



Implementatiegids voor Chrome-apparaten

Chrome-apparaten instellen en implementeren in je organisatie

Inhoudsopgave

Over deze gids

Inleiding

- Vereisten
- Chrome-apparaten beheren

Connectiviteit

- Belangrijkste functies
- Tips voor evaluatie en implementatie
- Netwerkprofielen beheren
- Wifi instellen
 - Wifi-instellingen toevoegen op apparaatniveau
 - Wifi instellen
 - 802.1x-implementatie
 - Webfilters

Accounts en Chrome-beleid instellen

- Belangrijke beleidsoverwegingen
- Aanbevolen instellingen

Je apparaten voorbereiden op de implementatie

- Chrome-apparaten updaten naar de nieuwste versie
- Een Chrome OS-image maken
- Je apparaten voorbereiden voor inschrijving
- Uitgebreide voorbereidingsservice (optioneel)

Afdrukken met Chrome-apparaten

- Overwegingen voor organisaties
- Integratie met bestaande infrastructuur

Externe toegang en virtualisatie (optioneel)

- Belangrijkste functies
- Overwegingen voor app-hosting

Speciale scenario's voor implementatie van Chrome-apparaten

- Kiosk-app voor één doel
- Kiosken voor beheerde gastsessies
- Digitale borden
- Proefwerken en toetsen

Checklist voor implementatie

Aanvullende bronnen en support

- Nieuws over Chrome-apparaten bijhouden
- Helpcentrum bekijken
- Tips om zelf support te bieden
- Support vragen

Over deze gids

Deze gids is een aanvulling bij de [snelstartgids voor Chrome-apparaten](#). Hierin staat (gedetailleerder beschreven):

- De belangrijke beslissingsmomenten bij het implementeren van Chrome-apparaten voor een grote school of een groot bedrijf.
- [Cloudbeleid](#), Chrome-apps en specifieke toepassingen. Ga voor uitgebreidere informatie naar het [Helpcentrum van Chrome Enterprise](#).

In deze gids ligt de focus op:

- **Instellingen en inschrijving:** hoe verbind je elk apparaat met je netwerk, hoe schrijf je deze apparaten in op je domein en hoe update je ze naar de laatste versie van Chrome OS.
- **Beheer:** hoe implementeer je beleid voor je domein om te voldoen aan je IT-vereisten, hoe stel je apparaten in met de nieuwste versie van Chrome OS en hoe beheer je ze.

Opmerking: De aanbevelingen voor het implementeren van Chrome-apparaten in school- en bedrijfsomgevingen zijn gebaseerd op onze ervaringen met verschillende klanten en partners. We bedanken onze klanten en partners voor het delen van hun ervaringen en kennis. Ga voor informatie over de implementatie van de beheerde Chrome-browser naar [Chrome implementeren](#).

Behandelde onderwerpen	Instructies, aanbevelingen en belangrijke overwegingen voor het implementeren van Chrome-apparaten in een school- of bedrijfsomgeving
Primaire doelgroep	IT-beheerders
IT-omgeving	Chrome OS, webomgeving
Conclusies	Best practices voor de belangrijke overwegingen en besluiten bij de implementatie van Chrome-apparaten

Laatst geüpdatet: 10 september 2019

Locatie van het document: <https://support.google.com/chrome/a/answer/6149448>

©2019 Google LLC Alle rechten voorbehouden. Google en het Google-logo zijn gedeponeerde handelsmerken van Google LLC. Alle andere bedrijfs- en productnamen zijn mogelijk handelsmerken van de bedrijven waarmee ze in verband worden gebracht. [CHROME-en-2.0]

Inleiding

Chrome-apparaten zijn computers die zijn ontwikkeld door Google en draaien op Chrome OS. Deze computers zijn uniek omdat ze volledig in een webomgeving draaien. Ze worden automatisch geüpdatet en je hoeft niet zelf regelmatig patches te installeren of een nieuwe image te maken. Ze starten snel op en hebben verschillende ingebouwde [veiligheidsfuncties](#).

Je kunt Chrome-apparaten centraal beheren met de Google Beheerdersconsole. In deze webconsole kun je meer dan 200 instellingen (zoals wifi-instellingen) definiëren, apps selecteren die je vooraf wilt installeren en instellen dat apparaten automatisch updaten naar de nieuwste versie van Chrome OS.

Vereisten

1. Hoewel Google Identity (Google Workspace-account) niet vereist is om een beheerd Chrome-apparaat te gebruiken, raden we je wel aan je gebruikers een Google-account te geven. Zie [Nieuwe gebruikers toevoegen](#) voor meer informatie.
2. Voor elk zelfstandig Chrome-apparaat dat je wilt beheren, heb je Chromebook Enterprise-apparaten nodig of een upgrade zoals Chrome Enterprise Upgrade of Chrome Education Upgrade. Koop upgrades voor een [school of bedrijf](#). Verder kunnen organisaties in de VS en Canada [Chrome Enterprise Upgrade online kopen](#).
3. Als je een groot aantal Chrome-apparaten wilt implementeren of deze voor de eerste keer samen met Google Workspace implementeert, raden we je aan samen te werken met een [Google Cloud Partner](#).

Chrome-apparaten beheren

Je kunt Chrome-apparaten instellen in vrijwel elke school- of bedrijfsomgeving. Wanneer je Chrome-apparaten implementeert, kun je (als beheerder) de toegang tot het wifi-netwerk, webfilters, vooraf geïnstalleerde apps en diverse andere zaken beheren via:

- **Apparaatbeleid:** Hiermee kun je instellingen en beleid afdwingen op de beheerde Chrome-apparaten, onafhankelijk van wie inlogt. Je kunt inloggen bijvoorbeeld beperken tot specifieke gebruikers, de gastmodus blokkeren en instellingen voor automatisch updaten definiëren. [Meer informatie](#)
- **Gebruikersbeleid:** Hiermee kun je instellingen en beleid afdwingen bij de gebruikers in je organisatie, ongeacht welk Chrome-apparaat ze gebruiken. Een IT-beheerder kan bijvoorbeeld apps vooraf installeren voor specifieke gebruikers, Safe Browsing afdwingen, Single Sign-On (SSO) instellen, specifieke plug-ins blokkeren, specifieke URL's op een blokkeerlijst zetten, bookmarks beheren en tientallen andere instellingen toepassen voor gebruikers in de hele organisatie. [Meer informatie](#)
- **Beleid voor beheerde gastsessies:** Hiermee kun je instellingen definiëren voor gedeelde apparaten in je domein. Met beheerde gastsessies kunnen meerdere gebruikers hetzelfde Chrome-apparaat delen zonder dat inloggen of verificatie nodig is. Je kunt instellingen afdwingen, zoals de gebruiker uitloggen na een bepaalde tijdsduur. [Meer informatie](#)

Connectiviteit

Wanneer je draadloze instellingen definieert voor een school of bedrijf, moet je voldoende draadloos bereik hebben in het hele gebouw en genoeg bandbreedte hebben waarmee al je apparaten online kunnen werken.

Belangrijkste functies

Chrome-apparaten ondersteunen alle gangbare wifi-protocollen: WEP, WPA, WPA2, EAP-TLS, EAP-TTLS, EAP-PEAP en LEAP. Daarnaast hebben sommige Chrome-apparaten hardware voor 3G- of 4G-internettoegang. Dit werkt zolang je mobiel bereik en een data-abonnement voor mobiele apparaten hebt.

Tips voor evaluatie en implementatie

Goede evaluatie en voorbereiding van de netwerkstructuur van je organisatie zijn belangrijke stappen voor het beste gebruiksgemak. IT-beheerders moeten adequate connectiviteit en bandbreedte bieden, met name in een gebied met hoge gebruiksdichtheid, zoals een kantoor of school waar veel Chrome-apparaten gelijktijdig worden gebruikt.

- **Test de wifi-dekking en -dichtheid** om te kijken of er extra toegangspunten nodig zijn. Dit kun je doen met de externe [app Wifi Analyzer](#) op een Android-apparaat.
- **Onderzoek de draadloze infrastructuur en topologie** van alle gebouwen voordat je implementaties uitvoert in een hele school of bedrijf om er zeker van te zijn dat je voldoende draadloos bereik hebt. Het is meestal het beste als een partner die is gespecialiseerd in draadloze topologie het volgende doet:
 - **Locatieonderzoek:** analyseer eerst je bestaande wifi-netwerk en de omliggende storing door apparaten of andere wifi-netwerken.
 - **Implementatie:** implementeer of verplaats toegangspunten met goede beveiliging, kanaalselectie en ontvangst-/zendvermogen (Rx/Tx).
- **Chrome-apparaten moeten toegang hebben tot de vereiste URL's.** Chrome-apparaten moeten toegang hebben tot het netwerk van Google, zodat deze correct werken en beleid en beveiligingsupdates krijgen. Als je internettoegang in je omgeving beperkt, moeten je geïmplementeerde apparaten nog toegang hebben tot deze specifieke Google-[URL](#)'s zonder dat ze een geverifieerde proxy of SSL-inspectie moeten ondergaan.

Zie [Zakelijke netwerken voor Chrome-apparaten](#) voor meer informatie.

Netwerkprofielen beheren

Je kunt op elk gewenst moment handmatig wifi-netwerken toevoegen aan het Chrome-apparaat, maar Google adviseert om de [Beheerdersconsole te gebruiken om wifi-profielen te pushen](#). Deze profielen worden tijdens het inschrijvingsproces gedownload en toegepast op het Chrome-apparaat. Updates voor wifi-netwerkprofielen worden ook gepusht wanneer je beleid op het Chrome-apparaat automatisch vernieuwt. Het voordeel van deze configuraties pushen via de Beheerdersconsole is dat de vooraf gedeelde sleutel (PSK) mogelijk voldoende complex is en nooit hoeft te worden gedeeld met eindgebruikers.

Wifi instellen

Veel gebruikers van Chrome-apparaten gebruiken WPA2-PSK om het apparaat eenvoudig te kunnen instellen. Chrome-apparaten kunnen worden gebruikt in diverse onderwijs- en bedrijfsomgevingen, waaronder scenario's met een complexe wifi-implementatie waarbij clientcertificaten en SSO nodig zijn en waar oplossingen met webfilters zijn geïmplementeerd. Hieronder staan tips over het instellen van wifi en optionele netwerkinstellingen.

Wifi-instellingen toevoegen op apparaatniveau

Onderliggende organisatie-eenheden nemen de wifi-netwerkprofielen over van hun bovenliggende organisatie. Als je een profiel wilt instellen, moet je netwerkgegevens als de SSID en het type beveiliging opgeven. Let met name op de Service Set Identifier (SSID) en de wachtwoordzin. Beide zijn hoofdlettergevoelig. Wanneer je een nieuw wifi-netwerkprofiel definieert, moet je ook de selectievakjes **Automatisch verbinding maken** en **Chromebooks** aanvinken in het gedeelte **Toegang tot dit wifi-netwerk beperken op basis van platform**. Meer technische informatie over netwerkinstellingen vind je [hier](#).

Device management > Networks > Wi-Fi

ORGANIZATIONS

- solarmora.com
- Cloud Identity
- Development
- Finance
- Legal
- Marketing
- Sales
- Support
- Vault
- XEdu
- XInfoX

SETTINGS for solarmora.com

Name [Help](#)

Service set identifier (SSID)

☐ This SSID is not broadcast

☒ Automatically connect

Security type

None

Proxy settings

Direct Internet Co

Restrict access to this Wi-Fi network by platform

This Wi-Fi network will be available to users using:

☒ Mobile devices

☒ Chromebooks

☒ Google meeting room hardware

Apply network

by user

Users in this Organizational Unit will automatically get access to this network when signed in.

[ADD](#) [CANCEL](#)

Wifi instellen

De eenvoudigste manier is vaak om een open of ongefilterd netwerk te gebruiken om de Chrome-apparaten in te schrijven en een eerste synchronisatie van het managementbeleid uit te voeren. Met deze instellingen kan het Chrome-apparaat de netwerkprofielen krijgen die zijn gedefinieerd door de IT-beheerder. Nadat je de apparaten hebt ingesteld, verwijder je dit tijdelijke inschrijvingsnetwerk uit de lijst met voorkeursnetwerken. Zie [Een netwerk vergeten](#).

802.1x-implementatie

Chrome-apparaten ondersteunen 802.1x-verificatie. Neem contact op met je netwerkleverancier om te zien hoe je [Chrome-apparaten met clientcertificaten](#) instelt. [ClearPass Onboard](#) van Aruba Networks is bijvoorbeeld een extensie voor de introductie van Chrome-apparaten en installeert het certificaat op een veilige manier.

Beheerders en partners van Google Cloud System kunnen documentatie voor de uitgebreide configuratie van zakelijke wifi-netwerken met 802.1x vinden op [Google Cloud Connect](#).

Je moet verbinding hebben met het netwerk om het 802.1x-certificaat te downloaden. Daarom moet je een open WPA/WPA2-PSK-netwerk instellen of adapters voor USB naar ethernet gebruiken om het certificaat te laden op het apparaat. Zie [Netwerken beheren](#).

Ga voor meer informatie hierover naar [Clientcertificaten beheren op Chrome-apparaten](#).

Webfilters

Bij organisaties met apparaten voor netwerkfiltering die SSL-inspecties (Secure Socket Layer) uitvoeren, moet over het algemeen een rootcertificaat worden toegevoegd op het tabblad **Certificeringsinstanties** in `chrome://settings/Certificates`. Hoewel dit werkt voor de meeste webverzoeken van gebruikers, maken sommige verzoeken op systeemniveau geen gebruik van dit certificaat om de gebruiker te beschermen tegen bepaalde soorten beveiligingsrisico's. Zie [deze lijst met hosts](#) die moeten worden uitgesloten van SSL-inspectie.

Als je Chrome-apparaten wilt laten werken met een netwerk met SSL-inspectie, ga je naar [Netwerken met SSL-inhoudsfilters instellen](#). Hierin wordt uitgelegd hoe je een aangepast rootcertificaat installeert op alle domeingebruikers die inloggen bij de Chromebooks die zijn ingeschreven bij de organisatie.

Accounts en Chrome OS-beleid instellen

Met de Google Beheerdersconsole kun je al je Chrome-apparaten centraal ordenen en beheren. Zodra je gebruikers beheert met de Beheerdersconsole, kun je vanuit het gedeelte Chrome-beheer van de Beheerdersconsole het apparaat- en gebruikersbeleid instellen op basis van de organisatie-eenheid.

Via de apparatenlijst van de Beheerdersconsole vind je een lijst van je Chrome-apparaten en kun je apparaten zoeken en informatie erover bekijken (serienummer, inschrijvingsstatus, einddatum van support, gebruikersnaam bij inschrijving en handmatig ingevulde opmerkingen, zoals de locatie). Als je elk apparaat nader bekijkt op serienummer, kun je ook details bekijken, zoals de geïnstalleerde OS-versie en het MAC-adres van het apparaat en de gebruiker die het laatst heeft ingelogd. Dit apparaatbeleid wordt afgedwongen op elk Chrome-apparaat dat is ingeschreven voor beheer in je domein.

Gebruikersbeleid wordt afgedwongen overal waar je gebruikers inloggen, zowel op ingeschreven als op niet-ingeschreven Chrome-apparaten. Deze instellingen omvatten de mogelijkheid om beveiligingsbeleid in te stellen en te bepalen welke apps gebruikers kunnen downloaden en openen. Zie [Over Chrome OS-apparaatbeheer](#) voor meer informatie.

Belangrijke beleidsoverwegingen

De juiste instellingen voor je school of bedrijf definiëren:

1. Noteer hoe je het Chrome-modelapparaat wilt instellen voor je omgeving.
2. Definieer dezelfde instellingen als het beleid in de Beheerdersconsole met een enkelvoudige organisatie-eenheid voor testen.
3. Nadat de instellingen (zoals de standaardpagina die wordt geladen bij opstarten, webapps die vooraf worden geïnstalleerd of URL's die op de blokkeerlijst worden geplaatst) zijn ingesteld en geverifieerd op Chrome-apparaten in die organisatie-eenheid, kun je die instellingen repliceren in het hele domein.

Voor meer informatie over het gebruik van organisatie-eenheden met Chrome-apparaten ga je naar [Een Chrome-apparaat naar een organisatie-eenheid verplaatsen](#).

Aanbevolen instellingen

In de Beheerdersconsole heb je onder **Apparaatbeheer > Chrome-beheer** toegang tot veel instellingen in **Gebruikersinstellingen** en **Apparaatinstellingen**. Hoewel de meeste organisaties de standaardinstellingen gebruiken, vind je hieronder instellingen die sommige organisaties graag aanpassen.

Toestaan dat ingelogde gebruikers op het apparaat van account wisselen in het browservenster	Je kunt toestaan of blokkeren dat gebruikers in- of uitloggen bij Google-accounts vanuit de browser. Je kunt ook instellen dat gebruikers alleen inloggen bij specifieke Google Workspace-domeinen. Lees meer over Inloggen in de browser .
Opnieuw inschrijven afdwingen	Google raadt aan om deze instelling niet uit te zetten. Met deze instelling dwing je af dat een gewist apparaat opnieuw wordt ingeschreven bij je domein. Als je niet wilt dat een Chrome-apparaat opnieuw wordt ingeschreven bij je domein, moet je het apparaat uitschrijven . Lees meer over gedwongen opnieuw inschrijven .
Schermsgrendeling	Selecteer Scherf altijd automatisch vergrendelen bij inactiviteit om de beveiliging te verhogen en de kans te verkleinen dat iemand de computers van je gebruikers gebruikt terwijl ze afwezig zijn.
Vooraf geïnstalleerde apps en extensies	Kies de webapps die van toepassing zijn voor je gebruikers, zoals Gmail Offline of Google Drive. Je kunt apps altijd op de lijst met geblokkeerde of toegestane apps zetten als je meer controle wilt over welke apps gebruikers kunnen installeren vanuit de Chrome Web Store .
Vastgezette apps	Selecteer welke apps zichtbaar of verborgen zijn op de taakbalk van het systeem. Opmerking: Met deze instelling zijn alleen door de beheerder opgegeven apps toegestaan. Voor gebruikers is hun eigen aangepaste set apps niet meer zichtbaar op de taakbalk van het systeem.

Te laden pagina's bij opstarten	Dit wordt meestal ingesteld op een intranetportal of homepage. Het nadeel van deze instelling is dat de tabbladen op Chrome-apparaten na een herstart niet meer worden hersteld naar de meest recente browsesessie.
Inloggen beperken tot lijst met gebruikers	Als je inloggen beperkt tot <i>*@uwdomein.com</i> kunnen gebruikers niet inloggen met een consumentenaccount van Gmail of een ander niet-domeinaccount. Je kunt bepalen wie mag inloggen bij een beheerd (ingeschreven) Chrome-apparaat.
Alle lokale gegevens, instellingen en de status van gebruikers wissen na uitloggen	Activeer dit niet. Hierdoor wordt het gebruikersbeleid opnieuw gedownload bij elke inlogsessie, dus activeer het alleen als je alle gebruikersstatussen tussen gebruikerssessies wilt wissen van het Chrome-apparaat.
Instellingen voor automatisch updaten	Laat de instellingen voor automatisch updaten op de standaardwaarden staan. Chrome-apparaten voeren zelf elke 6 tot 8 weken een update uit. Er worden dan nieuwe functies toegevoegd en bugfixes en beveiligingspatches toegepast. We raden ook aan dat je 5% van je organisatie op het bèta- of Dev-kanaal houdt om te testen hoe toekomstige releases van Chrome OS functioneren in je organisatie. Bekijk onze lijst met aanbevelingen in Automatische updates voor Chrome-apparaten implementeren. Opmerking: Als je niet wilt dat apparaten op de achtergrond worden geüpdatet voordat ze zijn ingeschreven en opnieuw zijn opgestart, druk je in het scherm 'Licentieovereenkomst eindgebruiker' op Ctrl + Alt + E. Anders worden gedownloade updates die door het beleid moeten worden geblokkeerd, uitgevoerd als de gebruiker het apparaat opnieuw opstart.
Single Sign-on	Organisaties die Single Sign-On (SSO) gebruiken, moeten een test uitvoeren om te checken of een klein aantal gebruikers kan inloggen op hun Chrome-apparaten voordat deze functie wordt uitgerold in de hele organisatie. Als je SSO gebruikt voor inloggen bij Google Workspace op je bestaande apparaten, kun je overwegen Google Workspace Password Sync te gebruiken.

Je apparaten voorbereiden op de implementatie

Voordat je Chrome-apparaten distribueert naar de eindgebruikers, moeten deze worden 'gefaseerd' voor optimaal gebruiksgemak. Het absolute minimum is om de Chrome-apparaten in te schrijven bij je domein voor beheer. Op deze manier kunnen eventuele toekomstige updates in het apparaatbeleid worden toegepast op alle Chrome-apparaten.

Als je een klein aantal apparaten implementeert, raadpleeg je de [Snelstartgids](#) voor gestroomlijnde instructies over het inschrijven en implementeren van je apparaten. Zie de onderstaande instructies als je apparaten implementeert naar een grotere groep, zoals naar meerdere klassen of scholen, of naar meerdere kantoorlocaties.

Chrome-apparaten updaten naar de nieuwste versie

Apparaten met Chrome OS checken automatisch op updates en downloaden deze wanneer ze verbonden zijn met wifi of ethernet. Apparaten worden geüpdatet naar de nieuwste versie, tenzij de beheerder een beperking heeft ingesteld in [Update-instellingen voor apparaat](#). Als je veel apparaten moet updaten en de netwerkbandbreedte wilt behouden, kun je een USB-herstelstick met de nieuwste versie van Chrome OS gebruiken.

Updaten via USB-drives is de meest effectieve en efficiënte manier om images te maken voor honderden of duizenden Chrome-apparaten. Updaten via USB is een goede manier om bandbreedte te besparen, omdat je vanaf elk apparaat een volledige OS-update installeert die groter kan zijn dan 400 MB per apparaat.

Een Chrome OS-image maken

Als je met een USB-stick handmatig Chrome-apparaten wilt updaten naar de nieuwste versie van Chrome OS, heb je het volgende nodig:

1. Informatie over de fabrikant en het model van het Chrome-apparaat dat je wilt updaten.
2. Een flashdrive met USB 2.0 of hoger van 4 GB of meer
3. Chrome-browser die draait op Chrome OS, Microsoft Windows of macOS
4. Installeer [Chromebook-herstelprogramma](#) en kies het juiste merk en model van het apparaat om de USB-herstelstick te maken.

Bekijk [hier](#) meer informatie over het updaten, herstellen of wissen van apparaten.

Opmerking: Bij een stabiele release kan het een week duren voordat deze beschikbaar is in de image-brandtool.

Je apparaten voorbereiden voor inschrijving

Je apparaten voorbereiden en implementeren:

1. [Maak USB-herstelapparaten](#) of update je apparaten draadloos. De USB-methode wordt aanbevolen bij meer dan 10 apparaten.
2. Nadat je de apparaten opnieuw hebt opgestart, selecteer je de taal, het type toetsenbord en het wifi-netwerk.
3. Nadat je de Servicevoorwaarden hebt geaccepteerd en *voordat je inlogt bij het Chrome-apparaat*, druk je op **Ctrl-Alt-E**. Je ziet linksboven Zakelijke inschrijving staan.
4. Vul een gebruikersnaam en wachtwoord in (beheerder of ingeschreven gebruiker van het domein) en klik op **Apparaat registreren**.
Nadat je het apparaat hebt ingeschreven, verschijnt het bericht: Je apparaat is aangemeld voor bedrijfsbeheer.
5. Klik op **Gereed** om terug te keren naar de oorspronkelijke inlogpagina. Onder aan de pagina verschijnt de melding: Dit apparaat wordt beheerd door *uwdomein.com*.

Herhaal deze stappen voor alle Chrome-apparaten in je organisatie. Zie [Chrome-apparaten inschrijven](#) voor meer informatie over apparaatinschrijving.

Uitgebreide voorbereidingsservice voor inschrijving (optioneel)

De uitgebreide voorbereidingsservice is ontworpen voor een implementatie van Chrome-apparaten zonder dat de IT-afdeling eraan te pas komt. De uitgebreide voorbereidingsservice van een reseller heeft als voordeel dat je de Chromebooks gebruiksklaar krijgt. Gebruikers kunnen hun eigen Chrome-apparaat uitpakken of het Chrome-apparaat uit de laptopkar halen en direct productief zijn, zonder dat ze iets hoeven in te stellen. Natuurlijk moeten voor de Chrome-apparaten net zoals voor elke andere computer voor eindgebruikers enkele instellingen worden gedefinieerd in de Beheerdersconsole om het apparaat te koppelen aan het juiste beheerbeleid. Veel officiële resellers van Google Chrome-apparaten bieden deze service voorafgaand aan de verzending.

Je kunt de reseller of een andere organisatie die de uitgebreide voorbereidingsservice voor Chromebooks biedt een niet-beheerdersaccount geven op je Google Workspace-domein. Dit inschrijvingsaccount kan zelfs worden geplaatst in een organisatie-eenheid waarin alle services zijn uitgezet.

De werkelijke stappen van de uitgebreide voorbereidingsservice omvatten mogelijk:

- Chrome OS-versie updaten
- Inschrijven bij Chrome OS-beheer
- Beleid valideren, inclusief vooraf geconfigureerde wifi-netwerken
- Apparaten taggen
- Serienummers graveren in apparaten
- Randapparatuur bundelen

Neem voor meer informatie contact op met je reseller van Google Chrome-apparaten. Als je geen partner hebt, kun je een [Google Cloud Partner](#) bij jou in de buurt zoeken.

Android-apps implementeren op Chrome-apparaten

Als je organisatie gebruikmaakt van [Chrome-apparaten met ondersteuning voor Android-apps](#), kun je installatie afdwingen of bepalen welke Android-apps je gebruikers kunnen downloaden. Je kunt de apps op 3 manieren beschikbaar stellen aan gebruikers:

- Je kunt apps afgedwongen installeren op apparaten
- Je kunt een selectie van apps maken die je gebruikers mogen downloaden
- Je kunt gebruikers toegang geven tot de hele content van de Managed Google Play Store (niet ondersteund voor Chrome Education-klanten)

Lees meer over het activeren van Android-apps voor Chrome-apparaten in je domein en het goedkeuren van apps voor je gebruikers in [Android-apps gebruiken op Chrome-apparaten](#).

Voordat je begint

- Google adviseert om Android-apps voor Chrome-apparaten te testen in een testorganisatie-eenheid (OE) voordat je ze naar iedereen uitrolt. Als je ze niet langer wilt gebruiken, kun je ze uitzetten en je apparaten blijven gebruiken zoals voorheen.
- Zie [Veelgestelde vragen over Android-apps op Chrome](#) voor meer informatie die mogelijk relevant is voor je implementatie.

Android-apps uitvoeren in kioskmodus

Je kunt je [Google Beheerdersconsole](#) gebruiken om [Android-apps te installeren op beheerde Chrome-apparaten in de vergrendelde kioskmodus](#). Hiermee kun je een Android-app implementeren op een kioskapparaat en instellen dat deze automatisch opstart.

Lokaal afdrukken met Chrome-apparaten

Chrome OS ondersteunt lokaal afdrukken waarmee gebruikers eenvoudig direct verbinding kunnen maken met printers en printerservers, zonder dat toegang tot cloudgebaseerde infrastructuur nodig is. Chrome gebruikt Common UNIX Printing System (CUPS) voor ondersteuning van lokaal afdrukken en het Internet Printing Protocol (IPP) voor afdrukken naar lokale printers en netwerkprinters.

Als Beheerder kun je de Google Beheerdersconsole gebruiken om CUPS in te stellen. Als je een printer toevoegt, verschijnt deze automatisch voor je gebruikers in de lijst met Chrome-printers. Ze kunnen dus afdrukken zonder dat ze iets hoeven in te stellen. Zie [Lokale printers en netwerkprinters beheren](#).

CUPS ondersteunt printers van veel en zeer diverse fabrikanten, en ondersteunt afdrukken op lokale printers en netwerkprinters.

Voor meer informatie over aanvullende printopties in Chrome OS ga je naar [Afdrukken op Chrome-apparaten](#).

Externe toegang en virtualisatie (optioneel)

Je kunt je Chrome-apparaten gebruiken voor toegang tot traditionele, verouderde apps wanneer gebruikers toegang nodig hebben tot:

- Verouderde client-apps zoals Microsoft® Office®
- Webpagina's waarvoor oudere of alleen Microsoft-technologieën nodig zijn (bijvoorbeeld Internet Explorer)
- Plug-ins ouder dan Flash (bijvoorbeeld Java®-plug-ins of Silverlight) voor webapps

Belangrijkste functies

Met virtualisatie-apps kun je je verouderde apps uitvoeren op Chrome-apparaten of je Chrome-apparaten gebruiken met je bestaande, gevirtualiseerde app-infrastructuur. Er zijn verschillende oplossingen beschikbaar die gebruikmaken van gangbare protocollen voor externe toegang. Een voorbeeld:

- [Citrix Workspace](#)
- [VMware Horizon Client for Chrome](#)
- [ChromeRDP](#)

Er zijn ook app-virtualisatieoplossingen zoals [Chromotif](#) en [Fra.me](#) die goed werken op Chrome OS.

Overwegingen voor app-hosting

Als de apps die je wilt gebruiken zich op een andere locatie kunnen bevinden (bijvoorbeeld Microsoft® Office 365, Oracle® Cloud-apps of gehoste SaaS-apps), is een gehoste oplossing meestal het eenvoudigst te implementeren. Hiervoor hoeft je geen server in te stellen.

Als de app die je wilt gebruiken moet worden gehost binnen je firewall of als je je bestaande servers of VDI-oplossingen (virtueledesktop-infrastructuur) wilt gebruiken, werken deze oplossingen mogelijk beter:

- [VMware Horizon™ DaaS®](#)
- [Chrome Remote Desktop](#)

Speciale scenario's voor implementatie van Chrome-apparaten

Chrome-apparaten kunnen worden gebruikt in zeer uiteenlopende situaties. Door hun lage kosten, externe beheer en minimale onderhoud worden ze vaak geïmplementeerd voor specifieke bedrijfs- en schooltoepassingen. Deze scenario's variëren van het tonen van een schoolagenda op een digitaal bord tot het delen van laptops in een bibliotheek en het beheren van toetsen. Zie de onderstaande links voor meer bronnen over het implementeren van Chrome-apparaten op een manier die het best aansluit bij je behoeften.

Cloudwerker

Chrome-apparaten zijn ideaal voor bedrijfsmedewerkers. Een Chrome-apparaat kan worden toegewezen aan gebruikers als hun fulltime-apparaat voor toegang tot webapps en productiviteitstools en om samen te werken met collega's.

Als je meer wilt weten over hoe je cloudwerkers kunnen werken met Chrome Enterprise, bekijk je deze video's op [Cloud Worker Live](#).

Kiosk-app voor één doel

Je kunt een kiosk-app voor één doel maken, bijvoorbeeld om een klant een kredietaanvraag te laten invullen, een enquête te laten invullen in een winkel of om leerlingen te registreren. [Meer informatie](#)

Kiosken voor beheerde gastsessies

Je kunt kiosken voor beheerde gastsessies instellen voor locaties, zoals een pauzeruimte voor medewerkers, winkelschermen of als een gedeeld apparaat in een bibliotheek. Hier hoeven gebruikers dan niet in te loggen om het Chrome-apparaat te gebruiken. [Meer informatie](#)

Digitale borden

Je kunt Chromeboxes gebruiken voor digitale borden, zoals schoolagenda's, digitale billboards, restaurantmenu's en interactieve games. Je kunt een gehoste of verpakte app maken en deze starten op volledig scherm in de kioskmodus voor één app. [Meer informatie](#)

Proefwerken en toetsen

Chromebooks vormen een beveiligd platform om toetsen voor leerlingen te beheren. Als de apparaten goed zijn ingesteld, voldoen ze aan de toetsnormen voor het basisonderwijs en middelbaar onderwijs. Met Chromebooks kun je de toegang van leerlingen tot het internet tijdens een toets uitzetten. Daarnaast kun je externe opslag, screenshots en de mogelijkheid om af te drukken uitzetten.

Je kunt Chromebooks voor toetsen op diverse manieren instellen, afhankelijk van de aard van de toets: als een kiosk voor één app, op een domein van de toetsaanbieder of via kiosken voor beheerde gastsessies. Zie [Chromebooks gebruiken voor toetsen en proefwerken](#) voor meer informatie.

Checklist voor implementatie

☐ Netwerkinfrastructuur	Heb je een wifi-infrastructuur en bandbreedte waarmee al je apparaten gelijktijdig verbinding kunnen maken met het internet? • Wat is je huidige bandbreedtegebruik, dus voordat je Chrome-apparaten toevoegt? Voldoet je bandbreedte aan de geschatte behoefte? • Zijn er gedeelten in het gebouw zonder wifi-dekking?
☐ Verouderde apps versus webapps	Hoeveel van je gebruikers hebben verouderde apps nodig in plaats van webapps? Wil je meer webapps en online bronnen voor je gebruikers? Zo ja, wat is je tijdlijn?
☐ Gebruik van plug-ins	Weet je welke plug-ins vereist zijn voor toegang tot de sites die je gebruikers nodig hebben? Moet je hiervoor een externe oplossing instellen? Meer informatie
☐ Printers	Heb je je printers ingesteld voor lokaal afdrukken (CUPS)? Mogen al je gebruikers afdrukken of alleen sommige ervan?
☐ Randapparatuur	Heb je geverifieerd of de randapparaten die je gebruikers nodig hebben werken met je Chrome-apparaten? Test bijvoorbeeld je headsets, barcodescanners en de andere randapparaten die je wilt implementeren voordat je deze uitrolt naar deze gebruikers.
☐ Verificatieschema	Hoe loggen gebruikers in op hun computers? Hoe beheer je wifi-wachtwoorden en toegang tot je wifi-netwerk? Vertrouw je op SSO voor de verificatie van Chrome-apparaten? Gebruik je ook Google Workspace Password Sync (GSPS)? Gebruik je Cloud Identity?
☐ Mijlpaaldata van project	Heb je een tijdlijn voor de uitrol? Heb je een manier om gebruikers feedback te geven over hun gebruik van Chrome-apparaten? Hoe lang is je evaluatieperiode, welke typen enquêtes laat je gebruikers doen en hoe vaak verzamel je gebruiksgegevens en andere gebruikersfeedback?
☐ Training voor gebruikers	Als je overstapt vanaf een ander platform naar Chromebooks, geef je dan een training voor de gebruikers? Als je een trainingsafdeling hebt, kun je de training intern maken. Anders kun je door sommige Google Cloud Premier Partners een Chromebook-training laten verzorgen.
☐ Gereedheid voor helpdesk	Is je helpdesk bekend met het Helpcentrum van Chrome Enterprise? Door de bronnen op de volgende pagina te lezen en deel te nemen aan trainingen, kunnen je helpdesk- en IT-medewerkers bekend raken met vragen over Chromebook.

Aanvullende bronnen en support

Nieuws over Chrome-apparaten bijhouden

- Volg het [Google Chrome-blog](#) en [Chrome-releasesblog](#)
- Volg [release-opmerkingen van Chrome Enterprise](#)

Google Workspace-klanten kunnen ook het volgende bekijken:

- Google Workspace-[website over nieuwe functies](#)
- [Google Cloud-blog](#)

Helpcentrum bekijken

- [Chrome Enterprise](#)
- [Chromebook \(eindgebruiker\)](#)
- [Chromebox voor vergaderingen](#)
- [Inloggen bij de Beheerdersconsole](#)

Tips om zelf support te bieden

- [Logboeken van Chrome-apparaten verzamelen](#)
- [Problemen met Chromebooks oplossen \(Chromebook-consumenten\)](#)
- [Bekende problemen \(Chrome Enterprise\)](#)
- [Log Analyzer](#) (Google Workspace Toolbox)—Analyseren `/var/log/messages` en `/var/log/chrome/` voor fouten
- [Toetsen beheren op Chromebooks](#)

Support krijgen

We bieden support via telefoon en e-mail voor problemen die je hebt met software en services voor Chrome-apparaten. [Zie onze support-opties voor Chrome-apparaten](#).