Technische handleiding voor Google Workspace for Education

Augustus 2021

Inhoudsopgave

1. Introductie

In juli 2021 hebben SURF en SIVON met Google overeenstemming bereikt over het beperken van alle 8 hoge privacyrisico's die samenhangen met het gebruik van Google Workspace for Education (Plus). Deze overeenstemming omvat onder meer een set aan centraal vastgestelde maatregelen die onderwijsinstellingen zelf moeten nemen om de risico's te beperken. Het gaat om instellingen die beheerders (*admins*) wijzigen in de Workspace en Chrome Admin console. De meeste maatregelen beperken het aantal gegevensverwerkingen: de data wordt geminimaliseerd en de verwerking daarvan beperkt.

Alle in deze handleiding genoemde handelingen zijn privacy-bevorderende maatregelen die meegewogen zijn bij het beperken van de risico's van het gebruik van Workspace for Education (Plus) in het onderwijs. Indien een onderwijsinstelling besluit één of meerdere van de maatregelen niet te implementeren, dan heeft dit gevolgen voor de afweging van de privacyrisico's. De onderwijsinstelling moet dan zelf onderbouwen dat het niet nemen van de technische maatregel geen gevolgen heeft voor de privacyrisico's en/of wat de compenserende maatregelen zijn die de onderwijsinstelling neemt om het privacyrisico van het gebruik van Workspace for Education niet te laten toenemen. Het niet opvolgen van de technische maatregelen is dus niet zonder gevolg en moet nadrukkelijk beschreven en getoetst worden door de functionaris voor gegevensbescherming.

Verscheidene producten of functionaliteiten van Google Workspace for Education werken door (potentieel) privacygevoelige data te delen met Google. In deze handleiding wordt uitgelegd hoe u de data kunt minimaliseren door het aanpassen van instellingen voor gebruikersaccounts en producten. We leggen uit welke maatregelen u moet nemen, waarom dit nodig is en hoe u dit kunt uitvoeren.

Deze handleiding maakt onderdeel uit van 3 stappen die scholen zelf moeten uitvoeren voordat zij Google Workspace for Education kunnen (blijven) gebruiken:

1. Accepteren gewijzigde voorwaarden Education Agreement Workspace for Education.
2. Deze technische stappen doorlopen en uitvoeren.
3. Uitvoeren onderwijsspecifieke DPIA (op basis van documentatie SURF, SIVON en Kennisnet).

2. Algemene adviezen en informatie

Informatievoorziening medewerkers, leerlingen, studenten en hun ouders

Het verdient de voorkeur om bij het begin van het schooljaar uw medewerkers, leerlingen, studenten en hun ouders te informeren over het gebruik van Google Workspace for Education en de gekozen privacy-instellingen. SIVON stelt hiervoor voorbeeldbrieven voor medewerkers en ouders beschikbaar. Het gaat hierbij specifiek om informatie over de verwerking van gegevens door Google, de afspraken van de onderwijsinstelling met Google en 'high level information' over de risico's van het gebruik van Workspace for Education. Dit laatste betekent dat de afspraken met Google alleen gelden zolang medewerkers, leerlingen en studenten ingelogd zijn in hun account en niet met een privé-account bij Google. Het is belangrijk om leerlingen en studenten erop te wijzen dat als hun profielfoto verdwijnt uit hun account, dit betekent dat ze de beschermde Workspace for Education-omgeving hebben verlaten.

Verder geldt het algemene advies aan medewerkers, leerlingen en studenten om zo min mogelijk (bijzondere) persoonsgegevens op te nemen in hun accountinformatie en in de informatie die zij met anderen delen.

Inzageverzoeken

Studenten die meer informatie willen over de gegevens die Google van en over hen verwerkt, kunnen bij hun onderwijsinstelling via de Administrator van Workspace for Education informatie opvragen. Als een medewerker, leerling of student klaagt dat het antwoord op diens inzageverzoek onvolledig is beantwoord, dan is het argument van Google dat zij zich beroept op de uitzondering van de AVG dat er geen inzage wordt gegeven als de betrokkene niet kan worden geïdentificeerd. Alleen de onderwijsinstelling en niet Google kan gebruikers identificeren. Bij het uitblijven van identificatie van de gebruiker, stelt Google geen informatie te mogen verstrekken over de betrokkenen.

Doorgifte van persoonsgegevens naar derde landen

In 2021 wordt een *data transfer impact assessment* (dtia) uitgevoerd zoals dat beschreven is in de adviezen van de Autoriteit Persoonsgegeven (AP) en de EDPB. Accepteer de (nieuwe) standard contractuale clausules van Google zodra deze beschikbaar worden gesteld. Deze dtia wordt beschikbaar gesteld zodra deze is afgerond door SURF en SIVON. Meer informatie over doorgifte van persoonsgegevens leest u in het artikel Aanbevelingen voor doorgifte data naar onveilige landen definitief.

Subverwerkers

Een van de risico's is het gebrek aan informatie over de leveranciers van Google (subverwerkers). Google gebruikt twee subverwerkers voor Nederland en kent subverwerkers voor 3 type activiteiten (doelbinding).

Data Center Operations: Beheer van het Google datacenter waar opslag van klantdata plaatsvindt. De subverwerker heeft geen toegang tot klantdata.

Service Maintenance: Subverwerker voor technisch onderhoud en probleemoplossing op software en hardware. De subverwerker kan beperkt toegang nodig hebben tot klantdata om technische problemen op te lossen.

Technical Support: Als een schoolbestuur een supportvraag heeft komt deze bij een subverwerker terecht. De subverwerker heeft toegang tot de data die het schoolbestuur meestuurt met een supportvraag.

De subverwerkers voor Nederland zijn:

Entity name	Relevant Google Cloud Platform Service(s)	Activity	Country where processing is performed	Registered address	Country of registration	Company number
Google Netherlands B.V.	All Google Workspace and Cloud Identity Services	Service Maintenance Technical Support	Netherlands	Claude Debussylaan 34, 15th Floor Amsterdam	Netherlands	34198589
Green Box Computing B.V.	All Google Workspace and Cloud Identity Services	Data Center Operations	Netherlands	Oostpolder 4 Eemshaven	Netherlands	58465197

Informatie over alle subverwerkers van Google is te vinden op de pagina Google Workspace and Cloud Identity Subprocessors.

Meer informatie over privacy

Meer informatie over Chrome privacy is te vinden in de Google Chrome Privacy Whitepaper.

Meer informatie over welke adviezen Google geeft voor nakoming van de AVG is te vinden in de Google Workspace Edu Data Protection Implementation Guide.

3. Overzicht maatregelen

De onderwijsinstelling dient verscheidene functionaliteiten van Google Workspace for Education op een specifieke wijze in te stellen of uit te zetten. In onderstaande tabel is een overzicht opgenomen van de maatregelen die u moet nemen en de bijbehorende wijze van beheer. In de volgende hoofdstukken worden de maatregelen verder toegelicht inclusief informatie over implementatie.

N.B. Chromebooks vormen onderwerp van een aparte DPIA waarvan de resultaten in oktober 2021 verwacht worden. Het gaat hier specifiek over de maatregelen in Google Workspace.

Implementatiewijzes

Er zijn drie manieren van implementatie voor de te nemen maatregelen:

- Centraal beheer van instellingen via Google Workspace Admin console.
- Centraal beheer van instellingen via groepsbeleid (Group Policy) van het besturingssysteem.
- Individuele instellingen.

Maatregelen die de gebruiker en bijbehorende gebruikersaccounts betreffen, kunnen veelal alleen via de Google Workspace omgeving in de Admin console ingesteld worden. U kunt deze beheerdersomgeving bereiken via admin.google.com.

Maatregelen die dataminimalisatie bij het gebruik van producten of functionaliteiten betreffen kunnen ofwel via de Admin console, ofwel via het groepsbeleid van het besturingssysteem geïmplementeerd worden.

Slechts in een enkel geval zal een individuele gebruiker maatregelen hoeven nemen. In deze handleiding wordt zo veel mogelijk uitgegaan van gecentraliseerd beheer van de te treffen maatregelen.

Maatregelen betreffende gebruikersaccounts

Gebruikersprofiel	K-12 profiel instellen voor alle gebruikers
	Geen gebruik make van echte namen van leerlingen en leraren in gebruikersnamen
	Gebruikers verbieden profiel zelf aan te passen
Geografische locatie dataopslag	Google Cloud opslaglocatie aanpassen naar Europa
Aanvullende Google diensten	Uitzetten van aanvullende Google-services
Google Workspace Marketplace-apps	Gebruikers niet toestaan apps uit de Google Workspace Marketplace te installeren
Nieuwe Google producten	Nieuwe producten niet automatisch beschikbaar te stellen voor gebruikers

Maatregelen betreffende dataminimalisatie in producten en functionaliteiten

Product of functionaliteit	Admin console instelling	Besturingssysteem groepsbeleid
Spellingcontrole	Spellingcontrole uitzetten	SpellCheckEnabled: false
Spellingcontrole Webservice	Webservice voor spellingcontrole uitzetten	SpellCheckServiceEnabled: false
Chromebrowser	Inloggen op Chromebrowser niet toestaan	BrowserSignin: 0
Automatische vertaling websites	Nooit een vertaling voorstellen	TranslateEnabled: false
Geolocatie	Niet toestaan dat sites de geolocatie van gebruikers vaststellen	DefaultGeolocationSetting: 2
Gebruikersfeedback formulier	Gebruikersfeedback niet toestaan	UserFeedbackAllowed: false
Rapportage van statistieken	Anonieme gebruikersrapporten en rapporten met gegevens over crashes nooit naar Google sturen	MetricsReportingEnabled: false
Nieuw Tabblad Contentsuggesties	Geen contentsuggesties weergeven op de pagina Nieuw tabblad	NTPCardsVisible: false
Tabblad promotionele content	Weergave promotionele content op volledig tabblad uitschakelen	PromotionalTabsEnabled: false

Nieuw Tabblad Kaarten	Kaarten niet weergeven op de pagina Nieuw Tabblad	NTPContentSuggestionsEnabled: false
Search suggested service	Gebruikers nooit toestaan search suggest te gebruiken	SearchSuggestEnabled: false
Inloggen op secundaire accounts	Gebruikers alleen toestaan met een account op het schooldomein in te loggen	SecondaryGoogleAccountSigninAllowed: false
Cookies	Cookies van derden blokkeren	BlockThirdPartyCookies: true
Cookies	Cookies alleen bewaren voor de duur van de sessie	DefaultCookieSettings: 4
Systeemrapportages van bezochte pagina's	Het verzenden van aanvullende gegevens om Safe Browsing te helpen verbeteren, uitschakelen	SafeBrowsingExtendedReportingEnabled: false
Chrome Cleanup	Niet toestaan periodiek te scannen of Resultaten van Chrome Cleanup worden nooit gedeeld met Google	ChromeCleanupEnabled: false - OF - ChromeCleanupReportingEnabled: false

Individuele maatregelen en instructies

Advertentiepersonalisatie	Individueel instellen, indien er géén sprake is van een K-12 gebruikersprofiel.
Youtube video embedding	Gebruik alleen embedded video's met 'privacy-enhanced mode'.
Gebruik geen Chrome browser	Gebruik een alternatieve browser, totdat de nieuwe versie uitkomt waar Google als data verwerker optreedt.
Gebruik Google niet als zoekmachine	Gebruik een privacyvriendelijke zoekmachine, zoals DuckDuckGo of Startpage.
Gebruik een advertentie- en/of tracking blocker	Installeer een browserextensie die tracking blokkeert.
Gebruik geen privacy gevoelige informatie in file en folder namen	Instrueer gebruikers over privacy gevoelige informatie in file en folder namen

4. Centrale beheeropties mogelijk maken

Onder beheer plaatsen van Chromebooks en Chromebrowsers

Beheerders van Google Workspace hebben een type account waarmee veel controle kan worden uitgeoefend op de data die met Google gedeeld wordt. De meeste maatregelen kunnen gecentraliseerd vanuit de Google Workspace Admin console beheerd worden.

Om dit mogelijk te maken moeten de Chromebooks en Chromebrowsers van een organisatie ook daadwerkelijk onder beheer geplaatst zijn. De Chromebooks en Chromebrowsers moeten hiervoor aangemeld zijn bij uw organisatie en desbetreffende organisatie-eenheid binnen Google Workspace. Deze nemen vervolgens alle instellingen over die u in de Google Workspace Admin console aangeeft.

Bij Chromebooks dient het gehele apparaat onder beheer gesteld te worden. Bij de besturingssystemen Windows, Mac en Linux dient de Chromebrowser onder beheer geplaatst te worden. Hieronder volgen de instructies om dit te bewerkstelligen.

Chromebooks onder beheer brengen

Chromebooks onder beheer brengen gebeurt veelal via uw leverancier. Voor centraal beheer van Chromebooks heeft u de Chrome Education Upgrade licentie nodig. Indien uw leverancier uw Chromebooks nog niet onder centraal beheer gebracht heeft, doet u het volgende.

Bij opstart van een nieuwe Chromebook of een Chromebook waar een powerwash (factory reset) op uitgevoerd is, klikt u na het verbinden met wifi en het accepteren van de voorwaarden op “Aanmelden voor Enterprise”. Hier voert u de inloggegevens in van een gebruiker met inschrijfrechten. Het Chromebook wordt nu geregistreerd in uw Workspace omgeving voor centraal beheer.

Vanuit de beheeromgeving van Google Workspace kunt u deze Chromebook nu in de gewenste organisatie-eenheid, zoals de klas, plaatsen.

Chromebook beheerde gastsessie

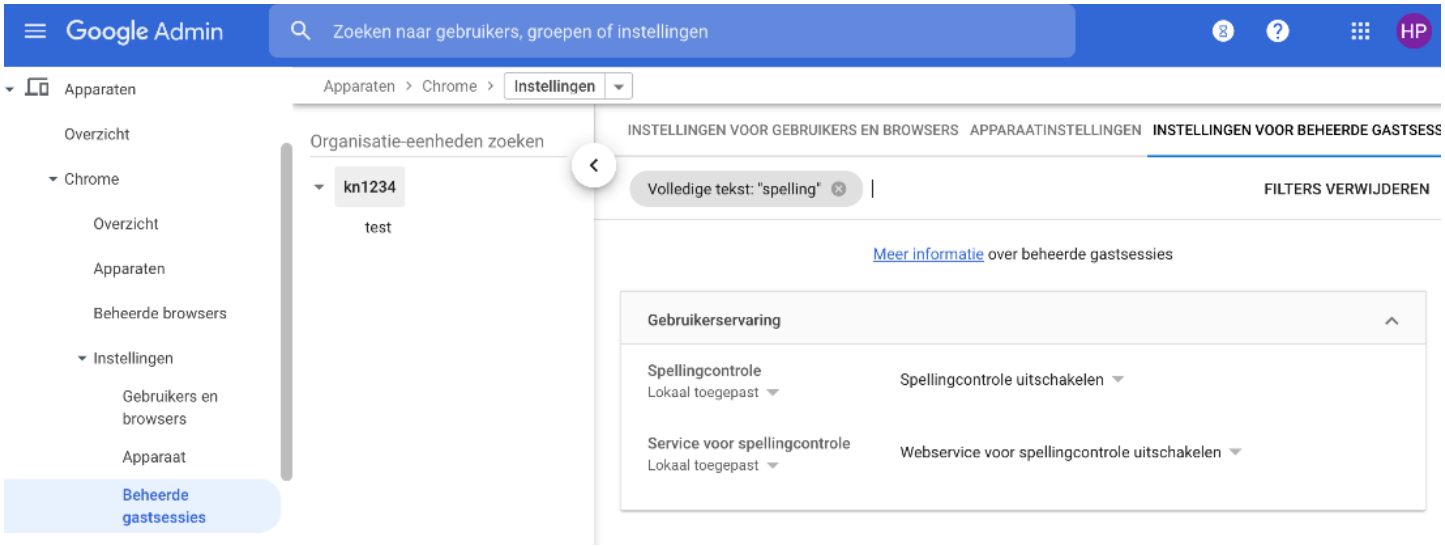
In een beheerde gastsessie start de gebruiker het Chromebook besturingssysteem op als gast in plaats van als gebruiker. De instellingen voor o.a. netwerk- en printerbeheer van het apparaat worden wel centraal door de ict-beheerder beheerd. De opslag van bestanden op het apparaat is van tijdelijke aard. Als u bijvoorbeeld een plaatje downloadt, dan wordt deze automatisch verwijderd bij het afsluiten van de Chromebook. Daarnaast opent gedurende een beheerde gastsessie de Chromebrowser ook altijd in gastmodus. Alle browsergerelateerde data (formulieren, browsergeschiedenis, cookies en inlogsessies op websites en webapplicaties) zijn tijdelijk en worden bij afsluiten van het apparaat verwijderd.

Bij het onder beheer plaatsen van een Chromebook, kunt u ervoor kiezen om een Chromebook zonder gebruikersaccounts te gebruiken. Dit doet u door het Chromebook automatisch te laten opstarten in een beheerde gastsessie. In de Workspace Admin Console doet u dit onder Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies > Beheerde gastsessie automatisch starten.

In deze handleiding staan veel instellingen die voor gebruikers en browsers gelden. Deze zijn in te stellen via Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers. Als u Chromebooks in beheerde gastsessie binnen uw organisatie gebruikt dan zult u al deze instellingen ook moeten uitvoeren voor de gastsessies onder Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies.

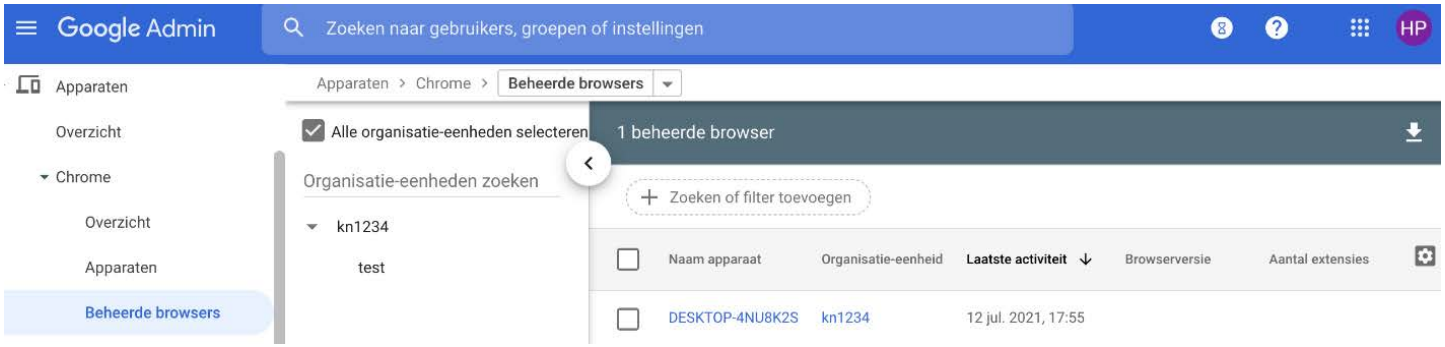
Als voorbeeld hieronder de instellingen voor spellingcontrole. Alle instellingen beschreven voor gebruikers en browsers zult u dus ook voor beheerde gastsessie moeten uitvoeren.

Spelling controle uitzetten voor beheerde gastsessies onder: Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies.



Chromebrowsers onder beheer brengen

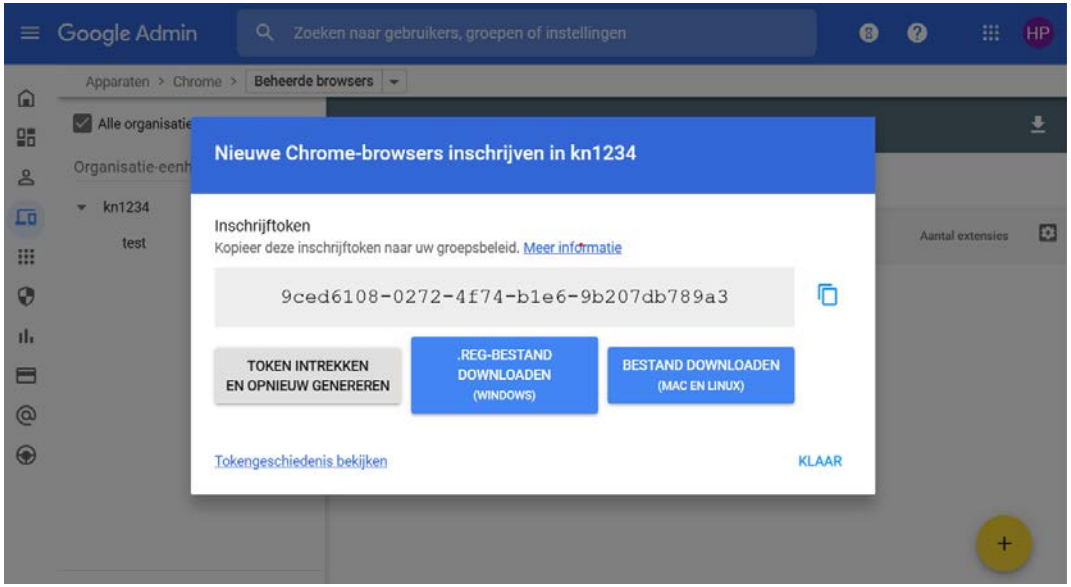
U kunt de Chromebrowser instellingen alleen centraal beheren als deze onder beheer staan. Dit is te controleren in de Admin console onder Apparaten > Chrome > Beheerde browsers



Als u een ander besturingssysteem gebruikt, zoals Windows of Mac, dan voert u de volgende stappen uit:

1. Token voor beheer genereren vanuit de Admin Console.
2. Beheerderspolicy met de beerderstoken instellen op uw besturingssysteem.

U genereert de token onder Apparaten > Chrome > Beheerde browsers. Rechtsonder in beeld klikt u op het gele plusteken (‘+’).



De token installeert u vervolgens het groepsbeleid van uw besturingssysteem via het beleid ‘CloudManagementEnrollmentToken’. In de hieropvolgende sectie leest u meer over groepsbeleid.

Instellingen op het besturingssysteem via groepsbeleid

Sommige van de te nemen maatregelen kunt u direct op het besturingssysteem bewerkstelligen via een zogenaamde ‘group policy’, ofwel groepsbeleid. De instelling van het besturingssysteem hebben voorrang over de instellingen die via de Admin console zijn ingesteld. In de overzichtstabel van de maatregelen is terug te vinden welke policies u op welke manier kunt instellen via het groepsbeleid.

Als beheerder zult u of uw leverancier voor het beheren van groepsbeleid gebruik maken van een zogenaamde Group Policy beheertool. Het algemene beheer van de apparaten van uw organisatie valt buiten het bestek van deze handleiding. Hiervoor kunt u eventueel terecht bij uw leverancier.

Meer informatie over de instellingen via het besturingssysteem vindt u op de pagina Lijst met Chrome Enterprise-beleid.

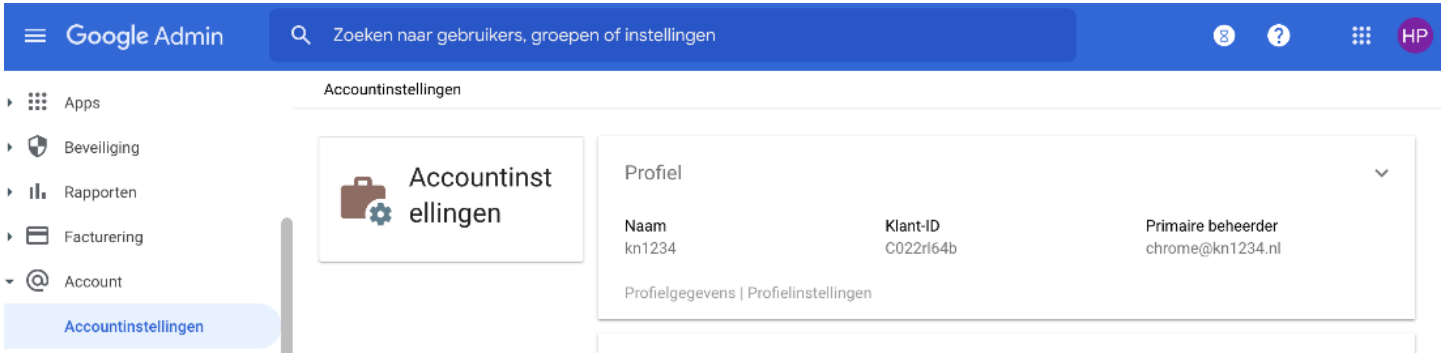
5. Instellingen in de Admin console

Google Workspace als K-12 instellen

Het verplichte onderwijs in de Verenigde Staten beslaat dertien jaar. Het begint met een jaar kindergarten, een soort kleuterschool, gevolgd door 12 jaar klassikaal onderwijs, van de eerste tot en met de twaalfde klas. Daarom wordt dit systeem wel K-through-12 of K-12 genoemd. K-12 komt grofweg overeen met primair en voortgezet onderwijs in Nederland.

Om de privacy van kinderen op deze 'K-12 scholen' te beschermen kent Google Workspace for Education een speciale K-12 instelling. Met deze instelling staan alle personalisatie instellingen uit. Google Workspace als K-12 school gebruiken geeft de hoogte bescherming van persoonsgegevens. Ook voor onderwijsinstellingen in andere sectoren dan het po en vo bestaat de mogelijkheid om zelf te kiezen deze om deze K-12 instellingen in te stellen. Google zal hier niet op controleren of de onderwijsinstellingen een K-12 instelling is, of vrijwillig kiest deze instellingen toe passen op de eigen organisatie. Het kiezen voor deze instelling betekent de keuze voor *privacy by default*: één van de eisen is van de AVG.

In de Admin console van Google Workspace selecteert u organisatietype Primary/secundairy education onder: Accountinstellingen > Profiel > organisatietype.



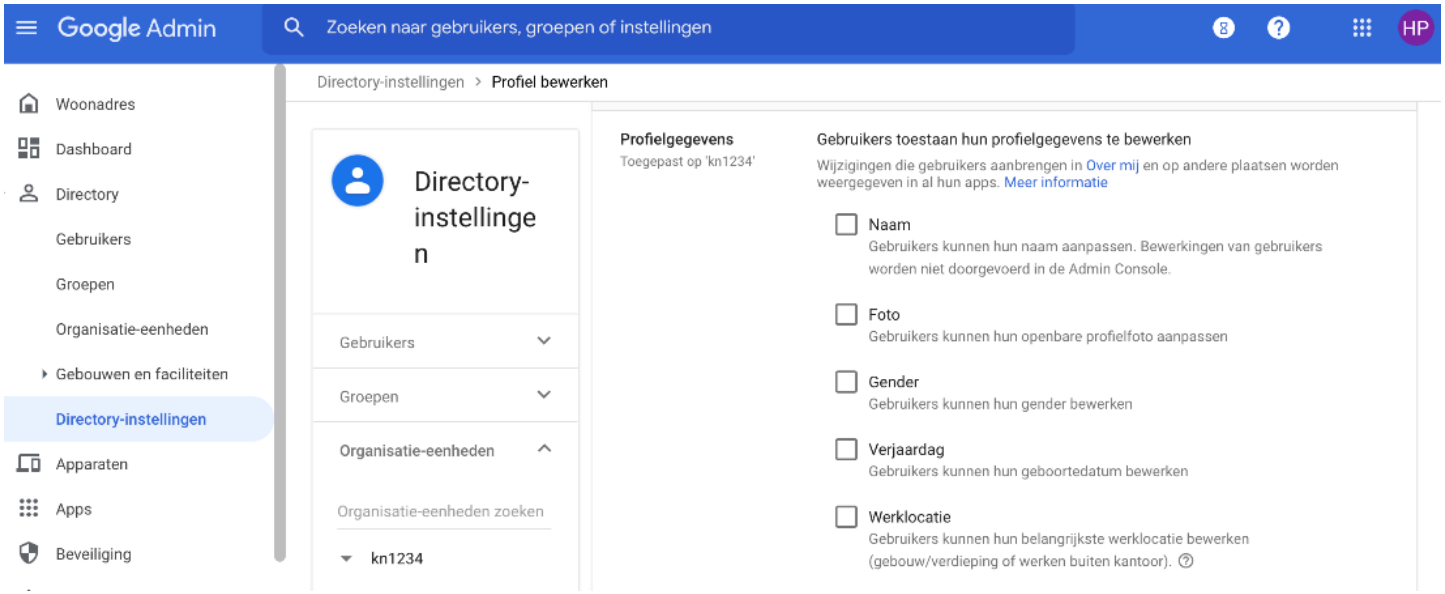
Gebruikersnamen

Het is aan te bevelen om leraren en leerlingen niet onder hun echte naam als gebruiker in Google Workspace te zetten. Ook het beheeraccount kan een fictieve naam hebben. Dit staat beschreven in de Workspace for Education Data Protection Implementation Guide.

Gebruikersprofielen

Beheerders kunnen instellen dat gebruikers hun profiel niet kunnen aanpassen. Hierdoor voorkomt u dat leraren en leerlingen alsnog persoonlijke data toevoegen en hun profiel aanvullen met gevoelige gegevens.

Instellen onder: Directory instellingen > Profiel bewerken.



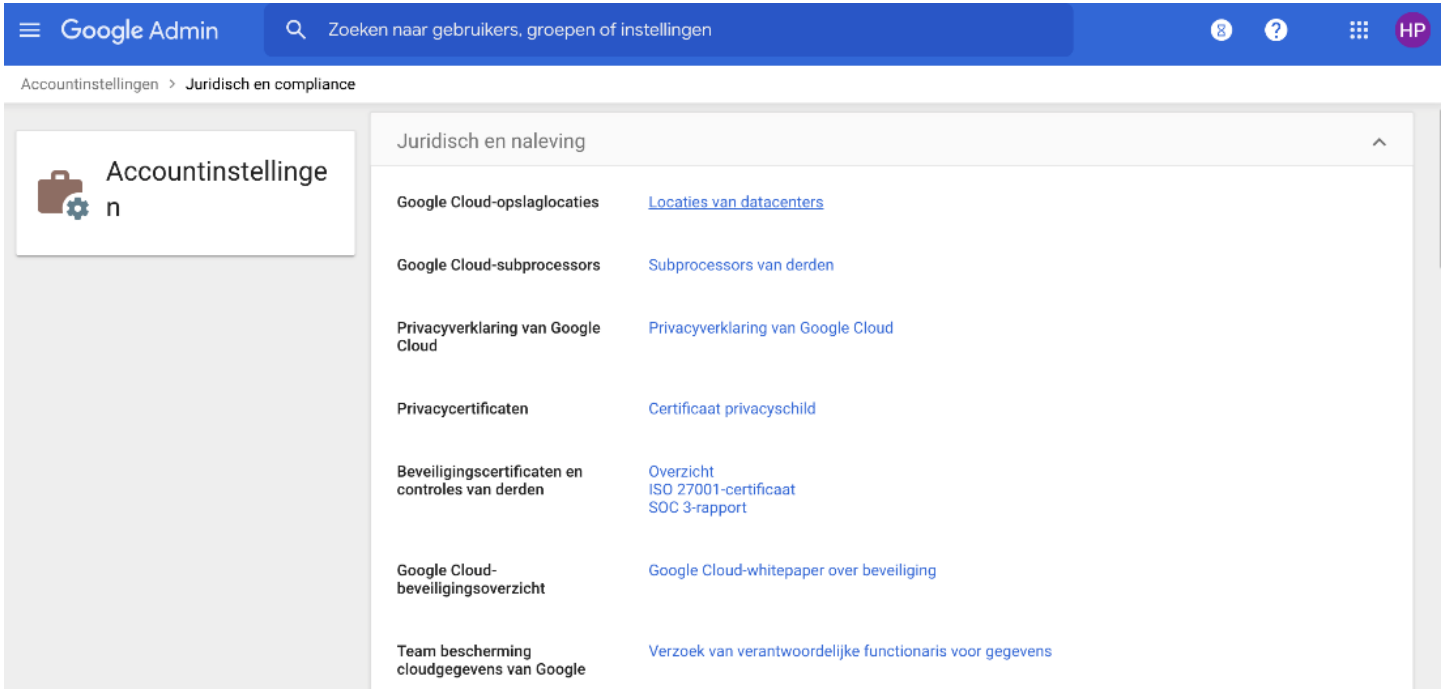
Geografische locatie dataopslag

Als beheerder kunt u bepaalde gegevens opslaan in een specifieke geografische locatie door een beleid voor gegevensregio's te gebruiken. De opties voor geografische locaties zijn de Verenigde Staten en Europa.

Dataopslag in Europe geeft u de hoogste bescherming van persoonsgegevens. Om Europa als dataopslag te kunnen instellen heeft u de versie Educations standard of plus van Workspace for Education nodig.

Door deze instelling wordt het dataverkeer met de Verenigde Staten beperkt en blijven gegevens binnen Europa, één van de maatregelen om de risico's te beperken. Data die door deze instelling geografisch beheerd worden vindt u bij de Google Workspace Admin Help.

Instellen onder > Admin console > Account instellingen > Juridisch en Compliance.



Aanvullende Google diensten (Additional Services)

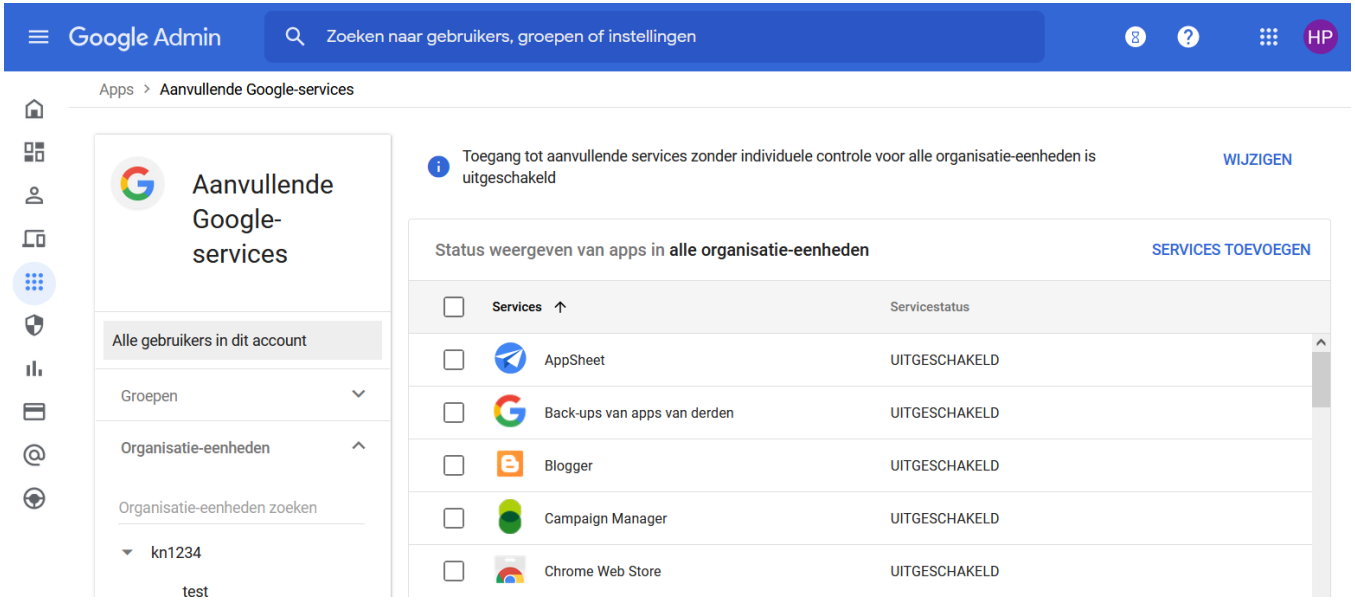
Aanvullende Google diensten vallen niet onder de Google Workspace overeenkomst die SURF en SIVON met Google hebben afgesloten. Deze aanvullende diensten moeten dus uit staan.

Door het gebruik van deze Additional Services zouden onderwijsinstellingen Google toegang geven tot informatie van hun leerlingen en studenten, zonder dat de onderwijsinstellingen de volledige controle houden over hun gegevens. Dat zou in strijd zijn met de AVG. Dat betekent dat toegang tot aanvullende services (standaard) uitgeschakeld moet zijn.

- Wanneer de toegang tot Aanvullende diensten is geblokkeerd, kunnen leerlingen wel Zoeken (Google Search) nog steeds gebruiken omdat automatisch uitloggen in SafeSearch-modus aanstaat. Hierdoor worden zij niet gevolgd door Google omdat zij 'onzichtbaar' worden uitgelogd zodat Google de gebruiker van Zoeken niet kent. Een privacyvriendelijke zoekmachine gebruiken is ook mogelijk zoals bijvoorbeeld Duck-Duck-Go.
- Het gebruik van YouTube door leerlingen en studenten is niet mogelijk zolang zij ingelogd zijn in hun account van Workspace for Education. Leraren kunnen alleen gebruik maken van YouTube-video's door deze te embedden, bijvoorbeeld door de (link naar de) video op te nemen in Classroom of Slides. Hierdoor kunnen video's nog wel bekeken worden.
- Studenten in het mbo en ho die er zelf voor willen kiezen om Scholar, YouTube of andere aanvullende services te gebruiken, moeten zich afzonderlijk bij Google aanmelden voor een consumentenaccount. Zij moeten uitloggen uit hun account van Workspace for Education bij de onderwijsinstelling. Google, en niet de universiteit, is dan verantwoordelijk voor het verkrijgen van geldige toestemming van deze studenten (van 16 jaar en ouder) voor de gegevensverwerking in dergelijke privé Google-accounts.

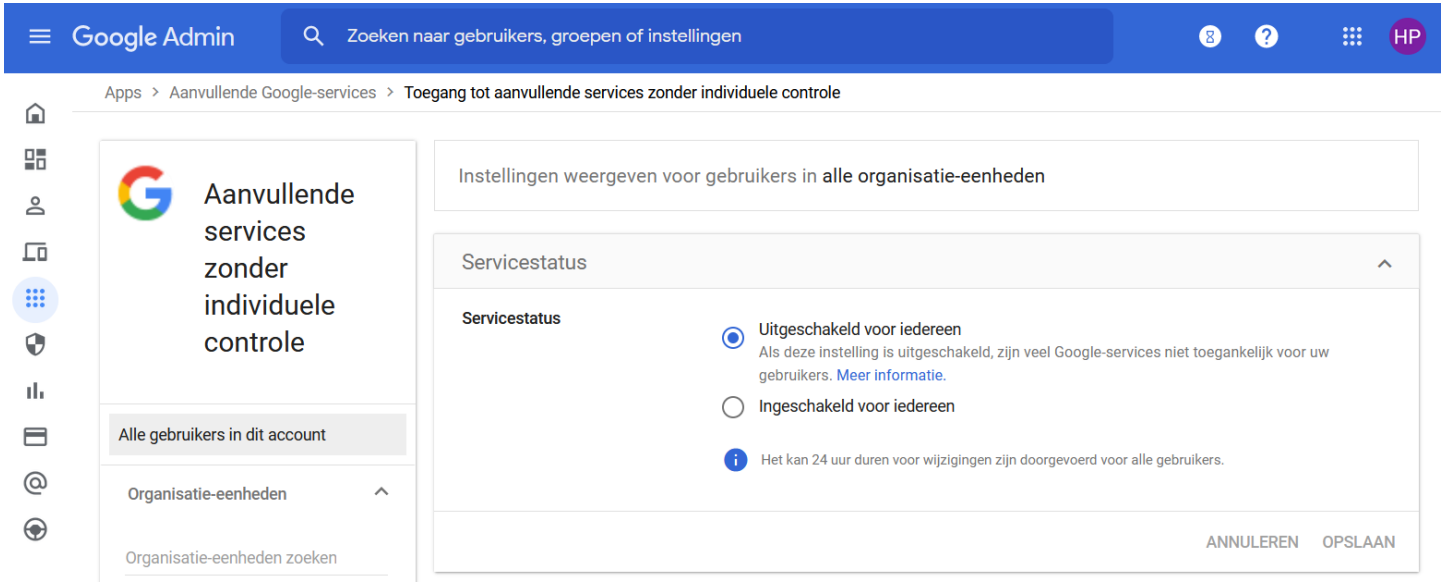
Aanvullende services kunnen individueel aan- of uitgezet worden.

Instellen onder: Admin console > Apps > Aanvullende Google services > Uitschakelen voor iedereen.



De instelling kan ook generiek voor de hele organisatie.

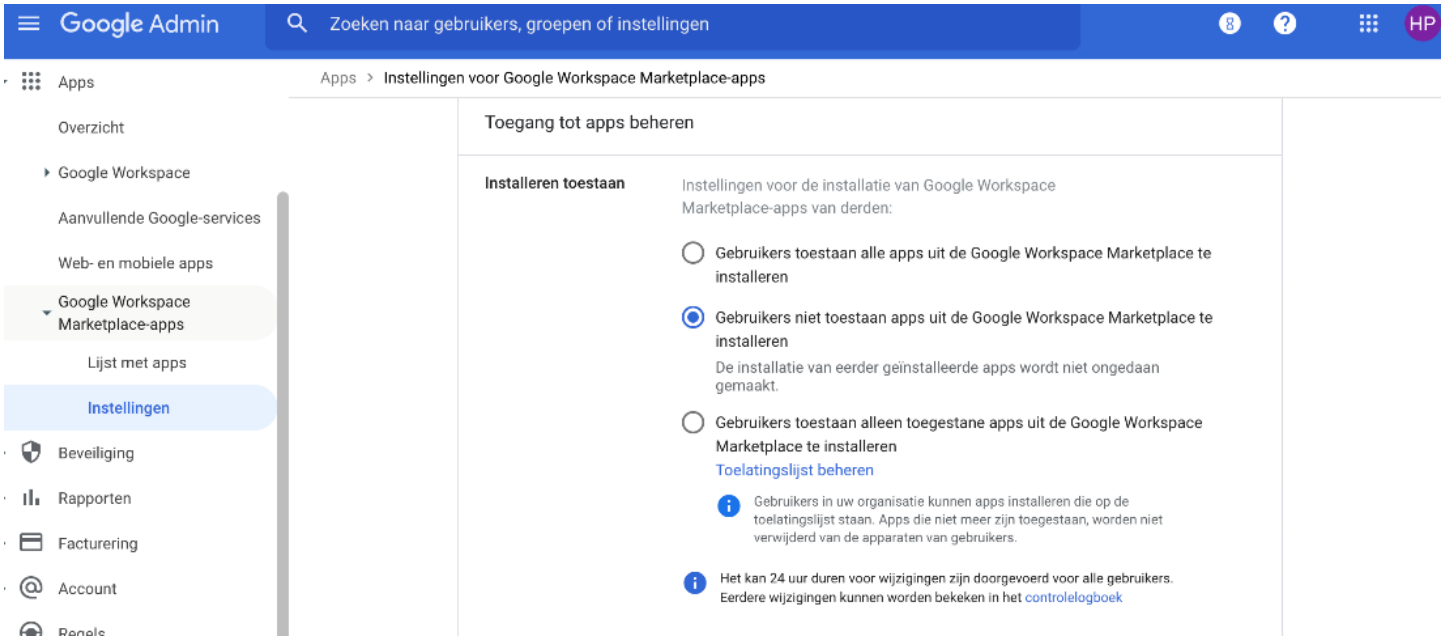
Instellen onder: Apps > Aanvullende Google services> Toegang tot aanvullende services zonder individuele controle > Uitgeschakeld voor iedereen.



Google Workspace Marketplace-apps

Het gebruik van allerlei (niet-geverifieerde) Marketplace-apps leidt tot privacyrisico's. Als leerlingen en studenten vanuit het Workspace for Education account dergelijke apps aanschaffen of downloaden, wordt de school daar verantwoordelijk voor. Dat is niet wenselijk omdat de onderwijsinstelling de controle kwijt is over de gegevens die naar (al) deze leveranciers toegaan. Daarom wort deze optie uitgezet, en kunnen medewerkers, leerlingen en studenten alleen Marketplace-apps gebruiken die vooraf door de onderwijsinstelling zijn goedgekeurd.

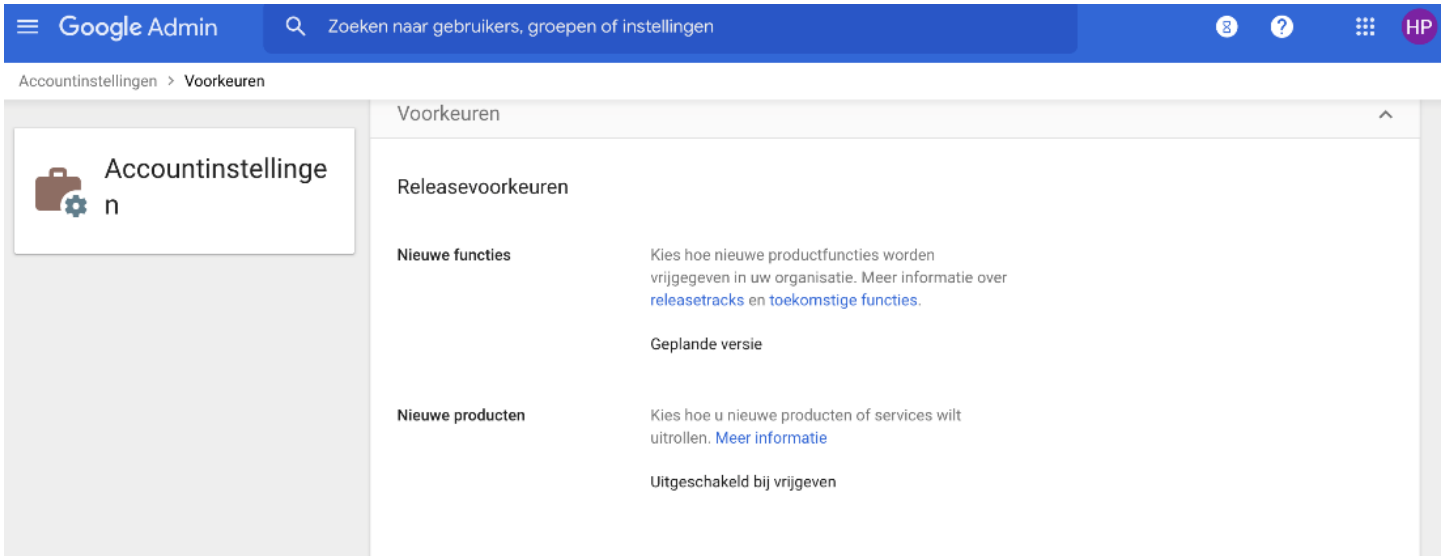
Instellen onder: Admin console > Apps > Instellingen voor Google Workspace Marketplace-apps > Gebruikers niet toestaan apps uit de Google Workspace Marketplace te installeren.



Nieuwe Google producten

Beheerders kunnen privacy risico's vermijden door nieuwe producten niet automatisch beschikbaar te stellen voor gebruikers. Nieuwe diensten kunnen dan eerst aan een analyse én DPIA onderworpen worden voordat ze beschikbaar gemaakt worden.

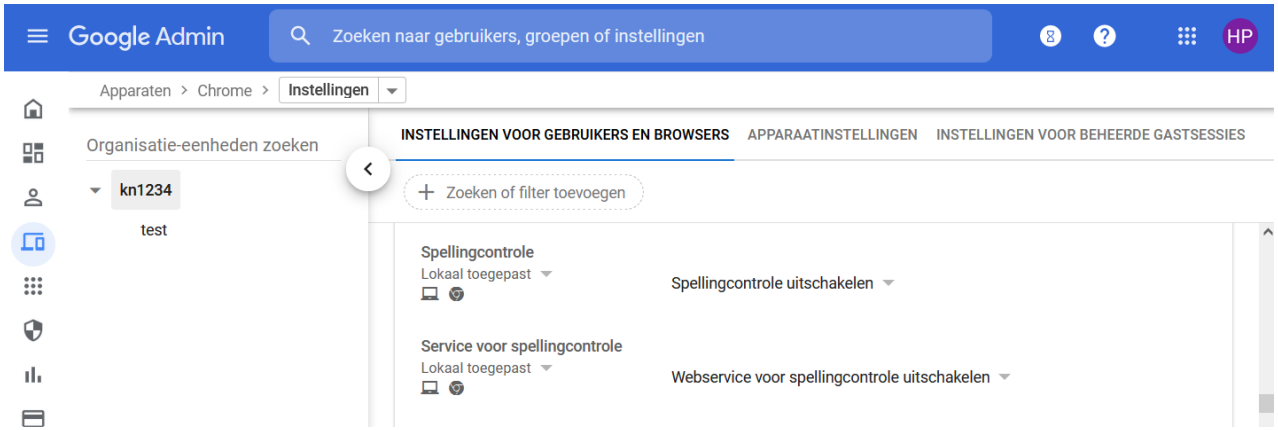
Instellen onder: Admin console > Account instellingen > Voorkeuren > Nieuwe producten > Uitschakelen bij vrijgeven.



Spellingcontrole en Spellingcontrole Webservice

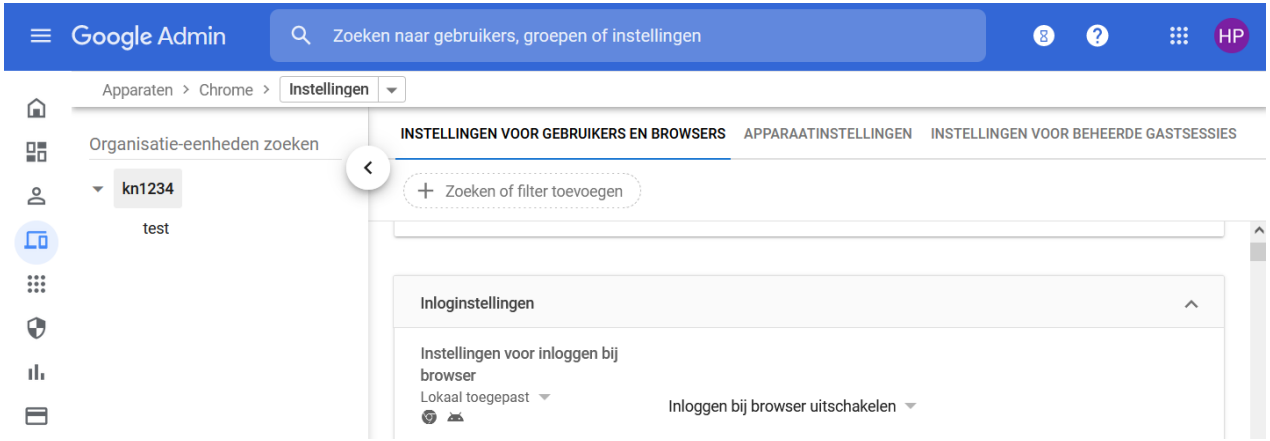
De functie spellingcontrole werkt uiteraard alleen als de data door Google op spelling gecontroleerd kan worden. Hierbij worden woorden, zinnen of zinsdelen uitgewisseld met Google. Dit is een hoog risico omdat deze verwerking in de Verenigde Staten en niet lokaal op de computer van de gebruiker plaatsvindt. Daarom moet de spellingscontrole uitstaan om de data niet te delen.

Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > Gebruikerservaring > Spellingcontrole > beide opties uitschakelen.



In aanvulling hierop moet het inloggen bij Chromebrowser verboden worden.

Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > Instellingen voor inloggen bij browser > inloggen bij browser uitschakelen.

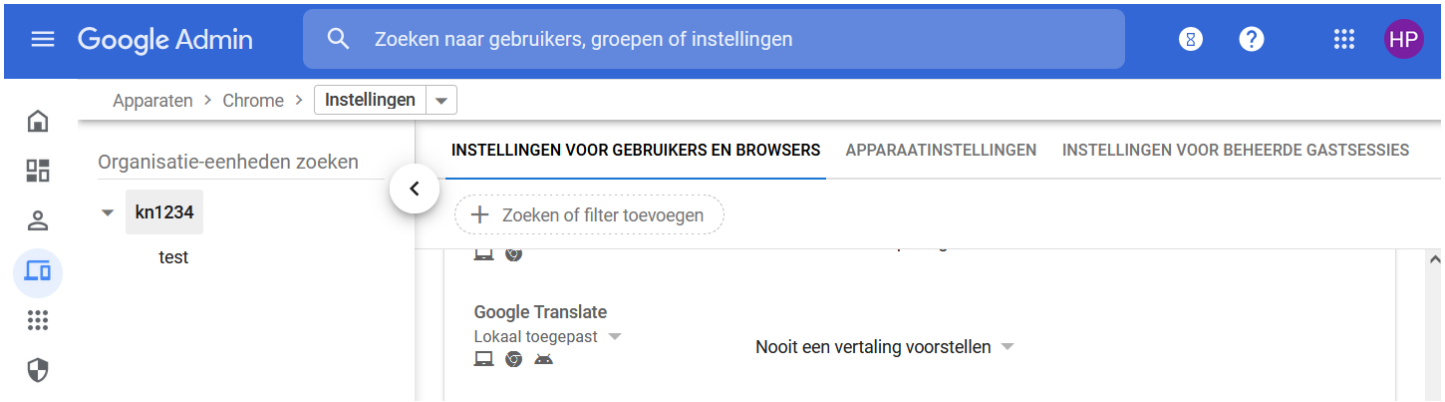


Meer informatie vindt u in de [Google Chrome Spelling Privacy Whitepaper](#).

Automatische vertaling websites uitzetten

Wat geldt voor het uitzetten van de spellingscontrole, geldt ook voor de vertaalfunctie van Google voor websites die worden bezocht. Deze werkt uiteraard alleen als de data door Google verwerkt kan worden. Om de data niet te delen moet deze functionaliteit uit staan.

Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browser > Gebruikerservaring > Nooit een vertaling voorstellen.

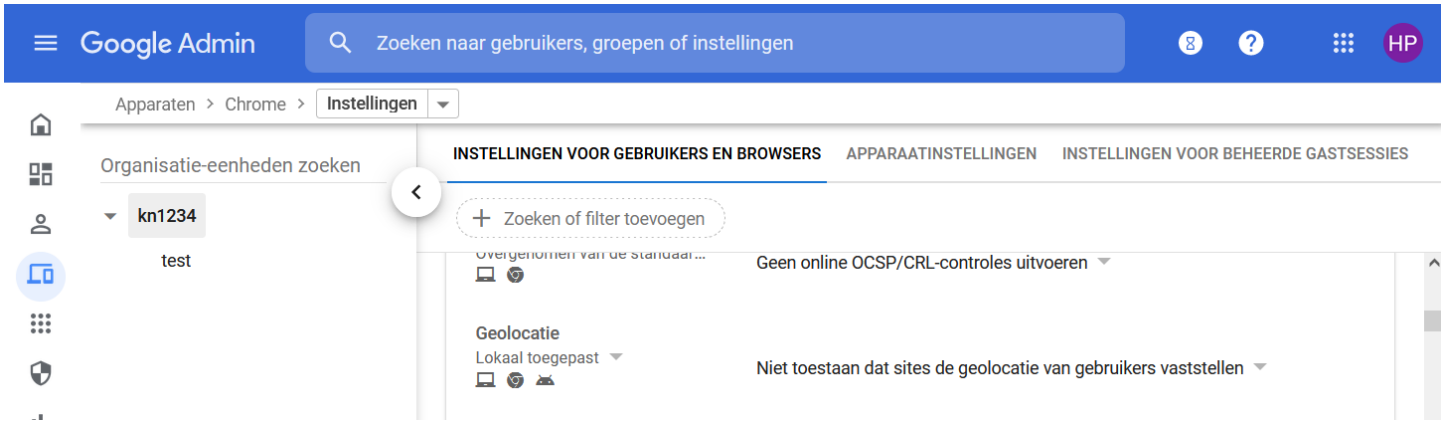


Meer informatie vindt u in de Google Chrome Privacy Whitepaper in de paragraaf Translate.

Geolocatie uitzetten

De geolocatie functie stelt websites in staat om op basis van IP-adres de locatie van de gebruiker te bepalen. Door dit uit te zetten, weet Google niet (standaard) waar de gebruiker zich bevindt en wordt het aantal verwerkte persoonsgegevens beperkt. Deze functie moet daarom uit gezet worden.

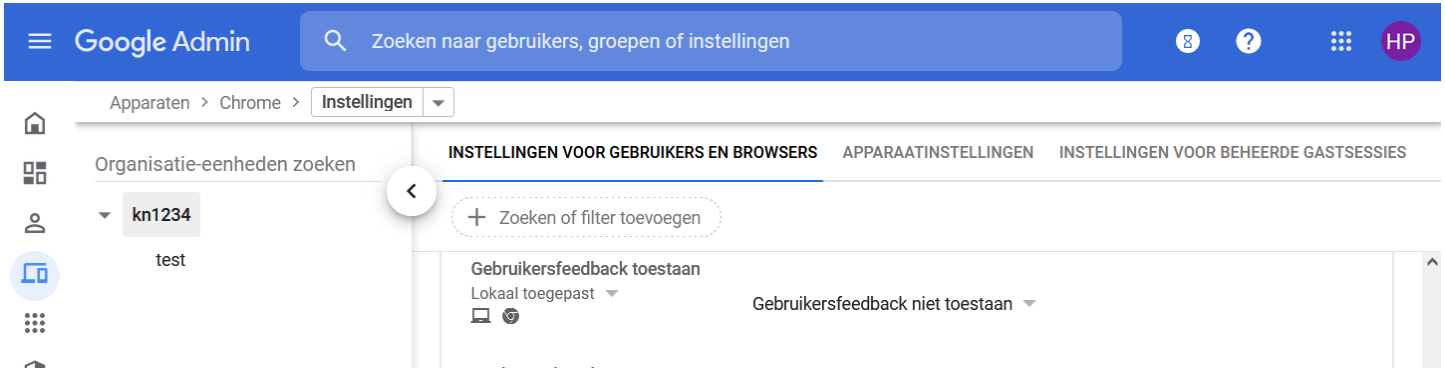
Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > Geolocatie > Niet toestaan dat sites de geolocatie van gebruikers vaststellen.



Gebruikersfeedback niet toestaan

Gebruikers niet toestaan dat ze feedback delen met Google. Als u het beleid niet instelt, kunnen gebruikers feedback naar Google sturen. Hierbij kan veel persoonlijke of zelfde gevoelige informatie worden gedeeld waar Google (en niet de onderwijsinstelling) verantwoordelijk voor is.

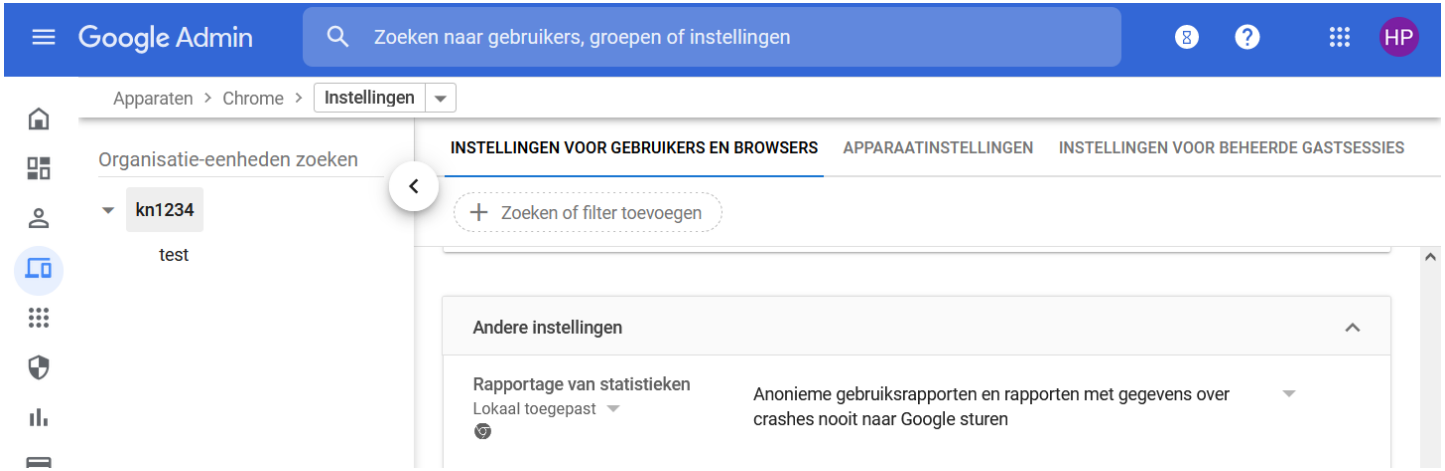
Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > Gebruikerservaring > Gebruikersfeedback Toestaan > Gebruikersfeedback niet toestaan.



Rapportage van statistieken: turn off

Voor het maken van gebruiksstatistieken en –rapportages, verzamelt Google gegevens. Door dit uit te zetten, wordt het aantal persoonsgegevens dat Google gebruikt, beperkt. Daarmee worden privacyrisico's beperkt.

Instellen onder: Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > andere instellingen > Rapportage van statistieken > Anonieme gebruikersrapporten en rapporten met gegevens over crashes nooit naar Google sturen.

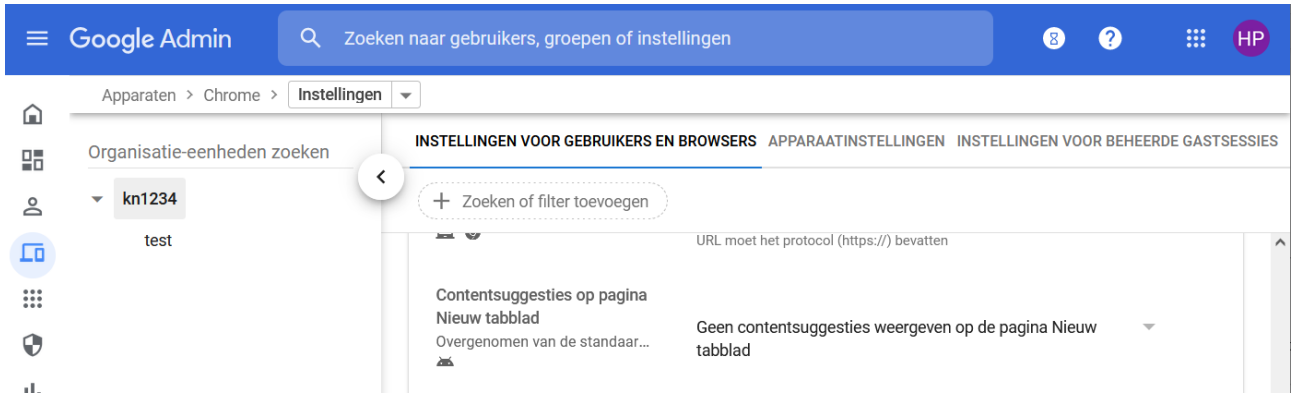


Nieuw Tabblad

Bij een nieuw tabblad kan Google helpen met het doen van suggesties. Hiervoor houdt Google informatie bij over welke websites de gebruiker bezoekt. Dat is niet wenselijk want het aantal verwerkte persoonsgegevens moet zo beperkt mogelijk zijn. Daarom moet deze instelling worden uitgezet.

In de Admin console zijn drie plekken onder Apparaten > Chrome > Instellingen waar nieuw tabblad-beleid gewijzigd moet worden.

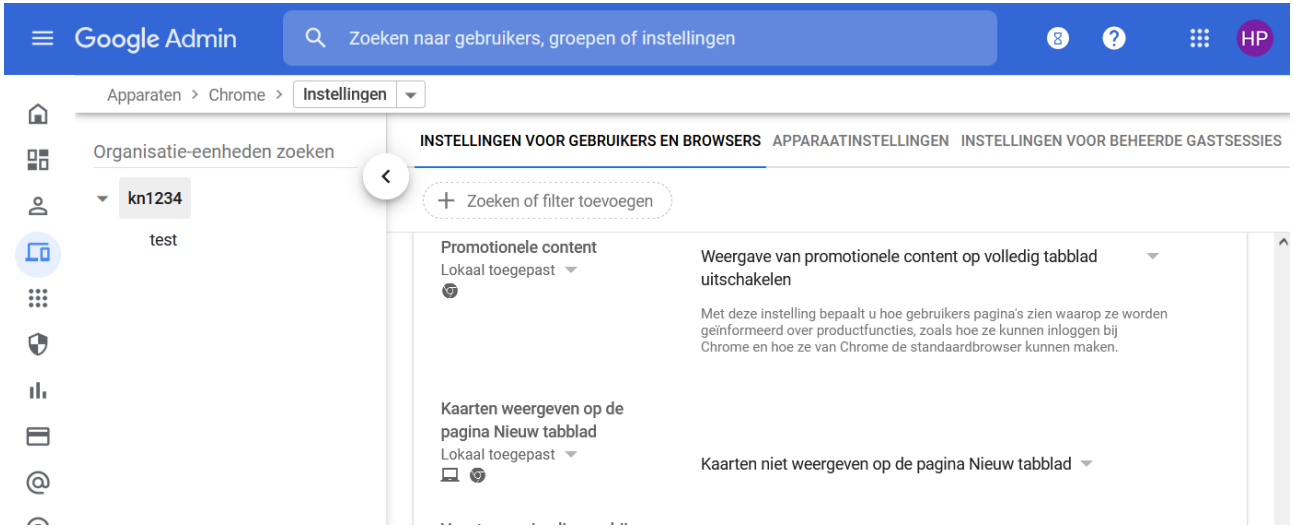
1) Apparaten > Chrome > instellingen voor gebruikers en browser > Geen contentsuggesties weergeven op pagina nieuw tabblad.



2) Apparaten > Chrome > Instellingen voor gebruikers en browser > Weergave promotionele content op volledig tabblad uitschakelen.

3) Apparaten > Chrome > Instellingen voor gebruikers en browser > Kaarten niet weergeven op de pagina nieuw tabblad.

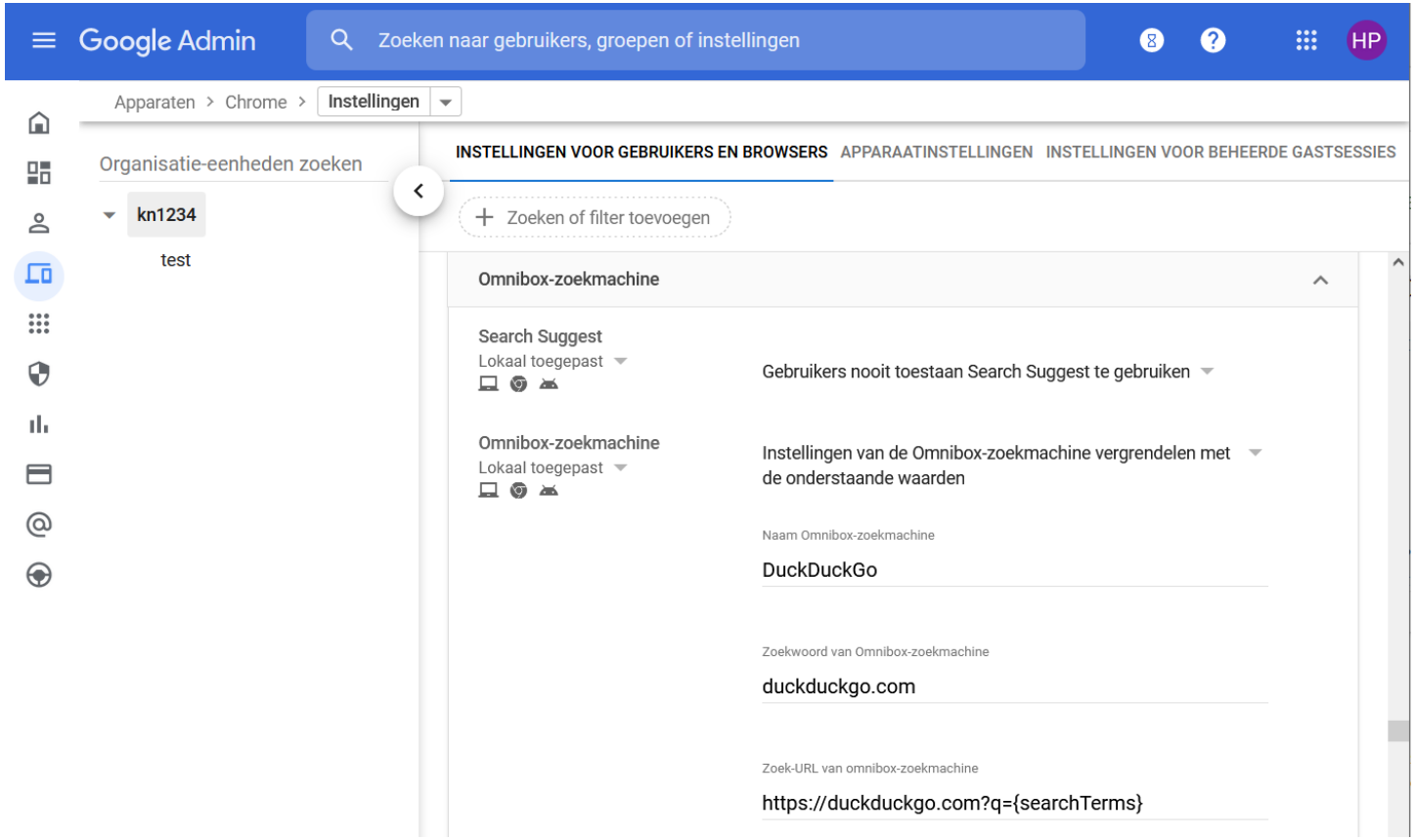
Kaarten zijn “buttons” in het nieuwe venster van veel bezochte websites of populaire websites geselecteerd door Google als er nog geen browser geschiedenis is.



Search suggested service (omnibox)

De functie *download search suggesties* wordt getoond aan ingelogde gebruikers bij het openen van een nieuw tabblad. Voor deze suggesties moet Google webbrowser historie bijhouden. Om het verzamelen en delen van deze persoonlijke data met Google te voorkomen moet deze functie uit staan.

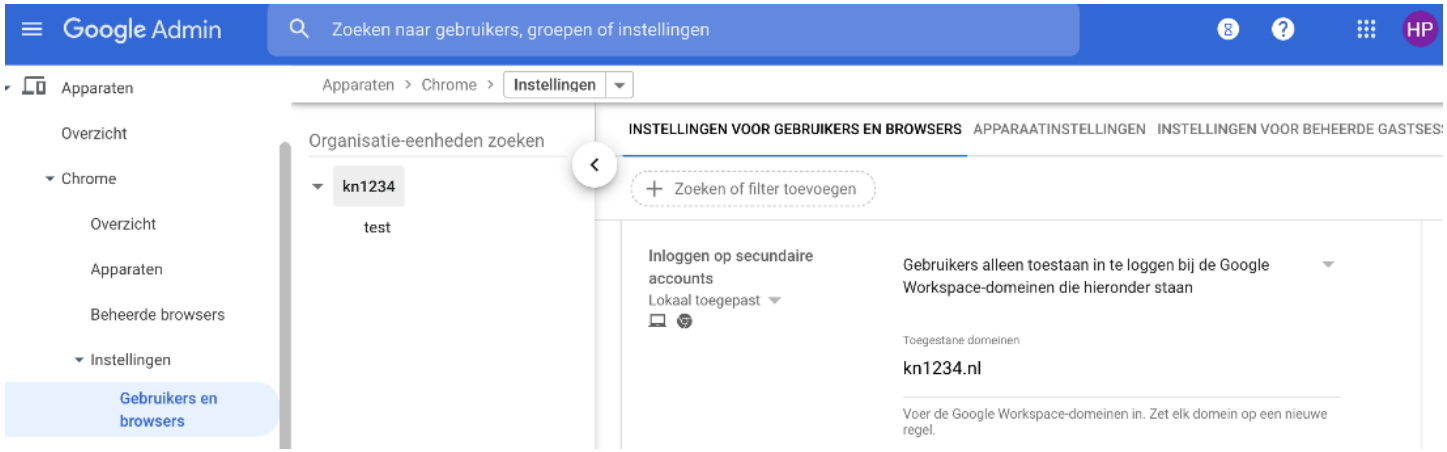
Instellen onder: Apparaten > Chrome> Instellingen> Instellingen voor gebruikers en browsers > Omnibox-zoekmachine > Gebruikers nooit toestaan search suggest te gebruiken



Inloggen op secundaire accounts

Om te voorkomen dat leerlingen hun privé Google-account koppelen aan het schoolaccount en daarmee alsnog worden blootgesteld aan privacyrisico's moet het inloggen op secundaire accounts verboden worden.

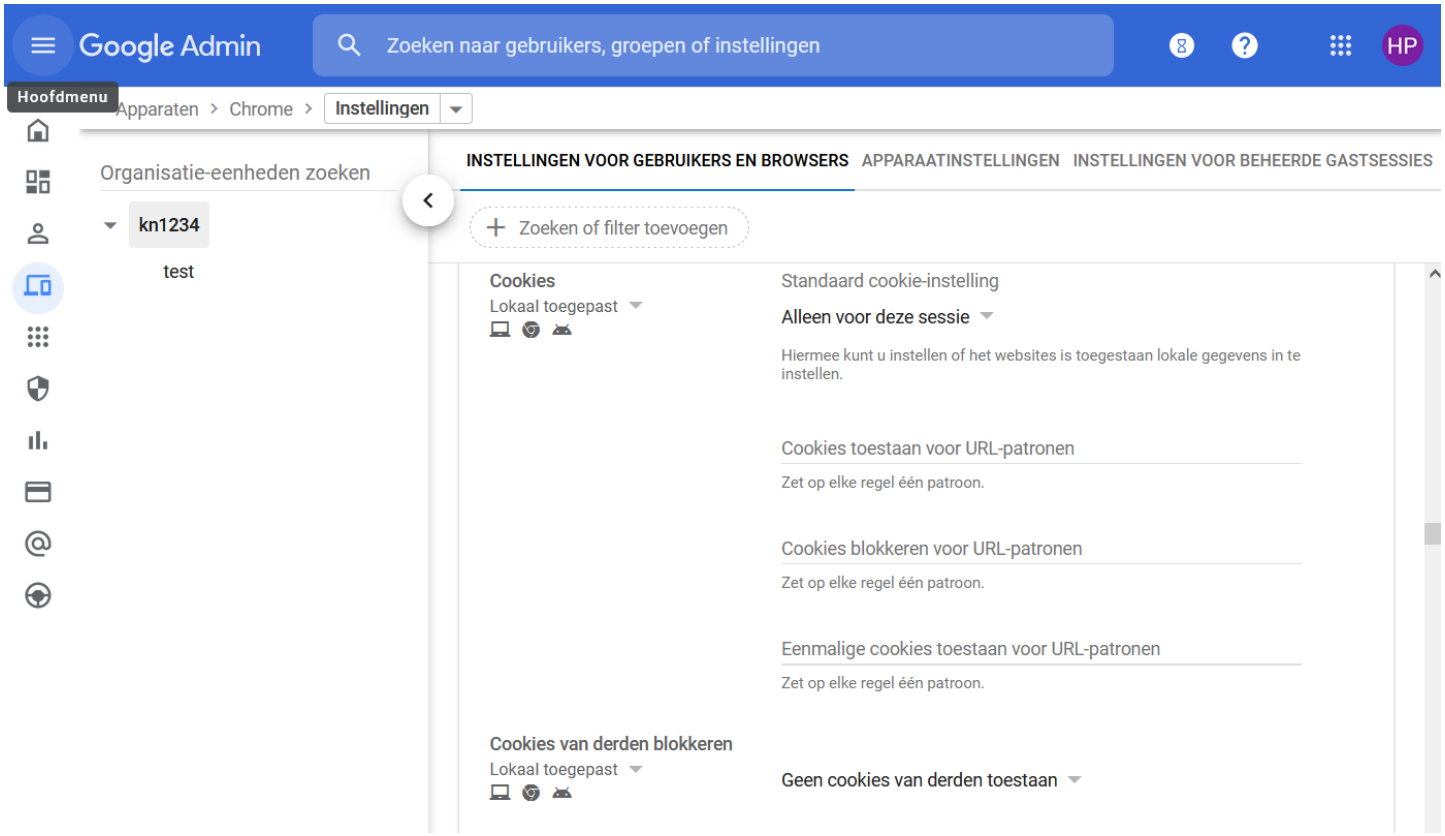
Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > Gebruikerservaring > Inloggen op secundaire accounts > Gebruikers alleen toestaan in te loggen op Workspace domeinen die hieronder staan (alleen schooldomein toevoegen).



Cookies

Leerlingen klikken bij cookies op akkoord zonder zich goed te realiseren waarop ze akkoord geven. Daarom is het aan te bevelen cookies te blokkeren.

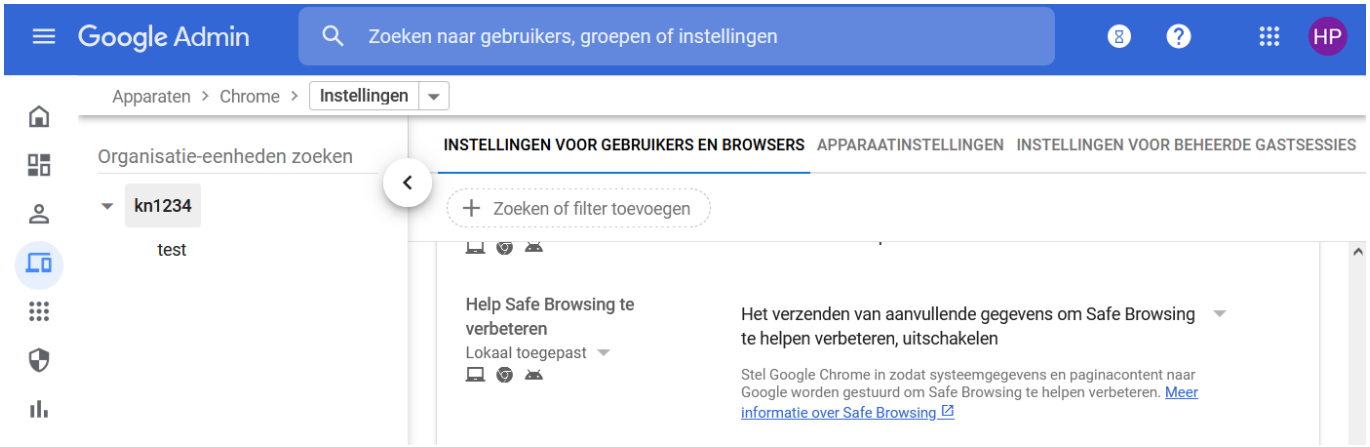
Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > Content > Cookie & Cookies van derden.



Systeemrapportages van bezochte pagina's

Ten behoeve van de safe browsing functie stuurt de Chromebrowser regelmatig systeeminformatie en de inhoud van bezochte pagina's naar Google. De inhoud van dergelijke pagina's kunnen persoonsgegevens bevatten bij bijvoorbeeld het gebruik van leermiddelen. Het is niet nodig deze informatie bij te houden en te delen met Google. Zet deze systeemrapportages daarom uit.

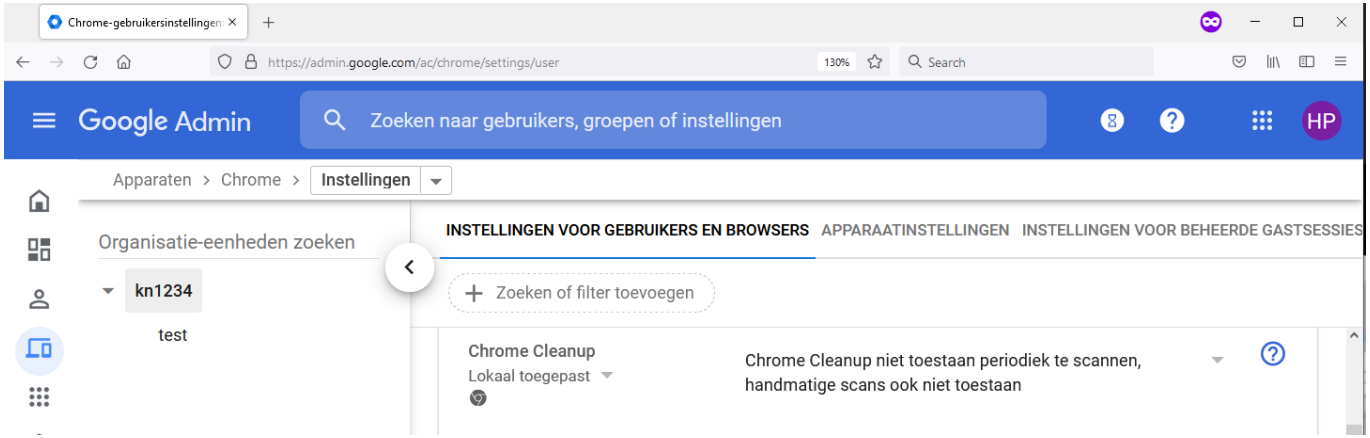
Instellen onder: Apparaten > Chrome > Instellingen voor gebruikers en browsers > andere instellingen > Help safe browsing te verbeteren > Het verzenden van aanvullende gegevens om safe browsing te helpen verbeteren uitschakelen.



Chrome Cleanup

Chrome Cleanup is een onderdeel van de Chromebrowser dat regelmatig de browser en systeemomgeving scant. Om de overdracht van gegevens te stoppen, moeten de resultaten van Chrome cleanup nooit met Google gedeeld worden.

Instellen onder: Apparaten > Chrome > Instlelingen voor gebruikers en browsers > Chrome cleanup > Resultaten van Chrome cleanup worden nooit gedeeld met Google.



6. Individuele instellingen en instructies

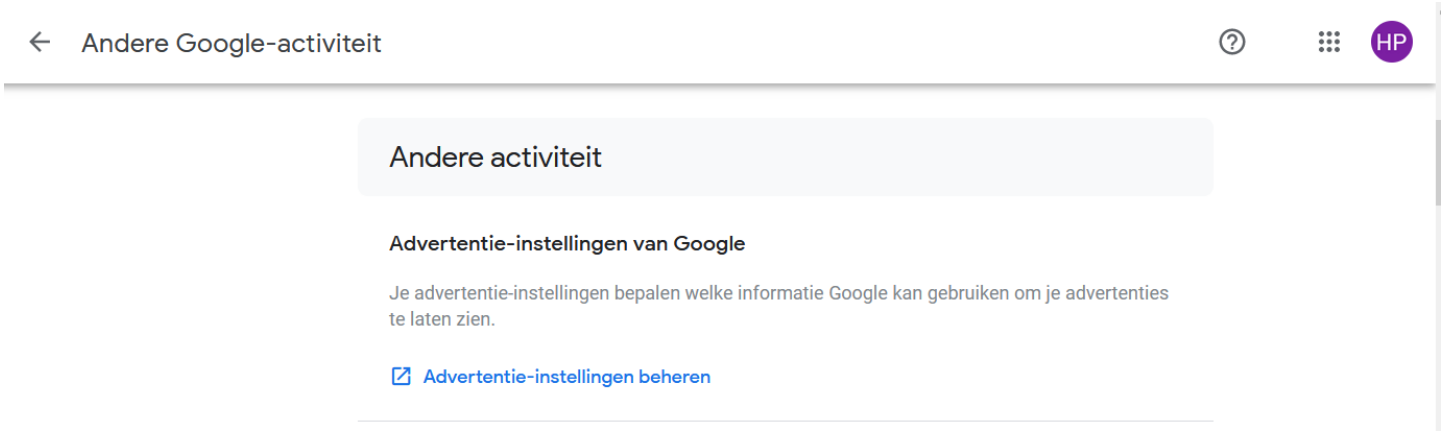
Advertentiepersonalisatie

Let op: deze maatregel is alleen van toepassing als het hierboven genoemde ‘K-12 profiel’ **niet** is ingesteld voor de gebruikersaccounts. Onderwijsinstellingen die niet gekozen hebben voor K-12, moeten de volgende instellingen dus zelf handmatig toepassen.

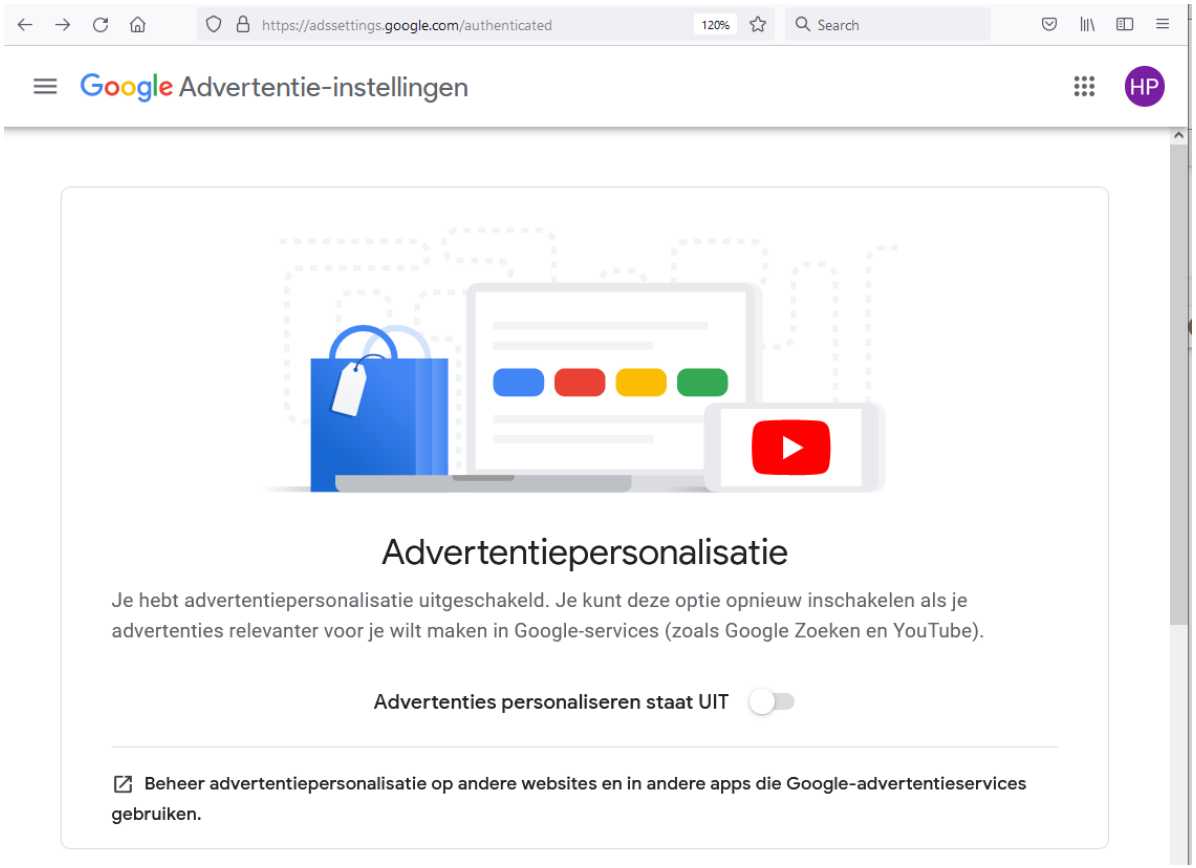
Advertenties die door Google op internetpagina's worden getoond aan een gebruiker worden gebaseerd op de persoonlijke informatie uit een Google-account, persoonlijke zoekopdrachten, browsegedrag en profilering aan de hand daarvan.

Advertentiepersonalisatie maakt gebruik van verscheidene persoonsgegevens die tijdens het browsen over internet worden verzameld. Om de data-overdracht en ontwikkeling van persoonsgegevens te onderbreken dient advertentiepersonalisatie uitgeschakeld te zijn.

Google zal bij nieuwe 'Higher Education’ accounts voor Workspace for Education deze personalisatie van advertenties uitzetten. Bestaande gebruikers moeten dit echter per gebruiker op hun eigen ‘MyActivity’ pagina wijzigen via myactivity.google.com.



Ga via het menu naar ‘Andere Google-activiteit' en klik op ‘Advertentie-instellingen beheren’. Verschuif op deze pagina de knop naar ‘Uit’.

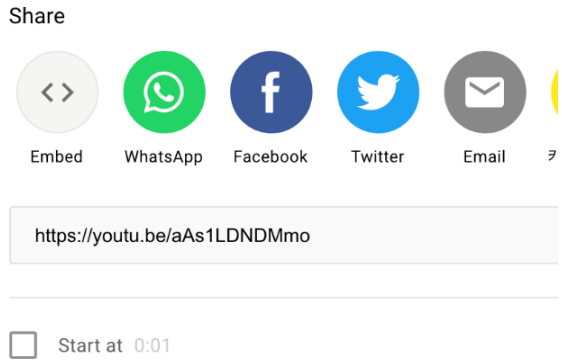


YouTube video embedding

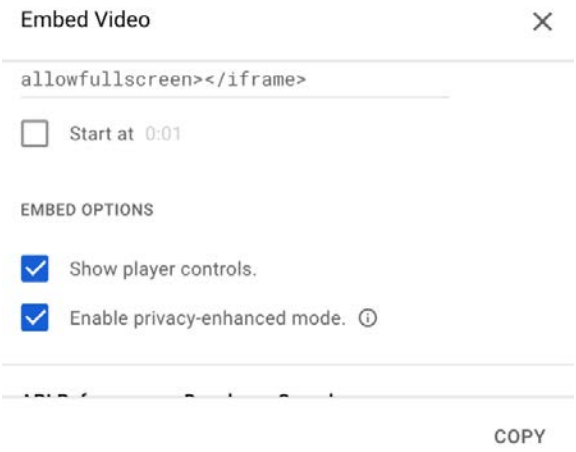
Bij direct gebruik van de Aanvullende dienst YouTube ontvangt Google privacygevoelige tracking data. Het is aan te bevelen YouTube video's in embedded mode te gebruiken. In embedded mode worden er geen tracking cookies gebruikt. SURF en SIVON zijn verder in gesprek met Google over verdere privacyverbeteringen rondom YouTube.

Onder elke YouTube video staat een share button

Klik hierop om op het volgende scherm te komen en selecteer “embed”



Vervolgens is het mogelijk een stukje code te kopiëren met enable privacy-enhanced mode.



Deze code kunt u vervolgens publiceren op een website zoals Google sites. Vanaf daar kunt u nu direct de YouTube video afspelen.

Gebruik geen Chrome browser

Er komt een nieuwe versie van Chrome browser beschikbaar waarbij Google als data verwerker optreedt in plaats van data controller. Tot die versie beschikbaar is adviseren we om een andere browser te gebruiken. Dit advies geld voor PC's die geen Chrome OS gebruiken (Windows, Mac, Linux). Alternatieve browsers zijn bijvoorbeeld Mozilla Firefox of Safari.

Gebruik Google niet als zoekmachine

In plaats van Google search adviseren we het gebruik van een privacyvriendelijk alternatief zoals DuckDuckGo of Startpage.

Gebruik een advertentie- en/of tracking blocker

Overweeg het gebruik van een advertentie- en/of tracking blocker. Advertenties op website gebruiken tracking om browse gedrag te volgen.

Een adblocker (zoals uBlock Origin of Adblock plus) of tracking blockers (zoals Ghostery of Privacy Badger) kunnen als extensie in de browser geïnstalleerd worden.

Gebruik geen privacygevoelige informatie in file en folder namen

Gebruik geen namen van personen of andere privacygevoelige informatie in bestandsnamen of folders.

Colofon

Technische handleiding voor Google Workspace for Education

Datum van uitgave
2 augustus 2021

Auteurs
Hans-Peter Ligthart (Kennisnet), Job Vos (SIVON), Theresa Song Loong (Kennisnet)

Redactie
Juwan Mizouri

Over Kennisnet

Goed onderwijs legt de basis voor leven, leren en werken en daagt leerlingen en studenten uit om het beste uit zichzelf te halen. Dat vraagt om onderwijs dat inspeelt op sociale, economische en technologische ontwikkelingen. Kennisnet ondersteunt besturen in het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo) bij een professionele inzet van ict en is voor scholen de gids en bouwer van het ict-fundament.

Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

Deze publicatie is tot stand gekomen in samenwerking met SURF en SIVON. SIVON en Kennisnet bevorderen samenwerking tussen onderwijsinstellingen op het gebied van ict-infrastructuur, leermiddelen en leeromgevingen en informatiebeveiliging en privacy (IBP).

kennisnet.nl