chrome enterprise

M88 Chrome Enterprise Release Notes

Each new Chrome release contains thousands of improvements. Here, you can review new features and changes that might be of interest to you and other administrators who manage Chrome Browser and device deployments.

These release notes were last updated on January 19, 2021

See the latest version of these release notes online at https://g.co/help/ChromeEnterpriseReleaseNotes

Sign up **here** for our email distribution for future releases.

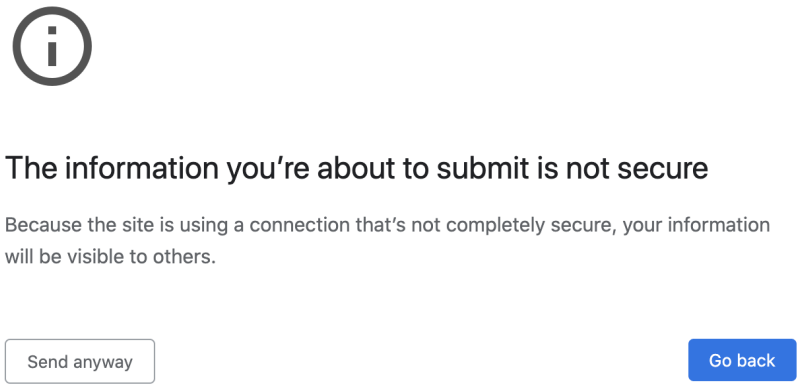
Chrome 88

Chrome Browser updates

Chrome will warn about mixed content forms

Web forms that load using HTTPS but submit their content using HTTP (unsecured) pose potential risk to user privacy. Chrome 85 and above shows a warning on such forms, letting the user know that the form is insecure. Chrome 88 will show an interstitial warning when the form is submitted, which stops any data transmission, so the user will be able to choose whether to proceed or cancel the submission. This was previously rolled out in Chrome 87 but was rolled back due to the way it interacted with redirects. It is being rolled out again in Chrome 88, but will only show warnings for forms that either submit directly to an http:// URL, or when a redirect to an http:// happens and the

form data is exposed across the redirect. For example, 307 or 308 code redirects for POST method forms.



You will be able to control this behavior using the InsecureFormsWarningsEnabled enterprise policy. To test this behavior before the rollout, use the Mixed Forms Interstitial Chrome flag.

- Improved resource consumption for background tabs
  To save on CPU load and prolong battery life, Chrome will limit the power consumption of background tabs. Specifically, Chrome will allow the timers in the background tabs to only run once per minute. Network event handlers are not affected, which allows sites like Gmail or Slack® to continue delivering timely notifications in the background. Some users saw this feature in Chrome 87. It's now available to all users in Chrome 88.

  You will be able to control this behavior using the IntensiveWakeUpThrottlingEnabled policy.

- Insecure downloads are blocked from secure pages, with changes through Chrome 88
  In Chrome 88 on Windows®, Mac®, and Linux®, downloads from insecure sources will no longer be allowed when started from secure pages. This change has been rolled out gradually, with different file types affected in different releases:

<table>
<tr><th></th><th>Chrome 81 and 83</th><th>Chrome 84</th><th>Chrome 85</th><th>Chrome 86</th><th>Chrome 87</th><th>Chrome 88 and later</th></tr>
<tr><td>Executables
(e.g. .exe, .apk, etc.)</td><td rowspan="4">Console warning</td><td>Warn</td><td colspan="4">Block</td></tr>
<tr><td>Archives
(e.g. .zip, .iso, etc.)</td><td rowspan="3">Console warning</td><td>Warn</td><td colspan="3">Block</td></tr>
<tr><td>All other non-safe types
(e.g. .pdf, .docx, etc.)</td><td rowspan="2">Console warning</td><td>Warn</td><td colspan="2">Block</td></tr>
<tr><td>Images, audio, video, text
(e.g. .png, .mp3, etc.)</td><td>Console warning</td><td>Warn</td><td>Block</td></tr>
</table>

- Executables—Users were warned in Chrome 84, and files were blocked in Chrome 85.
- Archives—Users were warned in the Chrome developer console in Chrome 85, and files were blocked in Chrome 86.
- Other non-safe types, for example, PDFs—Users were warned in the Chrome developer console in Chrome 86, and files were blocked in Chrome 87.
- Other files—Users were warned in the Chrome developer console in Chrome 87, and files will be blocked in Chrome 88.

  Warnings on Android will lag behind desktop warnings by one release. For example, executables showed a warning starting in Chrome 85.

  The existing InsecureContentAllowedForUrls policy can be used to allow specific URLs to download insecure files. You can read more details in our blog post.

- **The new tab page allows users to complete previously started workflows**
  The Chrome new tab page will show cards to help users return to searches and workflows that were already in progress, like searching for recipes or price comparisons. Users are able to control and remove these cards.

  These cards appeared for some users in Chrome 87, and are now included in Chrome 88. You can control these cards using the NTPCardsVisible policy.

- **Chrome introduces profiles for separating users or accounts**
  Some users will be given the option to create a new Chrome profile and move their account over when they sign in to a profile where another account is already signed in. This allows different users to keep bookmarks, history, and settings separate. If a user signs in with an account that is already signed in to another profile, they're offered to switch. Some users who have multiple profiles set up will see a profile picker on startup.

You can control whether Chrome offers to create or switch profiles with the SigninInterceptionEnabled enterprise policy. In Chrome 89, you'll also be able to control the startup behavior for the profile picker with the ProfilePickerOnStartupAvailability enterprise policy.

A wider release to more users is planned for a later release

- **Certain features are available to users who have signed in without having to enable Chrome Sync**
  Some users who have signed into Chrome might be able to access and save payment methods and passwords stored in their Google Account without Chrome Sync being enabled.

  On Chrome on Android, you can control a user's access to payment methods using the AutofillCreditCardEnabled enterprise policy. You can control access to passwords on Chrome on desktop by either setting the SyncDisabled enterprise policy to disabled, or by including "passwords" in SyncTypesListDisabled.

- **DTLS 1.0 has been removed**
  DTLS 1.0, a protocol used in WebRTC for interactive audio and video, has been removed by default. Any applications that depend on DTLS 1.0 (most likely gateways to other teleconferencing systems) should update to a more recent protocol. You can test if any of your applications will be impacted by using the following command line flag when launching Chrome:

  --force-fieldtrials=WebRTC-LegacyTlsProtocols/Disabled/

  If your enterprise needs additional time to adjust, the WebRtcAllowLegacyTLSProtocols enterprise policy will be made available to temporarily extend the removal.

- **Chrome supports manifest v3**
  Chrome 88 supports extensions written in the new Manifest V3 format. Manifest V3 is a new platform that makes extensions more secure, performant, and privacy-respecting by default. There is no breaking change at this time; extensions using Manifest v2 will continue to function normally in Chrome 88.

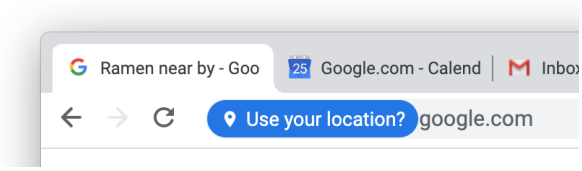
- **Chrome is launching an origin trial for detecting idle state**
  An early origin trial allows websites to request the ability to query if users are idle, allowing messaging apps to direct notifications to the best device.

- **Single words are no longer being treated as intranet locations by default**
  By default, Chrome improves user privacy and reduces load on DNS servers by avoiding DNS lookups

for single keywords entered into the address bar. This change may interfere with enterprises that use single-word domains in their intranet. For example, a user typing "helpdesk" will no longer be directed to "https://helpdesk/".
You can control the behavior of Chrome using the IntranetRedirectBehavior enterprise policy, including preserving the existing behavior (**value 3**: Allow DNS interception checks and did-you-mean "http://intranetsite/" infobars.).

- **Chrome introduces a new permission chip UI**
  Permission requests can feel disruptive and intrusive when they lack context – which often happens when prompts appear as soon as a page loads or without prior priming. This leads to a common reaction where end users dismiss the prompt in order to avoid making a decision.

  Chrome now shows a less intrusive permissions chip in the address bar. Since the prompt doesn't intrude in the content area, users who don't want to grant the permission no longer need to actively dismiss the prompt. Users who wish to grant permission can click on the chip to bring up the permission prompt.



  This change will be rolled out gradually throughout Chrome 88.

- **The Legacy Browser Support extension has been removed from the Chrome Web Store**
  Legacy Browser Support (LBS) is built into Chrome, and the old extension is no longer needed. The Chrome team unpublished LBS from the Chrome Web Store in Chrome 85, and it is disabled in Chrome 88. Legacy Browser Support will still be supported, please migrate away from the extension and towards using Chrome's built-in policies, documented here. The old policies set through the extension will no longer function, and you won't be able to force install the extension once it's been disabled.

- **Factor in scheme when determining if a request is cross-site (Schemeful Same-Site)**
  Chrome 88 modifies the definition of same-site for cookies such that requests on the same registrable domain but across schemes will be considered cross-site instead of same-site. For example, http://site.example and https://site.example will be considered cross-site to each other

which will restrict cookies using SameSite. For additional information please see the Schemeful Same-Site explainer. We recommend testing critical sites using the testing instructions.

You may revert to the previous, legacy behavior, by using the LegacySameSiteCookieBehaviorEnabledForDomainList and LegacySameSiteCookieBehaviorEnabled policies. These policies will be available at least until Chrome 93, with the domain list planned to be available longer. For more details, including availability, please see Cookie Legacy SameSite Policies.

- **Chrome 88 on Mac does not support OS X 10.10 (Yosemite)**
  Chrome 88 does not support OS X 10.10 (OS X Yosemite). Chrome on Mac requires OS X 10.11 or later.

- **Popup on page unload policy is no longer supported on Chrome 88**
  The AllowPopupsDuringPageUnload enterprise policies have been removed in Chrome 88, as previously communicated. For any apps that rely on the legacy web platform behavior, be sure to update them immediately.

- **Chrome treats an empty string as an unset policy on Android for some policies in Chrome 88**
  To integrate better with mobile management UEMs, Chrome on Android will not set list or dictionary policies from empty strings.

- **The BasicAuthOverHttpEnabled policy allows you to disable authentication over HTTP**
  You can set the new BasicAuthOverHttpEnabled policy to disabled to disallow non-secure HTTP requests from using the Basic authentication scheme. If you do, only secure HTTPS will be allowed.

- **The Chrome Cleanup Tool can reset Chrome shortcuts**
  When users run the Chrome Cleanup Tool, it will modify command line flags within Chrome shortcuts. This helps users restore Chrome to a safe state if malware has inserted malicious command line flags into the shortcut.

  You can control the Chrome Cleanup Tool using the ChromeCleanupEnabled policy, which will prevent this behavior.

- **Notifications will be suspended while presenting**
  While Chrome is sharing a screen, web-notifications from Chrome will not show their content by default. They will be presented to the user after the screen sharing session ends or by manually revealing them via a notification action. Note that sharing a single window or tab does not affect the

delivery of notifications from Chrome.

- **The microphone is visible beside the address bar for some users on Android**
  The microphone button is visible in the top UI bar of Chrome for some users on Android. Users can to ask the Google Assistant to read the current page, or translate it to another language.

  When users interact with the microphone button, the URL of the current page is shared with Google. You can control this feature using the AudioCaptureAllowed policy.

- **Cloud Print is no longer supported**
  The Google Cloud Print service is no longer supported on any Operating Systems.

  Chrome OS admins can select a print solution provider or migrate to the Chrome OS local and network printer solution. Admins of Windows®, Mac®, and Linux® operating systems can use the respective OS print workflow or engage with a print solution provider. Learn more about Cloud Print migration.

- **Save to Drive is no longer supported**
  Saving to Google Drive is no longer available from the Chrome print dialog on Mac®, Windows®, Linux® devices. Users can instead install the Save to Drive Chrome extension which has been updated to include this feature or print locally to PDF then upload the file to Google Drive through drive.google.com and select New > File upload. You can also set up automatic syncing between local files and Google Drive with Backup and Sync or Drive File Stream. More details on printing from Chrome are available here.

Chrome OS updates

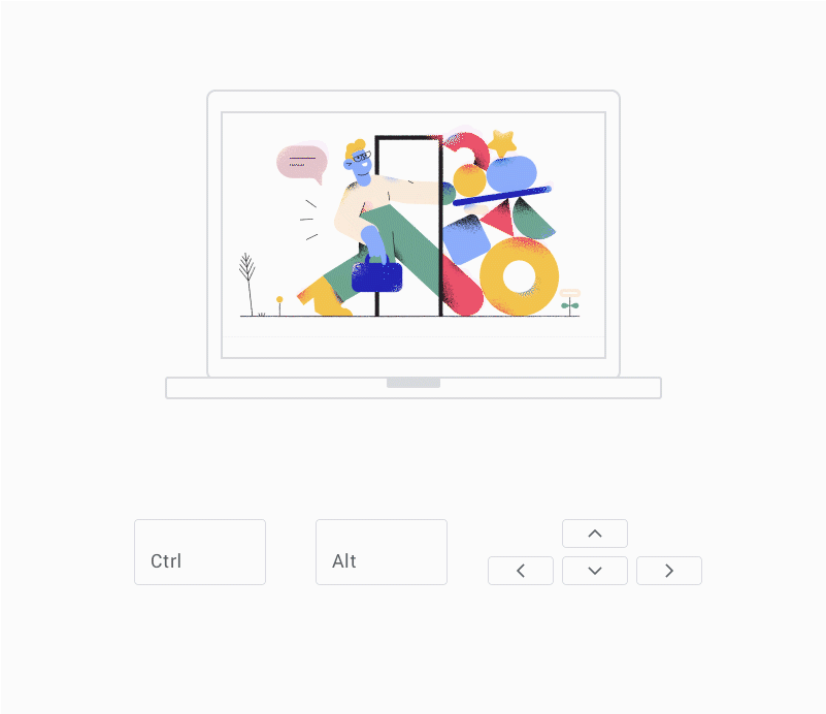
- **Enable Google Docs, Slides, Sheets files on Drive**
  Make files in your Google Drive available for offline access directly from the Files app.

- **WebAuthn using Fingerprint & PIN**
  Tired of typing long passwords? Chrome OS now lets you sign in to supported websites without having to type your passwords for that website, if you have set up a PIN or fingerprint on your Chromebook. This feature, called Web Authentication, makes use of established protocols to make authentication into website simpler and more secure. Your Chromebook PIN/fingerprint are never shared with the websites requesting verification from your Chromebook and you don't have to worry about malicious attackers phishing for your passwords to websites. If your organization has U2F

enabled, the Webauthn feature will not work; U2F will be supported in a future release.

- **Autocorrect UI improvements**
  For users with autocorrect enabled, we have improved the user interface with visual indications that autocorrects have happened, as well as new ways to undo them.

- **Magnifier Focus Following and Keyboard Support**
  Chrome OS Magnifier can now be panned using the keyboard. Use Ctrl + Alt and the arrow key to pan the viewport.



- **Text app Screen Reader mode**
  Text app now has a screen reader mode to support Chromevox users.

- **Improved switching between virtual desks**
  Switching between virtual desks with the keyboard and touchpad is now faster and more responsive. You can double or triple tap the <Search> + [or <Search> +] shortcut to move between multiple desks.

- **Reverse Scrolling + Touchpad gesture consistency**
  Touchpad gestures are now more consistent with your preference for Reverse Scrolling.

- **Chrome OS Camera now saves to a new location**

  Photos and videos captured with the Chrome OS Camera app will now get saved to a new Camera folder under My files. Any previously captured photos/videos will remain in your Downloads folder.

Admin Console updates

- **API for remote commands**
  The Admin SDK Directory API now supports issuing remote commands to devices, including wipe users, remote powerwash, remote reboot (kiosk only), screenshot (kiosk only), and set volume (kiosk only). See the developer documentation for details.

- **Filter Chrome devices by version**
  The Chrome device list now supports filtering by Chrome version. Now you can quickly check which devices are up to date or out of date.

- **Bookmark Management improvements**
  Admin Console has a new and improved bookmarks manager. Enterprise admins can more easily create, delete, and move around hundreds or even thousands of bookmarks. Details on the feature are described in the help center article.

- **New summary report for Chrome versions**
  Admin Console has a new version report that shows the number of managed browsers and devices on each Chrome version. Details on the feature are described in the help center article.

- **Group-based policy for printer management**
  Group-based management is now available for printers. From the printers page, select a group, and then configure which printers are available to users in that group.

- **Kerberos credential manager**
  As an admin, you can now enable Kerberos tickets on Chrome devices to enable single sign-on (SSO) for internal resources that support Kerberos authentication. Internal resources might include websites, file shares, certificates, and so on. Details on the feature are described in the help center article.

Additional policies in the Admin console

Many new policies are available in the Admin console, including:

Policy Name	Pages	Category / Field
AbusiveExperienceInterventionEnforce	User & Browser Settings; Managed Guest Session Settings	Chrome Safe Browsing / Abusive Experience Intervention

AccessibilityImageLabelsEnabled	User & Browser Settings; Managed Guest Session Settings	Accessibility / Image descriptions
AdsSettingForIntrusiveAdsSites	User & Browser Settings; Managed Guest Session Settings	Chrome Safe Browsing / Sites with intrusive ads
AdvancedProtectionAllowed	User & Browser Settings	Security / Advanced Protection program
AuthAndroidNegotiateAccountType	User & Browser Settings	Network / Account type for HTTP Negotiate authentication / Account type
AutoOpenAllowedForURLs	User & Browser Settings; Managed Guest Session Settings	Content / Auto open downloaded files / Auto open URLs
AutoOpenFileTypes	User & Browser Settings; Managed Guest Session Settings	Content / Auto open downloaded files / Auto open files types
BackForwardCacheEnabled	User & Browser Settings	Content / Back-forward cache
BrowserNetworkTimeQueriesEnabled	User & Browser Settings	Other settings / Google time service
CACertificateManagementAllowed	User & Browser Settings	Security / User management of installed CA certificates
ClientCertificateManagementAllowed	User & Browser Settings	Security / User management of installed client certificates.
CommandLineFlagSecurityWarningsEnabled	User & Browser Settings	Security / Command-line flags
ContextualSearchEnabled	User & Browser Settings	User experience / Touch to search
DefaultFileSystemReadGuardSetting	User & Browser Settings; Managed Guest Session Settings	Hardware / File system read access

DefaultFileSystemWriteGuardSetting	User & Browser Settings; Managed Guest Session Settings	Hardware / File system write access
DefaultSerialGuardSetting	User & Browser Settings; Managed Guest Session Settings	Hardware / Serial Port API / Control use of the Serial Port API
DefaultWebUsbGuardSetting	User & Browser Settings; Managed Guest Session Settings	Hardware / WebUSB API / Can web sites ask for access to connected USB devices
DeviceAllowRedeemChromeOsRegistrationOffers	Device Settings	Other settings / Redeem offers through Chrome OS registration
DeviceQuirksDownloadEnabled	Device Settings	Other settings / Hardware profiles
DeviceShowLowDiskSpaceNotification	Device Settings	Other settings / Low disk space notification
DeviceWebBasedAttestationAllowedUrls	Device Settings	Sign-in settings / Single sign-on verified access / Whitelist of IdP redirect URLs
DNSInterceptionChecksEnabled	User & Browser Settings; Managed Guest Session Settings	Network / DNS interception checks enabled
ExtensionCacheSize	Device Settings	Other settings / Apps and extensions cache size / Cache size in bytes
ExternalProtocolDialogShowAlwaysOpenCheckbox	User & Browser Settings	Content / Show "Always open" checkbox in external protocol dialog
FileSystemReadAskForUrls	User & Browser Settings; Managed Guest Session Settings	Hardware / File system read access / Allow file system read access on these sites
FileSystemReadBlockedForUrls	User & Browser Settings; Managed Guest Session Settings	Hardware / File system read access / Block read access on these sites

FileSystemWriteAskForUrls	User & Browser Settings; Managed Guest Session Settings	Hardware / File system write access / Allow write access to files and directories on these sites
FileSystemWriteBlockedForUrls	User & Browser Settings; Managed Guest Session Settings	Hardware / File system write access / Block write access to files and directories on these sites
GloballyScopeHTTPAuthCacheEnabled	User & Browser Settings; Managed Guest Session Settings	Network / Globally scoped HTTP authentication cache
GSSAPILibraryName	User & Browser Settings	Network / GSSAPI library name / Library name or full path
HSTSPolicyBypassList	User & Browser Settings; Managed Guest Session Settings	Network / HSTS policy bypass list / List of hostnames that will bypass the HSTS policy check
InsecureFormsWarningsEnabled	User & Browser Settings; Managed Guest Session Settings	Content / Insecure forms
KerberosAccounts	User & Browser Settings	Kerberos / Kerberos tickets
KerberosEnabled	User & Browser Settings	Kerberos / Kerberos tickets
LookalikeWarningAllowlistDomains	User & Browser Settings; Managed Guest Session Settings	Chrome Safe Browsing / Suppress lookalike domain warnings on domains / Allowlisted Domains
MaxConnectionsPerProxy	User & Browser Settings	Network / Max connections per proxy / Maximum number of concurrent connections to the proxy server
MaxInvalidationFetchDelay	User & Browser Settings; Managed Guest Session Settings	Other settings / Policy fetch delay / Maximum fetch delay after a policy invalidation

NativeMessagingAllowlist	User & Browser Settings	User experience / Native Messaging allowed hosts / Native Messaging hosts not subject to the blocklist
NativeMessagingBlocklist	User & Browser Settings	User experience / Native Messaging blocked hosts / Prohibited Native Messaging hosts
NativeMessagingUserLevelHosts	User & Browser Settings	User experience / Native Messaging user-level hosts
NtlmV2Enabled	User & Browser Settings	Network / NTLMv2 authentication
OverrideSecurityRestrictionsOnInsecureOrigin	User & Browser Settings; Managed Guest Session Settings	Security / Override insecure origin restrictions / Origin or hostname patterns to ignore insecure origins security restrictions
PaymentMethodQueryEnabled	User & Browser Settings; Managed Guest Session Settings	User experience / Payment methods
PrinterTypeDenyList	User & Browser Settings; Managed Guest Session Settings	Printing / Blocked printer types
PrintRasterizationMode	User & Browser Settings	Printing / Print rasterization mode
RequireOnlineRevocationChecksForLocalAnchors	User & Browser Settings; Managed Guest Session Settings	Network / Require online OCSP/CRL checks for local trust anchors
SafeBrowsingForTrustedSourcesEnabled	User & Browser Settings	Chrome Safe Browsing / Safe Browsing for trusted sources
ShowAppsShortcutInBookmarkBar	User & Browser Settings	User experience / Apps shortcut in the bookmark bar
SignedHTTPExchangeEnabled	User & Browser Settings; Managed Guest Session Settings	Network / Signed HTTP Exchange (SXG) support

SpellcheckEnabled	User & Browser Settings; Managed Guest Session Settings	User experience / Spell check
SuppressUnsupportedOSWarning	User & Browser Settings; Managed Guest Session Settings	Security / Unsupported system warning
UserFeedbackAllowed	User & Browser Settings; Managed Guest Session Settings	User experience / Allow user feedback
WebRtcLocalIpsAllowedUrls	User & Browser Settings	Network / WebRTC ICE candidate URLs for local IPs / URLs for which local IPs are exposed in WebRTC ICE candidates.
WebUsbAskForUrls	User & Browser Settings; Managed Guest Session Settings	Hardware / WebUSB API / Allow these sites to ask for USB access
WebUsbBlockedForUrls	User & Browser Settings; Managed Guest Session Settings	Hardware / WebUSB API / Block these sites from asking for USB access
WPADQuickCheckEnabled	User & Browser Settings; Managed Guest Session Settings	Network / WPAD optimization

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
BasicAuthOverHttpEnabled	Non-secure HTTP connections are not permitted to use Basic authentication; HTTPS is required
NTPCardsVisible	Show cards on the New Tab Page
ProfilePickerOnStartupAvailability *Browser only*	Specifies whether the profile picker is enabled, disabled or forced at the browser startup
SigninInterceptionEnabled *Browser only*	This settings enables or disables signin interception

TargetBlankImpliesNoOpener	Do not set window.opener for links targeting _blank

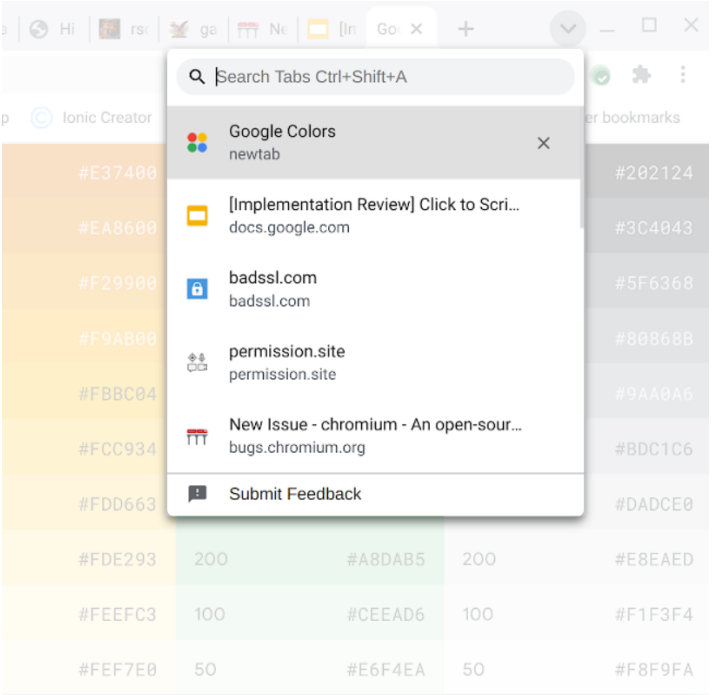
Coming soon

Note: The items listed below are experimental or planned updates. They might be changed, delayed, or canceled before launching to the Stable channel.

Upcoming Chrome Browser changes

- **Facilitated version pinning for self-hosted extensions & apps in Chrome 89**
  To increase the stability in high-reliability environments, Chrome 89 facilitates the pinning of extensions and apps to a specific version. Administrators will be able to self-host the extension or app of their choice, and instruct Chrome to use the update URL from the extension forcelist instead of the extension manifest. This will be via a new boolean parameter in ExtensionSettings policy. As a result, extensions & apps will not be updated via the updateURL that was originally configured in their manifest, and will stay on one specific version.

- **Users will be able to search open tabs in Chrome 89**
  Users will be able to search for open tabs across windows, as shown in this screenshot:

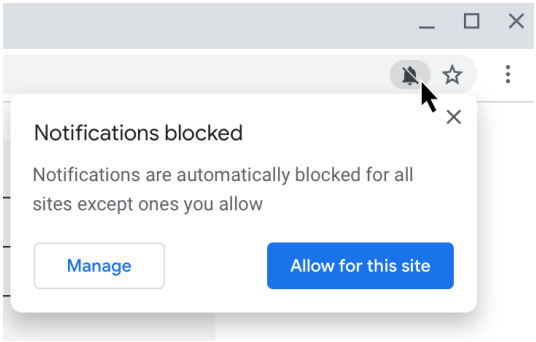


- **Chrome 89 will introduce privacy-preserving APIs to replace some of the functionality of third-party cookies**
  An interest-based targeting API will be introduced as an origin trial. This API allows working with cohorts—groups of users with similar interests. Users cannot be individually identified.

  An event-level conversion API will continue in origin-trial stage for Chrome 89 This API enables the correlation of an ad click on a website with a subsequent conversion on an advertiser site, such as a sale, a sign-up, and so on. Users cannot be individually identified.

  See the chromium privacy sandbox page for details on these APIs and the privacy sandbox.

- **Some permission requests will be less intrusive in Chrome 89**
  Permission requests that the user is unlikely to allow will be automatically blocked. A less intrusive UI will allow the user to manage permissions for each site.



- **Chrome 89 will require SSE3 for Chrome on x86**
  Chrome 89 and above will require x86 processors with SSE3 support. This change does not impact devices with non-x86 (ARM) processors. Chrome will not install and run on x86 processors that do not support SSE3. SSE3 was introduced on Intel CPUs in 2003, and on AMD CPUs in 2005.

- **Chrome 89 will prefer https to http when not specified in the address bar**
  When a user types an address into the address bar without specifying the protocol, Chrome will attempt to navigate using https first, then fallback to http if https is not available. For example, if the user navigates to google.com, Chrome will first attempt to navigate to https://google.com, then fallback to http://google.com if required. This change is planned for Windows, Mac, Linux, and Android in Chrome 89, and in Chrome 90 for iOS.

- **Chrome 89 will introduce the Serial API**
  The Serial API provides a way for websites to read and write from a serial device through script. You can read an explainer on the Serial API here.

  You will be able to control access to the Serial API using the DefaultSerialGuardSetting policy. You can also use the SerialAskForUrls and SerialBlockedForUrls policies to control serial device access on a site-by-site basis.

- **Insecure public pages will no longer allowed to make requests to private or local URLs in Chrome 91**
  Insecure pages will no longer be able to make requests to IPs belonging to a more private address space (as defined in CORS-RFC1918). For example, http://public.page.example.com will not be able to make requests targeting IP 192.168.0.1 or IP 127.0.0.1. You will be able to control this behavior using the InsecurePrivateNetworkRequestsAllowed and InsecurePrivateNetworkRequestsAllowedForUrls enterprise policies.

- **Chrome will maintain its own default root store as early as Chrome 92**
  In order to improve user security, and provide a consistent experience across different platforms, Chrome intends to maintain its own default root store. If you are an enterprise admin managing your own certificate authority, you should not have to manage multiple root stores. We do not anticipate any changes to be required for how enterprises currently manage their fleet and trusted enterprise CAs, such as through group policy, macOS Keychain Access, or system management tools like Puppet.

- **The address bar might show the domain rather than the full URL as early as Chrome 90**
  To protect your users from some common phishing strategies, Chrome will test showing only the domain in the address bar for some users. This change makes it more difficult for malicious actors to trick users with misleading URLs. For example, **https://example.com/secure-google-sign-in/** will appear only as **example.com** to the user.

  Although this change is designed to keep your users' credentials safe, you can revert to the old behavior through the ShowFullUrlsInAddressBar policy.

  This change has been enabled for some users, with a potential full rollout in a later release.

- **The SSLVersionMin policy will not allow TLS 1.0 or TLS 1.1 in Chrome 91**
  The SSLVersionMin enterprise policy allows you to bypass Chrome's interstitial warnings for legacy versions of TLS. This will be possible until Chrome 91 (May 2021), then the policy will no longer

allow TLS 1.0 or TLS 1.1 to be set as the minimum.

We previously communicated that this would happen as early as January 2021, but the deadline has since been extended.

- **SyncXHR policy will no longer be supported on Chrome 93**
  The AllowSyncXHRInPageDismissal enterprise policy will be removed in Chrome 93. For any apps that rely on the legacy web platform behavior, be sure to update them before Chrome 93. This change was previously planned for Chrome 88, but delayed to provide more time for enterprises to update legacy applications.