Chrome 98 Enterprise release notes

For administrators who manage Chrome browser or Chrome devices for a business or school.

These release notes were last updated on February 01, 2022.

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

Release summary

Chrome browser updates	**Security**	**User productivity /Apps**	**Management**
Use Chrome passwords in other apps on iOS		✓	
Update GREASE brand list generation	✓		✓
Chrome disables the U2F API by default	✓		✓
Chrome no longer allows TLS 1.0 or TLS 1.1	✓		
Private network access preflights for subresources	✓		
Integrate Enhanced Safe Browsing preference with account settings	✓		✓
TFLite model for client-side phishing detection	✓		
`Chrome deprecates the installed_browser_version` field in the Directory API			✓
New extensions must be submitted with Manifest v3	✓		
New and updated policies in Chrome browser			✓
Chrome OS updates	**Security**	**User productivity /Apps**	**Management**
Expanded keyboard shortcuts for Desks		✓	
Add *Save to* settings to screen capture		✓	
Support for Network Based Recovery (NBR)			✓
Admin console updates	**Security**	**User productivity /Apps**	**Management**
Search devices by version or mode			✓
New policies in the Admin console			✓

Upcoming Chrome browser changes	Security	User productivity /Apps	Management
Chrome Major Version number will reach 100		✓	✓
Network Service on Windows will be sandboxed	✓		
WebHID enterprise policies			✓
Default to origin-keyed agent clustering	✓		
Change tab-sharing blue order behavior		✓	

Chrome browser updates

Use Chrome passwords in other apps on iOS

Chrome 98 informs iOS users that they can use any passwords saved in Chrome in other apps on their device.

The **Chrome** > **Settings** > **Passwords** screen shows a new option for **Passwords in Other Apps**, which guides users to turn on this feature in iOS autofill settings.

You can control if users can save passwords using Chrome with the PasswordManagerEnabled policy.

Update GREASE brand list generation

User-Agent Client Hints GREASE aims to prevent bad or exclusionary assumptions from being built on top of the proposed replacement for User-Agent strings. This means that users of less well-tested browsers will not be rejected for not matching the precise format of a more-well tested browsers UA string.

This change aligns our implementation of GREASE in User-Agent Client Hints with the current spec, which includes additional GREASE characters beyond the current semicolon and space, and which recommends varying the arbitrary version. While we are rolling out this change gradually and continue to watch for negative impacts, such as WAF software flagging headers as invalid

traffic, admins can opt out using the UserAgentClientHintsGREASEUpdateEnabled enterprise policy.

Chrome disables the U2F API by default

The U2F API is Chrome's legacy API for interacting with USB security keys. It has been superseded by the W3C Web Authentication API (WebAuthn). Chrome 98 disables the U2F API by default. With Chrome 104, the U2F API will be removed from Chrome.

Sites can continue to use the U2F API beyond Chrome 98 if they enroll in an Origin Trial. Using the Origin Trial also suppresses the deprecation prompt on the enrolled pages. The Origin Trial will end on July 26, 2022, shortly before the release of Chrome 104.

Enterprises can suppress deprecation related changes, and keep the U2F enabled, by using the U2fSecurityKeyApiEnabled enterprise policy. This enterprise policy will be removed from Chrome, together with the U2F API, in Chrome 104.

If you run a website that still uses this API, please refer to the deprecation announcement and blog post for more details.

Chrome no longer allows TLS 1.0 or TLS 1.1

The SSLVersionMin policy no longer allows setting a minimum version of TLS 1.0 or 1.1. This means the policy can no longer be used to suppress Chrome's interstitial warnings for TLS 1.0 and 1.1. Administrators must upgrade any remaining TLS 1.0 and 1.1 servers to TLS 1.2. In Chrome 91, we announced that the policy no longer works, but users could still bypass the interstitial. In Chrome 98, it is not possible to bypass the interstitial.

Private network access preflights for subresources

Chrome sends a CORS preflight request ahead of any private network requests for subresources, asking for explicit permission from the target server. This request carries a new `Access-Control-Request-Private-Network: true` header, and the response must carry a matching `Access-Control-Allow-Private-Network: true` header.

A private network request is any request from a public website to a private IP address or localhost, or from a private website, for example, an Intranet, to a localhost. Sending a preflight request mitigates the risk of cross-site request forgery attacks against private network devices such as routers, which are often not prepared to defend against this threat.

Chrome 98 sends these preflight requests but does not yet require them to succeed. Failed preflights only display warnings in DevTools, which you can use to detect problematic fetches in your web apps. In Chrome 101 at the earliest, failed preflights will cause the entire request to fail depending on compatibility data. See the blog post for more information.

You can control this behavior using enterprise policies InsecurePrivateNetworkRequestsAllowed and InsecurePrivateNetworkRequestsAllowedForUrls.

Integrate Enhanced Safe Browsing preference with account settings

Chrome now prompts users who opt in to **Account Enhanced Safe Browsing** to enable **Enhanced Safe Browsing** in Chrome. Their Safe Browsing setting is still controlled by the SafeBrowsingProtectionLevel policy.

TFLite model for client-side phishing detection

Chrome uses an on-device Machine Language (ML) model to better detect phishing attempts, and better protect users. As in earlier versions, Chrome displays a full-page interstitial warning if Chrome detects a possible phishing attempt. This was previously launched for Android in Chrome 92, and is now on desktop platforms as well.

With this change, Chrome sends the following to the Safe Browsing service:

- the version of the model that was executed

- the scores the model gave for each category
- a boolean describing whether the new model was used to generate the scores

You can control Safe Browsing using the SafeBrowsingProtectionLevel policy. This feature applies to users with the protection level set at 1 or greater.

Chrome deprecates the installed_browser_version field in the Directory API

The `installed_browser_version` field in the Directory API: Chrome Browsers service has been deprecated and replaced by the `pending_browser_version` field. The `pending_browser_version` represents the version of Chrome browser that is installed on browser restart.

New extensions must be submitted with Manifest v3

As part of the gradual deprecation of Manifest V2, the Chrome Web Store has stopped accepting submissions of *new* Manifest V2 extensions as of January 17, 2022. This applies to all new extension submissions with visibility set to Public or Unlisted. The change does not affect updates to already published extensions. Also, it does not impact extensions with visibility set to Private.

This change is not expected to affect the operation of any existing extensions already deployed in Chrome. Note that the next phase of deprecation, in June of 2022, is expected to expand this restriction to extensions with Private visibility, which may have a more significant impact on Enterprise extension workflows. For more details, refer to the Manifest V2 support timeline.

New and updated policies in Chrome browser

Policy	Description
URLBlocklist (new on iOS)	Block access to a list of URLs
URLAllowlist (new on iOS)	Allow access to a list of URLs
UserAgentClientHintsGREASEUpdateEnabled	Control the User-Agent Client Hints GREASE Update feature
UserAgentReduction	Enable or disable the User-Agent Reduction

Chrome OS updates

Expanded keyboard shortcuts for Desks

Chrome 98 adds a new shortcut to make it faster and easier to switch Desks. Create up to 8 desks to organize your projects and use the shortcut **Shift** + **Search** + **1** through **Shift** + **Search** + **8** to jump from one desk to another using only the keyboard.

Add *Save to* settings to screen capture

Now users can save screen captures to any local or drive folder of their choice, making capturing and using content even more efficient.

Support for Network Based Recovery (NBR)

In Chrome 98, some users can re-flash their devices with a fresh copy of the OS and firmware, letting them recover if the message: *Chrome OS is missing or damaged* appears. NBR requires a network connection. This feature will roll out to more devices in later releases.

Admin console updates

Search devices by version or model

In the Chrome filters view for the devices page for ChromeOS, you can now filter and search the devices by version and by model.

New policies in the Admin console

Policy Name	Pages	Supported on	Category/Field
ScreenBrightnessPercent	User & Browser Settings; Managed Guest Session	Chrome OS	Security > Screen brightness
PrintPostScriptMode	User & Browser Settings	Chrome	Printing > PostScript printer mode
SandboxExternalProtocolBlocked	User & Browser Settings; Managed Guest Session	Chrome Chrome OS	Content > iframe navigation
U2fSecurityKeyApiEnabled	User & Browser Settings	Chrome	Security > U2F Security Key API
DeviceRebootOnUserSignout	Device Settings	Chrome OS	Power and shutdown > Reboot on sign-out

Coming soon

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

Upcoming Chrome browser changes

Chrome Major Version number will reach 100

Chrome will reach a 3-digit major version number in March, 2022. When browsers went from version 9 to 10, the increase in the number of digits uncovered many issues in User-Agent string parsing libraries. In order to avoid the same issue again, developers and IT admins should test their services in advance.

To help, the Chrome team created the *ForceMajorVersion100InUserAgent* flag (`chrome://flags/#force-major-version-to-100`). This forces the browser to send 100 as the major version number (blog). You should use this flag to uncover and address any issues before Chrome 100 rolls out. We encourage admins to submit any issues encountered here.

Network Service on Windows will be sandboxed

As early as Chrome 100, to improve security and reliability, the network service, already running in its own process, will be sandboxed on Windows. As part of this, third-party code that is currently able to tamper with the network service may be prevented from doing so. This might cause interoperability issues with software that injects code into Chrome's process space, such as Data Loss Prevention software. The NetworkServiceSandboxEnabled policy allows you to disable the sandbox if incompatibilities are discovered. You can test the sandbox in your environment using these instructions and report any issues you encounter.

WebHID enterprise policies

As early as Chrome 100, Chrome will add policies to manage the WebHID API. **DefaultWebHidGuardSetting** configures the default API behavior for all URLs and can be

configured to allow origins to Ask for new device permissions or Block all permission requests. The **WebHidAskForUrls** and **WebHidBlockedForUrls** policies override the default policy for specific URLs.

Three new policies are added for automatically granting device permissions. URLs contained in the **WebHidAllowAllDevicesForUrls** policy will be automatically granted permissions for any connected device. The **WebHidAllowDevicesForUrls** and **WebHidAllowDevicesWithHidUsagesForUrls** policies can be used to grant narrower permissions by matching against vendor and product IDs or application collection usages in the HID report descriptor.

Default to origin-keyed agent clustering

As early as Chrome 103, websites will be unable to set *document.domain*. Websites will need to use alternative approaches such as `postMessage()` or Channel Messaging API to communicate cross-origin. If a website relies on same-origin policy relaxation via *document.domain* to function correctly, it will need to send an `Origin-Agent-Cluster: ?0` header along with all documents that require that behavior.

Note: *document.domain* has no effect if only one document sets it.

An enterprise policy will be available when this change ships to extend the current behavior.

Change tab-sharing blueborder behavior

When a user chooses to share their tab from a site participating in the region capture origin trial, the blue border used to signify that a tab is being shared will no longer be shown.

Previous release notes

Chrome version & targeted Stable channel release date	PDF
Chrome 97: January 04, 2022	PDF
Chrome 96: November 16, 2021	PDF
Chrome 95: October 19, 2021	PDF
Chrome 94 OS: October 14, 2021	PDF
Archived release notes	

Additional resources

- For emails about future releases, sign up here.
- To try out new features before they're released, sign up for the trusted tester program.
- Connect with other Chrome Enterprise IT admins through the Chrome Enterprise Customer Forum.
- How Chrome releases work—Chrome Release Cycle
- Chrome Browser downloads and Chrome Enterprise product overviews—Chrome Browser for enterprise
- Chrome version status and timelines—Chrome Platform Status | Google Update Server Viewer
- Announcements: Chrome Releases Blog | Chromium Blog
- Developers: Learn about changes to the web platform and features planned for upcoming releases.

Still need help?

- Google Workspace, Cloud Identity customers (authorized access only)—Contact support
- Chrome Browser Enterprise Support—Sign up to contact a specialist
- Chrome Administrators Forum
- Chrome Enterprise Help Center