Beveiligingsinstellingen voor Google Workspace

Document opgesteld door	SIVON www.sivon.nl info@sivon.nl
Met dank aan	Google

Versie beheer

Datum	Versie	Wijziging
24 juni 2022	1.0	

Inhoudsopgave

Inleiding

Bedrijven en overheden die persoonsgegevens gebruiken, moeten deze volgens de Algemene verordening gegevensbescherming (AVG) beveiligen. Zo voorkomen ze datalekken. Volgens de AVG moeten bedrijven en overheden hiervoor passende technische en organisatorische maatregelen nemen:

- organisaties moeten moderne techniek gebruiken om persoonsgegevens te beveiligen.
- Verder moeten ze niet alleen naar de techniek kijken, maar ook naar hoe ze als organisatie met persoonsgegevens omgaan. Wie heeft er bijvoorbeeld toegang tot welke gegevens?

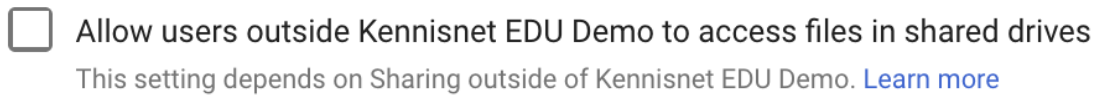
Google geeft veel aandacht aan beveiliging van haar diensten.
Maar u kunt zelf ook wat doen. Met onderstaande Google Workspace instellingen brengt u de informatie beveiliging op een hoger niveau.

Rechten voor delen instellen voor Drive-gebruikers

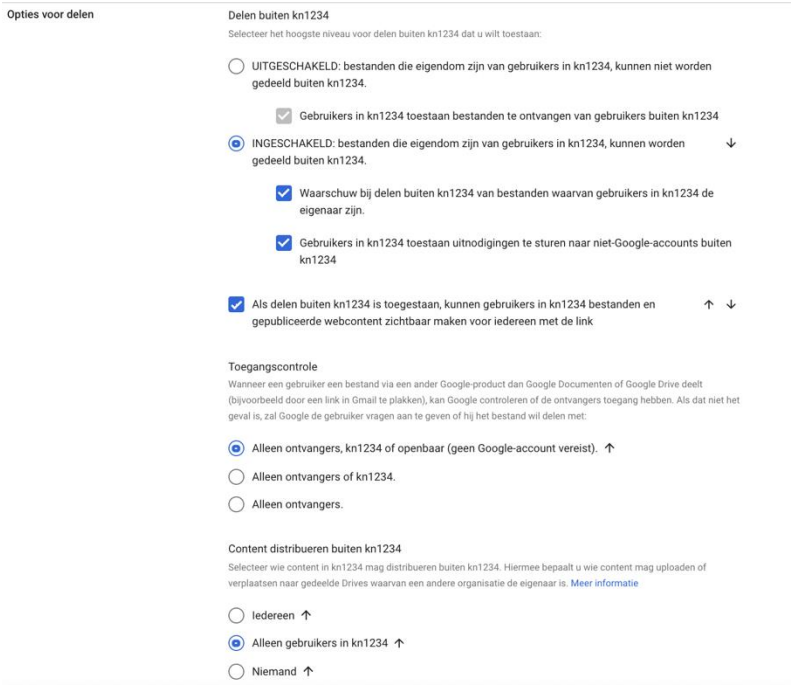
Als beheerder kunt u bepalen hoe gebruikers in uw organisatie Google Drive-bestanden en -mappen kunnen delen. Dit geldt voor Google Documenten, Spreadsheets, Presentaties, mappen en andere in Drive opgeslagen items.

In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Drive en Documenten -> Instellingen voor delen

Als delen buiten uw organisatie is toegestaan, kunnen gebruikers in uw organisatie bestanden en gepubliceerde webcontent zichtbaar maken voor iedereen met de link. Dit kunt u uitzetten, maar dat beperkt de functionaliteit.



Als u deze functionaliteit ingeschakeld “bestanden die eigendom zijn van gebruikers in uw organisatie, kunnen worden gedeeld buiten uw organisatie.” Dan moet u selecteren alleen gebruikers in uw organisatie mogen content distribueren.



Gebruikers toestaan gedeelde Drives te maken

In de default setting kunnen gebruikers geen share drive maken. Als het account van deze gebruiker verwijderd wordt, wordt ook alle drive opslag verwijderd. Door shared drive toe te staan kan verlies van data voorkomen worden. Als u wilt dat gebruikers gedeelde Drives kunnen maken, haalt u het vinkje weg bij “Voorkomen dat gebruikers in uw organisatie nieuwe gedeelde Drives kunnen maken.” Pas deze instelling alleen toe voor medewerkers en niet voor leerlingen.

Een voorbeeld is een docent die lesmateriaal in een shared drive heeft staan om bestanden te delen met anderen docenten. Als u deze instelling niet toe past zal na verwijderen van het account van deze docent verwijdert de andere docenten geen toegang meer hebben tot de bestanden in de shared drive.

Google Drive sharing instellingen

Alleen beheerders zouden rechten moeten hebben om shared drive settings te wijzigen.

In admin.google.com ga naar: Apps > Google Workspace -> Drive en Documenten -
> aanmaken shared drive -> voorkom volledige toegang

Alleen leden moeten toegang hebben tot de inhoud van een shared drive.

In admin.google.com ga naar: Apps > Google Workspace -> Drive en Documenten -
> aanmaken shared drive -> voorkom dat niet-leden toegang hebben

Voorkom delen buiten de organisatie

In admin.google.com ga naar: Apps > Google Workspace -> Drive en Documenten -> Haal vinkje weg bij “Allow users outside Kennisnet EDU Demo to access files in shared drives”

Alleen eigenaar moeten standaard toegang hebben tot bestanden die ze creëren.

General Access
In admin.google.com ga naar: Apps > Google Workspace -> Drive en Documenten -> instellingen voor delen -> Standaard voor links delen.
Uitgeschakeld: Alleen de eigenaar heeft toegang totdat deze het bestand deelt

Gmail beveiliging

Instellingen om Spam, spoofing en phishing voorkomen.

https://support.google.com/a/topic/9061731

E-mailspoofing houdt in dat de inhoud van een e-mail wordt gewijzigd, zodat het lijkt alsof het bericht van iemand anders of ergens anders afkomstig is. Verificatie zorgt dat spammers uw domein of organisatie niet kunnen nabootsen in spoofing- en phishingmails.

Activeer DKIM zodat voor de geselecteerde domeinen het DKIM-protocol (DomainKeys Identified Mail) wordt gebruikt om uitgaande e-mails te verifiëren. DKIM voegt een versleutelde digitale handtekening toe aan elk bericht dat vanuit uw organisatie wordt gestuurd. Ontvangstmailservers gebruiken een openbare sleutel om de handtekening te lezen en te controleren of het bericht echt van u afkomstig is. DKIM zorgt ook dat de inhoud van berichten niet kan worden gewijzigd als ze van de ene server naar de andere worden gestuurd.
U activeert DKIM door een key te genereren en deze in uw MX records van uw DNS server op te slaan en deze te laten verifiëren door Google. De DNS records kunt u wijzigen in de beheer console van uw domein leverancier. U moet dus de inloggegevens voor uw domeinhostaccount hebben. https://support.google.com/a/answer/174126?hl=nl

Met Sender Policy Framework (SPF) kunt u de servers en domeinen opgeven die e-mails mogen sturen namens uw organisatie. Zo kunnen ontvangstservers controleren of berichten echt van u afkomstig zijn.
U activeert SPF door een key te genereren en deze in uw MX records van uw DNS server op te slaan en deze te laten verifiëren door Google. De DNS records kunt u wijzigen in de beheer console van uw domein leverancier.
Als alle e-mails uit uw organisatie alleen worden verstuurd via Google Workspace, plaatst u de volgende TXT record in de DNS records van uw domein hosting partij. U moet dus de inloggegevens voor uw domeinhostaccount hebben.
v=spf1 include:_spf.google.com ~all
Als u naast Google Workspace e-mails stuurt via andere servers of services van derden, moet u een aangepaste SPF-record maken waarin deze afzenders worden geautoriseerd. Dat ziet er bijvoorbeeld zo uit:
v=spf1 include:_spf.google.com include:anotherserver.nl ~all

DMARC laat de ontvangstservers weten wat ze moeten doen met berichten uit uw organisatie die niet door de SPF- of DKIM-controle komen. DMARC stuurt u ook rapporten waarin u kunt zien welke berichten door de SPF- en DKIM-controle zijn gekomen en welke niet. Zo kunt u mogelijke e-mailaanvallen en andere kwetsbare plekken identificeren. Als u SPF en DKIM niet instelt voordat u DMARC inschakelt, leidt dit in veel gevallen tot bezorgingsproblemen voor berichten die vanuit uw domein worden gestuurd. Wacht 48 uur nadat u SPF en DKIM heeft ingesteld voordat u DMARC instelt.
U schakelt DMARC in bij uw domeinhost, niet in de Google Beheerdersconsole. U moet dus de inloggegevens voor uw domeinhostaccount hebben.
Met https://toolbox.googleapps.com/apps/main/ kunt u de instellingen van de MX (mail) records voor uw domein verifiëren. Als uw domein een DMARC-record heeft, is er een TXT-record die begint met v=DMARC.

Aanvullende instellingen

In de admin console activeer de aanvullende instellingen om het aantal phishing aanvallen te verminderen.

Sta delegatie niet toe

Niet toestaan dat gebruikers andere gebruikers in het domein machtigen voor toegang tot hun postvak.
In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Gmail -> Gebruikersinstellingen.

Voor non personal account of generieke accounts zoals info@..., finance@..., etc kan het wel handig zijn om delegatie toe te staan. Creëer hiervoor een organisational unit of group met afwijkende settings.

Activeer quarantaine

Quarantaines kunnen helpen spam te voorkomen, gegevensverlies minimaal te houden en vertrouwelijke gegevens te beschermen. Ze kunnen ook helpen bij de controle van berichtbijlagen, zodat gebruikers niet iets verzenden, openen of ergens op klikken waarvan dit niet de bedoeling is. Als een bericht in quarantaine wordt geplaatst, wordt het bezorgd in de beheerdersquarantaine, waar een beheerder de regel kan bekijken waardoor het bericht in quarantaine is geplaatst.

Blokkeer bijlage met onnodige bestandstypes

Filter mail op scripts, encypted en andere ongewenste bijlages

Links en externe afbeeldingen

In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Gmail -> Veiligheid
Activeer de onderstaande instellingen

- Links achter ingekorte URL’s identificeren
- Gelinkte afbeeldingen scannen
- Waarschuwingsmelding weergeven wanneer wordt geklikt op links naar niet-vertrouwde domeinen
- Toekomstige aanbevolen instellingen automatisch inschakelen.

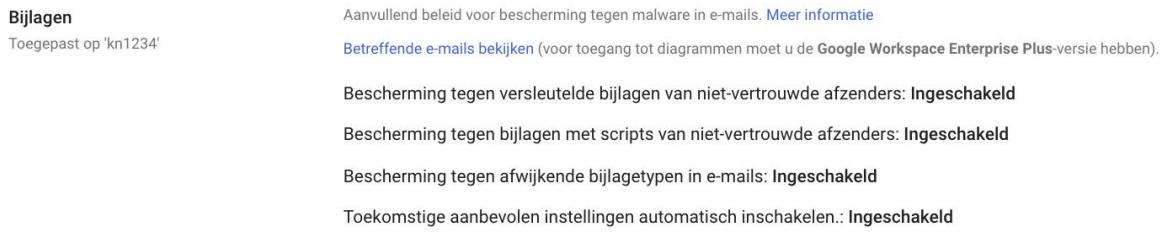
Bescherming tijdens bekijken in IMAP-accounts

In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Gmail -> Veiligheid

Schakel “Linkbescherming inschakelen voor berichten die worden geladen via het IMAP-protocol.” In. Deze functie kan berichtlinks scannen wanneer erop wordt geklikt.

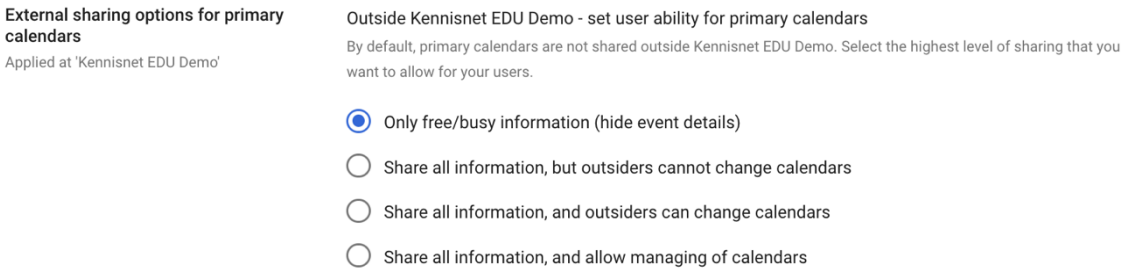
Bijlagen
In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Gmail -> Veiligheid activeer de volgende maatregelen

- Bescherming tegen versleutelde bijlagen van niet-vertrouwde afzenders
- Bescherming tegen bijlagen met scripts van niet-vertrouwde afzenders
- Bescherming tegen afwijkende bijlagetypen in e-mails
- Toekomstige aanbevolen instellingen automatisch inschakelen.

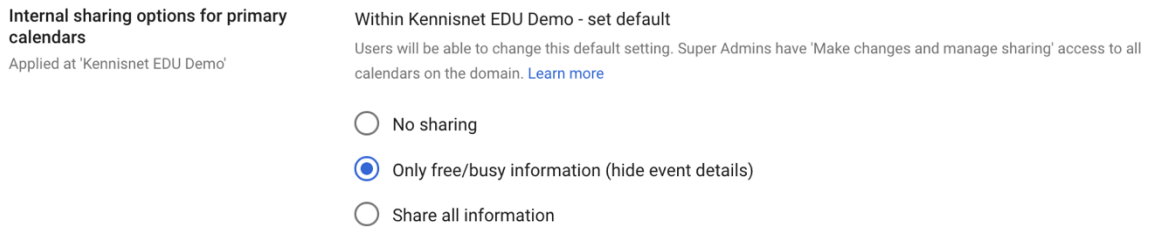


Google Agenda instellingen

Instellingen voor extern delen van primaire en secundaire agenda's
In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Agenda -> Instellingen voor delen
Stel in op: Alleen beschikbaar/bezet-informatie (afspraakdetails verbergen)

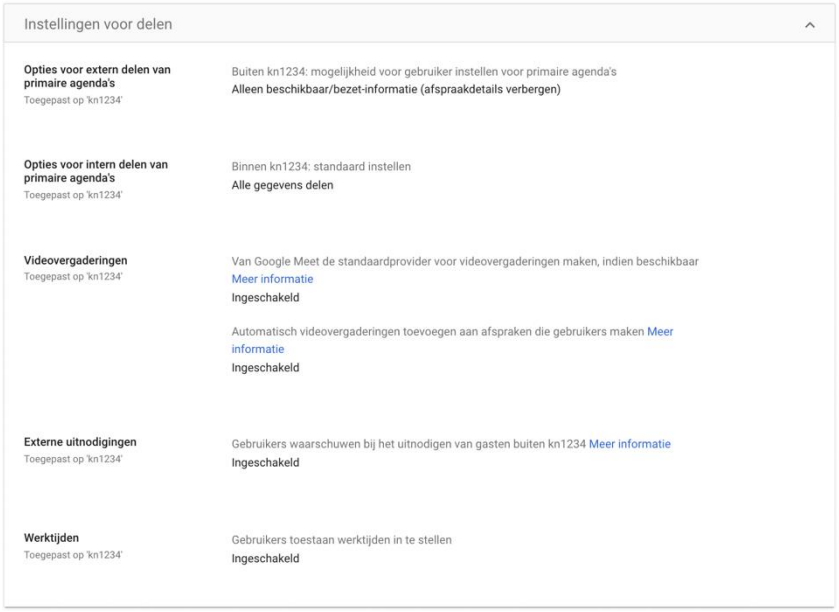


Instellingen voor intern delen van primaire en secundaire agenda's
In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Agenda -> Instellingen voor delen
Stel in op: Alleen beschikbaar/bezet-informatie (afspraakdetails verbergen)



Instellingen voor uitnodigen gasten van buiten.

In admin.google.com ga naar: Apps -> Google Workspace -> Instellingen voor Agenda -> Externe uitnodigingen
Stel in op: Gebruikers waarschuwen bij het uitnodigen van gasten buiten het domein.

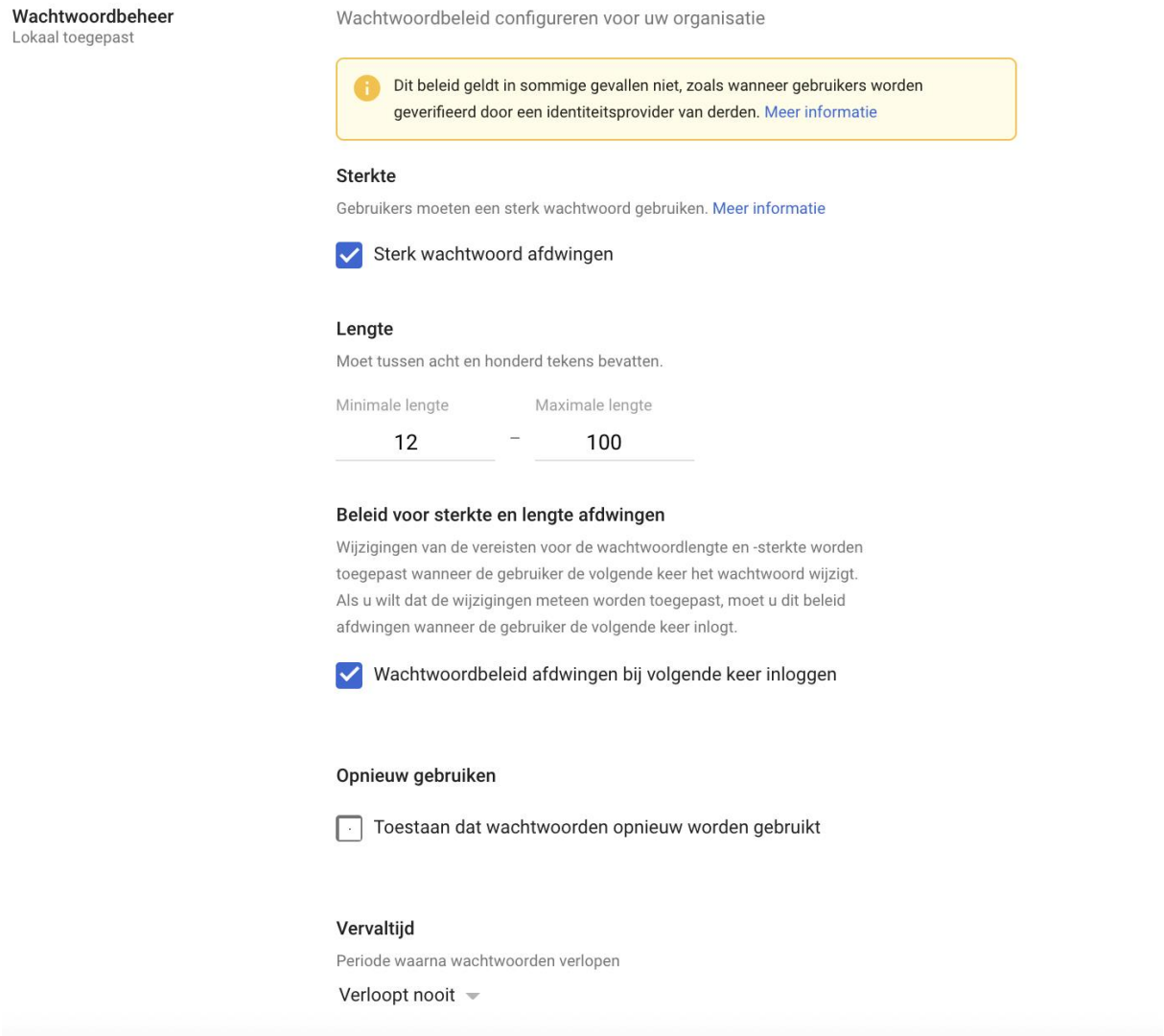


Sterk wachtwoord beleid

Alleen van toepassing indien niet gebruik gemaakt wordt van een SSO toepassing. Wel toepassen als Google gebruikersnaam en wachtwoord gebruikt wordt om in te loggen.

Een wachtwoordbeleid is een praktische maatregel die voortvloeit uit de Algemene Verordening Gegevensbescherming (AVG) om persoonsgegevens passend te beveiligen. Een goed wachtwoord bevat letters, cijfers en speciale tekens

In admin.google.com ga naar: Beveiliging -> Instellingen -> Wachtwoordbeheer
Wachtwoordbeleid afdwingen bij volgende keer inloggen
Sterk wachtwoord afdwingen
Niet Toestaan dat wachtwoorden opnieuw worden gebruikt
Periode waarna wachtwoorden verlopen: verloopt nooit (alleen als 2 stappen verificatie geactiveerd is)



De sessieduur instellen voor Google-services

Als beheerder kunt u bepalen hoelang gebruikers toegang hebben tot Google-services. Stel het beleid in voor opnieuw verifiëren op maximaal 12 uur.
Deze functie wordt ondersteund in de volgende versies: Business Plus, Enterprise, Education Fundamentals, Standard, Teaching and Learning Upgrade en Plus, G Suite Business.

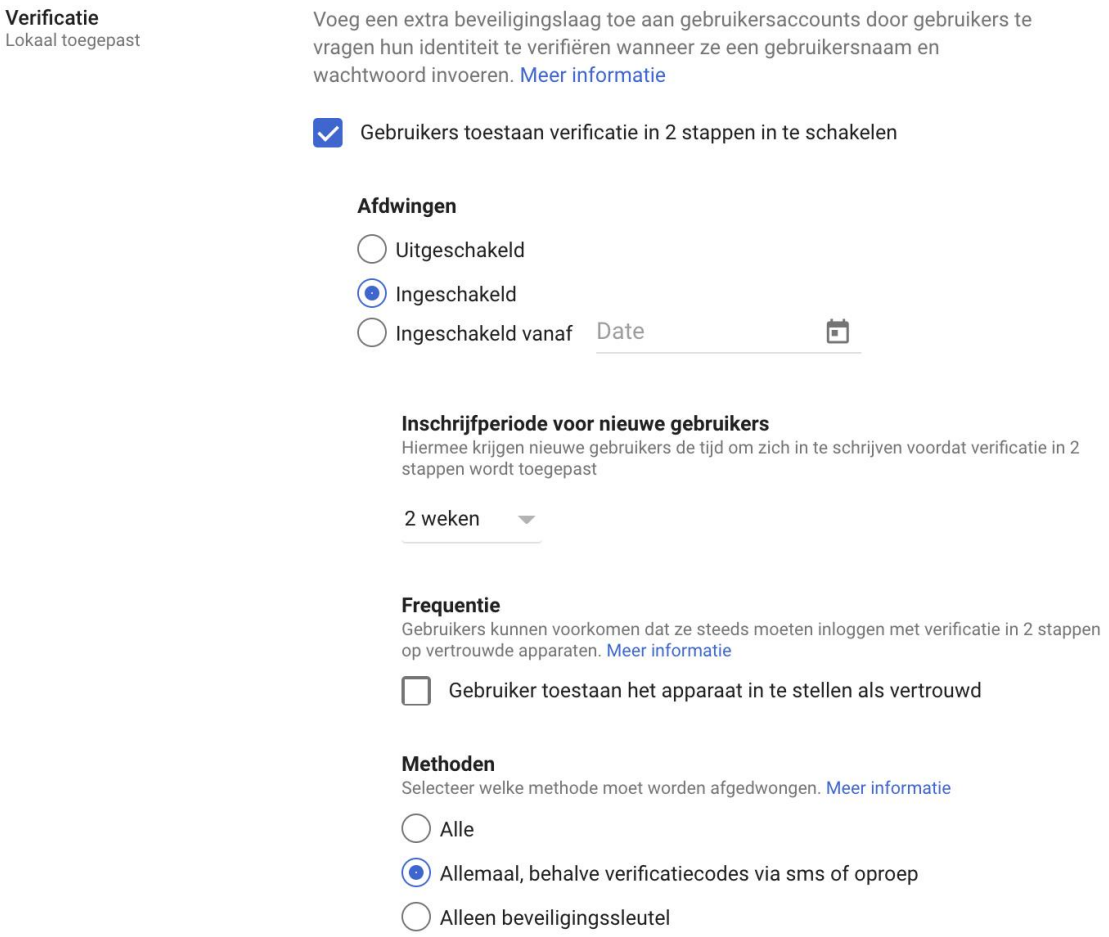
In admin.google.com ga naar: Beveiliging -> Instellingen -> Sessie beheer
Selecteer: Opnieuw verifiëren afdwingen
Frequentie van opnieuw verifiëren 12 uur

Activeer verificatie in 2 stappen

Verificatie in 2 stappen is een verificatie met “iets wat je weet” en “iets wat je hebt”. Iets wat je weet is je wachtwoord, iets wat je hebt is bijvoorbeeld je telefoon.
Met Verificatie in 2 stappen kunnen kwaadwillende geen toegang krijgen tot de Google Workspace omgeving zelfs als gebruikersnaam en wachtwoord gelekt zijn. Standaard: staat deze functie uit.

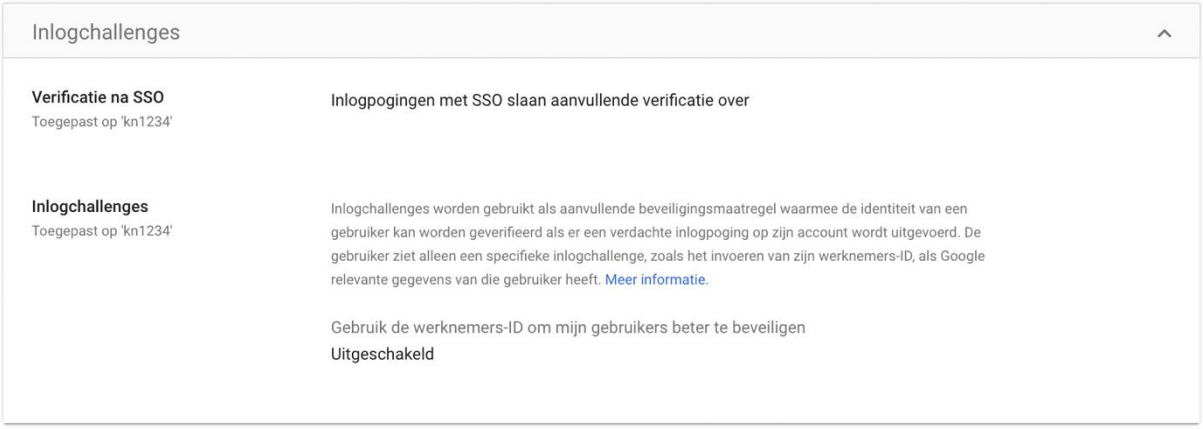
Beveiligingsniveau
Minimaal: Zet deze functie minimaal aan voor alle beheer rollen.
Optimaal: Zet deze functie aan voor alle medewerkers.
Perfect: Zet deze functie aan voor alle medewerkers en leerlingen

In admin.google.com ga naar: Beveiliging -> Instellingen -> Verificatie in 2 stappen
Afdwingen ingeschakeld
Gebruiker niet toestaan het apparaat in te stellen als vertrouwd
Methode: Allemaal, behalve verificatiecodes via sms of oproep



Login challenge bij gebruik van SAML SSO

Als je inlogt met single sign-on (SSO) via een identiteit management systeem zoals Microsoft Azure AD dan ontvangt Google een SAML assertion ter authenticatie van de gebruiker. Google kan hierna nog een extra beveiliging (login challenge) toevoegen door middel van de opgegeven recovery telefoon of email.
In admin.google.com ga naar: Beveiliging -> Instellingen -> Inlogchallenges
Selecteer: voor inlogpogingen met SSO kunnen aanvullende verificatie (indien nodig) of verificatie in 2 stappen (indien geconfigureerd) worden vereist
Selecteer niet: Gebruik de werknemers-ID om mijn gebruikers beter te beveiligen

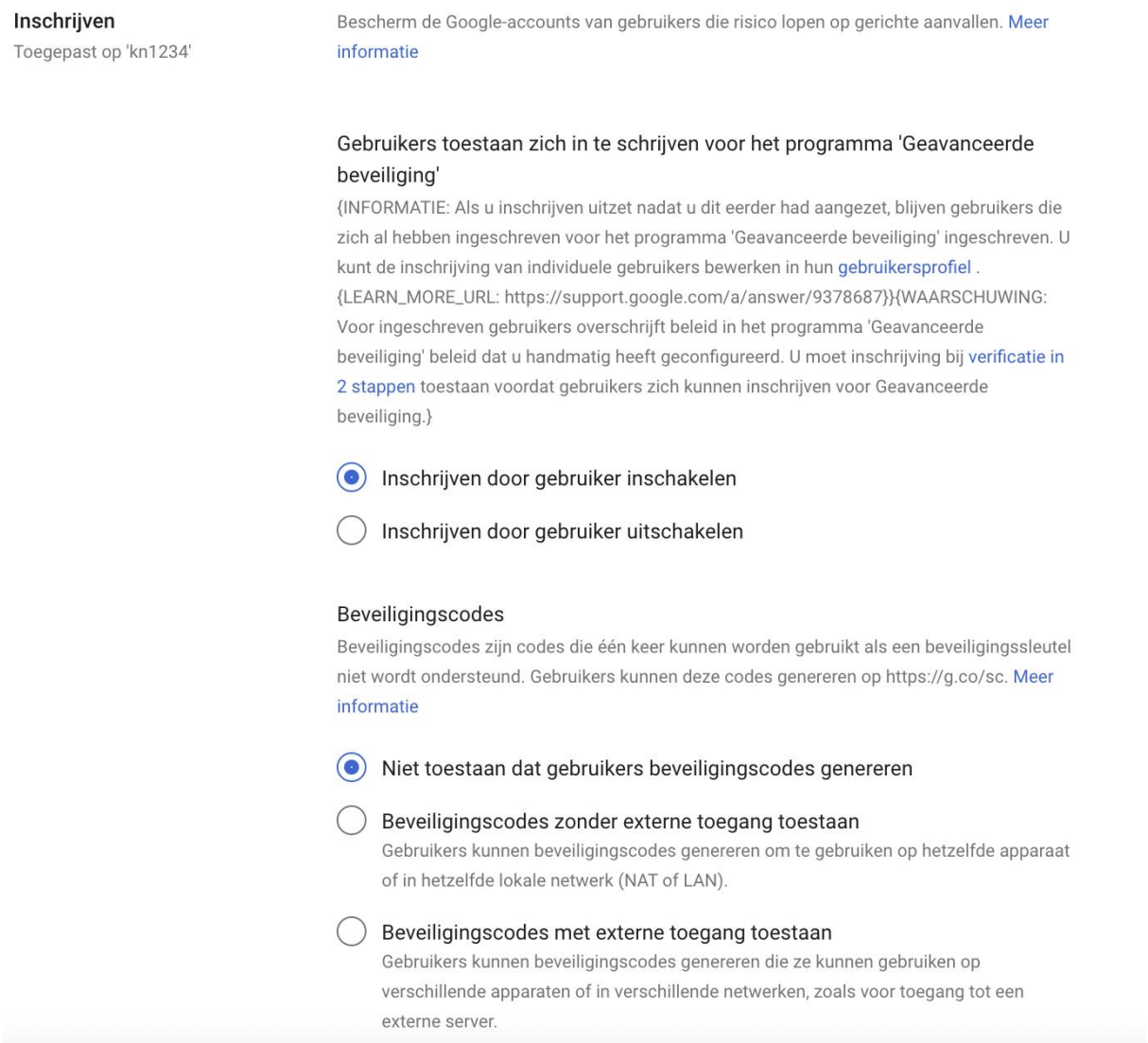


Beleid ‘Geavanceerde beveiliging’

Voor ingeschreven gebruikers overschrijft beleid in het programma 'Geavanceerde beveiliging' beleid dat u handmatig heeft geconfigureerd. U moet inschrijving bij verificatie in 2 stappen toestaan voordat gebruikers zich kunnen inschrijven voor Geavanceerde beveiliging.
Het programma ‘Geavanceerde beveiliging’ dwingt de volgende beveiligingsmaatregelen af:

- Sterke authenticatie met security keys (een security key is een fysiek apparaat die een gebruiker verifieert. Bijvoorbeeld een Android telefoon of een iPhone met Google smart lock app)
- Beperking van toegang door apps van derde partijen. Je kan nog wel inloggen bij apps met een Google ID, maar als de app toegang wil hebben tot Gmail of Drive data wordt dit geblokkeerd.
- Deep Gmail scans om phishing en malware mail te blokkeren
- Google Safe Browsing in Chrome
- Account recovery via admin

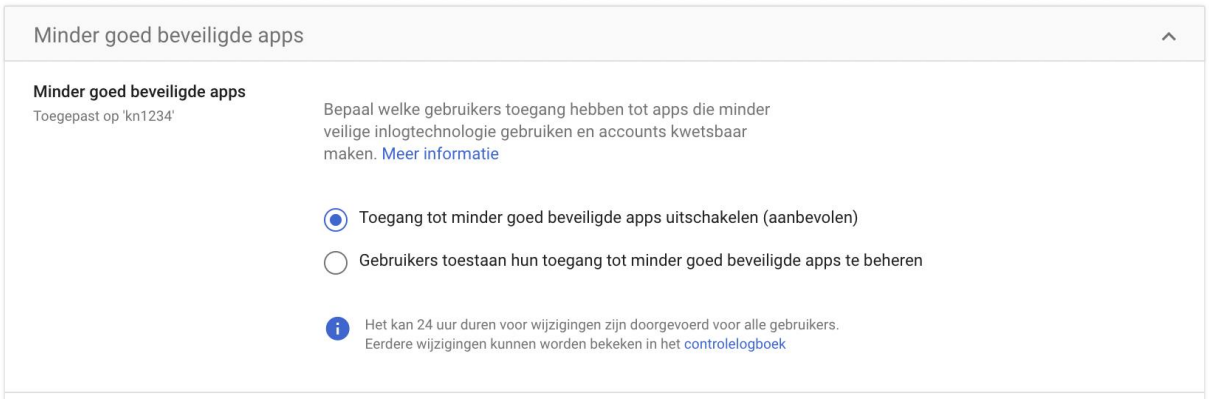
In admin.google.com ga naar: Beveiliging -> Instellingen -> Het programma ‘Geavanceerde beveiliging’
Inschrijven door gebruiker inschakelen
Niet toestaan dat gebruikers beveiligingscodes genereren



Toegang tot minder goed beveiligde apps

U kunt inlogpogingen blokkeren van bepaalde apps of apparaten die minder veilig zijn. Minder goed beveiligde apps gebruiken geen moderne beveiligingsstandaarden, zoals OAuth. U loopt bij gebruik van deze apps dus meer risico dat accounts en apparaten worden gehackt. Blokkeer deze apps en apparaten om uw gegevens beter te beveiligen.

In admin.google.com ga naar: Beveiliging -> Instellingen -> minder goed beveiligde apps Toegang tot minder goed beveiligde apps uitschakelen.



Directory extern delen

Contactgegevens worden niet buiten uw organisatie gedeeld.
Als uw organisatie apps van derden gebruikt die integreren met uw Google-services, kunt u bepalen tot welke directorygegevens de apps toegang hebben.
Openbaar zichtbare domeinprofielgegevens delen met externe apps en API's. De naam, de foto en het e-mailadres van de geverifieerde gebruiker ook delen om 'Inloggen bij Google' in te schakelen als het betreffende bereik wordt toegewezen. Andere, niet-openbare profielvelden van de geverifieerde gebruiker worden niet gedeeld. De niet-openbare profielgegevens van andere gebruikers in het domein worden niet gedeeld

In admin.google.com ga naar: Directory -> Instellingen -> minder goed beveiligde apps
Selecteer Openbare gegevens en algemene profielvelden van geverifieerde gebruikers

DLP voor Drive gebruiken om gegevensverlies te voorkomen

Met gegevensverlies voorkomen (Data Loss Prevention, DLP) kunt u regels maken en toepassen om te bepalen welke content gebruikers buiten de organisatie kunnen delen in Google Drive-bestanden. Met DLP krijgt u controle over wat gebruikers kunnen delen. Zo voorkomt u dat gevoelige informatie, zoals creditcardnummers of burgerservicenummers, onbedoeld openbaar wordt gemaakt. DLP-regels scannen bestanden op gevoelige content en voorkomen dat gebruikers die content kunnen delen. Regels bepalen de aard van DLP-incidenten. Incidenten triggeren acties, zoals het blokkeren van bepaalde content.

Deze functie wordt ondersteund in de volgende versies: Enterprise, Education Fundamentals, Standard, Teaching and Learning Upgrade en Plus.

In admin.google.com ga naar: Beveiliging -> Data protection -> DLP regels
Stel regels in en activeer de functie.
Aanbevelingen voor regels zijn niet beschikbaar in Education fundamentals editie. U kunt wel handmatig regels aanmaken.

Geavanceerde instellingen

Rechten voor delen voor Drive-gebruikers op basis van whitelist

Deze functie wordt ondersteund in de volgende versies: Business Standard en Plus, Enterprise, Education Fundamentals, Standard, Teaching and Learning Upgrade en Plus, G Suite Business, Nonprofits, Essentials.

Klik bij Delen buiten uw organisatie op Domeinen op de witte lijst en kies de opties voor delen:

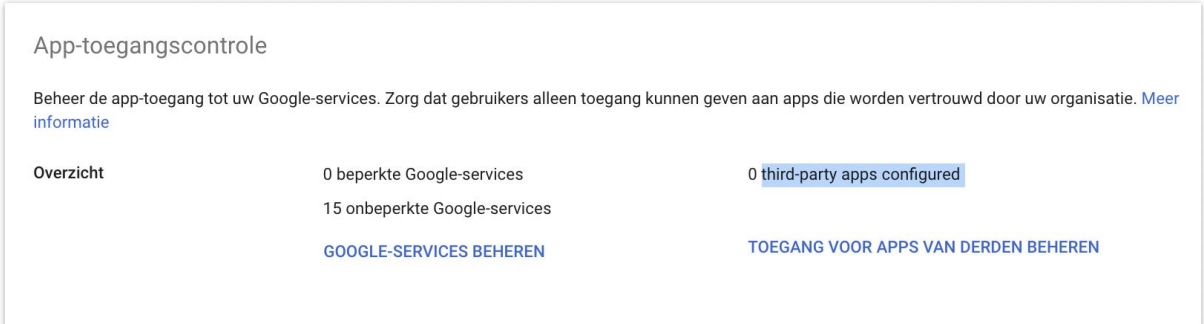
- Waarschuwen bij delen met gebruikers in domeinen op de witte lijst: Als gebruikers bestanden delen met gebruikers in een domein dat op de toelatingslijst staat, wordt er in de dialoogvensters van Editors van Documenten of Drive een waarschuwing weergegeven. Zo blijven uw bestanden vertrouwelijk.
- Gebruikers toestaan bestanden te ontvangen van gebruikers buiten witte lijst-domeinen: Gebruikers kunnen het volgende:
    - Bestanden openen uit domeinen die niet op de toelatingslijst staan.
    - Editors van Documenten gebruiken om Google-documenten, -spreadsheets en -presentaties te bewerken die zijn opgeslagen in opslagsystemen van derden, zoals Box.
- Gebruikers toestaan uitnodigingen voor delen te sturen naar mensen die geen Google-account gebruiken: Gebruikers kunnen bestanden delen met niet-Google-gebruikers in domeinen die op de toelatingslijst staan. Deze gebruikers moeten hun identiteit bevestigen met een pincode.

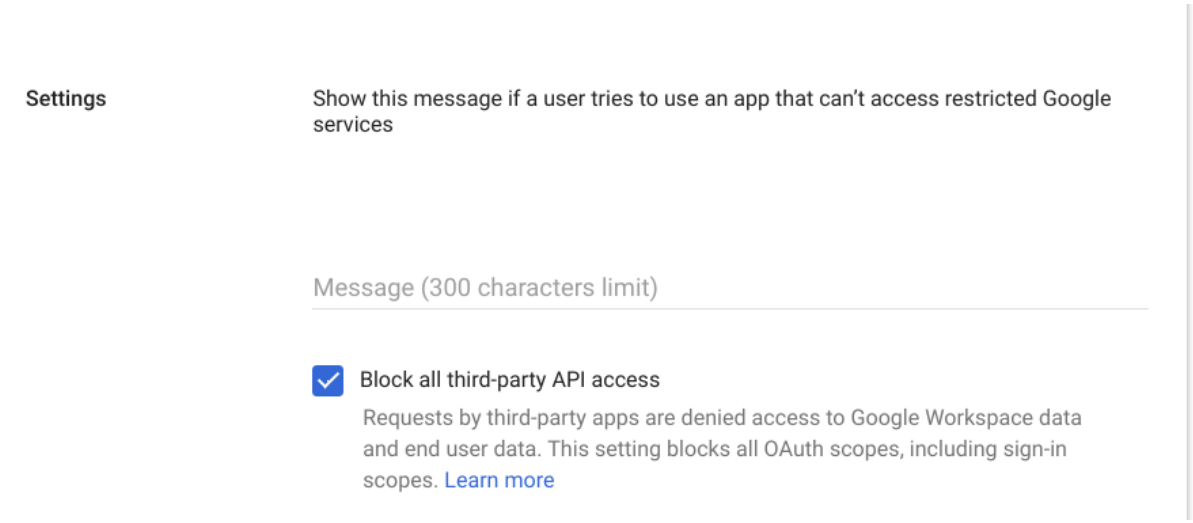
Beperkte toegang van apps tot Google Workspace-gegevens

U kunt bepalen welke apps van derden en apps die eigendom zijn van het domein toegang hebben tot gevoelige Google Workspace-gegevens

Beheer de app-toegang tot uw Google-services. Zorg dat gebruikers alleen toegang kunnen geven aan apps die worden vertrouwd door uw organisatie.

In admin.google.com ga naar: Beveiliging -> Instellingen -> API functies -> app toegangscontrole
Voor Google service stel in op beperkt: alleen vertrouwde apps hebben toegang tot een service
Bij third-party apps moeten de apps altijd aan een inspectie onderworpen zijn voordat toegang verleend wordt.





Domeinbrede machtingen

In admin.google.com ga naar: Beveiliging -> API-functies -> Domeinbrede machtiging
Controleer of alle apps in de lijst goedgekeurd zijn.