Extensies beheren in je bedrijf

Chrome-extensies beveiligd op schaal beheren

Inhoudsopgave

Doel van deze gids

Er worden veel nuttige extensies gemaakt voor de Chrome-browser. De kans is groot dat veel extensies zijn geïnstalleerd op de computers van je gebruikers. Hierdoor kan het lastig voor IT-beheerders zijn om extensies te beheren en te monitoren.

Deze gids is bedoeld voor IT-beheerders die op zoek zijn naar de beste manieren om extensies te beheren. De gids bevat stappen voor extensiebeheer via zowel Cloudbeheer voor de Chrome-browser als Windows-groepsbeleid.

Deze gids is geordend op de manieren waarop je extensies kunt beheren. Je kunt het volgende doen:

1. Extensies blokkeren op basis van rechten.
2. Beheren tot welke websites extensies toegang hebben.
3. Extensies toestaan of blokkeren via Cloudbeheer voor de Chrome-browser of Windows-groepsbeleid.
4. Je eigen extensies op locatie hosten.

De behandelde onderwerpen	Instructies en aanbevelingen voor het beheer van extensies voor de Chrome-browser in je onderneming
Primaire doelgroep	Beheerders van Microsoft® Windows® en Cloudbeheer voor de Chrome-browser (Windows, Mac en Linux ondersteund)
Conclusies	Praktische tips voor het beheer van extensies met de Chrome-browser

Laatst geüpdatet: *29 oktober 2021*

Publicatielocatie: *https://support.google.com/chrome/a/answer/9296680*

Inleiding

Bedrijven willen hun gebruikersgegevens beschermen. Ze willen extensies makkelijk kunnen checken op het gebied van veiligheid en relevantie voor gebruikers. IT-beheerders moeten het volgende doen:

1. Voorkomen dat slechte extensies worden geïnstalleerd.
2. Extensies behouden die gebruikers nodig hebben.
3. Beperkte toegang verlenen tot gebruikers- en bedrijfsgegevens.

Het doel van deze gids is om je te laten zien hoe je extensies makkelijk kunt beheren. Er zijn meerdere methoden om extensies te beheren. Deze gids toont je de opties en helpt je bij het kiezen van de juiste methode voor jou.

Overwegingen voor het beheer van Chrome-extensies

Je gebruikers hebben toegang nodig tot bepaalde apps, sites en extensies om hun werk te kunnen doen. Als IT-beheerder moet je de gebruikers- en bedrijfsgegevens beschermen. Je hebt een strategie nodig om een methode te kiezen voor beheer van extensies.

Belangrijke vragen om jezelf te stellen:

- Welke voorschriften en nalevingsmaatregelen moet ik volgen?
- Welke vorm van apparaat- of websitetoegang zou in strijd zijn met het beveiligingsbeleid van mijn bedrijf?
- Hoeveel gebruikers- of bedrijfsgegevens zijn er opgeslagen op de apparaten van mijn gebruikers?

Terwijl je hierover nadenkt, biedt Google je beleidsregels waarmee je het volgende kunt doen:

- Extensies blokkeren of toestaan op basis van je beleid inzake gegevensbescherming.
- Vereiste extensies afgedwongen installeren op apparaten van je gebruikers.
- Extensies beheren terwijl je ze de minimaal vereiste rechten verleent om te werken.

De traditionele beheermethode is specifieke extensies toestaan of blokkeren. Er is echter een makkelijkere optie. Je kunt beheren op basis van de rechten die nodig zijn voor extensies. Doe onderzoek naar de rechten die je wilt toestaan. Dwing daarna beleidsregels af waarmee extensies die aan je vereisten voldoen, worden toegestaan of geblokkeerd.

Wat zijn extensierechten?

Voor extensies kunnen rechten zijn vereist om wijzigingen aan te brengen op een apparaat of webpagina zodat de extensie naar behoren werkt. Dit noemen we extensierechten. Ontwikkelaars moeten vermelden welke rechten en toegangstypen hun extensies vereisen. Er zijn 2 primaire categorieën, maar op veel extensies zijn beide van toepassing:

- Siterechten waarmee om toegang wordt gevraagd tot de websites die je gebruikers bezoeken.
  Voorbeelden: Een webpagina wijzigen, toegang tot cookies, tabbladen wijzigen
- Apparaatrechten waarmee om toegang wordt gevraagd tot het apparaat waarop de browser actief is.
  Voorbeelden: Toegang tot USB-poort/opslag/weergegeven scherm

Hoe worden extensies geüpdatet?

Extensies worden alleen geüpdatet als Chrome actief is en de update in de eerste minuten na het openen van Chrome plaatsvindt. Daarna wordt er elke 5 uur gecheckt op updates.

- Extensies worden als volgt geüpdatet:
  a. Chrome stuurt een verzoek met een lijst van geïnstalleerde extensies en versies naar een Google-server.
  b. Onze servers reageren met een set instructies voor welke extensies moeten worden geüpdatet.
  c. Chrome vraagt nu om de CRX-bestanden voor elk van de verouderde extensies en past de update lokaal toe.
- Hoe extensies verouderd kunnen raken:
  a. Vanwege de aanzienlijke downloadgrootte van updates of als de gebruikers veel extensies hebben, kan het voorkomen dat de update niet wordt voltooid tijdens een korte gebruikerssessie.
  b. Chrome wordt niet geopend.
  c. Ontwikkelaars van extensies hebben ervoor gekozen het aantal clients te beperken waarvoor ze de update beschikbaar stellen.
  d. Als een organisatie een extensie zelf host, kan dit komen door een toegangsprobleem of configuratiefout.
  e. Andere problemen die kunnen worden toegeschreven aan fouten in de ontwikkeling van de extensie.

Eén oplossing voor verouderde extensies is een extensie verwijderen en weer installeren. Je kunt een extensie-update ook handmatig afdwingen via chrome://extension > zet de ontwikkelaarsmodus aan > klik op de knop Updaten.

Extensies beheren

De meeste organisaties moeten extensies beheren op basis van de rechten en tot welke websites ze toegang hebben. Deze methode is beter beveiligd, makkelijker te beheren en schaalbaar.

Je bespaart tijd doordat je de beleidsregels maar 1 keer hoeft in te stellen. Je hoeft niet meer lange blokkerings- en toelatingslijsten te beheren. Wel kun je nog steeds gebruikmaken van een korte lijst met extensies die niet moeten worden geïnstalleerd. Bovendien worden je belangrijkste websites beschermd door de beleidsregels voor runtime hosts. Extensies in je organisatie beheren volgens deze methode:

1. Bepaal welke extensies zijn geïnstalleerd op de computer van je gebruikers.
   - **Methode 1 (aanbevolen):** Gebruik Cloudbeheer voor de Chrome-browser. Deze functie wordt kosteloos aan je gebruikers aangeboden. Hiermee kun je het volgende zien van de extensies:

    - Geïnstalleerde versie, aantal installaties en of ze door gebruikers of beheerders zijn geïnstalleerd.
    - Vereiste rechten.
    - Status (actief of uitgezet).
- De stappen om Chrome Browser Cloud Management in te stellen vind je hier.
- Als de console is ingesteld en je je apparaten hebt ingeschreven met cloudrapportage actief, kun je alle geïnstalleerde extensies bekijken onder **Apparaten > Chrome > Gebruiksrapport voor apps en extensies**
    - Als je op een extensie klikt, zie je meer informatie over de vereiste rechten en voorbeelden van waar de extensie is geïnstalleerd
        - Later (eind 2021 of begin 2022) kun je ook op een extensie klikken om naar een nieuwe pagina met extensiegegevens te gaan (zie hieronder).
        - Hier vind je meer informatie over de extensie, waaronder de vereiste rechten en rechtstreekse informatie van de vermelding in de Chrome Web Store
        - Raadpleeg deze YouTube-video voor meer informatie over het beheer van extensies in Cloudbeheer voor de Chrome-browser.
    - Je kunt ook gebruikmaken van de Takeout-API van Cloudbeheer voor de Chrome-browser om alle extensiegegevens van ingeschreven browsers in een CSV-bestand te exporteren.
        - Meer informatie: Stapsgewijze handleiding | Blogpost | Demo Video
- **Methode 2:** Enquête**:** Vraag je collega's en hun managers welke extensies ze vaak gebruiken. Maak een lijst van de extensies die gebruikers nodig hebben.

2. Bepaal welke sites beveiligd moeten zijn:
    - Ga na op welke gevoelige websites en domeinen extensies geen wijzigingen mogen aanbrengen of gegevens mogen lezen.
        - Blokkeer de toegang tot deze sites door de API-aanroepen te blokkeren als de extensie wordt uitgevoerd. Dit omvat blokkeringen van webverzoeken, lezen van cookies, JavaScript-injectie, XHR, etc.

3. Bepaal welke rechten een risico kunnen vormen voor je gebruikers:
    - Check de lijst met extensies die je in stap 1 hebt gemaakt. Check de geïnstalleerde extensies en welke rechten ze vereisen.
        - **Toptip:** De door extensies gebruikte rechten kunnen vaag zijn. Neem voor vereiste extensies contact op met de leverancier voor meer informatie. Deze kan je als het goed is vertellen wat voor wijzigingen de extensie kan aanbrengen op apparaten en websites.
    - Bekijk de lijst Declare Permissions (Rechten definiëren). Hier vind je alle rechten die een extensie kan gebruiken. Bepaal dan welke rechten je wilt toestaan in je organisatie.

        - Raadpleeg voor meer informatie over de risico's van specifieke extensierechten dit document over de risico's van rechten.
4. Maak een lijst op basis van de verzamelde gegevens, waaronder:
    - **Vereiste extensies:** Deze lijst kun je onderverdelen op afdeling, kantoorlocatie of andere relevante gegevens.
    - **Toelatingslijst:** Vereiste extensies met rechten die zouden worden geblokkeerd, maar die moeten worden uitgevoerd. Mogelijke voorbeelden zijn:
        - Extensies de je gebruikers nodig hebben.
        - Extensies waarvan je op basis van gesprekken met de leverancier hebt bepaald dat deze geen risico vormen.
    - **Blokkeringslijst:**

        - Extensies die niet kunnen worden geïnstalleerd.

            - Deze lijst omvat de rechten die niet mogen worden uitgevoerd.

        - Vermeld de websites en domeinen die moeten worden beveiligd en niet toegankelijk zijn voor extensies.

            - Vergelijk deze lijst met je huidige blokkeringslijsten. Misschien kun je je huidige blokkeringslijstbeleid versoepelen.

5. Dien je lijst in bij je stakeholders en IT-team ter goedkeuring.
6. Test het nieuwe beleid in je lab of via een kleine pilot binnen je organisatie.
7. Rol deze nieuwe beleidssets in fasen uit voor je medewerkers.
8. Beoordeel de feedback van je gebruikers.
9. Herhaal en verfijn het proces maandelijks, per kwartaal of jaarlijks.

Zo creëer je een basis voor de rechten die je toestaat of blokkeert. Gevoelige websites worden beschermd. Je verhoogt de beveiliging van je browser en helpt gebruikers met een betere functionaliteit. Medewerkers kunnen misschien nu extensies installeren die eerder niet mogelijk waren. Deze werken simpelweg niet op gevoelige websites, tenzij je dit toestaat. Raadpleeg de volgende gedeelten in de handleiding voor informatie over hoe je deze methode instelt:

- Beheer van extensies door rechten te blokkeren/toe te staan
- Runtime hosts voor blokkering (ter bescherming van gevoelige websites)
- Extensies afgedwongen installeren voor je gebruikers
- Extensies toestaan/blokkeren (indien vereist)

Bekijk deze YouTube-video over beheer van extensies in de Beheerdersconsole voor een overzicht van beheer van extensies binnen Cloudbeheer voor de Chrome-browser.

Overzicht van de verschillende beleidsregels voor beheer van extensies

Veel van deze beleidsregels worden uitgebreid behandeld in de andere gedeelten van het document, maar hier is een overzicht van enkele van de huidige opties voor beheer van extensies (sommige zijn ook van toepassing op apps) via Windows-groepsbeleid of Plists voor Mac.

- Toelatingslijst met extensies die mogen worden geïnstalleerd: Dit zijn de extensies die je hebt goedgekeurd voor installatie in je omgeving.
- Blokkeringslijst met extensies die niet mogen worden geïnstalleerd: Dit zijn de extensies die niet mogen worden geïnstalleerd. Als ze al zijn geïnstalleerd, worden ze uitgezet. Pogingen om ze te installeren worden geblokkeerd. Daarnaast heeft de Chrome Web Store een nieuwe functie waarbij de knop 'Toevoegen aan Chrome' rood is als de extensie niet mag worden geïnstalleerd. Ook krijgt de gebruiker een melding met deze informatie.
- Lijst met extensies die afgedwongen worden geïnstalleerd: De extensies op deze lijst worden op de achtergrond geïnstalleerd op het apparaat van je gebruiker. De gebruiker kan deze extensie niet uitzetten of verwijderen. Deze instelling overschrijft het beleid van de blokkeringslijst voor extensies.
- Externe extensies blokkeren: Met deze instelling kunnen er geen extensies van externe bronnen worden geïnstalleerd. Als een geïnstalleerde app bijvoorbeeld een extensie aan Chrome wil toevoegen via het register, voorkomt deze instelling dat de extensie wordt geladen.
- Toegestane extensietypen: Hier kun je een lijst maken van de typen extensies en apps die kunnen worden geïnstalleerd. Ondersteunde waarden zijn extensies, thema's, gebruikersscripts, gehoste apps, ingepakte verouderde apps en platform-apps.
    - Alles wat je wilt toestaan, moet in de lijst staan. Als het niet op de lijst staat, wordt het niet geïnstalleerd.
    - Volg voor meer informatie over de verschillende typen deze link over extensies en apps in de Chrome Web Store.
- Installatiebronnen van extensies: Eerder konden gebruikers klikken op een link naar een crx-bestand, waarna Chrome de extensie na enkele waarschuwingen zou installeren. Deze functie is vanwege veiligheidsoverwegingen na Chrome 21 verwijderd.
    - Met dit beleid kun je deze oude functie voor installaties gebruiken voor de URL's die je hier opgeeft. Volg deze link voor de URL-overeenkomstpatronen die voor dit beleid kunnen worden gebruikt.

- Extensie-instellingen: Dit beleid biedt verschillende functies. Er moet een json-script voor worden gemaakt en het beleid moet uit een tekenreeks van een enkele regel bestaan.
    - Deze instelling kan complex zijn en wordt in meerdere gedeelten van dit document uitgebreid behandeld.
        - Het wordt aanbevolen om Cloudbeheer voor de Chrome-browser te overwegen, omdat dat bijna alle functies bevat zonder dat je json hoeft te schrijven. Ook kun je geïnstalleerde extensies checken.

Een opmerking van Google over zijn toewijding aan inclusieve naamgevingsconventies. De volgende beleidsregels zijn beëindigd en worden in Chrome 97 verwijderd. Zorg dus dat je tegen die tijd bent overgestapt op het nieuwe beleid.

- ExtensionInstallWhitelist vervangen door ExtensionInstallAllowlist
- ExtensionInstallBlacklist vervangen door ExtensionInstallBlocklist

Extensies blokkeren op basis van rechten

Je kunt op basis van rechten bepalen welke extensies je gebruikers kunnen installeren. Een al geïnstalleerde extensie met geblokkeerde rechten wordt uitgezet. Pogingen om een extensie met een geblokkeerd recht te installeren, worden geblokkeerd.

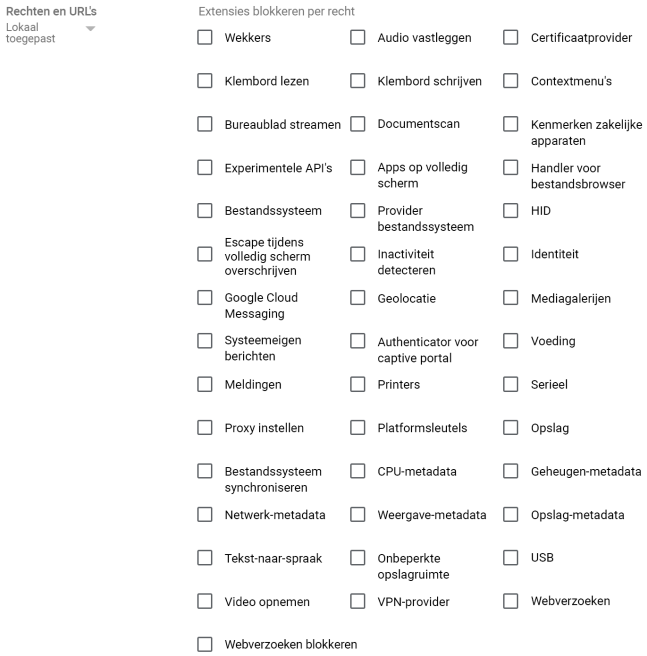
Extensies beheren op basis van rechten in Cloudbeheer voor de Chrome-browser

(Windows, Mac en Linux)

Je kunt extensies blokkeren die niet-toegestane rechten vereisen. Zo kun je voorkomen dat extensies verbinding maken met USB-apparaten of toegang hebben tot cookies.

1. Ga in de Beheerdersconsole naar **Apparaten > Chrome >Apps en extensies > Gebruikers en browsers**.
2. Selecteer de organisatie-eenheid met de gebruikers voor wie je de extensies wilt toestaan.
3. Klik op het tandwiel voor aanvullende instellingen 

4. Vink in het gedeelte **Rechten en URL's** elk recht aan dat je wilt blokkeren of toestaan.

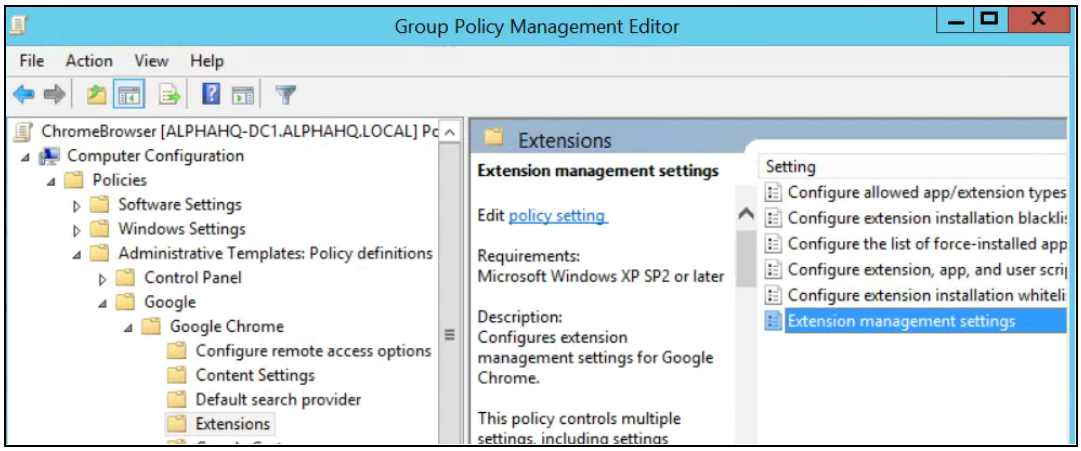


a. Je kunt ook op het tabblad 'Gebruikers en browsers' op een afzonderlijke extensie klikken en deze op basis van rechten beheren onder Rechten en URL-toegang > Rechten aanpassen voor deze app/extensie.
    i. Hierdoor worden alle algemene beleidsregels overschreven die al op deze extensie zijn toegepast.
    ii. Bekijk voor meer informatie over elk recht deze lijst met rechten.
5. Klik op **Opslaan**.

Extensies beheren op basis van rechten in Groepsbeleid

(Alleen voor Windows)

1. Browse naar het Groepsbeleid-object in de Microsoft Management Console.
2. Klik met de rechtermuisknop > klik op **Bewerken**.
3. Browse in de Editor voor groepsbeleidsbeheer naar **Beleid > Beheersjablonen > Google Chrome > Extensies > Extensiebeheerinstellingen**.



Pad voor extensiebeheerinstellingen configureren

4. Zet het beleid aan en vul de rechten die je wilt toestaan of blokkeren in als een enkele json-tekenreeks.

Gebruik de indeling van deze json-voorbeeldgegevens: (In dit voorbeeld worden alle extensies geblokkeerd die USB vereisen.)

```
{
        "*": {
                "blocked_permissions": ["usb"]
        }
}
```

Compacte json-gegevens:

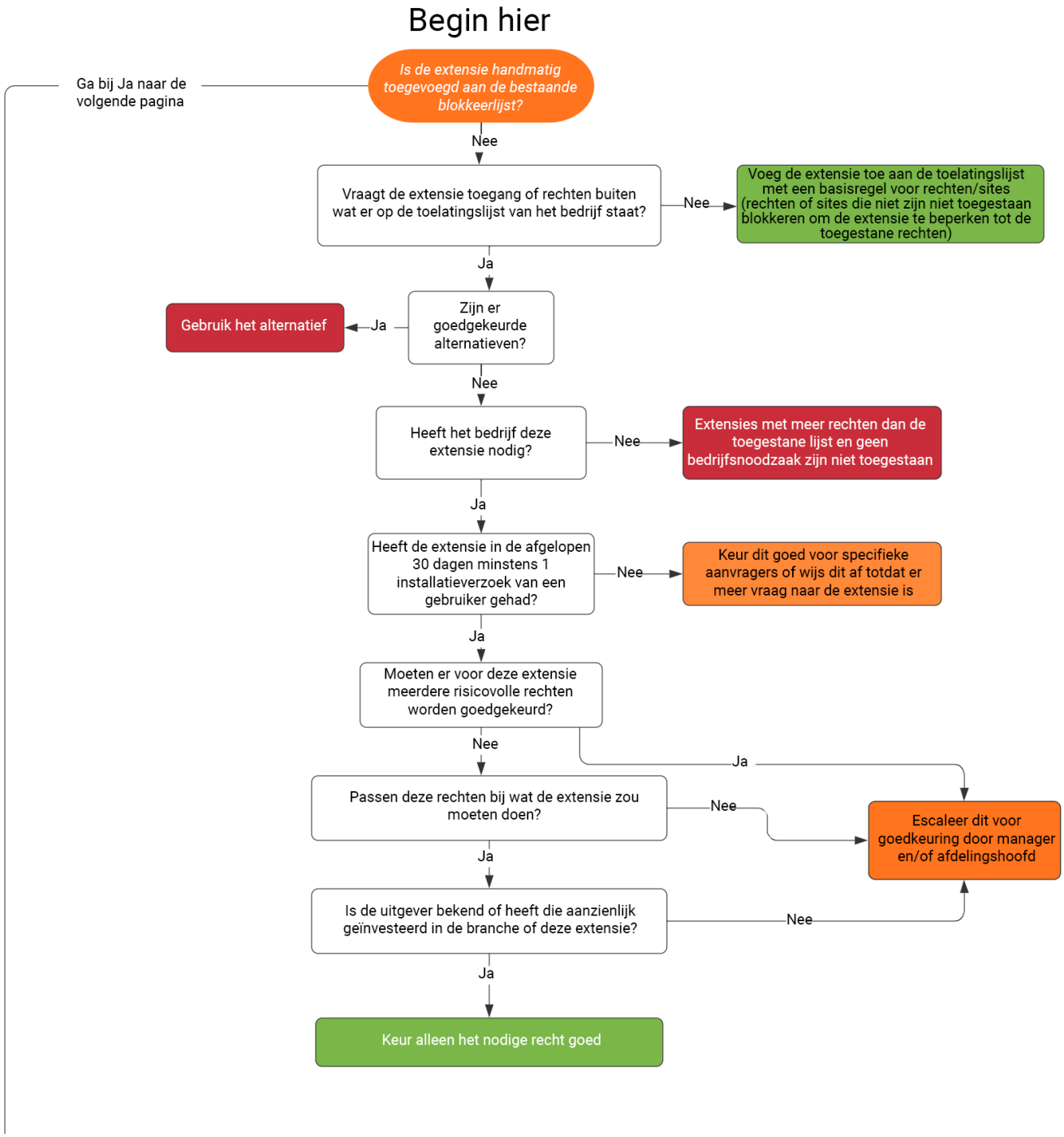
```
{"*":{"blocked_permissions":["usb"]}}
```

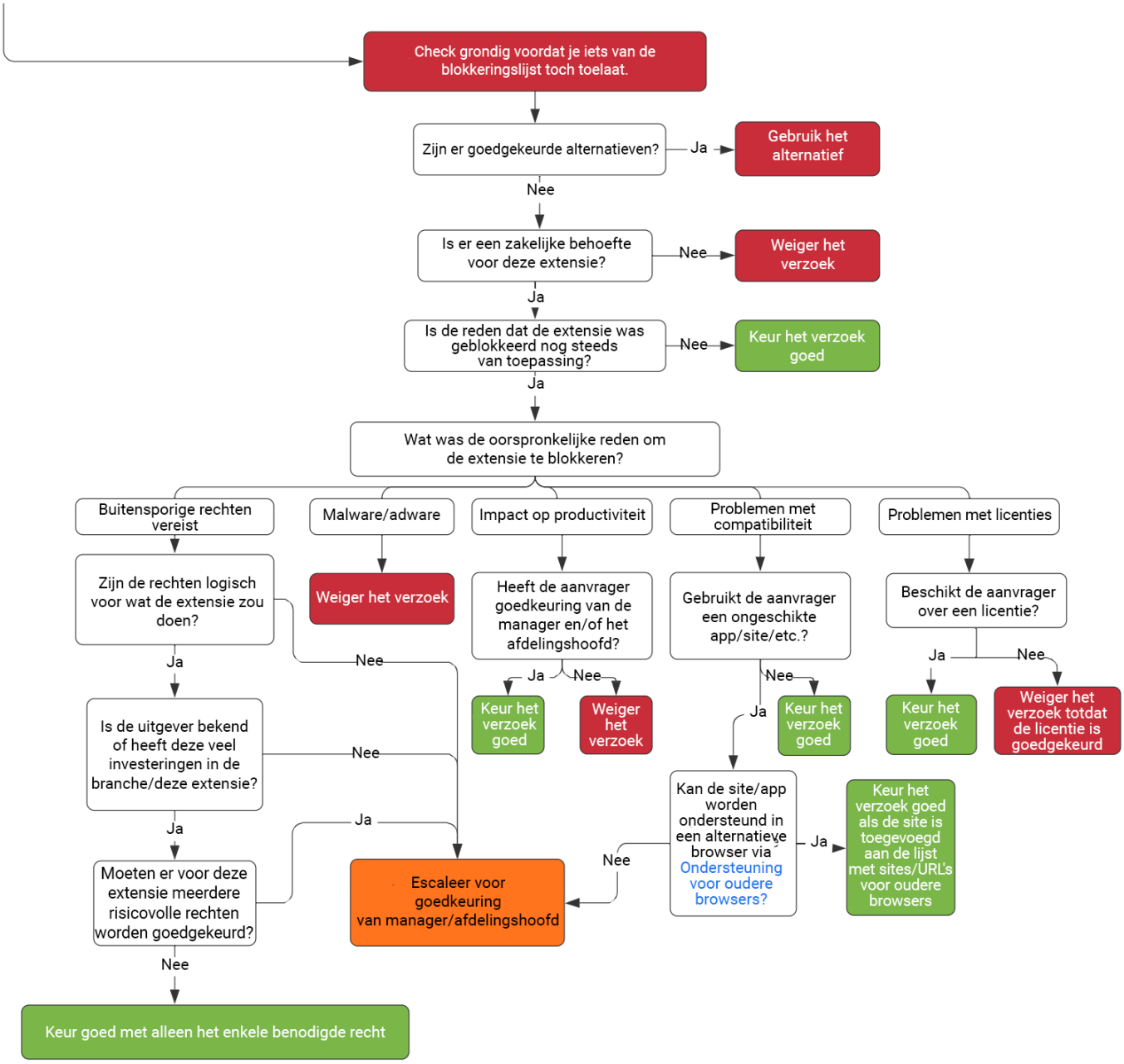
Toptip:

- Als je alle extensies wilt blokkeren die dit recht gebruiken, gebruik je een asterisk (zoals hierboven) voor de extensie-ID.
- Als je meerdere rechten op basis van json wilt blokkeren, zie je hier een voorbeeld waarmee 'power', 'printerProvider', 'serial' en 'usb' voor alle extensies worden geblokkeerd:
    - {"*":{"blocked_permissions":["power","printerProvider","serial","usb"]}}
- Als je 1 extensie-ID opgeeft, is het beleid alleen van toepassing op die extensie. Vervang in het bovenstaande voorbeeld de * door de extensie-ID. Je kunt meerdere blokkeren, maar je moet ze afzonderlijk invoeren in de json-tekenreeks.
    - Zie stap 3 van dit Help-artikel voor meer informatie over hoe je de extensie-ID vindt.

Een uitzondering maken voor extensies die risicovolle rechten vereisen

Mogelijk heeft je bedrijf extensies nodig die rechten vereisen die volgens jou te risicovol zijn om in je omgeving te worden uitgevoerd. Ter illustratie is hier een voorbeeldworkflow voor een gevraagde extensie die een momenteel geblokkeerde extensie vereist.





- Deze workflow is slechts een voorbeeld. Elk bedrijf heeft zijn eigen workflow of verandermanagementprocessen.

Extensies beheren op basis van beleid voor extensie-instellingen

Er zijn meerdere methoden om extensies te beheren in Windows. Gebruikelijk is om meerdere beleidsregels in te stellen met een json-tekenreeks of in het Windows-register met beleid voor extensie-instellingen.
Toptip: Dit beleid wordt ondersteund op Mac, Chrome OS en Linux. Op de beleidspagina vind je voorbeeldwaarden voor deze andere platforms.

Met dit beleid kun je instellingen beheren zoals de update-URL, waarmee de extensie wordt gedownload voor de initiële installatie, en geblokkeerde rechten, die niet mogen worden uitgevoerd. Lees voor meer informatie de volledige beschrijving van extensie-instellingen. In deze Help-artikelen vind je ook meer informatie: ExtensionSettings-beleid instellen en App- en extensiebeleid.

Je kunt bepalen of je alle extensiebeheerinstellingen via dit beleid wilt instellen of via afzonderlijke beleidsregels.

- De instelling voor runtime hosts voor toegestaan/geblokkeerd (waarbij extensies op specifieke websites worden geblokkeerd) kun je alleen instellen via GPO binnen het extensiebeheerbeleid.
    - Je kunt deze ook instellen via Cloudbeheer voor de Chrome-browser.
- Het extensiebeheerbeleid kan andere beleidsregels in groepsbeleid overschrijven, waaronder:
    - ExtensionAllowedTypes
    - ExtensionInstallAllowlist
    - ExtensionInstallForcelist
    - ExtensionInstallSources
    - ExtensionInstallBlocklist

Dit extensiebeheerbeleid kun je op 2 verschillende manieren instellen:

- Windows-register
- Json-tekenreeks in de groepsbeleidseditor van Windows

Toptips:

- Het kan lastig zijn om een json-tekenreeks goed op te stellen. Gebruik een json-checker voor je het beleid implementeert.
- Als het niet lukt de json-tekenreeks goed op te stellen, kun je de registersleutelmethode gebruiken. Chrome converteert deze op het doelapparaat binnen chrome://policy in de browser naar json.
    - Kopieer deze json en pas deze via GPO toe via het extensiebeheerbeleid.
    - Je kunt deze methode ook gebruiken door extensie-instellingen in te stellen via Cloudbeheer voor de Chrome-browser en de json-uitvoer te kopiëren.

Het extensiebeleid configureren via het Windows-register

Het ExtensionSettings-beleid moet naar het register worden geschreven onder:
`HKLM\Software\Policies\Google\Chrome\ExtensionSettings\`

- Je kunt HKCU gebruiken in plaats van HKLM. Het equivalente pad kun je configureren met GPO.
- De sleutels kun je maken zoals je wilt op het apparaat van je gebruiker.

Voor Chrome starten alle instellingen onder deze sleutel:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\`

De volgende sleutel die je maakt, is voor het bereik van het beleid. Geef de sleutel de naam van de extensie-ID om deze op 1 extensie toe te passen. Gebruik een asterisk als naam als je de sleutel op alle extensies wilt toepassen. Gebruik bijvoorbeeld de volgende locatie voor instellingen die alleen van toepassing zijn op de Google Hangouts-extensie:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\nckgahadagoaajjgafhacjanaoiihapd`

Gebruik deze locatie voor instellingen die van toepassing zijn op alle extensies:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*`

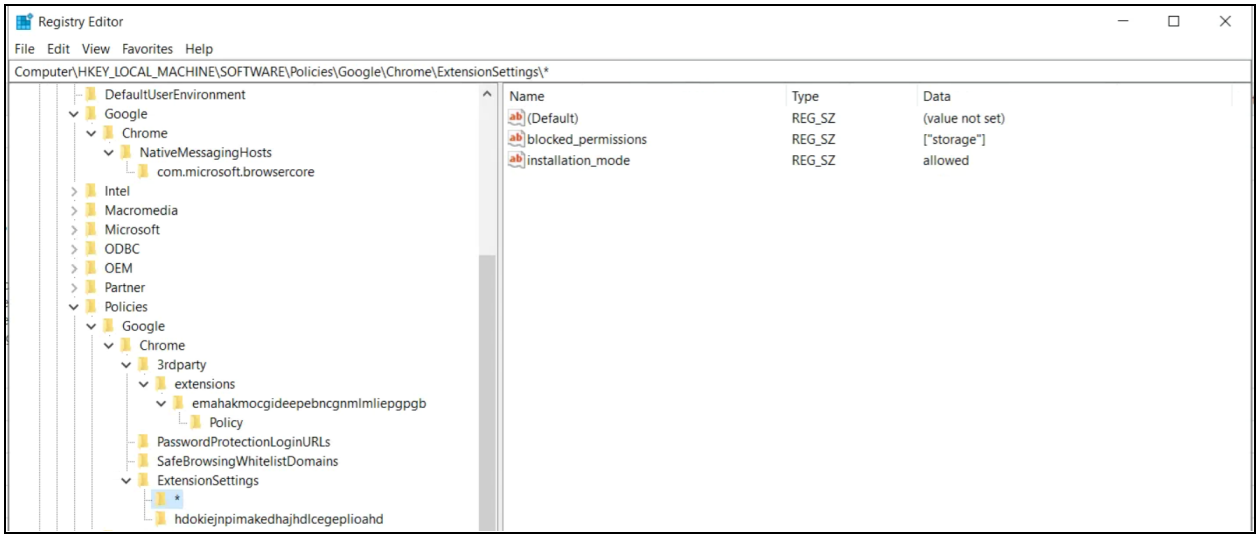
Verschillende instellingen vereisen verschillende indelingen, afhankelijk van of ze uit een tekenreeks of een tekenreeksmatrix bestaan. Matrixwaarden vereisen **`[ " value " ]`**. Tekenreekswaarden kun je invoeren zonder [“ ”]. De lijst van welke instellingen matrices of tekenreeksen zijn:

- Installation_mode = tekenreeks
- update_url = tekenreeks
- blocked_permissions = tekenreeksmatrix
- allowed_permissions = tekenreeksmatrix
- minimum_version_required = tekenreeks
- runtime_blocked_hosts = tekenreeksmatrix
- runtime_allowed_hosts = tekenreeksmatrix
- blocked_install_message = tekenreeks

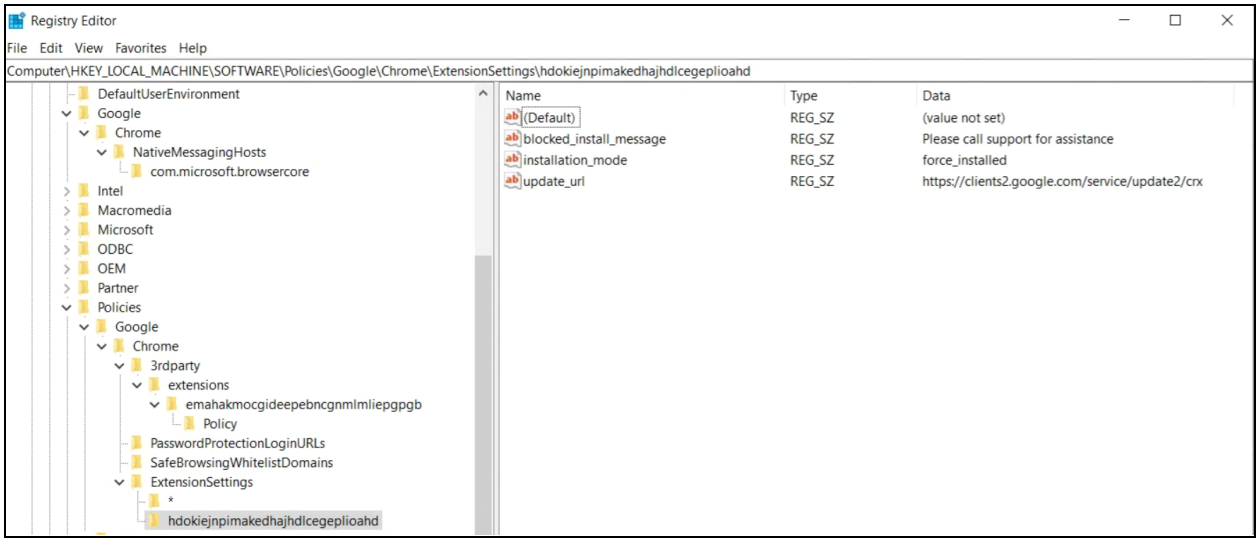
Als je meerdere waarden in een enkele tekenreeks wilt instellen (zoals geblokkeerde rechten), vind je hier een voorbeeld van de syntaxis:

- [“power”,”printerProvider”,”serial”,”usb”]

Voorbeelden van de sleutels binnen het register:



De standaard (*) bereiksleutel en de waarden,



Een afzonderlijk bereik en de waarden.

Hier worden de ingestelde sleutels in het register geconverteerd naar json met het beleid in chrome://policy binnen de browser:

Chrome policies

Geldt voor	Niveau	Bron	Beleidsnaam
Computer	Verplicht	Platform	DefaultBrowserSettingEnabled
Computer	Verplicht	Platform	ExtensionSettings


```
{
  "*": {
  "blocked-permissions": [ "storage" ],
  "installation_mode": "allowed"
  },
  "hdokiejnpimakedhajhdlcegeplioahd": {
  "blocked_install_message": "Please call support for assistance",
   "installation_mode": "force_installed",
  "update_url": "https://clients2.google.com/service/update2/crx"
   }
}
```


Configureren met een json-tekenreeks in de groepsbeleidseditor van Windows

Bij de stappen voor het gebruik van het extensiebeheerbeleid met GPO wordt ervan uitgegaan dat je de ADM/ADMX voor Chrome-beleid al hebt geïmporteerd.

Raadpleeg voor andere OS-platforms het volgende: Mac | Linux | Chrome OS

1. Ga in de GPO-beheereditor naar **Google Chrome > Extensies > Beleid voor extensiebeheerinstellingen**.
2. Zet het beleid aan en vul de compacte JavaScript® Object Notation-gegevens (json) van het beleid in het tekstvak in als een enkele regel zonder regeleinden.
   Gebruik deze json-compressietool van derden om beleid te valideren en het te comprimeren tot 1 regel (hieronder staat een voorbeeld van json-gegevens).

Json goed opstellen voor het extensiebeheerbeleid:
Voor deze methode moet je de 2 onderdelen van dit beleid begrijpen: het **standaard** en het **afzonderlijke** bereik. Het standaardbereik is van toepassing op alle extensies. Het afzonderlijke bereik is alleen van toepassing op de opgegeven extensie.

Het standaardbereik herken je aan de asterisk (*). In dit voorbeeld worden een standaardbereik en een enkel afzonderlijk extensiebereik gedefinieerd.

```
{
   "*": {},
   "nckgahadagoaajjgafhacjanaoiihapd": {}
}
```

Een extensie krijgt instellingen op basis van slechts 1 bereik. Als er een afzonderlijk bereik voor die extensie is, zijn die instellingen van toepassing. Als er geen afzonderlijk extensiebereik is, wordt het standaardbereik gebruikt.
In deze voorbeeld-json kunnen geen extensies worden uitgevoerd op .example.com en worden alle extensies geblokkeerd die het recht 'USB' vereisen.

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.example.com"],
    "blocked_permissions": ["usb"]
  }
}
```

Compacte json-gegevens:
`{"*":{"runtime_blocked_hosts":["*://*.example.com"],"blocked_permissions":["usb"]}}`

Referentievoorbeelden met voorbeeldwaarden voor installatiebeheer van extensies:

- "allowed" (default)
  Je gebruiker kan de extensie installeren via de Chrome Web Store.
  Voorbeeld van json:
  `{ "*": {"installation_mode": "allowed" }}`

- "blocked"
  Je gebruiker kan de extensie niet downloaden via de Chrome Web Store.
  Voorbeeld van json:
  `{ "*": {"installation_mode": "blocked" }}`

- "blocked_install_message"
  Hier kun je een aangepast bericht opgeven dat de gebruiker te zien krijgt bij de blokkering van de installatie.
  Voorbeeld van json - blocked_install_message:
  `{"*": {"blocked_install_message": ["Call IT(408 - 555 - 1234) for an exception"]}}`

- "force_installed"
  - De extensie wordt automatisch geïnstalleerd zonder dat je gebruiker iets doet.
  - De gebruiker kan de extensie niet uitzetten of verwijderen.

  `{ "*": {"installation_mode": "force_installed" }}`

- "normal_installed"
  De extensie wordt automatisch geïnstalleerd zonder dat je gebruiker iets doet, maar deze kan de extensie wel uitzetten.
  `{ "*": {"installation_mode": "normal_installed" }}`

- "removed"
  (Chrome-versie 75 of hoger) Gebruikers kunnen de extensie niet installeren. Als gebruikers de extensie eerder hebben geïnstalleerd, wordt deze verwijderd uit de Chrome-browser.
  `{ "*": {"installation_mode": "removed" }}`

- `"toolbar_pin"`

  Hiermee bepaal je of het extensie-icoon wordt vastgezet op de werkbalk. Je kunt dit instellen op het volgende:
  force_pinned: Het extensie-icoon wordt vastgezet op de werkbalk en is altijd zichtbaar. De gebruiker kan het niet verbergen in het extensiemenu.
  default_unpinned: De extensie wordt verborgen in het extensiemenu, maar de gebruiker kan het icoon vastzetten op de werkbalk.
  Als je dit veld niet instelt, wordt de standaardinstelling van default_unpinned gebruikt.
  `{ "*": {"toolbar_pin": "forced_pinned" }}`

Als een extensie de functie installation_mode gebruikt, moet er nog een veld 'update_url' worden gedefinieerd om aan te geven vanaf waar de extensie kan worden geïnstalleerd.

- Als de gedownloade extensie wordt gehost op de Chrome Web Store, gebruik je "https://clients2.google.com/service/update2/crx".

- Als je de extensie op je eigen server host, gebruik je een URL naar een locatie waar Chrome het ingepakte pakket kan downloaden (.crx-bestand).
  Voorbeeld van json - force_installed-extensie met update_url:
  `{"nckgahadagoaajjgafhacjanaoiihapd": {"installation_mode": "force_installed","update_url": "https://clients2.google.com/service/update2/crx"}}`
- Vanaf Chrome 89 kun je ook gebruikmaken van de instelling override_update_url om aan te geven dat Chrome voor volgende extensie-updates de URL in het veld update_url of de update-URL die is opgegeven in het beleid ExtensionInstallForcelist gebruikt.
  - Als dit beleid niet is ingesteld of is ingesteld op false, gebruikt Chrome de URL die is opgegeven in het manifest van de extensie voor updates.

Voorkomen dat extensies webpagina's aanpassen

Deze instelling voorkomt dat extensies je gevoeligste websites aanpassen en er gegevens van lezen.
Met dit beleid kunnen extensies het volgende niet doen:

- Scripts in je websites injecteren
- De cookies lezen
- Webverzoeken aanpassen

Met deze instelling kunnen gebruikers wel extensies installeren of verwijderen. Je voorkomt alleen dat extensies door jou opgegeven websites aanpassen.

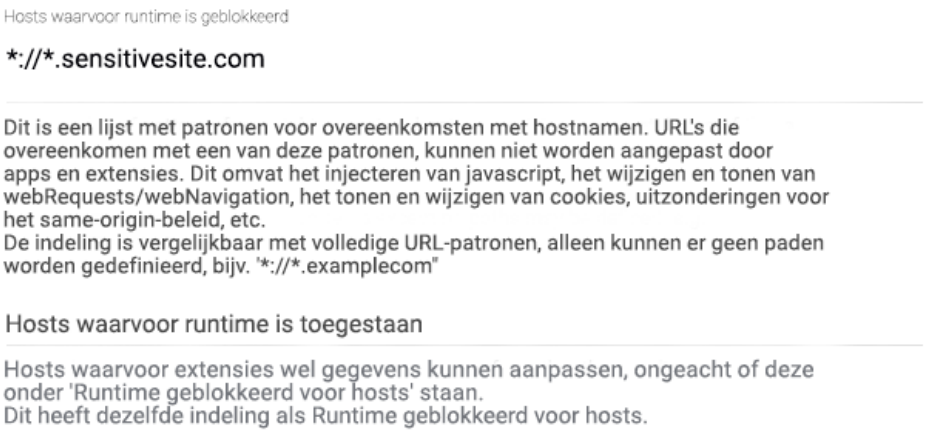
Er zijn 2 instellingen die je voor deze functie kunt gebruiken

- **runtime_blocked_hosts**: Extensies kunnen niets met deze hosts doen,
- **runtime_allowed_hosts** - Extensies kunnen interactie hebben met de hosts op deze lijst, zelfs als ze zijn gedefinieerd in runtime_blocked_hosts.

Toptip: Elke instantie van runtime_blocked_hosts en runtime_allowed_hosts kan maximaal 100 hostpatronen hebben. Als je meer definieert, wordt je beleid ongeldig.

Cloudbeheer voor de Chrome-browser
Blokkeren op basis van de runtime host is eenvoudiger in Cloudbeheer voor de Chrome-browser dan in GPO. Het vereist geen json. Je hoeft alleen maar de URL die je wilt blokkeren in te vullen in de extensie-instellingen. Hiervoor moet je je browserapparaten inschrijven in Cloudbeheer voor de Chrome-browser. De functie wordt kosteloos aangeboden. De inschrijvingsstappen vind je hier.

1. Ga in de Beheerdersconsole naar **Apparaten > Chrome >Apps en extensies > Gebruikers en browsers**.
2. Selecteer de organisatie-eenheid met de gebruikers voor wie je de extensies wilt toestaan.
3. Klik op het tandwiel voor aanvullende instellingen
4. Vul in het gedeelte 'Geblokkeerde runtime hosts' de URL in van de gevoelige websites waar de extensies niet mogen worden uitgevoerd. Raadpleeg voor informatie over de syntaxis Syntaxis voor geblokkeerde of toegestane URL's
    a. Je kunt meerdere URL's invullen door na elke URL op Enter te drukken voor een nieuwe invoer.
    b. Je kunt ook in het gedeelte 'Rechten en URL-toegang' klikken op een afzonderlijke extensie en toegestane en geblokkeerde hosts instellen.
        i. Hierdoor worden alle algemene beleidsregels overschreven die al op deze extensie zijn toegepast.
        ii. Er is ook een sectie allowed_hosts voor uitzonderingen voor URL's die staan in de sectie voor runtime hosts voor blokkeringen.
5. Klik op **Opslaan**.



Sectie Runtime hosts in Apparaten > Chrome >Apps en extensies > Gebruikers en browsers > Aanvullende instellingen

GPO
Deze instructies zijn voor het beheer van deze GPO op Windows-apparaten. Raadpleeg voor andere platforms het volgende: Mac | Linux

Binnen het beleid Extensie-instellingen kun je de volgende instellingen instellen om aanpassingen aan websites of domeinen te blokkeren (of toe te staan):

- Runtime_blocked_hosts
  Met deze instelling wordt voorkomen dat extensies aanpassingen doen aan jouw gekozen websites of er gegevens van lezen.

- Runtime_allowed_hosts
  Met deze instelling wordt toegestaan dat extensies aanpassingen doen aan jouw gekozen websites of er gegevens van lezen.

De indeling voor de opgave van je site(s) in de json-tekenreeks voor een van deze beleidsregels is:

```
[http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*] [http|https|ftp|*],
```

Opmerking: De secties [hostname|*] en [eTLD|*] zijn vereist, maar de sectie [subdomain|*] is optioneel.

Voorbeelden van geldige hostpatronen en overeenkomende patronen:

Geldige hostpatronen	Komt overeen met	Komt niet overeen met
://.example.*	http://example.com https://test.example.co.uk	https://example.google.com http://example.google.co.uk
http://example.*	http://example.com http://example.ly	https://example.com http://test.example.com
http://example.com	http://example.com	https://example.com http://test.example.co.uk
://	Alle URL's	

Dit is een voorbeeld van een json-tekenreeks die de toegang voor een enkele extensie blokkeert. Deze tekenreeks voorkomt dat een enkele extensie een specifieke site verbetert:

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

Compacte json-gegevens:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb":
{"runtime_blocked_hosts":["*://*.importantwebsite"]}}
```

Dit is een voorbeeld voor de blokkering van meerdere sites voor alle extensies:

```
{
   "*": {"runtime_blocked_hosts": [ "*://*.importantwebsite.com",
"*://*.importantwebsite2.com" ]
   }
```

Compacte json-gegevens:

```
{"*":{"runtime_blocked_hosts":["*://*.importantwebsite.com","*://*.importantweb
site2.com"]}}
```

Gebruik voor meerdere extensies voor elk een eigen invoer voor elke app-ID die je wilt blokkeren. Dit is een voorbeeld van hoe je voorkomt dat 2 extensies op hetzelfde domein worden uitgevoerd:

```
{
      "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      },
      "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {
            "runtime_blocked_hosts": ["*://*.importantwebsite"]
      }
}
```

Compacte json-gegevens:

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":
["*://,*.importantwebsite"]},"bfbmjmiodbnnpllbbbfblcplfjjepjdn":
{"runtime_blocked_hosts": ["*://*.importantwebsite"]}}
```

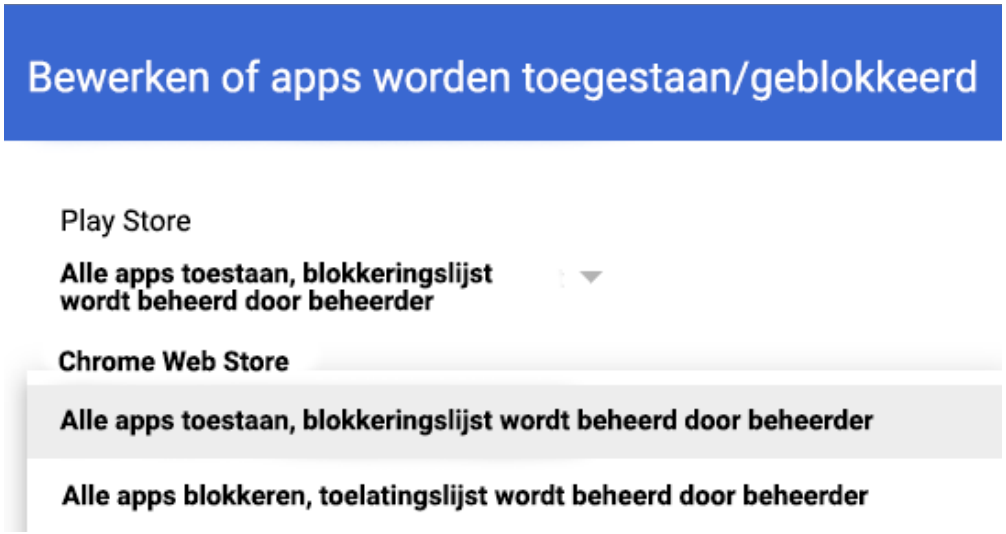
Extensies toestaan of blokkeren in de Google Beheerdersconsole

Beheerders kunnen bepalen welke extensies je gebruikers kunnen installeren door toelatings- en blokkeringslijsten te maken. Je kunt toestaan dat gebruikers elke app of extensie kunnen installeren. Je kunt beleidsregels instellen om apps voor alle gebruikers of bepaalde medewerkers te blokkeren of toe te staan.

Bij de volgende stappen wordt ervan uitgegaan dat je weet hoe je instellingen wijzigt in de Beheerdersconsole.

Alle extensies toestaan, behalve extensies die je wilt blokkeren

1. Ga in de Beheerdersconsole naar **Apparaten > Chrome > Apps en extensies > Gebruikers en browsers > Aanvullende instellingen**.
2. Selecteer links de organisatie-eenheid waarvoor je extensies wilt toestaan.
3. Scroll omlaag naar het gedeelte Toestaan/blokkeren onder Chrome Web Store, klik op Bewerken en selecteer de optie **Alle apps toestaan, blokkeringslijst wordt beheerd door beheerder**.

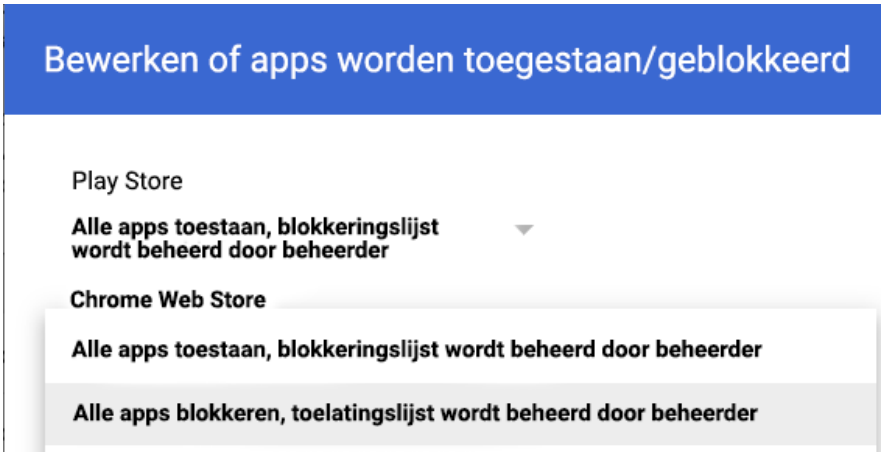


Instelling om apps toe te staan/te blokkeren

4. Klik op **Opslaan**.
5. Klik op het tabblad Gebruikers en browsers om terug te gaan naar de vorige pagina.
6. Voeg de extensies toe die je wilt blokkeren door rechts onderin op het gele plusje te klikken.
7. Kies de methode om deze toe te voegen aan de console (toevoegen via de Chrome Web Store, toevoegen via extensie-ID, toevoegen via URL).
8. Selecteer het dropdownmenu bij de extensie en dan **Blokkeren**.
9. Klik op **Opslaan**.

Blokkeer alle extensies die je niet wilt toestaan.

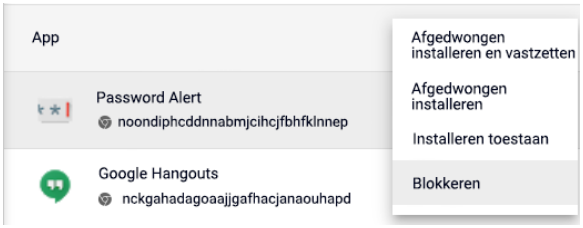
1. Ga in de Beheerdersconsole naar **Apparaten > Chrome > Apps en extensies > Gebruikers en browsers > Aanvullende instellingen**.
2. Selecteer links de organisatie-eenheid waarvoor je extensies wilt blokkeren.
3. Scroll omlaag naar het gedeelte Toestaan/blokkeren onder Chrome Web Store en selecteer de optie **Alle apps blokkeren, toelatingslijst wordt beheerd door beheerder**.



4. Klik op **Opslaan**.
5. Klik op het tabblad Gebruikers en browsers om terug te gaan naar de vorige pagina.
6. Voeg de extensies toe die je wilt toestaan door rechts onderin op het gele plusje te klikken.
7. Kies de methode om deze toe te voegen aan de console (toevoegen via de Chrome Web Store, toevoegen via extensie-ID, toevoegen via URL).
8. Selecteer het dropdownmenu bij de extensie en selecteer daarna **Installeren toestaan**.
   a. Je kunt de extensie ook afgedwongen installeren op de apparaten van je gebruikers door Afgedwongen installeren te selecteren.
9. Klik op **Opslaan**.

Eén extensie blokkeren of toestaan

1. Ga in de Beheerdersconsole naar **Apparaten > Chrome > Apps en extensies > Gebruikers en browsers**.
2. Selecteer de organisatie-eenheid waarvoor je de extensie wilt toestaan of blokkeren.
   - De organisatie-eenheid neemt de instellingen over van de bovenliggende organisatie-eenheid, maar je kunt deze overschrijven per suborganisatie-eenheid.
3. Selecteer de extensie die je wilt blokkeren of toestaan, of voeg deze toe (zie stap 6 en 7 van het vorige gedeelte).
4. Selecteer in de kolom voor installatiebeleid Blokkeren, Afgedwongen installeren of Installeren toestaan.

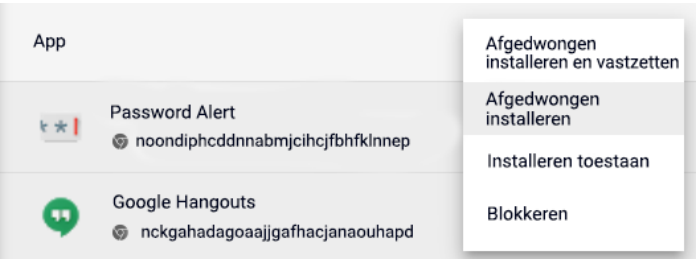


5. Klik op **Opslaan**.

Extensies afgedwongen installeren

Als je weet dat de gebruiker een extensie nodig heeft, kun je deze voor hem of haar installeren. Als je een extensie afgedwongen installeert, krijgt deze alle benodigde rechten om te worden uitgevoerd. De gebruiker kan de extensie niet verwijderen en deze wordt op de achtergrond geïnstalleerd. Als je een extensie verwijdert van de lijst voor afgedwongen installatie, wordt deze van het apparaat van de gebruiker verwijderd.

1. Ga in de Beheerdersconsole naar **Apparaten > Chrome > Apps en extensies > Gebruikers en browsers**.
2. Selecteer de organisatie-eenheid waarvoor je extensies afgedwongen wilt installeren.
3. Selecteer de bestaande extensie(s) die je afgedwongen wilt installeren of voeg deze toe.
   a. Klik hiervoor rechtsonder op het gele plusje.
   b. Kies de methode om deze toe te voegen aan de console (toevoegen via de Chrome Web Store, toevoegen via extensie-ID, toevoegen via URL).
4. Selecteer de extensie(s) die je afgedwongen wilt installeren en selecteer in de kolom voor installatiebeleid **Afgedwongen installeren** in het dropdownmenu.



5. Klik op **Opslaan**.

Je kunt een aangepaste Chrome Web Store-collectie maken van door beheerders geselecteerde extensies die aan je gebruikers worden getoond. Voor deze instelling moeten je gebruikers wel op een Google-identiteit zijn ingelogd met inloggegevens van het bedrijf.

- Deze extensie kun je vinden in de Beheerdersconsole onder Apparaten > Chrome > Apps en extensies > Gebruikers en browsers > Aanvullende instellingen > Chrome Web Store-homepage > De collectie uit de Chrome Web Store gebruiken
  - Daarna kun je al je extensies op deze pagina bekijken of op afzonderlijke extensies onder het gedeelte Gebruikers en browsers klikken en de schakelaar selecteren om ze op te nemen in de collectie uit de Chrome Web Store.

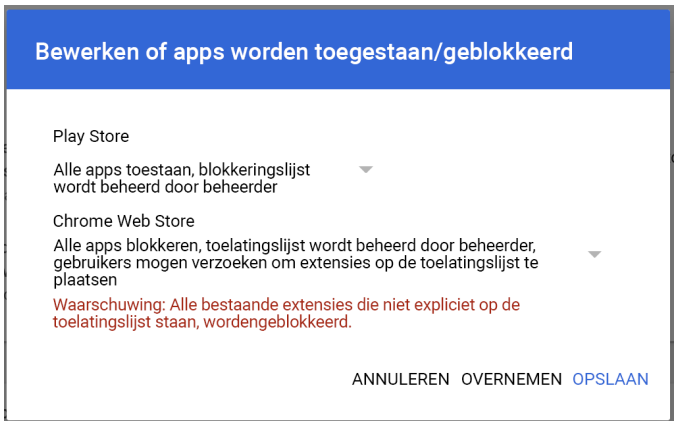
Gebruikers extensies laten gebruiken: Extensieworkflows

Als beheerder kun je in de Google Beheerdersconsole instellen dat gebruikers extensies die ze nodig hebben, kunnen aanvragen via de Chrome Web Store. Daarna kun je extensies die gebruikers hebben aangevraagd toestaan, blokkeren of automatisch laten installeren.

Voorbeeld van aanvraagdialoog uit Chrome Web Store

Deze functie werkt zoals een toelatings-/blokkeringslijst. Als de functie aanstaat, worden **alle** extensies standaard geblokkeerd. Volg bij voorkeur het volgende proces om problemen te voorkomen:

1. Ontdek welke extensies je gebruikers momenteel gebruiken via het rapport van geëxporteerde extensies in Cloudbeheer voor de Chrome-browser.
    - Bekijk voor meer informatie deze YouTube-video over hoe je de Takeout-API instelt.
2. Maak een lijst van essentiële extensies (GPO of Beheerdersconsole) op basis van de gegevens die je bij stap 1 hebt verzameld.
3. Zet de functie voor extensieworkflows aan onder **Apparaten > Chrome > Apps en extensies > Gebruikers en browsers > Aanvullende instellingen** > Toestaan/blokkeren en klik op de knop Bewerken.
4. Selecteer onder Chrome Web Store **Alle apps blokkeren, toelatingslijst wordt beheerd door beheerder, gebruikers mogen verzoeken om extensies op de toelatingslijst te plaatsen** in het dropdownmenu.



Extensieworkflows aanzetten in de Beheerdersconsole

    - We raden je aan instellingen eerst toe te passen op een klein aantal gebruikers en apparaten in een testorganisatie-eenheid. Zo voorkom je problemen met eindgebruikers en kun je feedback verzamelen. Daarna kun je ze op je hele organisatie toepassen.
5. Goedkeurings- en weigeringsverzoeken kun je beheren onder **Apparaten > Chrome > Apps en extensies > Verzoeken**
6. Klik op de rij van het extensieverzoek dat je wilt beoordelen.
7. Hier zie je de gegevens van de extensie en kun je een installatiebeleid selecteren in het dropdownmenu:
    - Afgedwongen installeren: De extensie wordt op de achtergrond geïnstalleerd en kan niet worden verwijderd.
    - Installeren toestaan: Gebruikers kunnen de extensie installeren.
    - Blokkeren: Gebruikers kunnen de extensie niet installeren. De extensie wordt verwijderd voor gebruikers die deze hebben geïnstalleerd.

Lees voor meer informatie over deze functie het Helpcentrum-artikel voor extensieworkflows of bekijk deze YouTube-video over extensieworkflows.

Extensies toestaan of blokkeren in groepsbeleid

Voordat je begint: Bij de volgende stappen wordt aangenomen dat je al Chrome beheert voor je gebruikers. Raadpleeg voor meer informatie over de implementatie van Chrome in Windows de implementatiehandleiding voor de Chrome-browser (Windows). Ga voor informatie over implementatie en beleidsbeheer op een Mac® naar De Chrome-browser instellen op Mac-apparaten.

Voor Windows zijn er 2 soorten beleidstemplates: een ADM- en een ADMX-template. Check welk type je op je netwerk kunt gebruiken. In deze templates staat welke registersleutels je kunt instellen om Chrome te configureren en wat de acceptabele waarden zijn. Chrome checkt de waarden in deze registersleutels om te bepalen welke acties moeten worden uitgevoerd.

1. Download Chrome-beleidstemplates.
   Je kunt Windows-templates en algemene beleidsdocumentatie voor alle besturingssystemen vinden via deze link

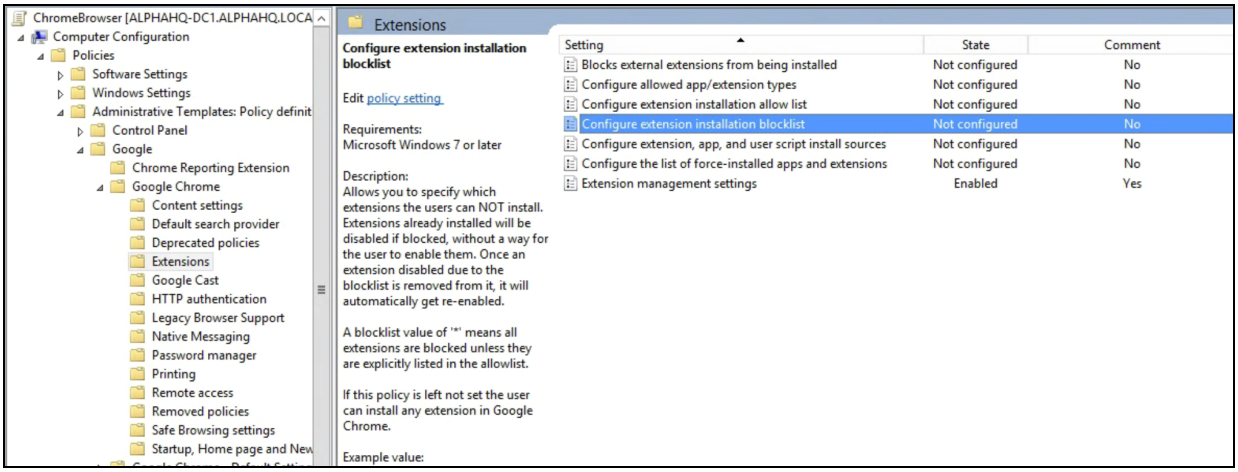
2. Open de ADM- of ADMX-template die je hebt gedownload:
    a. Ga naar **Start > Uitvoeren: gpedit.msc**.
    b. Ga naar **Beleid voor lokale computer > Computerconfiguratie > Beheersjablonen**.
    c. Klik met de rechtermuisknop op **Beheersjablonen** en selecteer **Sjablonen toevoegen/verwijderen**.
    d. Voeg de template chrome.adm toe in het dialoogvenster.

Er verschijnt een Google Chrome-map onder Beheersjablonen, als deze er niet al was.

- Als je de ADM-template in Windows 7 of 10 hebt toegevoegd, komt deze onder Klassieke beheersjablonen/Google/Google Chrome te staan.

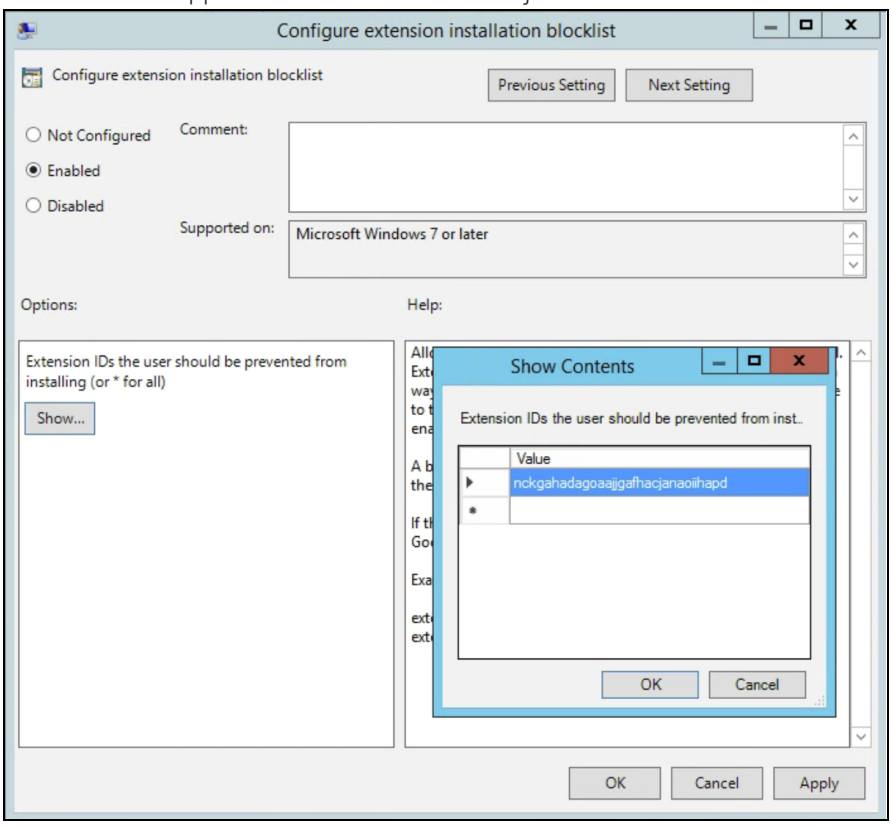
Alle extensies toestaan, behalve extensies die je wilt blokkeren

1. Open in de editor voor groepsbeleid de template die je zojuist hebt toegevoegd.
2. Browse naar **Google > Google Chrome > Extensies > Blokkeringslijst voor installatie van extensies configureren**.



Pad naar extensiebeheerbeleid

2. Selecteer in de instellingen **Aangezet**.
3. Klik op **Tonen**.
4. Vul de app-ID in van de extensies die je wilt blokkeren.



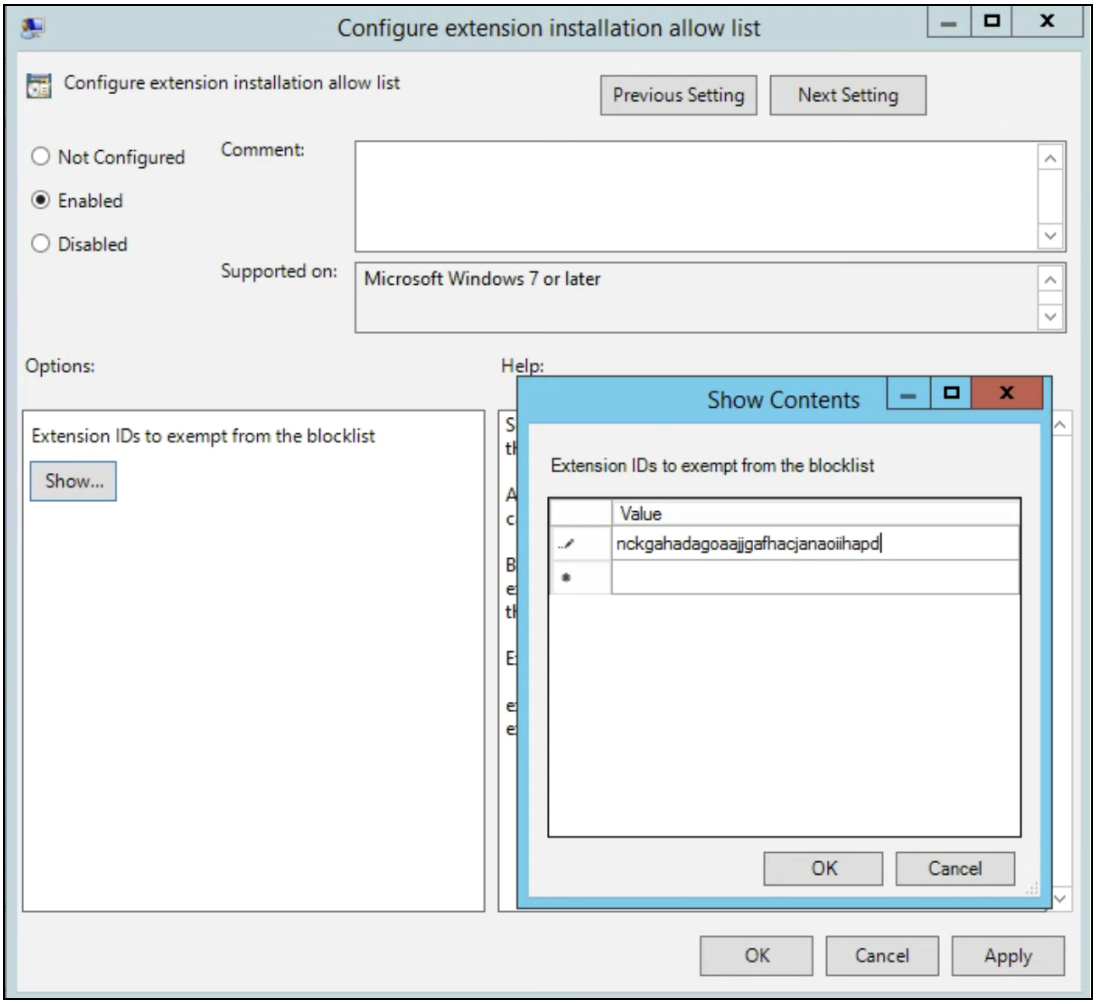
Blokkeringslijst voor installatie van extensies configureren

Opmerkingen:

- Als je de app-ID van een extensie niet kunt vinden, bekijk je deze in de Chrome Web Store. Zoek de specifieke extensie. De app-ID staat aan het eind van de URL in de Chrome-omnibox:

Voorbeeld van app-ID na google-hangouts/

- Voer ***** in het beleid in als je wilt dat geen enkele extensie kan worden geïnstalleerd. Dit kun je gebruiken met het beleid Toelatingslijst voor installatie van extensies configureren. Op deze manier kun je je gebruikers toestaan slechts bepaalde extensies te installeren en blokkeer je de rest.
- Je kunt een extensie aan de blokkeringslijst toevoegen die al op het apparaat van een gebruiker is geïnstalleerd. Dan wordt de extensie uitgezet en kan de gebruiker deze niet weer aanzetten. De extensie wordt niet verwijderd, alleen uitgezet.



Toelatingslijst voor installatie van extensies configureren

Eén extensie blokkeren of toestaan

Als je een enkele extensie wilt blokkeren, voeg je de app-ID van deze extensie toe aan het beleid Blokkeringslijst voor installatie van extensies configureren Al je andere extensies kunnen worden geïnstalleerd.

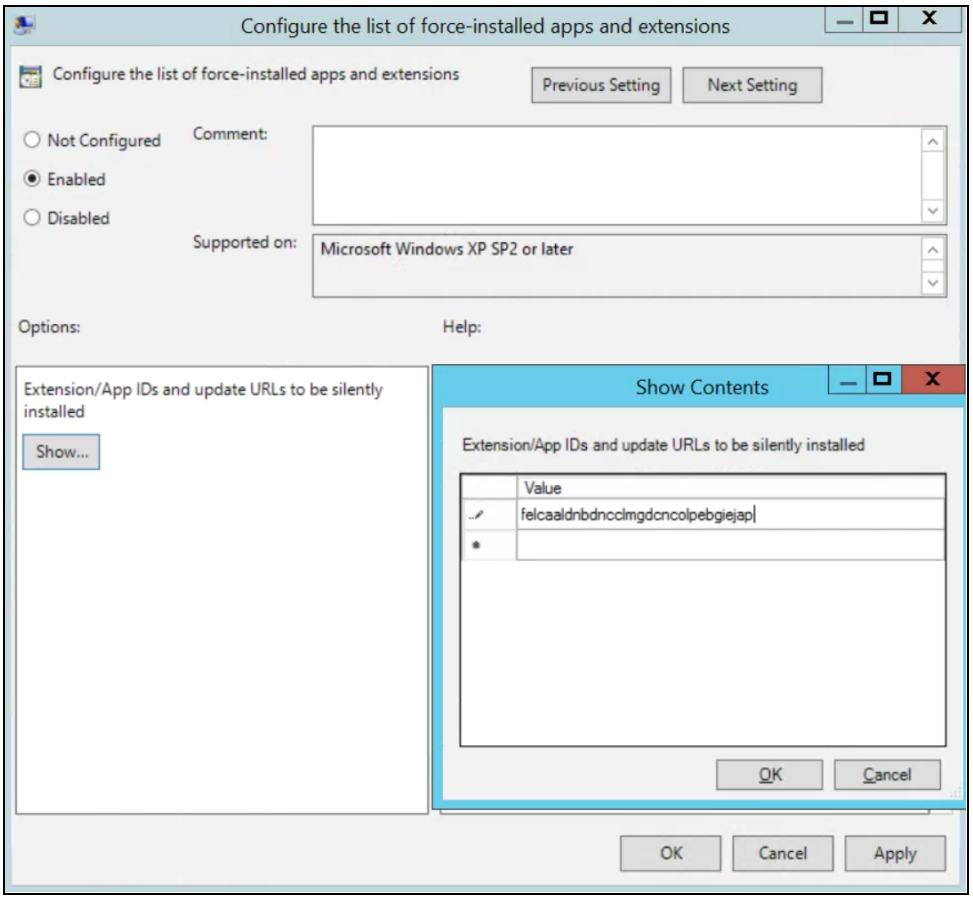
Slechts 1 extensie toestaan:

1. Geef ***** op in het contentgedeelte in het beleid Blokkeringslijst voor installatie van extensies configureren.
   Hierdoor kan geen enkele extensie op de lijst worden geïnstalleerd.
2. Voeg de app-ID van de toegestane extensie toe aan het beleid Toelatingslijst voor installatie van extensies configureren

Een extensie afgedwongen installeren

1. Browse in de editor voor groepsbeleid naar **Google > Google Chrome > Extensies > De lijst met automatisch geïnstalleerde apps en extensies configureren**.
2. Selecteer **Aangezet**.
3. Klik op **Tonen**.
4. Vul de app-ID in van een of meer extensies die je afgedwongen wilt installeren.

De extensie wordt op de achtergrond geïnstalleerd, zonder dat gebruikers iets hoeven te doen. Gebruikers kunnen de extensie ook niet uitzetten of verwijderen. Deze instelling overschrijft blokkeringslijstbeleid als je dit hebt aangezet.



De lijst met automatisch geïnstalleerde apps en extensies configureren

Je beleid valideren

Pas je beleid op een testapparaat toe om te checken of het geldig is en werkt zoals verwacht. Volg op het testapparaat de volgende stappen:

1. Ga naar chrome://policy.
2. Klik op de knop Beleid opnieuw laden.
3. In de rechterbovenhoek van de pagina staat het beleidsfilter. Typ 'ExtensionSettings' als je alleen dit beleid wilt tonen.
4. Vink het vakje aan voor Beleid zonder ingestelde waarde bekijken.
5. Check of de status van je beleid OK is.
6. Klik op Waarde tonen om het beleid uit te vouwen en check of het waardeveld niet leeg is.
7. Gefeliciteerd: je hebt een geldig beleid

Je extensies zelf hosten

De Chrome Web Store host extensies en biedt veel beveiligingsfuncties.

- Functies zoals geautomatiseerde en handmatige codescans.
    - Zo voorkom je dat je gebruikers schadelijke code ontvangen.

Je kunt je extensies ook op je eigen server hosten, los van de Chrome Web Store. Dit zijn enkele voor- en nadelen van deze methode:

Voordelen:

- Als je je eigen extensies host, val je buiten de regels en vereisten van de Chrome Web Store.
    - Er is dan minder controle en minder risico dat de extensie wordt verwijderd vanwege schending van de servicevoorwaarden.

Nadelen:

- Als je zelf host, moet je meer instellen en moet je je eigen bestandsserver hosten voor extensiebestanden.
- Het kan lastig zijn om de beveiliging van extensies te valideren en deze geüpdatet te houden. De Chrome Web Store doet dit automatisch.

Als je je extensies zelf wilt hosten, vind je in dit gedeelte meer informatie. Hier wordt beschreven hoe je een extensie inpakt en host zonder de Chrome Web Store. Ook bevat het gedeelte instructies over hoe je deze extensies implementeert op je apparaten en voor je gebruikers.

Alternatieven voor het zelf hosten van extensies

Publicatieopties voor extensies

In plaats van zelf te hosten, kun je interne extensies als privé markeren in de Chrome Web Store. Er zijn 3 publicatieopties voor extensies: openbaar, privé en verborgen. In dit diagram vind je meer informatie over de voor- en nadelen van de opties:

	Aanwezig in Chrome Zoekfunctie voor Web Search?	Inloggen vereist?	Ondersteund in Chrome Browser Cloudbeheer
Openbaar	Ja	Nee	Ja
Privé	Nee	Ja	Ja
Verborgen	Nee	Nee, gebruikers hebben een link nodig om te installeren	Ja

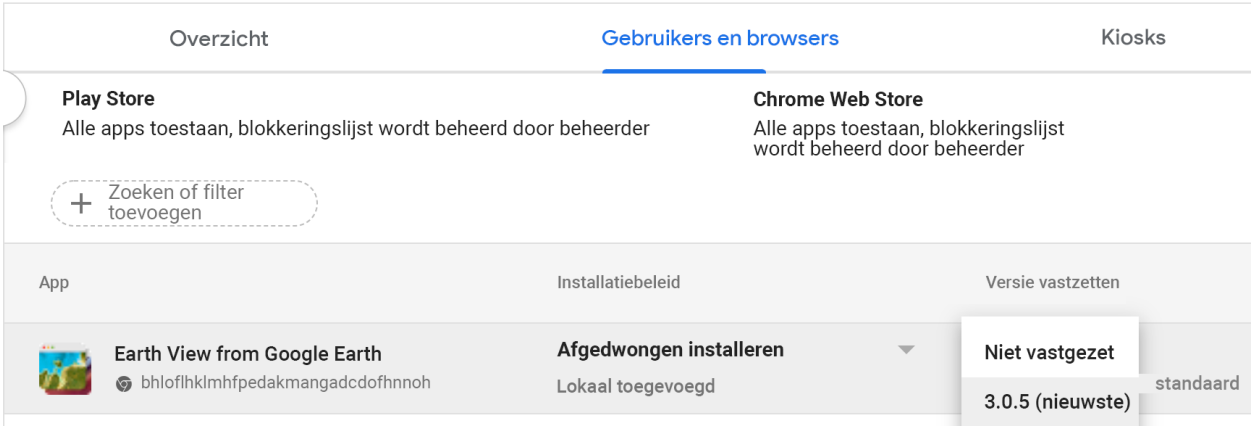
Raadpleeg voor meer informatie deze blog over hoe je je extensies niet-openbaar publiceert zonder dat je je extensies zelf hoeft te hosten.

- Als je je extensies beheert via de Beheerdersconsole, moet je de rechten voor Chrome Web Store zo instellen dat je gebruikers privé-extensies zien.
    - Dit kun je doen in de Beheerdersconsole onder Apparaten > Chrome > Apps en extensies > Aanvullende instellingen > Rechten voor Chrome Web Store > stel in dat gebruikers privé-apps die beperkt zijn tot jouw domein kunnen publiceren op de Chrome Web Store.

Een extensie vastzetten op een specifieke versie in de Beheerdersconsole

De Google Beheerdersconsole biedt nu enkele nieuwe opties voor extensiebeheer. Allereerst kun je een specifieke versie van een extensie vastzetten in de Beheerdersconsole. Dit biedt bedrijven meer stabiliteit als ze een bepaalde versie van een extensie moeten gebruiken. Het wordt niet aanbevolen om een oudere versie vast te zetten. Als je dit wel doet, zorg dan als tijdelijke maatregel dat je beschikt over de nieuwste functies en beveiligingsupdates. Deze functie is alleen beschikbaar voor extensies die afgedwongen zijn geïnstalleerd. Raadpleeg voor meer informatie dit Helpcentrum-artikel.

1. Ga in de Beheerdersconsole naar **Apparaten > Chrome > Apps en extensies > Gebruikers en browsers**.
2. Selecteer de organisatie-eenheid met de extensie die je wilt vastzetten.
3. Selecteer de bestaande extensie(s) (of voeg een nieuwe toe) die je wilt beheren op basis van versie en selecteer onder de kolom voor het vastzetten van versies de gewenste versie in het dropdownmenu. Klik dan op Opslaan.
   a. Als je een app of extensie vastzet, ontvangt deze geen updates meer, waaronder beveiligings- en compatibiliteitsupdates.
   b. Je kunt ook alleen vastzetten op de huidige versie van de extensie die tijdens de installatie op de Chrome Web Store staat.
   c. Je kunt ook zelfgehoste apps en extensies vastzetten en de URL in de Beheerdersconsole updaten. Zie het gedeelte Zelfgehoste apps vastzetten in dit Helpcentrum-artikel.



Versies vastzetten in de Beheerdersconsole

Vereisten voor extensies zelf hosten

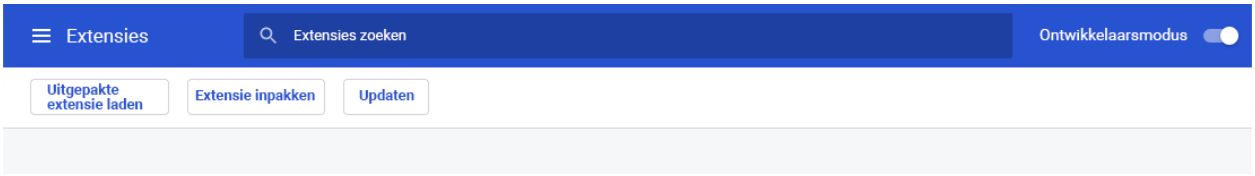
Als je je extensie wilt hosten, heb je eigen webhostingservices nodig voor de extensie en het manifestbestand. Deze hostinglocatie mag geen verificatie vereisen. Apparaten in gebruik moeten de locatie kunnen bereiken. Houd hier rekening mee als je het bestand wilt hosten op je interne opslagplaats.

Bij deze stappen wordt ervan uitgegaan dat je je extensie al hebt gemaakt en ervaring hebt met XML-bestanden. Daarnaast moet je bekend zijn met groepsbeleid en het gebruik van het Windows-register. Deze stappen zijn niet van toepassing op extensies van derden die je niet hebt ontwikkeld. Als je een extensie van derden zelf wilt hosten, moet je dit rechtstreeks met de leverancier van de extensie bespreken.

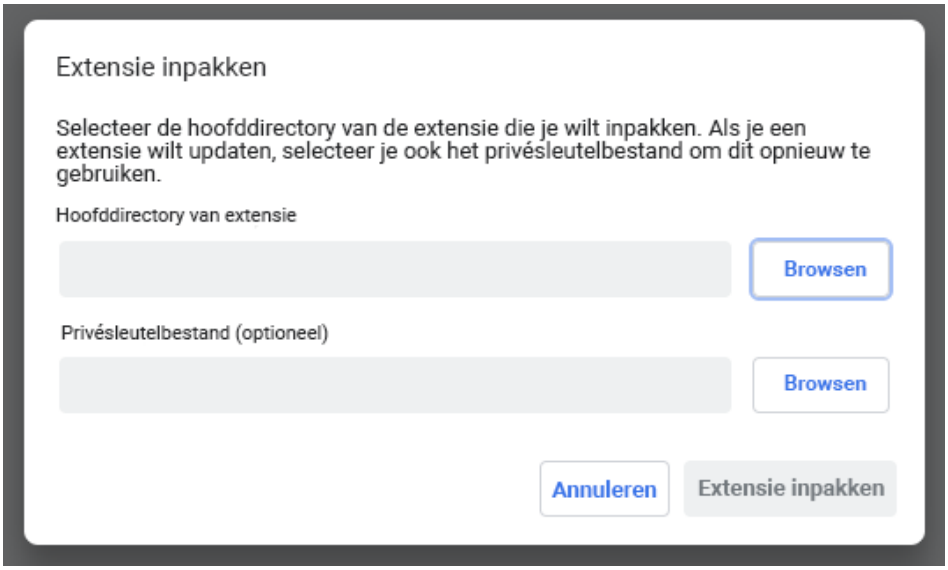
Je extensie inpakken

Extensies moeten eerst worden ingepakt in een CRX-bestand. Als dit nog niet is gebeurd, zijn hier de stappen:

1. Ga naar **chrome://extensions** in de adresbalk van Chrome en vink het selectievakje aan voor **Ontwikkelaarsmodus**.



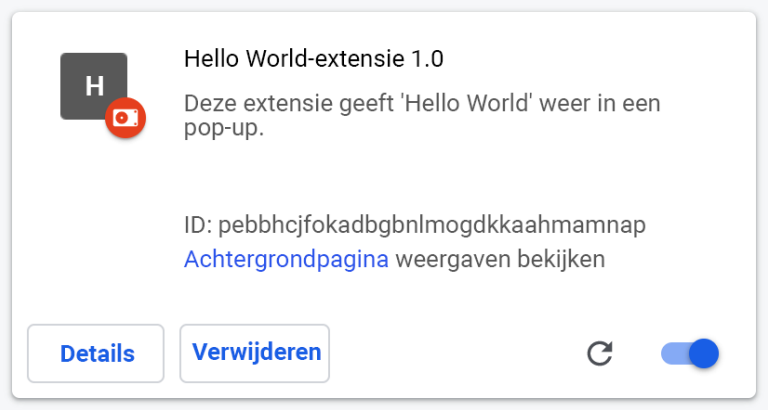
2. Klik in de ontwikkelaarsmodus op **Extensie inpakken** om het CRX-bestand te maken.



3. Selecteer de opslagplaats waar je bron zich bevindt. Zo wordt je CRX-bestand gemaakt, naast een PEM-bestand.

Toptip: Bewaar het PEM-bestand op een beveiligde plek, want dit is de sleutel voor je extensie. Je hebt het in de toekomst voor updates nodig.

4. Sleep het CRX-bestand naar het extensievenster en check of het wordt geladen.
    a. Op Windows en Mac wordt de extensie standaard uitgezet, maar niet op Linux.
5. Test de extensie en noteer het ID-veld en versienummer.
   Deze heb je later nodig.



5. Plaats het CRX-bestand in de hostlocatie vanaf waar je gebruikers of apparaten het downloaden.
    - Noteer de URL van waar het bestand wordt geüpload.
    - Deze is belangrijk voor het XML-manifestbestand.
6. Definieer deze 3 velden om een XML-manifestbestand te maken met de app-/extensie-ID, download-URL en versie.
    - **appid** (de extensie-ID van stap 5)
    - **codebase** (de downloadlocatie voor het CRX-bestand van stap 3)
    - **version** (de versie van de app/extensie, die moet overeenkomen met stap 5)

    Voorbeeld van XML-manifestbestand

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='abcdefghijklmnopqrstuvwxyz123456
'>
    <updatecheck codebase='https://example.com/chrome/helloworld.crx'
version='1.0' />
  </app>
</gupdate>
```

8. Upload het voltooide XML-bestand naar een locatie vanaf waar je gebruikers of apparaten het kunnen downloaden. Noteer de URL.

Je extensie hosten

De server die de .crx-bestanden van je extensie host, moet gebruikmaken van gepaste HTTP-headers zodat gebruikers op een link kunnen klikken om de extensie te installeren.
Google Chrome beschouwt een bestand als installeerbaar in een van de volgende gevallen:

- Het bestand heeft het contenttype application/x-chrome-extension.
- De bestandsextensie is .crx en de volgende 2 uitspraken zijn waar:
    - Het bestand is niet weergegeven met de HTTP-header X-Content-Type-Options: nosniff.
    - Het bestand is weergegeven met een van de volgende contenttypen:
        - lege tekenreeks
        - "text/plain"
        - "application/octet-stream"
        - "unknown/unknown"
        - "application/unknown"
        - "*/*"

De meestvoorkomende reden dat een installeerbaar bestand niet wordt herkend, is dat de server de header X-Content-Type-Options: nosniff stuurt. De op een na meestvoorkomende reden is dat de server een onbekend contenttype stuurt, een die niet in de vorige lijst staat. Als je een probleem met HTTP-headers wilt oplossen, wijzig je de configuratie van de server of probeer je het .crx-bestand op een andere server te hosten.

Updates voor je extensie publiceren

Zorg dat je de vereiste wijzigingen aan je extensie hebt aangebracht en getest. Updates publiceren:

1. Wijzig het versienummer in het json-manifestbestand van je extensie in een groter cijfer.
   Voorbeeld:
   `"version": "versionString"`
   Als de `"version":"1.0"` is, kun je updaten naar `"version":"1.1"` of elk cijfer hoger dan `"1.0"`.

2. Update de `"version"` van `<updatecheck>` in het XML-bestand naar het nummer dat je bij de laatste stap in het manifestbestand hebt gezet.
   Nog een voorbeeld:
   ```
   <updatecheck codebase='https://app.somecompany.com/chrome/helloworld.crx'
   version='1.1' />
   ```

3. Maak opnieuw een CRX-bestand met de volgende wijzigingen:
    a. Ga naar **chrome://extensions** in de adresbalk van Chrome.
    b. Vink het selectievakje aan voor **Ontwikkelaarsmodus**.

4. Maak het CRX-bestand door te klikken op **Extensie inpakken** en de directory te selecteren waar je bron zich bevindt.
   Opmerking: Gebruik voor het PEM-bestand hetzelfde bestand dat is gegenereerd en opgeslagen toen het CRX-bestand voor het eerst werd gemaakt.
5. Sleep het CRX-bestand naar het extensievenster en check of het wordt geladen.
6. Test de extensie.
7. Vervang het oude CRX-bestand en XML-bestand door het nieuwe bestand.
    a. Dit moet zich op dezelfde hostlocatie bevinden waarvandaan de gebruikers of apparaten de bestanden eerder hebben gedownload.

De wijzigingen worden van kracht tijdens de nieuwe beleidssynchronisatiecyclus.

Referentie-URL's:

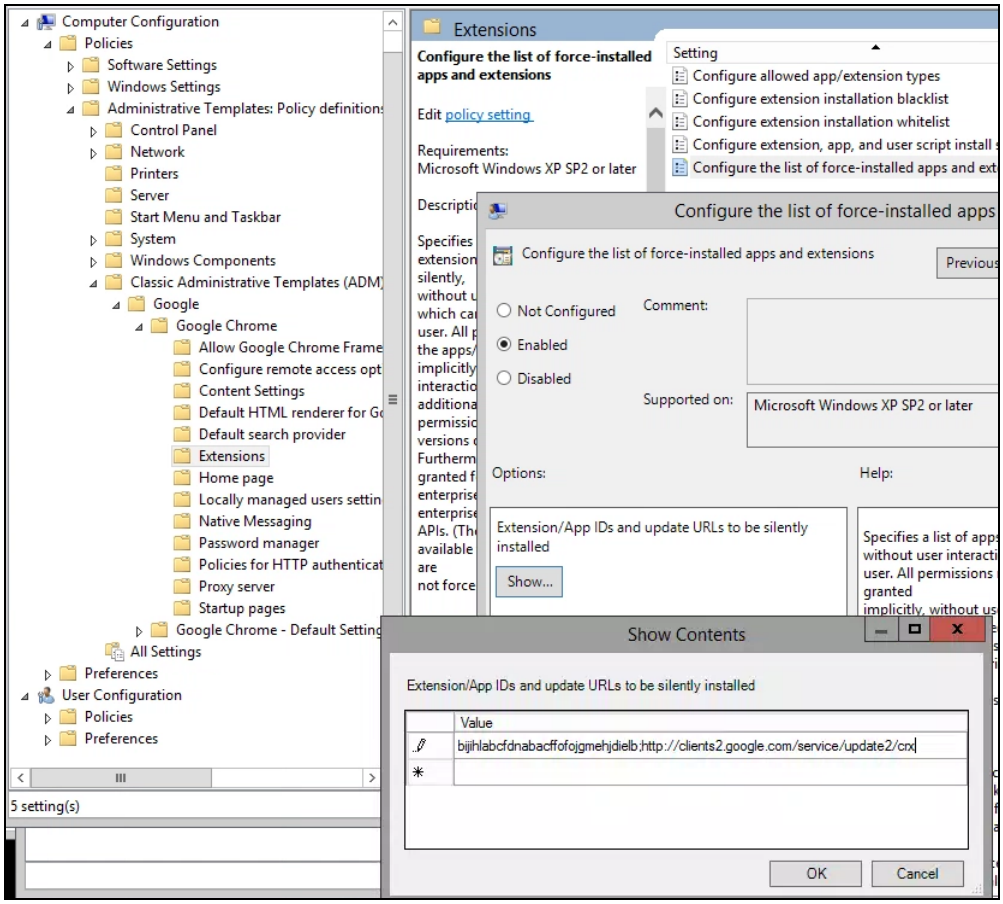
- Automatisch updaten
- Update-URL
- Manifest updaten

Privé gehoste extensies distribueren

In groepsbeleid: Momenteel wordt de distributie van zelfgehoste extensies alleen ondersteund via groepsbeleid. Je kunt het beleid 'De lijst met automatisch geïnstalleerde apps en extensies configureren' gebruiken om een extensie afgedwongen te installeren op het apparaat van je gebruiker.

Gebruik voor privé gehoste apps (niet in de Chrome Web Store) een tekenreeks als:
`pckdojakecnhhplcgfflhndiffaohfah;https://sites.google.com/site/pushcrx/privatewebstore/extension_info.xml`

Deze URL verwijst naar de **update.xml van de interne app**, in plaats van de openbare URL `clients2.google.com`.



GPO-beleid 'De lijst met automatisch geïnstalleerde apps en extensies configureren' (inhoud bekijken)

Daarna kun je de beleidsregels toepassen op de gewenste gebruikers, apparaten of beide. Het kan even duren voor het beleid van kracht is. Je kunt het proces versnellen door gpupdate op het apparaat van je gebruiker uit te voeren.

Extensies beheren met Cloudbeheer voor de Chrome-browser

Beheer de Chrome-browser voor je Windows-, Mac- en Linux-apparaten vanuit één plek en krijg een gedetailleerd overzicht van de status van de Chrome-browser in je omgeving. Cloudbeheer voor de Chrome-browser is een goede beheermethode voor de Chrome-browserinstellingen. Toegang tot deze console kost niets extra. Met deze functie van Chrome heb je toegang tot alle gedeelten van dit document die naar de Google Beheerdersconsole verwijzen. Met de console kun je snel inzicht krijgen in het volgende:

- De huidige Chrome-browserversies die op je apparaten zijn geïmplementeerd,
- De geïnstalleerde extensies in elke browser,
- De toegepaste beleidsregels in elke browser.
- Bekijk deze video voor meer informatie over het beheer van extensies in Cloudbeheer voor de Chrome-browser.

Aanvullende hulpbronnen

Aanvullende hulpbronnen om je te helpen de Chrome-browser te beheren in je organisatie:

- Landingspagina Cloudbeheer voor de Chrome-browser
- Enterprise-pakket voor de Chrome-browser
- Lijst met Chrome-beleid
- Release-opmerkingen voor Chrome Enterprise
- Beheerstrategieën voor updates voor de Chrome-browser
- Helpcentrum Chrome Enterprise
- Chrome instellen als de standaardbrowser (Windows 10)
- Chrome-blogserie voor insiders
- De overstap van Chrome-extensies naar Manifest V3