Google for Education

Meer dan 30 manieren om de betaalde versies van Google Workspace for Education te gebruiken

goo.gle/use-edu-workspace

Zo gebruik je deze presentatie

Deze presentatie bevat een aantal van de populairste toepassingen van de **betaalde versies van Google Workspace for Education**. Met deze tools kun je **de gegevensbeveiliging, de efficiëntie van de docent en de betrokkenheid van de leerling** verbeteren, **evenals de samenwerking op de hele school**, en nog veel meer.

Deze presentatie is ingedeeld op basis van **functies**, gevolgd door **veelgebruikte toepassingen** en daarna eenvoudige **instructies** voor het gebruik van de functies. Bekijk de hele presentatie en ontdek wat je allemaal kunt doen met Google Workspace for Education.

Betaalde versies van Google Workspace for Education

Met de 3 betaalde versies van Google Workspace for Education heb je meer keuze, controle en flexibiliteit om aan de behoeften van jouw organisatie te voldoen.

Google Workspace for Education Standard

Geavanceerde beveiligings- en analysetools, waarmee je risico's en bedreigingen inperkt dankzij meer zichtbaarheid en controle in de leeromgeving.

Teaching and Learning Upgrade

Verbeterde onderwijstools die communicatie en klassikale ervaringen verrijken en academische integriteit versterken.

Google Workspace for Education Plus

Een complete oplossing met alle functies van Education Standard, de Teaching and Learning Upgrade en meer.
Je scholengemeenschap krijgt de meest effectieve en uniforme leeromgeving.

Inhoudsopgave

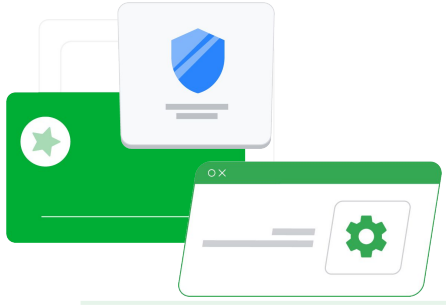
Inhoudsopgave

Tools voor lesgeven en leren

De tools van de **Teaching and Learning Upgrade** en **Education Plus**

Beveiliging en hulpprogramma's voor analyse

Krijg meer grip op het beheer van je domein met proactieve beveiligingstools waarmee je bedreigingen afhoudt, beveiligingsincidenten analyseert en de gegevens van leerlingen en de faculteit beschermt.



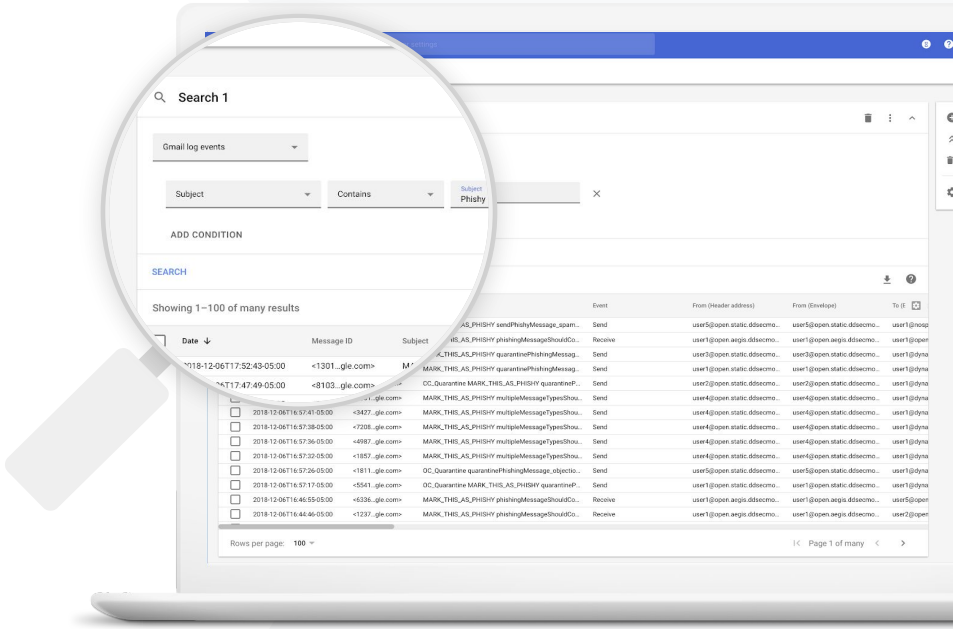
Onderzoekstool

Wat is dit?

Met de onderzoekstool kun je problemen met beveiliging en privacy in je domein identificeren, analyseren en er acties op uitvoeren.

Toepassingen

Ongewenst materiaal dat gedeeld is	Stapsgewijze instructies
Per ongeluk gedeelde documenten	Stapsgewijze instructies
Vooranalyse e-mail	Stapsgewijze instructies
Phishing/malwaremails	Stapsgewijze instructies
Kwaadwillende gebruikers tegenhouden	Stapsgewijze instructies



Ongewenst materiaal dat gedeeld is

"Ik weet dat er een bestand met ongepast materiaal wordt gedeeld. Ik wil weten wie het heeft gemaakt, wanneer het is gemaakt, wie het met wie heeft gedeeld, wie het heeft bewerkt en wie het heeft verwijderd."

Stapsgewijze instructies

Drive-logboeken in de **onderzoekstool** helpen je ongewenste bestanden in je domein te vinden, volgen, isoleren of verwijderen. Via je Drive-logboeken kun je:

- Documenten zoeken op naam, gebruiker, eigenaar enz.
- Actie ondernemen door de bestandsrechten te wijzigen of door het bestand te verwijderen
- Alle logoekinformatie over dat document bekijken
  - Aanmaakdatum
  - Wie de eigenaar van het document is, wie het heeft bekeken en wie het heeft bewerkt
  - Wanneer het werd gedeeld

Relevante Helpcentrum-documentatie

Voorwaarden voor Drive-logboekgebeurtenissen

Acties voor Drive-logboekgebeurtenissen

Per ongeluk gedeelde bestanden

"Er is per ongeluk een bestand gedeeld met een groep die daar GEEN toegang toe mag hebben. Ik wil hun toegang ertoe verwijderen."

Stapsgewijze instructies

Drive-logboeken in de **onderzoekstool** helpen je om problemen bij het delen van bestanden te volgen en op te lossen. Via je Drive-logboeken kun je:

- Naar documenten zoeken via naam, gebruiker, eigenaar, enzovoort
- Alle logboekinformatie over het betreffende document bekijken, zoals wie het heeft bekeken en wanneer het is gedeeld.
- Actie ondernemen door de bestandsrechten te wijzigen of door het downloaden, afdrukken en kopiëren uit te zetten

Relevante Helpcentrum-documentatie

Voorwaarden voor Drive-logboekgebeurtenissen

Acties voor Drive-logboekgebeurtenissen

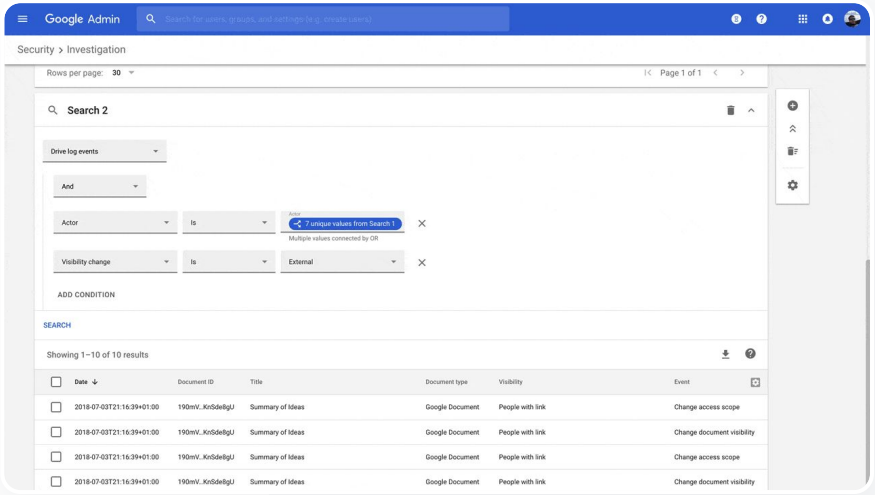
Instructies Drive-logboekgebeurtenissen

Op onderzoek uitgaan

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Onderzoekstool.**
- Kies **Drive-logboekgebeurtenissen.**
- Klik op **Voorwaarde toevoegen** > **Zoeken.**

In actie komen

- Selecteer de toepasselijke bestanden in de zoekresultaten.
- Klik op **Acties** > **Bestandsrechten controleren** om de pagina Rechten te openen.
- Klik op **Mensen** om te zien wie er toegang heeft.
- Klik op **Links** om de instellingen voor het delen van links te bekijken of te wijzigen voor de geselecteerde bestanden.
- Klik op **Wijzigingen in behandeling** om de wijzigingen te bekijken voordat je deze opslaat.



Relevante Helpcentrum-documentatie

Voorwaarden voor Drive-logboekgebeurtenissen

Acties voor Drive-logboekgebeurtenissen

Vooranalyse e-mail

De **Gmail-logboeken** in de **onderzoekstool** helpen je om gevaarlijke of ongepaste e-mails binnen je domein te identificeren en er actie tegen te ondernemen. Via je Gmail-logboeken kun je:

- Specifieke e-mails zoeken op onderwerp, bericht-ID, bijlage, afzender, en meer.
- Details van e-mails bekijken, zoals de auteur, de ontvanger en het aantal keren dat ze zijn geopend en doorgestuurd.
- Acties uitvoeren op basis van zoekresultaten. Mogelijke acties op Gmail-berichten zijn verwijderen, herstellen, als spam of phishing aangeven, naar inbox sturen en in quarantaine plaatsen.

> lemand heeft een e-mail gestuurd die NIET verstuurd had moeten worden. We willen weten naar wie het bericht is verstuurd, of de ontvangers het hebben geopend en of ze erop hebben gereageerd. We willen de e-mail ook verwijderen. Ik wil weten ook wat er in de e-mail staat."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Voorwaarden voor Gmail-logboek en -berichten

Acties voor Gmail-berichten en -logboekgebeurtenissen

Stappen om de inhoud van een e-mail te zien

Phishing- en malwaremails

Er is een phishing- of malwaremail naar gebruikers verstuurd. We willen weten of gebruikers op de link in de e-mail hebben geklikt of de bijlage hebben gedownload, want daardoor kunnen het domein en de gebruikers mogelijk risico lopen.

Stapsgewijze instructies

De **onderzoekstool**, en specifieker de **Gmail-logboeken**, helpen je om schadelijke e-mails in je domein te vinden en te isoleren. Via je Gmail-logboeken kun je:

- Naar e-mailberichten zoeken met specifieke content, inclusief bijlagen
- Informatie verkrijgen over specifieke e-mails, inclusief wie ze heeft ontvangen en geopend
- De berichten en het gesprek bekijken om te bepalen of ze schadelijk zijn
- Actie ondernemen, zoals de berichten markeren als spam of phishing, naar een speciale inbox sturen, in quarantaine plaatsen of verwijderen

Relevante Helpcentrum-documentatie

Voorwaarden voor Gmail-logboek en -berichten

Acties voor Gmail-berichten en -logboekgebeurtenissen

Stappen om de inhoud van een e-mail te zien

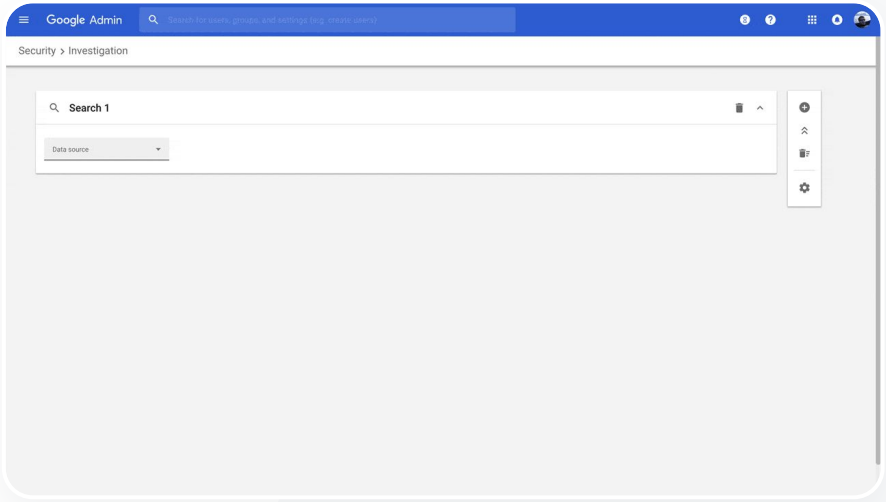
Instructies Gmail-logboeken

Op onderzoek uitgaan

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Onderzoekstool.**
- Kies **Gmail-logboekgebeurtenissen** OF **Gmail-berichten.**
- Klik op **Voorwaarde toevoegen** > **Zoeken.**

In actie komen

- Selecteer de relevante berichten in de zoekresultaten.
- Klik op **Acties.**
- Kies **Bericht verwijderen uit inbox.**
- Klik op **Verwijderen uit inbox.**
- Klik op **Bekijken** onder aan de pagina om de actie te bevestigen.
- In de kolom **Resultaat** kun je de status van de actie bekijken.



Relevante Helpcentrum-documentatie

Voorwaarden voor Gmail-logboek en -berichten

Acties voor Gmail-berichten en -logboekgebeurtenissen

Stappen om de inhoud van een e-mail te zien

Kwaadwillende gebruikers tegenhouden

Een kwaadwillig persoon zit constant achter vooraanstaande gebruikers van mijn domein aan. Ik word er gek van. Hoe kan ik zorgen dat dit ophoudt?

Met het **gebruikerslogboek** in de **onderzoekstool** kun je:

- Identificeren en onderzoeken welke pogingen zijn gedaan om gebruikersaccounts in je organisatie te hacken.
- Controleren welke methoden voor verificatie in 2 stappen gebruikers in je organisatie gebruiken.
- Meer informatie bekijken over mislukte inlogpogingen door gebruikers in je organisatie.
- Activiteitsregels maken met de onderzoekstool: Automatisch berichten en andere schadelijke activiteiten van specifieke gebruikers blokkeren.
- Vooraanstaande gebruikers beter beveiligen met Geavanceerde beveiliging.
- Gebruikers herstellen of opschorten.

Relevante Helpcentrum-documentatie

Stapsgewijze instructies

Gebeurtenissen in het logboek
Gebruikers vinden en onderzoeken

Activiteitsregels maken met de onderzoekstool

Instructies Gebeurtenissen in het logboek Gebruikers

Op onderzoek uitgaan

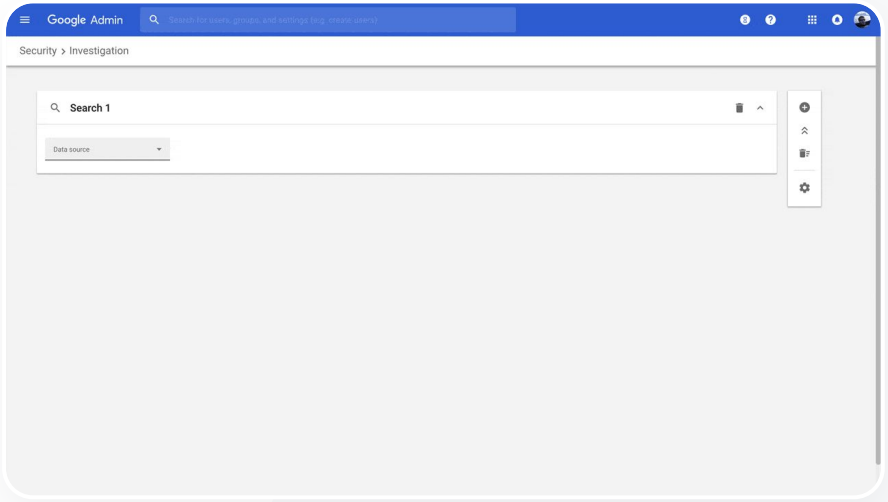
- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Onderzoekstool.**
- Kies **Gebeurtenissen in het logboek Gebruikers.**
- Klik op **Voorwaarde toevoegen** > **Zoeken.**

Gebruikers herstellen of opschorten

- Selecteer een of meer gebruikers uit de zoekresultaten.
- Klik op **Acties** dropdownmenu.
- Klik op **Gebruiker herstellen** of **Gebruiker opschorten.**

Details van een specifieke gebruiker bekijken

- Selecteer één gebruiker op de pagina met zoekresultaten.
- Klik in het dropdownmenu Acties op **Details bekijken.**



Relevante Helpcentrum-documentatie

Gebeurtenissen in het logboek Gebruikers vinden en onderzoeken

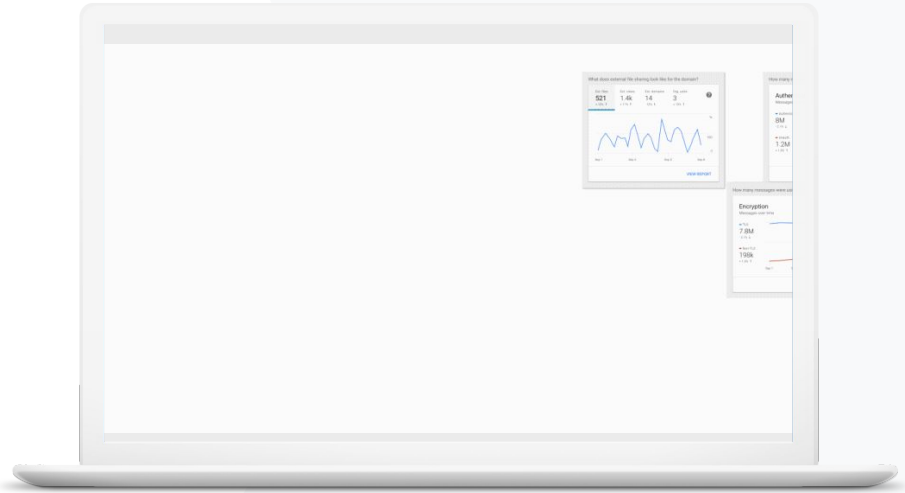
Beveiligingsdashboard

Wat is dit?

Een overzicht bekijken van de verschillende beveiligingsrapporten in het beveiligingsdashboard. Standaard staan in elk rapportvenster de gegevens van de afgelopen 7 dagen. Je kunt het dashboard aanpassen zodat gegevens van vandaag, gisteren, deze week, vorige week, deze maand, vorige maand of dagen geleden (maximaal 180 dagen) worden weergegeven.

Toepassingen

Hoeveelheid spam	Stapsgewijze instructies
Extern bestanden delen	Stapsgewijze instructies
Apps van derden	Stapsgewijze instructies
Poging tot phishing	Stapsgewijze instructies



Hoeveelheid spam

"Ik wil ervoor zorgen dat er minder onnodige e-mails worden verstuurd en ik wil de beveiligingsrisico's voor mijn school verminderen."

Het **beveiligingsdashboard** geeft op visuele wijze de activiteiten weer van je Google Workspace for Education-omgeving, inclusief:

- Spam
- Phishing
- Malware
- Verdachte bijlagen
- En meer

Stapsgewijze instructies

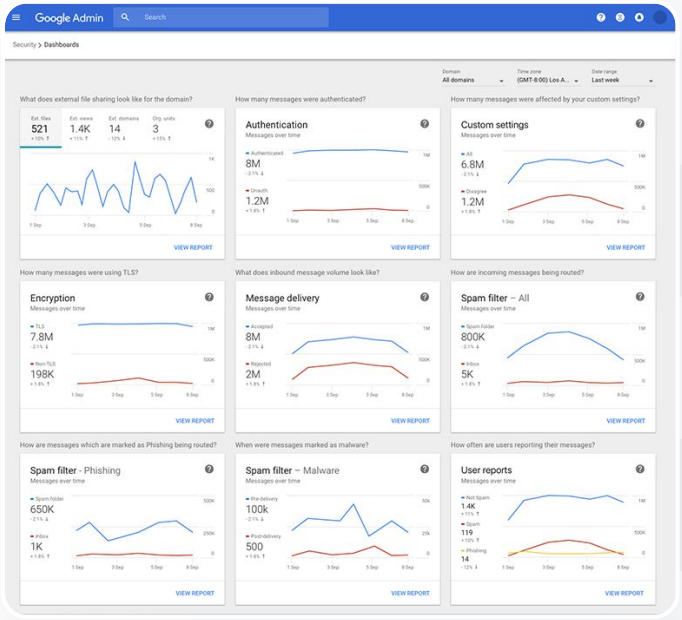
Relevante Helpcentrum-documentatie

Over het beveiligingsdashboard

Instructies Dashboardoverzicht

Het dashboard bekijken

- Log in bij de **Beheerdersconsole**.
- Klik op **Beveiliging** > **Dashboard**.
- Via het beveiligingsdashboard kun je gegevens onderzoeken, naar Spreadheets of naar een externe tool exporteren, of een onderzoek instellen met de onderzoekstool.



Relevante Helpcentrum-documentatie

Over het beveiligingsdashboard

Extern bestanden delen

"Ik wil zien welke bestanden er exter worden gedeeld zodat ik kan voorkomen dat gevoelige gegeven in handen van derden komen."

Gebruik het **rapport Bestandsbereik** in het **beveiligingsdashboard** om statistieken over het extern delen van bestanden te bekijken voor je domein, inclusief:

- Het aantal keer dat bestanden zijn gedeeld met gebruikers buiten je domein in een bepaalde periode.
- Het aantal keer dat een extern bestand is bekeken in een bepaalde periode.

Stapsgewijze instructies

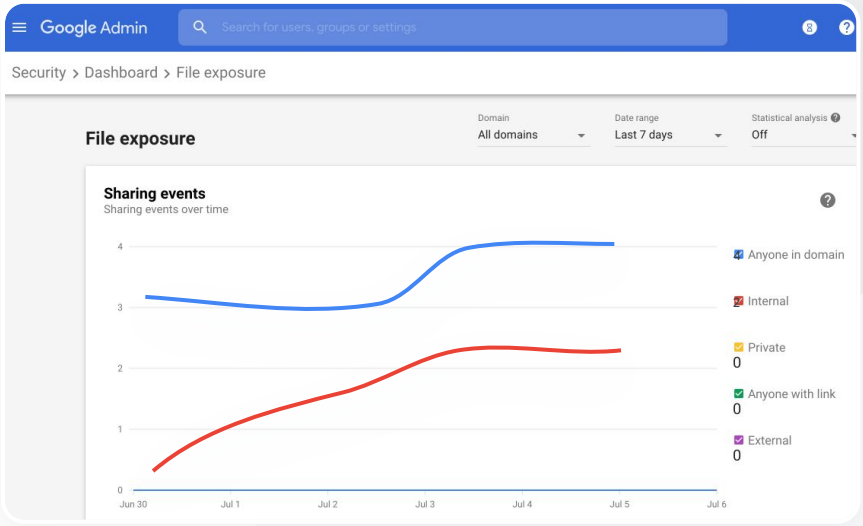
Relevante Helpcentrum-documentatie

Aan de slag met de pagina Beveiligingsstatus

Instructies Rapport Bestandsbereik

Een rapport weergeven

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Dashboard.**
- Klik in het deelvenster
  Hoe ziet extern delen eruit voor het domein?
  op **Rapport bekijken** in de rechterbenedenhoek.



Relevante Helpcentrum-documentatie

Over het beveiligingsdashboard rapport Bestandsbereik.

Apps van derden

Ik wil zien welke apps van derden toegang hebben tot de gegevens van mijn domein."

Gebruik het rapport **Activiteit OAuth-toewijzingen** in het **beveiligingsdashboard** om in de gaten te houden welke apps van derden zijn gekoppeld aan je domein en tot welke gegevens ze toegang hebben.

- OAuth geeft services van derden toegang tot de accountgegevens van een gebruiker, zonder dat het wachtwoord van de gebruiker bekend wordt. Het kan goed zijn om het aantal apps van derden die toegang hebben te beperken.
- Gebruik het deelvenster Activiteit van de OAuth-toewijzingen om de toewijzingen per app, bereik of gebruiker te controleren, en de toewijzingsrechten te updaten.

Stapsgewijze instructies

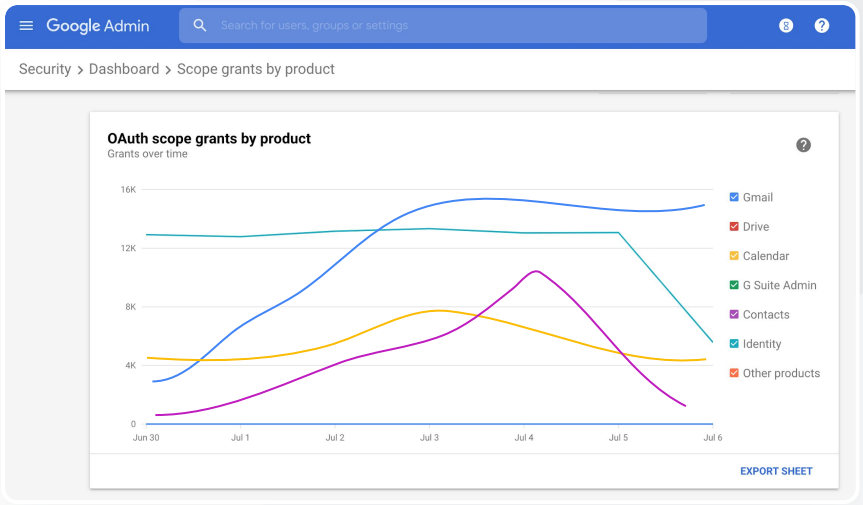
Relevante Helpcentrum-documentatie

Rapport Activiteit OAuth-toewijzingen

Instructies Rapport Activiteit OAuth-toewijzingen

Een rapport weergeven

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Dashboard.**
- Klik onderaan op **Rapport bekijken.**
- Je kunt het activiteitenrapport van OAuth-toewijzingen weergeven per product (app), bereik of gebruiker.
- Klik op **App**, **Bereik** of **Gebruiker om de informatie te filteren.**
- Als je een spreadsheetrapport wilt maken, klik je op **Spreadsheet exporteren.**



Relevante Helpcentrum-documentatie

Rapport Activiteit OAuth-toewijzingen

Poging tot phishing

In het **deelvenster Gebruikersrapporten** van het **beveiligingsdashboard** kun je berichten bekijken die tijdens een specifieke periode zijn gemarkeerd als phishing of spam. Je kunt gegevens bekijken over e-mails die als phishing zijn gemarkeerd, zoals de ontvangers en hoe vaak de berichten zijn geopend.

Gebruikers hebben een poging tot phishing gemeld. Ik wil kunnen zien wanneer de phishingmail binnen is gekomen, wat het precies voor e-mail was en aan welk risico de gebruiker is blootgesteld."

- In gebruikersrapporten zie je hoe gebruikers in een bepaalde periode hun berichten hebben gemarkeerd (als spam, phishing of geen spam).
- Je kunt het diagram ook zo aanpassen dat je alleen gegevens van bepaalde soorten berichten ziet, bijvoorbeeld of het bericht intern of extern is gestuurd, in welke periode, enzovoorts.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

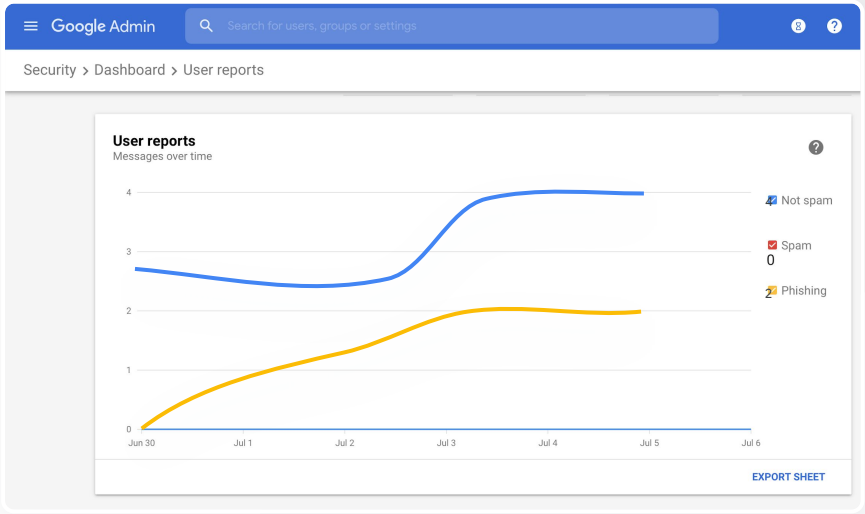
Hoe markeren gebruikers hun e-mails?

Gebruikersrapporten

Instructies Deelvenster gebruikersrapporten

Een rapport weergeven

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Dashboard.**
- Klik rechtsonder in het **deelvenster Gebruikersrapport op Rapport bekijken.**



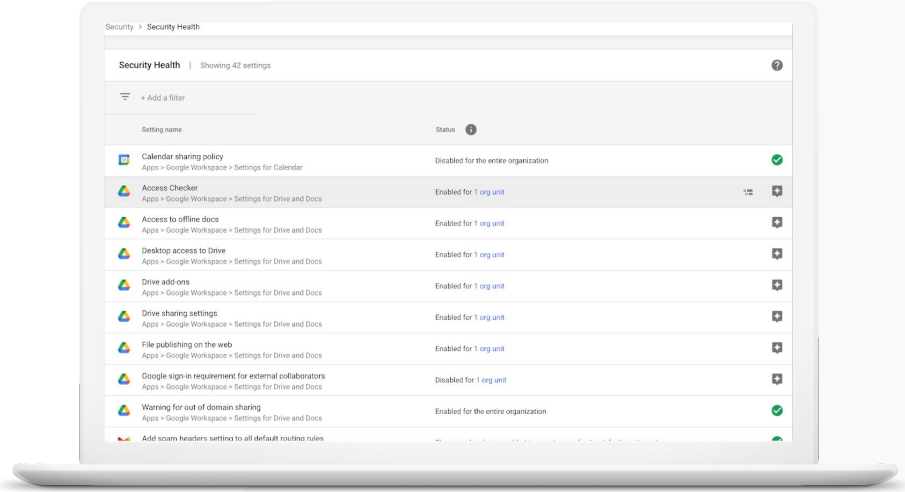
Relevante Helpcentrum-documentatie

Over het beveiligingsdashboard rapport Bestandsbereik.

Beveiligingsstatus

Wat is dit?

Op de pagina Beveiligingsstatus krijg je een uitgebreid overzicht van de beveiliging van je Google Workspace-omgeving. Vergelijk je instellingen met aanbevelingen van Google om je organisatie proactief te beschermen.



Toepassingen

Aanbevelingen voor risicogebieden	Stapsgewijze instructies
Op de hoogte blijven van best practices	Stapsgewijze instructies
Best practices voor beveiliging	Stapsgewijze instructies
Betere beveiliging voor een groeiende school	Stapsgewijze instructies

Aanbevelingen voor risicogebieden

Op de pagina **Beveiligingsstatus** kun je je beveiligingsinstellingen controleren en aanbevolen wijzigingen bekijken. Op de pagina Beveiligingsstatus kun je:

- Snel potentiële risicogebieden in je domein identificeren
- Aanbevelingen krijgen voor de optimale instellingen om de effectiviteit van je beveiliging te vergroten
- Extra informatie en supportartikelen lezen over aanbevelingen

> Ik wil een samenvattende momentopname van de beveiligingsinstellingen van mijn domein met praktische aanbevelingen voor potentiële risicogebieden."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Aan de slag met de pagina Beveiligingsstatus

Op de hoogte blijven van best practices

Op de pagina **Beveiligingsstatus** kun je je beveiligingsinstellingen controleren en aanbevolen wijzigingen bekijken. Op de pagina Beveiligingsstatus krijg je het volgende:

- Aanbevelingen voor potentiële risicogebieden in jouw domein
- Aanbevelingen voor de optimale instellingen om de effectiviteit van je beveiliging te vergroten
- Extra informatie en supportartikelen

> Ik beheer ons domein, maar ik weet niet wat ik niet weet. Help me ervoor te zorgen dat alles met de juiste instellingen is beveiligd."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Aan de slag met de pagina Beveiligingsstatus

Best practices voor beveiliging

Geef me de best practices of aanbevelingen over het instellen van een beveiligingsbeleid."

Gebruik de pagina Beveiligingsstatus om best practices te krijgen over beveiligingsbeleid met:

- Aanbevelingen voor potentiële risicogebieden in jouw domein
- Aanbevelingen voor de optimale instellingen om de effectiviteit van je beveiliging te vergroten
- Rechtstreekse links naar de instellingen
- Extra informatie en supportartikelen

Stapsgewijze instructies

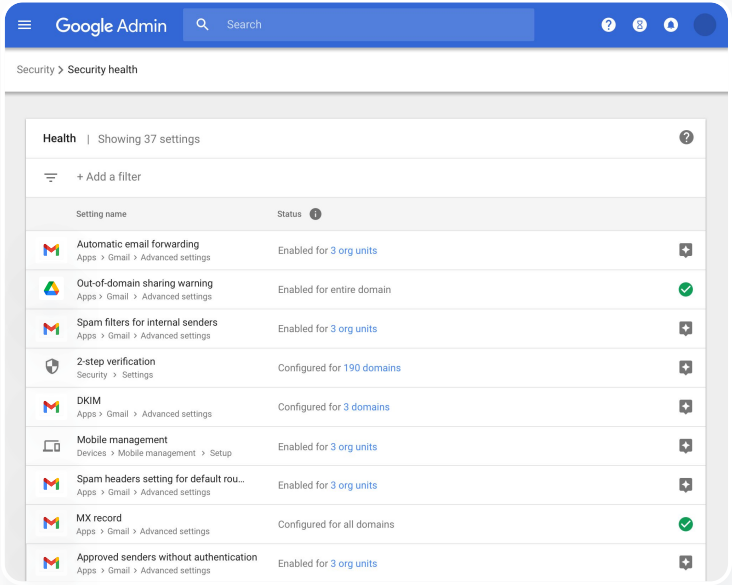
Relevante Helpcentrum-documentatie

Aan de slag met de pagina Beveiligingsstatus

Instructies Beveiligingsaanbevelingen

Aanbevelingen bekijken

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Beveiligingsstatus.**
- In de uiterst rechtse kolom zie je de status van instellingen.
  - Een groen vinkje staat voor een beveiligde instelling.
  - Een grijs icoon staat voor een aanbeveling om die instelling nog eens goed te bekijken. Klik op het icoon om de details en instructies te openen.



Relevante Helpcentrum-documentatie

Aan de slag met de pagina Beveiligingsstatus

Betere beveiliging voor een groeiende school

“

Ik wil ervoor zorgen dat mijn school zo goed mogelijk beveiligd is, omdat onze faculteit en het aantal leerlingen groeit."

We raden IT-beheerders aan deze best practices voor beveiliging te volgen om de beveiliging en privacy van bedrijfsgegevens te verbeteren. Gebruik een of meer instellingen in de Google Beheerdersconsole om de best practices van deze checklist te implementeren.

- Aanbevelingen om te voorkomen dat accounts worden gehackt en om problemen met gehackte accounts op te lossen
- Stappen om delen en samenwerken buiten je domein te beperken
- Functies om de toegang van derden tot kernservices te controleren

Stapsgewijze instructies

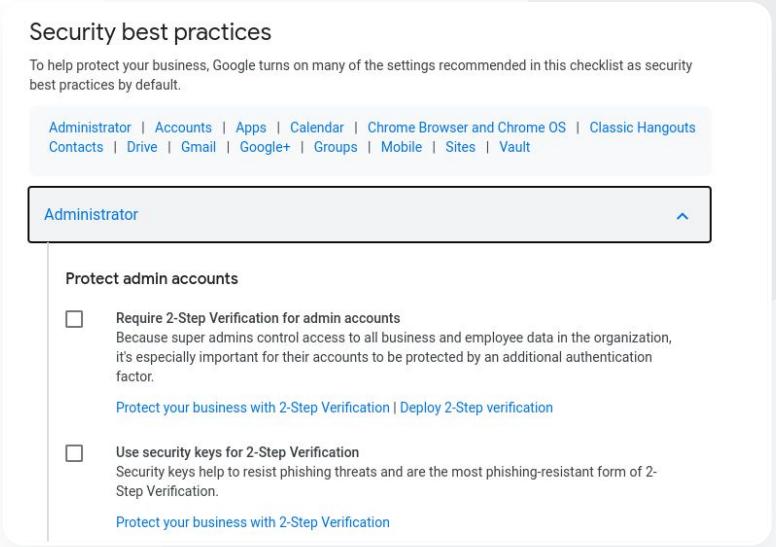
Relevante Helpcentrum-documentatie

Beveiligingschecklist voor middelgrote en grote bedrijven

Instructies Beveiligingschecklist

Veel van de instellingen die in deze checklist worden aanbevolen als best practices, zijn standaard aangezet door Google om je organisatie te beschermen. We raden je aan om de hieronder uitgelichte instellingen nader te bekijken.

- **Beheerder:** beheerdersaccounts beveiligen
- **Accounts:** voorkomen dat accounts worden gehackt en problemen met gehackte accounts oplossen
- **Apps:** de toegang van derden tot kernservices controleren
- **Agenda:** het extern delen van agenda's beperken
- **Drive:** delen en samenwerken buiten je domein beperken
- **Gmail:** verificatie en infrastructuur instellen
- **Vault:** Vault-accounts beheren, controleren en beveiligen



Relevante Helpcentrum-documentatie

De status van je beveiligingsinstellingen controleren

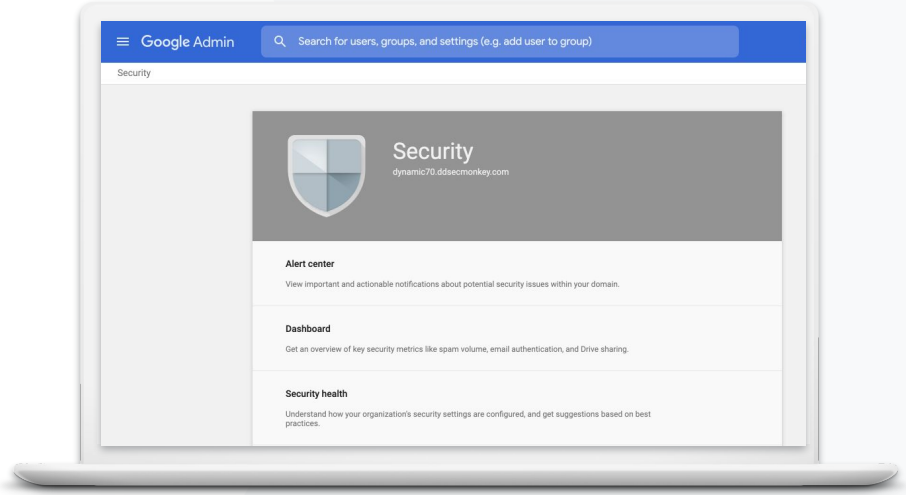
Geavanceerde beheeropties

Wat is dit?

Controleer en bepaal welke gebruikers en apparaten toegang krijgen tot jouw domein en gegevens.

Toepassingen

Wettelijke vereisten voor gegevens	Stapsgewijze instructies
Subsidieregelingen	Stapsgewijze instructies
App-beperkingen	Stapsgewijze instructies
Mobiele apparaten beheren	Stapsgewijze instructies
Gegevens migreren	Stapsgewijze instructies



Wettelijke vereisten voor gegevens

"De gegevens van mijn leerlingen, faculteit en personeel moeten vanwege wettelijke vereisten in de Verenigde Staten blijven."

Als beheerder kun je gegevens opslaan op een specifieke geografische locatie (de Verenigde Staten of het VK/Europa) met een **beleid voor gegevensregio's**.

- Je kunt één gegevensregio kiezen voor een deel van je gebruikers of verschillende gegevensregio's voor bepaalde afdelingen of teams.
- Plaats gebruikers in een organisatie-eenheid (om de instelling toe te passen op een bepaalde afdeling) of een configuratiegroep (om de instelling toe te passen op gebruikers in verschillende afdelingen).
- Gebruikers zonder een licentie voor Education Standard of Education Plus vallen buiten het beleid voor gegevensregio's.

Relevante Helpcentrum-documentatie

Een geografische locatie kiezen voor je gegevens

Stapsgewijze instructies

“

Het onderzoek van mijn faculteit moet in de Verenigde Staten blijven vanwege subsidieregelingen."

Subsidieregelingen

Als beheerder kun je ervoor kiezen het onderzoek van je faculteit op te slaan op een specifieke geografische locatie (in de Verenigde Staten of Europa) door een **beleid voor gegevensregio's te gebruiken**.

- Beleid voor gegevensregio's geldt voor het primaire exemplaar van 'data at rest' (inclusief back-ups) van de meeste Google Workspace-kernservices, die je in deze lijst kunt vinden.
- Bedenk van tevoren of het handig is om een beleid voor gegevensregio's in te stellen. Gebruikers die zich in een andere regio bevinden dan waar hun gegevens zijn opgeslagen, kunnen in sommige gevallen last hebben van grotere vertragingen.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Een geografische locatie kiezen voor je gegevens

Instructies Gegevensregio's*

Gegevensregio's bepalen

- Log in bij de **Beheerdersconsole.**
  - Opmerking: Je moet zijn ingelogd als hoofdbeheerder.
- Klik op **Bedrijfsprofiel** > **Meer bekijken** > **Gegevensregio's.**
- Selecteer de **organisatie-eenheid of configuratiegroep** die je wilt beperken tot een regio of selecteer de hele kolom om alle eenheden en groepen toe te voegen.
- Selecteer je regio: **Geen voorkeur, Verenigde Staten of Europa.**
- Klik op **Opslaan.**

Relevante Helpcentrum-documentatie

Een geografische locatie kiezen voor je gegevens

* Onderwijsinstellingen moeten Education Standard of Education Plus hebben om gegevens op te kunnen slaan in specifieke regio's met de functie voor gegevensregio's.

App-beperkingen

Met **contextbewuste toegang*** kun je gedetailleerd toegangscontrolebeleid maken voor apps, op basis van kenmerken als gebruikersidentiteit, apparaatbeveiligingsstatus en IP-adres. Je kunt zelfs de toegang tot apps buiten je netwerk beperken.

"Ik wil de toegang tot specifieke apps beperken wanneer gebruikers op het netwerk zitten."

- Je kunt beleid voor contextbewuste toegang toepassen op de kernservices van Google Workspace for Education.
- Als een gebruiker bijvoorbeeld inlogt bij een kernservice van Google Workspace op school en naar een koffiebar loopt, wordt het beleid voor contextbewuste toegang voor die service opnieuw gecontroleerd wanneer de gebruiker van locatie verandert.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Overzicht van contextbewuste toegang

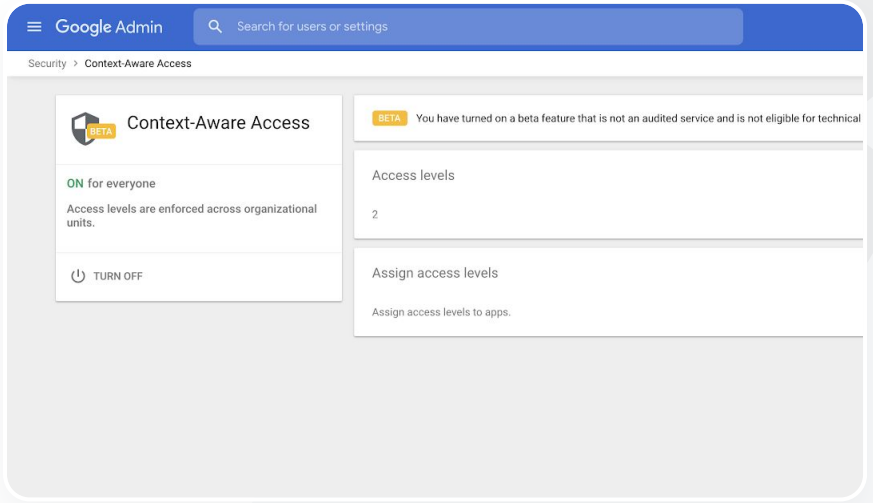
Niveaus voor contextbewuste toegang toewijzen aan apps

* Onderwijsinstellingen moeten Education Standard of Education Plus hebben om beleid voor contextbewuste toegang te kunnen toepassen.

Instructies Contextbewuste toegang

Contextbewuste toegang gebruiken

- Log in bij de **Beheerdersconsole.**
- Selecteer **Beveiliging** > **Contextbewuste toegang > Toewijzen.**
- Selecteer **Toegangsniveaus toewijzen** om je lijst met apps te bekijken.
- Selecteer een **organisatie-eenheid of een configuratiegroep** om de lijst te sorteren.
- Selecteer **Toewijzen** naast de app die je wilt wijzigen.
- Selecteer een of meer toegangsniveaus.
- Maak meerdere niveaus als je wilt dat gebruikers aan meerdere voorwaarden voldoen.
- Klik op **Opslaan.**



Relevante Helpcentrum-documentatie

Overzicht van contextbewuste toegang

Niveaus voor contextbewuste toegang toewijzen aan apps

Mobiele apparaten beheren

Met **geavanceerd mobiel beheer** krijg je meer controle over de gegevens van je organisatie via mobiele apparaten. Je kunt de functies van een mobiel apparaat beperken, apparaatversleuteling vereisen, apps beheren op Android-apparaten, iPhones en iPads, en zelfs gegevens wissen van een apparaat.

- In de Beheerdersconsole kun je apparaten goedkeuren of verwijderen, blokkeren of het blokkeren opheffen.
- Als iemand een apparaat kwijtraakt of zich uitschrijft bij de school, kun je het account of profiel van een gebruiker wissen, of zelfs alle gegevens uit de specifieke beheerde apparaatmodule verwijderen. Deze gegevens zijn wel nog beschikbaar op een computer of via een webbrowser.

> Ik wil beleid kunnen beheren en toepassen op alle soorten apparaten (iOS, Windows 10, enz.) binnen mijn district en niet alleen op Chromebooks; vooral als een apparaat is gehackt."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Geavanceerd mobiel beheer instellen

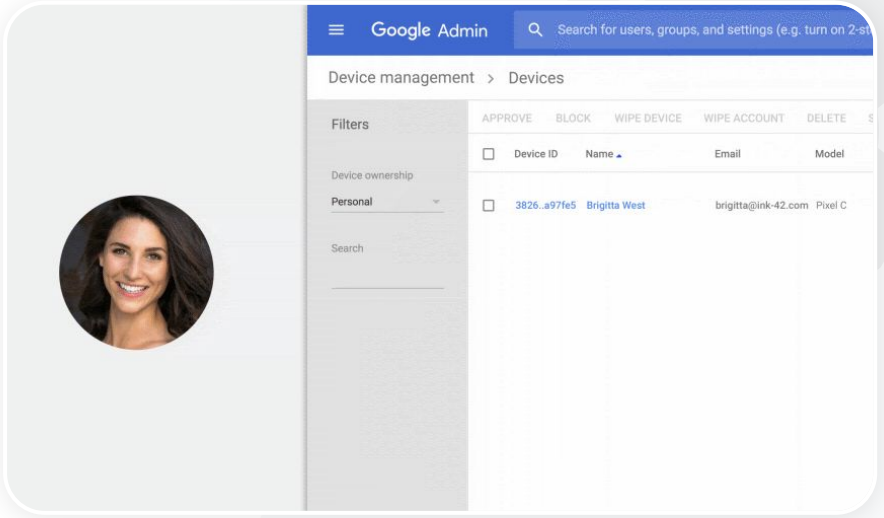
Een apparaat goedkeuren, blokkeren, verwijderen of het blokkeren opheffen

Gegevens van een apparaat verwijderen

Instructies Geavanceerd mobiel beheer inschakelen

Aanzetten

- Log in bij de **Beheerdersconsole**.
- Ga naar de **Beheerdersconsole** > **apparaten**.
- Klik links op **Instellingen** > **Algemene instellingen**.
- Klik op **Algemeen** > **Mobiel beheer**.
- Laat de organisatie-eenheid op het hoogste niveau staan als je wilt dat de instelling voor iedereen geldt. Selecteer anders een onderliggende organisatie-eenheid.
- Selecteer **Geavanceerd**.
- Klik op **Opslaan**.



Relevante Helpcentrum-documentatie

Geavanceerd mobiel beheer instellen

Een apparaat goedkeuren, blokkeren, verwijderen of het blokkeren opheffen

Gegevens van een apparaat verwijderen

Gegevens migreren

Gebruik de **migratiehandleidingen** om de gegevens van je hele organisatie (zoals e-mails, agenda's, contacten, mappen, bestanden en rechten) over te zetten naar Google Workspace.

> We stappen over op Google Workspace en moeten al onze gegevens migreren naar onze nieuwe Google-omgeving."

Stapsgewijze instructies

Gegevens van <1000 gebruikers

Bekijk de productmatrix om te achterhalen welke oplossing het beste werkt voor jouw onderwijsinstelling.

Meer informatie

Gegevens van 1000+ gebruikers

Gebruik Google Workspace Migrate om de grote hoeveelheid gegevens op een effectieve manier te migreren.

Meer informatie

Relevante Helpcentrum-documentatie

De gegevens van je organisatie migreren naar Google Workspace
Productmatrix voor Google Workspace-migraties
Over Google Workspace Migrate
Google Workspace Migrate installeren en instellen

Education Standard | Education Plus

Terug naar de inhoudsopgave

Geavanceerde beheeropties | Beveiligings- en analysetools

Instructies Google Workspace Migrate

Voordat je begint

Meld je aan voor de bètaversie en bevestig dat je voldoet aan de systeemvereisten.

Instructies

1. De **Google Cloud Console** instellen

API's inschakelen
De OAuth-webclient-ID maken
Een Google Workspace-serviceaccount maken

1. De **Beheerdersconsole** instellen

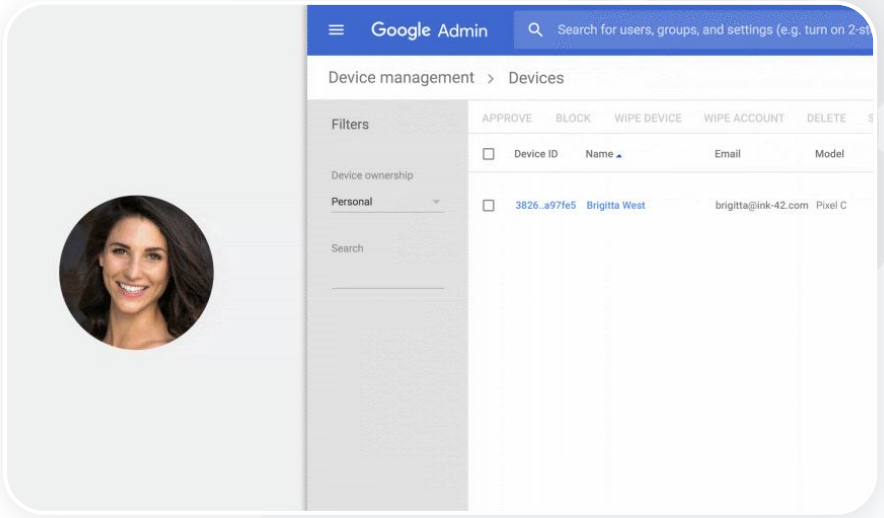
Beheerdersrollen instellen
Je client-ID autoriseren

3. **Downloaden en installeren**

De installatieprogramma's downloaden
De databases installeren
Het platform installeren en instellen
De nodeservers installeren
(Optioneel) De nodeserver instellen zodat deze TLS gebruikt

3. Een **migratieproduct** instellen

De versleutelingssleutel instellen
Database-instellingen aanpassen
Het callbackadres instellen
De nodeservers toevoegen
Een project maken



Relevante Helpcentrum-documentatie

Over Google Workspace Migrate
Google Workspace Migrate installeren en instellen
De gegevens van je organisatie migreren naar Google Workspace
Productmatrix voor Google Workspace-migraties

Hulp nodig? Neem contact op met een Google Cloud-partner.

Tools voor lesgeven en leren

Geef docenten extra opties in je digitale leeromgeving met verbeterde videocommunicatie, functies die lessen verrijken en tools om de academische integriteit te verbeteren.

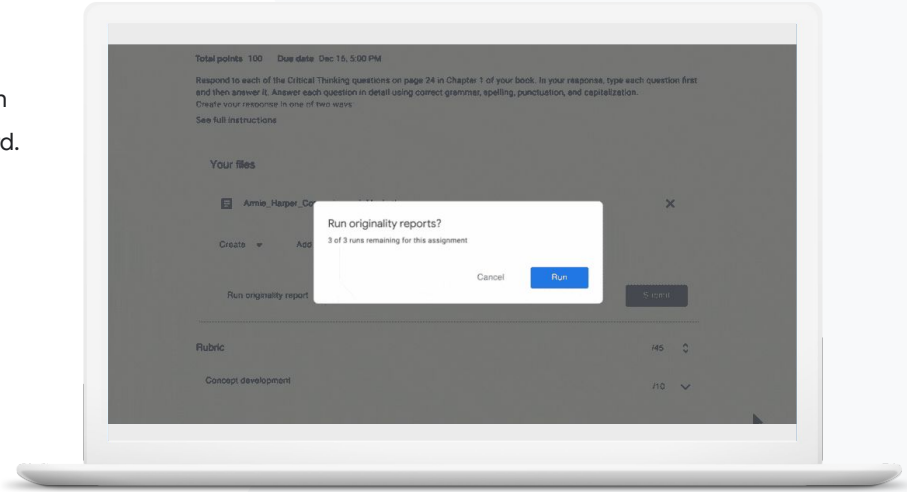
Originaliteitsrapporten

Google Meet

Originaliteitsrapporten

Wat is dit?

Docenten en leerlingen kunnen de authenticiteit van werk controleren. Originaliteitsrapporten gebruiken Google Zoeken om het werk van leerlingen te vergelijken met miljarden webpagina's en miljoenen boeken. In originaliteitsrapporten wordt gelinkt naar gevonden webpagina's en wordt niet-geciteerde tekst gemarkeerd.



Toepassingen

Scannen op plagiaat	Stapsgewijze instructies
Plagiaatcontroles als leerkans	Stapsgewijze instructies

Scannen op plagiaat

"Ik wil controleren of het werk van mijn leerlingen plagiaat of onjuiste citaten bevat."

Docenten kunnen de authenticiteit van werk van leerlingen controleren met **originaliteitsrapporten**. Originaliteitsrapporten gebruiken Google Zoeken om het werk van leerlingen te vergelijken met miljarden webpagina's en miljoenen boeken als bronmateriaal.

- Docenten die de Teaching and Learning Upgrade of Education Plus gebruiken, hebben onbeperkte toegang tot originaliteitsrapporten.
- Opmerking: Originaliteitsrapporten zijn momenteel alleen beschikbaar voor:
  - Google-accounts waarvan de ingestelde taal Engels is,
  - werk dat is gemaakt in Documenten,
  - Google for Education-accounts.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Originaliteitsrapporten aanzetten

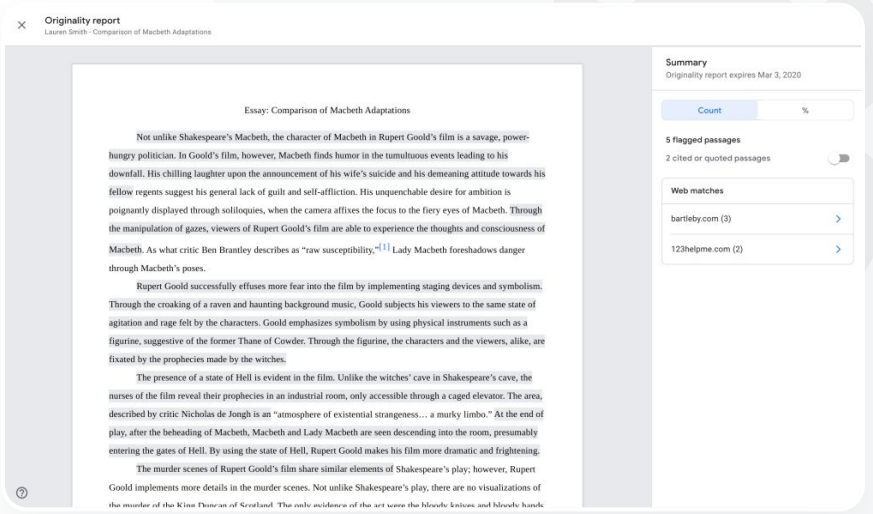
Instructies Controle achteraf door de docent

Originaliteitsrapporten aanzetten voor een opdracht

- Log in op je Classroom-account via **classroom.google.com.**
- Selecteer de relevante lesgroep uit de lijst en kies **Schoolwerk.**
- Selecteer **Maken** > **Opdracht.**
- Vink het vakje naast **Originaliteitsrapporten** aan om de functie aan te zetten.

Een originaliteitsrapport uitvoeren op werk van leerlingen

- Selecteer het betreffende bestand van de leerling uit de lijst en klik erop om het te openen in de nakijktool.
- Klik onder de opdracht van de leerling op **Originaliteit controleren.**



Relevante Helpcentrum-documentatie

Originaliteitsrapporten aanzetten

Plagiaatcontroles als leerkans

"Ik wil mijn leerlingen de mogelijkheid geven om hun werk op plagiaat te controleren en de 'controle op valsspelen' gebruiken als een leermoment."

Leerlingen kunnen content zonder citaat en onbedoelde plagiaat opsporen voordat ze hun werk inleveren door een **originaliteitsrapport** uit te voeren. Dit kunnen ze 3 keer per opdracht doen. In originaliteitsrapporten worden de documenten van leerlingen vergeleken met verschillende bronnen. Tekst zonder citaat wordt gemarkeerd, waardoor ze kunnen leren, fouten kunnen corrigeren en hun schoolwerk vol vertrouwen kunnen inleveren.

- Docenten die de Teaching and Learning Upgrade of Education Plus gebruiken, kunnen originaliteitsrapporten gebruiken zo vaak als ze willen. Met Education Fundamentals kunnen ze deze rapporten slechts 5 keer per lesgroep aanzetten.
- Nadat het werk is ingeleverd, maakt Classroom automatisch een rapport dat alleen zichtbaar is voor de docent. Als je een opdracht inlevert en dit weer ongedaan maakt, maakt Classroom opnieuw een originaliteitsrapport voor de docent.

Stapsgewijze instructies

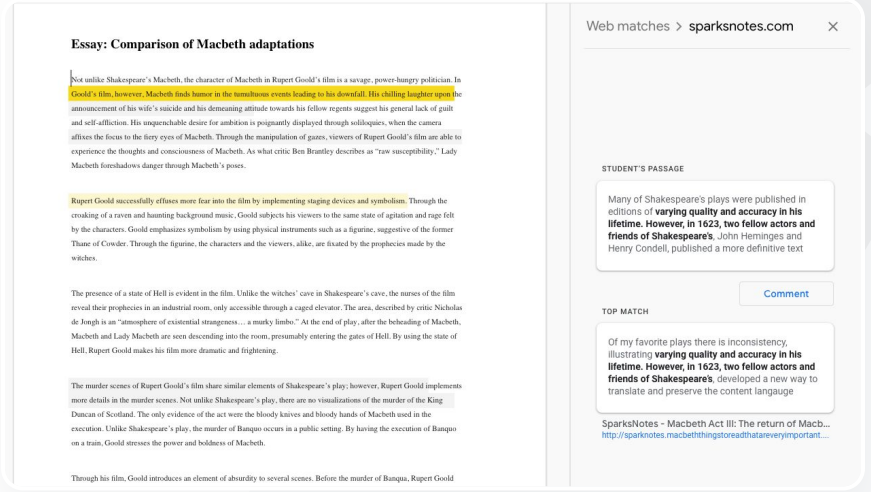
Relevante Helpcentrum-documentatie

Een originaliteitsrapport laten maken voor je werk

Instructies Controle vooraf door de leerling

Originaliteitsrapporten maken (leerlingen)

- Log in op je Classroom-account via classroom.google.com.
- Selecteer de relevante lesgroep uit de lijst en kies **Schoolwerk.**
- Selecteer de relevante opdracht in de lijst en klik op **Opdracht bekijken.**
- Ga naar **Jouw werk** en selecteer **Uploaden** of **Bestand maken.**
- Klik naast **Originaliteitsrapporten** op **Uitvoeren.**
- Klik op **Originaliteitsrapport bekijken** onder de bestandsnaam van de opdracht om het rapport te openen.
- Klik onderaan op **Bewerken** om de opdracht te reviseren, te herschrijven of om op de juiste manier de aangegeven passages te citeren.



Relevante Helpcentrum-documentatie

Een originaliteitsrapport laten maken voor je werk

Google Meet

Wat is dit?

De geavanceerde functies van Google Meet zijn onder andere livestreamen, breakoutruimtes, opnamen van vergaderingen in Drive, deelnamerapporten, vergaderingen met tot wel 250 deelnemers en meer.

Toepassingen

Beveiligde videovergaderingen	Stapsgewijze instructies
Betere beveiliging van videovergaderingen	Stapsgewijze instructies
Lessen opnemen	Stapsgewijze instructies
Faculteitsvergaderingen opnemen	Stapsgewijze instructies
Gemiste lessen	Stapsgewijze instructies
Vergaderingen livestreamen	Stapsgewijze instructies
Schoolevenementen livestreamen	Stapsgewijze instructies
Vragen stellen	Stapsgewijze instructies
Ideeën verzamelen	Stapsgewijze instructies
Kleine leerlinggroepen	Stapsgewijze instructies
Deelname bijhouden	Stapsgewijze instructies

Beveiligde videovergaderingen

Met Google Meet kunnen scholen gebruikmaken van dezelfde infrastructuur met een beveiligd ontwerp, ingebouwde bescherming en wereldwijde netwerken als Google gebruikt, om je informatie te beveiligen en je privacy te waarborgen.
Je kunt vertrouwen op de volgende beveiligingsmaatregelen van Google Meet:

> Hoe veilig is Google Meet nou echt?"

- **Privacy en naleving:** Handhaaf de strenge beveiligingsstandaarden voor het onderwijs om de gegevens van leerlingen en scholen beter te beveiligen.
- **Versleuteling:** Alle gegevens van de client naar Google zijn versleuteld.
- **Antimisbruikmaatregelen:** De moderator controleert wie er aanwezig is en zorgt dat alleen de juiste mensen toegang hebben.
- **Veilige implementatie, toegang en functies:** Er is een groot aantal voorzorgsmaatregelen genomen om vergaderingen privé en beveiligd te houden.
- **Reactie op incidenten:** Dit is een belangrijk onderdeel van het algemene beveiligings- en privacyprogramma van Google en is essentieel om te voldoen aan privacyregels over de hele wereld.
- **Betrouwbaarheid:** Onze cloudinfrastructuur met meerdere lagen is schaalbaar en in staat pieken in gebruik op te vangen.
- **Bepalen wie er deelneemt:** Verbeteringen in het aanklopmechanisme zodat verzoeken in bulk kunnen worden beheerd en aanklopverzoeken kunnen worden geblokkeerd wanneer er is voldaan aan bepaalde criteria.
- **Bedieningselementen voor vergrendeling:** Moderators bepalen wie kan chatten, presenteren en spreken tijdens een virtuele vergadering.

Stapsgewijze instructies

Betere beveiliging van videovergaderingen

"Hoe maak ik videovergaderingen nog veiliger voor mijn school?"

De Teaching and Learning Upgrade en Education Plus bevatten extra functies tegen misbruik, zoals verplichte goedkeuring voor externe deelnemers, verbeterde bedieningselementen voor het beheer van vergaderingen en **vergaderingen met bijnaam** om te voorkomen dat afgelopen vergaderingen opnieuw worden gebruikt. Wanneer de laatste deelnemer de vergadering heeft verlaten, kunnen deelnemers er niet opnieuw in. Leerlingen kunnen pas weer deelnemen als een docent de vergadering met de bijnaam opnieuw start.

- Bij een **vergadering met bijnaam** hebben de deelnemers geen toegang meer nadat de laatste deelnemer de vergadering heeft verlaten. De 10-cijferige code van de vergadering werkt dan niet meer.
- Leerlingen kunnen pas weer deelnemen als een docent de vergadering met de bijnaam opnieuw start.
- Docenten kunnen de vergadering voor alle deelnemers beëindigen, waardoor ze niet kunnen blijven nadat de docent is vertrokken.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

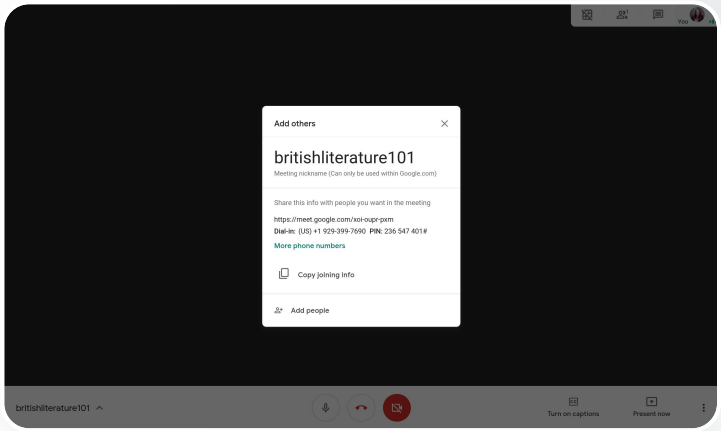
Beveiliging en privacy voor onderwijs in Google Meet

Een Google Meet-videovergadering starten

Instructies Vergaderingen met bijnaam

Een vergadering met bijnaam maken

- Gebruik een korte link, zoals g.co/meet/[BIJNAAM INVOEREN].
- Ga naar meet.google.com of open de mobiele app van Google Meet en geef de bijnaam van de vergadering op in het veld **Vergadering starten of deelnemen aan vergadering**.



Hoe het werkt

Als een docent een vergadering met een bijnaam start, wordt een code van de vergadering van 10 tekens gemaakt en wordt die code tijdelijk gekoppeld aan de bijnaam.

Nadat de laatste persoon de vergadering heeft verlaten of als de docent de vergadering beëindigt, verloopt de tijdelijke code van de vergadering en is de bijnaam niet meer gekoppeld aan de code van de vergadering.

Als leerlingen geen rechten hebben om vergaderingen te maken, kunnen ze de bijnaam of de code van de vergadering niet gebruiken.

Docenten kunnen de bijnaam opnieuw gebruiken. Er wordt dan een nieuwe tijdelijke code van de vergadering gemaakt. De leerlingen kunnen dan weer deelnemen met gebruik van de bijnaam.

Relevante Helpcentrum-documentatie

Beveiliging en privacy voor onderwijs in Google Meet

Een Google Meet-videovergadering starten

Lessen opnemen

Met de Teaching and Learning Upgrade en Education Plus kunnen gebruikers hun vergaderingen **opnemen** en ze automatisch en voor onbeperkte tijd opslaan in Drive. Dit maakt het makkelijk om lessen, workshops en werksessies te archiveren en te delen.

> Onze campus biedt grote online lesgroepen die we moeten opnemen voor mensen die op afstand leren en voor leerlingen die er niet bij kunnen zijn."

- Als je docenten Classroom gebruiken, kunnen ze de Google Meet-integratie gebruiken om een unieke link te maken voor elke les, die wordt weergegeven in de Classroom-stream en op de pagina Schoolwerk.
- De link fungeert als speciale vergaderruimte voor elke lesgroep, zodat docenten en leerlingen eenvoudig kunnen deelnemen.
- Gebruik deze integratie om eenvoudig lessen op te nemen.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Google Meet instellen voor onderwijs op afstand

Faculteitsvergaderingen opnemen

Met de Teaching and Learning Upgrade en Education Plus worden **opnamen** van videovergaderingen automatisch opgeslagen in Drive. Ze blijven daar bewaard zolang de gebruiker de opname nodig heeft. Zo kunnen vergaderingen, cursussen voor loopbaanontwikkeling of bestuursvergaderingen makkelijk worden gearchiveerd en gedeeld.

- We raden IT-beheerders aan om opnames alleen aan te zetten voor de faculteit en docenten.
- Je kunt aparte organisatie-eenheden toevoegen voor je faculteit en leerlingen, en voor beide groepen verschillende toegangsregels instellen.
- Als je Classroom gebruikt en geverifieerde docenten hebt, kun je de toegang inschakelen voor de docentengroep.

Relevante Helpcentrum-documentatie

Google Meet instellen voor onderwijs op afstand

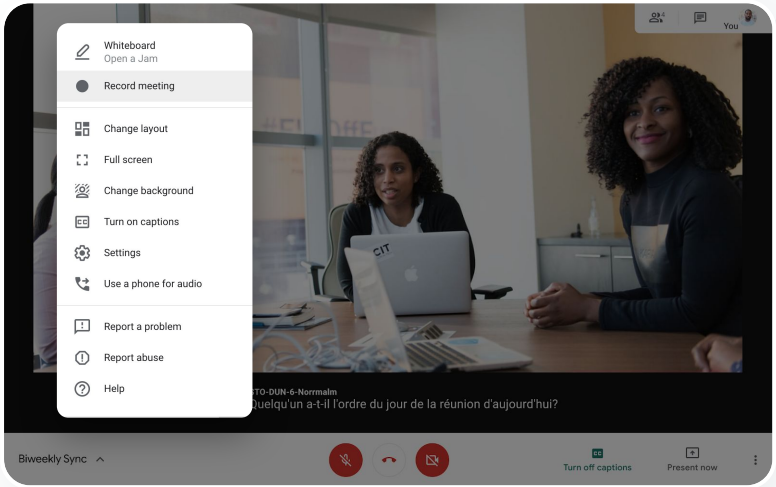
"We houden regelmatig online personeelsvergaderingen en al deze vergaderingen moeten worden opgenomen. Daarnaast willen we cursussen voor loopbaanontwikkeling en onze bestuursvergaderingen opnemen."

Stapsgewijze instructies

Instructies Opnemen

Een vergadering opnemen

- Open de vergadering in je Agenda en selecteer **Deelnemen via Google Meet.**
- Open op de bevestigingspagina van de vergadering **het optiemenu** door te klikken op de 3 verticale puntjes rechtsonder.
- Klik op **Vergadering opnemen**. Er verschijnt een rode stip rechtsonder in het scherm om aan te geven dat de vergadering wordt opgenomen.
- Er wordt automatisch een videobestand van de vergadering opgeslagen in je Drive.



Relevante Helpcentrum-documentatie

Google Meet instellen voor onderwijs op afstand

Gemiste lessen

Ik wil een opname bekijken van een les die ik heb gemist."

Alle gebruikers hebben toegang tot de Drive in het domein van de school.
Met de Teaching and Learning Upgrade en Education Plus worden opnamen van videovergaderingen automatisch opgeslagen in de Drive van de organisator van de vergadering. Als je de opgenomen vergadering wilt **bekijken**, vraag je de organisator om de link van de opname of open je deze via de Agenda-afspraak.

- Opnamen worden opgeslagen in de Drive van de organisator van de vergadering.
- Deelnemers aan een vergadering in dezelfde organisatie-eenheid als de organisator van de vergadering krijgen automatisch toegang tot de opname.
- Als de organisator van de vergadering wordt gewijzigd, wordt de link naar de oorspronkelijke organisator van de afspraak gestuurd.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Een videovergadering opnemen

Instructies Opnamen bekijken en delen

Een opname delen

- Selecteer het bestand.
- Klik op het icoon **Delen**.
- **Voeg** goedgekeurde kijkers **toe**.

OF

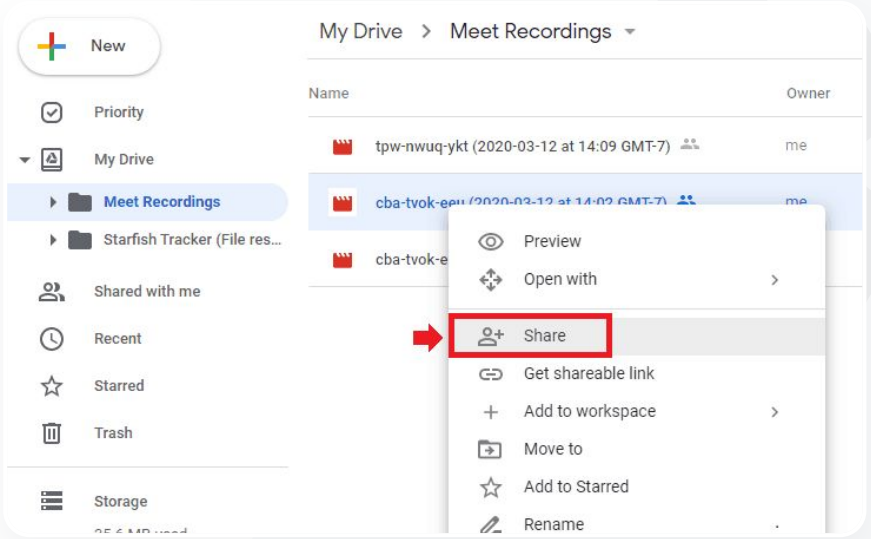
- Selecteer het **linkicoon**.
- **Plak** de link in een e-mail of chatbericht.

Een opname downloaden

- Selecteer het bestand.
- Klik op het icoon **Meer** > **Downloaden.**
- **Dubbelklik** op het gedownloade bestand om het af te spelen.

De opname afspelen vanuit Drive

- Dubbelklik in Drive op de opname om deze af te spelen. Er wordt Verwerken weergegeven tot het bestand online kan worden bekeken.
- Als je een opname wilt toevoegen aan je Drive, selecteer je het bestand en klik je op **Toevoegen aan mijn Drive.**



Relevante Helpcentrum-documentatie

Een videovergadering opnemen

Vergaderingen livestreamen

Je kunt livestreamen naar maximaal 10.000 kijkers binnen het domein met de Teaching and Learning Upgrade of naar maximaal 100.000 kijkers binnen het domein met Education Plus. Kijkers kunnen deelnemen door te klikken op de link van de livestream. Deze deelt de organisator in een e-mail of via de Agenda-uitnodiging. Vraag aan je IT-beheerder of je rechten hebt om te livestreamen.

- We raden IT-beheerders aan om livestreamen alleen aan te zetten voor de faculteit en het personeel.
- Gebruik voor grote evenementen een livestream in plaats van alle gebruikers mee te laten doen aan een interactieve videovergadering. Zo verloopt het evenement voor iedereen prettiger.
- Als een gebruiker de livestream mist, kan hij of zij de opname bekijken nadat de vergadering is beëindigd.

"We moeten onze personeels- en faculteitsvergaderingen kunnen livestreamen voor andere stakeholders en ouders."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Google Meet instellen voor onderwijs op afstand

Schoolevenementen livestreamen

> We willen onze sportevenementen en andere belangrijke gebeurtenissen zoals de diploma-uitreiking of het afstudeerfeest livestreamen voor degenen die er niet bij kunnen zijn."

Zend live uit naar je schoolcommunity met **livestreams**. Je hoeft alleen maar te klikken op de link van de livestream die je hebt gekregen van de organisator via een e-mail of de Agenda-afspraak. Vraag aan je IT-beheerder of je rechten hebt om te livestreamen. Anders kun je de opname bekijken nadat de vergadering is beëindigd.

- Gebruik de livestreamfunctie van Google Meet om je hele community te betrekken bij diploma-uitreikingen, sportevenementen of vergaderingen van de ouderraad.
- Met de Teaching and Learning Upgrade kun je naar maximaal 10.000 kijkers binnen het domein livestreamen en met Education Plus naar maximaal 100.000 kijkers binnen het domein.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

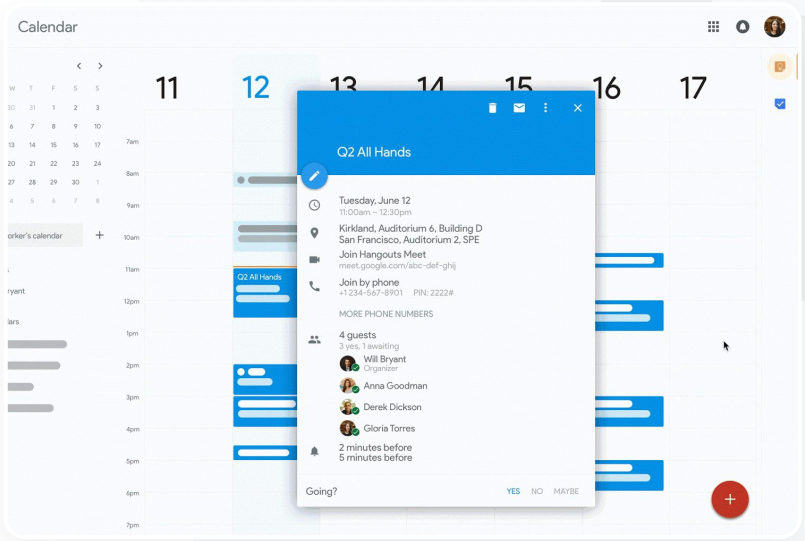
Google Meet instellen voor onderwijs op afstand

Instructies Livestreaming

Rechten voor een livestream geven

- Open **Google Agenda.**
- Selecteer **Maken** > **Meer opties.**
- Vul de afspraakgegevens in, zoals de datum, tijd en beschrijving.
- Voeg maximaal 250 gasten toe die kunnen deelnemen aan de videovergadering. Dit houdt in dat anderen ze kunnen zien en horen, en dat ze kunnen presenteren. Je kunt mensen van andere organisaties toevoegen.
- Klik op **Videovergadering Toevoegen** > **Meet.**
- Klik naast 'Deelnemen aan Meet' op de **pijl omlaag** en dan op **Livestream toevoegen.**
- Als je het maximale aantal personen binnen je domein wilt uitnodigen dat is toegestaan met je betaalde versie, klik je op **Kopiëren** en deel je de URL van de livestream via een e-mail of chatbericht.
- Selecteer **Opslaan.**
- Livestreams worden niet automatisch gestart. Selecteer tijdens de vergadering **Meer** > **Livestream starten.**

Opmerking: Tip: Alleen gasten binnen je organisatie kunnen de livestream bekijken.



Relevante Helpcentrum-documentatie

Google Meet instellen voor onderwijs op afstand

Vragen stellen

Gebruik de functie **Vraag en antwoord** in Google Meet om leerlingen betrokken te houden en de lesgroep interactiever te maken. Aan het einde van de virtuele lesgroep krijgen docenten zelfs een gedetailleerd rapport van alle vragen en antwoorden.

> Ik wil makkelijk vragen kunnen stellen, de kennis van de leerlingen meten en communiceren met de lesgroep om ze betrokken te houden."

- Moderators kunnen zoveel vragen stellen als nodig is. Ze kunnen vragen ook filteren, sorteren, als beantwoord markeren, verbergen of er prioriteit aan geven.
- Na elke vergadering waarin vragen zijn aangezet, krijgt de moderator automatisch een vragenrapport via e-mail.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Deelnemers vragen stellen in Google Meet

Instructies Vraag en antwoord

Een vraag stellen:

- Klik in een vergadering rechtsboven op het **activiteitenicoon** > **Vragen** (Als je vragen en antwoorden wilt aanzetten, selecteer je **Vragen en antwoorden aanzetten**).
- Als je een vraag wilt stellen, klik je rechtsonder op **Een vraag stellen**.
- **Voer je vragen in** > selecteer **Posten**.

Vragenrapport bekijken:

- Na een vergadering krijgt de moderator een **e-mail met het vragenrapport**.
- Open de e-mail > klik op het **rapport in de bijlage**.

Relevante Helpcentrum-documentatie

Deelnemers vragen stellen in Google Meet

Ideeën verzamelen

Ik wil makkelijk ideeën van leerlingen en andere docenten kunnen verzamelen terwijl ik een lesgroep of vergadering leid."

Degene die een virtuele meeting heeft gepland of start, kan een **poll** maken voor de deelnemers aan de vergadering. Met deze functie kun je op een snelle en aansprekende manier informatie verzamelen van alle leerlingen of deelnemers aan een vergadering.

- Moderators kunnen een poll opslaan en deze later tijdens een vergadering posten. Ze worden opgeslagen in het gedeelte Polls van een virtuele vergadering.
- Na de vergadering krijgt de moderator automatisch een rapport met de resultaten van de poll via e-mail.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Polls uitvoeren in Google Meet

Instructies Polls uitvoeren

Een poll maken

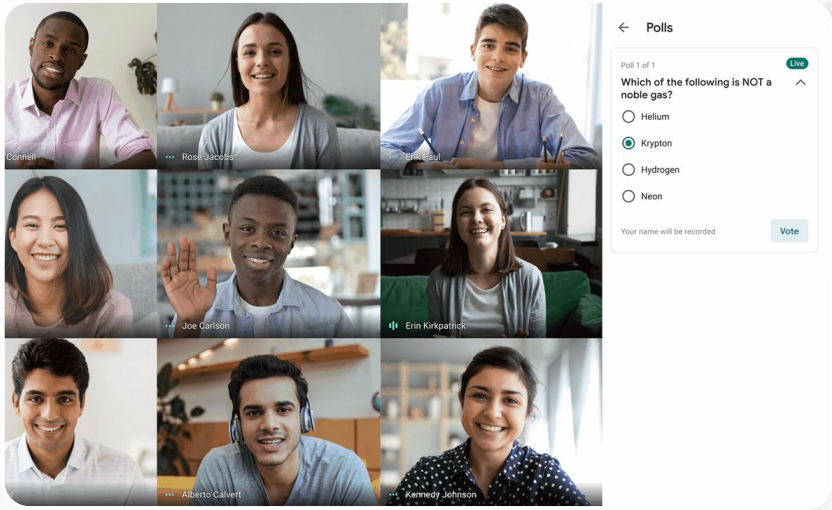
- Klik rechtsboven in een vergadering op het **activiteitenicoon** > **Poll**.
- Kies **Een poll starten.**
- Geef een vraag op.
- Selecteer **Lanceren** of **Opslaan.**

Een poll modereren:

- Klik rechtsboven in een vergadering op het **activiteitenicoon** > **Poll**.
- Als je wilt dat deelnemers de resultaten van een poll in realtime kunnen zien, zet je **Iedereen de resultaten laten zien** op **Aan.**
- Als je een poll wilt sluiten zodat mensen er niet meer op kunnen stemmen, klik je op **Poll beëindigen.**
- Als je een poll definitief wilt verwijderen, klik je op het **verwijdericoon.**

Het rapport van een poll bekijken:

- Na een vergadering krijgt de moderator **een e-mail met een rapport.**
- Open de e-mail > selecteer het **rapport in de bijlage.**



Relevante Helpcentrum-documentatie

[Polls uitvoeren in Google Meet]

Kleine leerlinggroepen

Docenten kunnen **breakoutruimtes** gebruiken om leerlingen in kleinere groepen te verdelen tijdens virtuele lesgroepen. Breakoutruimtes moeten door moderators worden gestart tijdens een videogesprek op een computer. Je kunt breakoutruimtes momenteel niet livestreamen of opnemen.

- Je kunt maximaal 100 breakoutruimtes maken in een videovergadering.
- Docenten kunnen makkelijk schakelen tussen breakoutruimtes zodat ze groepen kunnen helpen, indien nodig.
- Beheerders kunnen ervoor zorgen dat alleen de faculteit of het personeel breakoutruimtes kunnen maken.

Relevante Helpcentrum-documentatie

Breakoutruimtes gebruiken in Google Meet

> We bieden alleen leren op afstand aan en hebben een manier nodig om de kinderen makkelijk in groepen te verdelen, gesprekken in de gaten te houden, bij discussies aan te sluiten en de groep weer samen te voegen."

Stapsgewijze instructies

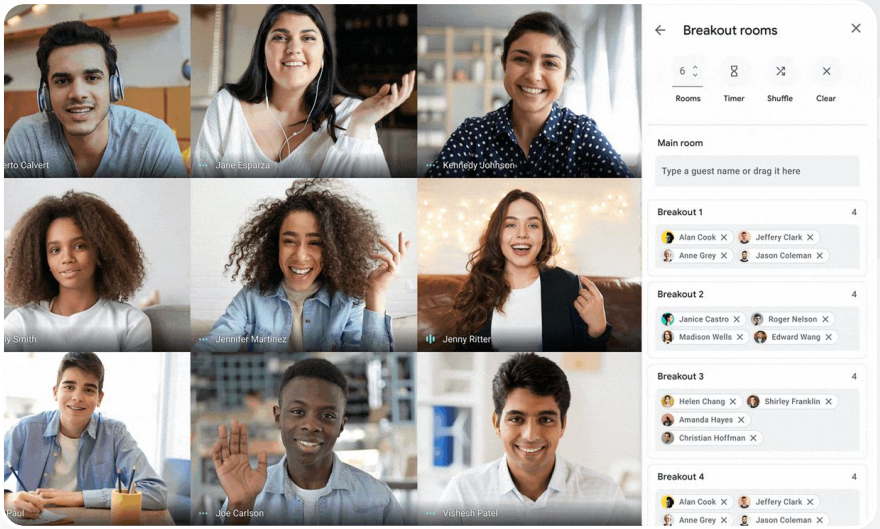
Instructies Breakoutruimtes maken

Breakoutruimtes maken

- Start een videogesprek.
- Selecteer rechtsboven het **activiteitenicoon** > **Breakoutruimtes.**
- Geef in het deelvenster Breakoutruimtes aan **hoeveel breakoutruimtes** je nodig hebt.
- Leerlingen worden vervolgens verdeeld over de ruimtes, maar de moderators kunnen mensen indien nodig verplaatsen naar een andere ruimte.
- Klik rechtsonder op **Chatruimtes** openen.

Vragen beantwoorden in verschillende breakoutruimtes

- Er verschijnt een melding onderaan in het scherm van de moderator als deelnemers om hulp vragen. Selecteer **Deelnemen** om naar de breakoutruimte van de betreffende deelnemer te gaan.



Relevante Helpcentrum-documentatie

[Breakoutruimtes gebruiken in Google Meet]

Deelname bijhouden

Deelname bijhouden geeft je een automatisch deelnamerapport voor elke vergadering met 5 of meer deelnemers. In het rapport zie je wie er heeft deelgenomen aan het gesprek, de e-mailadressen van de deelnemers en hoelang ze hebben meegedaan aan de virtuele lesgroep.

- Je kunt bijhouden wie aanwezig is tijdens livestreams met livestreamrapporten.
- Moderators kunnen deelname bijhouden en livestreamrapporten aan- of uitzetten in een vergadering of in de Agenda-afspraak.

"We vinden het moeilijk om bij te houden wie aanwezig is bij onze online lesgroepen. Ik heb een makkelijke manier nodig om de aanwezigheid voor alle lesgroepen in mijn hele domein bij te houden."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

Deelname bijhouden in Google Meet

Instructies Deelnamerapporten

Instructies voor tijdens de vergadering:

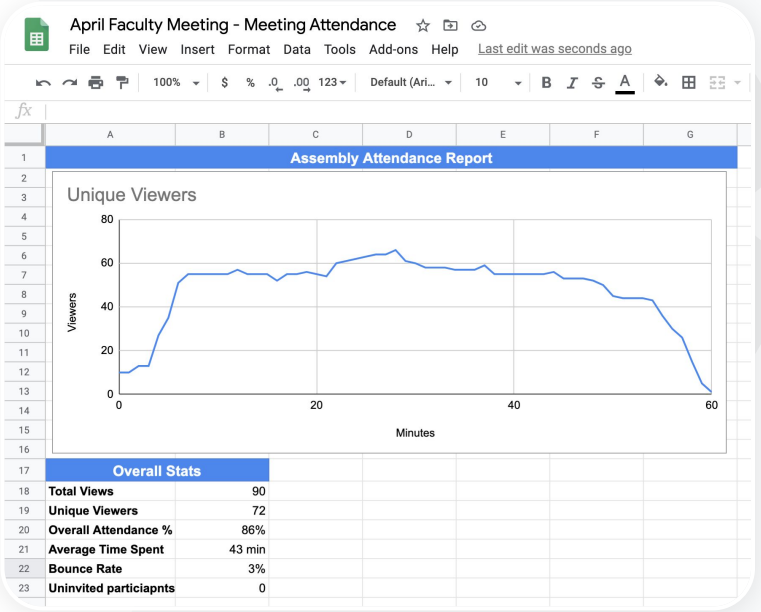
- Start een videogesprek.
- Selecteer onderaan het **menu-icoon.**
- Klik op het **instellingenicoon** > **Bedieningselementen voor host.**
- Zet **Deelname bijhouden** aan of uit.

Instructies voor het gebruik van de Agenda:

- **Zet Google Meet-vergaderingen aan** vanuit een Agenda-afspraak.
- Selecteer aan de rechterkant het **instellingenicoon**.
- Vink het vakje aan naast **Deelname bijhouden** > klik op **Opslaan.**

Het deelnamerapport downloaden:

- Na een vergadering krijgt de moderator **een e-mail met een rapport.**
- Open de e-mail > selecteer het **rapport in de bijlage.**



Relevante Helpcentrum-documentatie

[Deelname bijhouden in Google Meet]

Bedankt

Google for Education