D inputs, plus isolation of all GPU-related code into a sandboxed process.</p> <p>Disabling WebGL will break virtual globe and mapping products.</p>
I want to reduce the risk that side-channel attacks can be used by one website to extract data from another website.	Medium	None	<p>You can make site isolation more fine grained with <code>IsolateOrigins</code>. Learn more at Protect your data with site isolation.</p> <p>Note: This will use more memory.</p>

Threat prevention

Settings which degrade user functionality but reduce attack surface

Enterprise need	User impact	Potential adverse security impact	Options and notes
<p>I want to eliminate the risk that Chrome Remote Desktop can allow external users to control computers in our network.</p>	<p>Medium</p>	<p>None</p>	<p>The Chrome Remote Desktop app can be blocked like any other app or extension. Learn more at Control use of Chrome Remote Desktop.</p>
<p>I want to disable extensions and apps because I think they increase the potential attack surface, and I don't mind impacting user workflows.</p>	<p>High</p>	<p>Low</p>	<p>Users' productivity may be significantly affected by blocking all extensions. In addition, some extensions may actually improve user security, for example if the user makes use of a third-party password manager for their personal passwords.</p> <p>We recommend managing extensions by permission: Block installation of those extensions which use permissions that you deem risky and allowing all others. For the remaining extensions, block their access to sensitive hosts.</p> <p>For instance, you might allow any extension except those which use the webcam or grab the screen image. You might additionally prevent any other extension from accessing your most precious corporate sites.</p> <p>For more details, see Chrome app and extension permissions and the Managing Extensions in Your Enterprise whitepaper. You can also contact your Chrome enterprise specialist for additional material to explain why enterprises choose this approach.</p> <p>If you can't identify a specific set of permissions which concern you, you can block particular extensions by setting <code>ExtensionInstallBlacklist</code>. A blacklist value of '*' means all extensions are blacklisted unless they are explicitly listed in the whitelist. Consider setting up an approval process for added extensions. We do not recommend the approach of blocking/approving particular extensions because it does not scale well.</p> <p>All Chrome extensions must be distributed either directly from the Chrome Web Store or using the mechanisms described below. Read more about external extensions. <code>BlockExternalExtensions</code> policy can be used to Block external extensions from being installed.</p>

Threat prevention

Settings which degrade user functionality but reduce attack surface

Enterprise need	User impact	Potential adverse security impact	Options and notes
#I want to prevent users from adding exceptions to allow mixed content for specific sites.	Low	Low	<code>DefaultInsecureContentSetting</code> can be used to control use of insecure content exceptions. If this policy is left not set, users will be allowed to add exceptions to allow blocked mixed content and disable auto upgrades for optionally blockable mixed content.
#I want to remotely fix issues that could be result of cookies or cache that are on user devices.	High	None	Remote Commands can be sent from Admin Console to clear cookies and cache.

Indicates a new field since Chrome 75

Privacy

Chrome is committed to protecting the user's privacy. Many enterprises want to minimize personally identifiable information or personal data (collectively, "PII") on PCs, and many enterprises are unaware of the extent that Chrome protects this data.

Some of Chrome's strongest security features (for instance, safe browsing and password managers) require exchanging information with Google services. The Chrome security team strongly recommends enabling these features. If you have concerns about using submitted data, please discuss them with your Chrome enterprise specialist.

These needs are categorized into three categories:

- 1 PII being stored on corporate devices
- 2 Data flowing to the internet
- 3 Data flowing to Google

Settings relating to PII being stored on corporate devices

Enterprise need	User impact	Potential adverse security impact	Options and notes
<p>I'm worried that other (non-admin) users logged into the same machine (either later, or at the same time using VDI) might be able to access sensitive data such as passwords belonging to other users that are on the machine's disk.</p> <p>I'm worried that machines may be stolen and passwords may be read off the disk by thieves.</p>	N/A	N/A	<p>All the personal details of the user (browsing history, cache, passwords, autofill data) are stored in a bundle of information termed the user's "profile".</p> <p>Such profiles are protected using standard operating system permissions models, and so would not typically be accessible to another user account on the machine.</p> <p>In the event that another user or a thief has unrestricted access to the machine, then of course they may be able to read those files. But the most sensitive parts of the Chrome profile - like passwords and credit card details - are encrypted using Microsoft's Data Protection API (DPAPI). This is specifically designed to prevent data being accessible to admins or others with full disk access. It makes use of the users' login password to encrypt the data. (For full details see Microsoft DPAPI documentation. It may be possible for admins to decrypt this data so long as they have access to private keys held on a domain controller).</p> <p>So the only circumstances under which special steps would be required here is if you are concerned about:</p> <ul style="list-style-type: none">• Admin users or those who've got physical disk access;• Accessing data such as browser cache or other parts of the Chrome profile which are not encrypted. <p>Please see the next line if you are concerned.</p>

Enterprise need	User impact	Potential adverse security impact	Options and notes
<p>I'm worried that admin users who sign in to the same machine (either later, or at the same time using VDI) might be able to access sensitive data such as the browser cache belonging to other users that are on the machine's disk.</p>	<p>High</p>	<p>None</p>	<p>This is a very specific case and most enterprises do not take special measures to protect against this.</p> <p>Please note that the most sensitive data such as passwords and credit card numbers are not subject to this type of access - see the previous row for details.</p> <p>If you are still concerned about admin access to less sensitive parts of the profile such as the browser cache, use the policy: <code>ForceEphemeralProfiles</code> combined with forcing the user to sign into Chrome (<code>ForceBrowserSignIn</code>) such that their important bookmarks and other preferences are downloaded each time. You may also wish to set <code>BackgroundModeEnabled</code> to off, such that each session is of constrained length.</p> <p>The user impact is high due to the need to sign into Chrome each time they use it. There will, of course, also be some performance degradation as the profile information is downloaded each time and the cache is built up. Learn more about Ephemeral mode.</p> <p>Please contact your Chrome enterprise specialist for additional information.</p> <p>Some enterprise customers choose instead to change <code>DefaultCookiesSetting</code> such that no cookies are persisted. We recommend against that because it is very disruptive to normal operation of the internet. It may also have a serious security penalty by requiring users to enter passwords much more frequently, increasing the risk of phishing.</p> <p>A malicious admin or anyone with physical access to the computer may be able to install keyloggers or other spyware or even install a malicious fake Chrome binary. This answer relates specifically to their access to the on-disk profile data, and cannot be an exhaustive solution to the problems of a malicious admin. A broader solution beyond Chrome would be encrypted user home directories.</p>

Enterprise need	User impact	Potential adverse security impact	Options and notes
I'm worried that physical access to an unlocked machine could allow someone to view other users' passwords	High	High	<p>Some enterprises choose to disable Chrome password management facilities by turning off the policy <code>PasswordManagerEnabled</code>.</p> <p>Our advice is to keep the password manager enabled. By doing so, you make it easy for your users to use strong passwords across multiple websites, and that's one of the most important things you can do for user security.</p> <p>See Settings for data flowing to Google for more information on password management options.</p> <p>We instead recommend setting operating system screen lock policies and ensuring you have strong operating system passwords.</p>

Settings relating to data flowing to the internet (data-loss)

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to prevent uploads.	N/A	N/A	<p>At present, Chrome does not offer any policy options to prevent uploading files.</p> <p>Note in particular that the policy <code>AllowFileSelectionDialogs</code> does not achieve this goal, since uploads can still happen by drag-and-drop or other mechanisms.</p>
I want to monitor what users are doing to detect suspicious behavior.	None	None	You can monitor the resource consumption of the Chrome Browser, signed-in status, connectivity, usage patterns, and browsing behavior. See Track Chrome Browser usage on Windows .
I want to ensure confidential data can't be displayed except on the main computer screen, so I want to disable Chrome Cast.	Medium	None	Adjust the <code>EnableMediaRouter</code> policy.
I want to disable the ability for websites to capture video or audio (for example via WebRTC).	Medium	None	<p><code>VideoCaptureAllowed</code> and <code>AudioCaptureAllowed</code> can be used to turn off the ability to capture video and audio, along with corresponding 'AllowedUrls' policies which can provide a whitelist..</p> <p>Enterprises may hear advice suggesting to "disable WebRTC". There is no way to disable the WebRTC stack overall, because it is better to disable the specific sensors which are deemed a risk in your enterprise.</p> <p>We expect more videoconferencing and telephony tools to move to the web, so you should expect this to have an increasing impact on your users as time goes by. Perhaps revisit these decisions in a year.</p>
I want to disable the ability for websites to capture the screen image.	Medium	None	Current versions of Chrome do not provide APIs for screen-sharing without use of an extension. It is expected that such APIs will be made available to websites in the future, but they will be policed using the <code>VideoCaptureAllowed</code> policy referenced in the previous recommendation. Please contact your Chrome enterprise specialist for the most up-to-date information.

Enterprise need	User impact	Potential adverse security impact	Options and notes
#I want to disable malicious websites from asking for read access to access to serial ports, even if it stops legitimate websites from accessing it.	Medium	None	<p><code>DefaultSerialGuardSetting</code> can be used to control use of the File System API for reading. Setting the policy to 3 lets websites ask for read access to files and directories in the host operating system's file system via the File System API. Setting the policy to 2 denies access.</p> <p>Leaving it unset lets websites ask for access, but users can change this setting.</p>
#I want to disable malicious websites from asking for read access to files and directories in the host operating system's file system via the File System API, even if it stops legitimate websites from accessing it.	Medium	None	<p><code>DefaultFileSystemReadGuardSetting</code> can be used to control use of the File System API for reading. Setting the policy to 3 lets websites ask for read access to files and directories in the host operating system's file system via the File System API. Setting the policy to 2 denies access.</p> <p>Leaving it unset lets websites ask for access, but users can change this setting.</p>
#I want to disable malicious websites from asking for access and use sensors such as motion and light, even if it stops legitimate websites from accessing it.	Medium	None	<p><code>DefaultSensorsSetting</code> can be used to control use of the default sensors setting. Setting the policy to 1 lets websites access and use sensors such as motion and light. Setting the policy to 2 denies access to sensors.</p> <p>Leaving it unset means <code>AllowSensors</code> applies, but users can change this setting.</p>
I want to disable malicious website access to USB or Bluetooth devices even if it also stops legitimate websites accessing it.	Medium	Medium	<p><code>DefaultWebUsbGuardSetting</code> <code>DefaultWebBluetoothGuardSetting</code></p> <p>It's possible that some websites may require legitimate USB or Bluetooth access to hardware tokens for multi-factor authentication. By disabling USB or Bluetooth, you may negatively impact security for such websites.</p>
I want to disable malicious website access to location information even if it also stops legitimate websites accessing location.	High	Low	<p>Disable location access using: <code>DefaultGeolocationSetting</code></p> <p>This is regarded as very disruptive to user experience. It's conceivable that certain websites could also rely on location evidence to aid security, so this could have negative security implications.</p>
I want to prevent third-party sites tracking our users around the web.	High	Low	<p>Some enterprises disable third-party cookies using <code>BlockThirdPartyCookies</code>. This can break some websites, which may include certain authentication web services, so there is a chance that this could negatively affect security.</p>

Indicates a new field since Chrome 75

Settings relating to data flowing to Google

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to prevent Chrome from leaking information to Google's DNS servers.	N/A	N/A	There is a misconception that the policy option <code>BuiltInDnsClientEnabled</code> should be disabled to prevent Chrome using Google's DNS servers. This is incorrect - this option relates solely to the client-side DNS software stack on the endpoint and does not affect which servers are used. Under no circumstances will the Google DNS stack talk to Google servers unless the endpoint is configured that way in the first place. There is no privacy reason for enterprises to change this option.
I want to prevent confidential information about crashes and usage being sent to Google.	Low	None	You can disable anonymous crash reporting with the policy <code>MetricsReportingEnabled</code> . These metrics are anonymous. By allowing metrics reporting, your enterprise will benefit from Google better understanding your needs and any stability problems.
I want to stop confidential documents flowing via Google to cloud printers.	Medium	None	Adjust the policy <code>CloudPrintSubmitEnabled</code> . For more information, see Who can see what I'm printing?

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to stop the text of notifications flowing via Google services.	Medium	None	Some enterprises choose to turn off notifications using the <code>DefaultNotificationsSetting</code> policy on the basis that the notification text then does not need to flow via Google back-end services. For more info, see Push messaging .
I don't want Google to know our passwords.	Medium	Medium	<p>Google strongly recommends retaining password management functions for your users. It enables users to use strong passwords which can greatly benefit your overall security. For example, read the NCSC's post on password managers.</p> <p>If Chrome Browser sync is disabled, such passwords are not uploaded to Google. They are stored on the endpoint only, and encrypted using the users' login password such that even those with physical access to the disk cannot read them. (See earlier answers about PII on the endpoint.)</p> <p>If Chrome Browser sync is enabled, by default these passwords are stored in Google infrastructure. Google takes the safeguarding of such information extremely seriously, but Google may need to share it, for example, for legal reasons.</p> <p>Please see the next item for information on how you can ensure that Google simply cannot access this data.</p> <p>More generally, Google wants enterprise users to get the best security using a password manager. If there are further features or controls which would reassure you such that you would enable the password manager, please discuss with your Google Chrome enterprise specialist.</p> <p>Some enterprises choose to disable the option to import passwords from other browsers (<code>ImportSavedPasswords</code>). As with password managers in general, we think it's important to make it as easy as possible for users to use strong passwords, so we would advocate retaining this import ability.</p>
I don't want Google to find out any of the user's profile data, including passphrases and bookmarks.	Medium	Medium	<p>Your users can set a sync passphrase which encrypts their profile (passwords, bookmarks etc.) such that they are never uploaded in plaintext. Learn more.</p> <p>With a passphrase, your users can use Google's cloud to store and sync their Chrome data without letting Google read it.</p> <p>This setting does require the user to enter the passphrase on new devices, and has impacts on what history is synced, so it is disruptive to their workflows.</p> <p>At present, Chrome does not offer policy controls to enforce such a passphrase. If you have additional questions, please discuss with your Chrome Enterprise specialist.</p>

Enterprise need	User impact	Potential adverse security impact	Options and notes
I don't want to send any data to Google for compliance.	High	High	<p>Google's Safe Browsing is crucial for online safety. It provides superior protection against malware and phishing, leveraging contextual information for enhanced accuracy.</p> <p>For stronger security, we recommend keeping Safe Browsing active and utilizing Chrome's password manager. To increase privacy, disable syncing of bookmarks, history, and passwords with Google.</p> <p>Each Chrome service can be evaluated for its data exchange and security benefits. Services like Google Translate, triggered by user action, are generally accepted.</p> <p>Enhanced Safe Browsing provides real-time protection, deeper file scans, and tailored defenses against evolving threats across Chrome and other Google products.</p> <p>Our Chrome enterprise specialists can help you customize policies to meet your specific security and privacy needs. Click to learn more about Chrome's Security and privacy policies.</p>

User Journeys

As administrators, you're tasked with enabling a productive and secure digital environment. Chrome browser policies provide the tools to shape user journeys, striking the right balance between access and protection. By strategically managing these policies, you can empower users while mitigating online threats and ensuring a safe browsing experience.

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to prevent users from accidentally using plaintext HTTP instead of HTTPS.	N/A	N/A	<p>Setting <code>HTTPSOnlyMode</code> to <code>force_enabled</code> will require users to click through an interstitial before using plaintext HTTP. Click Throughs are remembered for sites that are repeatedly visited, and so users should see a small number of warnings.</p> <p>You can allowlist sites that are known to be HTTP, e.g. company intranet, to be accessed without an interstitial using the <code>HttpAllowlist</code> policy.</p>
I want to reduce my organization's exposure to zero-day vulnerabilities by disabling the attack surface in Chrome.	N/A	N/A	<p>You can disable the optimizing just-in-time (JIT) compilers in the V8 Javascript engine, which are a common target for in-the-wild exploitation, using the <code>DefaultJavaScriptOptimizerSetting</code>. This will reduce overall performance.</p> <p>You can individually allowlist and blocklist sites using the <code>JavaScriptOptimizerAllowedForSites</code> and <code>JavaScriptOptimizerBlockedForSites</code> policies.</p>
I want to use more memory to reduce the risk that a compromised renderer can exfiltrate data from another site on Android phones.	N/A	N/A	<p>You can enable <code>SitePerProcessAndroid</code> to force full site isolation on Android phones. This is already enabled by default on desktop. This will cause Chrome to use additional memory, which may reduce the number of tabs a user can interact with at once.</p>
I want to stop users from being tricked into installing a root certificate as part of a self-MITM attack.	N/A	N/A	<p>Use <code>CACertificateManagement</code> to block access to <code>chrome://certificate-manager</code>, and either disable platform root store integration with <code>CAPlatformIntegrationEnabled</code> or use platform-specific tools to lock down user access to the relevant platform configuration surface.</p>

User Journeys

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to deploy custom server root certificates so that my employees can authenticate internal resources without certificate errors.	N/A	N/A	Use the <code>CACertificates</code> or <code>CACertificatesWithConstraints</code> policies to deploy your organizations server root certificates. Chrome will trust any site that presents a matching certificate that chains up to a root certificate deployed with either policy. You can also deploy intermediate certificates to help with path building using the <code>CAHintCertificates</code> policies.
"I perform in-network filtering which requires access to the server name during a TLS handshake. I need to disable Encrypted Client Hello so that this filtering continues to work.	N/A	N/A	We recommend switching to a DNS-based filtering or client-side content blacklist using Chrome Enterprise Premium. However, you can disabled Encrypted Client Hello (ECH) using the <code>EncryptedClientHelloEnabled</code> policy. Disabling ECH will regress privacy for all users.

Management and performance

Chrome is committed to protecting the user's privacy. Many enterprises want to minimize personally identifiable information or personal data (collectively, "PII") on PCs, and many enterprises are unaware of the extent that Chrome protects this data.

Enterprise need	User impact	Potential adverse security impact	Options and notes
I'm worried that the Chrome password manager could cause support escalations by getting out of sync with the users' real passwords.	N/A	N/A	The Chrome security team strongly recommends using a password manager to make it easy for users to use strong passwords. It is our hope to make it as seamless and easy as possible. If you have concerns, contact your Chrome enterprise specialist.
I want to ensure users don't get their Google Workspace password phished.	None	None	Enable Password Alert. See instructions at Prevent password reuse .
My organization's testing needs make it difficult to stay on top of rolling out the latest version of Chrome.	None	None	<p>Chrome has multiple release channels which can give your enterprise early access to new features, bug fixes and security improvements. We recommend that some of your team subscribe to the beta or dev channel to test new features and give you time to update your enterprise applications. This may also give you the opportunity to discuss any concerns with your Chrome enterprise specialist before a breaking change hits the stable channel.</p> <p>We strongly recommend this approach rather than trying to delay updates which may make your organization vulnerable to known exploits. It is important to note that Chrome's development is done largely in the open. Once a security fix is released to the stable channel, details of that bug will be publicly visible. Keeping your users on the latest version of Chrome is extremely important.</p>
I want to ensure there is a full audit trail in case I have to retrospectively investigate a compromise.	Low	None	Users can normally disable the saving of browsing history. You can prevent this by adjusting the policy <code>SavingBrowserHistoryDisabled</code> . You may also wish to disable Incognito Mode using <code>IncognitoModeAvailability</code> .
I want users to use our corporate approved password manager instead of the built-in Chrome password manager.	Low	Low	It is a good decision to give your users a password manager. Please disable the built-in password manager using <code>PasswordManagerEnabled</code> . Please consider applying this policy just for your corporate profile so that users can continue to use the Chrome password manager if they sign in to their personal Chrome profile.

Management and performance

Enterprise need	User impact	Potential adverse security impact	Options and notes
I want to prevent users visiting particular sites due to corporate policy.	Medium	None	This can be configured through whitelist and blacklisting policies. See Allow or block access to websites .
#I want to make Chrome behavior predictable so that behavior changes only happen on version upgrade.	Medium	None	<p>Variations provide a means for offering modifications to Google Chrome without shipping a new version of the browser by selectively enabling or disabling already existing features.</p> <p>Setting <code>ChromeVariations</code> to <code>VariationsEnabled</code> (value <code>0</code>), or leaving the policy not set allows all variations to be applied to the browser.</p> <p>We do not recommend disabling the Chrome variations framework. By doing this you can potentially prevent Google from quickly providing critical security fixes and significantly increases the risk of security and compatibility issues in your organization</p>
I want to ensure that all browser startups go through a central login page or other corporate page so that users agree to policy or see information that my organization deems important.	Medium	None	Please look into <code>RestoreOnStartupURLs</code> , <code>HomepageIsNewTabPage</code> , <code>NewTabPageLocation</code> , <code>HomepageLocation</code> .
I don't want to allow users to use incognito mode as I'm afraid it may encourage them to visit websites that may not be appropriate for a work environment.	Medium	None	Adjust the policy <code>IncognitoModeAvailability</code> .
I have endpoint software which is incompatible with Chrome's DNS stack.	Medium	Medium	Disabling the built-in DNS client will prevent Chrome from leveraging network security features such as Encrypted Client Hello (ECH) and HTTPS RR. If you wish to disable ECH, use the <code>EncryptedClientHelloEnabled</code> policy instead.

Management and performance

Enterprise need	User impact	Potential adverse security impact	Options and notes
I need to inspect internet traffic with middleboxes.	Medium	Medium	You will need to install a root certificate on each endpoint. You can do so using platform management tools, or with Chrome Cloud Management, or with the CACertificates policy.
I need to inspect Chrome user behavior using a third-party product.	Medium	None	<p>You can force third-party security extensions to be installed using <code>ExtensionInstallForcelist</code>. Be aware, of course, that this may give those extensions access to browsing history, user data and page loads.</p> <p>This is preferable to allowing third-party code to inject code into the browser processes by adjusting the policy <code>ThirdPartyBlockingEnabled</code>. It is the Chrome team's experience that allowing third party code injection can increase enterprise risk by breaking some of the mitigations built into Chrome.</p>
My organization is applying policies using Google Cloud configuration, per-user. I want to ensure that users always have these settings applied, so I want to ensure Chrome is always signed into our enterprise profile.	High	None	<p>Force users to log into Chrome Browser using a work profile. Learn more.</p> <p>This prevents users from signing in to their own Chrome profiles and therefore syncing their own bookmarks, passwords etc. You may prefer to apply settings device-wide using either Chrome Enterprise Core or Windows Group Policy.</p>

Indicates a new field since Chrome 75

Managing Chrome

As an IT admin, you can deploy Chrome to users across platforms. You can then manage hundreds of policies that govern people's use of Chrome.

[Start managing Chrome now →](#)

Chrome Enterprise Premium

With the growing reliance on web browsers to access sensitive data, robust security is paramount. While the recommendations above provide a solid foundation, Chrome Enterprise Premium elevates your protection with advanced features specifically designed for today's hybrid work environments. It bolsters Chrome's built-in security to safeguard your organization's data and users against evolving threats.

Here's a breakdown:

Key Features



Enhanced Data Loss Prevention (DLP)

Prevent sensitive data leaks with granular controls over copy/paste, downloads, and uploads. This extends to cloud apps and even restricts data sharing in Generative AI platforms.



Zero Trust Access

Secure access to corporate resources from any location or device. Context-aware access policies ensure only authorized users reach sensitive data.



Advanced Malware and Phishing Protection

Real-time threat intelligence, deeper file scans, and tailored defenses provide comprehensive protection against evolving online threats.



Simplified Management

Centralized management tools allow IT to easily deploy policies, manage updates, and gain insights into browser activity across the organization.

Managing Chrome

Benefits



Reduced risk of data breaches

Proactive security measures help prevent accidental or malicious data exfiltration.



Enhanced compliance

Meet regulatory requirements with robust security and auditing capabilities.



Improved productivity

Users can work securely from anywhere with seamless access to the tools they need.



Lower total cost of ownership

Streamlined management and reduced security incidents save time and resources.

Learn More

Chrome Enterprise Premium product page

<https://chromeenterprise.google/products/chrome-enterprise-premium/>

Introducing Chrome Enterprise Premium blog post

<https://cloud.google.com/blog/products/identity-security/introducing-chrome-enterprise-premium>

Chrome Enterprise Premium Setup Guide

<https://support.google.com/chrome/a/answer/14804659?hl=en>

If you're looking to strengthen your organization's browser security and simplify management, Chrome Enterprise Premium offers a comprehensive solution.



Additional resources

Here are more resources to help you with managing Chrome in your organization:

[Chrome Browser Deployment Guide \(Windows\)](#)

[Chrome Enterprise policy list](#)

[Chrome Enterprise release notes](#)

[Chrome Enterprise Help Center](#)

[Managing Extensions in Your Enterprise](#)

[Chrome update management strategies](#)

[Setup Chrome Enterprise Core](#)