chrome enterprise

M79 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 December 11, 2019

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

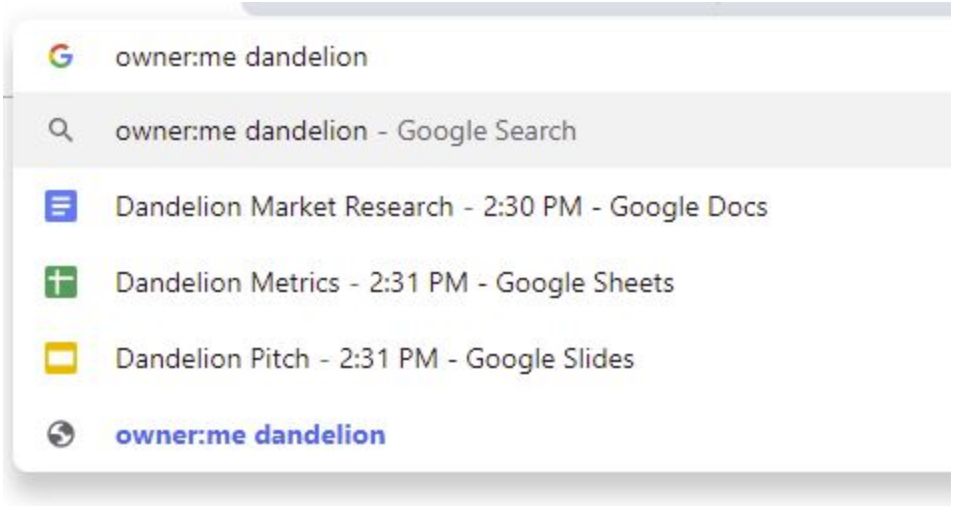
Sign up **here** for our email distribution for future releases.

Chrome 79

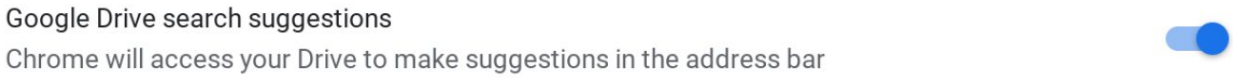
Chrome Browser updates

Drive integration in the address bar

Rolling out in the coming weeks, users will be able to search for Google Drive files that they have access to from the address bar. Their input will search through both titles and document contents and the most relevant documents based on their history will appear.



This behavior is on by default and can be controlled from the G Suite admin console or by individual users in their Chrome settings, under Sync and Google services. You can see more details in this G Suite announcement.



HTTPS pages will only be able to load secure subresources, with changes from Chrome 79 to Chrome 81

In Chrome 79, we're introducing a new setting to unblock mixed content on specific sites. This setting will apply to mixed scripts, iframes, and other types of content that Chrome currently blocks by default. End users can switch this setting by clicking the lock icon on any https:// page and clicking **Site Settings**.

In Chrome 80, mixed audio and video resources will be auto-upgraded to https://, and Chrome will block them by default if they fail to load over https://. Users can unblock affected audio and video resources with the setting described above. Also in Chrome 80, mixed images will still be allowed to load, but they will cause Chrome to show a "Not Secure" chip in the omnibox.

In Chrome 81, mixed images will be auto-upgraded to https://, and Chrome will block them by default if they fail to load over https://.

The breaking changes coming in Chrome 80 and 81 will be controllable by enterprise policy. Enterprise policies to control this feature will be StricterMixedContentTreatmentEnabled which disables autoupgrades for audio and video, and the warning for images, this one will be temporary and we'll remove it on Chrome 84. InsecureContentAllowedForUrls/InsecureContentBlockedForUrls will control the setting described above.

More information on these changes is available in the Chromium blog. Admins should begin ensuring that resources in pages under their control are fetched over HTTPS. Exceptions can be managed through policy.

Better password and phishing protections in Chrome

For more details on how these work, see this blog post.

- **Users warned if credentials are leaked:** Starting in Chrome 79, users will be notified if their credentials are part of a known data breach. The system can detect this without sending plain-text passwords to Google. Administrators will be able to enable or disable this feature for your users using the PasswordLeakDetectionEnabled policy.
- **Realtime phishing detection:** We'll also be offering enhanced protection against quick-changing sites, by inspecting page URLs with Safe Browsing's servers in real-time, resulting in a 30% increase in protections. We will initially be rolling out this protection for users who have already opted into the 'Make searches and browsing better' option in Chrome. Enterprises administrators can manage this setting directly using the UrlKeyedAnonymizedDataCollectionEnabled policy.
- **Expanding predictive phishing protection:** With this latest release, we're also expanding Chrome Safe Browsing's predictive phishing protections to everyone signed in to Chrome, even if they have not enabled Sync. In addition, this feature will now work for all the passwords users have stored in Chrome's password manager. This protection will not be enabled if users are not signed into Chrome and have not enabled Chrome Password Manager. Administrators can also choose to disable Chrome Safe Browsing using the SafeBrowsingEnabled policy. *We discourage doing this as it will disable all built-in anti-abuse protections in Chrome.*

CORS implementation is more secure

Chrome is modifying its Cross-Origin Resource Sharing (CORS) implementation to be more secure. As a result, the following changes will be introduced incrementally, starting on January 6th, 2020. This gradual rollout will happen over the following several weeks:

- E**xtensions' webRequest API**—Before this change, extensions that have the webRequest permission could modify any network request headers and they would be ignored by the CORS protocol. However, in Chrome 79, the CORS protocol inspects modified headers and will trigger a CORS preflight request to the destination servers when the modified request doesn't meet the SimpleRequest requirement. If users are using a Chrome extension that's affected by this change, the extension author will need to update the extension to specify 'extraHeaders' in opt_extraInfoSpec, or update the server-side logic to accept the CORS requests correctly. See the Extensions API document for more details.

- **Headers injected by Chrome**—Before this change, headers injected by Chrome for a particular enterprise policy didn't trigger the CORS protocol. However, in Chrome 79, this will trigger a CORS preflight request. Server implementations might need to be updated to handle CORS preflight requests.

If administrators need extra time to adapt to this CORS migration, there are two enterprise policies available. These are temporary policies which will only be available until Chrome 82.

- CorsLegacyModeEnabled—Enable the old CORS implementation, which is compatible with Chrome 78 and earlier versions. Admins can use this policy to opt-out of this gradual rollout.
- CorsMitigationList— sets the 'extraHeaders' in opt_extraInfoSpec internally so that any extension that is not ready for this CORS migration can work without modifications. Admins can also specify customized headers that should be ignored by CORS checks.

The OOR-CORS Troubleshooting page will help investigate incompatibility issues and customize these policies.

Trial of autoupgrade for DNS-over-HTTPS

The DNS requests of some users will autoupgrade to their DNS provider's DNS-over-HTTPS (DoH) service if available. During this trial, DoH will be disabled by default for managed devices running Chrome OS and for desktop Chrome Browser instances that are domain joined or have at least one active policy.

You can disable DNS-over-HTTPS for your users with the DnsOverHttpsMode policy. Setting it to "off" will ensure your users are not affected by DoH.

Click-to-call

Users will now be able to click on a phone number in Chrome to send it to their Android phone. To send the number, users need to have Chrome Browser installed and be signed in on both devices with the same account. The number is end-to-end encrypted and Google can't see the contents. You can control this behavior with the ClickToCallEnabled policy.

Audio sandbox

The audio service on Windows will be sandboxed in Chrome 79 for added security. We have seen incompatibilities with certain configurations of AppLocker in Chrome 77, although these have been fixed in Chrome 78. Other similar products might also have issues with the sandbox. If your users have issues with audio playing in Chrome 79, you can disable the audio sandbox using the AudioSandboxEnabled policy.

New Chrome UI for legacy TLS versions in Chrome 79 and Chrome 81

The Chrome team recently announced our updated plans around our deprecation and planned removal of legacy TLS versions (TLS 1.0 and 1.1). Starting in January 2020 in Chrome 79, we will mark sites that do not support TLS >=1.2 as "Not Secure" and no longer show the lock icon for them.

In Chrome 81, we will start showing a full-page interstitial warning telling users that the connection is not fully secure.

If enterprise users have sites affected by these changes and need to opt out, admins can use the existing SSLVersionMin policy to disable the security indicator and interstitial warning on all affected sites. Admins should set it to "tls1" to allow TLS 1.0 and later without additional warnings. This policy will work until January 2021. More details are available in our blog post.

New policy for controlling memory

We're introducing a new policy to give admins more control over Chrome's memory usage, which allows better management of shared virtual sessions. The TotalMemoryLimitMb policy configures the amount of memory that a single Chrome instance can use before starting to discard background tabs. When discarded, the memory used by the tab is freed, and the user will have to reload the tab when switching to it.

If the policy is set, Chrome will begin to discard tabs to save memory once the user exceeds the limit. However, there is no guarantee that Chrome will always run under the limit—for example, the active tab is never discarded. Any value under 1,024 will be rounded up to 1,024. If this policy is not set, the browser will only attempt to save memory after it has detected that the amount of physical memory on its machine is low (available on Windows and Mac).

On Linux, server certificate verification will use the built-in certificate verifier instead of NSS

Chrome on Linux will perform verification of server certificates using the built-in certificate verifier instead of NSS, starting in Chrome 79. The built-in verifier will still use the NSS trust store, so we expect that users won't see this change. However there are some cases where differences might occur:

- Certificates with invalid encodings: The built-in verifier is stricter about enforcing spec compliance and might reject some certificates that NSS allowed. This should not affect any publicly trusted certificates, but might affect enterprises with internal PKIs.
- Directly trusted end-entity (leaf) certificates: The built-in verifier does not support directly marking server certificates as trusted; certificates must be issued by a CA that is trusted.

The verifier can be toggled using the BuiltinCertificateVerifierEnabled policy, allowing affected enterprises a chance to update their certificate infrastructure if they are affected by the transition. The policy will be supported through Chrome 82 on Linux to give enterprises sufficient time to update and test their infrastructure. Chrome OS switched to the built-in verifier in Chrome 77, and the policy will be supported on that platform through Chrome 80.

Chrome Browser Cloud Management Reporting Companion is no longer required

The functionality previously provided by the "Chrome Cloud Management - Reporting Companion" extension has been integrated directly into Chrome. If Admins are using Chrome Browser Cloud Management, some users will no longer see the extension on their fleet when reporting is enabled. It will be completely removed for all users in Chrome 80. No action is required from Admins or their users.

Chrome Renderer Integrity protects users

Chrome Renderer Integrity is on by default for users on Microsoft® Windows® 10 version 1511 and later. It prevents unsigned modules from loading in Chrome Browser's renderer processes that deal with user content to prevent certain types of malicious attacks.

Chrome 78 enabled this feature, but it was rolled back due to unforeseen incompatibilities with other software. Those issues have been addressed, and this will be rolled out again in Chrome 79. Affected software and mitigations are listed in this support thread.

To help with any incompatibilities, you can temporarily disable Chrome Renderer Integrity using the RendererCodeIntegrityEnabled policy.

Chrome OS updates

Continued improvements to Virtual Desks

With Chrome 79, we are rolling out new improvements for virtual desktops, which are called Virtual Desks in Chrome OS. In Chrome 79, when a user opens a link, it will always open on their current desk. This will help users keep their workspaces separated.

New Overview mode for tablets

When in tablet mode, there's an updated Overview mode. It makes it easy to scroll through open windows, and works well on smaller screens. For split screen, just long press on a window to drag it to the left or right side to start split screen. The new Overview is available in tablet mode only on slates, convertibles, and detachables.

Lock Screen Media Controls

We are adding media controls to the Chrome OS lock screen. This will allow users to see what is playing and control playback while the device is locked.

Unified App Management for end users in Settings

Basic settings and permissions of apps in Chrome OS can now be managed from the new App Management feature, available in Settings.

Broader Crostini support for arbitrary ports on localhost

Previously, web developers using Linux Beta (aka Crostini) could only access local servers in Chrome if they were running on a small number of whitelisted ports. This restriction has been lifted, and now it no longer matters what port the local server is using.

Printing Metrics API

New printingMetrics API is now available for forced installed extensions to see a managed user's print history when printing to a native printer.

SAML default on for Enterprise

Currently, SAML SSO is deactivated for Chromebooks by default. This means that if you are using a SAML provider your users are able to access their accounts and their G Suite services on any device other than a Chromebook. From January 2020, we will activate SAML SSO for Chromebooks of new accounts, meaning your users will no longer be restricted to non-Chrome OS devices.

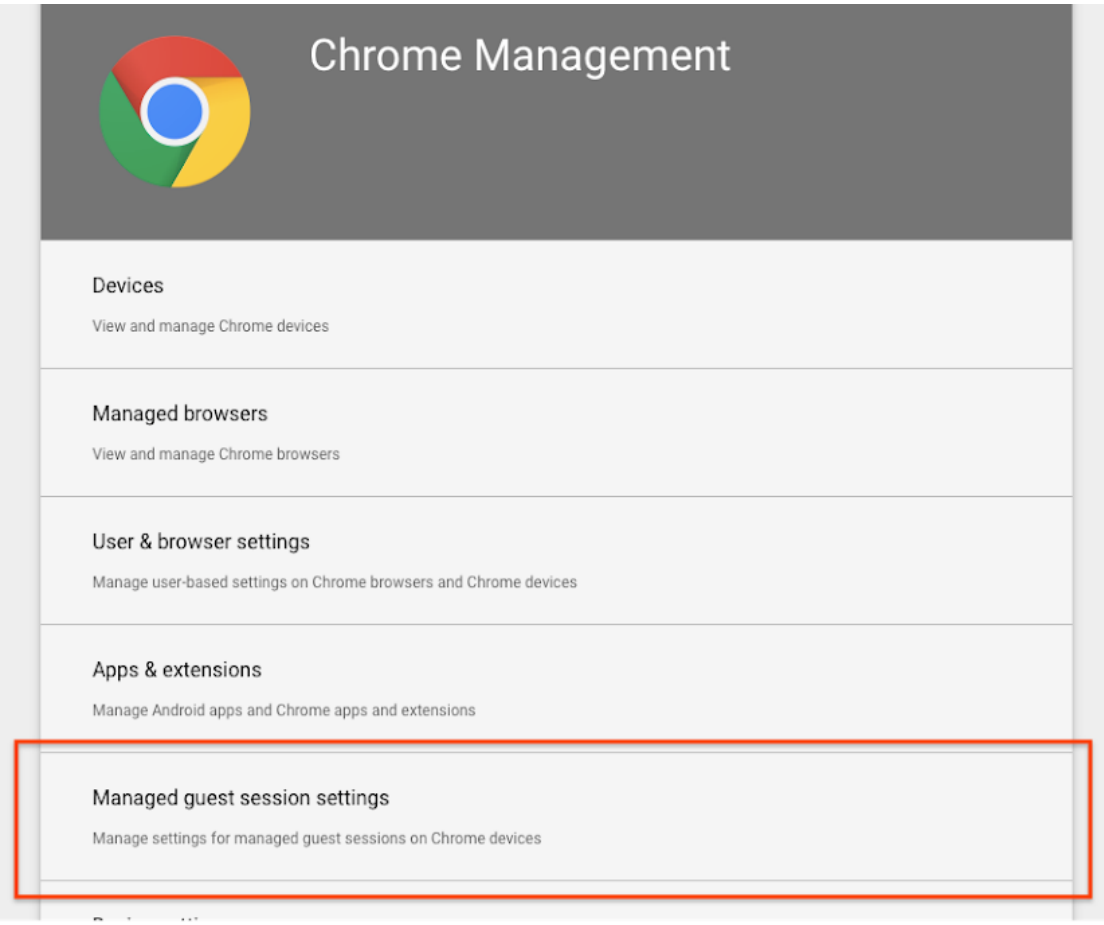
Simplifying the Out of Box experience for Android apps

Currently, Google Play is deactivated by default. When activated, the Managed mode, which allows you to restrict the apps that users can install, is selected by default. Starting on December 2, 2019, we activated Google Play by default in All Access Mode (for all managed accounts, except Education users). This means that enterprise users will be granted full access to the managed Google Play store; allowing them to search and install any app on their Chrome devices, including apps administrators haven't approved.

Admin Console updates

New managed guest session settings page rolling out soon

The new managed guest session settings page is rolling out and will be available for all customers soon. The new page features a redesigned search interface, more information about policy inheritance, and a few new policies.



Remote configuration of driverless printers

Driverless printers are now supported from the Printer Management page in the Admin console. Administrators can now remotely assign printers that rely on auto discovery (using IPP to query the printer and set job attributes for the print job) to connect. Previously, only PPD based printers could be configured from the admin console.

Initiate remote desktop connection for kiosk devices from Admin console

IT admins can now remotely initiate a Chrome Remote Desktop connection into a kiosk device and take control of the device for support and troubleshooting from the Device Details page in the Admin console.

New and updated policies (Chrome Browser and Chrome OS)

Policy	Description

AudioSandboxEnabled *Browser Only*	Allow the audio sandbox to run. If third-party software is interfering with Chrome's audio, setting this policy to false may resolve the issue.
ClickToCallEnabled	Enable the Click to Call feature which allows users to send phone numbers from Chrome Desktops to an Android device when the user is Signed-in.
CorsLegacyModeEnabled	Use the legacy CORS implementation rather than new CORS
CorsMitigationList	Enable CORS check mitigations in the new CORS implementation
DefaultInsecureContentSetting	Control use of insecure content exceptions
ExternalProtocolDialogShowAlwaysOpenCheckbox *Browser Only*	Show an "Always open" checkbox in external protocol dialog
InsecureContentAllowedForUrls	Allow insecure content on these sites
InsecureContentBlockedForUrls	Block insecure content on these sites
LegacySameSiteCookieBehaviorEnabled	Default legacy SameSite cookie behavior setting
LegacySameSiteCookieBehaviorEnabledForDomainList	Revert to legacy SameSite behavior for cookies on these sites
SharedClipboardEnabled	Enable the Shared Clipboard Feature
TLS13HardeningForLocalAnchorsEnabled	Enable a TLS 1.3 security feature for local trust anchors
WebRtcLocalIpsAllowedUrls	URLs for which local IPs are exposed in WebRTC ICE candidates

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

SyncTypesListDisabled policy in Chrome 80

Chrome users have the ability to granularly enable or disable each type of sync data. In Chrome 80, this control will also be an enterprise policy, so that admins can control the sync types across their organization.

PaymentMethodQueryEnabled in Chrome 80

We are working on an enterprise policy that allows you to set whether websites are allowed to check if your user has payment methods saved. If the setting is enabled or not set, then websites are allowed to check if the user has payment methods saved. If this policy is set to disabled, websites that use PaymentRequest.canMakePayment or PaymentRequest.hasEnrolledInstrument API will be informed that no payment methods are available.

Tab freezing on desktop in Chrome 80

Chrome 80 will introduce a new feature to save memory, CPU, and battery for Windows, Mac, Linux, and Chrome OS. Tabs that have been in the background for 5 minutes or more will be frozen, as long as Chrome detects that they are freezable (such as not playing audio). Frozen pages are not able to run any tasks. Web developers can opt their pages out of freezing with an origin trial. You will be able to disable this behavior with the TabFreezingEnabled policy.

Ambient authentication disabled by default in Incognito mode and Guest sessions in Chrome 81

Ambient authentication (NTLM/Kerberos) will be disabled by default in Incognito mode and Guest sessions in Chrome 81. You will be able to use a policy to revert to the old behavior and allow ambient authentication using the AmbientAuthenticationInPrivateModesEnabled policy, which will be available starting in Chrome 80.

Pop-ups and synchronous XHR requests not allowed on page unload in Chrome 80

Pop-ups and synchronous XHR requests won't be allowed on page unload. This change will improve page load time and make code paths simpler and more reliable. If you encounter incompatibilities with legacy software, you will be able to revert to behavior matching Chrome 79 and earlier using the following policies, which will be available until Chrome 82:

- Allow pop-ups on page unload: AllowPopupsDuringPageUnload
- Allow synchronous XHRs on page unload: AllowSyncXHRInPageDismissal

FTP support will be removed in Chrome 80

FTP won't be directly supported in Chrome Browser. Your users should use a native FTP client instead. To help with the transition, you will be able to use the FTPProtocolSupport policy to temporarily re-enable FTP until Chrome 82.

Updates to cookies with SameSite in Chrome 80

Starting in Chrome 80 on the Stable channel, cookies that don't specify a SameSite attribute will be treated as if they were SameSite=Lax. Cookies that still need to be delivered in a cross-site context can explicitly request SameSite=None. The attributes must also be marked Secure and delivered over HTTPS.

This new behavior will also take effect in Chrome 79 on the Beta channel only. Because this change might be disruptive, we recommend you test critical sites on the Chrome 79 Beta channel, which will be available starting Oct. 31. See instructions for testing.

You will be able to revert to the legacy cookie behavior using policies, starting in Chrome 79 in Beta. You can specify trusted domains using LegacySameSiteCookieBehaviorEnabledForDomainList or control the global default with LegacySameSiteCookieBehaviorEnabled. For more details, visit Cookie Legacy SameSite Policies.

Tab groups will be introduced in Chrome 80

Starting in Chrome 80, some users will be able to organize their tabs by grouping them on the tab strip. Each group can have a color and a name, to help your users keep track of their different tasks and workflows. A wider rollout is planned for Chrome 81.

Web Components v0 removed in Chrome 80

The Web Components v0 APIs (Shadow DOM v0, Custom Elements v0, and HTML Imports) were supported only by Chrome Browser. To ensure interoperability with other browsers, late last year, we announced that these v0 APIs were deprecated and will be removed in Chrome 80. You can find more information in the Web Components update.

If you need additional time to adjust to this removal, you will be able to use the WebComponentsV0Enabled policy to re-enable web components v0 for a limited time.

Policy to block external extensions in Chrome 80

In Chrome 80, you will be able to use the BlockExternalExtensions enterprise policy to stop external extensions from being installed on your fleet. It will not block kiosk apps, or extensions provided by recommended policies.

TLS 1.3 hardening measure implemented in Chrome 81

TLS 1.3 includes a hardening measure to strengthen the protocol's protections against a downgrade to TLS 1.2 and earlier. This measure is backward compatible and doesn't require that proxies support TLS 1.3. It only requires that proxies correctly implement TLS 1.2. However, last year, we had to partially disable this measure due to bugs in some noncompliant, TLS-terminating proxies.

The following list contains the minimum firmware versions for affected products that we're aware of:

Palo Alto Networks:

- PAN-OS 8.1 must be upgraded to 8.1.4 or later.
- PAN-OS 8.0 must be upgraded to 8.0.14 or later.
- PAN-OS 7.1 must be upgraded to 7.1.21 or later.

Cisco Firepower Threat Defense and ASA with FirePOWER Services when operating in "Decrypt - Resign mode/SSL Decryption Enabled" (advisory PDF):

- Firmware 6.2.3 must be upgraded to 6.2.3.4 or later.
- Firmware 6.2.2 must be upgraded to 6.2.2.5 or later.
- Firmware 6.1.0 must be upgraded to 6.1.0.7 or later.

Starting in Chrome 79, you will be able to opt in to the new measure to test it and confirm if your proxy is affected, using the TLS13HardeningForLocalAnchorsEnabled policy. If you encounter problems, you should upgrade affected proxies to fixed versions.

Starting in Chrome 81, the new measure will become the default. However, you will be able to use the same policy to opt out if you need extra time to upgrade affected proxies. This proxy will be available until Chrome 86.

Shared clipboard between computers and Android devices in Chrome 81

Users will have the option to share their clipboard content between their computers and Android devices. To share, they need to have Chrome Browser installed, be signed in on both devices with the same account, and have Chrome sync enabled.

The text is end-to-end encrypted, and Google can't see the contents. This feature will be controllable with the SharedClipboardEnabled policy.

Upcoming Chrome OS changes

Adding print server support for CUPS

We're working on a feature to add support for Common UNIX Printing System (CUPS) printing from print servers on Chrome OS. You and your users will be able to configure connections to external print servers and print from the printers on servers using CUPS.

Updates for USB devices with Linux

From the Chrome shell (crosh), you'll be able to attach a USB device to Linux apps running on a Chromebook so that Linux apps can access the Linux instance.

Upcoming Google Admin console changes

Managed guest session support for managed Google Play

A setting in the Admin console will allow Android apps to run in managed guest sessions (previously known as public sessions). Currently, Android apps can only run in a signed-in session.

Update blackout windows

The DeviceAutoUpdateTimeRestrictions policy will be in the Admin console. This policy allows admins to set time blocks when automatic update checks are not to be performed. This policy only affects devices configured to auto-launch a kiosk app.