chrome enterprise

M87 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 November 17, 2020

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 87

Important: Adobe will no longer update and distribute Flash Player after **December 31, 2020**. After this date, all versions of Chrome will stop supporting Flash content. **Pinning to an earlier version of Chrome (or keeping an earlier version of Chrome via any other mechanism) will not prevent this change**.

You can read more about Adobe's plans to discontinue Flash player and your options in Adobe's blog post. Adobe is working with HARMAN, their exclusive licensing/distribution partner, to provide support for Flash Player in legacy browsers.

Chrome is designed to meet the needs of Chrome Enterprise customers, including integration with legacy web content. Companies that need to use a legacy browser to run Flash content after December 31, 2020 should use a HARMAN solution with Legacy Browser Support.

With Flash removed, Chrome 88 will no longer support these policies: DefaultPluginsSetting, PluginsAllowedForUrls, PluginsBlockedForUrls, AllowOutdatedPlugins, DisabledPlugins, DisabledPluginsExceptions, EnabledPlugins.

Chrome Browser updates

Google Cloud Print will no longer be supported on after December 31, 2020

As of January 1, 2021 Google Cloud Print will no longer be supported on Chrome. You can continue to use the Windows®, Mac®, and Linux® operating system print solutions or engage with a print solution provider. Chrome OS admins can migrate to the Chrome OS local and network printer solution or select a print solution provider. Learn more about Cloud Print migration.

Saving to Google Drive will no longer be available from the print dialog after December 31, 2020

Mac®, Windows®, Linux® devices and Chrome Browser will no longer be able to save directly to Google Drive from the print dialog, beginning on January 1, 2021. Users can instead 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 has a new way of saving to Google Drive. See the Chrome OS section below for more information.

Legacy Browser Support may be affected by IE + Edge redirection

Beginning in November, Microsoft Edge may enable automatic redirection from Internet Explorer to Microsoft Edge for specific URLs. If you're using Legacy Browser Support, this may interfere with your existing setup. You can disable the redirection by setting the **Microsoft Edge** policy RedirectSitesFromInternetExplorerRedirectMode to 0.

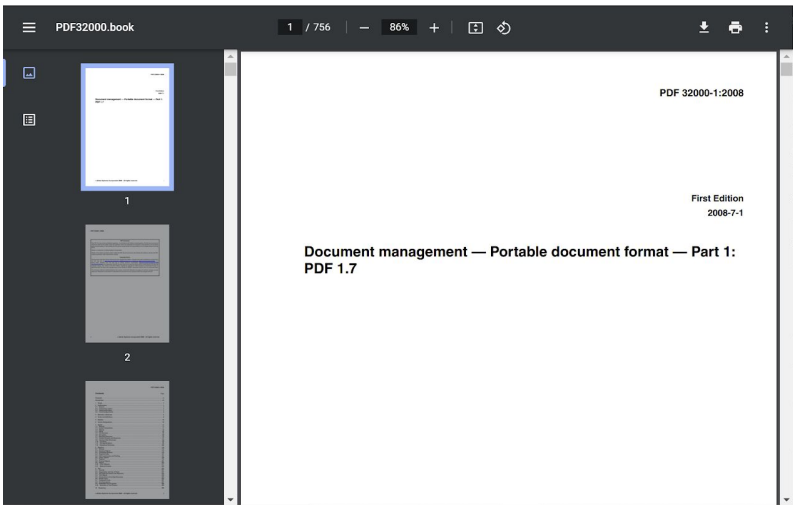
Improved resource consumption for background tabs

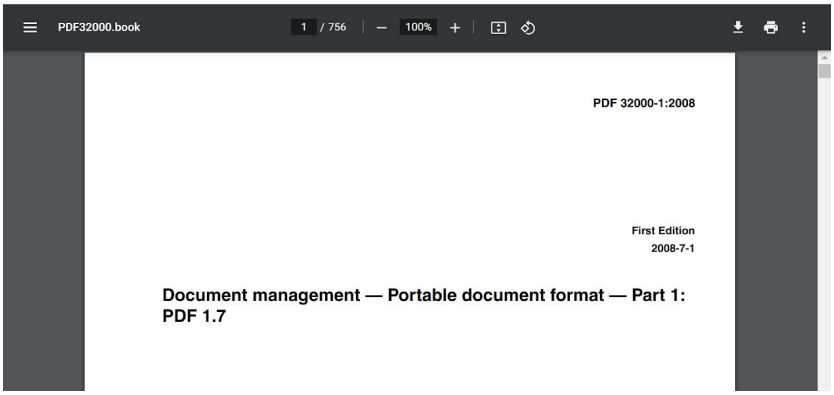
To save on CPU load and prolong battery life, Chrome limits the power consumption of background tabs. Specifically, Chrome allows the timers in the background tabs to only run once per minute. Network event handlers are not affected, which allows sites like Gmail® or Slack® to continue delivering timely notifications in the background. Some users will see this feature in Chrome 87, with a wider release planned for Chrome 88..

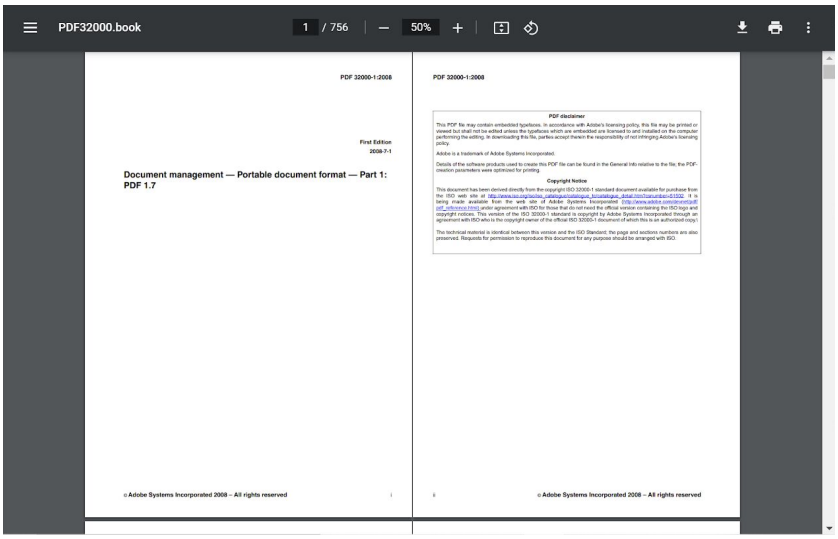
You will be able to control this behavior using the IntensiveWakeUpThrottlingEnabled policy.

Updated PDF viewer

Chrome has updated PDF viewer to include toolbar updates, table of contents, thumbnails, two-up view, and the ability to view annotations.







Users can sign into the browser when they sign into Google web services

When users sign into a Google web service while using an Android device, Chrome offers for them to sign in with the Google account already signed in on the device. Signing into Chrome doesn't turn on sync; that's a separate, optional step.

This simplifies Android sign-in, makes the feature more consistent with Chrome on desktop, and provides signed-in users access to features without sync enabled. For example, click-to-call.

You can control this feature with the BrowserSignin enterprise policy.

Certain features are available to users who have signed in without having to enable Chrome Sync

Users who have signed into Chrome may be able to access and save payment methods and passwords stored in their Google Account without Chrome Sync being enabled..

You can control users' access to payment methods on Chrome on Android 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.

Enhanced Safe Browsing

Users will be prompted to consider enabling Enhanced Safe Browsing in Chrome, which provides better protection against phishing attacks. These prompts may show up on security warning interstitials and the new tab page, but only if you are not setting either of the SafeBrowsingProtectionLevel or SafeBrowsingEnabled policies. If one of these policies is set, your users can't change the setting and will not see any prompts to do so.

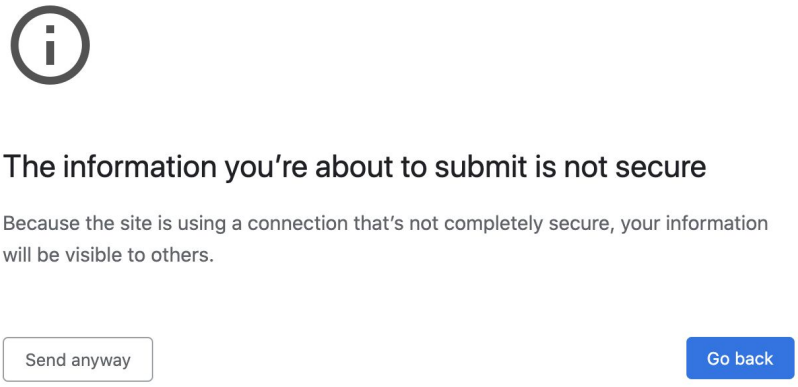
The new tab page will allow users to complete previously started workflows

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.

They appear for some users in Chrome 87, but a wider rollout, by way of policy, is planned for a later release.

Chrome warns 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 shows a warning on such forms, letting the user know that the form is insecure. Chrome 87 shows 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 planned for Chrome 86 but the rollout was delayed and is now available in Chrome 87.



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

Insecure downloads are blocked from secure pages, with changes through Chrome 88

By Chrome 88, downloads from insecure sources will no longer be allowed when started from secure pages. This change will be 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 will be blocked in Chrome 86.
- Other non-safe types (e.g. pdfs)—Users will be warned in the Chrome developer console in Chrome 86, and files will be blocked in Chrome 87.
- Other files—Users will be warned in the Chrome developer console in Chrome 87, and files will be blocked in Chrome 88.

Warnings on Android will lag behind computer 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.

Introducing more inclusive policy names

Chrome is moving to more inclusive policy names. The terms "whitelist" and "blacklist" have been replaced with "allowlist" and "blocklist". If you're already using the existing policies, they will continue to work, though you will see warnings in chrome://policy stating that they're deprecated.

The following policies have been deprecated, and equivalent policies are now available in Chrome 87 and 88. The deprecated policies will continue to work, and there is not yet any removal date planned. Future plans to remove the policies will be published in the enterprise release notes once confirmed.

Deprecated Policy Name	New Policy Name	Version
DeviceNativePrintersBlacklist	DevicePrintersBlocklist	87
DeviceNativePrintersWhitelist	DevicePrintersAllowlist	87
DeviceNativePrintersAccessMode	DevicePrintersAccessMode	87
DeviceNativePrinters	DevicePrinters	87
UsbDetachableWhitelist	UsbDetachableAllowlist	87
QuickUnlockModeWhitelist	QuickUnlockModeAllowlist	87

AttestationExtensionWhitelist	AttestationExtensionAllowlist	87
DeviceUserWhitelist	DeviceUserAllowlist	87
PrintingAPIExtensionsWhitelist	PrintingAPIExtensionsAllowlist	87
AllowNativeNotifications	AllowSystemNotifications	88

Chrome Actions will allow the user to accomplish tasks directly from the address bar

Some Chrome users will be able take actions directly from the address bar, like clearing browsing data, using a button that appears among auto-complete suggestions. A wider rollout is planned for a later release.

Chrome will support remote commands from Chrome Browser Cloud Management in the future

Admins using Chrome Browser Cloud Management will soon be able to issue remote commands to enrolled Chrome Browsers, for example remotely clearing cache and cookies. Although the functionality will come to the Admin console in the future, support for this set of features will be added in Chrome 87.

The CORB/CORS allowlist will be removed

Chrome will remove the CORB/CORS allowlist in Chrome 87. Please test Chrome extensions that your business depends on to make sure they work with the new behavior.

Please test Chrome 87.0.4266.0 or later versions of Chrome and run through critical workflows using your extension. Watch for fetches or XHRs that are initiated by content scripts and blocked by CORB or CORS. Some typical error messages are shown below:

- Cross-Origin Read Blocking (CORB) blocked cross-origin response <URL> with MIME type <type>. See https://www.chromestatus.com/feature/5629709824032768 for more details.
- Access to fetch at '**https://another-site.com**/' from origin '**https://example.com**' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource. If an opaque response serves your needs, set the request's mode to 'no-cors' to fetch the resource with CORS disabled .

If the extension's content scripts create requests that don't work when Chrome is launched with the chrome://flags listed above, then make sure you keep the extension updated so that it continues to work in Chrome 87 and above. In particular, the extensions must be updated to initiate cross-origin fetches from the extension background page (instead of from a content script).

For more details please see:
https://www.chromium.org/Home/chromium-security/extension-content-script-fetches

The Chrome Web Store displays more privacy-focused information for extension
The Chrome Web Store provides more information to users about how an extension uses their data, including authentication information, personally identifiable information, and user activity.

Developers are required to provide privacy disclosures regarding their data collection and usage. This is mandatory for every update and publishing of extensions.

Chrome OS updates

Tell us your opinion about Chrome OS - We are currently collecting feedback on your experience. If you manage Chrome OS devices in your organization please take this survey by November 25, 2020 and help us to improve our products and services..

Devices have a new way of saving to Google Drive
The Save to Drive feature, an option available to users when printing documents, has been expanded where users now have the ability to rename the file and/or save the file to a specified Google Drive folder location.

Switch Access

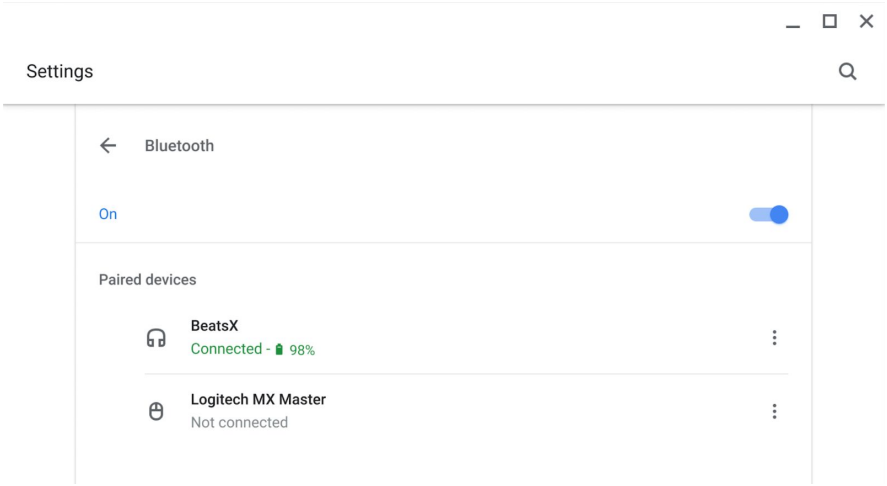
For users with motor impairments who are unable to use a traditional mouse and/or keyboard, Switch Access enables you to interact with your Chrome OS Device using one or more switches. Switch Access works by scanning the items on your screen until you make a selection. Ablenet, one of the top producers of switch devices, is now in our Works with Chromebooks program, as well.

Tab Search

Tab Search lets users search through their open tabs across all windows. This feature is currently available in Chrome 87 and will be available for Mac® and Windows® in Chrome 88.

Bluetooth battery levels

Users can now view their connected Bluetooth peripheral battery levels in Settings and Quick Settings.



Coexistence of Multiple sign-in access and policy-provided custom trust anchors for TLS

Starting in Chrome OS 87, the coexistence of Multiple sign-in access and policy-provided custom trust anchors for TLS is no longer blocked. If trust anchors are configured, they will be applied to the primary user account. As a result, users can switch faster between accounts in managed environments that require trust roots.

Language settings improvement for multilingual users

Language settings can get extremely confusing if you are bilingual or multilingual. In Chrome 87, we have updated the user experience to address the needs of multilingual users..

More interactive Alt + Tab

When using Alt+Tab to switch between windows, you can now select a window with your mouse, touch screen, or stylus.

Renaming Virtual Desks & Launcher folders

In Chrome 87, you will see visual improvements for the Virtual Desk renaming component. The visual improvements will also apply to folders in the Launcher as they use the same component.

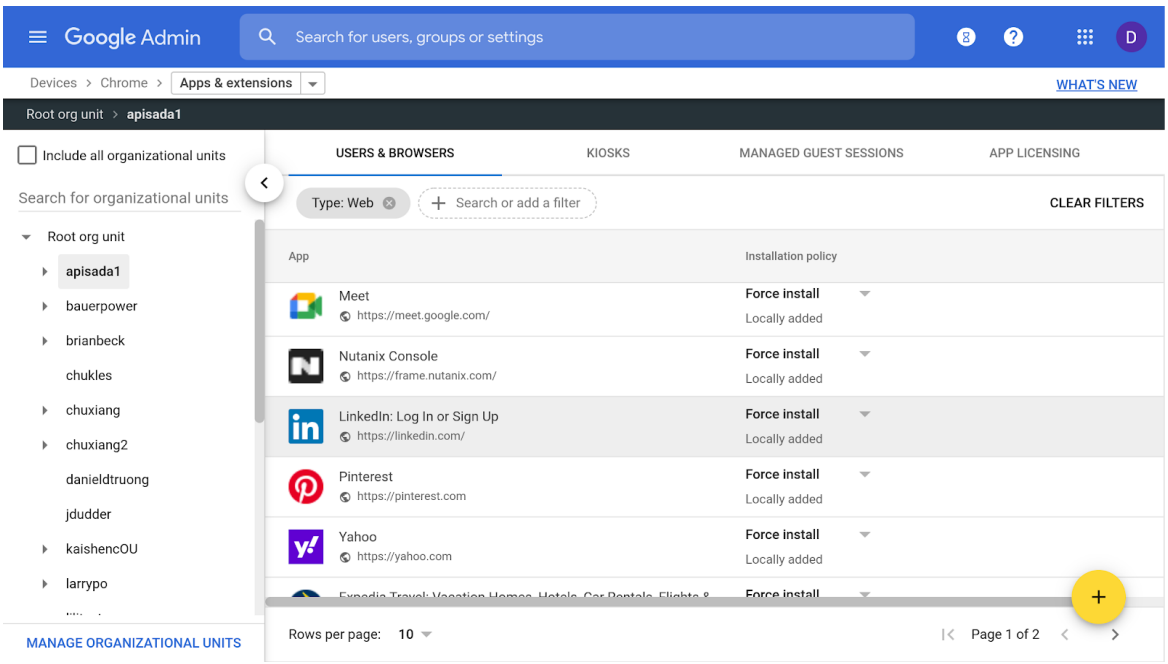
Zero-touch enrollment

Admins can configure devices to automatically enroll during the device setup process without requiring a user to invoke enterprise enrollment. More details can be found here.

Admin Console updates

WeWebsite icons and titles now display in the Admin console and Kiosk devices

In the Admin console, web apps that have been added under Apps & extensions now display the website's icon and title. In Kiosk devices, the website icons and titles are also displayed in the list of Kiosk web apps.



Restrict access to VPN (openVPN and L2TP)

Admins can now add VPN to the list of Restricted Network Interfaces in the Admin console. This prevents users from connecting to OS-supported VPN options (openVPN and L2TP). Any third-party VPNs will need to be blocked through application management policies.

Additional policies in the Admin console

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

Policy control	Admin console location	Description
Emoji suggestions	User & browser settings > User experience > Emoji suggestions	This policy enables Google Chrome to suggest emojis when users type text with their virtual or physical keyboards.
URLs in the address bar	User & browser settings > User experience > URLs in the address bar	This feature enables display of the full URL in the address bar
Audio sandbox	User & browser settings > Security > Audio sandbox	This policy controls the audio process sandbox.
Browser guest mode	User & browser settings > User experience > Browser guest mode	This policy controls guest logins
PIN auto-submit	User & browser settings > Security > PIN auto-submit	The PIN auto-submit feature changes how PINs are entered in Chrome OS. Instead of showing the same textfield that is used for password input, this feature shows a special UI that clearly shows to the user how many digits are necessary for their PIN. As a consequence, the user's PIN length will be stored outside the user encrypted data. Only supports PINs that are between 6 and 12 digits long.
Variations	Device Settings > Device update settings > Variations	Configuring this policy allows to specify which variations are allowed to be applied on an enterprise-managed Google Chrome OS device.
Single sign-on verified access	Device Settings > Device settings > Single sign-on verified access	This policy configures which URLs will be granted access to use remote attestation of device identity during the SAML flow on the sign-in screen.

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
MediaRecommendationsEnabled	Enable Media Recommendations

WebRtcAllowLegacyTLSProtocols	Allow legacy TLS/DTLS downgrade in WebRTC

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

Single words will not be treated as intranet locations by default in Chrome 88

By default, Chrome will improve user privacy and reduce 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. That is, a user typing "helpdesk" will no longer be directed to "**https://helpdesk/**".

You will be able to control the behavior of Chrome using the IntranetRedirectBehavior enterprise policy, including preserving the existing behavior (which will perform a search immediately and then ask the user if they're trying to reach the intranet site).

Chrome will introduce a new permission chip UI in Chrome 88

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 will begin showing 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.

Factor in scheme when determining if a request is cross-site (Schemeful Same-Site) in Chrome 88

Chrome 88 will modify 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. For more details, including availability, please see Cookie Legacy SameSite Policies.

Chrome 88 on Mac will not support OS X 10.10 (Yosemite)

Chrome 88 will not support OS X 10.10 (OS X Yosemite). Chrome on Mac will require OS X 10.11 or later.

Popup on page unload policy will no longer be supported on Chrome 88

The AllowPopupsDuringPageUnload enterprise policies will be removed in Chrome 88, as previously communicated. For any apps that rely on the legacy web platform behavior, be sure to update them before Chrome 88.

The Legacy Browser Support extension will be removed from the Chrome Web Store in Chrome 88

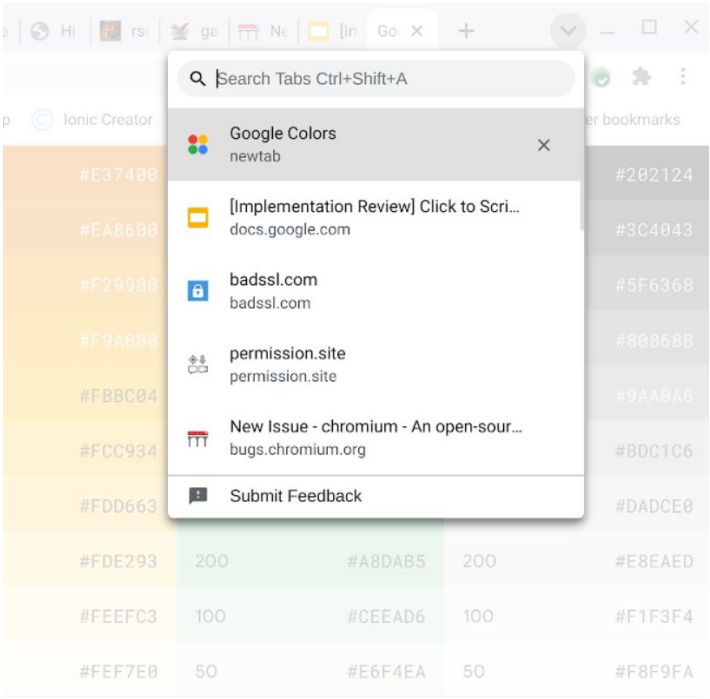
Legacy Browser Support (LBS) is built into Chrome, and the old extension is no longer needed. The Chrome team unpublished LBS from the Chrome Web Store in Chrome 85, and it will be disabled in Chrome 88. Legacy Browser Support will still be supported, please migrate away from the extension and towards 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.

Chrome will treat 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.

Users will be able to search open tabs in Chrome 88

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



The address bar will show the domain rather than the full URL in Chrome 88

To protect your users from some common phishing strategies, Chrome will show only the domain in the address bar. 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 full rollout planned for an upcoming release.

DTLS 1.0 will be removed in Chrome 88

DTLS 1.0, a protocol used in WebRTC for interactive audio and video, will be 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 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 88 will launch an origin trial for detecting idle state

An early origin trial will allow websites to request the ability to query if users are idle, allowing messaging apps to direct notifications to the best device.

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.

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 89

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.

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.

Chrome will maintain its own default root store as early as Chrome 90

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.

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.

Upcoming Admin console changes

New Version Report and Update Controls

There will be a new Version Report and Update Controls available in the Admin console. These features give increased visibility into the Chrome versions deployed in your enterprise and allows you to more granularly control how managed Chrome browsers update. If you would like to sign up to be a Trusted Tester for these features please enter your test domain and a contact email into this form.