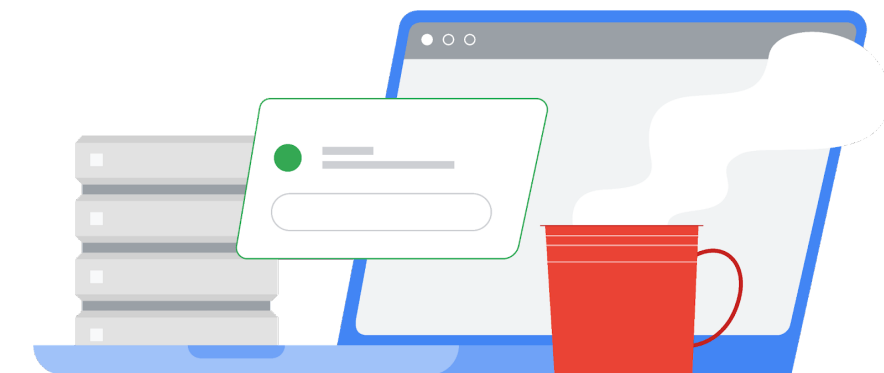


Google for Education

ChromeOS

Handleiding met best practices voor inventariscontrole

Februari 2023

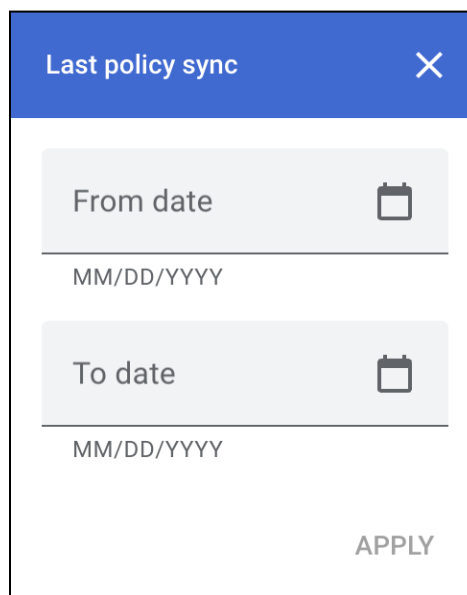


Inhoudsopgave

Apparaten zoeken waarop beleid al een tijdje niet is gesynchroniseerd	2
Op de hoogte blijven als gebruikers hun apparaat herhaaldelijk opnieuw inschrijven	4
Als je Workspace for Education Plus of Standard gebruikt	4
Apparaten onderzoeken	4
Een activiteitsregel maken voor apparaten die opnieuw worden ingeschreven	5
Als je Workspace for Education Fundamentals gebruikt	5
Controlelogboeken filteren	5
Voorkomen dat gebruikers ongeautoriseerde apparaten inschrijven	6
Checken of gebruikers inloggen op niet-ingeschreven apparaten	7
Onbeheerde apparaten in kaart brengen die verbinding hebben met een beheerd netwerk	7
Aanbevolen instellingen	8

Apparaten zoeken waarop beleid al een tijdje niet is gesynchroniseerd

Ga in de Beheerdersconsole naar Apparaten > Chrome > Apparaten om een [rapport van alle apparaten](#) te krijgen, gesorteerd op laatste keer gesynchroniseerd. Je kunt een filter toevoegen aan de lijst om apparaten te krijgen die binnen een bepaalde periode zijn gesynchroniseerd. Een beheerder kan bijvoorbeeld een filter instellen voor Laatste beleidssynchronisatie met bij Begindatum 01-01-2022 en bij Einddatum 13-01-2023 om alleen apparaten te krijgen waarop beleid tussen 13 januari 2023 of daarvoor, tot eerder vorig jaar, niet is gesynchroniseerd.



The image shows a modal dialog box titled "Last policy sync" with a close button (X) in the top right corner. Inside the dialog, there are two date selection fields. The first field is labeled "From date" and has a calendar icon to its right; below it is the placeholder text "MM/DD/YYYY". The second field is labeled "To date" and also has a calendar icon to its right; below it is the placeholder text "MM/DD/YYYY". At the bottom right of the dialog is an "APPLY" button.

Je kunt de kolommen voor deze lijst met apparaten bewerken om de kolom Meest recente gebruiker toe te voegen. Dit is de laatste persoon die het apparaat heeft gebruikt (in het veld Gebruiker staat de gebruiker die het apparaat heeft ingeschreven, dit is niet altijd de primaire gebruiker van het apparaat). Als je wilt bewerken welke kolommen er worden getoond, klik je op het tandwiel. Klik onderaan op *Nieuwe kolom toevoegen* en selecteer Meest recente gebruiker. Je kunt ook kolommen verwijderen door op de X te klikken. Klik als je klaar bent op OPSLAAN.

Manage columns	
Device list	
Serial number	
Status	×
Asset ID	×
Organizational unit (not currently visible)	×
Online status (not currently visible)	×
Enrollment time	×
Last policy sync	×
Location	×
Most recent user	×
 Last user activity	×
<i>Add new column</i>	▼
CANCEL SAVE	

Beheerders kunnen automatisch [een rapport krijgen met inactieve bedrijfsapparaten](#) waarop beleid in de afgelopen 30 dagen niet is gesynchroniseerd.

Op de hoogte blijven als gebruikers hun apparaat herhaaldelijk opnieuw inschrijven

Als gebruikers hun apparaat herhaaldelijk uitschrijven en opnieuw inschrijven, kan dit worden vastgelegd in de controlelogboeken waarin de beheerder dit kan checken. Als je Google Workspace for Education Plus of Standard gebruikt, kun je instellen dat herhaaldelijk opnieuw inschrijven automatische meldingen of acties triggert.

Als je Workspace for Education Plus of Standard gebruikt

Apparaten onderzoeken

Ga voor meer informatie over het gebruik van de onderzoekstool naar [Tool voor beveiligingsonderzoek](#).

- Ga naar Rapporten → Onderzoek → Gebeurtenissen in het beheerderslogboek.
- Klik op **Voorwaardenbuilder**.
- Voeg een voorwaarde toe. Kies bij Gebeurtenis de opties Is en Apparaatstatus gewijzigd.
- Voeg een voorwaarde toe. Kies bij Nieuwe waarde de opties Bevat en ACTIEF.
- Klik op **Resultaten groeperen op** en selecteer Groeperen op bron-ID('s).

Search 1 Create activity rule Create custom chart Discard search

Admin log events Filter Condition builder

AND

Event Is Change Device State <> X

New value Contains New value ACTIVE <> X

ADD CONDITION

Group results by Resource ID(s) X

SEARCH

- Klik op **Zoeken**.

Als bepaalde apparaten herhaaldelijk opnieuw worden ingeschreven, kan dit betekenen dat gebruikers dit met opzet doen.

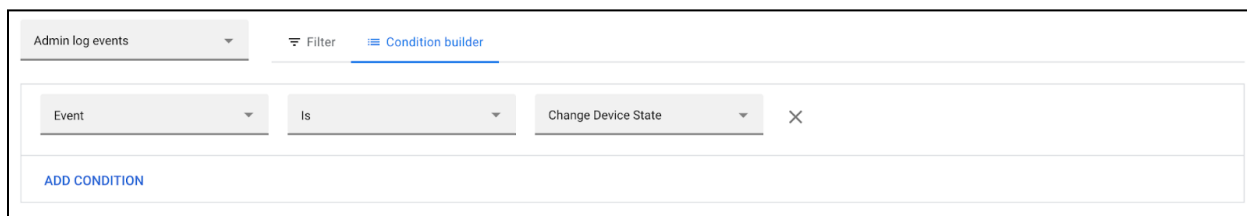
Een activiteitsregel maken voor apparaten die opnieuw worden ingeschreven

Optioneel: Klik bovenaan op Activiteitsregel maken om deze zoekopdracht op te slaan als regel en automatisch meldingen te sturen. We raden je af gebruikers die apparaten opnieuw inschrijven op te schorten, vanwege de kans op vals positieven. Ga voor meer informatie over hoe je activiteitsregels maakt naar [Activiteitsregels maken en beheren](#).

Als je Workspace for Education Fundamentals gebruikt

Controlelogboeken filteren

- Ga naar Rapporten → Onderzoek → [Gebeurtenissen in het beheerderslogboek](#).
- Klik op **Voorwaardenbuilder**.
- Voeg een voorwaarde toe. Kies bij Gebeurtenis de opties Is en Apparaatstatus gewijzigd.



- Klik op **Zoeken**.

De kolommen Bron-ID's en Beschrijving worden standaard getoond.

Klik op **Alles exporteren** om de resultaten te exporteren naar een Google-spreadsheet. Voer een naam in voor de export en klik op **Exporteren**.

Als de export klaar is, scroll je naar Actieresultaten exporteren en klik je op de naam van de export om de Google-spreadsheet te openen.

Je kunt apparaten die herhaaldelijk opnieuw worden ingeschreven herkennen door een kolom toe te voegen en de tekst ACTIVE to ACTIVE (ACTIEF naar ACTIEF) te zoeken in de beschrijving. Hieronder staat een voorbeeldformule, waarbij C het veld Description (Beschrijving) is: Stel deze formule in cel E1 van het blad in:

```
=Arrayformula(if(row(C:C)=1,"Reenrolled",REGEXMATCH(C:C,"ACTIVE to ACTIVE")))
```

[Voeg een draaitabel in](#) met de kolomkop Resource IDs (Bron-ID's) als de rijen, de kolomkop Reenrolled (Opnieuw ingeschreven) als de kolommen en het aantal van een ander veld, zoals de kolomkop Actor (Handelende gebruiker) als de waarde.

Voorkomen dat gebruikers ongeautoriseerde apparaten inschrijven

Sommige organisaties staan gebruikers toe apparaten in te schrijven of opnieuw in te schrijven. Gebruikers kunnen dan apparaten opnieuw inschrijven als ze op school of op het werk zijn en ze uitschrijven als ze buiten het organisatienetwerk zijn. Beheerders kunnen dit recht uitzetten voor gebruikers als ze niet willen dat gebruikers makkelijk zelf apparaten opnieuw kunnen inschrijven, en het aanzetten als ze willen dat gebruikers dit wel kunnen.

Als je deze instelling wilt aanzetten, ga je in de Beheerdersconsole naar Apparaten > Chrome > Instellingen > [Gebruikers en browser](#). Selecteer in de linkerkolom de juiste OE (zoals Leerlingen). Als je niet wilt dat gebruikers apparaten kunnen inschrijven, selecteer je bij Inschrijfrechten, onder Inschrijvingsfuncties, de optie Gebruikers in deze organisatie-eenheid niet toestaan nieuwe of bestaande apparaten in te schrijven of opnieuw in te schrijven. Als je wilt dat gebruikers bestaande apparaten wel opnieuw kunnen inschrijven, selecteer je Gebruikers in deze organisatie alleen toestaan bestaande apparaten opnieuw in te schrijven (en niet om nieuwe of uitgeschreven apparaten in te schrijven).

Checken of gebruikers inloggen op niet-ingeschreven apparaten

Je kunt het docenten of medewerkers makkelijk maken onbeheerde apparaten te herkennen door een visuele beleidsinstelling voor apparaten te wijzigen. Deze wijziging wordt alleen toegepast op apparaten die op dat moment worden beheerd. De wijziging wordt niet getoond op apparaten die niet worden beheerd.

Beheerders kunnen instellen dat apparaten [altijd systeemgegevens tonen](#) op het inlogscherf. Op onbeheerde apparaten staan niet de woorden Beheerd door, of de systeemgegevens. Je kunt ook de [inlogachtergrond](#) wijzigen in een beveiligde afbeelding.

In [de apparaatlijstconsole](#) kunnen beheerders checken of beleid is gesynchroniseerd voor recente gebruikers. Door de lijst met verwachte gebruikers te vergelijken met

gebruikers voor wie het beleid recent is gesynchroniseerd, krijg je een lijst met gebruikers van wie de apparaten mogelijk niet zijn gesynchroniseerd. Je kunt deze apparaten extra controleren, bijvoorbeeld door fysiek te checken of ze zijn ingeschreven.

Onbeheerde apparaten in kaart brengen die verbinding hebben met een beheerd netwerk

Je kunt mogelijk snel onbeheerde Chromebooks herkennen die beheerd zouden moeten zijn als ze verbinding maken met je wifi-netwerk. Met de beleidsregel [DeviceHostnameTemplate](#) kunnen beheerders een indeling voor de hostnaam instellen waardoor deze het serienummer en of de itemtag-ID van een apparaat bevat. Deze hostnaam wordt getoond in de DHCP-tabellen van het netwerk. Als een apparaat met een bekend MAC-adres verbinding maakt met het beheerde netwerk zonder de juiste hostnaam, is het waarschijnlijk een niet-ingeschreven apparaat.

Voorbeeld: Ga in de Beheerdersconsole naar Apparaten > Chrome > Instellingen > Apparaat. Scroll onder Andere instellingen naar Template voor hostnaam van apparaat in netwerk. Pas op beheerde Chromebooks het volgende beleid toe voor de template van de hostnaam in het netwerk: BeheerdeChromebook-`-${SERIAL_NUM}`. Deze worden getoond in de DHCP-groep van het netwerk van een school met deze hostnaam die makkelijk te herkennen is. Voor alle andere apparaten op die SSID of dat netwerk staat er een algemene of niet-opgegeven hostnaam. Als je de MAC-adressen van deze algemene of niet-opgegeven hostnamen exporteert en vergelijkt met een export van de bekende MAC-adressen van een Workspace-tenant, kun je achterhalen welke apparaten niet zijn ingeschreven.

Als je een lijst van apparaten met hun wifi-MAC-adressen wilt exporteren, ga je in de Beheerdersconsole naar Apparaten > Chrome > Apparaten. Selecteer de juiste OE en klik boven de lijst op Exporteren. Het exportproces wordt getoond in de takenlijst. Deze kun je openen door rechtsboven op het zandloperpict te klikken. Als de export klaar is, kun je het csv-bestand downloaden om de resultaten te checken. In de kolom `macAddress` staat het wifi-MAC-adres (zonder dubbele punten).

De beheerder kan dan verschillende acties uitvoeren op deze apparaten, zoals de apparaten/gebruikers vinden, instellen dat deze MAC-adressen helemaal geen verbinding meer kunnen maken met het netwerk of de apparaten toevoegen aan een VLAN met beperkte toegang. Met een contentfilter of captive-portalsysteem kunnen netwerkbeheerders die apparaten omleiden naar een pagina met instructies om contact

op te nemen met IT voor support of om het apparaat opnieuw in te schrijven (als de beheerder dit toestaat).

Aanbevolen instellingen

- [Afgedwongen opnieuw inschrijven](#): Stel dit in op Apparaat afgedwongen automatisch opnieuw inschrijven na wissen. [Supportartikel over afgedwongen opnieuw inschrijven](#)
- [Powerwash](#): Stel dit in op Niet toestaan dat powerwash wordt getriggerd, voor alle gebruikers met uitzondering van specifieke gebruikers [Supportartikel over powerwash](#)
- [Geverifieerde modus](#): Stel dit in op Opstarten via geverifieerde modus vereisen voor geverifieerde toegang. [Supportartikel over geverifieerde modus](#)
- [Geverifieerde toegang](#): Stel dit in op Aanzetten voor inhoudbescherming. [Supportartikel over geverifieerde toegang](#)
- [Rechten voor apparaten opnieuw inschrijven](#): Selecteer specifieke OE's met gebruikers voor wie je dit wilt toestaan. [Supportartikel over inschrijfrechten](#)
- [Blokkeer de toegang](#) tot de volgende interne URL's:

```
chrome://policy  
chrome://net-export  
chrome://prefs-internals  
chrome://version  
chrome://kill  
chrome://hang
```