

Het beheer van de Chrome-browser vereenvoudigen en centraliseren in de cloud

Inleiding

Naarmate meer medewerkers van organisaties in browsers werken, wordt het steeds belangrijker voor IT-teams om de browseromgeving te beheren en te beveiligen. Het kan een hele uitdaging zijn om combinaties van verschillende apparaten, besturingssystemen en vereisten voor beveiliging en naleving te balanceren met de behoefte van gebruikers aan snelle, betrouwbare en altijd beschikbare toegang tot web-apps.

In deze whitepaper lees je meer over hoe je via Cloudbeheer voor de Chrome-browser

het beheer van Chrome-browsers op alle grote computerbesturingssystemen kunt centraliseren.

We gaan het eerst hebben over de uitdagingen die je kunt tegenkomen als het gaat om browserbeheer.

Veel bedrijven hebben **geen standaardbrowser ingesteld** en gebruiken veel verschillende soorten oudere en moderne browsers. Hierdoor is het moeilijk om ervoor te zorgen dat elke browser up-to-date is en dat de juiste beleidsregels worden toegepast.

Omdat oudere en moderne browsers beleidsregels vaak verschillend implementeren op basis van het besturingssysteem waarop deze browsers worden gebruikt, moet je vaak **elke browser op elk besturingssysteem afzonderlijk beheren**. Dit is een complex en tijdrovend karwei.

Gebruikers kunnen browserextensies of plug-ins installeren zonder dat het IT-team hiervan op de hoogte is. Niet-goedgekeurde extensies en plug-ins kunnen verouderd raken en/of voldoen mogelijk niet aan interne vereisten voor beveiliging en naleving, waardoor het lastig wordt om risico's te beperken. Daarnaast kan

het **gebrek aan zichtbaarheid** wat betreft het aantal browsers in gebruik, de versie van elke browser en de apparaten waarop de browsers worden gebruikt, leiden tot risico's op het gebied van beveiliging en naleving.

Door Chrome-browsers centraal voor alle besturingssystemen te beheren, beschik je niet alleen over één plek waar je eenvoudig beleidsregels kunt instellen en toepassen, maar ook over informatie en inzichten die je nodig hebt om de beveiliging te garanderen en betere besluiten te nemen.

Gecentraliseerd browserbeheer met de Chrome-browser

Cloudbeheer voor de Chrome-browser is een gecentraliseerde, cloudgebaseerde console die je een uniforme manier biedt om meerdere versies en exemplaren van de Chrome-browser op Windows¹, Mac² en Linux te beheren. Cloudbeheer voor de Chrome-browser is toegankelijk via de Google Beheerdersconsole (die ook wordt gebruikt om Chrome OS en G Suite te beheren) en zorgt ervoor dat je geen verschillende beheertools hoeft te gebruiken voor verschillende besturingssystemen als je de Chrome-browser binnen je organisatie wilt beheren.

De console voor Cloudbeheer voor de Chrome-browser bevat gedetailleerde informatie over de Chrome-browsers die in je organisatie zijn geïnstalleerd. Door de informatie te analyseren en actie te ondernemen, kun je

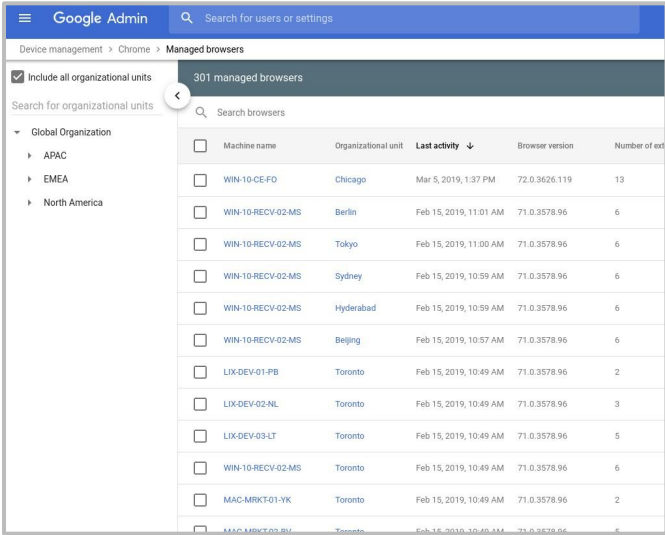
de beveiliging verbeteren, zorgen voor meer naleving en betere IT-beslissingen nemen.

Je kunt in één oogopslag kritieke gegevenspunten bekijken, zoals welke Chrome-versies zijn geïnstalleerd, hoeveel exemplaren van elke versie worden gebruikt, de typen apparaten en de besturingssystemen waarop Chrome wordt gebruikt, welke extensies er zijn geïnstalleerd, en welke beleidsregels voor elke instantie zijn toegepast en afgedwongen. Met een paar muisklikken kun je witte en zwarte lijsten voor extensies beheren. Ook kun je extensies toestaan (of juist niet) voor betere aansluiting op de bedrijfsrichtlijnen. Dankzij op rollen gebaseerd toegangsbeheer kunnen beheerders aangeven welke gebruikers toegang hebben tot specifieke functies of ze toepassen op bepaalde organisatie-eenheden. Aangezien

¹ Microsoft®, Windows® en Internet Explorer® zijn gedeponeerde handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen.

² Mac en macOS zijn handelsmerken van Apple Inc., gedeponeerd in de Verenigde Staten en andere landen.

de cloudinterface eenvoudig te gebruiken is, kan het IT-team het browserbeheer overdragen aan geschikte leden van het team. Cloudbeheer voor de Chrome-browser werkt met grote identiteitsproviders, zoals Microsoft Active Directory, Microsoft Azure Directory, Google Cloud Identity en alle andere SSO-services die een SAML 2.0-interface bieden. Als je al G Suite-klant bent, vind je het vast fijn om te horen dat Cloudbeheer voor de Chrome-browser niet vereist dat gebruikers met hun Google-account inloggen op de browser.



Machine name	Organizational unit	Last activity	Browser version	Number of extensions
WIN-10-CE-FD	Chicago	Mar 5, 2019, 1:37 PM	72.0.3626.119	13
WIN-10-RECY-02-MS	Berlin	Feb 15, 2019, 11:01 AM	71.0.3578.96	6
WIN-10-RECY-02-MS	Tokyo	Feb 15, 2019, 11:00 AM	71.0.3578.96	6
WIN-10-RECY-02-MS	Sydney	Feb 15, 2019, 10:59 AM	71.0.3578.96	6
WIN-10-RECY-02-MS	Hyderabad	Feb 15, 2019, 10:59 AM	71.0.3578.96	6
WIN-10-RECY-02-MS	Beijing	Feb 15, 2019, 10:57 AM	71.0.3578.96	6
LIX-DEV-01-PB	Toronto	Feb 15, 2019, 10:49 AM	71.0.3578.96	2
LIX-DEV-02-NL	Toronto	Feb 15, 2019, 10:49 AM	71.0.3578.96	3
LIX-DEV-03-LT	Toronto	Feb 15, 2019, 10:49 AM	71.0.3578.96	5
WIN-10-RECY-02-MS	Toronto	Feb 15, 2019, 10:49 AM	71.0.3578.96	6
MAC-MRKT-01-YK	Toronto	Feb 15, 2019, 10:49 AM	71.0.3578.96	2
MAC-MRKT-02-YK	Toronto	Feb 15, 2019, 10:49 AM	71.0.3578.96	2

Afbeelding 1: Homepage van Cloudbeheer voor de Chrome-browser

Wat kun je zien en doen via Cloudbeheer voor de Chrome-browser?

Cloudbeheer voor de Chrome-browser biedt inzichten in de volgende vier aspecten: browsers, gebruikersinstellingen, app-instellingen en de lijst met browserextensies. Zodra browsers zijn ingeschreven, kunnen IT-teams informatie bekijken die eerder mogelijk niet zichtbaar was.

Beheerders kunnen apparaten groeperen per domein (zoals example.com). Als je al gebruikmaakt van G Suite, Enterprise-support voor de Chrome-browser, Chrome Enterprise Upgrade of Cloud Identity, of als je al Chrome-apparaten beheert, kun je je bestaande domein gebruiken voor het beheer van Chrome-browsers.

Als je geen G Suite-beheerabonnement of Chrome Enterprise Upgrade hebt, kun je eenvoudig [een opgegeven domein instellen](#). Dit is een domein van Google dat aan je wordt toegewezen. Via deze optie kun je Cloudbeheer voor de Chrome-browser uitproberen. (Onthoud dat als je voor de optie kiest om een Google-domein te gebruiken, je Chrome 73 of hoger moet gebruiken op de apparaten die je wilt beheren. De kanalen Dev, Beta en Stable worden ondersteund. Canary wordt niet ondersteund.)

Beheer van gebruikersinstellingen, beleidsregels en extensies

Veel organisaties hebben niet door dat ze uit honderden beleidsregels kunnen kiezen om de Chrome-browser te configureren voor aansluiting op specifieke browser- en beveiligingseisen. Met Cloudbeheer voor de Chrome-browser kun je eenvoudig met een paar klikken beleidsregels op gebruikersniveau instellen en toepassen. Dit omvat het beheer van witte en zwarte lijsten voor apps en extensies, toepassing van beveiligingsinstellingen zoals of gebruikers de wachtwoordmanager van Chrome kunnen gebruiken, en specificatie van of en hoe gebruikers toegang hebben tot specifieke typen content (zo kun je 3D-content toestaan en blokkeren).

Via het gedeelte met gebruikersinstellingen kun je gemakkelijk meerdere Chrome-browsergebruikers beheren, omdat je met een paar muisklikken instellingen kunt toepassen op het niveau van afzonderlijke gebruikers, op het niveau van de organisatie-eenheid of zelfs op alle gebruikers binnen de organisatie. Cloudbeheer voor de Chrome-browser ondersteunt meerdere niveaus voor beleidsbeheer. Het is daarom van belang dat je de verschillende beleidstypen bekijkt en een beleidsmodel hanteert dat het beste bij jouw organisatie past. Je kunt de toegepaste browserbeleidsregels bekijken, net als via welke bron de beleidsregels zijn toegepast (lokale machine of cloudbeleid), de status van beleidsregels en de toegepaste waarde van een beleidsregel.

Apparaatbeleidsregels worden als eerste toegepast, gevolgd door gebruikersbeleidsregels van het besturingssysteem, het cloudbeleid en het Chrome-profiel.

Extension name	Version	Install type	Installed ↓	Disabled	Forced	Permissions
 SecureConnect Reporting		unknown	192	0	0	0
 Slides	0.1	unknown	168	0	0	0
 Google Docs Offline	1.7	multiple	157	0	0	8
 Sheets	1.2	multiple	157	0	0	0
 Google Play Music	1.396.0	unknown	156	0	0	0
 Docs	0.1	unknown	144	0	0	0
 Google Voice Search Hotword	0.1.1	unknown	132	0	0	0
 Policy Notifier	1.1.4	unknown	108	0	0	0
 Password Alert	1.26	unknown	96	0	0	0
 Chrome Remote Desktop	70.0.3538.21	unknown	96	0	0	0
 Password Alert	1.27	unknown	72	0	0	0
 Chrome Remote Desktop		unknown	60	0	0	0

Afbeelding 2: Voorbeeld van de weergave voor Chrome-extensies in de lijst met browserextensies

Block Extensions by Permission

Locally applied

Permissions and URLs

Block extensions by permissions and URLs. [Learn more](#)

If the extension uses one of the selected permissions, block:

☐ Alarms
☐ Clipboard Write
☐ Enterprise Device Attributes
☐ File System
☐ Detect Idle
☐ Media Galleries
☐ Notifications
☐ Platform Keys
☐ Memory Metadata
☐ 2-Factor Devices
☐ Video Capture

☐ Audio Capture
☐ Context Menus
☐ Experimental APIs
☐ File System Provider
☐ Identity
☐ Native Messaging
☐ Printers
☐ Storage
☐ Network Metadata
☐ Text to Speech
☐ VPN Provider

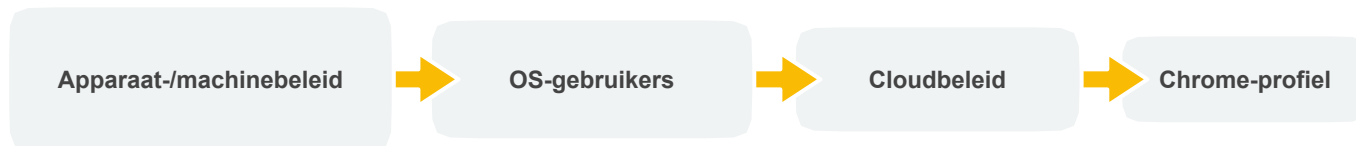
☐ Certificate Provider
☐ Desktop Capture
☐ Fullscreen Apps
☐ HID
☐ Google Cloud Messaging
☐ Captive Portal Authenticator
☐ Sync File System
☐ Display Metadata
☐ Unlimited Storage
☐ Web Requests

☐ Clipboard Read
☐ Document Scan
☐ File Browser Handler
☐ Override Fullscreen
☐ Escape Geo Location
☐ Power
☐ Set Proxy
☐ CPU Metadata
☐ Storage Metadata
☐ USB
☐ Block Web Requests

Blocked URLs

Allowed URLs

Afbeelding 3: Voorbeeld van extensieblokkering via rechten in de gebruikersinstellingen



Beleidsregels die zijn toegepast op de organisatie-eenheid van het hoogste niveau worden ook toegepast op de beheerde Chrome-browsers in de onderliggende organisatie-eenheden. Je kunt deze regels echter overschrijven via de verschillende opties in de console voor verschillende configuraties van organisatie-eenheden.

Cloudbeheer voor de Chrome-browser biedt ook een overzicht van de status van extensies binnen je organisatie. Zo heb je inzicht in elke extensie die in de organisatie en op elk apparaat is geïnstalleerd, en kun je informatie controleren over de extensies, waaronder de rechten. Met één klik kun je extensies gedwongen installeren, toestaan of verwijderen in je omgeving.

Inzichten en rapportage voor browsers

Veel bedrijven weten heel weinig over de browserimplementaties binnen hun organisatie. Met Cloudbeheer voor de Chrome-browser kun je een lijst bekijken van apparaten waarop momenteel beheerde Chrome-browserinstanties zijn geïnstalleerd. Daarnaast kun je gedetailleerdere informatie voor elke instantie inzien. Zo kun je de naam, versie van het besturingssysteem, gebruikersinformatie,

architectuur (32- of 64-bits) en inschrijvingsdatum van een beheerde machine bekijken. Ook kun je elke instantie en versie van de Chrome-browser op de machine zien, net als welk releasekanaal (Stable, Dev, Beta of Canary) de versie gebruikt, aan welke profielen de installatie is gekoppeld en welke Chrome-browserbeleidsregels zijn toegepast op de instantie.

Machine info		
Machine name	OS version	Enrollment date
WIN-10-CE-FO	Windows 10 (10.0.17763.316)	Feb 26, 2019
Machine user	Architecture	Machine Policies
ALPHAHQ\adminalpha	x86_64	12
Serial Number	Device ID	
6525-8116-0713-4454-6709-9753-41	a86edd53-a04b-4602-ba12-ee1cf1033cf5	

Afbeelding 4: Voorbeeld van apparaatgegevens die in rapporten kunnen worden opgenomen

Aan de slag

Als je al gebruikmaakt van G Suite, Enterprise -support voor de Chrome-browser, Chrome Enterprise Upgrade of Cloud Identity, heb je via de console al toegang tot Cloudbeheer voor de Chrome-browser. Je vindt deze mogelijkheid in het gedeelte Apparaatbeheer. Alle andere beheerders kunnen Cloudbeheer voor de Chrome-browser uitproberen door [een account te maken](#). Aangezien je de browser op apparaatniveau beheert, hebben gebruikers geen eigen account nodig. Met Cloudbeheer voor de Chrome-browser hoeven gebruikers niet over een Google-account te beschikken om zich in te schrijven, omdat de apparaten kunnen worden beheerd via inschrijvingstokens. Inschrijvingstokens worden uitsluitend gebruikt tijdens het inschrijvingsproces en bevatten globale, unieke identifiers (GUID's) die willekeurig door beheerders worden gegenereerd via de console voor Cloudbeheer voor de Chrome-browser. Deze tokens kunnen worden gebruikt voor bulksgewijze registratie of voor registratie van één apparaat.

Conclusie

Cloudbeheer voor de Chrome-browser vereenvoudigt de manier waarop je Chrome-browsers binnen de organisatie-omgeving beheert. De gecentraliseerde interface biedt inzicht in de browsers binnen je organisatie en biedt je de mogelijkheid om de beveiliging en naleving voor je medewerkers te verbeteren. Je hoeft geen afzonderlijke browserbeleidsregels meer te beheren voor Windows-, Mac-, Linux- en Chrome OS-gebruikers.

Je kunt honderden beleidsregels instellen en beheren, en alle instanties van de Chrome-browser beheren via één centrale cloudportal, ongeacht het platform dat je gebruikers gebruiken.

Voer deze drie stappen uit om vandaag nog aan de slag te gaan met Cloudbeheer voor de Chrome-browser:

- 1 [Meld je aan](#) om te starten met de inschrijving van browsers
- 2 Raadpleeg de [documentatie](#) voor specifieke stappen
- 3 Neem contact op met onze [Chrome Enterprise-browserexperts](#)

Raadpleeg de volgende informatiebronnen voor meer inzicht in Cloudbeheer voor de Chrome-browser:

Bekijk de opties voor [Cloudbeheer voor de Chrome-browser](#)

Lees meer over [hoe je Cloudbeheer voor de Chrome-browser](#) kunt implementeren

Downloads voor [Chrome Enterprise-browsers](#)
Meer informatie over [Enterprise Support voor de Chrome-browser](#)

Bekijk de [lijst met beleidsregels voor de Chrome-browser](#)

Lees de nieuwste [release-opmerkingen voor de Chrome Enterprise-browser](#)

Blijf up-to-date met de nieuwste release-updates voor de Chrome-browser via de [Chrome Releases-blog](#)

Bezoek het [Helpcentrum voor Chrome Enterprise-browsers](#) en het [Helpforum voor de Chrome-browser](#)

Bekijk de [openbare bugtracker voor de Chrome-browser](#)