chrome enterprise

M86 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 October 6, 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 86

Important: Adobe will no longer update and distribute Flash Player after **December 31, 2020**. Therefore, after this date, **all versions** of Chrome will stop supporting Flash content. 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.

Chrome Browser updates

Insecure downloads will be 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>

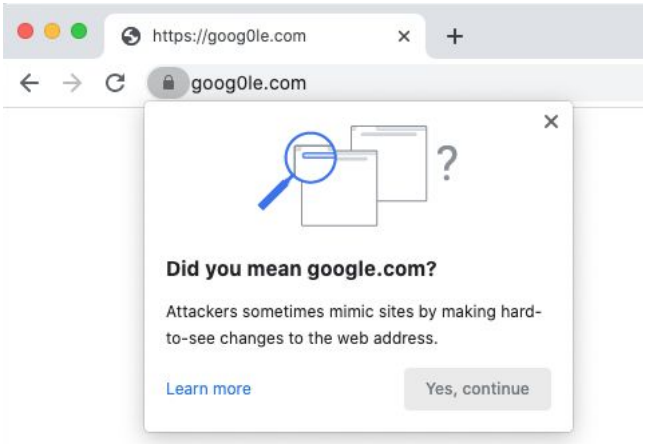
- Executables—Users were warned in Chrome 84, and files were blocked in Chrome 85.
- Archives—Users were warned in the Chrome developer console in Chrome 85, and files will be blocked in Chrome 86.
- Other non-safe types (e.g. pdfs)—Users will be warned in the Chrome developer console in Chrome 86, and 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.

New lookalikes policy and request flow

Chrome is introducing a new "Safety Tip" warning for sites with URLs that look very similar to those of other sites. This UI, as well as the existing lookalike interstitial warning, uses client-side heuristics to warn users about sites that might be spoofing other sites (For example, **goog0le.com** spoofing **google.com**).



Chrome is adding the LookalikeWarningAllowlistDomains enterprise policy to give you control of this behavior. This policy suppresses both the full-page interstitial warning and the smaller “Safety Tip” in the domains indicated.

In addition, if you think a site is triggering a warning incorrectly, you can file a request here.

Improved resource consumption when a window is not visible

To save on CPU and power consumption, Chrome detects when a window is covered by another window and will suspend work painting pixels. A previous version of this feature had incompatibility issues with some virtualization software, resulting in Chrome rendering blank white pages. Known bugs have been fixed, but if you experience any issues, you will be able to disable this feature using the NativeWindowOcclusionEnabled policy.

Some users have already seen this change since Chrome 85, however this feature is fully rolled out in Chrome 86.

User-Agent Client Hints is fully rolled out in Chrome 86

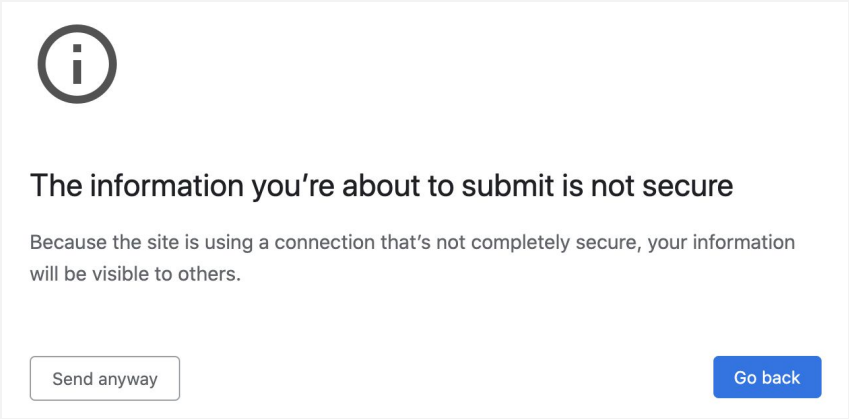
As part of an ongoing effort to reduce the ability of bad actors to track users, Chrome plans to reduce the granularity of information that is part of the user agent string and expose that information through User-Agent Client Hints. In Chrome 84, we introduced User-Agent Client Hints for some users. This is an additional change only, and should not have any negative effect when interacting with any standards-compliant server.

However, some servers may not be able to accept all characters in the User-Agent Client Hints headers as part of the broader Structured Headers emerging standard. If the addition of this header causes problems with servers that can’t be fixed quickly, you will be able to use the UserAgentClientHintsEnabled policy to disable the added headers.

This is a temporary policy that will be removed in Chrome 88.

Chrome warns about mixed content forms

Web forms that load via HTTPS but submit their content via HTTP (unsecured) pose a potential risk to users' privacy. Chrome 85 showed a warning on such forms, telling the user that the form is insecure. Chrome 86 shows an interstitial warning when the form is submitted, which stops any data transmission, and the user is able to choose whether to proceed or cancel the submission.



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

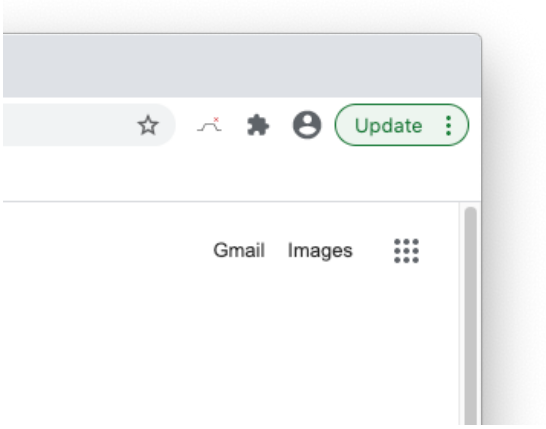
The address bar shows the domain rather than the full URL for some users

To protect your users from some common phishing strategies, Chrome shows 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 are now able to revert to the old behavior through the ShowFullUrlsInAddressBar policy.
This change is initially only rolled out to some users, however a full rollout is planned for a later release.

Chrome has a new way to show you it's time to update your browser

To make it more clear that Chrome should be restarted to apply an update, users will see a new UI, with the word "Update," replacing the colored arrow that users see today.



Chrome extensions are not able to inject Flash content settings

Extensions are not able to inject content settings for Flash. If you're using an extension to control Flash behavior in Chrome, you should instead use PluginsAllowedForUrls. Otherwise, users will see the default Flash behavior, which will require them to allow Flash to run on each site.

The Chrome Cloud Management - Reporting Companion extension no longer functions

The Chrome Cloud Management - Reporting Companion extension ID, oempjldejiginopiohodkdoklcjklbaa is no longer necessary, as its functionality has been integrated into Chrome browser. If you are manually force-installing this extension, you can safely stop doing so. Please ensure that you've set "Enable managed browser cloud reporting" in the admin console instead.

The TLS13HardeningForLocalAnchorsEnabled enterprise policy no longer functions

As documented in the policy description, support for the TLS13HardeningForLocalAnchorsEnabled enterprise policy will be removed in Chrome 86. As a result, the security feature will be enabled for all users, protecting your environment from certain TLS downgrade attacks.

The policy was introduced as a temporary measure to mitigate implementation flaws with some TLS-intercepting proxies. If you had previously set this policy to take advantage of the migration period, please ensure your TLS-intercepting policies are up to date and compliant. You can test Chrome by ensuring it works without this policy set.

More inclusive policy names are introduced

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 will be deprecated (but will still work), and equivalent policies will be introduced for each:

Deprecated Policy Name	New Policy Name	Version
NativeMessagingBlacklist	NativeMessagingBlocklist	86
NativeMessagingWhitelist	NativeMessagingAllowlist	86
AuthNegotiateDelegateWhitelist	AuthNegotiateDelegateAllowlist	86
AuthServerWhitelist	AuthServerAllowlist	86
SpellcheckLanguageBlacklist	SpellcheckLanguageBlocklist	86
AutoplayWhitelist	AutoplayAllowlist	86
SafeBrowsingWhitelistDomains	SafeBrowsingAllowlistDomains	86
ExternalPrintServersWhitelist	ExternalPrintServersAllowlist	86
NoteTakingAppsLockScreenWhitelist	NoteTakingAppsLockScreenAllowlist	86
PerAppTimeLimitsWhitelist	PerAppTimeLimitsAllowlist	86
URLWhitelist	URLAllowlist	86
URLBlacklist	URLBlocklist	86
ExtensionInstallWhitelist	ExtensionInstallAllowlist	86
ExtensionInstallBlacklist	ExtensionInstallBlocklist	86
UserNativePrintersAllowed	UserPrintersAllowed	86
NativePrinters	Printers	86
NativePrintersBulkConfiguration	PrintersBulkConfiguration	86
NativePrintersBulkAccessMode	PrintersBulkAccessMode	86
NativePrintersBulkBlacklist	PrintersBulkBlocklist	86
NativePrintersBulkWhitelist	PrintersBulkAllowlist	86
DeviceNativePrintersBlacklist	DevicePrintersBlocklist	87
DeviceNativePrintersWhitelist	DevicePrintersAllowlist	87
DeviceNativePrintersAccessMode	DevicePrintersAccessMode	87
DeviceNativePrinters	DevicePrinters	87
UsbDetachableWhitelist	UsbDetachableAllowlist	87
QuickUnlockModeWhitelist	QuickUnlockModeAllowlist	87
AttestationExtensionWhitelist	AttestationExtensionAllowlist	87
DeviceUserWhitelist	DeviceUserAllowlist	87

Chrome OS updates

Family Link and school account support for Android apps

Enables Family Link users to sign in to Android apps like Google Classroom using a school account to do schoolwork under parent supervision.

Smartcard support on the login screen

As an admin you can enable users to sign in using smart cards on the managed Chrome devices in your organization. The solution builds upon SAML SSO identity providers (IdP) that supports smart cards. Learn more.

Guide Parents to Set Up Devices for Children during OOBE/Add Person flow

Simplifies device setup for families that want to create parental controls for their kids on Chromebooks.

Redesigned Update Screen during OOBE

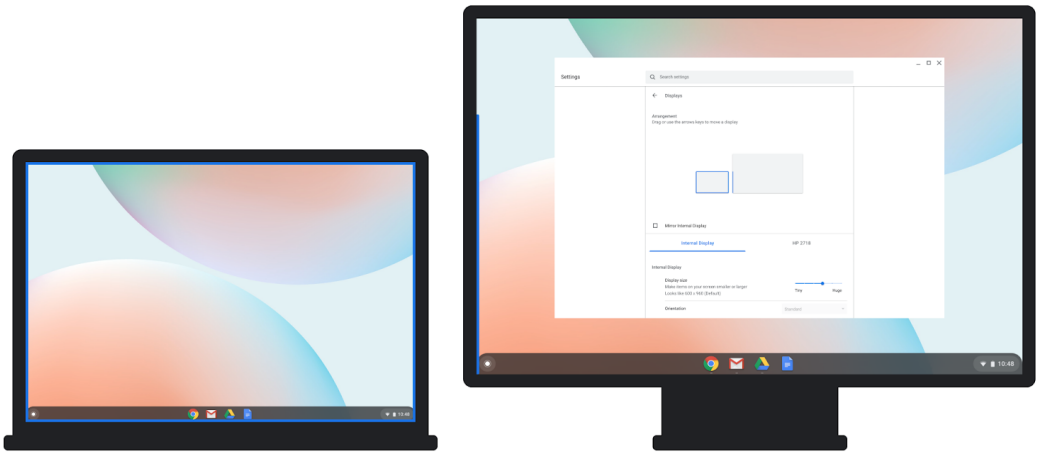
The update page during OOBE has been redesigned to include time/battery estimates and a progress tracker so users don't have to sit in front of the computer while it updates. We have also included educational cards on the screen; users who choose to wait in front of the computer or choose to check in during the update will learn more about the unique values that Chrome OS offers.

Option to view password/PIN on start screen and lock screen

Have a long password that you often type incorrectly? Need to refer to a password manager on your phone to log into your Chromebook? This is now easier as the login screen has a new button to let you review your password/PIN. Simply click the eye-shaped icon to show password/PIN in clear text, review or compare with your password manager, and then submit. For security, we will turn the clear text into ***** after 5 seconds of inactivity and clear the entire input after 30 seconds of inactivity.

Display Identification on multi-monitor setups

Managing multiple displays on Chrome OS has never been easier. We improved the ability for users to quickly identify which tab in the Display settings corresponds to a user's external display, and we've made it easier to align displays via a first-of-its-kind alignment overlay. These options are available for anyone using 2 or more displays.



Autocorrect UI improvements

For users with autocorrect enabled, we have improved the user interface with visual indicators which let you know that autocorrects have happened, as well as a new visual way to undo them.

Linux upgrade flow to Debian 10

If you have been using Linux (Beta) with Debian 9, you will now see an option to upgrade to Debian 10. You can start the upgrade at any time by going to Linux settings.

Virtual machine USB support beyond Android devices

More devices are able to use Linux (Beta), including Arduino and EdgeTPU. Attach a device to your Chromebook and share it through Linux settings.

Admin Console updates

Website icons and names on the Apps & extensions configuration page

Websites will now display their name and icon in addition to the URL in the Admin console. Admins can search by either name or URL to find websites. This change does not affect how website shortcuts display on the Chrome OS shelf.

Flash deprecation warnings

Flash Player will no longer be supported after December 2020 (roadmap). The Admin console no longer allows the configuration of Flash using wildcards. There are also additional reminders about the upcoming deprecation.

Always-on VPN for Android

Always-on VPN allows you to specify an Android VPN app that handles Android and Chrome OS user traffic as soon as users start their devices. For security reasons, virtual private networks (VPNs) don't apply to system traffic such as OS and policy updates. If the VPN connection fails, all user traffic is blocked until the VPN connection is re-established.

Remotely factory reset a managed device

You can now perform a full remote factory reset for managed devices, which can be useful for deprovisioning a device for RMA, clearing data on a disabled device that has been misplaced or stolen, and clearing data for troubleshooting purposes.

Note: After a device has been factory reset, it must go through the initial setup again. For a lighter touch reset, you can clear a user's profile instead.

Device-level system log export

This feature extends existing kiosk functionality to any managed device, allowing you to remotely capture device-level system log files. Once the LogUploadEnabled policy is enabled, you can manually request and download logs directly from the device details page, and fetch them through the Chrome Directory API.

Additional policies in the Admin console

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

Policy control	Admin console location	Description
Metrics reporting	User & browser settings > Other settings > Metrics	Controls anonymous reporting of usage and crash-related data about Google Chrome to

	reporting	Google
External extensions	Apps & extensions > Additional settings > External extensions	Controls installation of external extensions
Chrome Cleanup	User & browser settings > Security > Chrome Cleanup	Controls whether Chrome Cleanup periodically scans the system for unwanted software on browsers enrolled with Chrome Browser Cloud Management on Windows
Disabled system features	User & browser settings > User experience > Disabled system features	Controls whether users can access the camera, OS settings, and browser settings on Chrome OS devices
Privacy screen on sign-in screen	User & browser settings > Hardware > Privacy screen and Device settings > Sign-in settings > Privacy screen on sign-in screen	Controls whether the privacy screen is enabled on devices supporting an electronic privacy screen
Disk cache size	User & browser settings > Other settings > Disk cache size	Controls the cache size used by Chrome browser
PDF files	User & browser settings > Content > PDF files	Controls whether PDF files open in Chrome or using the system default application
Suggested content	User & browser settings > User experience > Suggested content	Enables suggestions for new content to explore on Chrome OS. Includes apps, webpages, and more. This policy is disabled by default for managed users
Default browser check	User & browser settings > Startup > Default browser check	Controls whether Chrome checks if it is the default browser at startup
Background mode	User & browser settings > Other settings > Background mode	Controls whether Chrome keeps running when the last browser window is closed, allowing background apps to remain active
Third party code	User & browser settings > Security > Third party code	Controls whether third party software will be allowed to inject executable code into Chrome's processes on Windows
Relaunch notification	User & browser settings > Chrome updates > Relaunch notification	Controls the notifications shown to users reminding them to update Chrome

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
AuthNegotiateDelegateAllowlist	Kerberos delegation server allowlist. Replaces

	AuthNegotiateDelegateWhitelist
AuthServerAllowlist	Authentication server allowlist. Replaces AuthServerWhitelist
AutoplayAllowlist	Allow media autoplay on a whitelist of URL patterns. Replaces AutoplayWhitelist
CloudPrintWarningsSuppressed	Suppress Google Cloud Print deprecation messages
DefaultFileSystemReadGuardSetting	Control use of the File System API for reading
DefaultFileSystemWriteGuardSetting	Do not allow any site to request write access to files and directories. See File System API for details
DefaultSerialGuardSetting	Control use of the Serial API
EnterpriseRealTimeUrlCheckMode	Check Safe Browsing status of URLs in real time
ExtensionInstallAllowlist	Configure extension installation allow list. Replaces ExtensionInstallWhitelist
ExtensionInstallBlocklist	Configure extension installation blocklist. Replaces ExtensionInstallBlacklist
FileSystemReadAskForUrls	Allow read access via the File System API on these sites
FileSystemReadBlockedForUrls	Block read access via the File System API on these sites
FileSystemWriteAskForUrls	Allow write access to files and directories on these sites. See File System API for details
FileSystemWriteBlockedForUrls	Block write access to files and directories on these sites. See File System API for details
InsecureFormsWarningsEnabled	Enable warnings for insecure forms
LookalikeWarningAllowlistDomains	Suppress lookalike domain warnings on domains
SafeBrowsingAllowlistDomains	Configure the list of domains on which Safe Browsing will not trigger warnings
SerialAskForUrls	Allow the Serial API on these sites
SerialBlockedForUrls	Block the Serial API on these sites
ShowFullUrlsInAddressBar	Show Full URLs
SpellcheckLanguageBlocklist	Force disable spellcheck languages. Replaces SpellcheckLanguageBlacklist
URLBlocklist	Block access to a list of URLs. Replaces URLBlacklist

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

ITP will block third party cookies in Chrome on iOS14

All Chrome versions on iOS14 will be subject to the new ITP (Intelligent Tracking Prevention) restriction in WebKit, which blocks third party cookies. Apple has provided more information on the changes here:

- Third Party Cookie Blocking
- Tracking prevention

Single words will not be treated as intranet locations by default in Chrome 87

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).

Improved resource consumption for background tabs in Chrome 87

To save on CPU and power consumption, Chrome will throttle the amount of CPU that background tabs can use. With this change, Chrome will only allow background tabs to wake up once per minute and to only use 1% CPU time.

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

DTLS 1.0 will be removed in Chrome 87

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.

New PDF UI in Chrome 87

Chrome will have an updated PDF viewer, including toolbar updates, table of contents, thumbnails, two-up view, and annotations.

The CORB/CORS allowlist will be removed in Chrome 87

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 and run through critical workflows with your extension. Watch for fetches or XHRs that are initiated by content scripts and blocked by CORB or CORS. 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

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 88

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 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 is experimenting with a permissions chip in the address bar next to the lock, which is less intrusive overall. 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.

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. We recommend testing critical sites using the testing instructions.

You may revert to the previous, legacy behavior, by using the LegacySameSiteCookieBehaviorEnabledForDomainList and LegacySameSiteCookieBehaviorEnabled policies. For more detail 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.

SyncXHR and Popup on page unload policies will no longer be supported on Chrome 88

The AllowPopupsDuringPageUnload and AllowSyncXHRInPageDismissal 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 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.

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.

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.