chrome enterprise

Privacygids voor de Chrome-browser voor bedrijven: meer informatie over je privacyopties

Inleiding

Je hebt via de browser overal toegang tot belangrijke apps en gegevens. Daarom besteden de zakelijke gebruikers die het internet het meest gebruiken meer dan de helft van hun werkdag in de browser. Maar organisaties krijgen ook te maken met steeds grotere vereisten voor beveiliging, privacy en naleving, terwijl gebruikers 24 uur per dag snelle, betrouwbare en beveiligde toegang moeten hebben tot hun web-apps.

Je mag verwachten dat de browser die je organisatie gebruikt betrouwbaar en beveiligd is en dat deze opties bevat om de gegevens van je organisatie en je werknemers efficiënt te beschermen. Als je organisatie meer privacy- en nalevingsvereisten heeft, kun je de verschillende beleidsregels in de Chrome-browser gebruiken om te voldoen aan deze vereisten. We laten je manieren zien waarop je beheerders privacymodi kunnen instellen, beleidsregels kunnen maken waardoor de werk- en gebruikersprofielen van je werknemers worden gescheiden en tools kunnen gebruiken waardoor werknemers beter begrijpen hoe de browser wordt beheerd.

chrome enterprise

Privacymodi in de Chrome-browser

Als IT-beheerder kun je beleidsregels toepassen op de browser die je beheert. Chrome controleert regelmatig of er updates zijn voor de beleidsregels in je omgeving. Als je privé browsen wilt implementeren in je bedrijf, kun je de volgende privacymodi in de Chrome-browser gebruiken. We raden deze aan voor gedeelde of openbare terminals die door meerdere werknemers worden gebruikt.

Gastmodus: In de gastmodus kun je geen Chrome-profielgegevens van andere gebruikers bekijken of aanpassen. Als je de gastmodus afsluit, wordt je browse-activiteit verwijderd van de computer. De gastmodus is ideaal als anderen jouw apparaat lenen, als jij het apparaat van iemand anders leent of als je een openbaar apparaat gebruikt.

Als je het beleid BrowserGuestModeEnabled instelt op 'waar' of het niet instelt, staan gastsessies aan voor Google Chrome. Gastsessies zijn kortstondige sessies die beginnen met de standaardinstellingen en waaruit alles wordt gewist als de sessie voorbij is. Als je dit beleid instelt op onwaar, staat Google Chrome niet toe dat er een gastprofiel wordt gestart.

Je kunt ook het beleid BrowerGuestModeEnforced gebruiken, waarmee de Chrome-browser afgedwongen altijd wordt gestart in de gastmodus. Als je dit beleid aanzet, dwingt Google Chrome het gebruik van gastsessies af en kan de Chrome-browser niet worden geopend met een bestaand profiel. Gastsessies zijn Google Chrome-profielen waarbij alle vensters in de incognitomodus worden uitgevoerd. Als je dit beleid uitzet of niet instelt, of als je gebruik van de gastmodus voor de browser uitzet met het beleid BrowserGuestModeEnabled, staat Google Chrome toe dat er nieuwe en bestaande profielen worden gebruikt.

Kortstondige modus: Als je wilt dat je werknemers kunnen werken op hun persoonlijke laptop of een gedeeld apparaat dat ze vertrouwen, kun je met een beleidsregel afdwingen dat het Chrome-profiel kortstondig is. Door de kortstondige modus af te dwingen, verklein je de kans dat eventuele browsegegevens op het apparaat achterblijven. Tijdens een kortstondige sessie hebben gebruikers toegang tot alle functies van een browsersessie. Zo kunnen ze inloggen om Chrome-synchronisatie, cloudprinter, cloudbeleid, wachtwoordopslag, bookmarks, automatisch invullen en andere gegevens te kunnen gebruiken die normaal gesproken aanwezig zijn in een gebruikersprofiel. Ze hebben ook toegang tot bedrijfsitems die beschikbaar zijn in de kortstondige modus, zoals bedrijfswebmail, documenten en intranetpagina's. Als je de kortstondige modus gebruikt, raden we je sterk aan ook Chrome-synchronisatie te gebruiken. Als Chrome-synchronisatie aanstaat, worden alle wijzigingen die gebruikers tijdens een kortstondige sessie aanbrengen in de instellingen van de browser of in hun Chrome-gegevens (zoals bookmarks, geschiedenis en apps) bewaard voor toekomstige sessies. De instellingen worden opgeslagen in het Google-account van de gebruiker in de cloud. Als Chrome-synchronisatie uitstaat, gaan eventuele wijzigingen verloren wanneer gebruikers de browser afsluiten.

Als je het beleid ForceEphemeralProfiles aanzet, wordt het profiel afgedwongen overgezet naar de kortstondige modus. Als je dit beleid opgeeft als OS-beleid (bijvoorbeeld via GPO in Windows), geldt het voor elk profiel in het systeem. Als je dit beleid instelt als cloudbeleid, geldt het alleen voor profielen waarop is ingelogd met een beheerd account.

chrome enterprise

Incognitomodus: Als je niet wilt dat Google Chrome de activiteiten van gebruikers onthoudt, kun je de incognitomodus aanzetten. Zo kunnen gebruikers privé browsen op het web op hun eigen apparaat. Ze zien hun gegevens en instellingen zonder dat de browsegeschiedenis wordt opgeslagen. Bij de incognitomodus kiezen de gebruikers van een organisatie er zelf voor of ze willen browsen in de incognitomodus. De kortstondige modus is een beleidsregel die wordt afgedwongen door de beheerder van de organisatie. Met het beleid hieronder kunnen beheerders bepalen of gebruikers mogen browsen in de incognitomodus. In de incognitomodus kunnen gebruikers niet inloggen en krijgen ze dus niet de voordelen van Chrome-synchronisatie, zoals zakelijke bookmarks.

Apps en extensies staan standaard uit in de incognitomodus, maar de gebruiker kan ze aanzetten. In de kortstondige modus staan apps en extensies standaard aan. De kortstondige modus biedt productiviteitsvoordelen voor de werknemer en vermindert het risico dat gegevens worden achtergelaten. Als je de kortstondige modus instelt op gebruikersniveau in de Beheerdersconsole, moeten gebruikers inloggen bij Chrome, anders krijgen ze geen synchronisatievoordelen en wordt het beleid niet doorgevoerd. Dit beleid mag alleen worden gebruikt op apparaten die gebruikers vertrouwen en die voldoen aan ander beleid van het bedrijf. Het profiel wordt pas gemarkeerd voor verwijdering nadat de gebruiker is uitgelogd of als elk venster dat bij het profiel hoort, handmatig is afgesloten. Het profiel wordt verwijderd als Chrome opnieuw wordt gestart. Gebruik de kortstondige modus niet als je de Windows-functie Chrome Roaming Profile Support gebruikt. Er is ook gedetailleerder beleid dat bepaalt of en hoe Chrome bepaalde soorten gegevens opslaat.

Met het beleid IncognitoModeAvailability bepaal je of gebruikers pagina's mogen openen in de incognitomodus. Als je dit beleid aanzet of niet instelt, mogen gebruikers pagina's openen in de incognitomodus. Als je dit beleid uitzet, kunnen ze geen pagina's openen in de incognitomodus. Als je dit beleid afdwingt, kunnen ze pagina's ALLEEN openen in de incognitomodus.

Je kunt deze modi aanzetten met beleid voor beheerde browsers via de Google Beheerdersconsole, groepsbeleid, een json-bestandseditor of je Chrome-configuratieprofiel, afhankelijk van welk besturingssysteem je instelt. Nadat je Chrome-beleid hebt toegepast, moeten gebruikers de Chrome-browser opnieuw starten voordat de instellingen van kracht worden. Check op de apparaten van gebruikers of het beleid correct is toegepast.

Door de incognito- of gastmodus te gebruiken, beperk je de hoeveelheid gegevens die Chrome opslaat in je systeem. Chrome slaat bepaalde gegevens niet op, zoals:

- Basisgegevens over de browsegeschiedenis, zoals URL's, paginatekst in het cachegeheugen of IP-adressen van pagina's waarnaar wordt gelinkt op de websites die je bezoekt.
- Momentopnamen van pagina's die je bezoekt.
- Gegevens met betrekking tot je downloads. De bestanden die je downloadt, blijven lokaal opgeslagen op een andere locatie op je computer of apparaat.

chrome enterprise

Wat Chrome doet met gegevens in de incognito- of gastmodus

Chrome deelt geen bestaande cookies met sites die je bezoekt in de incognito- of gastmodus. Als je de incognito- of gastmodus gebruikt, zijn er geen bestaande cookies, omdat je begint met de standaardinstellingen. Tijdens een kortdurende sessie kunnen sites cookies lezen en schrijven. De sessie wordt beëindigd als het laatste tabblad of venster wordt gesloten. Alle cookies worden dan definitief verwijderd. Als je in de incognitomodus wijzigingen aanbrengt in de browserconfiguratie, bijvoorbeeld als je een bookmark maakt voor een webpagina of toegankelijkheidsinstellingen wijzigt, worden deze gegevens opgeslagen. Dit gebeurt alleen in de incognitomodus, niet in de gastmodus. Als je rechten toewijst in de incognitomodus, worden deze niet opgeslagen in je bestaande profiel. In de incognitomodus heb je tijdens het browsen nog steeds toegang tot gegevens uit je bestaande profiel, zoals suggesties gebaseerd op je browsegeschiedenis en opgeslagen wachtwoorden. In de gastmodus kun je browsen zonder gegevens uit je bestaande profielen te zien. De gastmodus is altijd een hele nieuwe sessie en bevat geen bestaande gebruikersgegevens.

Met profielen kun je werk- en persoonlijke gegevens van werknemers gescheiden houden

Je kunt beleid instellen waardoor gebruikers op zakelijke Windows-, Mac- of Linux-computers moeten inloggen op een beheerd account om de Chrome-browser te kunnen gebruiken. Als er een conflict is tussen gebruikersbeleid dat is ingesteld in de Beheerdersconsole en apparaatbeleid dat bijvoorbeeld met Cloudbeheer voor de Chrome-browser of Windows-groepsbeleid is ingesteld, krijgt het apparaatbeleid voorrang.

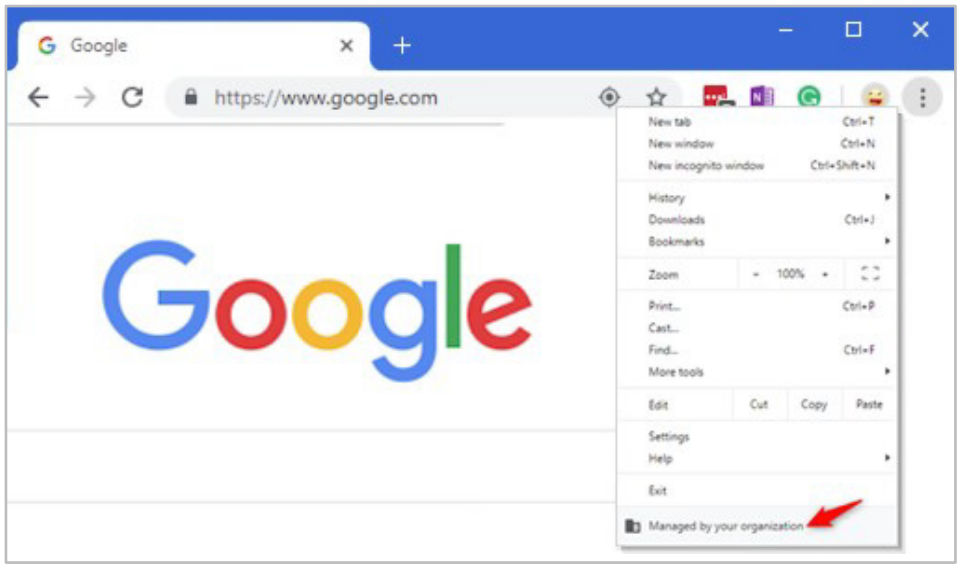
BrowserSignin
Hiermee bepaal je of gebruikers kunnen inloggen bij de Chrome-browser en browsergegevens kunnen synchroniseren met hun Google-account. Kies een van deze opties:
0: Inloggen bij browser uitzetten. Gebruikers kunnen niet inloggen bij de Chrome-browser en geen browsergegevens synchroniseren met hun Google-account.
1: Inloggen bij browser aanzetten. Gebruikers kunnen inloggen bij de Chrome-browser en browsergegevens synchroniseren met hun Google-account. Gebruikers worden automatisch ingelogd bij de Chrome-browser als ze inloggen bij een Google-service, zoals Gmail.
2: Inloggen bij browser afdwingen. Gebruikers moeten inloggen bij de Chrome-browser voordat ze deze kunnen gebruiken. Secundaire gebruikers kunnen niet inloggen bij de Chrome-browser. Synchronisatie staat standaard aan en gebruikers kunnen dit niet wijzigen. Gebruik het beleid SyncDisabled om synchronisatie uit te zetten.
Niet ingesteld: Gebruikers kunnen inloggen bij de Chrome-browser. Als gebruikers inloggen bij een Google-service, zoals Gmail, worden ze automatisch ingelogd bij de Chrome-browser. Gebruikers kunnen dit aanpassen.
RestrictSigninToPattern
Hiermee kun je instellen welke Google-accounts worden gebruikt als primaire gebruiker in de Chrome-browser.
Gebruik dit beleid met BrowserSignin om in te stellen dat gebruikers met meerdere Chrome-profielen moeten inloggen bij een bepaald profiel voordat ze Chrome kunnen gebruiken. Gebruikers kunnen alleen inloggen bij profielen die overeenkomen met de patronen die je opgeeft.
Niet ingesteld: Gebruikers kunnen met elk Google-account inloggen als primaire gebruiker in de Chrome-browser.

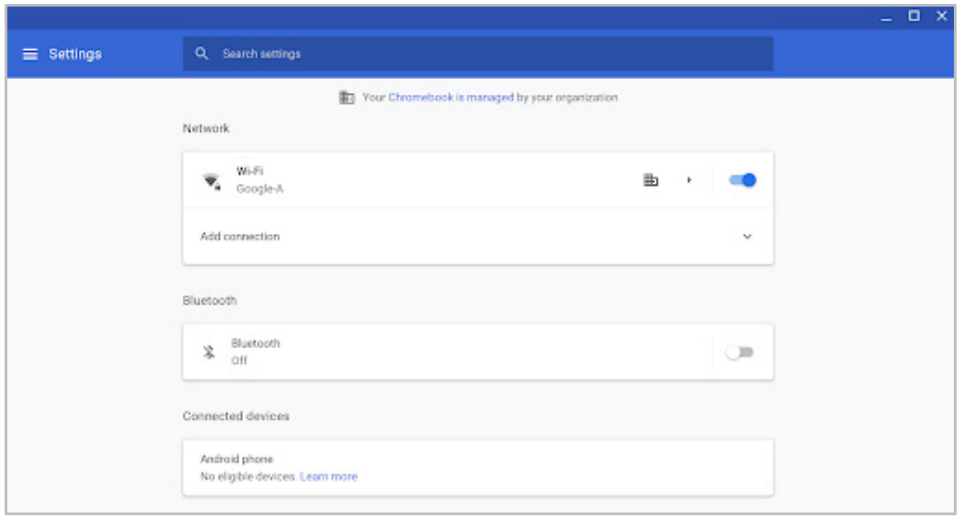
chrome enterprise

De gebruikers in je organisatie laten weten hoe de browser wordt beheerd

Privacy en transparantie gaan hand in hand. Chrome is gemaakt om gebruikers zichtbaarheid te geven in instellingen en configuraties, zelfs op bedrijfsniveau. Google biedt gebruikers 2 manieren om informatie te vinden over wat er wordt beheerd in de browser.

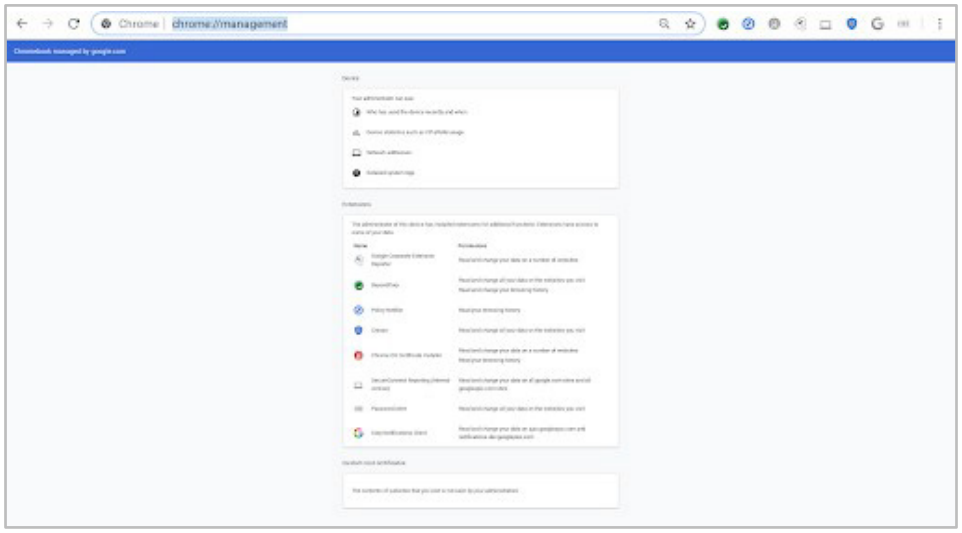
1. Beheerd door: Je gebruikers zien dat IT hun apparaat beheert vanuit hun organisatie en dat ze contact met je kunnen opnemen als ze vragen hebben. Ze zien het bericht '(Chrome wordt) beheerd door je organisatie' onderin het menu, onder de optie Afsluiten, of als ze op Instellingen klikken.





chrome enterprise

2. Als gebruikers naar chrome://management gaan, zien ze welke extensies jij als beheerder hebt geïmplementeerd en welke informatie je kunt zien als beheerder. En als ze naar chrome://policy gaan, zien ze welk beleid jij als beheerder hebt aangezet voor hun apparaat.



chrome enterprise

Conclusie

We raden je aan deze beheeropties te gebruiken om te zorgen dat je organisatie beter voldoet aan privacy- en nalevingsstandaarden of om te zorgen dat je gebruikers beter begrijpen hoe de browser wordt beheerd. Deze handleiding is bedoeld om beheerders die de Chrome-browser beheren voor een bedrijf of school te laten zien hoe ze beleid en instellingen voor de Chrome-browser kunnen aanpassen om te voldoen aan de behoeften voor privacy, gegevensbescherming of naleving van hun organisatie. We raden je aan te overleggen met een juridisch expert om in kaart te brengen welke vereisten van toepassing zijn voor je organisatie, omdat deze handleiding geen juridisch advies bevat.

Bekijk de volgende bronnen voor nog meer informatie over de modi voor privé browsen van de Chrome-browser:

Meer informatie over de kortstondige modus

Meer informatie over privé browsen

Bekijk hoe je in Chrome kunt browsen als gast

Lees hoe je privé browsen kunt toestaan

Bekijk de opties van Cloudbeheer voor de Chrome-browser

Download de Chrome-browser voor je bedrijf

Meer informatie over Enterprise Support voor de Chrome-browser

Bekijk de lijst met beleid voor de Chrome-browser

Lees de nieuwste release-opmerkingen voor de zakelijke Chrome-browser

Blijf op de hoogte van de nieuwste release-updates van de Chrome-browser via de Chrome Releases-blog

Bekijk de officiële Safety & Security-blog van Google

Ga naar het Helpcentrum voor de zakelijke Chrome-browser en het Helpforum voor de Chrome-browser

Bekijk de openbare bugtracker voor de Chrome-browser