chrome enterprise

M85 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 August 25, 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 85

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

User-Agent Client Hints will be introduced in Chrome 85

As part of an ongoing effort to reduce bad actors' ability 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 additive 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, part of the broader Structured Headers emerging standard. If the addition of this header causes problems with servers that cannot 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.

A full rollout of this change is planned in Chrome 85.

The default referrer policy will change in Chrome 85

The HTTP **referrer** header provides the full URL of the initiating document alongside many navigation and subresource requests. In practice, it can reveal users' browsing habits or identities. Chrome will improve user privacy and security by switching to **strict-origin-when-cross-origin** as the default policy, instead of **no-referrer-when-downgrade**. Web developers may specify a referrer policy on their documents if they need a different policy.

The expected long-term fix is to update all web apps to preferably not depend on the full URL for the referrer, and where unavoidable, specify a referrer policy when they require something other than **strict-origin-when-cross-origin**. However, to help with the transition, enterprises will be able to use the ForceLegacyDefaultReferrerPolicy enterprise policy to revert to the old default behavior until Chrome 88.

Chrome 64-bit on Windows will be installed in "Program Files" instead of "Program Files (x86)"

New installations of 64-bit Chrome will be installed in "%ProgramFiles%" on Windows instead of "%ProgramFiles(x86)%". Existing installations won't be impacted.

Improvements to user productivity in Chrome 85

Chrome will be making several improvements to user productivity, including collapsible tab groups, tab previews, saving inputs in PDFs, and QR code sharing. You can read more about these improvements on the Keyword.

Compiler optimization performance improvements in Chrome 85

Chrome will use an improved compiler optimization technique called PGO (Profile-guided optimization) on Mac and Windows. Enterprises aren't expected to notice any changes, except how software interacts with Chrome in unexpected or unsupported ways. For example, code injection may not function as expected with this version of Chrome.

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 will be blocked in Chrome 85.
- Archives—Users will be warned in the Chrome developer console in Chrome 85, and files will be blocked in Chrome 86.
- Other non-safe types (For example, 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 Desktop warnings by one release. For example, executables will show a warning starting in Chrome 85.

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

Wildcards are no longer supported in PluginsAllowedForUrls in Chrome 85

In preparation for the Flash deprecation later this year, Chrome will be removing the ability for enterprises to define entries with wildcards in hostnames (For example, “https://*” or “https://[*.]mysite.foo”) for the PluginsAllowedForUrls policy. If you're using hostname wildcards, you will need to explicitly specify which hostnames still require Flash. For example, “https://[*.]mysite.foo” would need to be updated to match explicit entries like “https://flash.mysite.foo”. This change is intended to help determine which sites still require updating, with time to make an adjustment before support for Flash is removed completely in December, 2020.

The Legacy Browser Support extension will be removed from the Chrome Web Store in Chrome 85

Legacy Browser Support (LBS) is now built into Chrome, and the old extension is no longer needed. The Chrome team is planning to unpublish LBS from the Chrome Web Store in Chrome 85, and it will be removed from browsers in Chrome 86. To continue using Legacy Browser Support, ensure that you're using Chrome's built-in policies, documented here. The old policies set through the extension will no longer take effect when the extension is removed.

The Beta version of the extension (Extension ID `ebojbgfomggiamdflnhekjfkmdbeblpb`) will be removed in Chrome 85.

Cross-origin fetches will be disallowed from content scripts in Chrome Extensions in Chrome 85

As part of an effort to improve Chrome Extension security, cross-origin fetches are being disallowed from content scripts in Chrome Extensions. Cross-Origin Read Blocking (CORB) has already applied to content scripts since M73. We plan to also enable CORS for content script requests starting in M85. We expect most extensions to be unaffected by the CORS change, but there is a chance that some requests initiated from content scripts may start to fail.

Please test Chrome Extensions that your business depends on to make sure they work with the new behavior when Chrome is launched with the following cmdline flags (in 81.0.4035.0 or later):

```
--enable-features=OutOfBlinkCors,CorbAllowlistAlsoAppliesToOorCors
```

During the test, watch for fetches or XHRs that are initiated by content scripts and blocked by CORS. If extensions you depend on are affected, open a bug to add the affected extensions to a temporary allowlist which will exempt them from the change (the allowlist will be deprecated and removed in Chrome 87). The changes only affect fetches or XHRs for content types that are not blocked by CORB (such as images, JavaScript, and CSS) and only if the server does not approve the CORS request with an Access-Control-Allow-Origin response header.

Improved resource consumption when a window is not visible in Chrome 85

To save on CPU and power consumption, Chrome will detect when a window is covered by other windows and will suspend work painting pixels. A previous version of this feature had incompatibility issues with some virtualization software. 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 will see the change in Chrome 85, with a full rollout planned for Chrome 86.

The SafeBrowsingExtendedReportingOptInAllowed policy is no longer available in Chrome 85

The support of SafeBrowsingExtendedReportingOptInAllowed policy has been removed in Chrome 85. Please use SafeBrowsingExtendedReportingEnabled policy instead. You can find the migration instructions on the deprecated policy page.

Introduction of AutoLaunchProtocolsFromOrigins policy in Chrome 85

The new AutoLaunchProtocolsFromOrigins policy allows you to specify combinations of external protocols and origins that should be launched automatically, without requiring user confirmation.

Chrome on MacOS will have additional protections for sensitive enterprise policies in Chrome 85

Macs that are not managed by a UEM/EMM/MDM (or legacy MCX) will ignore sensitive enterprise policies that may be set by malware. This check already happens for sensitive policies on Windows, and will apply to the same set of policies on MacOS.

Cross-Origin Resource Setting (CORS) enterprise policies are no longer available

The CorsMitigationList and CorsLegacyModeEnabled policies have been removed in Chrome 84, as previously communicated.

The ForceNetworkInProcess policy is now deprecated

Chrome 73 introduced a change to move network activity into a separate process. We were aware of known incompatibilities with some third-party software that were injected into Chrome's process, so the ForceNetworkInProcess policy was provided as a temporary stop-gap to revert to the old behavior. The transition period for this change ended in Chrome 84, and the policy is no longer available.

Certificates issued on or after September 01, 2020 must have a lifetime of 398 days or less in Chrome 85

As part of our ongoing commitment to ensuring user security, Google is reducing the maximum allowed lifetimes of TLS certificates. More details here.

Chrome 85 uses the Windows-native spell checker for some users

For Windows users that have the corresponding language packs installed on their system, Chrome will use the Windows-native spell checker. Users without the corresponding language pack will default to the Chrome spell checker.

Some users will see this change in Chrome 85, with a full rollout planned in Chrome 86.

The Chrome Web Store will tell users if an extension has been blocked by their admin in Chrome 85

If you block an extension by policy, the Chrome Web Store extension listing will now show “Blocked by Admin” to the user.

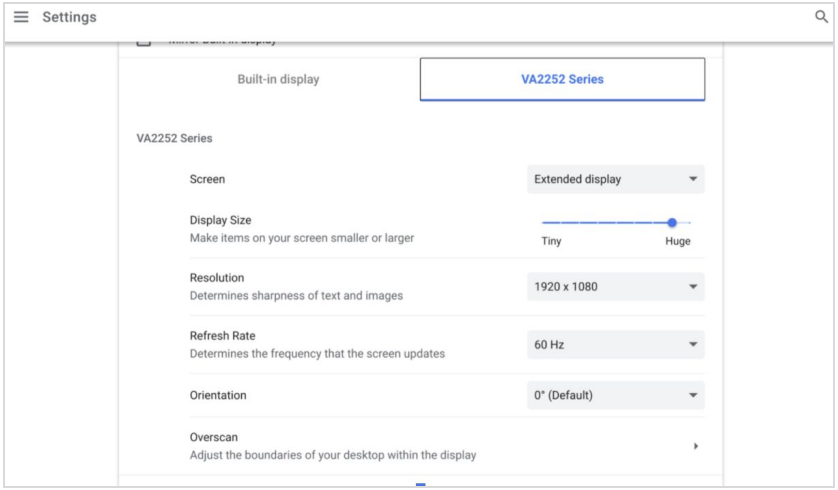
Chrome-on-iOS enterprise policies in Chrome 85

Chrome supports a limited set of policies on iOS, configurable with unified endpoint management systems.

Chrome OS updates

Separating Display Resolution and Refresh Rate for external monitors

The “Displays” page in Settings has been updated to allow independent configuration of the resolution and the refresh rate for external monitors. This setting will be split automatically and users do not need to take any action.



Sync Wi-Fi settings between devices

To help users avoid repeatedly joining the same set of networks and typing in the same difficult-to-remember passwords on each of their Chrome OS devices, Wi-Fi Sync helps keep known networks in sync between a user's devices. This can be controlled using the SyncTypesListDisabled policy.

Option for improved visuals for Select to Speak

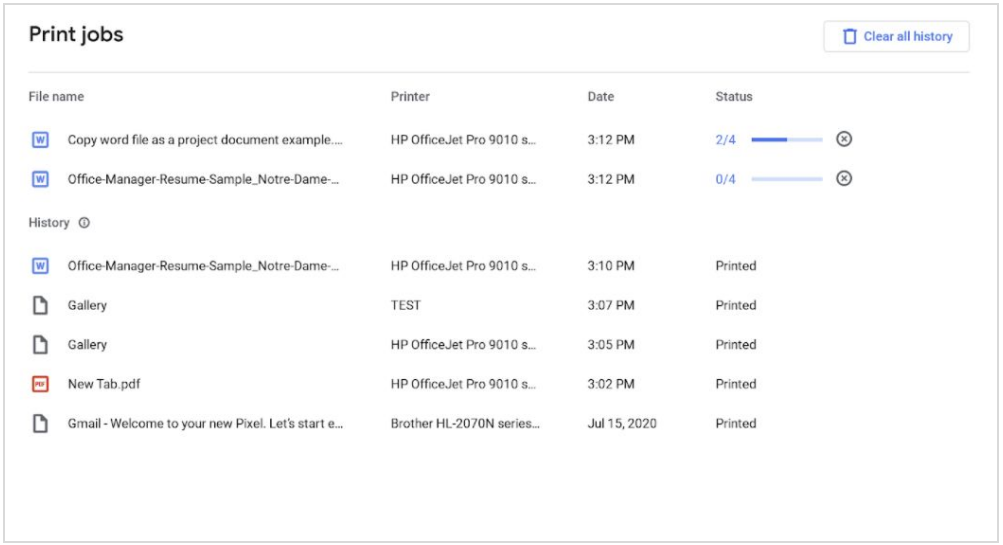
Select to speak lets users drag a box around a given area of text to have text in that area spoken aloud. We've now added the option to turn on screen shading behind the selected region of the screen. This screen shading will reduce distraction and help to enhance the user's focus on the core content being spoken aloud.

Improved gesture support for handwriting keyboard

When entering text using the handwriting keyboard, you can now use familiar gestures to edit your handwriting. Drawing a strikethrough will delete text, and a caret will give you space to insert text.

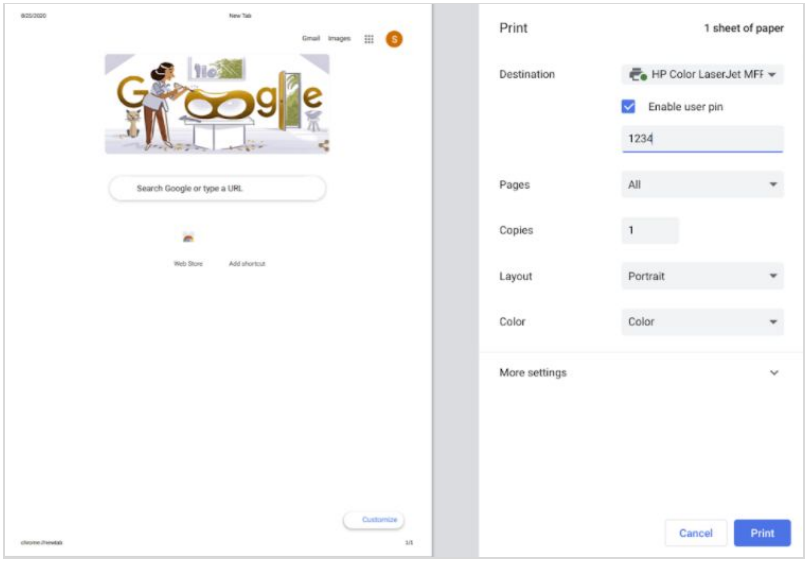
Improved Print management UI

Users can now manage their ongoing print jobs and view what has been completed.



PIN printing for HP, Ricoh, and Sharp printers

Extended PIN printing support is now available for all supported HP, Ricoh, and Sharp printers that require a PIN to release the print job to a printer.



Admin Console updates

Updated Admin console > Devices hub page

The Devices hub in the Admin console is refreshed with a new look and feel, faster load times, and a brand new navigation structure on the left side of the page.

View apps & extensions is configured across all organizational units

The apps & extensions page in the Admin console now supports “Include all organizational units.” Selecting this view will display all apps configured across all modes (User & browser, Kiosks, Managed guest session) and all organizational units.

Expanded ability to block system features

Admins can now block system features at a granular level directly, without URL blocking. The Camera app, Chrome browser settings and Chrome OS settings are all configurable through policy.

Connected devices policies for Android phones + Chrome OS devices

User settings > Connected devices is a suite of features that allows Android phones and Chrome devices to work together seamlessly. Education organizations can enable **Smart Lock** and **Click to Call**. In addition, Enterprise organizations can enable **Instant Tethering** and **Messages**.

Multi-select devices for clearing user profiles

From the Chrome > Devices list, admins can now multi-select devices to clear user profiles from all devices at the same time.

Additional policies now available in the Admin console

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

- **PrintingMaxSheetsAllowed**
  User settings > Printing > Maximum sheets - Set a maximum number of pages for a single print job.
- **PrintingMaxSheetsAllowed and PrintingPaperSizeDefault**
  User settings > Printing > Default printing page size - Set a default paper page size for print jobs.
- **AppCacheForceEnabled**
  User settings > Content > AppCache - Allow websites to use the deprecated AppCache browser feature.
- **HardwareAccelerationModeEnabled**
  User settings > Hardware > GPU - Enable or disable GPU hardware acceleration.
- **ScrollToTextFragmentEnabled**
  User settings > Content > Scroll to text fragment - Allow sites to scroll directly to a text fragment via URL.
- **HideWebStoreIcon**
  Apps & extensions > Additional settings > Chrome Web Store app icon - Hide the Chrome Web Store app and footer link from the New Tab Page and Google Chrome OS app launcher.

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description
AutoLaunchProtocolsFromOrigins	Define a list of protocols that can launch an external application from listed origins without prompting the user.
CloudExtensionRequestEnabled	Enables Google Chrome extension installation requests.
DefaultSearchProviderContextMenuAccessAllowed	Enables the use of a default search provider on the context menu.rch access.
EnableExperimentalPolicies	Enables experimental policies.
IntensiveWakeUpThrottlingEnabled	When enabled, the IntensiveWakeUpThrottling feature causes Javascript timers in the

	background tabs to be aggressively throttled and coalesced, running no more than once per minute after a page has been in the background for 5 minutes or more.
UserAgentClientHintsEnabled	Controls the User-Agent Client Hints feature.

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 by avoiding DNS lookups for single keywords entered into the address bar. However, this change to default behavior 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 via 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 warn about mixed content forms in Chrome 86

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 will show an interstitial warning when the form is submitted, which will stop any data transmission, and the user will be able to choose to proceed or cancel the submission.

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

The address bar will show the domain rather than the full URL for some users in Chrome 86

To protect your users from some common phishing strategies, Chrome will begin showing only the domain in the address bar in Chrome 86. 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 will be able to revert to the old behavior through the ShowFullUrls policy. This change will initially only roll out to some users, with a full rollout planned for a later release.

Improved resource consumption for background tabs in Chrome 86

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.

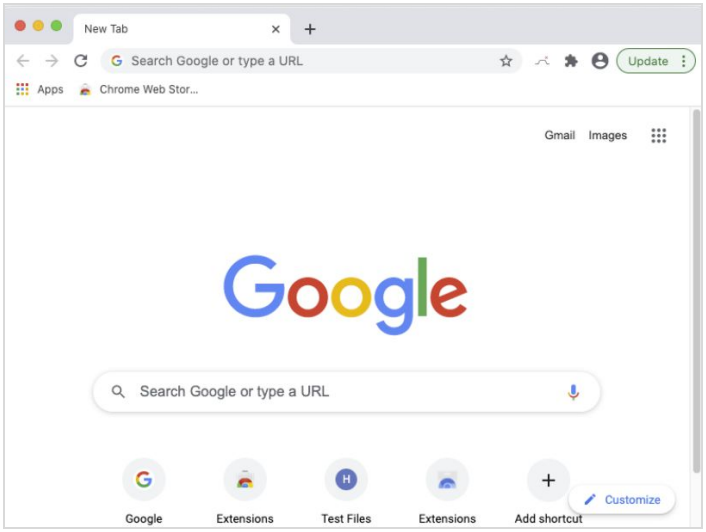
You will be able to control this behavior using the IntensiveWakeUpThrottlingEnabled policy.

Insecure public pages no longer allowed to make requests to private or local URLs in Chrome 86

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. A policy will be provided to turn off this mechanism, and another one to allow specific pages to make requests to more private IP Address Spaces.

Chrome 86 will have a new way of indicating it should be updated

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



Chrome extensions will not be able to inject Flash content settings in Chrome 86

Extensions will not be able to inject content settings for Flash. Admins should instead use policies to control Flash behavior on Chrome. See PluginsAllowedForUrls.

The Chrome Cloud Management - Reporting Companion extension will cease functionality in Chrome 86

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 extension will no longer function in Chrome 86.

The TLS13HardeningForLocalAnchorsEnabled enterprise policy will no longer function in Chrome 86

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 will be introduced in Chrome 86 and 87

Chrome will be moving to more inclusive policy names. The terms "whitelist" and "blacklist" will be replaced with "allowlist" and "blocklist". The following policies will be deprecated, 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
DeviceNativePrintersBlacklist	DevicePrintersBlocklist	87
DeviceNativePrintersWhitelist	DevicePrintersAllowlist	87
DeviceNativePrintersAccessMode	DevicePrintersAccessMode	87
DeviceNativePrinters	DevicePrinters	87
NativePrinters	Printers	86
NativePrintersBulkConfiguration	PrintersBulkConfiguration	86
NativePrintersBulkAccessMode	PrintersBulkAccessMode	86
NativePrintersBulkBlacklist	PrintersBulkBlocklist	86
NativePrintersBulkWhitelist	PrintersBulkAllowlist	86
UsbDetachableWhitelist	UsbDetachableAllowlist	87
QuickUnlockModeWhitelist	QuickUnlockModeAllowlist	87
AttestationExtensionWhitelist	AttestationExtensionAllowlist	87
DeviceUserWhitelist	DeviceUserAllowlist	87

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.

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, a policy will be made available to temporarily extend the removal.

Chrome will introduce a new permission chip UI in Chrome 87

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.

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 viewing.

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 are considered cross-site instead of same-site. For example, http://site.example and https://site.example will be considered cross-site to each other.

For enterprises that need extra time to adjust to these changes, policies will be made available.

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.