Both Chromium and Google Chrome support the same set of policies. Please note that this document may include policies that are targeted for unreleased software versions (i.e. their 'Supported on' entry refers to an unreleased version) and that such policies are subject to change or removal without prior notice.

These policies are strictly intended to be used to configure instances of Google Chrome internal to your organization. Use of these policies outside of your organization (for example, in a publicly distributed program) is considered malware and will likely be labeled as malware by Google and anti-virus vendors.

These settings don't need to be configured manually! Easy-to-use templates for Windows, Mac and Linux are available for download from https://www.chromium.org/administrators/policy-templates.

The recommended way to configure policy on Windows is via GPO, although provisioning policy via registry is still supported for Windows instances that are joined to an Active Directory domain.

Policy Name	Description
Accessibility settings	
ShowAccessibilityOptionsInSystemTrayMenu	Show accessibility options in system tray menu
LargeCursorEnabled	Enable large cursor
SpokenFeedbackEnabled	Enable spoken feedback
HighContrastEnabled	Enable high contrast mode
VirtualKeyboardEnabled	Enable on-screen keyboard
KeyboardDefaultToFunctionKeys	Media keys default to function keys
ScreenMagnifierType	Set screen magnifier type
DeviceLoginScreenDefaultLargeCursorEnabled	Set default state of the large cursor on the login screen
DeviceLoginScreenDefaultSpokenFeedbackEnabled	Set the default state of spoken feedback on the login screen
DeviceLoginScreenDefaultHighContrastEnabled	Set the default state of high contrast mode on the login screen
DeviceLoginScreenDefaultVirtualKeyboardEnabled	Set default state of the on-screen keyboard on the login screen
DeviceLoginScreenDefaultScreenMagnifierType	Set the default screen magnifier type enabled on the login screen
Allow Google Chrome Frame to handle the following content types	
ChromeFrameContentTypes	Allow Google Chrome Frame to handle the listed content types
Configure Google Drive options	
DriveDisabled	Disables Drive in the Google Chrome OS Files app

Policy Name	Description
DriveDisabledOverCellular	Disables Google Drive over cellular connections in the Google Chrome OS Files app
Configure remote access options	
RemoteAccessClientFirewallTraversal	Enable firewall traversal from remote access client
RemoteAccessHostClientDomain	Configure the required domain name for remote access clients
RemoteAccessHostFirewallTraversal	Enable firewall traversal from remote access host
RemoteAccessHostDomain	Configure the required domain name for remote access hosts
RemoteAccessHostRequireTwoFactor	Enable two-factor authentication for remote access hosts
RemoteAccessHostTalkGadgetPrefix	Configure the TalkGadget prefix for remote access hosts
RemoteAccessHostRequireCurtain	Enable curtaining of remote access hosts
RemoteAccessHostAllowClientPairing	Enable or disable PIN-less authentication for remote access hosts
RemoteAccessHostAllowGnubbyAuth	Allow gnubby authentication for remote access hosts
RemoteAccessHostAllowRelayedConnection	Enable the use of relay servers by the remote access host
RemoteAccessHostUdpPortRange	Restrict the UDP port range used by the remote access host
RemoteAccessHostMatchUsername	Requires that the name of the local user and the remote access host owner match
RemoteAccessHostTokenUrl	URL where remote access clients should obtain their authentication token
RemoteAccessHostTokenValidationUrl	URL for validating remote access client authentication token
RemoteAccessHostTokenValidationCertificateIssuer	Client certificate for connecting to RemoteAccessHostTokenValidationUrl
RemoteAccessHostDebugOverridePolicies	Policy overrides for Debug builds of the remote access host
RemoteAccessHostAllowUiAccessForRemoteAssistance	Allow remote users to interact with elevated windows in remote assistance sessions
Content Settings	
DefaultCookiesSetting	Default cookies setting

Policy Name	Description
DefaultImagesSetting	Default images setting
DefaultJavaScriptSetting	Default JavaScript setting
DefaultPluginsSetting	Default plugins setting
DefaultPopupsSetting	Default popups setting
DefaultNotificationsSetting	Default notification setting
DefaultGeolocationSetting	Default geolocation setting
DefaultMediaStreamSetting	Default mediastream setting
DefaultWebBluetoothGuardSetting	Control use of the Web Bluetooth API
DefaultKeygenSetting	Default key generation setting
AutoSelectCertificateForUrls	Automatically select client certificates for these sites
CookiesAllowedForUrls	Allow cookies on these sites
CookiesBlockedForUrls	Block cookies on these sites
CookiesSessionOnlyForUrls	Allow session only cookies on these sites
ImagesAllowedForUrls	Allow images on these sites
ImagesBlockedForUrls	Block images on these sites
JavaScriptAllowedForUrls	Allow JavaScript on these sites
JavaScriptBlockedForUrls	Block JavaScript on these sites
KeygenAllowedForUrls	Allow key generation on these sites
KeygenBlockedForUrls	Block key generation on these sites
PluginsAllowedForUrls	Allow plugins on these sites
PluginsBlockedForUrls	Block plugins on these sites
PopupsAllowedForUrls	Allow popups on these sites
RegisteredProtocolHandlers	Register protocol handlers
PopupsBlockedForUrls	Block popups on these sites
NotificationsAllowedForUrls	Allow notifications on these sites
NotificationsBlockedForUrls	Block notifications on these sites
Default HTML renderer for Google Chrome Frame	
ChromeFrameRendererSettings	Default HTML renderer for Google Chrome Frame
RenderInChromeFrameList	Always render the following URL patterns in

Policy Name	Description
	Google Chrome Frame
RenderInHostList	Always render the following URL patterns in the host browser
AdditionalLaunchParameters	Additional command line parameters for Google Chrome
SkipMetadataCheck	Skip the meta tag check in Google Chrome Frame
Default search provider	
DefaultSearchProviderEnabled	Enable the default search provider
DefaultSearchProviderName	Default search provider name
DefaultSearchProviderKeyword	Default search provider keyword
DefaultSearchProviderSearchURL	Default search provider search URL
DefaultSearchProviderSuggestURL	Default search provider suggest URL
DefaultSearchProviderInstantURL	Default search provider instant URL
DefaultSearchProviderIconURL	Default search provider icon
DefaultSearchProviderEncodings	Default search provider encodings
DefaultSearchProviderAlternateURLs	List of alternate URLs for the default search provider
DefaultSearchProviderSearchTermsReplacementKey	Parameter controlling search term placement for the default search provider
DefaultSearchProviderImageURL	Parameter providing search-by-image feature for the default search provider
DefaultSearchProviderNewTabURL	Default search provider new tab page URL
DefaultSearchProviderSearchURLPostParams	Parameters for search URL which uses POST
DefaultSearchProviderSuggestURLPostParams	Parameters for suggest URL which uses POST
DefaultSearchProviderInstantURLPostParams	Parameters for instant URL which uses POST
DefaultSearchProviderImageURLPostParams	Parameters for image URL which uses POST
Extensions	
ExtensionInstallBlacklist	Configure extension installation blacklist
ExtensionInstallWhitelist	Configure extension installation whitelist
ExtensionInstallForcelist	Configure the list of force-installed apps and extensions
ExtensionInstallSources	Configure extension, app, and user script install sources

Policy Name	Description
ExtensionAllowedTypes	Configure allowed app/extension types
Home page	
HomepageLocation	Configure the home page URL
HomepageIsNewTabPage	Use New Tab Page as homepage
Locally managed users settings	
SupervisedUsersEnabled	Enable supervised users
SupervisedUserCreationEnabled	Enable creation of supervised users
SupervisedUserContentProviderEnabled	Enable the supervised user content provider
Native Messaging	
NativeMessagingBlacklist	Configure native messaging blacklist
NativeMessagingWhitelist	Configure native messaging whitelist
NativeMessagingUserLevelHosts	Allow user-level Native Messaging hosts (installed without admin permissions).
Password manager	
PasswordManagerEnabled	Enable saving passwords to the password manager
PasswordManagerAllowShowPasswords	Allow users to show passwords in Password Manager (deprecated)
Policies for HTTP authentication	
AuthSchemes	Supported authentication schemes
DisableAuthNegotiateCnameLookup	Disable CNAME lookup when negotiating Kerberos authentication
EnableAuthNegotiatePort	Include non-standard port in Kerberos SPN
AuthServerWhitelist	Authentication server whitelist
AuthNegotiateDelegateWhitelist	Kerberos delegation server whitelist
GSSAPILibraryName	GSSAPI library name
AuthAndroidNegotiateAccountType	Account type for HTTP Negotiate authentication
AllowCrossOriginAuthPrompt	Cross-origin HTTP Basic Auth prompts
Power management	
ScreenDimDelayAC	Screen dim delay when running on AC power
ScreenOffDelayAC	Screen off delay when running on AC power
ScreenLockDelayAC	Screen lock delay when running on AC power

Policy Name	Description
IdleWarningDelayAC	Idle warning delay when running on AC power
IdleDelayAC	Idle delay when running on AC power
ScreenDimDelayBattery	Screen dim delay when running on battery power
ScreenOffDelayBattery	Screen off delay when running on battery power
ScreenLockDelayBattery	Screen lock delay when running on battery power
IdleWarningDelayBattery	Idle warning delay when running on battery power
IdleDelayBattery	Idle delay when running on battery power
IdleAction	Action to take when the idle delay is reached
IdleActionAC	Action to take when the idle delay is reached while running on AC power
IdleActionBattery	Action to take when the idle delay is reached while running on battery power
LidCloseAction	Action to take when the user closes the lid
PowerManagementUsesAudioActivity	Specify whether audio activity affects power management
PowerManagementUsesVideoActivity	Specify whether video activity affects power management
PresentationIdleDelayScale	Percentage by which to scale the idle delay in presentation mode (deprecated)
PresentationScreenDimDelayScale	Percentage by which to scale the screen dim delay in presentation mode
AllowScreenWakeLocks	Allow screen wake locks
UserActivityScreenDimDelayScale	Percentage by which to scale the screen dim delay if the user becomes active after dimming
WaitForInitialUserActivity	Wait for initial user activity
PowerManagementIdleSettings	Power management settings when the user becomes idle
ScreenLockDelays	Screen lock delays
Proxy server	
ProxyMode	Choose how to specify proxy server settings
ProxyServerMode	Choose how to specify proxy server settings
ProxyServer	Address or URL of proxy server
ProxyPacUrl	URL to a proxy .pac file

Policy Name	Description
ProxyBypassList	Proxy bypass rules
Remote Attestation	
AttestationEnabledForDevice	Enable remote attestation for the device
AttestationEnabledForUser	Enable remote attestation for the user
AttestationExtensionWhitelist	Extensions allowed to to use the remote attestation API
AttestationForContentProtectionEnabled	Enable the use of remote attestation for content protection for the device
Startup pages	
RestoreOnStartup	Action on startup
RestoreOnStartupURLs	URLs to open on startup
AllowDinosaurEasterEgg	Allow Dinosaur Easter Egg Game
AllowFileSelectionDialogs	Allow invocation of file selection dialogs
AllowKioskAppControlChromeVersion	Allow the auto launched with zero delay kiosk app to control Google Chrome OS version
AllowOutdatedPlugins	Allow running plugins that are outdated
AllowScreenLock	Permit locking the screen
AllowedDomainsForApps	Define domains allowed to access Google Apps
AlternateErrorPagesEnabled	Enable alternate error pages
AlwaysAuthorizePlugins	Always runs plugins that require authorization
AlwaysOpenPdfExternally	Always Open PDF files externally
ApplicationLocaleValue	Application locale
ArcBackupRestoreEnabled	Enable Android Backup Service
ArcCertificatesSyncMode	Set certificate availability for ARC-apps
ArcEnabled	Enable ARC
ArcPolicy	Configure ARC
AudioCaptureAllowed	Allow or deny audio capture
AudioCaptureAllowedUrls	URLs that will be granted access to audio capture devices without prompt
AudioOutputAllowed	Allow playing audio
AutoCleanUpStrategy	Selects the strategy used to free up disk space during automatic clean-up (deprecated)

Policy Name	Description
AutoFillEnabled	Enable AutoFill
BackgroundModeEnabled	Continue running background apps when Google Chrome is closed
BlockThirdPartyCookies	Block third party cookies
BookmarkBarEnabled	Enable Bookmark Bar
BrowserAddPersonEnabled	Enable add person in profile manager
BrowserGuestModeEnabled	Enable guest mode in browser
BuiltInDnsClientEnabled	Use built-in DNS client
CaptivePortalAuthenticationIgnoresProxy	Captive portal authentication ignores proxy
CertificateTransparencyEnforcementDisabledForUrls	Disable Certificate Transparency enforcement for a list of URLs
ChromeOsLockOnIdleSuspend	Enable lock when the device become idle or suspended
ChromeOsMultiProfileUserBehavior	Control the user behavior in a multiprofile session
ChromeOsReleaseChannel	Release channel
ChromeOsReleaseChannelDelegated	Whether the release channel should be configurable by the user
ClearSiteDataOnExit	Clear site data on browser shutdown (deprecated)
CloudPrintProxyEnabled	Enable Google Cloud Print proxy
CloudPrintSubmitEnabled	Enable submission of documents to Google Cloud Print
ComponentUpdatesEnabled	Enables component updates in Google Chrome.
ContextualSearchEnabled	Enable Touch to Search
DHEEnabled	Whether DHE cipher suites in TLS are enabled
DataCompressionProxyEnabled	Enable the data compression proxy feature
DefaultBrowserSettingEnabled	Set Google Chrome as Default Browser
DefaultPrinterSelection	Default printer selection rules
DeveloperToolsDisabled	Disable Developer Tools
DeviceAllowBluetooth	Allow bluetooth on device
DeviceAllowNewUsers	Allow creation of new user accounts
DeviceAllowRedeemChromeOsRegistrationOffers	Allow users to redeem offers through Chrome OS Registration
DeviceAppPack	List of AppPack extensions

Policy Name	Description
DeviceAutoUpdateDisabled	Disables Auto Update
DeviceAutoUpdateP2PEnabled	Auto update p2p enabled
DeviceBlockDevmode	Block developer mode
DeviceDataRoamingEnabled	Enable data roaming
DeviceEphemeralUsersEnabled	Wipe user data on sign-out
DeviceGuestModeEnabled	Enable guest mode
DeviceIdleLogoutTimeout	Timeout until idle user log-out is executed
DeviceIdleLogoutWarningDuration	Duration of the idle log-out warning message
DeviceLocalAccountAutoLoginBailoutEnabled	Enable bailout keyboard shortcut for auto-login
DeviceLocalAccountAutoLoginDelay	Public session auto-login timer
DeviceLocalAccountAutoLoginId	Public session for auto-login
DeviceLocalAccountPromptForNetworkWhenOffline	Enable network configuration prompt when offline
DeviceLocalAccounts	Device-local accounts
DeviceLoginScreenDomainAutoComplete	Enable domain name autocomplete during user sign in
DeviceLoginScreenPowerManagement	Power management on the login screen
DeviceLoginScreenSaverId	Screen saver to be used on the sign-in screen in retail mode
DeviceLoginScreenSaverTimeout	Duration of inactivity before the screen saver is shown on the sign-in screen in retail mode
DeviceMetricsReportingEnabled	Enable metrics reporting
DeviceOpenNetworkConfiguration	Device-level network configuration
DevicePolicyRefreshRate	Refresh rate for Device Policy
DeviceQuirksDownloadEnabled	Enable queries to Quirks Server for hardware profiles
DeviceRebootOnShutdown	Automatic reboot on device shutdown
DeviceShowUserNamesOnSignin	Show usernames on login screen
DeviceStartUpFlags	System wide flags to be applied on Google Chrome start-up
DeviceStartUpUrls	Load specified urls on demo login
DeviceTargetVersionPrefix	Target Auto Update Version
DeviceTransferSAMLCookies	Transfer SAML IdP cookies during login

Policy Name	Description
DeviceUpdateAllowedConnectionTypes	Connection types allowed for updates
DeviceUpdateHttpDownloadsEnabled	Allow autoupdate downloads via HTTP
DeviceUpdateScatterFactor	Auto update scatter factor
DeviceUserWhitelist	Login user white list
Disable3DAPIs	Disable support for 3D graphics APIs
DisablePluginFinder	Specify whether the plugin finder should be disabled
DisablePrintPreview	Disable Print Preview (deprecated)
DisableSSLRecordSplitting	Disable TLS False Start
DisableSafeBrowsingProceedAnyway	Disable proceeding from the Safe Browsing warning page
DisableScreenshots	Disable taking screenshots
DisableSpdy	Disable SPDY protocol
DisabledPlugins	Specify a list of disabled plugins
DisabledPluginsExceptions	Specify a list of plugins that the user can enable or disable
DisabledSchemes	Disable URL protocol schemes
DiskCacheDir	Set disk cache directory
DiskCacheSize	Set disk cache size in bytes
DisplayRotationDefault	Set default display rotation, reapplied on every reboot
DnsPrefetchingEnabled	Enable network prediction
DownloadDirectory	Set download directory
EasyUnlockAllowed	Allows Smart Lock to be used
EditBookmarksEnabled	Enables or disables bookmark editing
EnableDeprecatedWebBasedSignin	Enables the old web-based signin
EnableDeprecatedWebPlatformFeatures	Enable deprecated web platform features for a limited time
EnableMediaRouter	Enables cast
EnableOnlineRevocationChecks	Whether online OCSP/CRL checks are performed
EnableSha1ForLocalAnchors	Whether SHA-1 signed certificates issued by local trust anchors are allowed
EnabledPlugins	Specify a list of enabled plugins

Policy Name	Description
EnterpriseWebStoreName	Enterprise web store name (deprecated)
EnterpriseWebStoreURL	Enterprise web store URL (deprecated)
ExtensionCacheSize	Set Apps and Extensions cache size (in bytes)
ExternalStorageDisabled	Disable mounting of external storage
ExternalStorageReadOnly	Treat external storage devices as read-only.
ForceEphemeralProfiles	Ephemeral profile
ForceGoogleSafeSearch	Force Google SafeSearch
ForceMaximizeOnFirstRun	Maximize the first browser window on first run
ForceSafeSearch	Force SafeSearch
ForceYouTubeRestrict	Force minimum YouTube Restricted Mode
ForceYouTubeSafetyMode	Force YouTube Safety Mode
FullscreenAllowed	Allow fullscreen mode
GCFUserDataDir	Set Google Chrome Frame user data directory
HardwareAccelerationModeEnabled	Use hardware acceleration when available
HeartbeatEnabled	Send network packets to the management server to monitor online status
HeartbeatFrequency	Frequency of monitoring network packets
HideWebStoreIcon	Hide the web store from the New Tab Page and app launcher
HideWebStorePromo	Prevent app promotions from appearing on the new tab page
Http09OnNonDefaultPortsEnabled	Enables HTTP/0.9 support on non-default ports
ImportAutofillFormData	Import autofill form data from default browser on first run
ImportBookmarks	Import bookmarks from default browser on first run
ImportHistory	Import browsing history from default browser on first run
ImportHomepage	Import of homepage from default browser on first run
ImportSavedPasswords	Import saved passwords from default browser on first run
ImportSearchEngine	Import search engines from default browser on first run

Policy Name	Description
IncognitoEnabled	Enable Incognito mode
IncognitoModeAvailability	Incognito mode availability
InstantEnabled	Enable Instant
JavascriptEnabled	Enable JavaScript
KeyPermissions	Key Permissions
LogUploadEnabled	Send system logs to the management server
LoginApps	Configure the list of installed apps on the login screen
LoginAuthenticationBehavior	Configure the login authentication behavior
LoginVideoCaptureAllowedUrls	URLs that will be granted access to video capture devices on SAML login pages
ManagedBookmarks	Managed Bookmarks
MaxConnectionsPerProxy	Maximal number of concurrent connections to the proxy server
MaxInvalidationFetchDelay	Maximum fetch delay after a policy invalidation
MediaCacheSize	Set media disk cache size in bytes
MetricsReportingEnabled	Enable reporting of usage and crash-related data
NTPContentSuggestionsEnabled	Show content suggestions on the New Tab page
NetworkPredictionOptions	Enable network prediction
OpenNetworkConfiguration	User-level network configuration
PacHttpsUrlStrippingEnabled	Enable PAC URL stripping (for https://)
PinnedLauncherApps	List of pinned apps to show in the launcher
PolicyRefreshRate	Refresh rate for user policy
PrintingEnabled	Enable printing
QuicAllowed	Allows QUIC protocol
RC4Enabled	Whether RC4 cipher suites in TLS are enabled
RebootAfterUpdate	Automatically reboot after update
ReportArcStatusEnabled	Report information about status of Android
ReportDeviceActivityTimes	Report device activity times
ReportDeviceBootMode	Report device boot mode
ReportDeviceHardwareStatus	Report hardware status

Policy Name	Description
ReportDeviceNetworkInterfaces	Report device network interfaces
ReportDeviceSessionStatus	Report information about active kiosk sessions
ReportDeviceUsers	Report device users
ReportDeviceVersionInfo	Report OS and firmware version
ReportUploadFrequency	Frequency of device status report uploads
RequireOnlineRevocationChecksForLocalAnchors	Whether online OCSP/CRL checks are required for local trust anchors
RestrictSigninToPattern	Restrict which users are allowed to sign in to Google Chrome
SAMLOfflineSigninTimeLimit	Limit the time for which a user authenticated via SAML can log in offline
SSLErrorOverrideAllowed	Allow proceeding from the SSL warning page
SSLVersionFallbackMin	Minimum TLS version to fallback to
SSLVersionMin	Minimum SSL version enabled
SafeBrowsingEnabled	Enable Safe Browsing
SafeBrowsingExtendedReportingOptInAllowed	Allow users to opt in to Safe Browsing extended reporting
SavingBrowserHistoryDisabled	Disable saving browser history
SearchSuggestEnabled	Enable search suggestions
SessionLengthLimit	Limit the session length
SessionLocales	Set the recommended locales for a public session
ShelfAutoHideBehavior	Control shelf auto-hiding
ShowAppsShortcutInBookmarkBar	Show the apps shortcut in the bookmark bar
ShowHomeButton	Show Home button on toolbar
ShowLogoutButtonInTray	Add a logout button to the system tray
SigninAllowed	Allows sign in to Google Chrome
SpellCheckServiceEnabled	Enable or disable spell checking web service
SuppressChromeFrameTurndownPrompt	Suppress the Google Chrome Frame turndown prompt
SuppressUnsupportedOSWarning	Suppress the unsupported OS warning
SyncDisabled	Disable synchronization of data with Google
SystemTimezone	Timezone

Policy Name	Description
SystemTimezoneAutomaticDetection	Configure the automatic timezone detection method
SystemUse24HourClock	Use 24 hour clock by default
TaskManagerEndProcessEnabled	Enables ending processes in Task Manager
TermsOfServiceURL	Set the Terms of Service for a device-local account
TouchVirtualKeyboardEnabled	Enable virtual keyboard
TranslateEnabled	Enable Translate
URLBlacklist	Block access to a list of URLs
URLWhitelist	Allows access to a list of URLs
UnifiedDesktopEnabledByDefault	Make Unified Desktop available and turn on by default.
UptimeLimit	Limit device uptime by automatically rebooting
UsbDetachableWhitelist	Whitelist of USB detachable devices
UserAvatarImage	User avatar image
UserDataDir	Set user data directory
UserDisplayName	Set the display name for device-local accounts
VideoCaptureAllowed	Allow or deny video capture
VideoCaptureAllowedUrls	URLs that will be granted access to video capture devices without prompt
WPADQuickCheckEnabled	Enable WPAD optimization
WallpaperImage	Wallpaper image
WebRtcUdpPortRange	Restrict the range of local UDP ports used by WebRTC
WelcomePageOnOSUpgradeEnabled	Enable showing the welcome page on the first browser launch following OS upgrade.

Accessibility settings

Configure Google Chrome OS accessibility features.

Back to top

ShowAccessibilityOptionsInSystemTrayMenu

Show accessibility options in system tray menu
Data type:
Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 27

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Show Google Chrome OS accessibility options in the system menu.

If this policy is set to true, Accessibility options always appear in system tray menu.

If this policy is set to false, Accessibility options never appear in system tray menu.

If you set this policy, users cannot change or override it.

If this policy is left unset, Accessibility options will not appear in the system tray menu, but the user can cause the Accessibility options to appear via the Settings page.

Back to top

LargeCursorEnabled

Enable large cursor
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enable the large cursor accessibility feature.

If this policy is set to true, the large cursor will always be enabled.

If this policy is set to false, the large cursor will always be disabled.

If you set this policy, users cannot change or override it.

If this policy is left unset, the large cursor is disabled initially but can be enabled by the user anytime.

Back to top

SpokenFeedbackEnabled

Enable spoken feedback
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enable the spoken feedback accessibility feature.

If this policy is set to true, spoken feedback will always be enabled.

If this policy is set to false, spoken feedback will always be disabled.

If you set this policy, users cannot change or override it.

If this policy is left unset, spoken feedback is disabled initially but can be enabled by the user anytime.

Back to top

HighContrastEnabled

Enable high contrast mode
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enable the high contrast mode accessibility feature.

If this policy is set to true, high contrast mode will always be enabled.

If this policy is set to false, high contrast mode will always be disabled.

If you set this policy, users cannot change or override it.

If this policy is left unset, high contrast mode is disabled initially but can be enabled by the user anytime.

Back to top

VirtualKeyboardEnabled

Enable on-screen keyboard
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 34

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enable the on-screen keyboard accessibility feature.

If this policy is set to true, the on-screen keyboard will always be enabled.

If this policy is set to false, the on-screen keyboard will always be disabled.

If you set this policy, users cannot change or override it.

If this policy is left unset, the on-screen keyboard is disabled initially but can be enabled by the user anytime.

Back to top

KeyboardDefaultToFunctionKeys

Media keys default to function keys
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 35

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Changes the default behaviour of the top row keys to function keys.

If this policy is set to true, the keyboard's top row of keys will produce function key commands per default. The search key has to be pressed to revert their behavior back to media keys.

If this policy is set to false or left unset, the keyboard will produce media key commands per default and function key commands when the search key is held.

Back to top

ScreenMagnifierType

Set screen magnifier type
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Set the type of screen magnifier that is enabled.

If this policy is set, it controls the type of screen magnifier that is enabled. Setting the policy to "None" disables the screen magnifier.

If you set this policy, users cannot change or override it.

If this policy is left unset, the screen magnifier is disabled initially but can be enabled by the user anytime.

- 0 = Screen magnifier disabled
- 1 = Full-screen magnifier enabled

Back to top

DeviceLoginScreenDefaultLargeCursorEnabled

Set default state of the large cursor on the login screen
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes
Description:

Set the default state of the large cursor accessibility feature on the login screen.

If this policy is set to true, the large cursor will be enabled when the login screen is shown.

If this policy is set to false, the large cursor will be disabled when the login screen is shown.

If you set this policy, users can temporarily override it by enabling or disabling the large cursor. However, the user's choice is not persistent and the default is restored whenever the login screen is shown anew or the user remains idle on the login screen for a minute.

If this policy is left unset, the large cursor is disabled when the login screen is first shown. Users can enable or disable the large cursor anytime and its status on the login screen is persisted between users.

Back to top

DeviceLoginScreenDefaultSpokenFeedbackEnabled

Set the default state of spoken feedback on the login screen
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes
Description:

Set the default state of the spoken feedback accessibility feature on the login screen.

If this policy is set to true, spoken feedback will be enabled when the login screen is shown.

If this policy is set to false, spoken feedback will be disabled when the login screen is shown.

If you set this policy, users can temporarily override it by enabling or disabling spoken feedback. However, the user's choice is not persistent and the default is restored whenever the login screen is shown anew or the user remains idle on the login screen for a minute.

If this policy is left unset, spoken feedback is disabled when the login screen is first shown. Users can enable or disable spoken feedback anytime and its status on the login screen is persisted between users.

Back to top

DeviceLoginScreenDefaultHighContrastEnabled

Set the default state of high contrast mode on the login screen

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:

Dynamic Policy Refresh: Yes

Description:

Set the default state of the high contrast mode accessibility feature on the login screen.

If this policy is set to true, high contrast mode will be enabled when the login screen is shown.

If this policy is set to false, high contrast mode will be disabled when the login screen is shown.

If you set this policy, users can temporarily override it by enabling or disabling high contrast mode. However, the user's choice is not persistent and the default is restored whenever the login screen is shown anew or the user remains idle on the login screen for a minute.

If this policy is left unset, high contrast mode is disabled when the login screen is first shown. Users can enable or disable high contrast mode anytime and its status on the login screen is persisted between users.

Back to top

DeviceLoginScreenDefaultVirtualKeyboardEnabled

Set default state of the on-screen keyboard on the login screen

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 34

Supported features:

Dynamic Policy Refresh: Yes

Description:

Set the default state of the on-screen keyboard accessibility feature on the login screen.

If this policy is set to true, the on-screen keyboard will be enabled when the login screen is shown.

If this policy is set to false, the on-screen keyboard will be disabled when the login screen is shown.

If you set this policy, users can temporarily override it by enabling or disabling the on-screen keyboard. However, the user's choice is not persistent and the default is restored whenever the login screen is shown anew or the user remains idle on the login screen for a minute.

If this policy is left unset, the on-screen keyboard is disabled when the login screen is first shown. Users can enable or disable the on-screen keyboard anytime and its status on the login screen is persisted between users.

Back to top

DeviceLoginScreenDefaultScreenMagnifierType

Set the default screen magnifier type enabled on the login screen
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes
Description:

Set the default type of screen magnifier that is enabled on the login screen.

If this policy is set, it controls the type of screen magnifier that is enabled when the login screen is shown. Setting the policy to "None" disables the screen magnifier.

If you set this policy, users can temporarily override it by enabling or disabling the screen magnifier. However, the user's choice is not persistent and the default is restored whenever the login screen is shown anew or the user remains idle on the login screen for a minute.

If this policy is left unset, the screen magnifier is disabled when the login screen is first shown. Users can enable or disable the screen magnifier anytime and its status on the login screen is persisted between users.

- 0 = Screen magnifier disabled
- 1 = Full-screen magnifier enabled

Back to top

Allow Google Chrome Frame to handle the following content types

Allow Google Chrome Frame to handle the following content types.

Back to top

ChromeFrameContentTypes

Allow Google Chrome Frame to handle the listed content types
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\ChromeFrameContentTypes`

Supported on:

- Google Chrome Frame (Windows) since version 8 until version 32

Supported features:
Dynamic Policy Refresh: No
Description:

Allow Google Chrome Frame to handle the listed content types.

If this policy is not set the default renderer will be used for all sites as specified by the 'ChromeFrameRendererSettings' policy.

Example value:
Windows:
```
Software\Policies\Google\Chrome\ChromeFrameContentTypes\1 =
"text/xml"
Software\Policies\Google\Chrome\ChromeFrameContentTypes\2 =
"application/xml"
```
Back to top

Configure Google Drive options

Configure Google Drive in Google Chrome OS.

Back to top

DriveDisabled

Disables Drive in the Google Chrome OS Files app
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Disables Google Drive syncing in the Google Chrome OS Files app when set to True. In that case, no data is uploaded to Google Drive.

If not set or set to False, then users will be able to transfer files to Google Drive.

Note for Google Chrome OS devices supporting Android apps:

This policy does not prevent the user from using the Android Google Drive app. If you want to prevent access to Google Drive, you should disallow installation of the Android Google Drive app as well.

Back to top

DriveDisabledOverCellular

Disables Google Drive over cellular connections in the Google Chrome OS Files app

Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Disables Google Drive syncing in the Google Chrome OS Files app when using a cellular connection when set to True. In that case, data is only synced to Google Drive when connected via WiFi or Ethernet.

If not set or set to False, then users will be able to transfer files to Google Drive via cellular connections.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the Android Google Drive app. If you want to prevent use of Google Drive over cellular connections, you should disallow installation of the Android Google Drive app.

Back to top

Configure remote access options

Configure remote access options in Chrome Remote Desktop host. Chrome Remote Desktop host is a native service that runs on the target machine that a user can connect to using Chrome Remote Desktop application. The native service is packaged and executed separately from the Google Chrome browser. These policies are ignored unless the Chrome Remote Desktop host is installed.

Back to top

RemoteAccessClientFirewallTraversal (deprecated)

Enable firewall traversal from remote access client
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessClientFirewallTraversal`
Mac/Linux preference name:
`RemoteAccessClientFirewallTraversal`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 14 until version 16
- Google Chrome OS (Google Chrome OS) since version 14 until version 16

Supported features:
Dynamic Policy Refresh: Yes
Description:

This policy is no longer supported. Enables usage of STUN and relay servers when connecting to a remote client.

If this setting is enabled, then this machine can discover and connect to remote host machines even if they are separated by a firewall.

If this setting is disabled and outgoing UDP connections are filtered by the firewall, then this machine can only connect to host machines within the local network.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

RemoteAccessHostClientDomain

Configure the required domain name for remote access clients

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostClientDomain`

Mac/Linux preference name:
`RemoteAccessHostClientDomain`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Configures the required client domain name that will be imposed on remote access clients and prevents users from changing it.

If this setting is enabled, then only clients from the specified domain can connect to the host.

If this setting is disabled or not set, then the default policy for the connection type is applied. For remote assistance, this allows clients from any domain can connect to the host; for anytime remote access, only the host owner can connect.

See also RemoteAccessHostDomain.

Example value:
"my-awesome-domain.com"

Back to top

RemoteAccessHostFirewallTraversal

Enable firewall traversal from remote access host

Data type:
Boolean [Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostFirewallTraversal`

Mac/Linux preference name:
`RemoteAccessHostFirewallTraversal`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 14
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Enables usage of STUN servers when remote clients are trying to establish a connection to this machine.

If this setting is enabled, then remote clients can discover and connect to this machines even if they are separated by a firewall.

If this setting is disabled and outgoing UDP connections are filtered by the firewall, then this machine will only allow connections from client machines within the local network.

If this policy is left not set the setting will be enabled.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

RemoteAccessHostDomain

Configure the required domain name for remote access hosts
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostDomain`
Mac/Linux preference name:
`RemoteAccessHostDomain`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Configures the required host domain name that will be imposed on remote access hosts and prevents users from changing it.

If this setting is enabled, then hosts can be shared only using accounts registered on the specified domain name.

If this setting is disabled or not set, then hosts can be shared using any account.

See also RemoteAccessHostClientDomain.

Example value:
"my-awesome-domain.com"
Back to top

RemoteAccessHostRequireTwoFactor (deprecated)

Enable two-factor authentication for remote access hosts
Data type:
Boolean [Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostRequireTwoFactor`
Mac/Linux preference name:
`RemoteAccessHostRequireTwoFactor`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22 until version 22

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Enables two-factor authentication for remote access hosts instead of a user-specified PIN.

If this setting is enabled, then users must provide a valid two-factor code when accessing a host.

If this setting is disabled or not set, then two-factor will not be enabled and the default behavior of having a user-defined PIN will be used.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

RemoteAccessHostTalkGadgetPrefix

Configure the TalkGadget prefix for remote access hosts
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostTalkGadgetPrefix`
Mac/Linux preference name:
`RemoteAccessHostTalkGadgetPrefix`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Configures the TalkGadget prefix that will be used by remote access hosts and prevents users from changing it.

If specified, this prefix is prepended to the base TalkGadget name to create a full domain name for the TalkGadget. The base TalkGadget domain name is '.talkgadget.google.com'.

If this setting is enabled, then hosts will use the custom domain name when accessing the TalkGadget instead of the default domain name.

If this setting is disabled or not set, then the default TalkGadget domain name ('chromoting-host.talkgadget.google.com') will be used for all hosts.

Remote access clients are not affected by this policy setting. They will always use 'chromoting-client.talkgadget.google.com' to access the TalkGadget.

Example value:
"chromoting-host"
Back to top

RemoteAccessHostRequireCurtain

Enable curtaining of remote access hosts
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostRequireCurtain`
Mac/Linux preference name:
`RemoteAccessHostRequireCurtain`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 23
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Enables curtaining of remote access hosts while a connection is in progress.

If this setting is enabled, then hosts' physical input and output devices are disabled while a remote connection is in progress.

If this setting is disabled or not set, then both local and remote users can interact with the host when it is being shared.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

RemoteAccessHostAllowClientPairing

Enable or disable PIN-less authentication for remote access hosts
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostAllowClientPairing`
Mac/Linux preference name:
`RemoteAccessHostAllowClientPairing`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 30
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If this setting is enabled or not configured, then users can opt to pair clients and hosts at connection time, eliminating the need to enter a PIN every time.

If this setting is disabled, then this feature will not be available.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

RemoteAccessHostAllowGnubbyAuth

Allow gnubby authentication for remote access hosts
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostAllowGnubbyAuth`
Mac/Linux preference name:
`RemoteAccessHostAllowGnubbyAuth`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 35
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If this setting is enabled, then gnubby authentication requests will be proxied across a remote host connection.

If this setting is disabled or not configured, gnubby authentication requests will not be proxied.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

RemoteAccessHostAllowRelayedConnection

Enable the use of relay servers by the remote access host
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostAllowRelayedConnection`
Mac/Linux preference name:
`RemoteAccessHostAllowRelayedConnection`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 36
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Enables usage of relay servers when remote clients are trying to establish a connection to this machine.

If this setting is enabled, then remote clients can use relay servers to connect to this machine when a direct connection is not available (e.g. due to firewall restrictions).

Note that if the policy RemoteAccessHostFirewallTraversal is disabled, this policy will be ignored.

If this policy is left not set the setting will be enabled.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

RemoteAccessHostUdpPortRange

Restrict the UDP port range used by the remote access host
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostUdpPortRange`
Mac/Linux preference name:
`RemoteAccessHostUdpPortRange`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 36
- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Restricts the UDP port range used by the remote access host in this machine.

If this policy is left not set, or if it is set to an empty string, the remote access host will be allowed to use any available port, unless the policy RemoteAccessHostFirewallTraversal is disabled, in which case the remote access host will use UDP ports in the 12400-12409 range.

Example value:
"12400-12409"
Back to top

RemoteAccessHostMatchUsername

Requires that the name of the local user and the remote access host owner match
Data type:
Boolean
Mac/Linux preference name:
`RemoteAccessHostMatchUsername`
Supported on:

- Google Chrome (Linux) since version 25
- Google Chrome (Mac) since version 25
- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Requires that the name of the local user and the remote access host owner match.

If this setting is enabled, then the remote access host compares the name of the local user (that the host is associated with) and the name of the Google account registered as the host owner (i.e. "johndoe" if the host is owned by "johndoe@example.com" Google account). The remote access host will not start if the name of the host owner is different from the name of the local user that the host is associated with. RemoteAccessHostMatchUsername policy should be used together with RemoteAccessHostDomain to also enforce that the Google account of the host owner is associated with a specific domain (i.e. "example.com").

If this setting is disabled or not set, then the remote access host can be associated with any local user.

Example value:
false (Linux), <false /> (Mac)

Back to top

RemoteAccessHostTokenUrl

URL where remote access clients should obtain their authentication token

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostTokenUrl`

Mac/Linux preference name:
`RemoteAccessHostTokenUrl`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 28
- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No

Description:

URL where remote access clients should obtain their authentication token.

If this policy is set, the remote access host will require authenticating clients to obtain an authentication token from this URL in order to connect. Must be used in conjunction with RemoteAccessHostTokenValidationUrl.

This feature is currently disabled server-side.

Example value:
"https://example.com/issue"

Back to top

RemoteAccessHostTokenValidationUrl

URL for validating remote access client authentication token

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostTokenValidationUrl`

Mac/Linux preference name:
`RemoteAccessHostTokenValidationUrl`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 28
- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

URL for validating remote access client authentication token.

If this policy is set, the remote access host will use this URL to validate authentication tokens from remote access clients, in order to accept connections. Must be used in conjunction with RemoteAccessHostTokenUrl.

This feature is currently disabled server-side.

Example value:
"https://example.com/validate"
Back to top

RemoteAccessHostTokenValidationCertificateIssuer

Client certificate for connecting to RemoteAccessHostTokenValidationUrl
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostTokenValidationCertificateIssuer`
Mac/Linux preference name:
`RemoteAccessHostTokenValidationCertificateIssuer`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 28
- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Client certificate for connecting to RemoteAccessHostTokenValidationUrl.

If this policy is set, the host will use a client certificate with the given issuer CN to authenticate to RemoteAccessHostTokenValidationUrl. Set it to "*" to use any available client certificate.

This feature is currently disabled server-side.

Example value:
"Example Certificate Authority"
Back to top

RemoteAccessHostDebugOverridePolicies

Policy overrides for Debug builds of the remote access host
Data type:
String [Windows:REG_SZ]
Windows registry location:

`Software\Policies\Google\Chrome\RemoteAccessHostDebugOverridePolicies`

Mac/Linux preference name:
`RemoteAccessHostDebugOverridePolicies`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25 until version 47
- Google Chrome OS (Google Chrome OS) since version 42 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Overrides policies on Debug builds of the remote access host.

The value is parsed as a JSON dictionary of policy name to policy value mappings.

Example value:
"{ "RemoteAccessHostMatchUsername": true }"

Back to top

RemoteAccessHostAllowUiAccessForRemoteAssistance

Allow remote users to interact with elevated windows in remote assistance sessions

Data type:
Boolean [Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\RemoteAccessHostAllowUiAccessForRemoteAssistance`

Supported on:

- Google Chrome (Windows) since version 55

Supported features:
Dynamic Policy Refresh: No, Per Profile: No

Description:

If this setting is enabled, the remote assistance host will be run in a process with uiAccess permissions. This will allow remote users to interact with elevated windows on the local user's desktop.

If this setting is disabled or not configured, the remote assistance host will run in the user's context and remote users cannot interact with elevated windows on the desktop.

Example value:
0x00000001 (Windows)

Back to top

Content Settings

Content Settings allow you to specify how contents of a specific type (for example Cookies, Images or JavaScript) is handled.

Back to top

DefaultCookiesSetting

Default cookies setting

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultCookiesSetting`

Mac/Linux preference name:

`DefaultCookiesSetting`

Android restriction name:

`DefaultCookiesSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to set local data. Setting local data can be either allowed for all websites or denied for all websites.

If this policy is set to 'Keep cookies for the duration of the session' then cookies will be cleared when the session closes. Note that if Google Chrome is running in 'background mode', the session may not close when the last window is closed. Please see the 'BackgroundModeEnabled' policy for more information about configuring this behavior.

If this policy is left not set, 'AllowCookies' will be used and the user will be able to change it.

- 1 = Allow all sites to set local data
- 2 = Do not allow any site to set local data
- 4 = Keep cookies for the duration of the session

Example value:

0x00000001 (Windows), 1 (Linux), 1 (Android), 1 (Mac)

Back to top

DefaultImagesSetting

Default images setting

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultImagesSetting`

Mac/Linux preference name:

`DefaultImagesSetting`

Android restriction name:

`DefaultImagesSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to display images. Displaying images can be either allowed for all websites or denied for all websites.

If this policy is left not set, 'AllowImages' will be used and the user will be able to change it.

- 1 = Allow all sites to show all images
- 2 = Do not allow any site to show images

Example value:

0x00000001 (Windows), 1 (Linux), 1 (Android), 1 (Mac)

Back to top

DefaultJavaScriptSetting

Default JavaScript setting

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultJavaScriptSetting`

Mac/Linux preference name:

`DefaultJavaScriptSetting`

Android restriction name:

`DefaultJavaScriptSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to run JavaScript. Running JavaScript can be either allowed for all websites or denied for all websites.

If this policy is left not set, 'AllowJavaScript' will be used and the user will be able to change it.

- 1 = Allow all sites to run JavaScript
- 2 = Do not allow any site to run JavaScript

Example value:

0x00000001 (Windows), 1 (Linux), 1 (Android), 1 (Mac)

Back to top

DefaultPluginsSetting

Default plugins setting

Data type:

Integer [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultPluginsSetting`

Mac/Linux preference name:

`DefaultPluginsSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to automatically run plugins. Automatically running plugins can be either allowed for all websites or denied for all websites.

Click to play allows plugins to run but the user must click them to start their execution.

If this policy is left not set, 'AllowPlugins' will be used and the user will be able to change it.

- 1 = Allow all sites to automatically run plugins
- 2 = Block all plugins
- 3 = Click to play

Example value:

0x00000001 (Windows), 1 (Linux), 1 (Mac)

Back to top

DefaultPopupsSetting

Default popups setting

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultPopupsSetting`

Mac/Linux preference name:

`DefaultPopupsSetting`

Android restriction name:

`DefaultPopupsSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (iOS) since version 34 until version 47
- Google Chrome (Android) since version 33

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to show pop-ups. Showing popups can be either allowed for all websites or denied for all websites.

If this policy is left not set, 'BlockPopups' will be used and the user will be able to change it.

- 1 = Allow all sites to show pop-ups
- 2 = Do not allow any site to show popups

Example value:

0x00000001 (Windows), 1 (Linux), 1 (Android), 1 (Mac)

Back to top

DefaultNotificationsSetting

Default notification setting

Data type:

Integer [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultNotificationsSetting`

Mac/Linux preference name:

`DefaultNotificationsSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to display desktop notifications. Displaying desktop notifications can be allowed by default, denied by default or the user can be asked every time a website wants to show desktop notifications.

If this policy is left not set, 'AskNotifications' will be used and the user will be able to change it.

- 1 = Allow sites to show desktop notifications
- 2 = Do not allow any site to show desktop notifications
- 3 = Ask every time a site wants to show desktop notifications

Example value:

0x00000002 (Windows), 2 (Linux), 2 (Mac)

Back to top

DefaultGeolocationSetting

Default geolocation setting

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultGeolocationSetting`

Mac/Linux preference name:

`DefaultGeolocationSetting`

Android restriction name:

`DefaultGeolocationSetting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set whether websites are allowed to track the users' physical location. Tracking the users' physical location can be allowed by default, denied by default or the user can be asked every time a website requests the physical location.

If this policy is left not set, 'AskGeolocation' will be used and the user will be able to change it.

- 1 = Allow sites to track the users' physical location
- 2 = Do not allow any site to track the users' physical location
- 3 = Ask whenever a site wants to track the users' physical location

Note for Google Chrome OS devices supporting Android apps:

If this policy is set to BlockGeolocation, Android apps cannot access location information. If you set this policy to any other value or leave it unset, the user is asked to consent when an Android app wants to access location information.

Example value:
0x00000000 (Windows), 0 (Linux), 0 (Android), 0 (Mac)

Back to top

DefaultMediaStreamSetting (deprecated)

Default mediastream setting
Data type:
Integer [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultMediaStreamSetting`
Mac/Linux preference name:
`DefaultMediaStreamSetting`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22
- Google Chrome OS (Google Chrome OS) since version 22

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set whether websites are allowed to get access to media capture devices. Access to media capture devices can be allowed by default, or the user can be asked every time a website wants to get access to media capture devices.

If this policy is left not set, 'PromptOnAccess' will be used and the user will be able to change it.

- 2 = Do not allow any site to access the camera and microphone
- 3 = Ask every time a site wants to access the camera and/or microphone

Example value:
0x00000002 (Windows), 2 (Linux), 2 (Mac)

Back to top

DefaultWebBluetoothGuardSetting

Control use of the Web Bluetooth API
Data type:
Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\DefaultWebBluetoothGuardSetting`
Mac/Linux preference name:
`DefaultWebBluetoothGuardSetting`
Android restriction name:
`DefaultWebBluetoothGuardSetting`
Supported on:

- Google Chrome OS (Google Chrome OS) since version 50
- Google Chrome (Android) since version 50
- Google Chrome (Linux, Mac, Windows) since version 50

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set whether websites are allowed to get access to nearby Bluetooth devices. Access can be completely blocked, or the user can be asked every time a website wants to get access to nearby Bluetooth devices.

If this policy is left not set, '3' will be used, and the user will be able to change it.

- 2 = Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API
- 3 = Allow sites to ask the user to grant access to a nearby Bluetooth device

Example value:
0x00000002 (Windows), 2 (Linux), 2 (Android), 2 (Mac)
Back to top

DefaultKeygenSetting

Default key generation setting
Data type:
Integer [Android:choice, Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultKeygenSetting`
Mac/Linux preference name:
`DefaultKeygenSetting`
Android restriction name:
`DefaultKeygenSetting`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 49
- Google Chrome OS (Google Chrome OS) since version 49
- Google Chrome (Android) since version 49

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set whether websites are allowed to use key generation. Using key generation can be either allowed for all websites or denied for all websites.

If this policy is left not set, 'BlockKeygen' will be used and the user will be able to change it.

- 1 = Allow all sites to use key generation

- 2 = Do not allow any site to use key generation

Example value:
0x00000002 (Windows), 2 (Linux), 2 (Android), 2 (Mac)
Back to top

AutoSelectCertificateForUrls

Automatically select client certificates for these sites
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\AutoSelectCertificateForUrls`
Mac/Linux preference name:
`AutoSelectCertificateForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15
- Google Chrome OS (Google Chrome OS) since version 15

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to specify a list of url patterns that specify sites for which Google Chrome should automatically select a client certificate, if the site requests a certificate.

The value must be an array of stringified JSON dictionaries. Each dictionary must have the form { "pattern": "$URL_PATTERN", "filter" : $FILTER }, where $URL_PATTERN is a content setting pattern. $FILTER restricts from which client certificates the browser will automatically select. Independent of the filter, only certificates will be selected that match the server's certificate request. If $FILTER has the form { "ISSUER": { "CN": "$ISSUER_CN" } }, additionally only client certificates are selected that are issued by a certificate with the CommonName $ISSUER_CN. If $FILTER is the empty dictionary {}, the selection of client certificates is not additionally restricted.

If this policy is left not set, no auto-selection will be done for any site.

Example value:
Windows:
```
Software\Policies\Google\Chrome\AutoSelectCertificateForUrls\1 =
"{\"pattern\":\"https://www.example.com\",\"filter\":{\"ISSUER\":{
\"CN\":\"certificate issuer name\"}}}"
```
Android/Linux:
```
["{\"pattern\":\"https://www.example.com\",\"filter\":{\"ISSUER\":
{\"CN\":\"certificate issuer name\"}}}"]
```
Mac:
```
<array>

<string>{\"pattern\":\"https://www.example.com\",\"filter\":{\"ISS
UER\":{\"CN\":\"certificate issuer name\"}}}</string>
</array>
```
Back to top

CookiesAllowedForUrls

Allow cookies on these sites

Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\CookiesAllowedForUrls`
Mac/Linux preference name:
`CookiesAllowedForUrls`
Android restriction name:
`CookiesAllowedForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set a list of url patterns that specify sites which are allowed to set cookies.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultCookiesSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:
Windows:
```
Software\Policies\Google\Chrome\CookiesAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\CookiesAllowedForUrls\2 =
"[*.]example.edu"
```
Android/Linux:
```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

CookiesBlockedForUrls

Block cookies on these sites
Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\CookiesBlockedForUrls`
Mac/Linux preference name:
`CookiesBlockedForUrls`
Android restriction name:
`CookiesBlockedForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11

- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set a list of url patterns that specify sites which are not allowed to set cookies.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultCookiesSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:
Windows:
```
Software\Policies\Google\Chrome\CookiesBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\CookiesBlockedForUrls\2 =
"[*.]example.edu"
```
Android/Linux:
```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

CookiesSessionOnlyForUrls

Allow session only cookies on these sites
Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\CookiesSessionOnlyForUrls`
Mac/Linux preference name:
`CookiesSessionOnlyForUrls`
Android restriction name:
`CookiesSessionOnlyForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set a list of url patterns that specify sites which are allowed to set session only cookies.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultCookiesSetting' policy if it is set, or the user's personal configuration otherwise.

Note that if Google Chrome is running in 'background mode', the session may not be closed when the last browser window is closed, but will instead stay active until the browser exits. Please see the 'BackgroundModeEnabled' policy for more information about configuring this behavior.

If the "RestoreOnStartup" policy is set to restore URLs from previous sessions this policy will not be respected and cookies will be stored permanently for those sites.

Example value:

Windows:

```
Software\Policies\Google\Chrome\CookiesSessionOnlyForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\CookiesSessionOnlyForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

ImagesAllowedForUrls

Allow images on these sites

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\ImagesAllowedForUrls`

Mac/Linux preference name:

`ImagesAllowedForUrls`

Android restriction name:

`ImagesAllowedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are allowed to display images.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultImagesSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\ImagesAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\ImagesAllowedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

ImagesBlockedForUrls

Block images on these sites

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\ImagesBlockedForUrls`

Mac/Linux preference name:

`ImagesBlockedForUrls`

Android restriction name:

`ImagesBlockedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are not allowed to display images.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultImagesSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:
```
Software\Policies\Google\Chrome\ImagesBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\ImagesBlockedForUrls\2 =
"[*.]example.edu"
```
Android/Linux:
```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

JavaScriptAllowedForUrls

Allow JavaScript on these sites

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:
`Software\Policies\Google\Chrome\JavaScriptAllowedForUrls`
Mac/Linux preference name:
`JavaScriptAllowedForUrls`
Android restriction name:
`JavaScriptAllowedForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set a list of url patterns that specify sites which are allowed to run JavaScript.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultJavaScriptSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:
Windows:
```
Software\Policies\Google\Chrome\JavaScriptAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\JavaScriptAllowedForUrls\2 =
"[*.]example.edu"
```
Android/Linux:
```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

JavaScriptBlockedForUrls

Block JavaScript on these sites
Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\JavaScriptBlockedForUrls`
Mac/Linux preference name:
`JavaScriptBlockedForUrls`
Android restriction name:
`JavaScriptBlockedForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are not allowed to run JavaScript.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultJavaScriptSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\JavaScriptBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\JavaScriptBlockedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

KeygenAllowedForUrls

Allow key generation on these sites

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\KeygenAllowedForUrls`

Mac/Linux preference name:

`KeygenAllowedForUrls`

Android restriction name:

`KeygenAllowedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 49
- Google Chrome OS (Google Chrome OS) since version 49
- Google Chrome (Android) since version 49

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are allowed to use key generation. If a url pattern is in 'KeygenBlockedForUrls', that overrides these exceptions.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultKeygenSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\KeygenAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\KeygenAllowedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:
```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

KeygenBlockedForUrls

Block key generation on these sites
Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\KeygenBlockedForUrls`
Mac/Linux preference name:
`KeygenBlockedForUrls`
Android restriction name:
`KeygenBlockedForUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 49
- Google Chrome OS (Google Chrome OS) since version 49
- Google Chrome (Android) since version 49

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to set a list of url patterns that specify sites which are not allowed to use key generation. If a url pattern is in 'KeygenAllowedForUrls', this policy overrides these exceptions.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultKeygenSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:
Windows:
```
Software\Policies\Google\Chrome\KeygenBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\KeygenBlockedForUrls\2 =
"[*.]example.edu"
```
Android/Linux:
```
["https://www.example.com", "[*.]example.edu"]
```
Mac:
```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```
Back to top

PluginsAllowedForUrls

Allow plugins on these sites
Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\PluginsAllowedForUrls`

Mac/Linux preference name:

`PluginsAllowedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are allowed to run plugins.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultPluginsSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\PluginsAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\PluginsAllowedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

PluginsBlockedForUrls

Block plugins on these sites

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\PluginsBlockedForUrls`

Mac/Linux preference name:

`PluginsBlockedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are not allowed to run plugins.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultPluginsSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\PluginsBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\PluginsBlockedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

PopupsAllowedForUrls

Allow popups on these sites

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\PopupsAllowedForUrls`

Mac/Linux preference name:

`PopupsAllowedForUrls`

Android restriction name:

`PopupsAllowedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (iOS) since version 34 until version 47
- Google Chrome (Android) since version 34

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are allowed to open popups.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultPopupsSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\PopupsAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\PopupsAllowedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

RegisteredProtocolHandlers

Register protocol handlers

Data type:

Dictionary [Windows:REG_SZ] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\Recommended\RegisteredProtocolHandlers`

Mac/Linux preference name:

`RegisteredProtocolHandlers`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 37
- Google Chrome OS (Google Chrome OS) since version 37

Supported features:

Can Be Mandatory: No, Can Be Recommended: Yes, Dynamic Policy Refresh: No, Per Profile: Yes

Description:

Allows you to register a list of protocol handlers. This can only be a recommended policy. The property |protocol| should be set to the scheme such as 'mailto' and the property |url| should be set to the URL pattern of the application that handles the scheme. The pattern can include a '%s', which if present will be replaced by the handled URL.

The protocol handlers registered by policy are merged with the ones registered by the user and both are available for use. The user can override the protocol handlers installed by policy by installing a new default handler, but cannot remove a protocol handler registered by policy.

Note for Google Chrome OS devices supporting Android apps:

The protocol handlers set via this policy are not used when handling Android intents.

Example value:

Windows:

```
Software\Policies\Google\Chrome\Recommended\RegisteredProtocolHandlers = [{"url": "https://mail.google.com/mail/?extsrc=mailto&url=%s", "default": true, "protocol": "mailto"}]
```

Android/Linux:

```
RegisteredProtocolHandlers: [{"url": "https://mail.google.com/mail/?extsrc=mailto&url=%s", "default": true, "protocol": "mailto"}]
```

Mac:

```
<key>RegisteredProtocolHandlers</key>
<array>
  <dict>
    <key>default</key>
    <true/>
    <key>protocol</key>
    <string>mailto</string>
    <key>url</key>
```

```
<string>https://mail.google.com/mail/?extsrc=mailto&url=%s</string
>
  </dict>
</array>
```

Back to top

PopupsBlockedForUrls

Block popups on these sites

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\PopupsBlockedForUrls`

Mac/Linux preference name:

`PopupsBlockedForUrls`

Android restriction name:

`PopupsBlockedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (iOS) since version 34 until version 47
- Google Chrome (Android) since version 34

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are not allowed to open popups.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultPopupsSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\PopupsBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\PopupsBlockedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

NotificationsAllowedForUrls

Allow notifications on these sites

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\NotificationsAllowedForUrls`

Mac/Linux preference name:

`NotificationsAllowedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 16
- Google Chrome OS (Google Chrome OS) since version 16

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are allowed to display notifications.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultNotificationsSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\NotificationsAllowedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\NotificationsAllowedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

NotificationsBlockedForUrls

Block notifications on these sites

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\NotificationsBlockedForUrls`

Mac/Linux preference name:

`NotificationsBlockedForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 16
- Google Chrome OS (Google Chrome OS) since version 16

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to set a list of url patterns that specify sites which are not allowed to display notifications.

If this policy is left not set the global default value will be used for all sites either from the 'DefaultNotificationsSetting' policy if it is set, or the user's personal configuration otherwise.

Example value:

Windows:

```
Software\Policies\Google\Chrome\NotificationsBlockedForUrls\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\NotificationsBlockedForUrls\2 =
"[*.]example.edu"
```

Android/Linux:

```
["https://www.example.com", "[*.]example.edu"]
```

Mac:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

Default HTML renderer for Google Chrome Frame

Allows you to configure the default HTML renderer when Google Chrome Frame is installed. The default setting is to allow the host browser do the rendering, but you can optionally override this and have Google Chrome Frame render HTML pages by default.

Back to top

ChromeFrameRendererSettings

Default HTML renderer for Google Chrome Frame

Data type:

Integer [Windows:REG_DWORD]

Windows registry location:

```
Software\Policies\Google\Chrome\ChromeFrameRendererSettings
```

Supported on:

- Google Chrome Frame (Windows) since version 8 until version 32

Supported features:

Dynamic Policy Refresh: No

Description:

Allows you to configure the default HTML renderer when Google Chrome Frame is installed. The default setting used when this policy is left not set is to allow the host browser do the rendering, but you can optionally override this and have Google Chrome Frame render HTML pages by default.

- 0 = Use the host browser by default
- 1 = Use Google Chrome Frame by default

Example value:

0x00000001 (Windows)

Back to top

RenderInChromeFrameList

Always render the following URL patterns in Google Chrome Frame

Data type:

List of strings

Windows registry location:

```
Software\Policies\Google\Chrome\RenderInChromeFrameList
```

Supported on:

- Google Chrome Frame (Windows) since version 8 until version 32

Supported features:
Dynamic Policy Refresh: No
Description:

Customize the list of URL patterns that should always be rendered by Google Chrome Frame.

If this policy is not set the default renderer will be used for all sites as specified by the 'ChromeFrameRendererSettings' policy.

For example patterns see https://www.chromium.org/developers/how-tos/chrome-frame-getting-started.

Example value:
Windows:
```
Software\Policies\Google\Chrome\RenderInChromeFrameList\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\RenderInChromeFrameList\2 =
"https://www.example.edu"
```
Back to top

RenderInHostList

Always render the following URL patterns in the host browser
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\RenderInHostList`
Supported on:

- Google Chrome Frame (Windows) since version 8 until version 32

Supported features:
Dynamic Policy Refresh: No
Description:

Customize the list of URL patterns that should always be rendered by the host browser.

If this policy is not set the default renderer will be used for all sites as specified by the 'ChromeFrameRendererSettings' policy.

For example patterns see https://www.chromium.org/developers/how-tos/chrome-frame-getting-started.

Example value:
Windows:
```
Software\Policies\Google\Chrome\RenderInHostList\1 =
"https://www.example.com"
Software\Policies\Google\Chrome\RenderInHostList\2 =
"https://www.example.edu"
```
Back to top

AdditionalLaunchParameters

Additional command line parameters for Google Chrome

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\AdditionalLaunchParameters`

Supported on:

- Google Chrome Frame (Windows) since version 19 until version 32

Supported features:

Dynamic Policy Refresh: No

Description:

Allows you to specify additional parameters that are used when Google Chrome Frame launches Google Chrome.

If this policy is not set the default command line will be used.

Example value:

"--enable-media-stream --enable-media-source"

Back to top

SkipMetadataCheck

Skip the meta tag check in Google Chrome Frame

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\SkipMetadataCheck`

Supported on:

- Google Chrome Frame (Windows) since version 31 until version 32

Supported features:

Dynamic Policy Refresh: No

Description:

Normally pages with X-UA-Compatible set to chrome=1 will be rendered in Google Chrome Frame regardless of the 'ChromeFrameRendererSettings' policy.

If you enable this setting, pages will not be scanned for meta tags.

If you disable this setting, pages will be scanned for meta tags.

If this policy is not set, pages will be scanned for meta tags.

Example value:

0x00000000 (Windows)

Back to top

Default search provider

Configures the default search provider. You can specify the default search provider that the user will use or choose to disable default search.

Back to top

DefaultSearchProviderEnabled

Enable the default search provider

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultSearchProviderEnabled`

Mac/Linux preference name:

`DefaultSearchProviderEnabled`

Android restriction name:

`DefaultSearchProviderEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables the use of a default search provider.

If you enable this setting, a default search is performed when the user types text in the omnibox that is not a URL.

You can specify the default search provider to be used by setting the rest of the default search policies. If these are left empty, the user can choose the default provider.

If you disable this setting, no search is performed when the user enters non-URL text in the omnibox.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

If this policy is left not set, the default search provider is enabled, and the user will be able to set the search provider list.

This policy is not available on Windows instances that are not joined to an Active Directory domain.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

DefaultSearchProviderName

Default search provider name

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultSearchProviderName`

Mac/Linux preference name:

`DefaultSearchProviderName`

Android restriction name:

`DefaultSearchProviderName`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the name of the default search provider. If left empty or not set, the host name specified by the search URL will be used.

This policy is only considered if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"My Intranet Search"
Back to top

DefaultSearchProviderKeyword

Default search provider keyword
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderKeyword`
Mac/Linux preference name:
`DefaultSearchProviderKeyword`
Android restriction name:
`DefaultSearchProviderKeyword`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the keyword, which is the shortcut used in the omnibox to trigger the search for this provider.

This policy is optional. If not set, no keyword will activate the search provider.

This policy is only considered if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"mis"
Back to top

DefaultSearchProviderSearchURL

Default search provider search URL

Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderSearchURL`
Mac/Linux preference name:
`DefaultSearchProviderSearchURL`
Android restriction name:
`DefaultSearchProviderSearchURL`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the URL of the search engine used when doing a default search. The URL should contain the string '{searchTerms}', which will be replaced at query time by the terms the user is searching for.

Google's search URL can be specified as: '{google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:searchClient}{google:sourceId}{google:instantExtendedEnabledParameter}ie={inputEncoding}'.

This option must be set when the 'DefaultSearchProviderEnabled' policy is enabled and will only be respected if this is the case.

Example value:
"https://search.my.company/search?q={searchTerms}"
Back to top

DefaultSearchProviderSuggestURL

Default search provider suggest URL
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderSuggestURL`
Mac/Linux preference name:
`DefaultSearchProviderSuggestURL`
Android restriction name:
`DefaultSearchProviderSuggestURL`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the URL of the search engine used to provide search suggestions. The URL should contain the string '{searchTerms}', which will be replaced at query time by the text the user has entered so far.

This policy is optional. If not set, no suggest URL will be used.

Google's suggest URL can be specified as: '{google:baseURL}complete/search?output=chrome&q={searchTerms}'.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"https://search.my.company/suggest?q={searchTerms}"

Back to top

DefaultSearchProviderInstantURL

Default search provider instant URL

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderInstantURL`

Mac/Linux preference name:
`DefaultSearchProviderInstantURL`

Android restriction name:
`DefaultSearchProviderInstantURL`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Specifies the URL of the search engine used to provide instant results. The URL should contain the string '{searchTerms}', which will be replaced at query time by the text the user has entered so far.

This policy is optional. If not set, no instant search results will be provided.

Google's instant results URL can be specified as: '{google:baseURL}suggest?q={searchTerms}'.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"https://search.my.company/suggest?q={searchTerms}"

Back to top

DefaultSearchProviderIconURL

Default search provider icon

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderIconURL`

Mac/Linux preference name:
`DefaultSearchProviderIconURL`
Android restriction name:
`DefaultSearchProviderIconURL`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the favorite icon URL of the default search provider.

This policy is optional. If not set, no icon will be present for the search provider.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"https://search.my.company/favicon.ico"
Back to top

DefaultSearchProviderEncodings

Default search provider encodings
Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderEncodings`
Mac/Linux preference name:
`DefaultSearchProviderEncodings`
Android restriction name:
`DefaultSearchProviderEncodings`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the character encodings supported by the search provider. Encodings are code page names like UTF-8, GB2312, and ISO-8859-1. They are tried in the order provided.

This policy is optional. If not set, the default will be used which is UTF-8.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
Windows:

```
Software\Policies\Google\Chrome\DefaultSearchProviderEncodings\1 =
"UTF-8"
Software\Policies\Google\Chrome\DefaultSearchProviderEncodings\2 =
"UTF-16"
Software\Policies\Google\Chrome\DefaultSearchProviderEncodings\3 =
"GB2312"
Software\Policies\Google\Chrome\DefaultSearchProviderEncodings\4 =
"ISO-8859-1"
```

Android/Linux:

```
["UTF-8", "UTF-16", "GB2312", "ISO-8859-1"]
```

Mac:

```
<array>
  <string>UTF-8</string>
  <string>UTF-16</string>
  <string>GB2312</string>
  <string>ISO-8859-1</string>
</array>
```

Back to top

DefaultSearchProviderAlternateURLs

List of alternate URLs for the default search provider

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\DefaultSearchProviderAlternateURLs`

Mac/Linux preference name:

`DefaultSearchProviderAlternateURLs`

Android restriction name:

`DefaultSearchProviderAlternateURLs`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 24
- Google Chrome OS (Google Chrome OS) since version 24
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Specifies a list of alternate URLs that can be used to extract search terms from the search engine. The URLs should contain the string '{searchTerms}', which will be used to extract the search terms.

This policy is optional. If not set, no alternate urls will be used to extract search terms.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:

Windows:

```
Software\Policies\Google\Chrome\DefaultSearchProviderAlternateURLs
\1 = "https://search.my.company/suggest#q={searchTerms}"
Software\Policies\Google\Chrome\DefaultSearchProviderAlternateURLs
\2 = "https://search.my.company/suggest/search#q={searchTerms}"
```

Android/Linux:

```
["https://search.my.company/suggest#q={searchTerms}",
"https://search.my.company/suggest/search#q={searchTerms}"]
```

Mac:

```
<array>

<string>https://search.my.company/suggest#q={searchTerms}</string>

<string>https://search.my.company/suggest/search#q={searchTerms}</
string>
</array>
```

Back to top

DefaultSearchProviderSearchTermsReplacementKey

Parameter controlling search term placement for the default search provider

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultSearchProviderSearchTermsReplacementKey`

Mac/Linux preference name:

`DefaultSearchProviderSearchTermsReplacementKey`

Android restriction name:

`DefaultSearchProviderSearchTermsReplacementKey`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25
- Google Chrome OS (Google Chrome OS) since version 25
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

If this policy is set and a search URL suggested from the omnibox contains this parameter in the query string or in the fragment identifier, then the suggestion will show the search terms and search provider instead of the raw search URL.

This policy is optional. If not set, no search term replacement will be performed.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:

"espv"

Back to top

DefaultSearchProviderImageURL

Parameter providing search-by-image feature for the default search provider

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultSearchProviderImageURL`

Mac/Linux preference name:

`DefaultSearchProviderImageURL`

Android restriction name:

`DefaultSearchProviderImageURL`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the URL of the search engine used to provide image search. Search requests will be sent using the GET method. If the DefaultSearchProviderImageURLPostParams policy is set then image search requests will use the POST method instead.

This policy is optional. If not set, no image search will be used.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"https://search.my.company/searchbyimage/upload"
Back to top

DefaultSearchProviderNewTabURL

Default search provider new tab page URL
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderNewTabURL`
Mac/Linux preference name:
`DefaultSearchProviderNewTabURL`
Android restriction name:
`DefaultSearchProviderNewTabURL`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 30
- Google Chrome OS (Google Chrome OS) since version 30
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the URL that a search engine uses to provide a new tab page.

This policy is optional. If not set, no new tab page will be provided.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"https://search.my.company/newtab"
Back to top

DefaultSearchProviderSearchURLPostParams

Parameters for search URL which uses POST
Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderSearchURLPostParams`
Mac/Linux preference name:
`DefaultSearchProviderSearchURLPostParams`
Android restriction name:
`DefaultSearchProviderSearchURLPostParams`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the parameters used when searching a URL with POST. It consists of comma-separated name/value pairs. If a value is a template parameter, like {searchTerms} in above example, it will be replaced with real search terms data.

This policy is optional. If not set, search request will be sent using the GET method.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"q={searchTerms},ie=utf-8,oe=utf-8"
Back to top

DefaultSearchProviderSuggestURLPostParams

Parameters for suggest URL which uses POST
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderSuggestURLPostParams`
Mac/Linux preference name:
`DefaultSearchProviderSuggestURLPostParams`
Android restriction name:
`DefaultSearchProviderSuggestURLPostParams`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the parameters used when doing suggestion search with POST. It consists of comma-separated name/value pairs. If a value is a template parameter, like {searchTerms} in above example, it will be replaced with real search terms data.

This policy is optional. If not set, suggest search request will be sent using the GET method.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"q={searchTerms},ie=utf-8,oe=utf-8"

Back to top

DefaultSearchProviderInstantURLPostParams

Parameters for instant URL which uses POST

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderInstantURLPostParams`

Mac/Linux preference name:
`DefaultSearchProviderInstantURLPostParams`

Android restriction name:
`DefaultSearchProviderInstantURLPostParams`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Specifies the parameters used when doing instant search with POST. It consists of comma-separated name/value pairs. If a value is a template parameter, like {searchTerms} in above example, it will be replaced with real search terms data.

This policy is optional. If not set, instant search request will be sent using the GET method.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"q={searchTerms},ie=utf-8,oe=utf-8"

Back to top

DefaultSearchProviderImageURLPostParams

Parameters for image URL which uses POST

Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\DefaultSearchProviderImageURLPostParams`

Mac/Linux preference name:
`DefaultSearchProviderImageURLPostParams`

Android restriction name:
`DefaultSearchProviderImageURLPostParams`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29

- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the parameters used when doing image search with POST. It consists of comma-separated name/value pairs. If a value is a template parameter, like {imageThumbnail} in above example, it will be replaced with real image thumbnail data.

This policy is optional. If not set, image search request will be sent using the GET method.

This policy is only respected if the 'DefaultSearchProviderEnabled' policy is enabled.

Example value:
"content={imageThumbnail},url={imageURL},sbisrc={SearchSource}"
Back to top

Extensions

Configures extension-related policies. The user is not allowed to install blacklisted extensions unless they are whitelisted. You can also force Google Chrome to automatically install extensions by specifying them in ExtensionInstallForcelist. Force-installed extensions are installed regardless whether they are present in the blacklist.

Back to top

ExtensionInstallBlacklist

Configure extension installation blacklist
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\ExtensionInstallBlacklist`
Mac/Linux preference name:
`ExtensionInstallBlacklist`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blacklisted.

A blacklist value of '*' means all extensions are blacklisted unless they are explicitly listed in the whitelist.

If this policy is left not set the user can install any extension in Google Chrome.

Example value:
Windows:

```
Software\Policies\Google\Chrome\ExtensionInstallBlacklist\1 =
"extension_id1"
Software\Policies\Google\Chrome\ExtensionInstallBlacklist\2 =
"extension_id2"
```
Android/Linux:
```
["extension_id1", "extension_id2"]
```
Mac:
```
<array>
  <string>extension_id1</string>
  <string>extension_id2</string>
</array>
```
Back to top

ExtensionInstallWhitelist

Configure extension installation whitelist

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\ExtensionInstallWhitelist`

Mac/Linux preference name:

`ExtensionInstallWhitelist`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to specify which extensions are not subject to the blacklist.

A blacklist value of * means all extensions are blacklisted and users can only install extensions listed in the whitelist.

By default, all extensions are whitelisted, but if all extensions have been blacklisted by policy, the whitelist can be used to override that policy.

Example value:

Windows:
```
Software\Policies\Google\Chrome\ExtensionInstallWhitelist\1 =
"extension_id1"
Software\Policies\Google\Chrome\ExtensionInstallWhitelist\2 =
"extension_id2"
```
Android/Linux:
```
["extension_id1", "extension_id2"]
```
Mac:
```
<array>
  <string>extension_id1</string>
  <string>extension_id2</string>
</array>
```
Back to top

ExtensionInstallForcelist

Configure the list of force-installed apps and extensions

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\ExtensionInstallForcelist`

Mac/Linux preference name:

`ExtensionInstallForcelist`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Specifies a list of apps and extensions that are installed silently, without user interaction, and which cannot be uninstalled by the user. All permissions requested by the apps/extensions are granted implicitly, without user interaction, including any additional permissions requested by future versions of the app/extension. Furthermore, permissions are granted for the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. (These two APIs are not available to apps/extensions that are not force-installed.)

This policy takes precedence over a potentially conflicting ExtensionsInstallBlacklist policy. If an app or extension that previously had been force-installed is removed from this list, it is automatically uninstalled by Google Chrome.

For Windows instances that are not joined to an Active Directory domain, forced installation is limited to apps and extensions listed in the Chrome Web Store.

Note that the source code of any extension may be altered by users via Developer Tools (potentially rendering the extension dysfunctional). If this is a concern, the DeveloperToolsDisabled policy should be set.

Each list item of the policy is a string that contains an extension ID and an "update" URL separated by a semicolon (;). The extension ID is the 32-letter string found e.g. on chrome://extensions when in developer mode. The "update" URL should point to an Update Manifest XML document as described at https://developer.chrome.com/extensions/autoupdate. Note that the "update" URL set in this policy is only used for the initial installation; subsequent updates of the extension employ the update URL indicated in the extension's manifest.

For example, gbchcmhmhahfdphkhkmpfmihenigjmpp;https://clients2.google.com/service/update2/crx installs the Chrome Remote Desktop app from the standard Chrome Web Store "update" URL. For more information about hosting extensions, see: https://developer.chrome.com/extensions/hosting.

If this policy is left not set, no apps or extensions are installed automatically and the user can uninstall any app or extension in Google Chrome.

Note for Google Chrome OS devices supporting Android apps:

Android apps can be force-installed from the Google Admin console using Google Play. They do not use this policy.

Example value:

Windows:

```
Software\Policies\Google\Chrome\ExtensionInstallForcelist\1 =
"gbchcmhmhahfdphkhkmpfmihenigjmpp;https://clients2.google.com/serv
ice/update2/crx"
```
Android/Linux:
```
["gbchcmhmhahfdphkhkmpfmihenigjmpp;https://clients2.google.com/ser
vice/update2/crx"]
```
Mac:
```
<array>

<string>gbchcmhmhahfdphkhkmpfmihenigjmpp;https://clients2.google.c
om/service/update2/crx</string>
</array>
```
Back to top

ExtensionInstallSources

Configure extension, app, and user script install sources

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\ExtensionInstallSources`

Mac/Linux preference name:

`ExtensionInstallSources`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 21
- Google Chrome OS (Google Chrome OS) since version 21

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to specify which URLs are allowed to install extensions, apps, and themes.

Starting in Google Chrome 21, it is more difficult to install extensions, apps, and user scripts from outside the Chrome Web Store. Previously, users could click on a link to a *.crx file, and Google Chrome would offer to install the file after a few warnings. After Google Chrome 21, such files must be downloaded and dragged onto the Google Chrome settings page. This setting allows specific URLs to have the old, easier installation flow.

Each item in this list is an extension-style match pattern (see https://developer.chrome.com/extensions/match_patterns). Users will be able to easily install items from any URL that matches an item in this list. Both the location of the *.crx file and the page where the download is started from (i.e. the referrer) must be allowed by these patterns.

ExtensionInstallBlacklist takes precedence over this policy. That is, an extension on the blacklist won't be installed, even if it happens from a site on this list.

Example value:

Windows:
```
Software\Policies\Google\Chrome\ExtensionInstallSources\1 =
"https://corp.mycompany.com/*"
```
Android/Linux:
```
["https://corp.mycompany.com/*"]
```
Mac:
```
<array>
```

```
    <string>https://corp.mycompany.com/*</string>
  </array>
```

Back to top

ExtensionAllowedTypes

Configure allowed app/extension types

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\ExtensionAllowedTypes`

Mac/Linux preference name:

`ExtensionAllowedTypes`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25
- Google Chrome OS (Google Chrome OS) since version 25

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Controls which app/extension types are allowed to be installed.

This setting white-lists the allowed types of extension/apps that can be installed in Google Chrome. The value is a list of strings, each of which should be one of the following: "extension", "theme", "user_script", "hosted_app", "legacy_packaged_app", "platform_app". See the Google Chrome extensions documentation for more information on these types.

Note that this policy also affects extensions and apps to be force-installed via ExtensionInstallForcelist.

If this setting is configured, extensions/apps which have a type that is not on the list will not be installed.

If this settings is left not-configured, no restrictions on the acceptable extension/app types are enforced.

Example value:

Windows:

```
Software\Policies\Google\Chrome\ExtensionAllowedTypes\1 =
"hosted_app"
```

Android/Linux:

```
["hosted_app"]
```

Mac:

```
<array>
  <string>hosted_app</string>
</array>
```

Back to top

Home page

Configure the default home page in Google Chrome and prevents users from changing it. The user's home page settings are only completely locked down, if you either select the home page to be the new tab page, or set it to be a URL and specify a home page URL. If you don't specify the home page URL, then the user is still able to set the home page to the new tab page by specifying 'chrome://newtab'.

Back to top

HomepageLocation

Configure the home page URL

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\HomepageLocation`

Mac/Linux preference name:

`HomepageLocation`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Configures the default home page URL in Google Chrome and prevents users from changing it.

The home page is the page opened by the Home button. The pages that open on startup are controlled by the RestoreOnStartup policies.

The home page type can either be set to a URL you specify here or set to the New Tab Page. If you select the New Tab Page, then this policy does not take effect.

If you enable this setting, users cannot change their home page URL in Google Chrome, but they can still choose the New Tab Page as their home page.

Leaving this policy not set will allow the user to choose their home page on their own if HomepageIsNewTabPage is not set too.

This policy is not available on Windows instances that are not joined to an Active Directory domain.

Example value:

"https://www.chromium.org"

Back to top

HomepageIsNewTabPage

Use New Tab Page as homepage

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\HomepageIsNewTabPage`

Mac/Linux preference name:

`HomepageIsNewTabPage`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Configures the type of the default home page in Google Chrome and prevents users from changing home page preferences. The home page can either be set to a URL you specify or set to the New Tab Page.

If you enable this setting, the New Tab Page is always used for the home page, and the home page URL location is ignored.

If you disable this setting, the user's homepage will never be the New Tab Page, unless its URL is set to 'chrome://newtab'.

If you enable or disable this setting, users cannot change their homepage type in Google Chrome.

Leaving this policy not set will allow the user to choose whether the new tab page is their home page on their own.

This policy is not available on Windows instances that are not joined to an Active Directory domain.

Example value:

0x00000001 (Windows), true (Linux), <true /> (Mac)

Back to top

Locally managed users settings

Configure settings for managed users.

Back to top

SupervisedUsersEnabled

Enable supervised users

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:

Dynamic Policy Refresh: No

Description:

If set to true, supervised users can be created and used.

If set to false or not configured, supervised-user creation and login will be disabled. All existing supervised users will be hidden.

NOTE: The default behavior for consumer and enterprise devices differs: on consumer devices supervised users are enabled by default, but on enterprise devices they are disabled by default.

Back to top

SupervisedUserCreationEnabled

Enable creation of supervised users
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SupervisedUserCreationEnabled`
Mac/Linux preference name:
`SupervisedUserCreationEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

If set to false, supervised-user creation by this user will be disabled. Any existing supervised users will still be available.

If set to true or not configured, supervised users can be created and managed by this user.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

SupervisedUserContentProviderEnabled

Enable the supervised user content provider
Data type:
Boolean
Android restriction name:
`SupervisedUserContentProviderEnabled`
Supported on:

- Google Chrome (Android) since version 49

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

If true and the user is a supervised user then other Android apps can query the user's web restrictions through a content provider.

If false or unset then the content provider returns no information.

Example value:
true (Android)
Back to top

Native Messaging

Configures policies for Native Messaging. Blacklisted native messaging hosts won't be allowed unless they are whitelisted.

Back to top

NativeMessagingBlacklist

Configure native messaging blacklist

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\NativeMessagingBlacklist`

Mac/Linux preference name:

`NativeMessagingBlacklist`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 34

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to specify which native messaging hosts that should not be loaded.

A blacklist value of '*' means all native messaging hosts are blacklisted unless they are explicitly listed in the whitelist.

If this policy is left not set Google Chrome will load all installed native messaging hosts.

Example value:

Windows:

```
Software\Policies\Google\Chrome\NativeMessagingBlacklist\1 =
"com.native.messaging.host.name1"
Software\Policies\Google\Chrome\NativeMessagingBlacklist\2 =
"com.native.messaging.host.name2"
```

Android/Linux:

```
["com.native.messaging.host.name1",
"com.native.messaging.host.name2"]
```

Mac:

```
<array>
  <string>com.native.messaging.host.name1</string>
  <string>com.native.messaging.host.name2</string>
</array>
```

Back to top

NativeMessagingWhitelist

Configure native messaging whitelist

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\NativeMessagingWhitelist`

Mac/Linux preference name:

`NativeMessagingWhitelist`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 34

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to specify which native messaging hosts are not subject to the blacklist.

A blacklist value of * means all native messaging hosts are blacklisted and only native messaging hosts listed in the whitelist will be loaded.

By default, all native messaging hosts are whitelisted, but if all native messaging hosts have been blacklisted by policy, the whitelist can be used to override that policy.

Example value:

Windows:

```
Software\Policies\Google\Chrome\NativeMessagingWhitelist\1 =
"com.native.messaging.host.name1"
Software\Policies\Google\Chrome\NativeMessagingWhitelist\2 =
"com.native.messaging.host.name2"
```

Android/Linux:

```
["com.native.messaging.host.name1",
"com.native.messaging.host.name2"]
```

Mac:

```
<array>
  <string>com.native.messaging.host.name1</string>
  <string>com.native.messaging.host.name2</string>
</array>
```

Back to top

NativeMessagingUserLevelHosts

Allow user-level Native Messaging hosts (installed without admin permissions).

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\NativeMessagingUserLevelHosts`

Mac/Linux preference name:

`NativeMessagingUserLevelHosts`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 34

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables user-level installation of Native Messaging hosts.

If this setting is enabled then Google Chrome allows usage of Native Messaging hosts installed on user level.

If this setting is disabled then Google Chrome will only use Native Messaging hosts installed on system level.

If this setting is left not set Google Chrome will allow usage of user-level Native Messaging hosts.

Example value:

0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

Password manager

Configures the password manager.

Back to top

PasswordManagerEnabled

Enable saving passwords to the password manager

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\PasswordManagerEnabled`

Mac/Linux preference name:

`PasswordManagerEnabled`

Android restriction name:

`PasswordManagerEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

If this setting is enabled, users can have Google Chrome memorize passwords and provide them automatically the next time they log in to a site.

If this settings is disabled, users cannot save new passwords but they may still use passwords that have been saved previously.

If this policy is enabled or disabled, users cannot change or override it in Google Chrome. If this policy is unset, password saving is allowed (but can be turned off by the user).

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on Android apps.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

PasswordManagerAllowShowPasswords (deprecated)

Allow users to show passwords in Password Manager (deprecated)

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\PasswordManagerAllowShowPasswords`

Mac/Linux preference name:

`PasswordManagerAllowShowPasswords`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8 until version 50
- Google Chrome OS (Google Chrome OS) since version 11 until version 50

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

The associated setting was used before reauthentication on viewing passwords was introduced. Since then, the setting and hence this policy had no effect on the behavior of Chrome. The current behavior of Chrome is now the same as if the the policy was set to disable showing passwords in clear text in the password manager settings page. That means that the settings page contains just a placeholder, and only upon the user clicking "Show" (and reauthenticating, if applicable) Chrome shows the password. Original description of the policy follows below.

Controls whether the user may show passwords in clear text in the password manager.

If you disable this setting, the password manager does not allow showing stored passwords in clear text in the password manager window.

If you enable or do not set this policy, users can view their passwords in clear text in the password manager.

Example value:

0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

Policies for HTTP authentication

Policies related to integrated HTTP authentication.

Back to top

AuthSchemes

Supported authentication schemes

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\AuthSchemes`

Mac/Linux preference name:

`AuthSchemes`

Android restriction name:

`AuthSchemes`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome (Android) since version 46

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

Specifies which HTTP authentication schemes are supported by Google Chrome.

Possible values are 'basic', 'digest', 'ntlm' and 'negotiate'. Separate multiple values with commas.

If this policy is left not set, all four schemes will be used.

Example value:

"basic,digest,ntlm,negotiate"

Back to top

DisableAuthNegotiateCnameLookup

Disable CNAME lookup when negotiating Kerberos authentication

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DisableAuthNegotiateCnameLookup`

Mac/Linux preference name:

`DisableAuthNegotiateCnameLookup`

Android restriction name:

`DisableAuthNegotiateCnameLookup`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome (Android) since version 46

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

Specifies whether the generated Kerberos SPN is based on the canonical DNS name or the original name entered.

If you enable this setting, CNAME lookup will be skipped and the server name will be used as entered.

If you disable this setting or leave it not set, the canonical name of the server will be determined via CNAME lookup.

Example value:

0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)

Back to top

EnableAuthNegotiatePort

Include non-standard port in Kerberos SPN

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\EnableAuthNegotiatePort`

Mac/Linux preference name:

`EnableAuthNegotiatePort`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

Specifies whether the generated Kerberos SPN should include a non-standard port.

If you enable this setting, and a non-standard port (i.e., a port other than 80 or 443) is entered, it will be included in the generated Kerberos SPN.

If you disable this setting or leave it not set, the generated Kerberos SPN will not include a port in any case.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

AuthServerWhitelist

Authentication server whitelist
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\AuthServerWhitelist`
Mac/Linux preference name:
`AuthServerWhitelist`
Android restriction name:
`AuthServerWhitelist`
Android WebView restriction name:
`com.android.browser:AuthServerWhitelist`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome (Android) since version 46
- Android System WebView (Android) since version 49

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Specifies which servers should be whitelisted for integrated authentication. Integrated authentication is only enabled when Google Chrome receives an authentication challenge from a proxy or from a server which is in this permitted list.

Separate multiple server names with commas. Wildcards (*) are allowed.

If you leave this policy not set Google Chrome will try to detect if a server is on the Intranet and only then will it respond to IWA requests. If a server is detected as Internet then IWA requests from it will be ignored by Google Chrome.

Example value:
"*example.com,foobar.com,*baz"
Back to top

AuthNegotiateDelegateWhitelist

Kerberos delegation server whitelist
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\AuthNegotiateDelegateWhitelist`
Mac/Linux preference name:
`AuthNegotiateDelegateWhitelist`
Android restriction name:
`AuthNegotiateDelegateWhitelist`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome (Android) since version 46

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Servers that Google Chrome may delegate to.

Separate multiple server names with commas. Wildcards (*) are allowed.

If you leave this policy not set Google Chrome will not delegate user credentials even if a server is detected as Intranet.

Example value:
"foobar.example.com"
Back to top

GSSAPILibraryName

GSSAPI library name
Data type:
String
Mac/Linux preference name:
`GSSAPILibraryName`
Supported on:

- Google Chrome (Linux) since version 9

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Specifies which GSSAPI library to use for HTTP authentication. You can set either just a library name, or a full path.

If no setting is provided, Google Chrome will fall back to using a default library name.

Example value:
"libgssapi_krb5.so.2"
Back to top

AuthAndroidNegotiateAccountType

Account type for HTTP Negotiate authentication
Data type:
String
Android restriction name:
`AuthAndroidNegotiateAccountType`
Android WebView restriction name:
`com.android.browser:AuthAndroidNegotiateAccountType`
Supported on:

- Google Chrome (Android) since version 46
- Android System WebView (Android) since version 49

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Specifies the account type of the accounts provided by the Android authentication app that supports HTTP Negotiate authentication (e.g. Kerberos authentication). This information should be available from the supplier of the authentication app. For more details see https://goo.gl/hajyfN.

If no setting is provided, HTTP Negotiate authentication is disabled on Android.

Example value:
"com.example.spnego"
Back to top

AllowCrossOriginAuthPrompt

Cross-origin HTTP Basic Auth prompts
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AllowCrossOriginAuthPrompt`
Mac/Linux preference name:
`AllowCrossOriginAuthPrompt`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 13

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Controls whether third-party sub-content on a page is allowed to pop-up an HTTP Basic Auth dialog box.

Typically this is disabled as a phishing defense. If this policy is not set, this is disabled and third-party sub-content will not be allowed to pop up a HTTP Basic Auth dialog box.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

Power management

Configure power management in Google Chrome OS. These policies let you configure how Google Chrome OS behaves when the user remains idle for some amount of time.

Back to top

ScreenDimDelayAC (deprecated)

Screen dim delay when running on AC power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the screen is dimmed when running on AC power.

When this policy is set to a value greater than zero, it specifies the length of time that the user must remain idle before Google Chrome OS dims the screen.

When this policy is set to zero, Google Chrome OS does not dim the screen when the user becomes idle.

When this policy is unset, a default length of time is used.

The policy value should be specified in milliseconds. Values are clamped to be less than or equal the screen off delay (if set) and the idle delay.

Back to top

ScreenOffDelayAC (deprecated)

Screen off delay when running on AC power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the screen is turned off when running on AC power.

When this policy is set to a value greater than zero, it specifies the length of time that the user must remain idle before Google Chrome OS turns off the screen.

When this policy is set to zero, Google Chrome OS does not turn off the screen when the user becomes idle.

When this policy is unset, a default length of time is used.

The policy value should be specified in milliseconds. Values are clamped to be less than or equal the idle delay.

Back to top

ScreenLockDelayAC (deprecated)

Screen lock delay when running on AC power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the screen is locked when running on AC power.

When this policy is set to a value greater than zero, it specifies the length of time that the user must remain idle before Google Chrome OS locks the screen.

When this policy is set to zero, Google Chrome OS does not lock the screen when the user becomes idle.

When this policy is unset, a default length of time is used.

The recommended way to lock the screen on idle is to enable screen locking on suspend and have Google Chrome OS suspend after the idle delay. This policy should only be used when screen locking should occur a significant amount of time sooner than suspend or when suspend on idle is not desired at all.

The policy value should be specified in milliseconds. Values are clamped to be less than the idle delay.

Back to top

IdleWarningDelayAC (deprecated)

Idle warning delay when running on AC power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 27

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which a warning dialog is shown when running on AC power.

When this policy is set, it specifies the length of time that the user must remain idle before Google Chrome OS shows a warning dialog telling the user that the idle action is about to be taken.

When this policy is unset, no warning dialog is shown.

The policy value should be specified in milliseconds. Values are clamped to be less than or equal the idle delay.

Back to top

IdleDelayAC (deprecated)

Idle delay when running on AC power

Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the idle action is taken when running on AC power.

When this policy is set, it specifies the length of time that the user must remain idle before Google Chrome OS takes the idle action, which can be configured separately.

When this policy is unset, a default length of time is used.

The policy value should be specified in milliseconds.

Back to top

ScreenDimDelayBattery (deprecated)

Screen dim delay when running on battery power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the screen is dimmed when running on battery power.

When this policy is set to a value greater than zero, it specifies the length of time that the user must remain idle before Google Chrome OS dims the screen.

When this policy is set to zero, Google Chrome OS does not dim the screen when the user becomes idle.

When this policy is unset, a default length of time is used.

The policy value should be specified in milliseconds. Values are clamped to be less than or equal the screen off delay (if set) and the idle delay.

Back to top

ScreenOffDelayBattery (deprecated)

Screen off delay when running on battery power
Data type:
Integer

Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the screen is turned off when running on battery power.

When this policy is set to a value greater than zero, it specifies the length of time that the user must remain idle before Google Chrome OS turns off the screen.

When this policy is set to zero, Google Chrome OS does not turn off the screen when the user becomes idle.

When this policy is unset, a default length of time is used.

The policy value should be specified in milliseconds. Values are clamped to be less than or equal the idle delay.

Back to top

ScreenLockDelayBattery (deprecated)

Screen lock delay when running on battery power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the screen is locked when running on battery power.

When this policy is set to a value greater than zero, it specifies the length of time that the user must remain idle before Google Chrome OS locks the screen.

When this policy is set to zero, Google Chrome OS does not lock the screen when the user becomes idle.

When this policy is unset, a default length of time is used.

The recommended way to lock the screen on idle is to enable screen locking on suspend and have Google Chrome OS suspend after the idle delay. This policy should only be used when screen locking should occur a significant amount of time sooner than suspend or when suspend on idle is not desired at all.

The policy value should be specified in milliseconds. Values are clamped to be less than the idle delay.

Back to top

IdleWarningDelayBattery (deprecated)

Idle warning delay when running on battery power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 27

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which a warning dialog is shown when running on battery power.

When this policy is set, it specifies the length of time that the user must remain idle before Google Chrome OS shows a warning dialog telling the user that the idle action is about to be taken.

When this policy is unset, no warning dialog is shown.

The policy value should be specified in milliseconds. Values are clamped to be less than or equal the idle delay.

Back to top

IdleDelayBattery (deprecated)

Idle delay when running on battery power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the length of time without user input after which the idle action is taken when running on battery power.

When this policy is set, it specifies the length of time that the user must remain idle before Google Chrome OS takes the idle action, which can be configured separately.

When this policy is unset, a default length of time is used.

The policy value should be specified in milliseconds.

Back to top

IdleAction (deprecated)

Action to take when the idle delay is reached

Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specify the action to take when the idle delay is reached.

Note that this policy is deprecated and will be removed in the future.

This policy provides a fallback value for the more-specific IdleActionAC and IdleActionBattery policies. If this policy is set, its value gets used if the respective more-specific policy is not set.

When this policy is unset, behavior of the more-specific policies remains unaffected.

- 0 = Suspend
- 1 = Log the user out
- 2 = Shut down
- 3 = Do nothing

Back to top

IdleActionAC (deprecated)

Action to take when the idle delay is reached while running on AC power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specify the action to take when the idle delay is reached while running on AC power.

When this policy is set, it specifies the action that Google Chrome OS takes when the user remains idle for the length of time given by the idle delay, which can be configured separately.

When this policy is unset, the default action is taken, which is suspend.

If the action is suspend, Google Chrome OS can separately be configured to either lock or not lock the screen before suspending.

- 0 = Suspend
- 1 = Log the user out
- 2 = Shut down
- 3 = Do nothing

Back to top

IdleActionBattery (deprecated)

Action to take when the idle delay is reached while running on battery power
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specify the action to take when the idle delay is reached while running on battery power.

When this policy is set, it specifies the action that Google Chrome OS takes when the user remains idle for the length of time given by the idle delay, which can be configured separately.

When this policy is unset, the default action is taken, which is suspend.

If the action is suspend, Google Chrome OS can separately be configured to either lock or not lock the screen before suspending.

- 0 = Suspend
- 1 = Log the user out
- 2 = Shut down
- 3 = Do nothing

Back to top

LidCloseAction

Action to take when the user closes the lid
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specify the action to take when the user closes the lid.

When this policy is set, it specifies the action that Google Chrome OS takes when the user closes the device's lid.

When this policy is unset, the default action is taken, which is suspend.

If the action is suspend, Google Chrome OS can separately be configured to either lock or not lock the screen before suspending.

- 0 = Suspend
- 1 = Log the user out
- 2 = Shut down

- 3 = Do nothing

Back to top

PowerManagementUsesAudioActivity

Specify whether audio activity affects power management
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies whether audio activity affects power management.

If this policy is set to True or is unset, the user is not considered to be idle while audio is playing. This prevents the idle timeout from being reached and the idle action from being taken. However, screen dimming, screen off and screen lock will be performed after the configured timeouts, irrespective of audio activity.

If this policy is set to False, audio activity does not prevent the user from being considered idle.

Back to top

PowerManagementUsesVideoActivity

Specify whether video activity affects power management
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies whether video activity affects power management.

If this policy is set to True or is unset, the user is not considered to be idle while video is playing. This prevents the idle delay, screen dim delay, screen off delay and screen lock delay from being reached and the corresponding actions from being taken.

If this policy is set to False, video activity does not prevent the user from being considered idle.

Note for Google Chrome OS devices supporting Android apps:

Video playing in Android apps is not taken into consideration, even if this policy is set to True.

Back to top

PresentationIdleDelayScale (deprecated)

Percentage by which to scale the idle delay in presentation mode (deprecated)
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26 until version 28

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

This policy has been retired as of Google Chrome OS version 29. Please use the PresentationScreenDimDelayScale policy instead.

Back to top

PresentationScreenDimDelayScale

Percentage by which to scale the screen dim delay in presentation mode
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies the percentage by which the screen dim delay is scaled when the device is in presentation mode.

If this policy is set, it specifies the percentage by which the screen dim delay is scaled when the device is in presentation mode. When the screen dim delay is scaled, the screen off, screen lock and idle delays get adjusted to maintain the same distances from the screen dim delay as originally configured.

If this policy is unset, a default scale factor is used.

The scale factor must be 100% or more. Values that would make the screen dim delay in presentation mode shorter than the regular screen dim delay are not allowed.

Back to top

AllowScreenWakeLocks

Allow screen wake locks
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 28

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies whether screen wake locks are allowed. Screen wake locks can be requested by extensions via the power management extension API.

If this policy is set to true or left not set, screen wake locks will be honored for power management.

If this policy is set to false, screen wake lock requests will get ignored.

Back to top

UserActivityScreenDimDelayScale

Percentage by which to scale the screen dim delay if the user becomes active after dimming

Data type:

Integer

Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Specifies the percentage by which the screen dim delay is scaled when user activity is observed while the screen is dimmed or soon after the screen has been turned off.

If this policy is set, it specifies the percentage by which the screen dim delay is scaled when user activity is observed while the screen is dimmed or soon after the screen has been turned off. When the dim delay is scaled, the screen off, screen lock and idle delays get adjusted to maintain the same distances from the screen dim delay as originally configured.

If this policy is unset, a default scale factor is used.

The scale factor must be 100% or more.

Back to top

WaitForInitialUserActivity

Wait for initial user activity

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 32

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Specifies whether power management delays and the session length limit should only start running after the first user activity has been observed in a session.

If this policy is set to True, power management delays and the session length limit do not start running until after the first user activity has been observed in a session.

If this policy is set to False or left unset, power management delays and the session length limit start running immediately on session start.

Back to top

PowerManagementIdleSettings

Power management settings when the user becomes idle

Data type:

Dictionary

Supported on:

- Google Chrome OS (Google Chrome OS) since version 35

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Configure power management settings when the user becomes idle.

This policy controls multiple settings for the power management strategy when the user becomes idle.

There are four types of action: * The screen will be dimmed if the user remains idle for the time specified by |ScreenDim|. * The screen will be turned off if the user remains idle for the time specified by |ScreenOff|. * A warning dialog will be shown if the user remains idle for the time specified by |IdleWarning|, telling the user that the idle action is about to be taken. * The action specified by |IdleAction| will be taken if the user remains idle for the time specified by |Idle|.

For each of above actions, the delay should be specified in milliseconds, and needs to be set to a value greater than zero to trigger the corresponding action. In case the delay is set to zero, Google Chrome OS will not take the corresponding action.

For each of the above delays, when the length of time is unset, a default value will be used.

Note that |ScreenDim| values will be clamped to be less than or equal to |ScreenOff|, |ScreenOff| and |IdleWarning| will be clamped to be less than or equal to |Idle|.

|IdleAction| can be one of four possible actions: * |Suspend| * |Logout| * |Shutdown| * |DoNothing|

When the |IdleAction| is unset, the default action is taken, which is suspend.

There are also separate settings for AC power and battery.

Back to top

ScreenLockDelays

Screen lock delays

Data type:

Dictionary

Supported on:

- Google Chrome OS (Google Chrome OS) since version 35

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Specifies the length of time without user input after which the screen is locked when running on AC power or battery.

When the length of time is set to a value greater than zero, it represents the length of time that the user must remain idle before Google Chrome OS locks the screen.

When the length of time is set to zero, Google Chrome OS does not lock the screen when the user becomes idle.

When the length of time is unset, a default length of time is used.

The recommended way to lock the screen on idle is to enable screen locking on suspend and have Google Chrome OS suspend after the idle delay. This policy should only be used when screen locking should occur a significant amount of time sooner than suspend or when suspend on idle is not desired at all.

The policy value should be specified in milliseconds. Values are clamped to be less than the idle delay.

Back to top

Proxy server

Allows you to specify the proxy server used by Google Chrome and prevents users from changing proxy settings. If you choose to never use a proxy server and always connect directly, all other options are ignored. If you choose to auto detect the proxy server, all other options are ignored. For detailed examples, visit: https://www.chromium.org/developers/design-documents/network-settings#TOC-Command-line-options-for-proxy-sett. If you enable this setting, Google Chrome and ARC-apps ignore all proxy-related options specified from the command line. Leaving these policies not set will allow the users to choose the proxy settings on their own.

Back to top

ProxyMode

Choose how to specify proxy server settings

Data type:

String [Android:choice, Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\ProxyMode`

Mac/Linux preference name:

`ProxyMode`

Android restriction name:

`ProxyMode`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to specify the proxy server used by Google Chrome and prevents users from changing proxy settings.

If you choose to never use a proxy server and always connect directly, all other options are ignored.

If you choose to use system proxy settings, all other options are ignored.

If you choose to auto detect the proxy server, all other options are ignored.

If you choose fixed server proxy mode, you can specify further options in 'Address or URL of proxy server' and 'Comma-separated list of proxy bypass rules'. Only the HTTP proxy server with the highest priority is available for ARC-apps.

If you choose to use a .pac proxy script, you must specify the URL to the script in 'URL to a proxy .pac file'.

For detailed examples, visit: https://www.chromium.org/developers/design-documents/network-settings#TOC-Command-line-options-for-proxy-sett.

If you enable this setting, Google Chrome and ARC-apps ignore all proxy-related options specified from the command line.

Leaving this policy not set will allow the users to choose the proxy settings on their own.

- "direct" = Never use a proxy
- "auto_detect" = Auto detect proxy settings
- "pac_script" = Use a .pac proxy script
- "fixed_servers" = Use fixed proxy servers
- "system" = Use system proxy settings

Note for Google Chrome OS devices supporting Android apps:

You cannot force Android apps to use a proxy. A subset of proxy settings is made available to Android apps, which they may voluntarily choose to honor:

If you choose "never use a proxy server," Android apps are informed that no proxy is configured.

If you choose "use system proxy settings" or "fixed server proxy," Android apps are provided with the http proxy server address and port.

If you choose "auto detect proxy server," the script URL "http://wpad/wpad.dat" is provided to Android apps. No other part of the proxy auto-detection protocol is used.

If you choose ".pac proxy script," the script URL is provided to Android apps.

Example value:

"direct"

Back to top

ProxyServerMode (deprecated)

Choose how to specify proxy server settings

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\ProxyServerMode`
Mac/Linux preference name:
`ProxyServerMode`
Android restriction name:
`ProxyServerMode`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy is deprecated, use ProxyMode instead.

Allows you to specify the proxy server used by Google Chrome and prevents users from changing proxy settings.

If you choose to never use a proxy server and always connect directly, all other options are ignored.

If you choose to use system proxy settings or auto detect the proxy server, all other options are ignored.

If you choose manual proxy settings, you can specify further options in 'Address or URL of proxy server', 'URL to a proxy .pac file' and 'Comma-separated list of proxy bypass rules'. Only the HTTP proxy server with the highest priority is available for ARC-apps.

For detailed examples, visit: https://www.chromium.org/developers/design-documents/network-settings#TOC-Command-line-options-for-proxy-sett.

If you enable this setting, Google Chrome ignores all proxy-related options specified from the command line.

Leaving this policy not set will allow the users to choose the proxy settings on their own.

- 0 = Never use a proxy
- 1 = Auto detect proxy settings
- 2 = Manually specify proxy settings
- 3 = Use system proxy settings

Note for Google Chrome OS devices supporting Android apps:

You cannot force Android apps to use a proxy. A subset of proxy settings is made available to Android apps, which they may voluntarily choose to honor. See the ProxyMode policy for more details.

Example value:
0x00000002 (Windows), 2 (Linux), 2 (Android), 2 (Mac)
Back to top

ProxyServer

Address or URL of proxy server

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\ProxyServer`

Mac/Linux preference name:

`ProxyServer`

Android restriction name:

`ProxyServer`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

You can specify the URL of the proxy server here.

This policy only takes effect if you have selected manual proxy settings at 'Choose how to specify proxy server settings'.

You should leave this policy not set if you have selected any other mode for setting proxy policies.

For more options and detailed examples, visit: https://www.chromium.org/developers/design-documents/network-settings#TOC-Command-line-options-for-proxy-sett.

Note for Google Chrome OS devices supporting Android apps:

You cannot force Android apps to use a proxy. A subset of proxy settings is made available to Android apps, which they may voluntarily choose to honor. See the ProxyMode policy for more details.

Example value:

"123.123.123.123:8080"

Back to top

ProxyPacUrl

URL to a proxy .pac file

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\ProxyPacUrl`

Mac/Linux preference name:

`ProxyPacUrl`

Android restriction name:

`ProxyPacUrl`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

You can specify a URL to a proxy .pac file here.

This policy only takes effect if you have selected manual proxy settings at 'Choose how to specify proxy server settings'.

You should leave this policy not set if you have selected any other mode for setting proxy policies.

For detailed examples, visit: https://www.chromium.org/developers/design-documents/network-settings#TOC-Command-line-options-for-proxy-sett.

Note for Google Chrome OS devices supporting Android apps:

You cannot force Android apps to use a proxy. A subset of proxy settings is made available to Android apps, which they may voluntarily choose to honor. See the ProxyMode policy for more details.

Example value:
"https://internal.site/example.pac"
Back to top

ProxyBypassList

Proxy bypass rules
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\ProxyBypassList`
Mac/Linux preference name:
`ProxyBypassList`
Android restriction name:
`ProxyBypassList`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Google Chrome will bypass any proxy for the list of hosts given here.

This policy only takes effect if you have selected manual proxy settings at 'Choose how to specify proxy server settings'.

You should leave this policy not set if you have selected any other mode for setting proxy policies.

For more detailed examples, visit: https://www.chromium.org/developers/design-documents/network-settings#TOC-Command-line-options-for-proxy-sett.

Note for Google Chrome OS devices supporting Android apps:

You cannot force Android apps to use a proxy. A subset of proxy settings is made available to Android apps, which they may voluntarily choose to honor. See the ProxyMode policy for more details.

Example value:
"https://www.example1.com,https://www.example2.com,https://internalsite/"

Back to top

Remote Attestation

Configure the remote attestation with TPM mechanism.

Back to top

AttestationEnabledForDevice

Enable remote attestation for the device
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 28

Supported features:
Dynamic Policy Refresh: Yes
Description:

If true, remote attestation is allowed for the device and a certificate will automatically be generated and uploaded to the Device Management Server.

If it is set to false, or if it is not set, no certificate will be generated and calls to the enterprise.platformKeysPrivate extension API will fail.

Back to top

AttestationEnabledForUser

Enable remote attestation for the user
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 28

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

If true, the user can use the hardware on Chrome devices to remote attest its identity to the privacy CA via the Enterprise Platform Keys API chrome.enterprise.platformKeysPrivate.challengeUserKey().

If it is set to false, or if it is not set, calls to the API will fail with an error code.

Back to top

AttestationExtensionWhitelist

Extensions allowed to to use the remote attestation API
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 28

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy specifies the allowed extensions to use Enterprise Platform Keys API chrome.enterprise.platformKeysPrivate.challengeUserKey() for remote attestation. Extensions must be added to this list to use the API.

If an extension is not in the list, or the list is not set, the call to the API will fail with an error code.

Back to top

AttestationForContentProtectionEnabled

Enable the use of remote attestation for content protection for the device
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 31

Supported features:
Dynamic Policy Refresh: Yes
Description:

Chrome OS devices can use remote attestation (Verified Access) to get a certificate issued by the Chrome OS CA that asserts the device is eligible to play protected content. This process involves sending hardware endorsement information to the Chrome OS CA which uniquely identifies the device.

If this setting is false, the device will not use remote attestation for content protection and the device may be unable to play protected content.

If this setting is true, or if it is not set, remote attestation may be used for content protection.

Back to top

Startup pages

Allows you to configure the pages that are loaded on startup. The contents of the list 'URLs to open at startup' are ignored unless you select 'Open a list of URLs' in 'Action on startup'.

Back to top

RestoreOnStartup

Action on startup

Data type:

Integer [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\RestoreOnStartup`

Mac/Linux preference name:

`RestoreOnStartup`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows you to specify the behavior on startup.

If you choose 'Open New Tab Page' the New Tab Page will always be opened when you start Google Chrome.

If you choose 'Restore the last session', the URLs that were open last time Google Chrome was closed will be reopened and the browsing session will be restored as it was left. Choosing this option disables some settings that rely on sessions or that perform actions on exit (such as Clear browsing data on exit or session-only cookies).

If you choose 'Open a list of URLs', the list of 'URLs to open on startup' will be opened when a user starts Google Chrome.

If you enable this setting, users cannot change or override it in Google Chrome.

Disabling this setting is equivalent to leaving it not configured. The user will still be able to change it in Google Chrome.

This policy is not available on Windows instances that are not joined to an Active Directory domain.

- 5 = Open New Tab Page
- 1 = Restore the last session
- 4 = Open a list of URLs

Example value:

0x00000004 (Windows), 4 (Linux), 4 (Mac)

Back to top

RestoreOnStartupURLs

URLs to open on startup

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\RestoreOnStartupURLs`

Mac/Linux preference name:

`RestoreOnStartupURLs`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

If 'Open a list of URLs' is selected as the startup action, this allows you to specify the list of URLs that are opened. If left not set no URL will be opened on start up.

This policy only works if the 'RestoreOnStartup' policy is set to 'RestoreOnStartupIsURLs'.

This policy is not available on Windows instances that are not joined to an Active Directory domain.

Example value:
Windows:
```
Software\Policies\Google\Chrome\RestoreOnStartupURLs\1 =
"https://example.com"
Software\Policies\Google\Chrome\RestoreOnStartupURLs\2 =
"https://www.chromium.org"
```
Android/Linux:
```
["https://example.com", "https://www.chromium.org"]
```
Mac:
```
<array>
  <string>https://example.com</string>
  <string>https://www.chromium.org</string>
</array>
```
Back to top

AllowDinosaurEasterEgg

Allow Dinosaur Easter Egg Game

Data type:
Boolean [Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\AllowDinosaurEasterEgg`

Mac/Linux preference name:
`AllowDinosaurEasterEgg`

Supported on:

- Google Chrome OS (Google Chrome OS) since version 48
- Google Chrome (Linux, Mac, Windows) since version 48

Supported features:
Dynamic Policy Refresh: No, Per Profile: Yes

Description:

Allow users to play dinosaur easter egg game when device is offline.

If this policy is set to False, users will not be able to play the dinosaur easter egg game when device is offline. If this setting is set to True, users are allowed to play the dinosaur game. If this policy is not set, users are not allowed to play the dinosaur easter egg game on enrolled Chrome OS, but are allowed to play it under other circumstances.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

AllowFileSelectionDialogs

Allow invocation of file selection dialogs
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AllowFileSelectionDialogs`
Mac/Linux preference name:
`AllowFileSelectionDialogs`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 12

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Allows access to local files on the machine by allowing Google Chrome to display file selection dialogs.

If you enable this setting, users can open file selection dialogs as normal.

If you disable this setting, whenever the user performs an action which would provoke a file selection dialog (like importing bookmarks, uploading files, saving links, etc.) a message is displayed instead and the user is assumed to have clicked Cancel on the file selection dialog.

If this setting is not set, users can open file selection dialogs as normal.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

AllowKioskAppControlChromeVersion

Allow the auto launched with zero delay kiosk app to control Google Chrome OS version
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 51

Supported features:
Dynamic Policy Refresh: Yes
Description:

Whether to allow the auto launched with zero delay kiosk app to control Google Chrome OS version.

This policy controls whether to allow the auto launched with zero delay kiosk app to control Google Chrome OS version by declaring a required_platform_version in its manifest and use it as the auto update target version prefix.

If the policy is set to true, the value of required_platform_version manifest key of the auto launched with zero delay kiosk app is used as auto update target version prefix.

If the policy is not configured or set to false, the required_platform_version manifest key is ignored and auto update proceeds as normal.

Note for Google Chrome OS devices supporting Android apps:

If the kiosk app is an Android app, it will have no control over the Google Chrome OS version, even if this policy is set to True.

Back to top

AllowOutdatedPlugins

Allow running plugins that are outdated
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AllowOutdatedPlugins`
Mac/Linux preference name:
`AllowOutdatedPlugins`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 12
- Google Chrome OS (Google Chrome OS) since version 12

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows Google Chrome to run plugins that are outdated.

If you enable this setting, outdated plugins are used as normal plugins.

If you disable this setting, outdated plugins will not be used and users will not be asked for permission to run them.

If this setting is not set, users will be asked for permission to run outdated plugins.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

AllowScreenLock

Permit locking the screen
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 52

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Permit locking the screen.

If this policy is set to false, users will not be able to lock the screen (only signing out from the user session will be possible). If this setting is set to true or not set, users who authenticated with a password can lock the screen.

Back to top

AllowedDomainsForApps

Define domains allowed to access Google Apps
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\AllowedDomainsForApps`
Mac/Linux preference name:
`AllowedDomainsForApps`
Android restriction name:
`AllowedDomainsForApps`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 51
- Google Chrome OS (Google Chrome OS) since version 51
- Google Chrome (Android) since version 51

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables Google Chrome's restricted log in feature in Google Apps and prevents users from changing this setting.

If you define this setting, the user will only be able to access Google Apps (such as Gmail) using accounts from the specified domains.

This setting will NOT prevent the user from loging in on a managed device that requires Google authentication. The user will still be allowed to sign in to accounts from other domains, but they will receive an error when trying to use Google Apps with those accounts.

If you leave this setting empty/not-configured, the user will be able to access Google Apps with any account.

This policy causes the X-GoogApps-Allowed-Domains header to be appended to all HTTP and HTTPS requests to all google.com domains, as described in https://support.google.com/a/answer/1668854.

Users cannot change or override this setting.

Example value:
"managedchrome.com,gmail.com"
Back to top

AlternateErrorPagesEnabled

Enable alternate error pages
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AlternateErrorPagesEnabled`

Mac/Linux preference name:
`AlternateErrorPagesEnabled`
Android restriction name:
`AlternateErrorPagesEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables the use of alternate error pages that are built into Google Chrome (such as 'page not found') and prevents users from changing this setting.

If you enable this setting, alternate error pages are used.

If you disable this setting, alternate error pages are never used.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

If this policy is left not set, this will be enabled but the user will be able to change it.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

AlwaysAuthorizePlugins

Always runs plugins that require authorization
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AlwaysAuthorizePlugins`
Mac/Linux preference name:
`AlwaysAuthorizePlugins`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 13
- Google Chrome OS (Google Chrome OS) since version 13

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allows Google Chrome to run plugins that require authorization.

If you enable this setting, plugins that are not outdated always run.

If this setting is disabled or not set, users will be asked for permission to run plugins that require authorization. These are plugins that can compromise security.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)

Back to top

AlwaysOpenPdfExternally

Always Open PDF files externally
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AlwaysOpenPdfExternally`
Mac/Linux preference name:
`AlwaysOpenPdfExternally`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 55

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Disables the internal PDF viewer in Google Chrome. Instead it treats it as download and allows the user to open PDF files with the default application.

If this policy is left not set or disabled the PDF plugin will be used to open PDF files unless the user disables it.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ApplicationLocaleValue

Application locale
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\ApplicationLocaleValue`
Supported on:

- Google Chrome (Windows) since version 8

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: No, Per Profile: No
Description:

Configures the application locale in Google Chrome and prevents users from changing the locale.

If you enable this setting, Google Chrome uses the specified locale. If the configured locale is not supported, 'en-US' is used instead.

If this setting is disabled or not set, Google Chrome uses either the user-specified preferred locale (if configured), the system locale or the fallback locale 'en-US'.

Example value:
"en"
Back to top

ArcBackupRestoreEnabled

Enable Android Backup Service
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 53

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

When this policy is set to true, Android app data is uploaded to Android Backup servers and restored from them upon app re-installations for compatible apps.

When this policy is set to false, Android Backup Service will be switched off.

If this setting is configured then users are not able change it themselves.

If this setting is not configured then users are able to turn Android Backup Service on and off in the Android Settings app.

Back to top

ArcCertificatesSyncMode

Set certificate availability for ARC-apps
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 52

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If set to SyncDisabled or not configured, Google Chrome OS certificates are not available for ARC-apps.

If set to CopyCaCerts, all ONC-installed CA certificates with Web TrustBit are available for ARC-apps.

- 0 = Disable usage of Google Chrome OS certificates to ARC-apps
- 1 = Enable Google Chrome OS CA certificates to ARC-apps

Back to top

ArcEnabled

Enable ARC
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 50

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

When this policy is set to true, ARC will be enabled for the user (subject to additional policy settings checks - ARC will still be unavailable if either ephemeral mode or multiple sign-in is enabled in the current user session).

If this setting is disabled or not configured then enterprise users are unable to use ARC.

Back to top

ArcPolicy

Configure ARC
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 50

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Specifies a set of policies that will be handed over to the ARC runtime. The value must be valid JSON.

Back to top

AudioCaptureAllowed

Allow or deny audio capture
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\AudioCaptureAllowed`
Mac/Linux preference name:
`AudioCaptureAllowed`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25
- Google Chrome OS (Google Chrome OS) since version 23

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Allow or deny audio capture.

If enabled or not configured (default), the user will be prompted for audio capture access except for URLs configured in the AudioCaptureAllowedUrls list which will be granted access without prompting.

When this policy is disabled, the user will never be prompted and audio capture only be available to URLs configured in AudioCaptureAllowedUrls.

This policy affects all types of audio inputs and not only the built-in microphone.

Note for Google Chrome OS devices supporting Android apps:

For Android apps, this policy affects the microphone only. When this policy is set to true, the microphone is muted for all Android apps, with no exceptions.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

AudioCaptureAllowedUrls

URLs that will be granted access to audio capture devices without prompt
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\AudioCaptureAllowedUrls`
Mac/Linux preference name:
`AudioCaptureAllowedUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Patterns in this list will be matched against the security origin of the requesting URL. If a match is found, access to audio capture devices will be granted without prompt.

NOTE: Until version 45, this policy was only supported in Kiosk mode.

Example value:
Windows:
```
Software\Policies\Google\Chrome\AudioCaptureAllowedUrls\1 =
"https://www.example.com/"
Software\Policies\Google\Chrome\AudioCaptureAllowedUrls\2 =
"https://[*.]example.edu/"
```
Android/Linux:
```
["https://www.example.com/", "https://[*.]example.edu/"]
```
Mac:
```
<array>
  <string>https://www.example.com/</string>
  <string>https://[*.]example.edu/</string>
</array>
```
Back to top

AudioOutputAllowed

Allow playing audio
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 23

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Allow playing audio.

When this policy is set to false, audio output will not be available on the device while the user is logged in.

This policy affects all types of audio output and not only the built-in speakers. Audio accessibility features are also inhibited by this policy. Do not enable this policy if a screen reader is required for the user.

If this setting is set to true or not configured then users can use all supported audio outputs on their device.

Back to top

AutoCleanUpStrategy (deprecated)

Selects the strategy used to free up disk space during automatic clean-up (deprecated)
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 32 until version 35

Supported features:
Dynamic Policy Refresh: Yes
Description:

This policy is deprecated. Google Chrome OS will always use the 'RemoveLRU' clean-up strategy.

Controls the automatic clean-up behavior on Google Chrome OS devices. Automatic clean-up is triggered when the amount of free disk space reaches a critical level to recover some disk space.

If this policy is set to 'RemoveLRU', the automatic clean-up will keep removing users from the device in least-recently-logged-in order until there is enough free space.

If this policy is set to 'RemoveLRUIfDormant', the automatic clean-up will keep removing users who have not logged in for at least 3 months in least-recently-logged-in order until there is enough free space.

If this policy is not set, automatic clean-up uses the default built-in strategy. Currently, it is the 'RemoveLRUIfDormant' strategy.

- "remove-lru" = Least recently used users are removed until there is enough free space
- "remove-lru-if-dormant" = Least recently used users who have not logged in within last 3 months are removed until there is enough free space

Back to top

AutoFillEnabled

Enable AutoFill
Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\AutoFillEnabled`

Mac/Linux preference name:

`AutoFillEnabled`

Android restriction name:

`AutoFillEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables Google Chrome's AutoFill feature and allows users to auto complete web forms using previously stored information such as address or credit card information.

If you disable this setting, AutoFill will be inaccessible to users.

If you enable this setting or do not set a value, AutoFill will remain under the control of the user. This will allow them to configure AutoFill profiles and to switch AutoFill on or off at their own discretion.

Example value:

0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)

Back to top

BackgroundModeEnabled

Continue running background apps when Google Chrome is closed

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\BackgroundModeEnabled`

Mac/Linux preference name:

`BackgroundModeEnabled`

Supported on:

- Google Chrome (Windows) since version 19
- Google Chrome (Linux) since version 19

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Determines whether a Google Chrome process is started on OS login and keeps running when the last browser window is closed, allowing background apps and the current browsing session to remain active, including any session cookies. The background process displays an icon in the system tray and can always be closed from there.

If this policy is set to True, background mode is enabled and cannot be controlled by the user in the browser settings.

If this policy is set to False, background mode is disabled and cannot be controlled by the user in the browser settings.

If this policy is left unset, background mode is initially disabled and can be controlled by the user in the browser settings.

Example value:
0x00000001 (Windows), true (Linux)
Back to top

BlockThirdPartyCookies

Block third party cookies
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\BlockThirdPartyCookies`
Mac/Linux preference name:
`BlockThirdPartyCookies`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 10
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Blocks third party cookies.

Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browser's address bar.

Disabling this setting allows cookies to be set by web page elements that are not from the domain that is in the browser's address bar and prevents users from changing this setting.

If this policy is left not set, third party cookies will be enabled but the user will be able to change that.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

BookmarkBarEnabled

Enable Bookmark Bar
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\BookmarkBarEnabled`
Mac/Linux preference name:
`BookmarkBarEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 12
- Google Chrome OS (Google Chrome OS) since version 12

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables the bookmark bar on Google Chrome.

If you enable this setting, Google Chrome will show a bookmark bar.

If you disable this setting, users will never see the bookmark bar.

If you enable or disable this setting, users cannot change or override it in Google Chrome.

If this setting is left not set the user can decide to use this function or not.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

BrowserAddPersonEnabled

Enable add person in profile manager
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\BrowserAddPersonEnabled`
Mac/Linux preference name:
`BrowserAddPersonEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 39

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If this policy is set to true or not configured, Google Chrome will allow Add Person from the user manager.

If this policy is set to false, Google Chrome will not allow creation of new profiles from the profile manager.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

BrowserGuestModeEnabled

Enable guest mode in browser
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\BrowserGuestModeEnabled`
Mac/Linux preference name:
`BrowserGuestModeEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 38

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If this policy is set to true or not configured, Google Chrome will enable guest logins. Guest logins are Google Chrome profiles where all windows are in incognito mode.

If this policy is set to false, Google Chrome will not allow guest profiles to be started.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

BuiltInDnsClientEnabled

Use built-in DNS client
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\BuiltInDnsClientEnabled`
Mac/Linux preference name:
`BuiltInDnsClientEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Controls whether the built-in DNS client is used in Google Chrome.

If this policy is set to true, the built-in DNS client will be used, if available.

If this policy is set to false, the built-in DNS client will never be used.

If this policy is left not set, the users will be able to change whether the built-in DNS client is used by editing chrome://flags or specifying a command-line flag.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

CaptivePortalAuthenticationIgnoresProxy

Captive portal authentication ignores proxy
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

This policy allows Google Chrome OS to bypass any proxy for captive portal authentication.

This policy only takes effect if a proxy is configured (for example through policy, by the user in chrome://settings, or by extensions).

If you enable this setting, any captive portal authentication pages (i.e. all web pages starting from captive portal signin page until Google Chrome detects succesful internet connection) will be displayed in a separate window ignoring all policy settings and restrictions for the current user.

If you disable this setting or leave it unset, any captive portal authentication pages will be shown in a (regular) new browser tab, using the current user's proxy settings.

Back to top

CertificateTransparencyEnforcementDisabledForUrls

Disable Certificate Transparency enforcement for a list of URLs

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDisabledForUrls`

Mac/Linux preference name:

`CertificateTransparencyEnforcementDisabledForUrls`

Android restriction name:

`CertificateTransparencyEnforcementDisabledForUrls`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 53
- Google Chrome OS (Google Chrome OS) since version 53
- Google Chrome (Android) since version 53

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Disables enforcing Certificate Transparency requirements to the listed URLs.

This policy allows certificates for the hostnames in the specified URLs to not be disclosed via Certificate Transparency. This allows certificates that would otherwise be untrusted, because they were not properly publicly disclosed, to continue to be used, but makes it harder to detect misissued certificates for those hosts.

A URL pattern is formatted according to https://www.chromium.org/administrators/url-blacklist-filter-format. However, because certificates are valid for a given hostname independent of the scheme, port, or path, only the hostname portion of the URL is considered. Wildcard hosts are not supported.

If this policy is not set, any certificate that is required to be disclosed via Certificate Transparency will be treated as untrusted if it is not disclosed according to the Certificate Transparency policy.

Example value:

Windows:

```
Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDis
abledForUrls\1 = "example.com"
Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDis
abledForUrls\2 = ".example.com"
```
Android/Linux:
```
["example.com", ".example.com"]
```
Mac:
```
<array>
  <string>example.com</string>
  <string>.example.com</string>
</array>
```
Back to top

ChromeOsLockOnIdleSuspend

Enable lock when the device become idle or suspended
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 9

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enable lock when Google Chrome OS devices become idle or suspended.

If you enable this setting, users will be asked for a password to unlock the device from sleep.

If you disable this setting, users will not be asked for a password to unlock the device from sleep.

If you enable or disable this setting, users cannot change or override it.

If the policy is left not set the user can choose whether they want to be asked for password to unlock the device or not.

Back to top

ChromeOsMultiProfileUserBehavior

Control the user behavior in a multiprofile session
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 31

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Control the user behavior in a multiprofile session on Google Chrome OS devices.

If this policy is set to 'MultiProfileUserBehaviorUnrestricted', the user can be either primary or secondary user in a multiprofile session.

If this policy is set to 'MultiProfileUserBehaviorMustBePrimary', the user can only be the primary user in a multiprofile session.

If this policy is set to 'MultiProfileUserBehaviorNotAllowed', the user cannot be part of a multiprofile session.

If you set this setting, users cannot change or override it.

If the setting is changed while the user is signed into a multiprofile session, all users in the session will be checked against their corresponding settings. The session will be closed if any one of the users is no longer allowed to be in the session.

If the policy is left not set, the default value 'MultiProfileUserBehaviorMustBePrimary' applies for enterprise-managed users and 'MultiProfileUserBehaviorUnrestricted' will be used for non-managed users.

- "unrestricted" = Allow enterprise user to be both primary and secondary (Default behavior for non-managed users)
- "primary-only" = Allow enterprise user to be primary multiprofile user only (Default behavior for enterprise-managed users)
- "not-allowed" = Do not allow enterprise user to be part of multiprofile (primary or secondary)

Note for Google Chrome OS devices supporting Android apps:

When multiple users are logged in, only the primary user can use Android apps.

Back to top

ChromeOsReleaseChannel

Release channel
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies the release channel that this device should be locked to.

- "stable-channel" = Stable channel
- "beta-channel" = Beta channel
- "dev-channel" = Dev channel (may be unstable)

Back to top

ChromeOsReleaseChannelDelegated

Whether the release channel should be configurable by the user
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19

Supported features:
Dynamic Policy Refresh: Yes
Description:

If this policy is set to True and the ChromeOsReleaseChannel policy is not specified then users of the enrolling domain will be allowed to change the release channel of the device. If this policy is set to false the device will be locked in whatever channel it was last set.

The user selected channel will be overridden by the ChromeOsReleaseChannel policy, but if the policy channel is more stable than the one that was installed on the device, then the channel will only switch after the version of the more stable channel reaches a higher version number than the one installed on the device.

Back to top

ClearSiteDataOnExit (deprecated)

Clear site data on browser shutdown (deprecated)
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ClearSiteDataOnExit`
Mac/Linux preference name:
`ClearSiteDataOnExit`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11 until version 28
- Google Chrome OS (Google Chrome OS) since version 11 until version 28

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy has been retired as of Google Chrome version 29.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

CloudPrintProxyEnabled

Enable Google Cloud Print proxy
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\CloudPrintProxyEnabled`
Mac/Linux preference name:
`CloudPrintProxyEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 17

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables Google Chrome to act as a proxy between Google Cloud Print and legacy printers connected to the machine.

If this setting is enabled or not configured, users can enable the cloud print proxy by authentication with their Google account.

If this setting is disabled, users cannot enable the proxy, and the machine will not be allowed to share it's printers with Google Cloud Print.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

CloudPrintSubmitEnabled

Enable submission of documents to Google Cloud Print
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\CloudPrintSubmitEnabled`
Mac/Linux preference name:
`CloudPrintSubmitEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 17

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables Google Chrome to submit documents to Google Cloud Print for printing. NOTE: This only affects Google Cloud Print support in Google Chrome. It does not prevent users from submitting print jobs on web sites.

If this setting is enabled or not configured, users can print to Google Cloud Print from the Google Chrome print dialog.

If this setting is disabled, users cannot print to Google Cloud Print from the Google Chrome print dialog

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ComponentUpdatesEnabled

Enables component updates in Google Chrome.
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ComponentUpdatesEnabled`
Mac/Linux preference name:
`ComponentUpdatesEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 54
- Google Chrome OS (Google Chrome OS) since version 54

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Enables component updates for all components in Google Chrome when not set or set to True.

If set to False, updates to components are disabled. However, some components are exempt from this policy: updates to any component that does not contain executable code, or does not significantly alter the behavior of the browser, or is critical for its security will not be disabled. Examples of such components include the certificate revocation lists and safe browsing data.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ContextualSearchEnabled

Enable Touch to Search
Data type:
Boolean
Android restriction name:
`ContextualSearchEnabled`
Supported on:

- Google Chrome (Android) since version 40

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables the availability of Touch to Search in Google Chrome's content view.

If you enable this setting, Touch to Search will be available to the user and they can choose to turn the feature on or off.

If you disable this setting, Touch to Search will be disabled completely.

If this policy is left not set, it is equivalent to being enabled, see description above.

Example value:
true (Android)
Back to top

DHEEnabled

Whether DHE cipher suites in TLS are enabled
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DHEEnabled`
Mac/Linux preference name:
`DHEEnabled`
Android restriction name:

`DHEEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 53 until version 57
- Google Chrome OS (Google Chrome OS) since version 53 until version 57
- Google Chrome (Android) since version 53 until version 57
- Google Chrome (iOS) since version 53 until version 57

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Warning: DHE will be completely removed from Google Chrome after version 57 (around March 2017) and this policy will stop working then.

If the policy is not set, or is set to false, then DHE cipher suites in TLS will not be enabled. Otherwise it may be set to true to enable DHE cipher suites and retain compatibility with an outdated server. This is a stopgap measure and the server should be reconfigured.

Servers are encouraged to migrated to ECDHE cipher suites. If these are unavailable, ensure a cipher suite using RSA key exchange is enabled.

Example value:

0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)

Back to top

DataCompressionProxyEnabled

Enable the data compression proxy feature

Data type:

Boolean

Android restriction name:

`DataCompressionProxyEnabled`

Supported on:

- Google Chrome (Android) since version 31

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enable or disable the data compression proxy and prevents users from changing this setting.

If you enable or disable this setting, users cannot change or override this setting.

If this policy is left not set, the data compression proxy feature will be available for the user to choose whether to use it or not.

Example value:

true (Android)

Back to top

DefaultBrowserSettingEnabled

Set Google Chrome as Default Browser

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultBrowserSettingEnabled`

Mac/Linux preference name:

`DefaultBrowserSettingEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Configures the default browser checks in Google Chrome and prevents users from changing them.

If you enable this setting, Google Chrome will always check on startup whether it is the default browser and automatically register itself if possible.

If this setting is disabled, Google Chrome will never check if it is the default browser and will disable user controls for setting this option.

If this setting is not set, Google Chrome will allow the user to control whether it is the default browser and whether user notifications should be shown when it isn't.

Example value:

0x00000001 (Windows), true (Linux), <true /> (Mac)

Back to top

DefaultPrinterSelection

Default printer selection rules

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\DefaultPrinterSelection`

Mac/Linux preference name:

`DefaultPrinterSelection`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 48
- Google Chrome OS (Google Chrome OS) since version 48

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Overrides Google Chrome default printer selection rules.

This policy determines the rules for selecting the default printer in Google Chrome which happens the first time the print function is used with a profile.

When this policy is set, Google Chrome will attempt to find a printer matching all of the specified attributes, and select it as default printer. The first printer found matching the policy is selected, in case of non-unique match any matching printer can be selected, depending on the order printers are discovered.

If this policy is not set or matching printer is not found within the timeout, the printer defaults to built-in PDF printer or no printer selected, when PDF printer is not available.

The value is parsed as JSON object, conforming to the following schema: { "type": "object", "properties": { "kind": { "description": "Whether to limit the search of the matching printer to a specific set of printers.", "type": { "enum": ["local", "cloud"] } }, "idPattern": { "description": "Regular expression to match printer id.", "type": "string" }, "namePattern": { "description": "Regular expression to match printer display name.", "type": "string" } } }

Printers connected to Google Cloud Print are considered "cloud", the rest of the printers are classified as "local". Omitting a field means all values match, for example, not specifying connectivity will cause Print Preview to initiate the discovery of all kinds of printers, local and cloud. Regular expression patterns must follow the JavaScript RegExp syntax and matches are case sensistive.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on Android apps.

Example value:
"{ "kind": "cloud", "idPattern": ".*public", "namePattern": ".*Color" }"
Back to top

DeveloperToolsDisabled

Disable Developer Tools
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DeveloperToolsDisabled`
Mac/Linux preference name:
`DeveloperToolsDisabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Disables the Developer Tools and the JavaScript console.

If you enable this setting, the Developer Tools can not be accessed and web-site elements can not be inspected anymore. Any keyboard shortcuts and any menu or context menu entries to open the Developer Tools or the JavaScript Console will be disabled.

Setting this option to disabled or leaving it not set allows the user to use the Developer Tools and the JavaScript console.

Note for Google Chrome OS devices supporting Android apps:

This policy also controls access to Android Developer Options. If you set this policy to true, users cannot access Developer Options. If you set this policy to false or leave it unset, users can access Developer Options by tapping seven times on the build number in the Android settings app.

Example value:

0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

DeviceAllowBluetooth

Allow bluetooth on device

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 52

Supported features:

Dynamic Policy Refresh: No

Description:

If this policy is set to false, Google Chrome OS will disable Bluetooth and the user cannot enable it back.

If this policy is set to true or left unset, the user will be able to enable or disable Bluetooth as they wish.

If this policy is set, the user cannot change or override it.

After enabling Bluetooth, the device must be rebooted for the changes to take effect (no need to reboot the device when disabling Bluetooth).

Back to top

DeviceAllowNewUsers

Allow creation of new user accounts

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 12

Supported features:

Dynamic Policy Refresh: Yes

Description:

Controls whether Google Chrome OS allows new user accounts to be created. If this policy is set to false, users that do not have an account already will not be able to login.

If this policy is set to true or not configured, new user accounts will be allowed to be created provided that DeviceUserWhitelist does not prevent the user from logging in.

Note for Google Chrome OS devices supporting Android apps:

This policy controls whether new users can be added to Google Chrome OS. It does not prevent users from signing in to additional Google accounts within Android. If you want to prevent this, configure the Android-specific accountTypesWithManagementDisabled policy as part of ArcPolicy.

Back to top

DeviceAllowRedeemChromeOsRegistrationOffers

Allow users to redeem offers through Chrome OS Registration
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes
Description:

IT admins for enterprise devices can use this flag to control whether to allow users to redeem offers through Chrome OS Registration.

If this policy is set to true or left not set, users will be able to redeem offers through Chrome OS Registration.

If this policy is set to false, user will not be able to redeem offers.

Back to top

DeviceAppPack

List of AppPack extensions
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19 until version 40

Supported features:
Dynamic Policy Refresh: Yes
Description:

This policy is active in retail mode only.

Lists extensions that are automatically installed for the Demo user, for devices in retail mode. These extensions are saved in the device and can be installed while offline, after the installation.

Each list entry contains a dictionary that must include the extension ID in the 'extension-id' field, and its update URL in the 'update-url' field.

Back to top

DeviceAutoUpdateDisabled

Disables Auto Update
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19

Supported features:
Dynamic Policy Refresh: Yes
Description:

Disables automatic updates when set to True.

Google Chrome OS devices automatically check for updates when this setting is not configured or set to False.

Back to top

DeviceAutoUpdateP2PEnabled

Auto update p2p enabled
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 31

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies whether p2p is to be used for OS update payloads. If set to True, devices will share and attempt to consume update payloads on the LAN, potentially reducing Internet bandwidth usage and congestion. If the update payload is not available on the LAN, the device will fall back to downloading from an update server. If set to False or not configured, p2p will not be used.

Back to top

DeviceBlockDevmode

Block developer mode
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 37

Supported features:
Dynamic Policy Refresh: Yes
Description:

Block developer mode.

If this policy is set to True, Google Chrome OS will prevent the device from booting into developer mode. The system will refuse to boot and show an error screen when the developer switch is turned on.

If this policy is unset or set to False, developer mode will remain available for the device.

Note for Google Chrome OS devices supporting Android apps:

This policy controls Google Chrome OS developer mode only. If you want to prevent access to Android Developer Options, you need to set the DeveloperToolsDisabled policy.

Back to top

DeviceDataRoamingEnabled

Enable data roaming
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 12

Supported features:
Dynamic Policy Refresh: Yes
Description:

Determines whether data roaming should be enabled for the device. If set to true, data roaming is allowed. If left unconfigured or set to false, data roaming will be not available.

Back to top

DeviceEphemeralUsersEnabled

Wipe user data on sign-out
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19

Supported features:
Dynamic Policy Refresh: Yes
Description:

Determines whether Google Chrome OS keeps local account data after logout. If set to true, no persistent accounts are kept by Google Chrome OS and all data from the user session will be discarded after logout. If this policy is set to false or not configured, the device may keep (encrypted) local user data.

Back to top

DeviceGuestModeEnabled

Enable guest mode
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 12

Supported features:
Dynamic Policy Refresh: Yes
Description:

If this policy is set to true or not configured, Google Chrome OS will enable guest logins. Guest logins are anonymous user sessions and do not require a password.

If this policy is set to false, Google Chrome OS will not allow guest sessions to be started.

Back to top

DeviceIdleLogoutTimeout

Timeout until idle user log-out is executed
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19 until version 40

Supported features:
Dynamic Policy Refresh: Yes
Description:

This policy is active in retail mode only.

When the value of this policy is set and is not 0 then the currently logged in demo user will be logged out automatically after an inactivity time of the specified duration has elapsed.

The policy value should be specified in milliseconds.

Back to top

DeviceIdleLogoutWarningDuration

Duration of the idle log-out warning message
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19 until version 40

Supported features:
Dynamic Policy Refresh: Yes
Description:

This policy is active in retail mode only.

When DeviceIdleLogoutTimeout is specified this policy defines the duration of the warning box with a count down timer that is shown to the user before the logout is executed.

The policy value should be specified in milliseconds.

Back to top

DeviceLocalAccountAutoLoginBailoutEnabled

Enable bailout keyboard shortcut for auto-login
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 28

Supported features:
Dynamic Policy Refresh: Yes
Description:

Enable bailout keyboard shortcut for auto-login.

If this policy is unset or set to True and a device-local account is configured for zero-delay auto-login, Google Chrome OS will honor the keyboard shortcut Ctrl+Alt+S for bypassing auto-login and showing the login screen.

If this policy is set to False, zero-delay auto-login (if configured) cannot be bypassed.

Back to top

DeviceLocalAccountAutoLoginDelay

Public session auto-login timer
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes
Description:

The public session auto-login delay.

If the |DeviceLocalAccountAutoLoginId| policy is unset, this policy has no effect. Otherwise:

If this policy is set, it determines the amount of time without user activity that should elapse before automatically logging into the public session specified by the |DeviceLocalAccountAutoLoginId| policy.

If this policy is unset, 0 milliseconds will be used as the timeout.

This policy is specified in milliseconds.

Back to top

DeviceLocalAccountAutoLoginId

Public session for auto-login
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes
Description:

A public session to auto-login after a delay.

If this policy is set, the specified session will be automatically logged in after a period of time has elapsed at the login screen without user interaction. The public session must already be configured (see |DeviceLocalAccounts|).

If this policy is unset, there will be no auto-login.

Back to top

DeviceLocalAccountPromptForNetworkWhenOffline

Enable network configuration prompt when offline
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 33

Supported features:
Dynamic Policy Refresh: Yes
Description:

Enable network configuration prompt when offline.

If this policy is unset or set to True and a device-local account is configured for zero-delay auto-login and the device does not have access to the Internet, Google Chrome OS will show a network configuration prompt.

If this policy is set to False, an error message will be displayed instead of the network configuration prompt.

Back to top

DeviceLocalAccounts

Device-local accounts
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 25

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies the list of device-local accounts to be shown on the login screen.

Every list entry specifies an identifier, which is used internally to tell the different device-local accounts apart.

Back to top

DeviceLoginScreenDomainAutoComplete

Enable domain name autocomplete during user sign in
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 44

Supported features:

Dynamic Policy Refresh: Yes

Description:

If this policy is set to a blank string or not configured, Google Chrome OS will not show an autocomplete option during user sign-in flow. If this policy is set to a string representing a domain name, Google Chrome OS will show an autocomplete option during user sign-in allowing the user to type in only their user name without the domain name extension. The user will be able to overwrite this domain name extension.

Back to top

DeviceLoginScreenPowerManagement

Power management on the login screen

Data type:

Dictionary

Supported on:

- Google Chrome OS (Google Chrome OS) since version 30

Supported features:

Dynamic Policy Refresh: Yes

Description:

Configure power management on the login screen in Google Chrome OS.

This policy lets you configure how Google Chrome OS behaves when there is no user activity for some amount of time while the login screen is being shown. The policy controls multiple settings. For their individual semantics and value ranges, see the corresponding policies that control power management within a session. The only deviations from these policies are: * The actions to take on idle or lid close cannot be to end the session. * The default action taken on idle when running on AC power is to shut down.

If a setting is left unspecified, a default value is used.

If this policy is unset, defaults are used for all settings.

Back to top

DeviceLoginScreenSaverId

Screen saver to be used on the sign-in screen in retail mode

Data type:

String

Supported on:

- Google Chrome OS (Google Chrome OS) since version 19 until version 40

Supported features:

Dynamic Policy Refresh: Yes

Description:

This policy is active in retail mode only.

Determines the id of the extension to be used as a screen saver on the sign-in screen. The extension must be part of the AppPack that is configured for this domain through the DeviceAppPack policy.

Back to top

DeviceLoginScreenSaverTimeout

Duration of inactivity before the screen saver is shown on the sign-in screen in retail mode
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 19 until version 40

Supported features:
Dynamic Policy Refresh: Yes
Description:

This policy is active in retail mode only.

Determines the duration before the screen saver is shown on the sign-in screen for devices in retail mode.

The policy value should be specified in milliseconds.

Back to top

DeviceMetricsReportingEnabled

Enable metrics reporting
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 14

Supported features:
Dynamic Policy Refresh: Yes
Description:

Controls whether usage metrics are reported back to Google. If set to true, Google Chrome OS will report usage metrics. If not configured or set to false, metrics reporting will be disabled.

Note for Google Chrome OS devices supporting Android apps:

This policy also controls Android usage and diagnostic data collection.

Back to top

DeviceOpenNetworkConfiguration

Device-level network configuration
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 16

Supported features:

Dynamic Policy Refresh: Yes

Description:

Allows pushing network configuration to be applied for all users of a Google Chrome OS device. The network configuration is a JSON-formatted string as defined by the Open Network Configuration format described at https://sites.google.com/a/chromium.org/dev/chromium-os/chromiumos-design-docs/open-network-configuration

Note for Google Chrome OS devices supporting Android apps:

Android apps can use the network configurations and CA certificates set via this policy, but do not have access to some configuration options.

Back to top

DevicePolicyRefreshRate

Refresh rate for Device Policy

Data type:

Integer

Supported on:

- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes

Description:

Specifies the period in milliseconds at which the device management service is queried for device policy information.

Setting this policy overrides the default value of 3 hours. Valid values for this policy are in the range from 1800000 (30 minutes) to 86400000 (1 day). Any values not in this range will be clamped to the respective boundary.

Leaving this policy not set will make Google Chrome OS use the default value of 3 hours.

Note that if the platform supports policy notifications, the refresh delay will be set to 24 hours (ignoring all defaults and the value of this policy) because it is expected that policy notifications will force a refresh automatically whenever policy changes, making more frequent refreshes unnecessary.

Back to top

DeviceQuirksDownloadEnabled

Enable queries to Quirks Server for hardware profiles

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 51

Supported features:

Dynamic Policy Refresh: Yes

Description:

The Quirks Server provides hardware-specific configuration files, like ICC display profiles to adjust monitor calibration.

When this policy is set to false, the device will not attempt to contact the Quirks Server to download configuration files.

If this policy is true or not configured then Google Chrome OS will automatically contact the Quirks Server and download configuration files, if available, and store them on the device. Such files might, for example, be used to improve display quality of attached monitors.

Back to top

DeviceRebootOnShutdown

Automatic reboot on device shutdown
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 41

Supported features:
Dynamic Policy Refresh: Yes
Description:

If this policy is set to false or not configured, Google Chrome OS will allow the user to shut down the device. If this policy is set to true, Google Chrome OS will trigger a reboot when the user shuts down the device. Google Chrome OS replaces all occurrences of shutdown buttons in the UI by reboot buttons. If the user shuts down the device using the power button, it will not automatically reboot, even if the policy is enabled.

Back to top

DeviceShowUserNamesOnSignin

Show usernames on login screen
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 12

Supported features:
Dynamic Policy Refresh: Yes
Description:

If this policy is set to true or not configured, Google Chrome OS will show existing users on the login screen and allow to pick one. If this policy is set to false, Google Chrome OS will use the username/password prompt for login.

Back to top

DeviceStartUpFlags

System wide flags to be applied on Google Chrome start-up
Data type:

List of strings

Supported on:

- Google Chrome OS (Google Chrome OS) since version 27

Supported features:

Dynamic Policy Refresh: No

Description:

Specifies the flags that should be applied to Google Chrome when it starts. The specified flags are applied on the login screen only. Flags set via this policy do not propagate into user sessions.

Back to top

DeviceStartUpUrls

Load specified urls on demo login

Data type:

List of strings

Supported on:

- Google Chrome OS (Google Chrome OS) since version 19 until version 40

Supported features:

Dynamic Policy Refresh: Yes

Description:

This policy is active in retail mode only.

Determines the set of URLs to be loaded when the demo session is started. This policy will override any other mechanisms for setting the initial URL and thus can only be applied to a session not associated with a particular user.

Back to top

DeviceTargetVersionPrefix

Target Auto Update Version

Data type:

String

Supported on:

- Google Chrome OS (Google Chrome OS) since version 19

Supported features:

Dynamic Policy Refresh: Yes

Description:

Sets a target version for Auto Updates.

Specifies the prefix of a target version Google Chrome OS should update to. If the device is running a version that's before the specified prefix, it will update to the latest version with the given prefix. If the device is already on a later version, there is no effect (i.e. no downgrades are performed) and the device will remain on the current version. The prefix format works component-wise as is demonstrated in the following example:

"" (or not configured): update to latest version available. "1412.": update to any minor version of 1412 (e.g. 1412.24.34 or 1412.60.2) "1412.2.": update to any minor version of 1412.2 (e.g. 1412.2.34 or 1412.2.2) "1412.24.34": update to this specific version only

Back to top

DeviceTransferSAMLCookies

Transfer SAML IdP cookies during login
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 38

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies whether authentication cookies set by a SAML IdP during login should be transferred to the user's profile.

When a user authenticates via a SAML IdP during login, cookies set by the IdP are written to a temporary profile at first. These cookies can be transferred to the user's profile to carry forward the authentication state.

When this policy is set to true, cookies set by the IdP are transferred to the user's profile every time they authenticate against the SAML IdP during login.

When this policy is set to false or unset, cookies set by the IdP are transferred to the user's profile during their first login on a device only.

This policy affects users whose domain matches the device's enrollment domain only. For all other users, cookies set by the IdP are transferred to the user's profile during their first login on the device only.

Note for Google Chrome OS devices supporting Android apps:

Cookies transferred to the user's profile are not accessible to Android apps.

Back to top

DeviceUpdateAllowedConnectionTypes

Connection types allowed for updates
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 21

Supported features:
Dynamic Policy Refresh: Yes
Description:

The types of connections that are allowed to use for OS updates. OS updates potentially put heavy strain on the connection due to their size and may incur additional cost. Therefore, they are by default not enabled for connection types that are considered expensive, which include WiMax, Bluetooth and Cellular at the moment.

The recognized connection type identifiers are "ethernet", "wifi", "wimax", "bluetooth" and "cellular".

Back to top

DeviceUpdateHttpDownloadsEnabled

Allow autoupdate downloads via HTTP
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes
Description:

Auto-update payloads on Google Chrome OS can be downloaded via HTTP instead of HTTPS. This allows transparent HTTP caching of HTTP downloads.

If this policy is set to true, Google Chrome OS will attempt to download auto-update payloads via HTTP. If the policy is set to false or not set, HTTPS will be used for downloading auto-update payloads.

Back to top

DeviceUpdateScatterFactor

Auto update scatter factor
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 20

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies the number of seconds up to which a device may randomly delay its download of an update from the time the update was first pushed out to the server. The device may wait a portion of this time in terms of wall-clock-time and the remaining portion in terms of the number of update checks. In any case, the scatter is upper bounded to a constant amount of time so that a device does not ever get stuck waiting to download an update forever.

Back to top

DeviceUserWhitelist

Login user white list
Data type:
List of strings

Supported on:

- Google Chrome OS (Google Chrome OS) since version 12

Supported features:
Dynamic Policy Refresh: Yes
Description:

Defines the list of users that are allowed to login to the device. Entries are of the form user@domain, such as madmax@managedchrome.com. To allow arbitrary users on a domain, use entries of the form *@domain.

If this policy is not configured, there are no restrictions on which users are allowed to sign in. Note that creating new users still requires the DeviceAllowNewUsers policy to be configured appropriately.

Note for Google Chrome OS devices supporting Android apps:

This policy controls who may start a Google Chrome OS session. It does not prevent users from signing in to additional Google accounts within Android. If you want to prevent this, configure the Android-specific accountTypesWithManagementDisabled policy as part of ArcPolicy.

Back to top

Disable3DAPIs

Disable support for 3D graphics APIs
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\Disable3DAPIs`
Mac/Linux preference name:
`Disable3DAPIs`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 9
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Disable support for 3D graphics APIs.

Enabling this setting prevents web pages from accessing the graphics processing unit (GPU). Specifically, web pages can not access the WebGL API and plugins can not use the Pepper 3D API.

Disabling this setting or leaving it not set potentially allows web pages to use the WebGL API and plugins to use the Pepper 3D API. The default settings of the browser may still require command line arguments to be passed in order to use these APIs.

If HardwareAccelerationModeEnabled is set to false, Disable3DAPIs is ignored and it is equivalent to Disable3DAPIs being set to true.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

DisablePluginFinder

Specify whether the plugin finder should be disabled
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DisablePluginFinder`
Mac/Linux preference name:
`DisablePluginFinder`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If you set this setting to enabled the automatic search and installation of missing plugins will be disabled in Google Chrome.

Setting this option to disabled or leave it not set the plugin finder will be active.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

DisablePrintPreview (deprecated)

Disable Print Preview (deprecated)
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DisablePrintPreview`
Mac/Linux preference name:
`DisablePrintPreview`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 18

Supported features:
Dynamic Policy Refresh: No, Per Profile: Yes
Description:

Show the system print dialog instead of print preview.

When this setting is enabled, Google Chrome will open the system print dialog instead of the built-in print preview when a user requests a page to be printed.

If this policy is not set or is set to false, print commands trigger the print preview screen.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

DisableSSLRecordSplitting

Disable TLS False Start

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DisableSSLRecordSplitting`

Mac/Linux preference name:

`DisableSSLRecordSplitting`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 18 until version 46
- Google Chrome OS (Google Chrome OS) since version 18 until version 46

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Specifies whether the TLS False Start optimization should be disabled. For historical reasons, this policy is named DisableSSLRecordSplitting.

If the policy is not set, or is set to false, then TLS False Start will be enabled. If it is set to true, TLS False Start will be disabled.

Example value:

0x00000001 (Windows), true (Linux), <true /> (Mac)

Back to top

DisableSafeBrowsingProceedAnyway

Disable proceeding from the Safe Browsing warning page

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\DisableSafeBrowsingProceedAnyway`

Mac/Linux preference name:

`DisableSafeBrowsingProceedAnyway`

Android restriction name:

`DisableSafeBrowsingProceedAnyway`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22
- Google Chrome OS (Google Chrome OS) since version 22
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

The Safe Browsing service shows a warning page when users navigate to sites that are flagged as potentially malicious. Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site.

If this setting is disabled or not configured then users can choose to proceed to the flagged site after being shown the warning.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

DisableScreenshots

Disable taking screenshots
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DisableScreenshots`
Mac/Linux preference name:
`DisableScreenshots`
Supported on:

- Google Chrome OS (Google Chrome OS) since version 22
- Google Chrome (Linux, Mac, Windows) since version 22

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Disables taking screenshots.

If enabled screenshots cannot be taken using keyboard shortcuts or extension APIs.

If disabled or not specified, taking screenshots is allowed.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

DisableSpdy (deprecated)

Disable SPDY protocol
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DisableSpdy`
Mac/Linux preference name:
`DisableSpdy`
Android restriction name:
`DisableSpdy`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8 until version 53
- Google Chrome OS (Google Chrome OS) since version 11 until version 53
- Google Chrome (Android) since version 30 until version 53

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

This policy is deprecated in M53 and removed in M54, because SPDY/3.1 support is removed.

Disables use of the SPDY protocol in Google Chrome.

If this policy is enabled the SPDY protocol will not be available in Google Chrome.

Setting this policy to disabled will allow the usage of SPDY.

If this policy is left not set, SPDY will be available.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

DisabledPlugins

Specify a list of disabled plugins
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\DisabledPlugins`
Mac/Linux preference name:
`DisabledPlugins`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies a list of plugins that are disabled in Google Chrome and prevents users from changing this setting.

The wildcard characters '*' and '?' can be used to match sequences of arbitrary characters. '*' matches an arbitrary number of characters while '?' specifies an optional single character, i.e. matches zero or one characters. The escape character is '\', so to match actual '*', '?', or '\' characters, you can put a '\' in front of them.

If you enable this setting, the specified list of plugins is never used in Google Chrome. The plugins are marked as disabled in 'about:plugins' and users cannot enable them.

Note that this policy can be overridden by EnabledPlugins and DisabledPluginsExceptions.

If this policy is left not set the user can use any plugin installed on the system except for hard-coded incompatible, outdated or dangerous plugins.

Example value:
Windows:
```
Software\Policies\Google\Chrome\DisabledPlugins\1 = "Java"
Software\Policies\Google\Chrome\DisabledPlugins\2 = "Shockwave Flash"
Software\Policies\Google\Chrome\DisabledPlugins\3 = "Chrome PDF
Viewer"
```
Android/Linux:
```
["Java", "Shockwave Flash", "Chrome PDF Viewer"]
```
Mac:
```
<array>
  <string>Java</string>
  <string>Shockwave Flash</string>
  <string>Chrome PDF Viewer</string>
</array>
```

Back to top

DisabledPluginsExceptions

Specify a list of plugins that the user can enable or disable

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\DisabledPluginsExceptions`

Mac/Linux preference name:

`DisabledPluginsExceptions`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Specifies a list of plugins that user can enable or disable in Google Chrome.

The wildcard characters '*' and '?' can be used to match sequences of arbitrary characters. '*' matches an arbitrary number of characters while '?' specifies an optional single character, i.e. matches zero or one characters. The escape character is '\', so to match actual '*', '?', or '\' characters, you can put a '\' in front of them.

If you enable this setting, the specified list of plugins can be used in Google Chrome. Users can enable or disable them in 'about:plugins', even if the plugin also matches a pattern in DisabledPlugins. Users can also enable and disable plugins that don't match any patterns in DisabledPlugins, DisabledPluginsExceptions and EnabledPlugins.

This policy is meant to allow for strict plugin blacklisting where the 'DisabledPlugins' list contains wildcarded entries like disable all plugins '*' or disable all Java plugins '*Java*' but the administrator wishes to enable some particular version like 'IcedTea Java 2.3'. This particular versions can be specified in this policy.

Note that both the plugin name and the plugin's group name have to be exempted. Each plugin group is shown in a separate section in about:plugins; each section may have one or more plugins. For example, the "Shockwave Flash" plugin belongs to the "Adobe Flash Player" group, and both names have to have a match in the exceptions list if that plugin is to be exempted from the blacklist.

If this policy is left not set any plugin that matches the patterns in the 'DisabledPlugins' will be locked disabled and the user won't be able to enable them.

Example value:

Windows:

```
Software\Policies\Google\Chrome\DisabledPluginsExceptions\1 = "Java"
Software\Policies\Google\Chrome\DisabledPluginsExceptions\2 =
"Shockwave Flash"
Software\Policies\Google\Chrome\DisabledPluginsExceptions\3 = "Chrome
PDF Viewer"
```

Android/Linux:

```
["Java", "Shockwave Flash", "Chrome PDF Viewer"]
```

Mac:

```
<array>
```

```
    <string>Java</string>
    <string>Shockwave Flash</string>
    <string>Chrome PDF Viewer</string>
  </array>
```

Back to top

DisabledSchemes (deprecated)

Disable URL protocol schemes

Data type:

List of strings

Windows registry location:

`Software\Policies\Google\Chrome\DisabledSchemes`

Mac/Linux preference name:

`DisabledSchemes`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 12
- Google Chrome OS (Google Chrome OS) since version 12

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

This policy is deprecated, please use URLBlacklist instead.

Disables the listed protocol schemes in Google Chrome.

URLs using a scheme from this list will not load and can not be navigated to.

If this policy is left not set or the list is empty all schemes will be accessible in Google Chrome.

Example value:

Windows:

```
Software\Policies\Google\Chrome\DisabledSchemes\1 = "file"
Software\Policies\Google\Chrome\DisabledSchemes\2 = "https"
```

Android/Linux:

```
["file", "https"]
```

Mac:

```
<array>
  <string>file</string>
  <string>https</string>
</array>
```

Back to top

DiskCacheDir

Set disk cache directory

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\DiskCacheDir`

Mac/Linux preference name:

`DiskCacheDir`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 13

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Configures the directory that Google Chrome will use for storing cached files on the disk.

If you set this policy, Google Chrome will use the provided directory regardless whether the user has specified the '--disk-cache-dir' flag or not. To avoid data loss or other unexpected errors this policy should not be set to a volume's root directory or to a directory used for other purposes, because Google Chrome manages its contents.

See https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables for a list of variables that can be used.

If this policy is left not set the default cache directory will be used and the user will be able to override it with the '--disk-cache-dir' command line flag.

Example value:
"${user_home}/Chrome_cache"
Back to top

DiskCacheSize

Set disk cache size in bytes
Data type:
Integer [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DiskCacheSize`
Mac/Linux preference name:
`DiskCacheSize`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 17

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Configures the cache size that Google Chrome will use for storing cached files on the disk.

If you set this policy, Google Chrome will use the provided cache size regardless whether the user has specified the '--disk-cache-size' flag or not. The value specified in this policy is not a hard boundary but rather a suggestion to the caching system, any value below a few megabytes is too small and will be rounded up to a sane minimum.

If the value of this policy is 0, the default cache size will be used but the user will not be able to change it.

If this policy is not set the default size will be used and the user will be able to override it with the --disk-cache-size flag.

Example value:
0x06400000 (Windows), 104857600 (Linux), 104857600 (Mac)
Back to top

DisplayRotationDefault

Set default display rotation, reapplied on every reboot
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 48

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: No
Description:

If this policy is set, each display is rotated to the specified orientation on every reboot, and the first time it is connected after the policy value has changed. Users may change the display rotation via the settings page after logging in, but their setting will be overridden by the policy value at the next reboot.

This policy applies to both the primary and all secondary displays.

If the policy is not set, the default value is 0 degrees and the user is free to change it. In this case, the default value is not reapplied at restart.

- 0 = Rotate screen by 0 degrees
- 1 = Rotate screen clockwise by 90 degrees
- 2 = Rotate screen by 180 degrees
- 3 = Rotate screen clockwise by 270 degrees

Back to top

DnsPrefetchingEnabled (deprecated)

Enable network prediction
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\DnsPrefetchingEnabled`
Mac/Linux preference name:
`DnsPrefetchingEnabled`
Android restriction name:
`DnsPrefetchingEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8 until version 53
- Google Chrome OS (Google Chrome OS) since version 11 until version 53
- Google Chrome (Android) since version 30 until version 53

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy is deprecated in M48 in favor of NetworkPredictionOptions, and removed in M54.

Enables network prediction in Google Chrome and prevents users from changing this setting.

This controls not only DNS prefetching but also TCP and SSL preconnection and prerendering of web pages. The policy name refers to DNS prefetching for historical reasons.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

If this policy is left not set, this will be enabled but the user will be able to change it.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

DownloadDirectory

Set download directory
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\DownloadDirectory`
Mac/Linux preference name:
`DownloadDirectory`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 35

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Configures the directory that Google Chrome will use for downloading files.

If you set this policy, Google Chrome will use the provided directory regardless whether the user has specified one or enabled the flag to be prompted for download location every time.

See https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables for a list of variables that can be used.

If this policy is left not set the default download directory will be used and the user will be able to change it.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on Android apps. Android apps always use the default downloads directory and cannot access any files downloaded by Google Chrome OS into a non-default downloads directory.

Example value:
"/home/${user_name}/Downloads"
Back to top

EasyUnlockAllowed

Allows Smart Lock to be used
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 38

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows Smart Lock to be used on Google Chrome OS devices.

If you enable this setting, users will be allowed to use Smart Lock if the requirements for the feature are satisfied.

If you disable this setting, users will not be allowed to use Smart Lock.

If this policy is left not set, the default is not allowed for enterprise-managed users and allowed for non-managed users.

Back to top

EditBookmarksEnabled

Enables or disables bookmark editing

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\EditBookmarksEnabled`

Mac/Linux preference name:

`EditBookmarksEnabled`

Android restriction name:

`EditBookmarksEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 12
- Google Chrome OS (Google Chrome OS) since version 12
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables or disables editing bookmarks in Google Chrome.

If you enable this setting, bookmarks can be added, removed or modified. This is the default also when this policy is not set.

If you disable this setting, bookmarks can not be added, removed or modified. Existing bookmarks are still available.

Example value:

0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)

Back to top

EnableDeprecatedWebBasedSignin (deprecated)

Enables the old web-based signin

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\EnableDeprecatedWebBasedSignin`

Mac/Linux preference name:

`EnableDeprecatedWebBasedSignin`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 35 until version 42

Supported features:
Dynamic Policy Refresh: No, Per Profile: No

Description:

Enables the old web-based signin flow.

This setting was named EnableWebBasedSignin prior to Chrome 42, and support for it will be removed entirely in Chrome 43.

This setting is useful for enterprise customers who are using SSO solutions that are not compatible with the new inline signin flow yet. If you enable this setting, the old web-based signin flow would be used. If you disable this setting or leave it not set, the new inline signin flow would be used by default. Users may still enable the old web-based signin flow through the command line flag --enable-web-based-signin.

The experimental setting will be removed in the future when the inline signin fully supports all SSO signin flows.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

EnableDeprecatedWebPlatformFeatures

Enable deprecated web platform features for a limited time

Data type:
List of strings [Android:multi-select]

Windows registry location:
`Software\Policies\Google\Chrome\EnableDeprecatedWebPlatformFeatures`

Mac/Linux preference name:
`EnableDeprecatedWebPlatformFeatures`

Android restriction name:
`EnableDeprecatedWebPlatformFeatures`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 37
- Google Chrome OS (Google Chrome OS) since version 37
- Google Chrome (Android) since version 37

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Specify a list of deprecated web platform features to re-enable temporarily.

This policy gives administrators the ability to re-enable deprecated web platform features for a limited time. Features are identified by a string tag and the features corresponding to the tags included in the list specified by this policy will get re-enabled.

If this policy is left not set, or the list is empty or does not match one of the supported string tags, all deprecated web platform features will remain disabled.

While the policy itself is supported on the above platforms, the feature it is enabling may be available on fewer platforms. Not all deprecated Web Platform features can be re-enabled. Only the ones explicitly listed below can be for a limited period of time, which is different per feature. The general format of the string tag will be [DeprecatedFeatureName]_EffectiveUntil[yyyymmdd]. As reference, you can find the intent behind the Web Platform feature changes at https://bit.ly/blinkintents.

- "ExampleDeprecatedFeature_EffectiveUntil20080902" = Enable ExampleDeprecatedFeature API through 2008/09/02

Example value:

Windows:

```
Software\Policies\Google\Chrome\EnableDeprecatedWebPlatformFeatures\1
= "ExampleDeprecatedFeature_EffectiveUntil20080902"
```

Android/Linux:

```
["ExampleDeprecatedFeature_EffectiveUntil20080902"]
```

Mac:

```
<array>
  <string>ExampleDeprecatedFeature_EffectiveUntil20080902</string>
</array>
```

Back to top

EnableMediaRouter

Enables cast

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\EnableMediaRouter`

Mac/Linux preference name:

`EnableMediaRouter`

Android restriction name:

`EnableMediaRouter`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 52
- Google Chrome OS (Google Chrome OS) since version 52
- Google Chrome (Android) since version 52

Supported features:

Dynamic Policy Refresh: No, Per Profile: Yes

Description:

If this is set to true or is not set, users will be able to cast tabs, sites or the desktop from the browser. If set to false, this option will be disabled.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

EnableOnlineRevocationChecks

Whether online OCSP/CRL checks are performed

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\EnableOnlineRevocationChecks`

Mac/Linux preference name:
`EnableOnlineRevocationChecks`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 19
- Google Chrome OS (Google Chrome OS) since version 19

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

In light of the fact that soft-fail, online revocation checks provide no effective security benefit, they are disabled by default in Google Chrome version 19 and later. By setting this policy to true, the previous behavior is restored and online OCSP/CRL checks will be performed.

If the policy is not set, or is set to false, then Google Chrome will not perform online revocation checks in Google Chrome 19 and later.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

EnableSha1ForLocalAnchors

Whether SHA-1 signed certificates issued by local trust anchors are allowed
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\EnableSha1ForLocalAnchors`
Mac/Linux preference name:
`EnableSha1ForLocalAnchors`
Android restriction name:
`EnableSha1ForLocalAnchors`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 54
- Google Chrome OS (Google Chrome OS) since version 54
- Google Chrome (Android) since version 54

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

When this setting is enabled, Google Chrome allows SHA-1 signed certificates as long as they successfully validate and chain to a locally-installed CA certificates.

Note that this policy depends on the operating system certificate verification stack allowing SHA-1 signatures. If an OS update changes the OS handling of SHA-1 certificates, this policy may no longer have effect. Further, this policy is intended as a temporary workaround to give enterprises more time to move away from SHA-1. This policy will be removed on or around January 1st 2019.

If this policy is not set, or it is set to false, then Google Chrome follows the publicly announced SHA-1 deprecation schedule.

Example value:
0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)

Back to top

EnabledPlugins

Specify a list of enabled plugins
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\EnabledPlugins`
Mac/Linux preference name:
`EnabledPlugins`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies a list of plugins that are enabled in Google Chrome and prevents users from changing this setting.

The wildcard characters '*' and '?' can be used to match sequences of arbitrary characters. '*' matches an arbitrary number of characters while '?' specifies an optional single character, i.e. matches zero or one characters. The escape character is '\', so to match actual '*', '?', or '\' characters, you can put a '\' in front of them.

The specified list of plugins is always used in Google Chrome if they are installed. The plugins are marked as enabled in 'about:plugins' and users cannot disable them.

Note that this policy overrides both DisabledPlugins and DisabledPluginsExceptions.

If this policy is left not set the user can disable any plugin installed on the system.

Example value:
Windows:
```
Software\Policies\Google\Chrome\EnabledPlugins\1 = "Java"
Software\Policies\Google\Chrome\EnabledPlugins\2 = "Shockwave Flash"
Software\Policies\Google\Chrome\EnabledPlugins\3 = "Chrome PDF
Viewer"
```
Android/Linux:
```
["Java", "Shockwave Flash", "Chrome PDF Viewer"]
```
Mac:
```
<array>
  <string>Java</string>
  <string>Shockwave Flash</string>
  <string>Chrome PDF Viewer</string>
</array>
```
Back to top

EnterpriseWebStoreName (deprecated)

Enterprise web store name (deprecated)
Data type:
String [Windows:REG_SZ]

Windows registry location:
`Software\Policies\Google\Chrome\EnterpriseWebStoreName`
Mac/Linux preference name:
`EnterpriseWebStoreName`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 17 until version 28
- Google Chrome OS (Google Chrome OS) since version 17 until version 28

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This setting has been retired as of Google Chrome version 29. The recommended way to set up organization-hosted extension/app collections is to include the site hosting the CRX packages in ExtensionInstallSources and put direct download links to the packages on a web page. A launcher for that web page can be created using the ExtensionInstallForcelist policy.

Example value:
"WidgCo Chrome Apps"
Back to top

EnterpriseWebStoreURL (deprecated)

Enterprise web store URL (deprecated)
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\EnterpriseWebStoreURL`
Mac/Linux preference name:
`EnterpriseWebStoreURL`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 17 until version 28
- Google Chrome OS (Google Chrome OS) since version 17 until version 28

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This setting has been retired as of Google Chrome version 29. The recommended way to set up organization-hosted extension/app collections is to include the site hosting the CRX packages in ExtensionInstallSources and put direct download links to the packages on a web page. A launcher for that web page can be created using the ExtensionInstallForcelist policy.

Example value:
"https://company-intranet/chromeapps"
Back to top

ExtensionCacheSize

Set Apps and Extensions cache size (in bytes)
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 43

Supported features:
Dynamic Policy Refresh: No
Description:

Google Chrome OS caches Apps and Extensions for installation by multiple users of a single device to avoid re-downloading them for each user. If this policy is not configured or the value is lower than 1 MB, Google Chrome OS will use the default cache size.

Note for Google Chrome OS devices supporting Android apps:

The cache is not used for Android apps. If multiple users install the same Android app, it will be downloaded anew for each user.

Back to top

ExternalStorageDisabled

Disable mounting of external storage
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 22

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Disable mounting of external storage.

When this policy is set to true, external storage will not be available in the file browser.

This policy affects all types of storage media. For example: USB flash drives, external hard drives, SD and other memory cards, optical storage etc. Internal storage is not affected, therefore files saved in the Download folder can still be accessed. Google Drive is also not affected by this policy.

If this setting is disabled or not configured then users can use all supported types of external storage on their device.

Back to top

ExternalStorageReadOnly

Treat external storage devices as read-only.
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 54

Supported features:
Dynamic Policy Refresh: No, Per Profile: Yes
Description:

When this policy is set to true, users cannot write anything to external storage devices.

Back to top

ForceEphemeralProfiles

Ephemeral profile
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ForceEphemeralProfiles`
Mac/Linux preference name:
`ForceEphemeralProfiles`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 32

Supported features:
Dynamic Policy Refresh: No, Per Profile: Yes
Description:

If set to enabled this policy forces the profile to be switched to ephemeral mode. If this policy is specified as an OS policy (e.g. GPO on Windows) it will apply to every profile on the system; if the policy is set as a Cloud policy it will apply only to a profile signed in with a managed account.

In this mode the profile data is persisted on disk only for the length of the user session. Features like browser history, extensions and their data, web data like cookies and web databases are not preserved after the browser is closed. However this does not prevent the user from downloading any data to disk manually, save pages or print them.

If the user has enabled sync all this data is preserved in their sync profile just like with regular profiles. Incognito mode is also available if not explicitly disabled by policy.

If the policy is set to disabled or left not set signing in leads to regular profiles.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ForceGoogleSafeSearch

Force Google SafeSearch
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ForceGoogleSafeSearch`
Mac/Linux preference name:
`ForceGoogleSafeSearch`
Android restriction name:
`ForceGoogleSafeSearch`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 41
- Google Chrome OS (Google Chrome OS) since version 41
- Google Chrome (Android) since version 41

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Forces queries in Google Web Search to be done with SafeSearch set to active and prevents users from changing this setting.

If you enable this setting, SafeSearch in Google Search is always active.

If you disable this setting or do not set a value, SafeSearch in Google Search is not enforced.

Example value:
0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)
Back to top

ForceMaximizeOnFirstRun

Maximize the first browser window on first run
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 43

Supported features:
Dynamic Policy Refresh: No, Per Profile: Yes
Description:

If this policy is set to true, Google Chrome will unconditionally maximize the the first window shown on first run. If this policy is set to false or not configured, the decision whether to maximize the first window shown will be based on the screen size.

Back to top

ForceSafeSearch (deprecated)

Force SafeSearch
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ForceSafeSearch`
Mac/Linux preference name:
`ForceSafeSearch`
Android restriction name:
`ForceSafeSearch`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25
- Google Chrome OS (Google Chrome OS) since version 25
- Google Chrome (Android) since version 30

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy is deprecated, please use ForceGoogleSafeSearch and ForceYouTubeRestrict instead. This policy is ignored if either the ForceGoogleSafeSearch, the ForceYouTubeRestrict or the (deprecated) ForceYouTubeSafetyMode policies are set.

Forces queries in Google Web Search to be done with SafeSearch set to active and prevents users from changing this setting. This setting also forces Moderate Restricted Mode on YouTube.

If you enable this setting, SafeSearch in Google Search and Moderate Restricted Mode YouTube is always active.

If you disable this setting or do not set a value, SafeSearch in Google Search and Restricted Mode in YouTube is not enforced.

Example value:
0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)
Back to top

ForceYouTubeRestrict

Force minimum YouTube Restricted Mode
Data type:
Integer [Android:choice, Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ForceYouTubeRestrict`
Mac/Linux preference name:
`ForceYouTubeRestrict`
Android restriction name:
`ForceYouTubeRestrict`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 55
- Google Chrome OS (Google Chrome OS) since version 55
- Google Chrome (Android) since version 55

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enforces a minimum Restricted Mode on YouTube and prevents users from picking a less restricted mode.

If this setting is set to Strict, Strict Restricted Mode on YouTube is always active.

If this setting is set to Moderate, the user may only pick Moderate Restricted Mode and Strict Restricted Mode on YouTube, but cannot disable Restricted Mode.

If this setting is set to Off or no value is set, Restricted Mode on YouTube is not enforced by Google Chrome. External policies such as YouTube policies might still enforce Restricted Mode, though.

- 0 = Do not enforce Restricted Mode on YouTube
- 1 = Enforce at least Moderate Restricted Mode on YouTube
- 2 = Enforce Strict Restricted Mode for YouTube

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the Android YouTube app. If Safety Mode on YouTube should be enforced, installation of the Android YouTube app should be disallowed.

Example value:
0x00000000 (Windows), 0 (Linux), 0 (Android), 0 (Mac)
Back to top

ForceYouTubeSafetyMode (deprecated)

Force YouTube Safety Mode
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ForceYouTubeSafetyMode`
Mac/Linux preference name:
`ForceYouTubeSafetyMode`
Android restriction name:
`ForceYouTubeSafetyMode`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 41
- Google Chrome OS (Google Chrome OS) since version 41
- Google Chrome (Android) since version 41

Supported features:
Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy is deprecated. Consider using ForceYouTubeRestrict, which overrides this policy and allows more fine-grained tuning.

Forces YouTube Moderate Restricted Mode and prevents users from changing this setting.

If this setting is enabled, Restricted Mode on YouTube is always enforced to be at least Moderate.

If this setting is disabled or no value is set, Restricted Mode on YouTube is not enforced by Google Chrome. External policies such as YouTube policies might still enforce Restricted Mode, though.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the Android YouTube app. If Safety Mode on YouTube should be enforced, installation of the Android YouTube app should be disallowed.

Example value:
0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)
Back to top

FullscreenAllowed

Allow fullscreen mode
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\FullscreenAllowed`
Mac/Linux preference name:
`FullscreenAllowed`

Supported on:

- Google Chrome (Windows) since version 31
- Google Chrome (Linux) since version 31
- Google Chrome OS (Google Chrome OS) since version 31

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allow fullscreen mode.

This policy controls the availability of fullscreen mode in which all Google Chrome UI is hidden and only web content is visible.

If this policy is set to true or not not configured, the user, apps and extensions with appropriate permissions can enter fullscreen mode.

If this policy is set to false, neither the user nor any apps or extensions can enter fullscreen mode.

On all platforms except Google Chrome OS, kiosk mode is unavailable when fullscreen mode is disabled.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the Android apps. They will be able to enter fullscreen mode even if this policy is set to False.

Example value:
0x00000001 (Windows), true (Linux)
Back to top

GCFUserDataDir

Set Google Chrome Frame user data directory
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\GCFUserDataDir`
Supported on:

- Google Chrome Frame (Windows) since version 12 until version 32

Supported features:
Dynamic Policy Refresh: No
Description:

Configures the directory that Google Chrome Frame will use for storing user data.

If you set this policy, Google Chrome Frame will use the provided directory.

See https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables for a list of variables that can be used.

If this setting is left not set the default profile directory will be used.

Example value:
"${user_home}/Chrome Frame"
Back to top

HardwareAccelerationModeEnabled

Use hardware acceleration when available
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\HardwareAccelerationModeEnabled`
Mac/Linux preference name:
`HardwareAccelerationModeEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 46

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Use hardware acceleration when available.

If this policy is set to true or left unset, hardware acceleration will be enabled unless a certain GPU feature is blacklisted.

If this policy is set to false, hardware acceleration will be disabled.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

HeartbeatEnabled

Send network packets to the management server to monitor online status
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 43

Supported features:
Dynamic Policy Refresh: Yes
Description:

Send network packets to the management server to monitor online status, to allow the server to detect if the device is offline.

If this policy is set to true, monitoring network packets (so-called heartbeats) will be sent. If set to false or unset, no packets will be sent.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

HeartbeatFrequency

Frequency of monitoring network packets
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 43

Supported features:
Dynamic Policy Refresh: Yes
Description:

How frequently monitoring network packets are sent, in milliseconds.

If this policy is unset, the default frequency is 3 minutes. The minimum frequency is 30 seconds and the maximum frequency is 24 hours - values outside of this range will be clamped to this range.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

HideWebStoreIcon

Hide the web store from the New Tab Page and app launcher
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\HideWebStoreIcon`
Mac/Linux preference name:
`HideWebStoreIcon`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Hide the Chrome Web Store app and footer link from the New Tab Page and Google Chrome OS app launcher.

When this policy is set to true, the icons are hidden.

When this policy is set to false or is not configured, the icons are visible.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

HideWebStorePromo (deprecated)

Prevent app promotions from appearing on the new tab page
Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\HideWebStorePromo`

Mac/Linux preference name:

`HideWebStorePromo`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15 until version 21
- Google Chrome OS (Google Chrome OS) since version 15 until version 21

Supported features:

Dynamic Policy Refresh: No

Description:

When set to True, promotions for Chrome Web Store apps will not appear on the new tab page.

Setting this option to False or leaving it not set will make the promotions for Chrome Web Store apps appear on the new tab page

Example value:

0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

Http09OnNonDefaultPortsEnabled

Enables HTTP/0.9 support on non-default ports

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\Http09OnNonDefaultPortsEnabled`

Mac/Linux preference name:

`Http09OnNonDefaultPortsEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 54
- Google Chrome OS (Google Chrome OS) since version 54

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

This policy enables HTTP/0.9 on ports other than 80 for HTTP and 443 for HTTPS.

This policy is disabled by default, and if enabled, leaves users open to the security issue https://crbug.com/600352.

This policy is intended to give enterprises a chance to migrate exising servers off of HTTP/0.9, and will be removed in the future.

If this policy is not set, HTTP/0.9 will be disabled on non-default ports.

Example value:

0x00000000 (Windows), false (Linux), <false /> (Mac)

Back to top

ImportAutofillFormData

Import autofill form data from default browser on first run
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ImportAutofillFormData`
Mac/Linux preference name:
`ImportAutofillFormData`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 39

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy forces the autofill form data to be imported from the previous default browser if enabled. If enabled, this policy also affects the import dialog.

If disabled, the autofill form data is not imported.

If it is not set, the user may be asked whether to import, or importing may happen automatically.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ImportBookmarks

Import bookmarks from default browser on first run
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ImportBookmarks`
Mac/Linux preference name:
`ImportBookmarks`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy forces bookmarks to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog.

If disabled, no bookmarks are imported.

If it is not set, the user may be asked whether to import, or importing may happen automatically.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ImportHistory

Import browsing history from default browser on first run
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ImportHistory`
Mac/Linux preference name:
`ImportHistory`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy forces the browsing history to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog.

If disabled, no browsing history is imported.

If it is not set, the user may be asked whether to import, or importing may happen automatically.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ImportHomepage

Import of homepage from default browser on first run
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ImportHomepage`
Mac/Linux preference name:
`ImportHomepage`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy forces the home page to be imported from the current default browser if enabled.

If disabled, the home page is not imported.

If it is not set, the user may be asked whether to import, or importing may happen automatically.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ImportSavedPasswords

Import saved passwords from default browser on first run

Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ImportSavedPasswords`
Mac/Linux preference name:
`ImportSavedPasswords`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy forces the saved passwords to be imported from the previous default browser if enabled. If enabled, this policy also affects the import dialog.

If disabled, the saved passwords are not imported.

If it is not set, the user may be asked whether to import, or importing may happen automatically.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ImportSearchEngine

Import search engines from default browser on first run
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ImportSearchEngine`
Mac/Linux preference name:
`ImportSearchEngine`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy forces search engines to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog.

If disabled, the default search engine is not imported.

If it is not set, the user may be asked whether to import, or importing may happen automatically.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

IncognitoEnabled (deprecated)

Enable Incognito mode

Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\IncognitoEnabled`
Mac/Linux preference name:
`IncognitoEnabled`
Android restriction name:
`IncognitoEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy is deprecated. Please, use IncognitoModeAvailability instead. Enables Incognito mode in Google Chrome.

If this setting is enabled or not configured, users can open web pages in incognito mode.

If this setting is disabled, users cannot open web pages in incognito mode.

If this policy is left not set, this will be enabled and the user will be able to use incognito mode.

Example value:
0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)
Back to top

IncognitoModeAvailability

Incognito mode availability
Data type:
Integer [Android:choice, Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\IncognitoModeAvailability`
Mac/Linux preference name:
`IncognitoModeAvailability`
Android restriction name:
`IncognitoModeAvailability`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 14
- Google Chrome OS (Google Chrome OS) since version 14
- Google Chrome (Android) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies whether the user may open pages in Incognito mode in Google Chrome.

If 'Enabled' is selected or the policy is left unset, pages may be opened in Incognito mode.

If 'Disabled' is selected, pages may not be opened in Incognito mode.

If 'Forced' is selected, pages may be opened ONLY in Incognito mode.

- 0 = Incognito mode available
- 1 = Incognito mode disabled
- 2 = Incognito mode forced

Example value:
0x00000001 (Windows), 1 (Linux), 1 (Android), 1 (Mac)
Back to top

InstantEnabled (deprecated)

Enable Instant
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\InstantEnabled`
Mac/Linux preference name:
`InstantEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 11 until version 28
- Google Chrome OS (Google Chrome OS) since version 11 until version 28

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables Google Chrome's Instant feature and prevents users from changing this setting.

If you enable this setting, Google Chrome Instant is enabled.

If you disable this setting, Google Chrome Instant is disabled.

If you enable or disable this setting, users cannot change or override this setting.

If this setting is left not set the user can decide to use this function or not.

This setting has been removed from Google Chrome 29 and higher versions.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

JavascriptEnabled (deprecated)

Enable JavaScript
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\JavascriptEnabled`
Mac/Linux preference name:
`JavascriptEnabled`
Android restriction name:

`JavascriptEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

This policy is deprecated, please use DefaultJavaScriptSetting instead.

Can be used to disabled JavaScript in Google Chrome.

If this setting is disabled, web pages cannot use JavaScript and the user cannot change that setting.

If this setting is enabled or not set, web pages can use JavaScript but the user can change that setting.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

KeyPermissions

Key Permissions

Data type:

Dictionary

Supported on:

- Google Chrome OS (Google Chrome OS) since version 45

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Grants access to corporate keys to extensions.

Keys are designated for corporate usage if they're generated using the chrome.enterprise.platformKeys API on a managed account. Keys imported or generated in another way are not designated for corporate usage.

Access to keys designated for corporate usage is solely controlled by this policy. The user can neither grant nor withdraw access to corporate keys to or from extensions.

By default an extension cannot use a key designated for corporate usage, which is equivalent to setting allowCorporateKeyUsage to false for that extension.

Only if allowCorporateKeyUsage is set to true for an extension, it can use any platform key marked for corporate usage to sign arbitrary data. This permission should only be granted if the extension is trusted to secure access to the key against attackers.

Note for Google Chrome OS devices supporting Android apps:

Android apps cannot get access to corporate keys. This policy has no effect on them.

Back to top

LogUploadEnabled

Send system logs to the management server
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 46

Supported features:
Dynamic Policy Refresh: Yes
Description:

Send system logs to the management server, to allow admins to monitor system logs.

If this policy is set to true, system logs will be sent. If set to false or unset, then no system logs will be sent.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

LoginApps

Configure the list of installed apps on the login screen
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 54

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies a list of apps that are installed silently on the login screen, without user interaction, and which cannot be uninstalled. All permissions requested by the apps are granted implicitly, without user interaction, including any additional permissions requested by future versions of the app.

If an app that previously had been force-installed is removed from this list, it is automatically uninstalled by Google Chrome.

Each list item of the policy is a string that contains an extension ID and an "update" URL separated by a semicolon (;). The extension ID is the 32-letter string found e.g. on chrome://extensions when in developer mode. The "update" URL should point to an Update Manifest XML document as described at https://developer.chrome.com/extensions/autoupdate. Note that the "update" URL set in this policy is only used for the initial installation; subsequent updates of the extension employ the update URL indicated in the extension's manifest.

For example, gbchcmhmhahfdphkhkmpfmihenigjmpp;https://clients2.google.com/service/update2/crx installs the Chrome Remote Desktop app from the standard Chrome Web Store "update" URL. For more information about hosting extensions, see: https://developer.chrome.com/extensions/hosting.

Back to top

LoginAuthenticationBehavior

Configure the login authentication behavior
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 51

Supported features:
Dynamic Policy Refresh: Yes
Description:

When this policy is set, the login authentication flow will be in one of the following ways depending on the value of the setting:

If set to GAIA, login will be done via the normal GAIA authentication flow.

If set to SAML_INTERSTITIAL, login will show an interstitial screen offering the user to go forward with authentication via the SAML IdP of the device's enrollment domain, or go back to the normal GAIA login flow.

- 0 = Authentication via the default GAIA flow
- 1 = Redirect to SAML IdP after user confirmation

Back to top

LoginVideoCaptureAllowedUrls

URLs that will be granted access to video capture devices on SAML login pages
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 52

Supported features:
Dynamic Policy Refresh: Yes
Description:

Patterns in this list will be matched against the security origin of the requesting URL. If a match is found, access to video capture devices will be granted on SAML login pages. If no match is found, access will be automatically denied. Wildcard patterns are not allowed.

Back to top

ManagedBookmarks

Managed Bookmarks
Data type:
Dictionary [Android:string, Windows:REG_SZ] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\ManagedBookmarks`

Mac/Linux preference name:

`ManagedBookmarks`

Android restriction name:

`ManagedBookmarks`

Supported on:

- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 35 until version 47
- Google Chrome (Linux, Mac, Windows) since version 37
- Google Chrome OS (Google Chrome OS) since version 37

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Configures a list of managed bookmarks.

The policy consists of a list of bookmarks whereas each bookmark is a dictionary containing the keys "name" and "url" which hold the bookmark's name and its target. A subfolder may be configured by defining a bookmark without an "url" key but with an additional "children" key which itself contains a list of bookmarks as defined above (some of which may be folders again). Google Chrome amends incomplete URLs as if they were submitted via the Omnibox, for example "google.com" becomes "https://google.com/".

These bookmarks are placed in a "Managed bookmarks" folder that can't be modified by the user, but the user can choose to hide it from the bookmark bar. Managed bookmarks are not synced to the user account and can't be modified by extensions.

Starting with release 51, the folder name for the bookmarks is customizable by adding a {"toplevel_name": "some name"} list item.

Example value:

Windows:

```
Software\Policies\Google\Chrome\ManagedBookmarks = [{"toplevel_name":
"My managed bookmarks"}, {"url": "google.com", "name": "Google"},
{"url": "youtube.com", "name": "Youtube"}, {"name": "Chrome links",
"children": [{"url": "chromium.org", "name": "Chromium"}, {"url":
"dev.chromium.org", "name": "Chromium Developers"}]}]
```

Android/Linux:

```
ManagedBookmarks: [{"toplevel_name": "My managed bookmarks"}, {"url":
"google.com", "name": "Google"}, {"url": "youtube.com", "name":
"Youtube"}, {"name": "Chrome links", "children": [{"url":
"chromium.org", "name": "Chromium"}, {"url": "dev.chromium.org",
"name": "Chromium Developers"}]}]
```

Mac:

```
<key>ManagedBookmarks</key>
<array>
  <dict>
    <key>toplevel_name</key>
    <string>My managed bookmarks</string>
  </dict>
  <dict>
    <key>name</key>
    <string>Google</string>
    <key>url</key>
    <string>google.com</string>
  </dict>
```

```
    <dict>
      <key>name</key>
      <string>Youtube</string>
      <key>url</key>
      <string>youtube.com</string>
    </dict>
    <dict>
      <key>children</key>
      <array>
        <dict>
          <key>name</key>
          <string>Chromium</string>
          <key>url</key>
          <string>chromium.org</string>
        </dict>
        <dict>
          <key>name</key>
          <string>Chromium Developers</string>
          <key>url</key>
          <string>dev.chromium.org</string>
        </dict>
      </array>
      <key>name</key>
      <string>Chrome links</string>
    </dict>
  </array>
```

Back to top

MaxConnectionsPerProxy

Maximal number of concurrent connections to the proxy server

Data type:
Integer [Windows:REG_DWORD]

Windows registry location:
`Software\Policies\Google\Chrome\MaxConnectionsPerProxy`

Mac/Linux preference name:
`MaxConnectionsPerProxy`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 14

Supported features:
Dynamic Policy Refresh: No, Per Profile: No

Description:

Specifies the maximal number of simultaneous connections to the proxy server.

Some proxy servers can not handle high number of concurrent connections per client and this can be solved by setting this policy to a lower value.

The value of this policy should be lower than 100 and higher than 6 and the default value is 32.

Some web apps are known to consume many connections with hanging GETs, so lowering below 32 may lead to browser networking hangs if too many such web apps are open. Lower below the default at your own risk.

If this policy is left not set the default value will be used which is 32.

Example value:
0x00000020 (Windows), 32 (Linux), 32 (Mac)
Back to top

MaxInvalidationFetchDelay

Maximum fetch delay after a policy invalidation
Data type:
Integer [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\MaxInvalidationFetchDelay`
Mac/Linux preference name:
`MaxInvalidationFetchDelay`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 30
- Google Chrome OS (Google Chrome OS) since version 30

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the maximum delay in milliseconds between receiving a policy invalidation and fetching the new policy from the device management service.

Setting this policy overrides the default value of 5000 milliseconds. Valid values for this policy are in the range from 1000 (1 second) to 300000 (5 minutes). Any values not in this range will be clamped to the respective boundary.

Leaving this policy not set will make Google Chrome use the default value of 5000 milliseconds.

Example value:
0x00002710 (Windows), 10000 (Linux), 10000 (Mac)
Back to top

MediaCacheSize

Set media disk cache size in bytes
Data type:
Integer [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\MediaCacheSize`
Mac/Linux preference name:
`MediaCacheSize`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 17

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Configures the cache size that Google Chrome will use for storing cached media files on the disk.

If you set this policy, Google Chrome will use the provided cache size regardless whether the user has specified the '--media-cache-size' flag or not. The value specified in this policy is not a hard boundary

but rather a suggestion to the caching system, any value below a few megabytes is too small and will be rounded up to a sane minimum.

If the value of this policy is 0, the default cache size will be used but the user will not be able to change it.

If this policy is not set the default size will be used and the user will be able to override it with the --media-cache-size flag.

Example value:
0x06400000 (Windows), 104857600 (Linux), 104857600 (Mac)
Back to top

MetricsReportingEnabled

Enable reporting of usage and crash-related data
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\MetricsReportingEnabled`
Mac/Linux preference name:
`MetricsReportingEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: No, Per Profile: No
Description:

Enables anonymous reporting of usage and crash-related data about Google Chrome to Google and prevents users from changing this setting.

If this setting is enabled, anonymous reporting of usage and crash-related data is sent to Google. If it is disabled, this information is not sent to Google. In both cases, users cannot change or override the setting. If this policy is left not set, the setting will be what the user chose upon installation / first run.

This policy is not available on Windows instances that are not joined to an Active Directory domain. (For Chrome OS, see DeviceMetricsReportingEnabled.)

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

NTPContentSuggestionsEnabled

Show content suggestions on the New Tab page
Data type:
Boolean
Android restriction name:
`NTPContentSuggestionsEnabled`
Supported on:

- Google Chrome (Android) since version 54

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

If this is set to true or not set, the New Tab page may show content suggestions based on the user's browsing history, interests, or location.

If this is set to false, automatically-generated content suggestions are not shown on the New Tab page.

Example value:

true (Android)

Back to top

NetworkPredictionOptions

Enable network prediction

Data type:

Integer [Android:choice, Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\NetworkPredictionOptions`

Mac/Linux preference name:

`NetworkPredictionOptions`

Android restriction name:

`NetworkPredictionOptions`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 38
- Google Chrome OS (Google Chrome OS) since version 38
- Google Chrome (Android) since version 38

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables network prediction in Google Chrome and prevents users from changing this setting.

This controls DNS prefetching, TCP and SSL preconnection and prerendering of web pages.

If you set this preference to 'always', 'never', or 'WiFi only', users cannot change or override this setting in Google Chrome.

If this policy is left not set, network prediction will be enabled but the user will be able to change it.

- 0 = Predict network actions on any network connection
- 1 = Predict network actions on any network that is not cellular. (Deprecated in 50, removed in 52. After 52, if value 1 is set, it will be treated as 0 - predict network actions on any network connection.)
- 2 = Do not predict network actions on any network connection

Example value:

0x00000001 (Windows), 1 (Linux), 1 (Android), 1 (Mac)

Back to top

OpenNetworkConfiguration

User-level network configuration

Data type:

String

Supported on:

- Google Chrome OS (Google Chrome OS) since version 16

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows pushing network configuration to be applied per-user to a Google Chrome OS device. The network configuration is a JSON-formatted string as defined by the Open Network Configuration format described at https://sites.google.com/a/chromium.org/dev/chromium-os/chromiumos-design-docs/open-network-configuration

Note for Google Chrome OS devices supporting Android apps:

Android apps can use the network configurations and CA certificates set via this policy, but do not have access to some configuration options.

Back to top

PacHttpsUrlStrippingEnabled

Enable PAC URL stripping (for https://)

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\PacHttpsUrlStrippingEnabled`

Mac/Linux preference name:

`PacHttpsUrlStrippingEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 52
- Google Chrome OS (Google Chrome OS) since version 52

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

Strips privacy and security sensitive parts of https:// URLs before passing them on to PAC scripts (Proxy Auto Config) used by Google Chrome during proxy resolution.

When True, the security feature is enabled, and https:// URLs are stripped before submitting them to a PAC script. In this manner the PAC script is not able to view data that is ordinarily protected by an encrypted channel (such as the URL's path and query).

When False, the security feature is disabled, and PAC scripts are implicitly granted the ability to view all components of an https:// URL. This applies to all PAC scripts regardless of origin (including those fetched over an insecure transport, or discovered insecurely through WPAD).

This defaults to True (security feature enabled), except for Chrome OS enterprise users for which this currently defaults to False.

It is recommended that this be set to True. The only reason to set it to False is if it causes a compatibility problem with existing PAC scripts.

The desire is to remove this override in the future.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

PinnedLauncherApps

List of pinned apps to show in the launcher
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 20

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Lists the application identifiers Google Chrome OS shows as pinned apps in the launcher bar.

If this policy is configured, the set of applications is fixed and can't be changed by the user.

If this policy is left unset, the user may change the list of pinned apps in the launcher.

Back to top

PolicyRefreshRate

Refresh rate for user policy
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Specifies the period in milliseconds at which the device management service is queried for user policy information.

Setting this policy overrides the default value of 3 hours. Valid values for this policy are in the range from 1800000 (30 minutes) to 86400000 (1 day). Any values not in this range will be clamped to the respective boundary. If the platform supports policy notifications, the refresh delay will be set to 24 hours because it is expected that policy notifications will force a refresh automatically whenever policy changes.

Leaving this policy not set will make Google Chrome use the default value of 3 hours.

Note that if the platform supports policy notifications, the refresh delay will be set to 24 hours (ignoring all defaults and the value of this policy) because it is expected that policy notifications will force a refresh automatically whenever policy changes, making more frequent refreshes unnecessary.

Back to top

PrintingEnabled

Enable printing
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\PrintingEnabled`
Mac/Linux preference name:
`PrintingEnabled`
Android restriction name:
`PrintingEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 39

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables printing in Google Chrome and prevents users from changing this setting.

If this setting is enabled or not configured, users can print.

If this setting is disabled, users cannot print from Google Chrome. Printing is disabled in the wrench menu, extensions, JavaScript applications, etc. It is still possible to print from plugins that bypass Google Chrome while printing. For example, certain Flash applications have the print option in their context menu, which is not covered by this policy.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on Android apps.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

QuicAllowed

Allows QUIC protocol
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\QuicAllowed`
Mac/Linux preference name:
`QuicAllowed`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 43
- Google Chrome OS (Google Chrome OS) since version 43

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

If this policy is set to true or not set usage of QUIC protocol in Google Chrome is allowed. If this policy is set to false usage of QUIC protocol is disallowed.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

RC4Enabled

Whether RC4 cipher suites in TLS are enabled
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\RC4Enabled`
Mac/Linux preference name:
`RC4Enabled`
Android restriction name:
`RC4Enabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 48 until version 52
- Google Chrome OS (Google Chrome OS) since version 48 until version 52
- Google Chrome (Android) since version 48 until version 52
- Google Chrome (iOS) since version 48 until version 52

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Warning: RC4 will be completely removed from Google Chrome after version 52 (around September 2016) and this policy will stop working then.

If the policy is not set, or is set to false, then RC4 cipher suites in TLS will not be enabled. Otherwise it may be set to true to retain compatibility with an outdated server. This is a stopgap measure and the server should be reconfigured.

Example value:
0x00000000 (Windows), false (Linux), false (Android), <false /> (Mac)
Back to top

RebootAfterUpdate

Automatically reboot after update
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes
Description:

Schedule an automatic reboot after a Google Chrome OS update has been applied.

When this policy is set to true, an automatic reboot is scheduled when a Google Chrome OS update has been applied and a reboot is required to complete the update process. The reboot is scheduled immediately but may be delayed on the device by up to 24 hours if a user is currently using the device.

When this policy is set to false, no automatic reboot is scheduled after applying a Google Chrome OS update. The update process is completed when the user next reboots the device.

If you set this policy, users cannot change or override it.

Note: Currently, automatic reboots are only enabled while the login screen is being shown or a kiosk app session is in progress. This will change in the future and the policy will always apply, regardless of whether a session of any particular type is in progress or not.

Back to top

ReportArcStatusEnabled

Report information about status of Android
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 55

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Report information about the status of Android is send back to the server.

If the policy is set to false, the information will not be reported. If set to true or left unset, the information will be reported.

This policy only applies if Android apps are enabled.

Back to top

ReportDeviceActivityTimes

Report device activity times
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 18

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report device activity times.

If this setting is not set or set to True, enrolled devices will report time periods when a user is active on the device. If this setting is set to False, device activity times will not be recorded or reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportDeviceBootMode

Report device boot mode
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 18

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report the state of the device's dev switch at boot.

If the policy is set to false, the state of the dev switch will not be reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportDeviceHardwareStatus

Report hardware status
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report hardware statistics such as CPU/RAM usage.

If the policy is set to false, the statistics will not be reported. If set to true or left unset, statistics will be reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportDeviceNetworkInterfaces

Report device network interfaces
Data type:
Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report list of network interfaces with their types and hardware addresses to the server.

If the policy is set to false, the interface list will not be reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportDeviceSessionStatus

Report information about active kiosk sessions
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report information about the active kiosk session, such as application ID and version.

If the policy is set to false, the kiosk session information will not be reported. If set to true or left unset, kiosk session information will be reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportDeviceUsers

Report device users
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 32

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report list of device users that have recently logged in.

If the policy is set to false, the users will not be reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportDeviceVersionInfo

Report OS and firmware version
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 18

Supported features:
Dynamic Policy Refresh: Yes
Description:

Report OS and firmware version of enrolled devices.

If this setting is not set or set to True, enrolled devices will report the OS and firmware version periodically. If this setting is set to False, version info will not be reported.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

ReportUploadFrequency

Frequency of device status report uploads
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 42

Supported features:
Dynamic Policy Refresh: Yes
Description:

How frequently device status uploads are sent, in milliseconds.

If this policy is unset, the default frequency is 3 hours. The minimum allowed frequency is 60 seconds.

Note for Google Chrome OS devices supporting Android apps:

This policy has no effect on the logging done by Android.

Back to top

RequireOnlineRevocationChecksForLocalAnchors

Whether online OCSP/CRL checks are required for local trust anchors

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\RequireOnlineRevocationChecksForLocalAnchors`

Mac/Linux preference name:

`RequireOnlineRevocationChecksForLocalAnchors`

Supported on:

- Google Chrome OS (Google Chrome OS) since version 30
- Google Chrome (Linux) since version 30
- Google Chrome (Windows) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

When this setting is enabled, Google Chrome will always perform revocation checking for server certificates that successfully validate and are signed by locally-installed CA certificates.

If Google Chrome is unable to obtain revocation status information, such certificates will be treated as revoked ('hard-fail').

If this policy is not set, or it is set to false, then Google Chrome will use the existing online revocation checking settings.

Example value:

0x00000000 (Windows), false (Linux)

Back to top

RestrictSigninToPattern

Restrict which users are allowed to sign in to Google Chrome

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\RestrictSigninToPattern`

Mac/Linux preference name:

`RestrictSigninToPattern`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 21

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: No

Description:

Contains a regular expression which is used to determine which users can sign in to Google Chrome.

An appropriate error is displayed if a user tries to log in with a username that does not match this pattern.

If this policy is left not set or blank, then any user can sign in to Google Chrome.

Example value:

"*@domain.com"

Back to top

SAMLOfflineSigninTimeLimit

Limit the time for which a user authenticated via SAML can log in offline

Data type:

Integer

Supported on:

- Google Chrome OS (Google Chrome OS) since version 34

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Limit the time for which a user authenticated via SAML can log in offline.

During login, Google Chrome OS can authenticate against a server (online) or using a cached password (offline).

When this policy is set to a value of -1, the user can authenticate offline indefinitely. When this policy is set to any other value, it specifies the length of time since the last online authentication after which the user must use online authentication again.

Leaving this policy not set will make Google Chrome OS use a default time limit of 14 days after which the user must use online authentication again.

This policy affects only users who authenticated using SAML.

The policy value should be specified in seconds.

Back to top

SSLErrorOverrideAllowed

Allow proceeding from the SSL warning page

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\SSLErrorOverrideAllowed`

Mac/Linux preference name:

`SSLErrorOverrideAllowed`

Android restriction name:

`SSLErrorOverrideAllowed`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 44
- Google Chrome OS (Google Chrome OS) since version 44
- Google Chrome (Android) since version 44

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Chrome shows a warning page when users navigate to sites that have SSL errors. By default or when this policy is set to true, users are allowed to click through these warning pages. Setting this policy to false disallows users to click through any warning page.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

SSLVersionFallbackMin (deprecated)

Minimum TLS version to fallback to
Data type:
String [Android:choice, Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\SSLVersionFallbackMin`
Mac/Linux preference name:
`SSLVersionFallbackMin`
Android restriction name:
`SSLVersionFallbackMin`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 50 until version 52
- Google Chrome OS (Google Chrome OS) since version 50 until version 52
- Google Chrome (Android) since version 50 until version 52
- Google Chrome (iOS) since version 50 until version 52

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Warning: The TLS version fallback will be removed from Google Chrome after version 52 (around September 2016) and this policy will stop working then.

When a TLS handshake fails, Google Chrome would previously retry the connection with a lesser version of TLS in order to work around bugs in HTTPS servers. This setting configures the version at which this fallback process will stop. If a server performs version negotiation correctly (i.e. without breaking the connection) then this setting doesn't apply. Regardless, the resulting connection must still comply with SSLVersionMin.

If this policy is not configured or if it is set to "tls1.2" then Google Chrome no longer performs this fallback. Note this does not disable support for older TLS versions, only whether Google Chrome will work around buggy servers which cannot negotiate versions correctly.

Otherwise, if compatibility with a buggy server must be maintained, this policy may be set to "tls1.1". This is a stopgap measure and the server should be rapidly fixed.

- "tls1.1" = TLS 1.1
- "tls1.2" = TLS 1.2

Example value:
"tls1.1"
Back to top

SSLVersionMin

Minimum SSL version enabled

Data type:
String [Android:choice, Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\SSLVersionMin`
Mac/Linux preference name:
`SSLVersionMin`
Android restriction name:
`SSLVersionMin`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 39 until version 43
- Google Chrome OS (Google Chrome OS) since version 39 until version 43
- Google Chrome (Android) since version 39 until version 43
- Google Chrome (iOS) since version 39 until version 43

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Warning: SSLv3 support will be entirely removed from Google Chrome after version 43 (around July 2015) and this policy will be removed at the same time.

If this policy is not configured then Google Chrome uses a default minimum version which is SSLv3 in Google Chrome 39 and TLS 1.0 in later versions.

Otherwise it may be set to one of the following values: "sslv3", "tls1", "tls1.1" or "tls1.2". When set, Google Chrome will not use SSL/TLS versions less than the specified version. An unrecognized value will be ignored.

Note that, despite the number, "sslv3" is an earlier version than "tls1".

- "ssl3" = SSL 3.0
- "tls1" = TLS 1.0
- "tls1.1" = TLS 1.1
- "tls1.2" = TLS 1.2

Example value:
"ssl3"
Back to top

SafeBrowsingEnabled

Enable Safe Browsing
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SafeBrowsingEnabled`
Mac/Linux preference name:
`SafeBrowsingEnabled`
Android restriction name:
`SafeBrowsingEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables Google Chrome's Safe Browsing feature and prevents users from changing this setting.

If you enable this setting, Safe Browsing is always active.

If you disable this setting, Safe Browsing is never active.

If you enable or disable this setting, users cannot change or override the "Enable phishing and malware protection" setting in Google Chrome.

If this policy is left not set, this will be enabled but the user will be able to change it.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

SafeBrowsingExtendedReportingOptInAllowed

Allow users to opt in to Safe Browsing extended reporting
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SafeBrowsingExtendedReportingOptInAllowed`
Mac/Linux preference name:
`SafeBrowsingExtendedReportingOptInAllowed`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 44
- Google Chrome OS (Google Chrome OS) since version 44

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Setting this policy to false stops users from choosing to send information about security errors they encounter to Google servers. If this setting is true or not configured, then users will be allowed to send information when they encounter an SSL error or Safe Browsing warning.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

SavingBrowserHistoryDisabled

Disable saving browser history
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SavingBrowserHistoryDisabled`
Mac/Linux preference name:
`SavingBrowserHistoryDisabled`
Android restriction name:

`SavingBrowserHistoryDisabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Disables saving browser history in Google Chrome and prevents users from changing this setting.

If this setting is enabled, browsing history is not saved. This setting also disables tab syncing.

If this setting is disabled or not set, browsing history is saved.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

SearchSuggestEnabled

Enable search suggestions

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\SearchSuggestEnabled`

Mac/Linux preference name:

`SearchSuggestEnabled`

Android restriction name:

`SearchSuggestEnabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Enables search suggestions in Google Chrome's omnibox and prevents users from changing this setting.

If you enable this setting, search suggestions are used.

If you disable this setting, search suggestions are never used.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

If this policy is left not set, this will be enabled but the user will be able to change it.

Example value:

0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)

Back to top

SessionLengthLimit

Limit the session length
Data type:
Integer
Supported on:

- Google Chrome OS (Google Chrome OS) since version 25

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Limit the maximum length of a user session.

When this policy is set, it specifies the length of time after which a user is automatically logged out, terminating the session. The user is informed about the remaining time by a countdown timer shown in the system tray.

When this policy is not set, the session length is not limited.

If you set this policy, users cannot change or override it.

The policy value should be specified in milliseconds. Values are clamped to a range of 30 seconds to 24 hours.

Back to top

SessionLocales

Set the recommended locales for a public session
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 38

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Sets one or more recommended locales for a public session, allowing users to easily choose one of these locales.

The user can choose a locale and a keyboard layout before starting a public session. By default, all locales supported by Google Chrome OS are listed in alphabetic order. You can use this policy to move a set of recommended locales to the top of the list.

If this policy is not set, the current UI locale will be pre-selected.

If this policy is set, the recommended locales will be moved to the top of the list and will be visually separated from all other locales. The recommended locales will be listed in the order in which they appear in the policy. The first recommended locale will be pre-selected.

If there is more than one recommended locale, it is assumed that users will want to select among these locales. Locale and keyboard layout selection will be prominently offered when starting a public

session. Otherwise, it is assumed that most users will want to use the pre-selected locale. Locale and keyboard layout selection will be less prominently offered when starting a public session.

When this policy is set and automatic login is enabled (see the |DeviceLocalAccountAutoLoginId| and |DeviceLocalAccountAutoLoginDelay| policies), the automatically started public session will use the first recommended locale and the most popular keyboard layout matching this locale.

The pre-selected keyboard layout will always be the most popular layout matching the pre-selected locale.

This policy can only be set as recommended. You can use this policy to move a set of recommended locales to the top but users are always allowed to choose any locale supported by Google Chrome OS for their session.

Back to top

ShelfAutoHideBehavior

Control shelf auto-hiding
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 25

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Control auto-hiding of the Google Chrome OS shelf.

If this policy is set to 'AlwaysAutoHideShelf', the shelf will always auto-hide.

If this policy is set to 'NeverAutoHideShelf', the shelf never auto-hide.

If you set this policy, users cannot change or override it.

If the policy is left not set, users can choose whether the shelf should auto-hide.

- "Always" = Always auto-hide the shelf
- "Never" = Never auto-hide the shelf

Back to top

ShowAppsShortcutInBookmarkBar

Show the apps shortcut in the bookmark bar
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ShowAppsShortcutInBookmarkBar`
Mac/Linux preference name:
`ShowAppsShortcutInBookmarkBar`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 37

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables or disables the apps shortcut in the bookmark bar.

If this policy is not set then the user can choose to show or hide the apps shortcut from the bookmark bar context menu.

If this policy is configured then the user can't change it, and the apps shortcut is always shown or never shown.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

ShowHomeButton

Show Home button on toolbar
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\ShowHomeButton`
Mac/Linux preference name:
`ShowHomeButton`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Shows the Home button on Google Chrome's toolbar.

If you enable this setting, the Home button is always shown.

If you disable this setting, the Home button is never shown.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

Leaving this policy not set will allow the user to choose whether to show the home button.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

ShowLogoutButtonInTray

Add a logout button to the system tray
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 25

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Adds a logout button to the system tray.

If enabled, a big, red logout button is shown in the system tray while a session is active and the screen is not locked.

If disabled or not specified, no big, red logout button is shown in the system tray.

Back to top

SigninAllowed (deprecated)

Allows sign in to Google Chrome
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SigninAllowed`
Mac/Linux preference name:
`SigninAllowed`
Android restriction name:
`SigninAllowed`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 27
- Google Chrome (Android) since version 38

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy is deprecated, consider using SyncDisabled instead.

Allows the user to sign in to Google Chrome.

If you set this policy, you can configure whether a user is allowed to sign in to Google Chrome. Setting this policy to 'False' will prevent apps and extensions that use the chrome.identity API from functioning, so you may want to use SyncDisabled instead.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

SpellCheckServiceEnabled

Enable or disable spell checking web service
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SpellCheckServiceEnabled`
Mac/Linux preference name:
`SpellCheckServiceEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 22
- Google Chrome OS (Google Chrome OS) since version 22

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Google Chrome can use a Google web service to help resolve spelling errors. If this setting is enabled, then this service is always used. If this setting is disabled, then this service is never used.

Spell checking can still be performed using a downloaded dictionary; this policy only controls the usage of the online service.

If this setting is not configured then users can choose whether the spell checking service should be used or not.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

SuppressChromeFrameTurndownPrompt

Suppress the Google Chrome Frame turndown prompt
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SuppressChromeFrameTurndownPrompt`
Supported on:

- Google Chrome Frame (Windows) since version 29 until version 32

Supported features:
Dynamic Policy Refresh: No
Description:

Suppresses the turndown prompt that appears when a site is rendered by Google Chrome Frame.

Example value:
0x00000001 (Windows)
Back to top

SuppressUnsupportedOSWarning

Suppress the unsupported OS warning
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\SuppressUnsupportedOSWarning`
Mac/Linux preference name:
`SuppressUnsupportedOSWarning`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 49
- Google Chrome OS (Google Chrome OS) since version 49

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

Suppresses the warning that appears when Google Chrome is running on a computer or operating system that is no longer supported.

Example value:

0x00000001 (Windows), true (Linux), <true /> (Mac)

Back to top

SyncDisabled

Disable synchronization of data with Google

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\SyncDisabled`

Mac/Linux preference name:

`SyncDisabled`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 8
- Google Chrome OS (Google Chrome OS) since version 11

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Disables data synchronization in Google Chrome using Google-hosted synchronization services and prevents users from changing this setting.

If you enable this setting, users cannot change or override this setting in Google Chrome.

If this policy is left not set Google Sync will be available for the user to choose whether to use it or not.

To fully disable Google Sync, it is recommended that you disable the Google Sync service in the Google Admin console.

Note for Google Chrome OS devices supporting Android apps:

Disabling Google Sync will cause Android Backup and Restore to not function properly.

Example value:

0x00000001 (Windows), true (Linux), <true /> (Mac)

Back to top

SystemTimezone

Timezone

Data type:

String

Supported on:

- Google Chrome OS (Google Chrome OS) since version 22

Supported features:

Dynamic Policy Refresh: Yes

Description:

Specifies the timezone to be used for the device. Users can override the specified timezone for the current session. However, on logout it is set back to the specified timezone. If an invalid value is provided, the policy is still activated using "GMT" instead. If an empty string is provided, the policy is ignored.

If this policy is not used, the currently active timezone will remain in use however users can change the timezone and the change is persistent. Thus a change by one user affects the login-screen and all other users.

New devices start out with the timezone set to "US/Pacific".

The format of the value follows the names of timezones in the "IANA Time Zone Database" (see "https://en.wikipedia.org/wiki/Tz_database"). In particular, most timezones can be referred to by "continent/large_city" or "ocean/large_city".

Setting this policy completely disables automatic timezone resolve by device location. It also overrides SystemTimezoneAutomaticDetection policy.

Back to top

SystemTimezoneAutomaticDetection

Configure the automatic timezone detection method

Data type:

Integer

Supported on:

- Google Chrome OS (Google Chrome OS) since version 53

Supported features:

Dynamic Policy Refresh: Yes

Description:

When this policy is set, automatic timezone detection flow will be in one of the following ways depending on the value of the setting:

If set to TimezoneAutomaticDetectionUsersDecide, users would be able to control automatic timezone detection using normal controls in chrome://settings.

If set to TimezoneAutomaticDetectionDisabled, automatic timezone controls in chrome://settings will be disabled. Automatic timezone detection will be always off.

If set to TimezoneAutomaticDetectionIPOnly, timezone controls in chrome://settings will be disabled. Automatic timezone detection will be always on. Timezone detection will use IP-only method to resolve location.

If set to TimezoneAutomaticDetectionSendWiFiAccessPoints, timezone controls in chrome://settings will be disabled. Automatic timezone detection will be always on. The list of visible WiFi access-points will be always sent to Geolocation API server for fine-grained timezone detection.

If this policy is not set, it will behave as if TimezoneAutomaticDetectionUsersDecide is set.

If SystemTimezone policy is set, it overrides this policy. In this case automatic timezone detection is completely disabled.

- 0 = Let users decide.
- 1 = Never auto-detect timezone.
- 2 = Always use coarse timezone detection.
- 3 = Always send WiFi acess-points to server while resolving timezone.

Back to top

SystemUse24HourClock

Use 24 hour clock by default
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 30

Supported features:
Dynamic Policy Refresh: Yes
Description:

Specifies the clock format be used for the device.

This policy configures the clock format to use on the login screen and as a default for user sessions. Users can still override the clock format for their account.

If the policy is set to true, the device will use a 24 hour clock format. If the policy is set to false, the device will use 12 hour clock format.

If this policy is not set, the device will default to a 24 hour clock format.

Back to top

TaskManagerEndProcessEnabled

Enables ending processes in Task Manager
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\TaskManagerEndProcessEnabled`
Mac/Linux preference name:
`TaskManagerEndProcessEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 52
- Google Chrome OS (Google Chrome OS) since version 52

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Enables ending processes in Google Chrome's Task Manager.

If set to false, the 'End process' button is disabled in the Task Manager.

If set to true or not configured, the user can end processes in the Task Manager.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

TermsOfServiceURL

Set the Terms of Service for a device-local account
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 26

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Sets the Terms of Service that the user must accept before starting a device-local account session.

If this policy is set, Google Chrome OS will download the Terms of Service and present them to the user whenever a device-local account session is starting. The user will only be allowed into the session after accepting the Terms of Service.

If this policy is not set, no Terms of Service are shown.

The policy should be set to a URL from which Google Chrome OS can download the Terms of Service. The Terms of Service must be plain text, served as MIME type text/plain. No markup is allowed.

Back to top

TouchVirtualKeyboardEnabled

Enable virtual keyboard
Data type:
Boolean
Supported on:

- Google Chrome OS (Google Chrome OS) since version 37

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

This policy configures enabling the virtual keyboard as an input device on ChromeOS. Users cannot override this policy.

If the policy is set to true, the on-screen virtual keyboard will always be enabled.

If set to false, the on-screen virtual keyboard will always be disabled.

If you set this policy, users cannot change or override it. However, users will still be able to enable/disable an accessibility on-screen keyboard which takes precedence over the virtual keyboard controlled by this policy. See the |VirtualKeyboardEnabled| policy for controlling the accessibility on-screen keyboard.

If this policy is left unset, the on-screen keyboard is disabled initially but can be enabled by the user anytime. Heuristic rules may also be used to decide when to display the keyboard.

Back to top

TranslateEnabled

Enable Translate
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\TranslateEnabled`
Mac/Linux preference name:
`TranslateEnabled`
Android restriction name:
`TranslateEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 12
- Google Chrome OS (Google Chrome OS) since version 12
- Google Chrome (Android) since version 30
- Google Chrome (iOS) since version 34 until version 47

Supported features:
Can Be Recommended: Yes, Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Enables the integrated Google Translate service on Google Chrome.

If you enable this setting, Google Chrome will show an integrated toolbar offering to translate the page for the user, when appropriate.

If you disable this setting, users will never see the translation bar.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

If this setting is left not set the user can decide to use this function or not.

Example value:
0x00000001 (Windows), true (Linux), true (Android), <true /> (Mac)
Back to top

URLBlacklist

Block access to a list of URLs
Data type:
List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)
Windows registry location:
`Software\Policies\Google\Chrome\URLBlacklist`
Mac/Linux preference name:
`URLBlacklist`
Android restriction name:
`URLBlacklist`
Android WebView restriction name:
`com.android.browser:URLBlacklist`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15
- Google Chrome OS (Google Chrome OS) since version 15
- Google Chrome (Android) since version 30
- Android System WebView (Android) since version 47
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Blocks access to the listed URLs.

This policy prevents the user from loading web pages from blacklisted URLs. The blacklist provides a list of URL patterns that specify which URLs will be blacklisted.

A URL pattern has to be formatted according to https://www.chromium.org/administrators/url-blacklist-filter-format.

Exceptions can be defined in the URL whitelist policy. These policies are limited to 1000 entries; subsequent entries will be ignored.

Note that it is not recommended to block internal 'chrome://*' URLs since this may lead to unexpected errors.

If this policy is not set no URL will be blacklisted in the browser.

Note for Google Chrome OS devices supporting Android apps:

Android apps may voluntarily choose to honor this list. You cannot force them to honor it.

Example value:

Windows:

```
Software\Policies\Google\Chrome\URLBlacklist\1 = "example.com"
Software\Policies\Google\Chrome\URLBlacklist\2 =
"https://ssl.server.com"
Software\Policies\Google\Chrome\URLBlacklist\3 =
"hosting.com/bad_path"
Software\Policies\Google\Chrome\URLBlacklist\4 =
"https://server:8080/path"
Software\Policies\Google\Chrome\URLBlacklist\5 =
".exact.hostname.com"
Software\Policies\Google\Chrome\URLBlacklist\6 = "file://*"
Software\Policies\Google\Chrome\URLBlacklist\7 = "custom_scheme:*"
Software\Policies\Google\Chrome\URLBlacklist\8 = "*"
```

Android/Linux:

```
["example.com", "https://ssl.server.com", "hosting.com/bad_path",
"https://server:8080/path", ".exact.hostname.com", "file://*",
"custom_scheme:*", "*"]
```

Mac:

```
<array>
  <string>example.com</string>
  <string>https://ssl.server.com</string>
  <string>hosting.com/bad_path</string>
  <string>https://server:8080/path</string>
  <string>.exact.hostname.com</string>
```

```
    <string>file://*</string>
    <string>custom_scheme:*</string>
    <string>*</string>
  </array>
```

Back to top

URLWhitelist

Allows access to a list of URLs

Data type:

List of strings [Android:string] (encoded as a JSON string, for details see https://www.chromium.org/administrators/complex-policies-on-windows)

Windows registry location:

`Software\Policies\Google\Chrome\URLWhitelist`

Mac/Linux preference name:

`URLWhitelist`

Android restriction name:

`URLWhitelist`

Android WebView restriction name:

`com.android.browser:URLWhitelist`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 15
- Google Chrome OS (Google Chrome OS) since version 15
- Google Chrome (Android) since version 30
- Android System WebView (Android) since version 47
- Google Chrome (iOS) since version 34 until version 47

Supported features:

Dynamic Policy Refresh: Yes, Per Profile: Yes

Description:

Allows access to the listed URLs, as exceptions to the URL blacklist.

See the description of the URL blacklist policy for the format of entries of this list.

This policy can be used to open exceptions to restrictive blacklists. For example, '*' can be blacklisted to block all requests, and this policy can be used to allow access to a limited list of URLs. It can be used to open exceptions to certain schemes, subdomains of other domains, ports, or specific paths.

The most specific filter will determine if a URL is blocked or allowed. The whitelist takes precedence over the blacklist.

This policy is limited to 1000 entries; subsequent entries will be ignored.

If this policy is not set there will be no exceptions to the blacklist from the 'URLBlacklist' policy.

Note for Google Chrome OS devices supporting Android apps:

Android apps may voluntarily choose to honor this list. You cannot force them to honor it.

Example value:

Windows:

```
Software\Policies\Google\Chrome\URLWhitelist\1 = "example.com"
Software\Policies\Google\Chrome\URLWhitelist\2 =
"https://ssl.server.com"
```

```
Software\Policies\Google\Chrome\URLWhitelist\3 =
"hosting.com/good_path"
Software\Policies\Google\Chrome\URLWhitelist\4 =
"https://server:8080/path"
Software\Policies\Google\Chrome\URLWhitelist\5 =
".exact.hostname.com"
```

Android/Linux:

```
["example.com", "https://ssl.server.com", "hosting.com/good_path",
"https://server:8080/path", ".exact.hostname.com"]
```

Mac:

```
<array>
  <string>example.com</string>
  <string>https://ssl.server.com</string>
  <string>hosting.com/good_path</string>
  <string>https://server:8080/path</string>
  <string>.exact.hostname.com</string>
</array>
```

Back to top

UnifiedDesktopEnabledByDefault

Make Unified Desktop available and turn on by default.

Data type:

Boolean

Supported on:

- Google Chrome OS (Google Chrome OS) since version 47

Supported features:

Can Be Recommended: No, Dynamic Policy Refresh: Yes, Per Profile: No

Description:

If this policy is set to true, Unified Desktop is allowed and enabled by default, which allows applications to span multiple displays. The user may disable Unified Desktop for individual displays by unchecking it in the display settings.

If this policy is set to false or unset, Unified Desktop will be disabled. In this case, the user cannot enable the feature.

Back to top

UptimeLimit

Limit device uptime by automatically rebooting

Data type:

Integer

Supported on:

- Google Chrome OS (Google Chrome OS) since version 29

Supported features:

Dynamic Policy Refresh: Yes

Description:

Limit the device uptime by scheduling automatic reboots.

When this policy is set, it specifies the length of device uptime after which an automatic reboot is scheduled.

When this policy is not set, the device uptime is not limited.

If you set this policy, users cannot change or override it.

An automatic reboot is scheduled at the selected time but may be delayed on the device by up to 24 hours if a user is currently using the device.

Note: Currently, automatic reboots are only enabled while the login screen is being shown or a kiosk app session is in progress. This will change in the future and the policy will always apply, regardless of whether a session of any particular type is in progress or not.

The policy value should be specified in seconds. Values are clamped to be at least 3600 (one hour).

Back to top

UsbDetachableWhitelist

Whitelist of USB detachable devices
Data type:
List of strings
Supported on:

- Google Chrome OS (Google Chrome OS) since version 51

Supported features:
Dynamic Policy Refresh: No
Description:

Defines the list of USB devices that are allowed to be detached from their kernel driver in order to be used through the chrome.usb API directly inside a web application. Entries are pairs of USB Vendor Identifier and Product Identifier to identify a specific hardware.

If this policy is not configured, the list of a detachable USB devices is empty.

Back to top

UserAvatarImage

User avatar image
Data type:
External data reference
Supported on:

- Google Chrome OS (Google Chrome OS) since version 34

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Configure user avatar image.

This policy allows you to configure the avatar image representing the user on the login screen. The policy is set by specifying the URL from which Google Chrome OS can download the avatar image and

a cryptographic hash used to verify the integrity of the download. The image must be in JPEG format, its size must not exceed 512kB. The URL must be accessible without any authentication.

The avatar image is downloaded and cached. It will be re-downloaded whenever the URL or the hash changes.

The policy should be specified as a string that expresses the URL and hash in JSON format, conforming to the following schema: { "type": "object", "properties": { "url": { "description": "The URL from which the avatar image can be downloaded.", "type": "string" }, "hash": { "description": "The SHA-256 hash of the avatar image.", "type": "string" } } }

If this policy is set, Google Chrome OS will download and use the avatar image.

If you set this policy, users cannot change or override it.

If the policy is left not set, the user can choose the avatar image representing them on the login screen.

Back to top

UserDataDir

Set user data directory
Data type:
String [Windows:REG_SZ]
Windows registry location:
`Software\Policies\Google\Chrome\UserDataDir`
Mac/Linux preference name:
`UserDataDir`
Supported on:

- Google Chrome (Windows) since version 11
- Google Chrome (Mac) since version 11

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Configures the directory that Google Chrome will use for storing user data.

If you set this policy, Google Chrome will use the provided directory regardless whether the user has specified the '--user-data-dir' flag or not. To avoid data loss or other unexpected errors this policy should not be set to a volume's root directory or to a directory used for other purposes, because Google Chrome manages its contents.

See https://www.chromium.org/administrators/policy-list-3/user-data-directory-variables for a list of variables that can be used.

If this policy is left not set the default profile path will be used and the user will be able to override it with the '--user-data-dir' command line flag.

Example value:
"${users}/${user_name}/Chrome"
Back to top

UserDisplayName

Set the display name for device-local accounts
Data type:
String
Supported on:

- Google Chrome OS (Google Chrome OS) since version 25

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: No
Description:

Controls the account name Google Chrome OS shows on the login screen for the corresponding device-local account.

If this policy is set, the login screen will use the specified string in the picture-based login chooser for the corresponding device-local account.

If the policy is left not set, Google Chrome OS will use the device-local account's email account ID as the display name on the login screen.

This policy is ignored for regular user accounts.

Back to top

VideoCaptureAllowed

Allow or deny video capture
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\VideoCaptureAllowed`
Mac/Linux preference name:
`VideoCaptureAllowed`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 25
- Google Chrome OS (Google Chrome OS) since version 25

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Allow or deny video capture.

If enabled or not configured (default), the user will be prompted for video capture access except for URLs configured in the VideoCaptureAllowedUrls list which will be granted access without prompting.

When this policy is disabled, the user will never be prompted and video capture only be available to URLs configured in VideoCaptureAllowedUrls.

This policy affects all types of video inputs and not only the built-in camera.

Note for Google Chrome OS devices supporting Android apps:

For Android apps, this policy affects the built-in camera only. When this policy is set to true, the camera is disabled for all Android apps, with no exceptions.

Example value:
0x00000000 (Windows), false (Linux), <false /> (Mac)
Back to top

VideoCaptureAllowedUrls

URLs that will be granted access to video capture devices without prompt
Data type:
List of strings
Windows registry location:
`Software\Policies\Google\Chrome\VideoCaptureAllowedUrls`
Mac/Linux preference name:
`VideoCaptureAllowedUrls`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 29
- Google Chrome OS (Google Chrome OS) since version 29

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Patterns in this list will be matched against the security origin of the requesting URL. If a match is found, access to audio capture devices will be granted without prompt.

NOTE: Until version 45, this policy was only supported in Kiosk mode.

Example value:
Windows:
```
Software\Policies\Google\Chrome\VideoCaptureAllowedUrls\1 =
"https://www.example.com/"
Software\Policies\Google\Chrome\VideoCaptureAllowedUrls\2 =
"https://[*.]example.edu/"
```
Android/Linux:
```
["https://www.example.com/", "https://[*.]example.edu/"]
```
Mac:
```
<array>
  <string>https://www.example.com/</string>
  <string>https://[*.]example.edu/</string>
</array>
```
Back to top

WPADQuickCheckEnabled

Enable WPAD optimization
Data type:
Boolean [Windows:REG_DWORD]
Windows registry location:
`Software\Policies\Google\Chrome\WPADQuickCheckEnabled`
Mac/Linux preference name:
`WPADQuickCheckEnabled`
Supported on:

- Google Chrome (Linux, Mac, Windows) since version 35
- Google Chrome OS (Google Chrome OS) since version 35

Supported features:
Dynamic Policy Refresh: No, Per Profile: No
Description:

Allows to turn off WPAD (Web Proxy Auto-Discovery) optimization in Google Chrome.

If this policy is set to false, WPAD optimization is disabled causing Google Chrome to wait longer for DNS-based WPAD servers. If the policy is not set or is enabled, WPAD optimization is enabled.

Independent of whether or how this policy is set, the WPAD optimization setting cannot be changed by users.

Example value:
0x00000001 (Windows), true (Linux), <true /> (Mac)
Back to top

WallpaperImage

Wallpaper image
Data type:
External data reference
Supported on:

- Google Chrome OS (Google Chrome OS) since version 35

Supported features:
Dynamic Policy Refresh: Yes, Per Profile: Yes
Description:

Configure wallpaper image.

This policy allows you to configure the wallpaper image that is shown on the desktop and on the login screen background for the user. The policy is set by specifying the URL from which Google Chrome OS can download the wallpaper image and a cryptographic hash used to verify the integrity of the download. The image must be in JPEG format, its file size must not exceed 16MB. The URL must be accessible without any authentication.

The wallpaper image is downloaded and cached. It will be re-downloaded whenever the URL or the hash changes.

The policy should be specified as a string that expresses the URL and hash in JSON format, conforming to the following schema: { "type": "object", "properties": { "url": { "description": "The URL from which the wallpaper image can be downloaded.", "type": "string" }, "hash": { "description": "The SHA-256 hash of the wallpaper image.", "type": "string" } } }

If this policy is set, Google Chrome OS will download and use the wallpaper image.

If you set this policy, users cannot change or override it.

If the policy is left not set, the user can choose an image to be shown on the desktop and on the login screen background.

Back to top

WebRtcUdpPortRange

Restrict the range of local UDP ports used by WebRTC

Data type:

String [Windows:REG_SZ]

Windows registry location:

`Software\Policies\Google\Chrome\WebRtcUdpPortRange`

Mac/Linux preference name:

`WebRtcUdpPortRange`

Android restriction name:

`WebRtcUdpPortRange`

Supported on:

- Google Chrome (Linux, Mac, Windows) since version 54
- Google Chrome OS (Google Chrome OS) since version 54
- Google Chrome (Android) since version 54

Supported features:

Dynamic Policy Refresh: No, Per Profile: Yes

Description:

If the policy is set, the UDP port range used by WebRTC is restricted to the specified port interval (endpoints included).

If the policy is not set, or if it is set to the empty string or an invalid port range, WebRTC is allowed to use any available local UDP port.

Example value:

"10000-11999"

Back to top

WelcomePageOnOSUpgradeEnabled

Enable showing the welcome page on the first browser launch following OS upgrade.

Data type:

Boolean [Windows:REG_DWORD]

Windows registry location:

`Software\Policies\Google\Chrome\WelcomePageOnOSUpgradeEnabled`

Supported on:

- Google Chrome (Windows) since version 45

Supported features:

Dynamic Policy Refresh: No, Per Profile: No

Description:

Enable showing the welcome page on the first browser launch following OS upgrade.

If this policy is set to true or not configured, the browser will re-show the welcome page on the first launch following an OS upgrade.

If this policy is set to false, the browser will not re-show the welcome page on the first launch following an OS upgrade.

Example value:

0x00000000 (Windows)

Back to top