chrome enterprise

Chrome Browser Enterprise Security Configuration Guide

Table of contents

Purpose of this guide

This document is for Windows IT administrators managing the Chrome Browser on Windows computers. It explores in detail the various security policies Chrome offers and the different implications admins need to evaluate before enabling/disabling these policies to meet their organizations' security needs.

What's covered	Recommendations and critical considerations when enabling or disabling Chrome's security policies.
Primary audience	Microsoft® Windows® and Chrome Browser administrators
IT environment	Microsoft Windows 7 and later
Takeaways	A clear understanding of the implications of enabling or disabling Chrome's security policies on enterprise security and user functionality.

Last updated: July 21, 2019 for Chrome 75

Introduction

The Chrome team takes security very seriously, and is proud of its 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 the majority of users. Sometimes, enterprises may need to make adjustments to meet specific security goals. Chrome allows you, as the administrator, to configure Chrome to meet those goals by selecting the appropriate security policy settings for your enterprise environment.

This document describes some of the instances where Chrome offers security policies you can choose to enable or disable. It is organized around three distinct enterprise security needs:

1. Threat prevention
2. Privacy
3. Management and performance

Many of the recommendations here reference particular policy settings, full documentation for which can be found at https://cloud.google.com/docs/chrome-enterprise/policies/.

This document is focused on Chrome Browser on the Windows operating system, though most of the advice applies across all desktop platforms. For each enterprise need in the tables below, we cover the user impact and potential adverse security impact.

Threat Prevention

Chrome already takes steps to safeguard organizations from malicious websites, including:

- Site Isolation, which keeps each website isolated into its own independent memory space (operating system process). For more info, see Site isolation.
- Sandboxing, which reduces the chances of the rest of the computer being affected by a vulnerability.
- Safe Browsing, which finds malicious and deceptive content/software by constantly scanning the web and classifying potential threats. Users are warned before reaching a site that has been flagged as potentially harmful.

Depending on the specific security needs of your organization, you can further configure the browser in two approaches:

- Enforcing standard default Chrome behavior, so that users can't override it.
- Changing standard default Chrome behavior to reduce attack surface, which may potentially degrade user functionality.

The following two tables discuss potential configurations in these areas.

Table Key

For the tables below, here are the definitions of the table headings.

Enterprise need: Problem the enterprise is trying to solve
User impact: Impact on the user's experience
Potential adverse security impact: Security impact to changing from Chrome's defaults.
Options and notes: Recommendations, considerations, and notes from the Chrome team

Settings that enforce existing Chrome default behavior

Chrome's default settings are designed to safeguard businesses against potential security threats However, some default settings can be changed by the user and this can have a potential adverse impact on security. Admins can enforce some of the default settings by policy, as described below.

Enterprise need	User impact	Potential adverse security impact	Options and notes

I want to ensure no previous administrators have set insecure policies within our organisation.	None	None	Ensure that the following policies are not already set, so that you get the benefit of the default configuration:
			
			`Http09OnNonDefaultPortsEnabled`
			`EnableDeprecatedWebPlatformFeatures`
			`RunAllFlashInAllowMode`
			`SuppressUnsupportedOSWarning`
			`EnableOnlineRevocationChecks`
			`WebDriverOverridesIncompatiblePolicies`
			`OverrideSecurityRestrictionsOnInsecureOrigin`
			`CertificateTransparencyEnforcementDisabledForCas`
			`CertificateTransparencyEnforcementDisabledForLegacyCas`
			
			This is not an exhaustive list of security-related policies, but these particular policies are used by many enterprises.

I want to ensure users can't turn off fundamental security features.	None	None	Explicitly set the policies `AllowOutdatedPlugins`, `SafeBrowsingEnabled` and `ThirdPartyBlockingEnabled`. There will be no user experience change except that users will be prevented from changing these settings. More detail on some of these can be found in the following rows. See the Chrome Enterprise policy list for details on each of these policies.
I want to prevent users from downloading malware and avoid phishing, and ensure that these protections cannot be overridden by the user.	Low	None	Safe Browsing is the Chrome feature which aims to protect against malware download and phishing. 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. The Chrome security team recommends you keep Safe Browsing turned on. You can prevent the user turning off Safe Browsing with the policy `SafeBrowsingEnabled`. This should have no user-visible impact except that it prevents them from turning off Safe Browsing. You can enforce Safe Browsing more aggressively by setting: `DisableSafeBrowsingProceedAnyway` This may have user impact as it prevents a user continuing with their navigation if Safe Browsing has made a mistake and misclassified a website as a phishing attempt. You may also wish to set `DownloadRestrictions` to 2 in order to enforce Safe Browsing decisions a little more strictly. For more info, see Prevent users from downloading harmful files. 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).
I'm planning to use a third-party software that requires injecting code into Chrome.	High	High	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 setting (`ThirdPartyBlockingEnabled False`). 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. 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.

Settings that reduce attack surface, but may degrade user functionality

Depending on your organization's security needs, you can alter Chrome's default settings to reduce the attack surface available to malicious websites. Many of these changes disable Chrome features, which may cause users to experience degraded functionality.

Below are considerations to help you in making these 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	Low	None	You can enable revocation checks for such certificates using: `RequireOnlineRevocationChecksForLocalAnchors` Chrome does not guarantee it can distinguish certificates based on local anchors -- this relies

to be able to revoke the certificates.			on operating system facilities which vary between platforms and operating system versions. Should the revocation be inaccessible, these certificates will not be usable (hard-fail), which could prevent websites from being accessible.
Older versions of Chrome running in my environment may be exploitable by malicious websites.	Low	None	You can force users to relaunch Chrome to take updates more rapidly using the policies `RelaunchNotification` and `RelaunchNotificationPeriod`. We strongly recommend this in an enterprise environment, as it will keep users on the latest version of Chrome with the latest security fixes.
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	You can disable these older schemes using `AuthSchemes`. Few modern legitimate websites use these schemes and disabling them in an enterprise context makes sense. As of Chrome 75 we recommend NTLM and Negotiate. Make sure that your enterprise services also use modern authentication mechanisms.
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 `CloudPrintProxyEnabled`.
I'm concerned that attackers already in the network could compromise WPAD to move laterally.	Low	None	You can use ProxyMode 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 `PromptForDownloadLocation`.
I want to disable 3D graphics because I think it increases the attack surface and few	Medium	None	You can turn this off using `Disable3DAPIs`.

websites used by our users require it.			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. Disabling WebGL will break virtual globe and mapping products.
I want to reduce the risk that side-channel attacks can be used by one website to extract data from another website.	Medium	None	You can make site isolation more fine grained with IsolateOrigins. Learn more at Protect your data with site isolation. Note: This will use more memory.
I want to eliminate the risk that Chrome Remote Desktop can allow external users to control computers in our network.	Medium	None	The Chrome Remote Desktop app can be blocked in the same way as any other app or extension. Learn more at Control use of Chrome Remote Desktop.
I want to disable Flash because it is risky.	Medium	None	Block Flash entirely using: `DefaultPluginsSetting`. Also see the Flash Roadmap.
I want to disable extensions and apps because I think they increase the potential attack surface, and I don’t mind impacting user workflows.	High	Low	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. We recommend managing extensions by permission: 1. Block installation of those extensions which use permissions that you deem risky and allowing all others 2. For the remaining extensions, block their access to sensitive hosts. 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 sensitive corporate sites. 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.

			If you can't identify a specific set of permissions which concern you, you can block particular extensions by setting `ExtensionInstallBlacklist`. A blacklist value of '*' means all extensions are blacklisted unless they are explicitly listed in the whitelist. Consider putting in place an approval process for added extensions. We do not recommend the approach of blocking/approving particular extensions because it does not scale well.

Privacy

Some of Chrome's main security features (for instance, Safe Browsing and password managers) require exchanging information with Google services. You may have concerns about how certain types of personally identifiable information (PII) are protected by Google and wish to make adjustments to address your organization's security needs. Below are considerations to help you in making those decisions. You can also discuss any concerns about Google's usage of PII with your Chrome enterprise specialist.

The enterprise needs and considerations are categorized into three categories:

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

Settings relating to PII being stored on corporate devices

Enterprise need	User impact	Potential adverse security impact	Options and notes
I'm worried that other (**non-admin**) users logged into the same machine (either later, or at the same	N/A	N/A	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".

time using VDI) might be able to access sensitive data such as passwords belonging to other users that are on the machine's disk. I'm worried that machines may be stolen and passwords may be read off the disk by thieves.			Such profiles are protected using standard operating system permissions models, and so would not typically be accessible to another user account on the machine. 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 - for example 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, and 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). So the only circumstances under which special steps would be required here is if you are concerned about: ● 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. Please see the next row if you're concerned about this.
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.	High	None	This is a very specific case and most enterprises do not take special steps to protect against this. 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. If you are still concerned about admin access to less sensitive parts of the profile such as the browser cache, use the policy: `ForceEphemeralProfiles` combined with forcing the user to sign into Chrome (`ForceBrowserSignin`) such that their important bookmarks and other preferences are downloaded each time. You may also wish to set BackgroundModeEnabled to off, such that each session is of constrained length. 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.

			Please note that, at present, ephemeral profiles are only deleted the next time the browser starts up. Please contact your Chrome enterprise specialist for additional information. Some enterprise customers choose instead to change `DefaultCookiesSetting` such that no cookies are persisted. We recommend against that because it is very disruptive to the normal operation of the internet. It may also have serious security implications by requiring users to enter passwords much more frequently, increasing the risk of phishing. 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.
I'm worried that physical access to an unlocked machine could allow someone to view other users' passwords.	High	High	Some enterprises choose to disable Chrome password management facilities by turning off the policy `PasswordManagerEnabled`. 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. See Settings relating to data flowing to Google for more information on password management options. We instead recommend setting operating system screen lock policies and ensuring you have strong operating system passwords.

Settings relating to data flowing to the internet

Your need	User impact	Potential adverse	Options and notes

		security impact	
I want to prevent uploads.	N/A	N/A	At present, Chrome does not offer any policy options to prevent uploading files. Note in particular that the policy `AllowFileSelectionDialogs` does not achieve this goal, since uploads can still happen by drag-and-drop or other mechanisms.
I want to monitor what users are doing in order to spot 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 `EnableMediaRouter` policy.
I want to disable the ability for websites to capture video or audio (for example via WebRTC).	Medium	None	`VideoCaptureAllowed` and `AudioCaptureAllowed` can be used to turn off the ability to capture video and audio, along with corresponding "AllowedUrls" policies which can provide a whitelist. 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. 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. Consider revisiting these decisions in a year.
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 VideoCaptureAllowed policy referenced in the previous recommendation. Please contact your Chrome enterprise specialist for the most up-to-date information.
I want to disable malicious website access to USB or Bluetooth devices even if	Medium	Medium	`You can disable access to USB using DefaultWebUsbGuardSetting and disable access to Bluetooth devices using DefaultWebBluetoothGuardSetting`

it also stops legitimate websites accessing it.			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.
I want to disable malicious website access to location information even if it also stops legitimate websites accessing location.	High	Low	Disable location access using: `DefaultGeolocationSetting`. Disabling location access can be very disruptive to user experience. It can also have negative security implications as certain websites could rely on location evidence to aid security.
I want to prevent third-party sites tracking our users around the web.	High	Low	Some enterprises disable third-party cookies using `BlockThirdPartyCookies`. It is possible this may have a negative impact on security as it can break some websites, which may include certain authentication web services.

Settings relating to data flowing to Google

Enterprise need	**User impact**	**Potential adverse security impact**	**Options and notes**
I want to prevent Chrome leaking information to Google's DNS servers.	N/A	N/A	There is a misconception that the policy `BuiltInDnsClientEnabled` should be disabled to prevent Chrome from 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.
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 `MetricsReportingEnabled`. These metrics are anonymous. By allowing metrics reporting, your enterprise will benefit from Google better understanding your needs and any stability problems.
I do not want Google to find out about malware on my organization's PCs.	Low	Low	`ChromeCleanupReportingEnabled` is the policy that controls reporting of information towards Google.

			There is a separate policy, `ChromeCleanupEnabled`, that controls whether Chrome scans for malware and prompts users to remove it if found. The two policies allow you to separate the decisions of whether to use Chrome's built-in malware removal service and whether to have it share detection data with Google.
I want to stop confidential documents flowing via Google to cloud printers.	Medium	None	Adjust the policy `CloudPrintSubmitEnabled`. For more information, see Who can see what I'm printing?
I want to stop the text of notifications flowing via Google services.	Medium	None	Some enterprises choose to turn off notifications using the `DefaultNotificationsSetting` policy on the basis that the notification text then does not need to flow via Google's back-end services. For more info, see Push messaging.
I don't want Google to find out our passwords.	Medium	Medium	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. If Chrome Browser sync is turned off, 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.) If Chrome Browser sync is turned on, then by default these passwords are stored in Google infrastructure. Google takes the safeguarding of such information very seriously, but Google may need to share it, for example, for legal reasons. Please see the next item for information on how you can ensure that Google simply cannot access this data. For any additional questions on Google's password management functions, please discuss with your Google Chrome enterprise specialist. Some enterprises choose to disable the option to import passwords from other browsers (`ImportSavedPasswords`). 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.
I don't want Google to find out any of the user's profile data,	Medium	Medium	Your users can set a sync passphrase which encrypts their profile (passwords, bookmarks etc.) such that they are never uploaded in plaintext. Learn more.

including passphrases and bookmarks.			With a passphrase, your users can use Google's cloud to store and sync their Chrome data without letting Google read it. 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. 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.
I don't want to send any data whatsoever to Google because of compliance.	High	High	We strongly recommend that you retain Safe Browsing to protect users from malware and phishing. Chrome's Safe Browsing has access to the context by which users reach a page, and can be used to supplement other enterprise security products. Learn more about Chrome's Security and privacy policies. In addition, you can prevent sync of bookmarks/history/passwords to Google using the `SyncDisabled` policy. However, we strongly recommend retaining password manager functionality. See the previous 2 rows in this table for the options you have there. Different enterprises make different choices here. For instance, most enterprises are happy to retain those features which are triggered by explicit user action (for example Google Translate) as well as those which offer a clear security benefit. Please reach out to your Chrome enterprise specialist to discuss in more detail the data exchanged for each different service, and identify the right policies for your case.

Management and performance

This section discusses enterprise needs for Chrome management and performance, some of which pertain to security and privacy as well as other areas.

Enterprise need	User impact	Potential adverse	Options and notes

		security impact	
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 the use of a password manager in order 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, reach out to your Chrome enterprise specialist.
I want to ensure users don't get their G Suite 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	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. We strongly recommend this approach rather than trying to delay updates which may make your organisation 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.
I'm concerned that Chrome Cleanup may have a performance impact and is redundant given our existing AV. My organization wants its own corporate AV to spot trouble and report to us, instead of Chrome.	None	Medium	Some enterprises want to disable Chrome Cleanup because of performance concerns (especially on VDI environments) or because they want malware to be detected by enterprise anti-virus software such that its alerts flow through their security information and event management (SIEM) tools and other processes. You should note that this does have a security impact. The Chrome Cleanup tool focuses on "unwanted software" (UwS) rather than viruses, so it may detect and remove different software. However, if you wish to turn this off, please adjust the `ChromeCleanupEnabled` policy. Note: If you just wish to stop Chrome Cleanup communicating its findings back to Google, there are better

			ways - see the earlier answer about “We do not want Google to find out about malware on our PCs.”
My organization’s intranet isn’t https yet, and the security warnings are scaring users.	None	Medium	You can prevent these warnings using `OverrideSecurityRestrictionsOnInsecureOrigin`. This policy will likely eventually be deprecated so move to https as soon as you can.
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 `SavingBrowserHistoryDisabled`. You may also wish to disable Incognito Mode using `IncognitoModeAvailability`.
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 `PasswordManagerEnabled`. 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.
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 ensure that all browser startups go through a central login page or other corporate page so that users agree to a policy or see information that my organization deems important.	Medium	None	Please look into `RestoreOnStartupURLs`, `HomepageIsNewTabPage`, `NewTabPageLocation`, `HomepageLocation`.
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 `IncognitoModeAvailability`.
I have endpoint software which is	Medium	Medium	Chrome has a built-in DNS stack which can be disabled using the policy `BuiltInDnsClientEnabled`. (This only affects the DNS software stack that’s used--it does not affect which

incompatible with Chrome's DNS stack.			DNS servers are used.) If you have software on your endpoint which is modifying the normal behavior of DNS APIs, you might need to switch Chrome to using the system DNS stack. This may impact the speed and responsiveness of web pages, and it may also impact security by preventing Chrome from upgrading the connection to DNS-over-TLS, or other secure protocols in the future.
I need to inspect internet traffic with middleboxes.	Medium	Medium	You will need to install a root certificate on each endpoint. Google takes significant steps to verify the safety of certificates in use on the wider internet (for instance, certificate transparency) and is unable to verify the correct usage of your corporate certificates. See the earlier answer "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, we want to be able to revoke the certificates" for partial mitigation of these risks. Google recommends against downgrading TLS versions for compatibility with earlier middleboxes. Versions of TLS prior to 1.2 have known weaknesses, and TLS 1.3 is architected to protect against a range of unknown weaknesses.
I need to inspect Chrome user behavior using a third-party product.	Medium	Medium	You can force third-party security extensions to be installed using `ExtensionInstallForcelist`. Be aware, of course, that this may give those extensions access to browsing history, user data and page loads. This is preferable to allowing third-party code to inject code into the browser processes by adjusting the policy `ThirdPartyBlockingEnabled`. 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.
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	Force users to sign in to Chrome Browser using a work profile. Learn more. 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 Browser Cloud Management or Windows Group Policy.

Managing your Chrome Browser

As an IT admin, you can deploy Chrome Browser to users across Microsoft® Windows®, Apple® Mac®, Linux and Chrome OS computers. You can then manage 200+ policies that govern people's use of Chrome.
Start managing your Chrome browser now.

Additional resources

Here are more resources to help you with managing the Chrome Browser 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