Google for Education

Meer dan 40 manieren om de betaalde versies van Google Workspace for Education te gebruiken

goo.gle/use-edu-workspace

Hoe gebruik je deze presentatie?

Deze presentatie bestaat uit een selectie van populaire use-cases die beschikbaar zijn in de **betaalde versies van Google Workspace for Education**. Met deze tools verbeter je **de gegevensbeveiliging, de efficiëntie van de docent, de betrokkenheid van de leerling** en **de samenwerking op de hele school** en nog veel meer.

De presentatie is ingedeeld in **functies**, gevolgd door **gangbare use-cases** met daarna eenvoudige **instructies** voor het gebruik van de functies. Neem de hele presentatie door en ontdek wat je allemaal kunt doen met de betaalde versies van 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 Plus

Bestaat uit de Education Standard, de Teaching and Learning Upgrade en andere functies die alleen voor Plus beschikbaar zijn.

Education Plus biedt leerlingen, docenten, leidinggevenden in het onderwijs en IT-beheerders een **complete** edtech-oplossing met gebruiksvriendelijke tools voor **geavanceerde beveiliging en inzichten en uitgebreide lesmogelijkheden**.

Google Workspace for Education Standard

Geavanceerde tools voor beveiliging en inzichten waarmee je risico's en bedreigingen inperkt dankzij meer zichtbaarheid en controle in de leeromgeving.

Teaching and Learning Upgrade

Verbeterde tools voor lesgeven en leren hebben impact op het onderwijs. Lessen worden persoonlijker en lesgroepen efficiënter. Je kunt vanaf elke locatie lesgeven en leren.

Inhoudsopgave

Geavanceerde functies voor beveiliging en inzichten

Beveiligingsdashboard

- Hoeveelheid spam
- Extern bestanden delen
- Apps van derden
- Poging tot phishing

Pagina Beveiligingsstatus

- Best practices voor beveiliging
- Aanbevelingen voor risicogebieden

Onderzoekstool

- Ongepast materiaal dat wordt gedeeld
- Per ongeluk gedeelde bestanden
- Phishing- en malwaremails
- Kwaadwillende gebruikers tegenhouden
- Uitgebreidere beveiligingsinzichten
- Vergaderingen zonder toezicht voorkomen

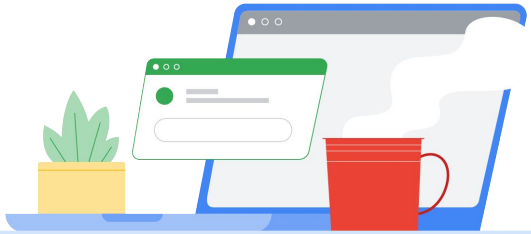
Domeinbeheer

- Gmail-bijlagen scannen op bedreigingen
- Gebruiksdashboards en -rapporten maken
- Bestanden makkelijker vinden
- Interne documenten ordenen
- Afdelingsgroepen automatisch vullen
- Doelgroep maken voor het intern delen van bestanden
- Het delen van bestanden beperken
- Beperkingen voor de Workspace-app
- Opslag beheren
- Gegevensregelgeving
- Subsidieregelingen
- Eindpuntapparaten beheren
- Windows-apparaten beheren
- Aangepaste instellingen voor Windows 10 apparaten
- Updates van Windows 10 apparaten automatiseren
- Versleuteling aan de clientzijde gebruiken

Inhoudsopgave

Geavanceerde functies voor beveiliging en inzichten

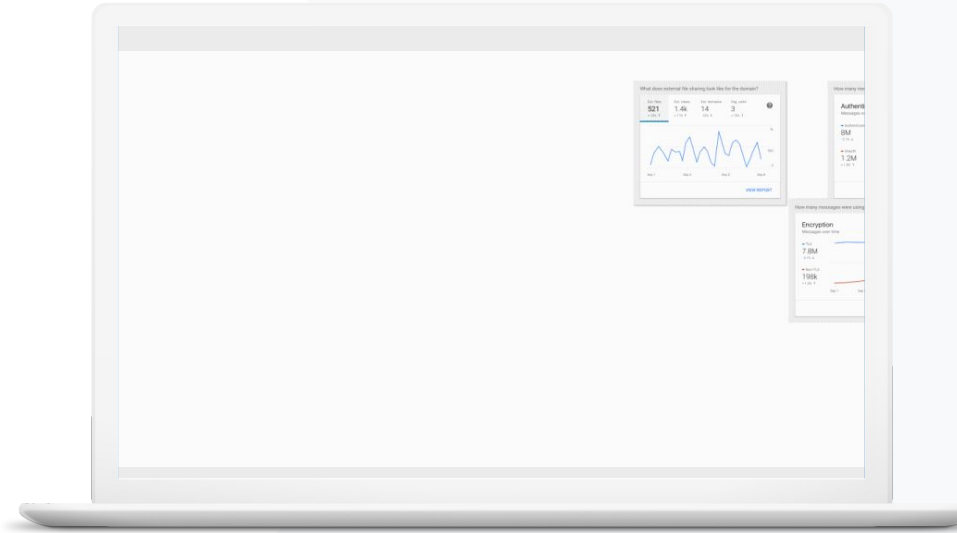
Krijg meer grip op het beheer van je domein met proactieve beveiligingstools waarmee je bedreigingen afhoudt, beveiligingsincidenten analyseert en de gegevens van leerlingen en docenten beschermt.



Beveiligingsdashboard

Wat is het?

In het beveiligingsdashboard zie je een overzicht van de verschillende beveiligingsrapporten. Standaard staan in elk rapportvenster de gegevens van de afgelopen 7 dagen. Je kunt het dashboard aanpassen om gegevens van Vandaag, Gisteren, Deze week, Vorige week, Deze maand, Vorige maand of Dagen geleden (maximaal 180 dagen) te bekijken.



Use cases

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

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

Hoeveelheid spam

Het **beveiligingsdashboard** geeft je een visueel overzicht van de activiteiten van je Google Workspace for Education-omgeving, inclusief:

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

Stapsgewijze instructies

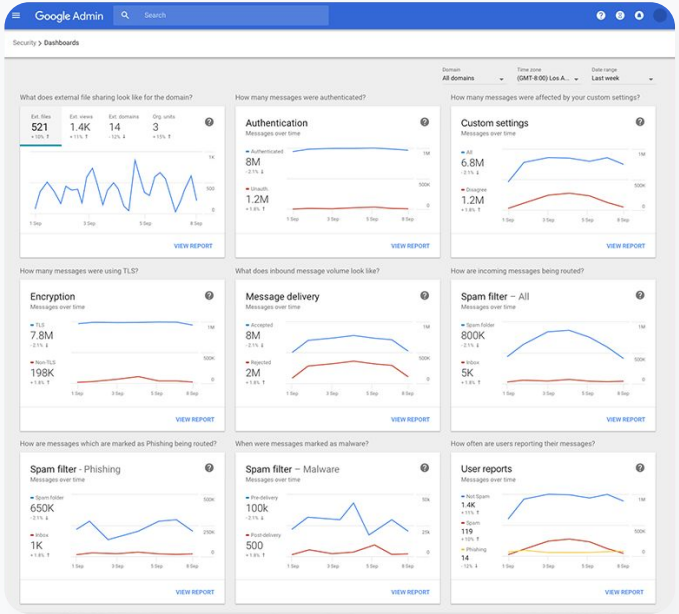
Relevante Helpcentrum-documentatie

- Over het beveiligingsdashboard

Instructies: Dashboardoverzicht

Het beveiligingsdashboard bekijken

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



Relevante Helpcentrum-documentatie

- Over het beveiligingsdashboard

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

Extern bestanden delen

Gebruik het **rapport Bestandsbereik** in het **beveiligingsdashboard** voor statistieken over het extern delen van bestanden 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

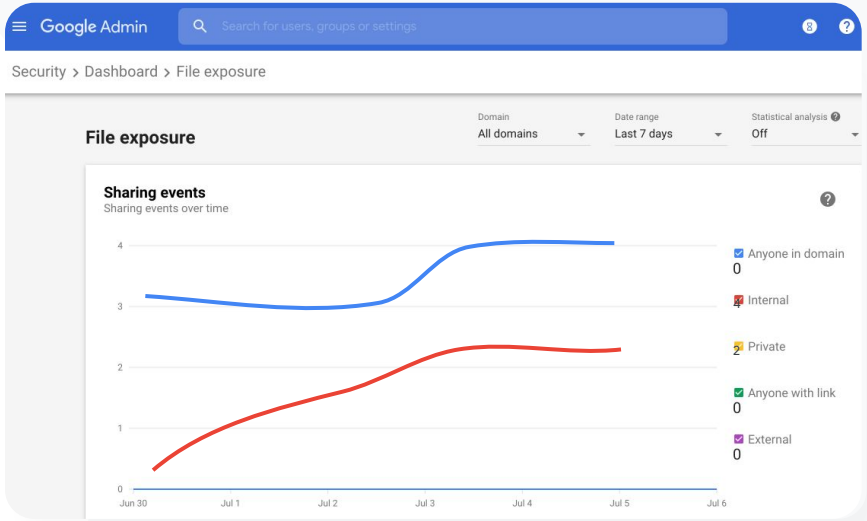
Relevante Helpcentrum-documentatie

- Aan de slag met de pagina Beveiligingsstatus

Instructies: Extern bestanden delen

Het rapport Bestandsbereik bekijken

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



Relevante Helpcentrum-documentatie

- Over het beveiligingsdashboard
- Rapport Bestandsbereik

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

Apps van derden

Gebruik het **rapport Activiteit OAuth-toewijzingen** in het **beveiligingsdashboard** om de apps van derden te monitoren die aan je domein gekoppeld zijn 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 is een goed idee om het aantal apps van derden die toegang hebben te beperken.
- Gebruik het deelvenster 'Activiteit OAuth-toewijzingen' om de toewijzingen per app, bereik of gebruiker te monitoren, en de toewijzingsrechten te updaten.

Stapsgewijze instructies

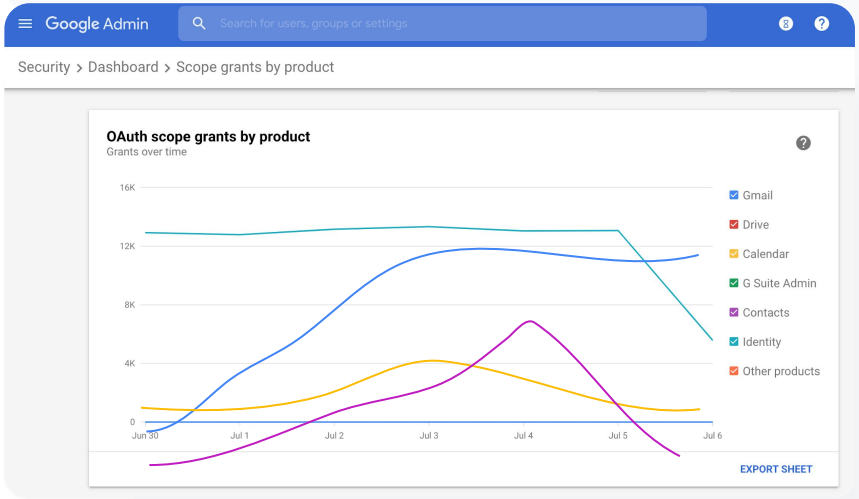
Relevante Helpcentrum-documentatie

- Rapport Activiteit OAuth-toewijzingen

Instructies: Apps van derden

Het rapport 'Activiteit OAuth-toewijzingen' bekijken

- Log in bij de **Beheerdersconsole.**
- Klik op **Beveiliging** > **Dashboard.**
- Klik onderaan op **Rapport bekijken.**
- Je kunt het rapport Activiteit OAuth-toewijzingen bekijken 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

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

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Hoe markeren gebruikers hun e-mails?
- Gebruikersrapporten

Poging tot phishing

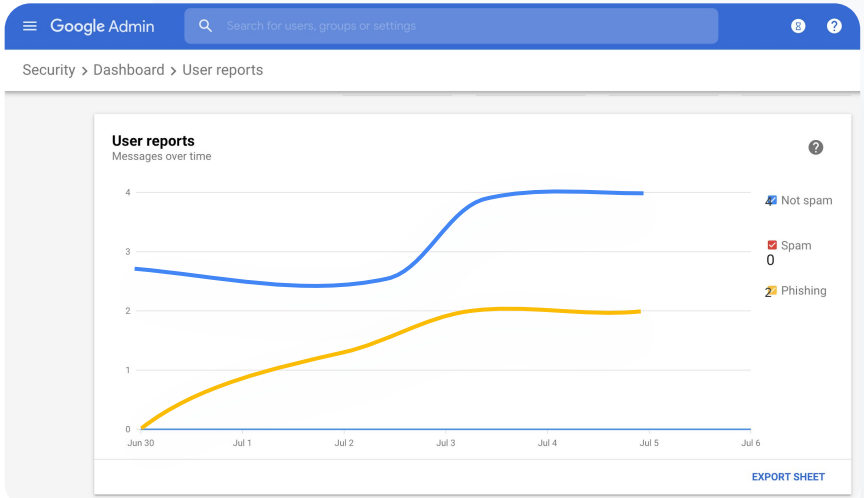
In het **deelvenster Gebruikersrapporten** van het **beveiligingsdashboard** kun je berichten bekijken die in een specifieke periode zijn gemarkeerd als phishing of spam. Je kunt gegevens bekijken over e-mails die als phishing zijn gemarkeerd, zoals wie de ontvangers zijn en hoe vaak berichten werden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

- 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 aanpassen, zodat er alleen gegevens van bepaalde soorten berichten worden getoond, bijvoorbeeld of het bericht intern of extern is gestuurd, in welke periode enzovoort.

Instructies: Poging tot phishing

Het deelvenster Gebruikersrapporten bekijken

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



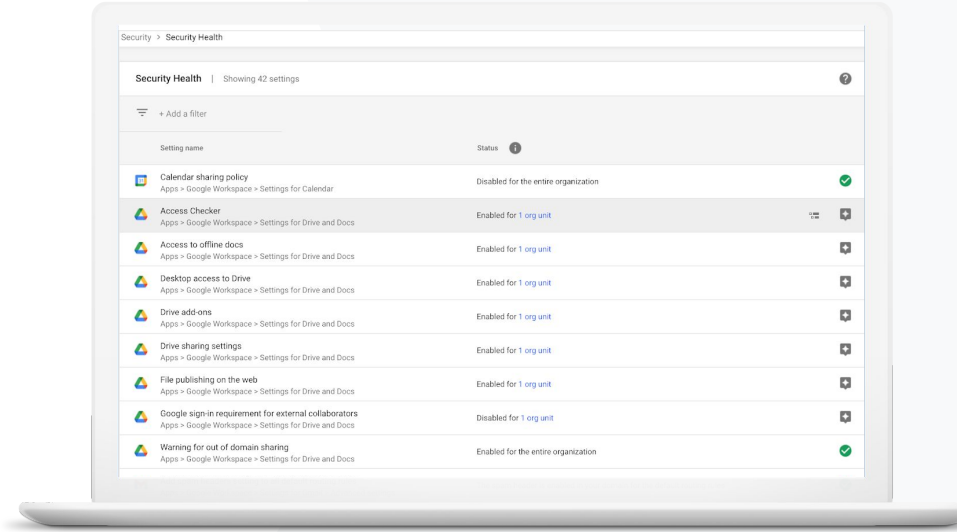
Relevante Helpcentrum-documentatie

- Over het beveiligingsdashboard
- Rapport Bestandsbereik

Beveiligingsstatus

Wat is het?

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

Best practices voor beveiliging	Stapsgewijze instructies
Aanbevelingen voor risicogebieden	Stapsgewijze instructies

Ik wil graag best practices of aanbevelingen over het instellen van een beveiligingsbeleid."

Best practices voor beveiliging

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

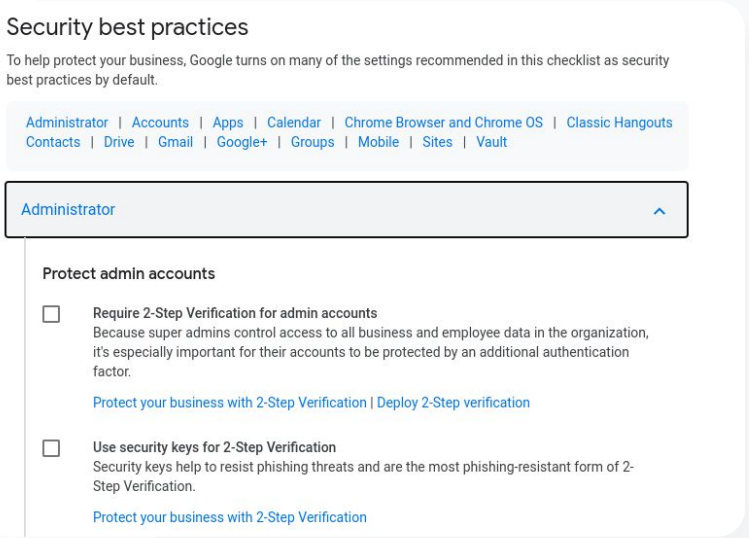
Relevante Helpcentrum-documentatie

- Aan de slag met de pagina Beveiligingsstatus

Instructies: Checklist met best practices voor beveiliging

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:** hacken van accounts voorkomen 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, checken en beveiligen



Relevante Helpcentrum-documentatie

- De status van beveiligingsinstellingen monitoren

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

Aanbevelingen voor risicogebieden

Op de pagina **Beveiligingsstatus** geeft een overzicht van de beveiligingsinstellingen en aanbevolen wijzigingen. 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

Stapsgewijze instructies

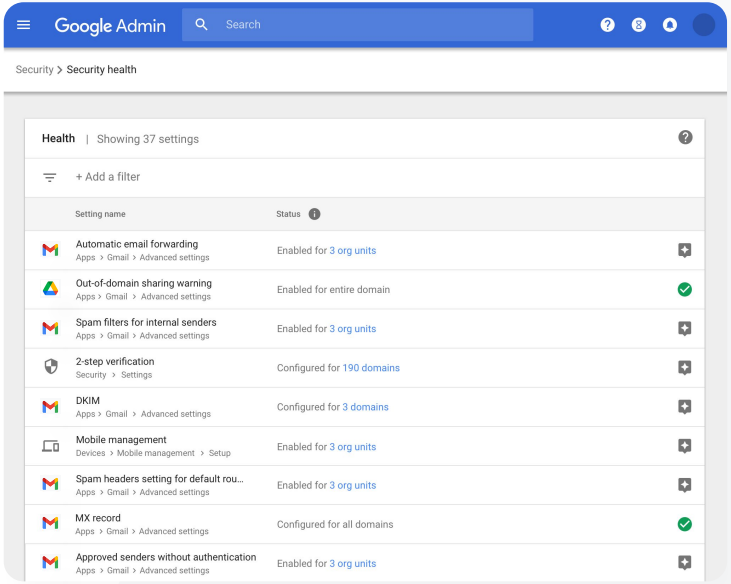
Relevante Helpcentrum-documentatie

- 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 door te nemen. Klik op het icoon om de details en instructies te openen.



Relevante Helpcentrum-documentatie

- Aan de slag met de pagina Beveiligingsstatus

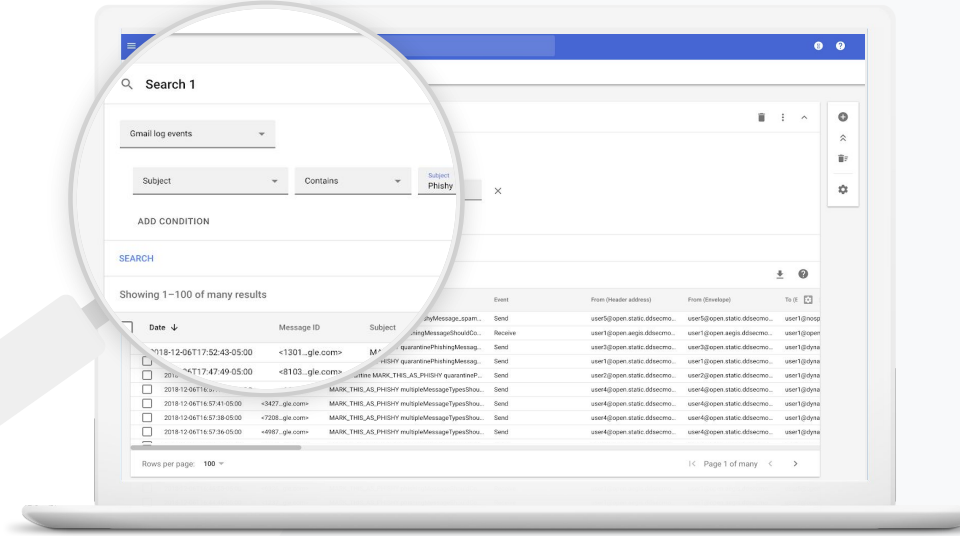
Onderzoekstool

Wat is het?

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

Toepassingen

Ongepast materiaal dat wordt gedeeld	Stapsgewijze instructies
Per ongeluk gedeelde bestanden	Stapsgewijze instructies
E-mailanalyse	Stapsgewijze instructies
Phishing/malwaremails	Stapsgewijze instructies
Kwaadwillende gebruikers tegenhouden	Stapsgewijze instructies
Uitgebreidere beveiligingsinzichten	Stapsgewijze instructies
Vergaderingen zonder toezicht voorkomen	Stapsgewijze instructies



"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 ik wil dit bestand verwijderen."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Voorwaarden voor Drive-logboekgebeurtenissen
- Acties voor Drive-logboekgebeurtenissen

Ongepast materiaal dat wordt gedeeld

Aan de hand van Drive-logboekgebeurtenissen in de **onderzoekstool** kun je ongewenste bestanden in je domein vinden, volgen, isoleren of verwijderen. Je kunt gegevens over Drive-logboekgebeurtenissen hiervoor gebruiken:

- Documenten zoeken op naam, gebruiker, eigenaar, enzovoort
- Actie ondernemen door de bestandsrechten te wijzigen of door het bestand te verwijderen
- Content zoeken die gebruikers maken in Google Workspace of uploaden naar Drive
- Alle logboekinformatie over dat document bekijken
  - Aanmaakdatum
  - Wie de eigenaar van het document is, wie het heeft bekeken en wie het heeft bewerkt
  - Wanneer het is gedeeld

Er is per ongeluk een bestand gedeeld met een groep die daar GEEN toegang toe mag hebben.

Ik wil hun toegang daartoe verwijderen.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Zoeken met de onderzoekstool
- Acties uitvoeren op basis van zoekresultaten

Per ongeluk gedeelde bestanden

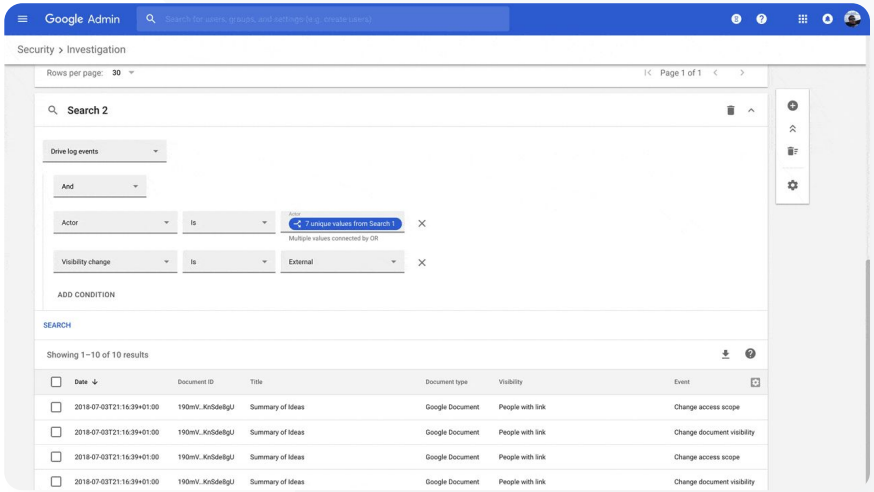
Met Drive-logboekgebeurtenissen in de **onderzoekstool** kun je problemen met het delen van bestanden volgen en oplossen. Je kunt gegevens over Drive-logboekgebeurtenissen hiervoor gebruiken:

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

Instructies: Drive-logboekgebeurtenissen

Drive-logboekgebeurtenissen onderzoeken

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



Actie ondernemen

- Selecteer het bestand 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 controleren, voordat je deze opslaat

Relevante Helpcentrum-documentatie

- Zoeken met de onderzoekstool
- Acties uitvoeren op basis van zoekresultaten

> Iemand heeft een e-mail gestuurd die NIET verzonden had mogen 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 ook weten wat er in de e-mail staat."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Voorwaarden voor Gmail-logboeken en -berichten
- Acties voor Gmail-berichten en Gmail-logboekgebeurtenissen
- Stappen om de content van een e-mail te zien

E-mailanalyse

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

- Specifieke e-mails zoeken op onder meer onderwerp, bericht-ID, bijlage en afzender.
- 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, markeren als spam of phishing, naar inbox sturen en in quarantaine plaatsen.

“

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

Relevante Helpcentrum-documentatie

- Voorwaarden voor Gmail-logboeken en -berichten
- Acties voor Gmail-berichten en Gmail-logboekgebeurtenissen
- Stappen om de content van een e-mail te zien
- VirusTotal-rapporten bekijken

Phishing- en malwaremails

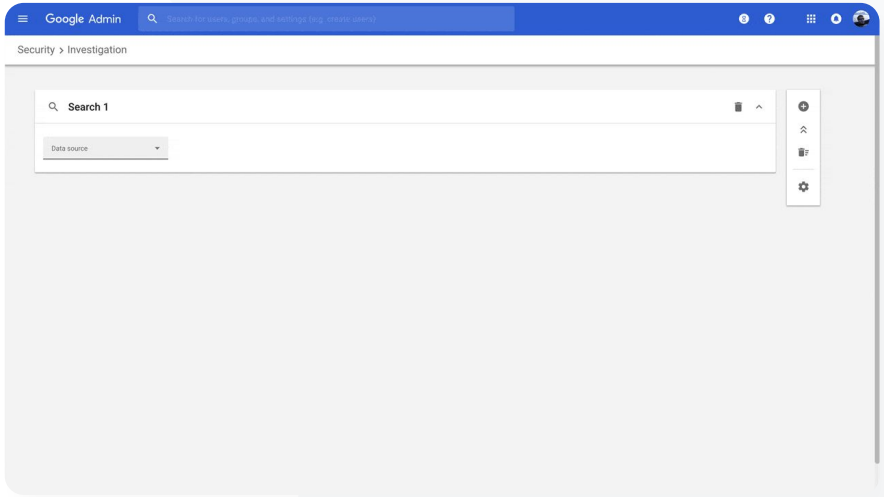
Met de **onderzoekstool**, en dan met name de **Gmail-logboeken**, kun je schadelijke e-mails in je domein vinden en isoleren. Via je Gmail-logboeken kun je:

- Naar e-mailberichten zoeken met specifieke content, inclusief bijlagen
- Informatie bekijken over specifieke e-mails, inclusief wie ze heeft gekregen en geopend
- De berichten en het gesprek bekijken om te bepalen of ze schadelijk zijn
- E-mailbijlagen scannen op de context en reputatie van dreigingen met VirusTotal-rapporten
- Actie ondernemen door berichten te markeren als spam of phishing, naar een speciale inbox te sturen, in quarantaine te plaatsen of te verwijderen

Instructies: Gmail-logboeken

Gmail-logboeken onderzoeken

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



Actie ondernemen

- Selecteer het bestand in de zoekresultaten
- Klik op **Acties**
- Kies **Bericht verwijderen (uit de inbox van de eigenaar)**
- Klik onderaan de pagina op Bekijken om de actie te bevestigen
- In de kolom **Resultaat** kun je de status van de actie bekijken

Relevante Helpcentrum-documentatie

- Voorwaarden voor Gmail-logboeken en -berichten
- Acties voor Gmail-berichten en Gmail-logboekgebeurtenissen
- Stappen om de content van een e-mail te zien

> Iemand die te kwader trouw handelt, heeft het doorlopend op vooraanstaande gebruikers van mijn domein gemunt. Ik word er gek van.
>
> Hoe kan ik dit stoppen?

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Logboekgebeurtenissen over gebruikers zoeken en onderzoeken
- Activiteitsregels maken met de onderzoekstool

Kwaadwillende gebruikers tegenhouden

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

- Pogingen identificeren en onderzoeken om gebruikersaccounts in je organisatie te hacken
- Nagaan welke methoden voor verificatie in 2 stappen gebruikers in je organisatie gebruiken
- Meer informatie krijgen 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

Instructies: Kwaadwillende gebruikers tegenhouden

Logboekgebeurtenissen over gebruikers onderzoeken

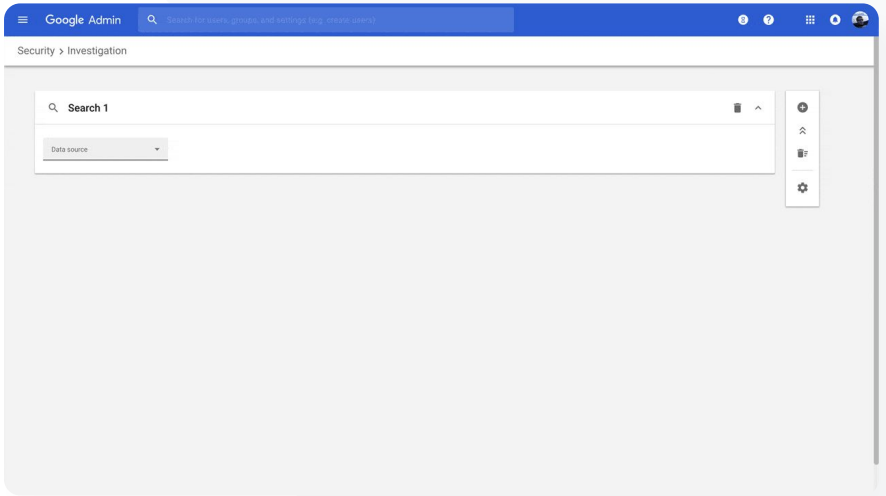
- Log in bij de **Beheerdersconsole**
- Klik op **Beveiliging** > **Onderzoekstool**
- Kies **Logboekgebeurtenissen over gebruikers**
- Klik op **Voorwaarde toevoegen** > **Zoeken**

Gebruikers herstellen of opschorten

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

Gegevens over een specifieke gebruiker bekijken

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



Relevante Helpcentrum-documentatie

- Logboekgebeurtenissen over gebruikers zoeken en onderzoeken

Eén van onze docenten meldt dat een bijlage in Gmail er verdacht uitziet.

Hoe kan onze IT-afdeling vaststellen of het bestand een beveiligingsrisico is?”

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Zoeken met de onderzoekstool
- VirusTotal-rapporten bekijken via de onderzoekstool

Meer inzicht in de beveiliging

De uitgebreide overzichten in VirusTotal-rapporten zijn een goede aanvulling op een beveiligingsonderzoek. In de rapporten staan inzichten die zijn verzameld via crowdsourcing. Beheerders kunnen ze gebruiken om de beveiliging van een domein, bijlage, IP-adres of URL na te gaan.

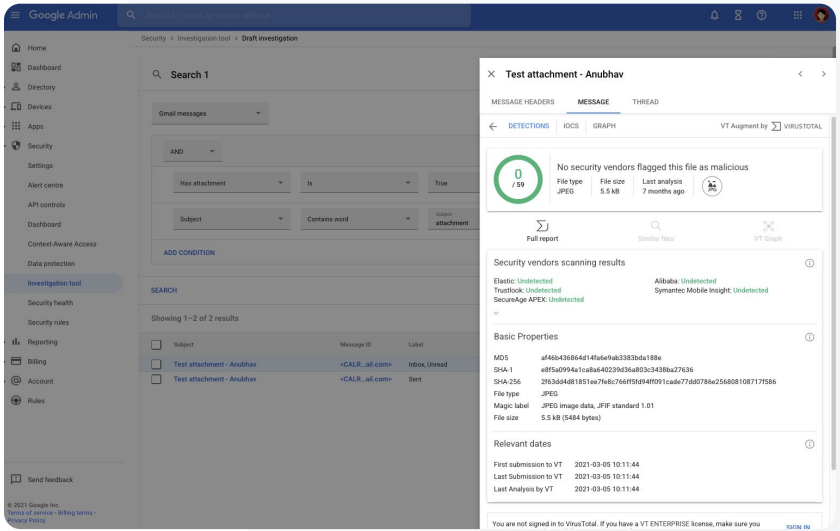
- Meer beveiligingsinzichten krijgen over Gmail en Chrome-logboekgebeurtenissen
- Verdachte bestanden, URL's, domeinen en IP-adressen analyseren
- Toegang krijgen tot via crowdsourcing verzamelde gegevens die aangeven waarom een bijlage of website riskant is
- Hulp krijgen om te beslissen hoe je beveiligingsproblemen aanpakt

Instructies: Meer inzicht in de beveiliging

VirusTotal-rapporten over Gmail bekijken

- Log in bij de **Beheerdersconsole**
- Klik op **Beveiliging** > **Beveiligingscentrum** > **Onderzoekstool**
- Kies **Gmail-berichten**
- Klik op **Voorwaarde toevoegen** > **Bevat bijlage**
- Klik in de zoekresultaten op de **bericht-ID** of de **onderwerplink**
- Klik in het zijvenster op het tabblad **Bericht** of **Thread**
- Selecteer **VirusTotal-rapport bekijken**

Beheerders kunnen ook VirusTotal-rapporten specifiek voor Chrome bekijken. Volg dan de instructies hierboven en selecteer **Chrome-logboekgebeurtenissen** in de onderzoekstool.



Relevante Helpcentrum-documentatie

- VirusTotal-rapporten bekijken via de onderzoekstool

Leerlingen blijven in een Google Meet hangen nadat de les is afgelopen. Ik wil de Meet voor iedereen kunnen beëindigen zodat het leerproces niet wordt onderbroken."

Virtuele vergaderingen zonder toezicht voorkomen

Google Workspace-beheerders kunnen in de onderzoekstool **Vergadering beëindigen voor iedereen** gebruiken om alle gebruikers uit vergaderingen binnen je organisatie te verwijderen. Voor individuele Google Meet-gesprekken kunnen de hosts van de vergadering dat ook doen.

- De vergadering eindigt voor alle deelnemende gebruikers, ook de gebruikers in breakoutruimtes.
- Niemand kan deelnemen aan toekomstige instanties van die vergadering zonder dat de host aanwezig is.

Stapsgewijze instructies

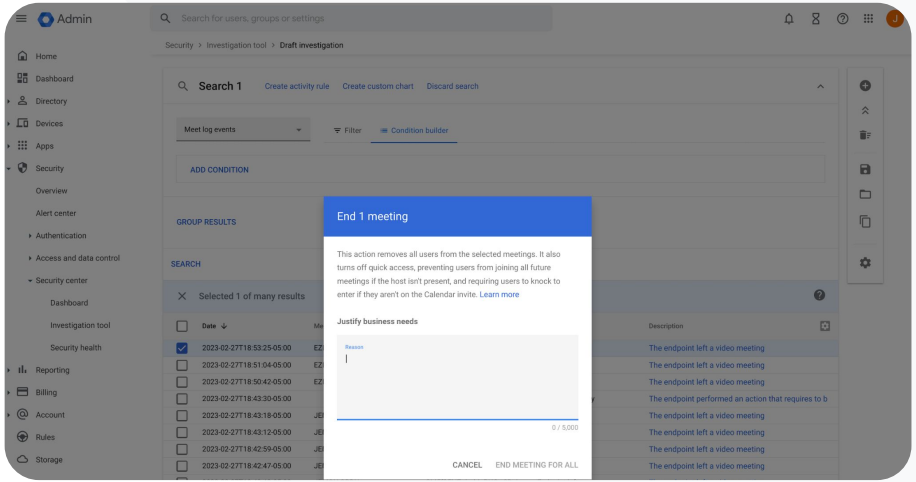
Relevante Helpcentrum-documentatie

- Vergaderingen beëindigen via de onderzoekstool

Instructies: Virtuele vergaderingen zonder toezicht voorkomen

Met de onderzoekstool een vergadering beëindigen voor alle gebruikers

- Log in bij de **Beheerdersconsole**
- Klik op **Beveiliging** > **Beveiligingscentrum** > **Onderzoekstool**
- Kies **Gebeurtenissen in het logboek Meet**
- Klik op **Zoeken**. In de zoekresultaten zie je een lijst met Meet-logboekgebeurtenissen
- Vink de vakjes aan voor de vergaderingen die je wilt beëindigen voor alle gebruikers
- Selecteer **Acties**
- Klik op **Vergadering beëindigen voor iedereen**



Relevante Helpcentrum-documentatie

- Vergaderingen beëindigen via de onderzoekstool

Domeinbeheer

Beheerders kunnen met geavanceerde Google Workspace-tools de gegevens van hun organisatie beheren, instellingen configureren, gebruik monitoren en zorgen dat onderwijsnormen worden gevolgd.

Use cases

Gmail-bijlagen scannen op bedreigingen	Stapsgewijze instructies
Gebruiksdashboards en -rapporten maken	Stapsgewijze instructies
Bestanden makkelijker vinden	Stapsgewijze instructies
Interne documenten ordenen	Stapsgewijze instructies
Afdelingsgroepen automatisch vullen	Stapsgewijze instructies
Doelgroepen maken voor het intern delen van bestanden	Stapsgewijze instructies
Het delen van bestanden beperken	Stapsgewijze instructies
Beperkingen voor de Workspace-app	Stapsgewijze instructies
Opslag beheren	Stapsgewijze instructies
Gegevensregelgeving	Stapsgewijze instructies
Subsidieregelingen	Stapsgewijze instructies
Eindpuntapparaten beheren	Stapsgewijze instructies
Windows-apparaten beheren	Stapsgewijze instructies
Aangepaste instellingen voor Windows-apparaten	Stapsgewijze instructies
Updates van Windows-apparaten automatiseren	Stapsgewijze instructies
Versleuteling aan de clientzijde gebruiken	Stapsgewijze instructies

Gmail-bijlagen scannen op bedreigingen

E-mailbijlagen kunnen schadelijke software bevatten. Gmail kan bijlagen scannen of uitvoeren in sandbox-beveiliging om deze bedreigingen te identificeren. Bijlagen die worden geïdentificeerd als schadelijk worden in de map Spam geplaatst.

- Detecteer malware door deze virtueel ‘uit te voeren’ in een privé, beveiligde sandbox-omgeving en de bijwerkingen te analyseren om kwaadaardig gedrag vast te stellen
- Scan Microsoft Word, PowerPoint, PDF, zip-bestanden, en meer
- Scannen voor het hele domein inschakelen of scanregels maken op basis van specifieke voorwaarden zoals onder meer afzender en domein

“Hoe kan ik mijn domein beter beveiligen tegen zero-day malware en ransomware-bedreigingen?”

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Regels instellen om schadelijke bijlagen te detecteren

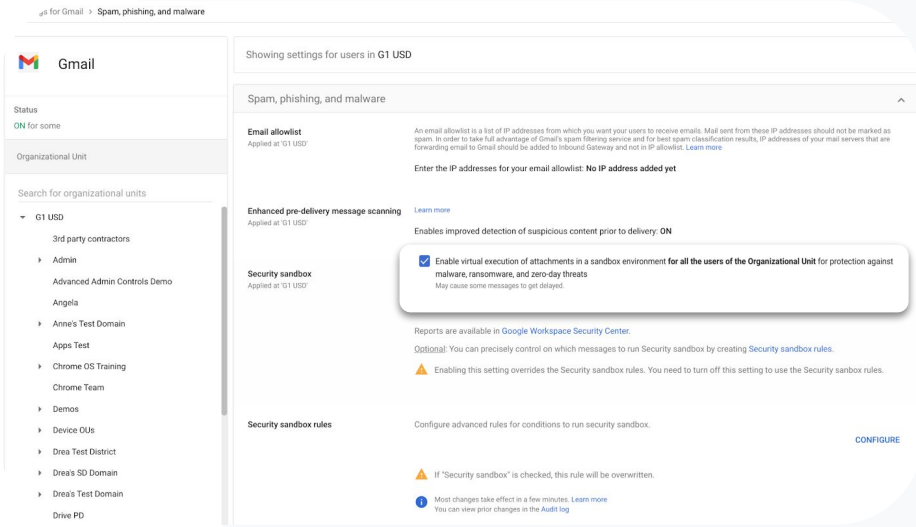
Instructies: Gmail-bijlagen scannen op bedreigingen

Hoe het werkt

E-mailbijlagen worden binnen enkele minuten voordat de e-mail wordt bezorgd in een sandbox gescand, waardoor een extra beveiligingslaag wordt geboden.

Alle bijlagen scannen met sandbox-beveiliging

- Log in bij de **Beheerdersconsole**
- Klik **Menu** > **Apps** > **Google Workspace** > **Gmail** > **Spam, phishing en malware**
- Selecteer een organisatie-eenheid of pas instellingen toe op je domein
- Scroll naar **Sandbox-beveiliging** onder **Spam, phishing en malware**
- Vink het vakje **Virtueel openen van bijlagen in een sandbox-omgeving toestaan** aan
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Regels instellen om schadelijke bijlagen te detecteren

“Hoe krijg ik inzicht in het gebruik van Classroom in mijn domein?”

Gebruiksdashboards en -rapporten maken

Beheerders kunnen **BigQuery Export en de Looker Studio-template** gebruiken voor Classroom-activiteitenlogboeken. Op deze manier kunnen ze aangepaste dashboards en rapportages maken met analysetools als Looker Studio en externe visualisatiepartners die in BigQuery zijn geïntegreerd.

- Exporteer Classroom-logboekgegevens uit de Beheerdersconsole naar BigQuery en Looker Studio.
- Bekijk heel makkelijk gebruiks- en acceptatierapporten voor je hele domein. Zoek bijvoorbeeld uit wie een leerling uit een lesgroep heeft verwijderd of wie een lesgroep op een bepaalde datum heeft gearchiveerd.
- Aanpasbare dashboardtemplates voor Looker Studio maken het makkelijker om inzicht in grote trends te krijgen en actie te ondernemen.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- BigQuery Export en Data Studio-template instellen

Instructies: Gebruiksdashboards en -rapporten maken

01 Een BigQuery-project instellen en exporteren

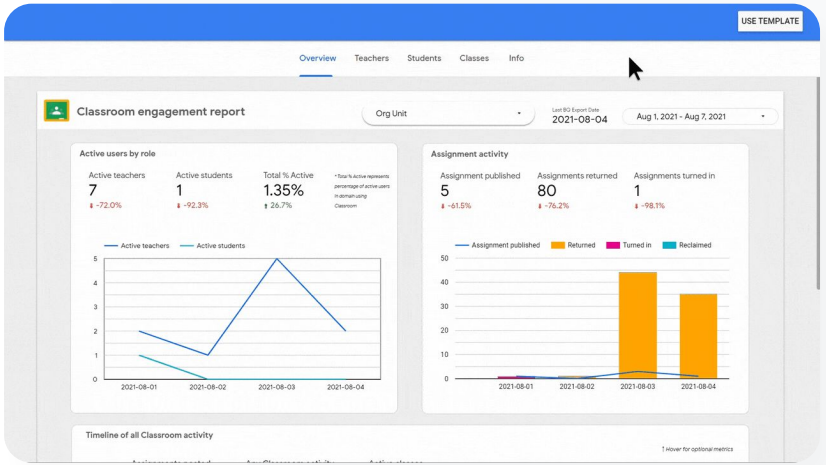
- Log in op console.cloud.google.com > **Nieuw project maken**
- Log in op admin.google.com > **Rapporten** > **BigQuery Export**
- Klik op het **Cloud BigQuery-project** > geef je dataset een naam > **Opslaan**

02 Je BigQuery-export toevoegen aan Looker Studio

- Log in bij Looker Studio > **Maken** > **Gegevensbron**
- Selecteer de **BigQuery-connector** > **Mijn projecten** > klik op het project dat je hebt gemaakt > **Activiteit**
- Vink **Gepartitioneerde tabel** aan > klik op **Verbinden**

03 Een Looker Studio-dashboard maken

- Open de template > selecteer **Template gebruiken**
- Kies bij **Nieuwe gegevensbron** de gegevensbron **Activiteit**
- Klik op **Rapport kopiëren**



Relevante Helpcentrum-documentatie

- BigQuery Export en Data Studio-template instellen

“Ik wil toestemmingsformulieren voor schoolreizen verzamelen die ouders hebben opgestuurd via Gmail, Chat en Documenten.

Hoe vind ik deze bestanden in mijn domein?”

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Gids voor Google Cloud Search
- Cloud Search aan- of uitzetten voor gebruikers

Bestanden makkelijker vinden

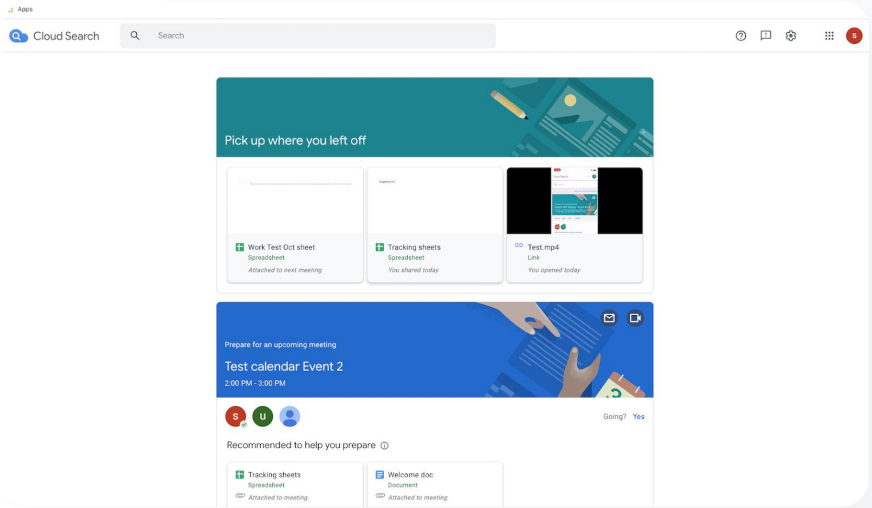
Met Google Cloud Search kunnen docenten in je onderwijsinstelling snel content vinden in Google Workspace en apps van derden.

- Vind overal de juiste informatie, gewoon met je laptop, mobiele telefoon of tablet
- Zoek in Google Workspace-apps, zoals Drive, Contacten en Gmail, en in gegevensbronnen van derden

Instructies: Bestanden makkelijker vinden

Cloud Search aanzetten voor gebruikers

- Log in bij de **Beheerdersconsole** > ga naar **Menu** > **Apps** > **Google**
- Klik op **Servicestatus**
- Als je een service wilt aan- of uitzetten voor iedereen in de organisatie, klik je op **Staat aan voor iedereen** of **Uit voor iedereen**
- Klik op **Opslaan**
- Als je een service wilt aanzetten voor een groep gebruikers binnen een organisatie-eenheid of in verschillende organisatie-eenheden, selecteer je een **toegangsgroep**
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Gids voor Google Cloud Search
- Cloud Search aan- of uitzetten voor gebruikers

“Ik wil de bestanden van mijn onderwijsinstelling gevoeligheidslabels geven om aan de regels te voldoen, misbruik te voorkomen en bestanden geordend te houden.”

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Drive-labels beheren

Documenten ordenen in je domein

Drive-labels zijn voor gebruikers een handige manier om in het domein bestanden te zoeken en te ordenen en om beleid toe te passen. Beheerders maken en beheren Drive-labels om misbruik van bestanden te voorkomen en ervoor te zorgen dat gegevens van leerlingen voldoen aan de vereisten.

- Labels zijn metadata waarmee je gevoelige onderwijsbestanden (zoals individuele leerplannen) en andere documenten kunt ordenen.
- Alleen beheerders kunnen labels maken, structureren en publiceren. Gebruikers in je organisatie kunnen labels toepassen op bestanden die ze bewerken. Ze kunnen ook de veldwaarden aanpassen.
- Drive-labels zijn handig bij het automatisch voorkomen van gegevensverlies.

Instructies: Documenten ordenen in je domein

Hoe het werkt

Google Drive heeft labels met een badge (een visuele indicator) en standaardlabels waarmee je bestanden in je domein kunt ordenen.

Drive-labels aanzetten voor je onderwijsinstelling

- Log in bij de **Beheerdersconsole**
- Klik op **Menu** > **Apps** > **Google Workspace** > **Drive en Documenten**
- Selecteer **Labels**
- Zet labels **aan** of **uit**
- Klik op **Opslaan**

Relevante Helpcentrum-documentatie

- Drive-labels beheren

"Hoe automatiseer ik groepslidmaatschap? Als er een nieuwe docent bijkomt, wil ik dat deze aan de mailinglijst voor docenten wordt toegevoegd."

Afdelingsgroepen automatisch vullen

Met **dynamische groepen** kunnen beheerders groepslidmaatschap voor de hele school updaten met aangepaste criteria.

- Maak dynamische groepen waarvan het lidmaatschap automatisch wordt beheerd
- Houd groepen up-to-date op basis van een lidmaatschapsquery die je instelt
- Gebruik dynamische groepen voor:
  - Mailing- en distributielijsten
  - Gemodereerde groepen en gezamenlijke inboxen
  - Beveiligingsgroepen

Stapsgewijze instructies

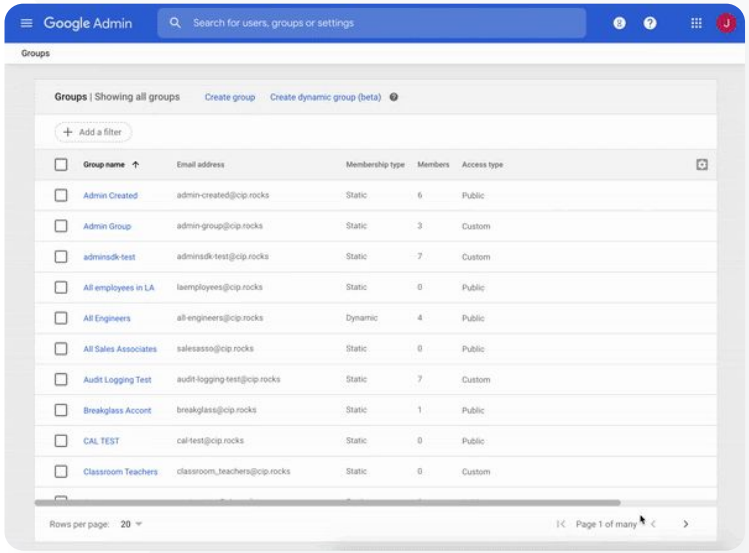
Relevante Helpcentrum-documentatie

- Lidmaatschap automatisch beheren met dynamische groepen

Instructies: Groepen automatisch vullen

Een dynamische groep maken

- Log in bij de **Beheerdersconsole** > ga naar **Menu** > **Directory** > **Groepen**
- Klik op **Dynamische groep maken**
- Stel je lidmaatschapsquery op in:
  - Lijst met voorwaarden: criteria voor lidmaatschap, bijvoorbeeld een bepaalde afdeling
  - Veld Waarde: de waarde die je wilt gebruiken.
- Voer de volgende gegevens in:
  - Naam: de naam waarmee de groep wordt aangeduid in lijsten en berichten.
  - Beschrijving: het doel van de groep.
  - E-mailadres groep: het e-mailadres van de groep.
- Klik op **Opslaan**
- Klik op **Klaar**



Relevante Helpcentrum-documentatie

- Lidmaatschap automatisch beheren met dynamische groepen

Mijn medewerkers delen per ongeluk documenten met de hele organisatie, waardoor gevoelige gegevens blootgesteld worden. Hoe zorg ik dat ze deze alleen delen met de kleine groep voor wie ze bestemd zijn?"

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Over doelgroepen
- Best practices voor de implementatie van doelgroepen
- Een doelgroep maken

Doelgroepen maken voor het intern delen van bestanden

Een doelgroep instellen is veiliger voor de gegevens van je organisatie, omdat de kans minder groot wordt dat gebruikers per ongeluk bestanden delen met te veel mensen.

- Bestanden worden gedeeld met de juiste mensen, zoals een gekozen team of afdeling
- Doelgroepen zijn groepen mensen die beheerders aan gebruikers kunnen aanraden om items mee te delen
- Beheerders kunnen doelgroep toevoegen aan instellingen voor delen, zodat gebruikers worden aangespoord alleen te delen met een specifieke doelgroep
- Beschikbaar in Google Drive, Documenten en Chat

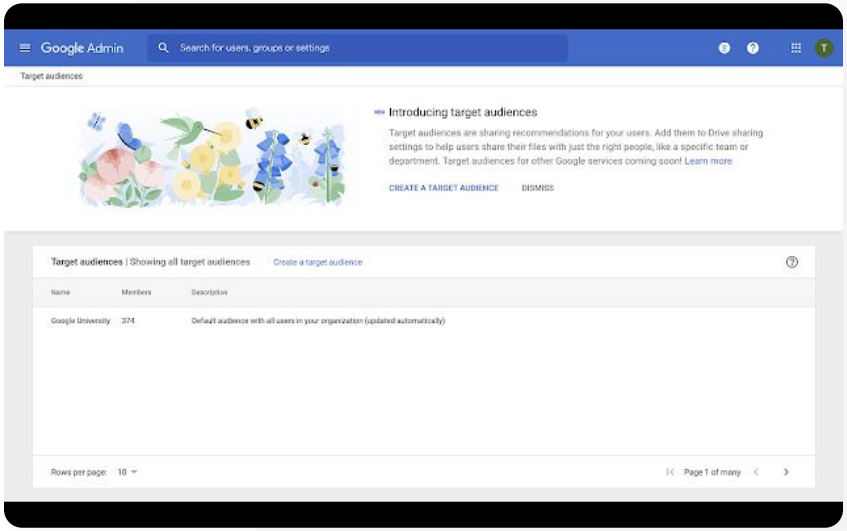
Instructies: Doelgroepen maken voor het intern delen van bestanden

Hoe het werkt

Nadat je een doelgroep hebt gemaakt, kun je leden toevoegen. Ook kun je de doelgroep toepassen op Google Drive, zodat deze beschikbaar is in de instellingen voor delen van gebruikers. Je kunt bijvoorbeeld instellen dat een medewerker een doelgroep 'Alle medewerkers' ziet als deze Drive-bestanden wil delen.

Drive-labels aanzetten voor je onderwijsinstelling

- Log in bij de **Beheerdersconsole** > ga naar **Menu** > **Directory** > **Doelgroepen**
- Klik op **Doelgroep maken**
- Vul bij **Naam** een naam voor de doelgroep in
- Selecteer **Leden toevoegen** > voeg de gewenste leden toe
- Klik op **Klaar**



Relevante Helpcentrum-documentatie

- Over doelgroepen
- Best practices voor de implementatie van doelgroepen
- Een doelgroep maken

Hoe voorkom ik dat leerlingen uit een hogere klas documenten delen met leerlingen uit een lagere klas?"

Het delen van bestanden beperken

Via **Drive-vertrouwensregels** kunnen beheerders regels instellen om te bepalen wie toegang kan krijgen tot Google Drive-bestanden. Dit komt de privacy binnen de onderwijsinstelling ten goede. Je kunt beleid toepassen op individuele gebruikers, groepen, organisatie-eenheden en domeinen.

- Beveilig gevoelige informatie en voldoe aan de normen en regels van de branche
- Beperk delen binnen en/of buiten het domein. Beheerders kunnen een vertrouwensregel instellen waarmee leerlingen Drive-bestanden alleen binnen je organisatie kunnen delen
- Vertrouwensregels vervangen bestaande opties voor delen in de beheerdersinstellingen van Google Drive

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Vertrouwensregels maken en beheren voor delen in Drive

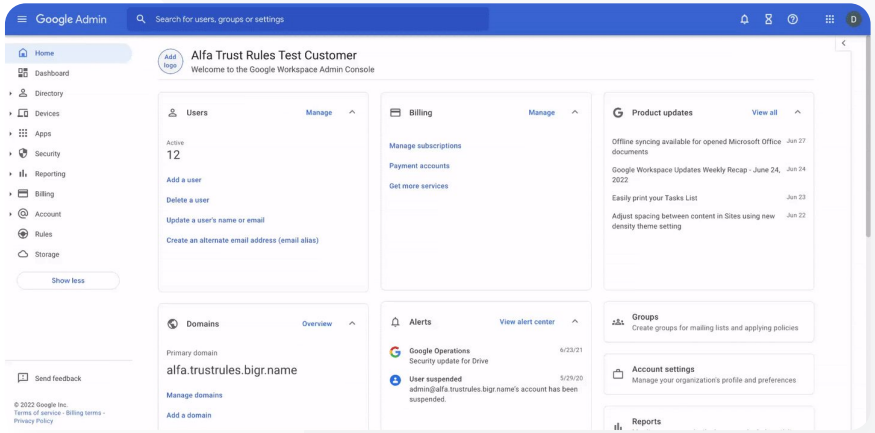
Instructies: Het delen van bestanden beperken

Drive-vertrouwensregels aanzetten

- Log in bij de **Beheerdersconsole** > ga naar **Menu** > **Regels**
- Klik in de kaart **Veilig samenwerken** bovenaan op de pagina op **Vertrouwensregels aanzetten**
- De takenlijst wordt automatisch geopend en toont de voortgang van het activeren van vertrouwensregels

Beheerders kunnen een vertrouwensregel maken, bewerken en verwijderen. Ook kunnen ze logboekgebeurtenissen van de vertrouwensregel bekijken.

In het Helpcentrum voor beheerders vind je stapsgewijze instructies voor het beheer van vertrouwensregels.



Relevante Helpcentrum-documentatie

- Vertrouwensregels maken en beheren voor delen in Drive

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

Beperkingen stellen aan Google Workspace-apps

Met **contextbewuste toegang** kun je gedetailleerd beleid voor toegangscontrole maken voor **Google Workspace- en SAML-apps** (Security Assertion Markup Language) van derden. Dit kun je doen op basis van kenmerken als gebruikersidentiteit, locatie, apparaatbeveiligingsstatus en IP-adres. Je kunt zelfs de toegang tot apps buiten je netwerk beperken.

- Je kunt beleid voor contextbewuste toegang toepassen op de kernservices van Google Workspace for Education
- Je kunt bijvoorbeeld de toegang tot Workspace-apps beperken op apparaten die door de onderwijsinstelling zijn verstrekt. Een ander voorbeeld is dat Drive alleen toegankelijk is als het opslagapparaat van de gebruiker versleuteld is.

Stapsgewijze instructies

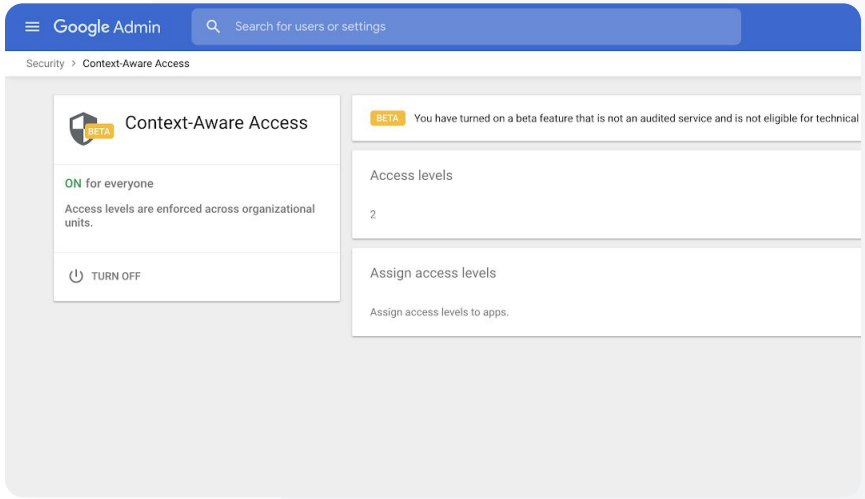
Relevante Helpcentrum-documentatie

- Overzicht van contextbewuste toegang
- Niveaus voor contextbewuste toegang toewijzen aan apps

Instructies: Gebruik van Google Workspace-apps beperken

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 één 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

"Ik wil een nieuw abonnement voor opslagbeheer implementeren in mijn domein."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Opslaggids voor beheerders
- Over de beschikbaarheid en het gebruik van opslag
- Opslag vrijmaken of meer opslag kopen
- Opslaglimieten instellen

Opslag beheren in je domein

Met Google Workspace for Education hebben onderwijsinstellingen standaard 100 TB gecombineerde opslag. Dat komt overeen met ongeveer 100 miljoen documenten, 8 miljoen presentaties of 400.000 uur aan video. **Beheer de gecombineerde Drive-opslag** om deze zo effectief mogelijk te gebruiken in je onderwijsinstelling.

Gebruik beheerderstools, rapporten en logboeken hiervoor:

- Inzicht krijgen in hoeveel opslag je gebruikt
- Opslaglimieten instellen
- Vaststellen welke accounts onevenredig veel opslag gebruiken

De Teaching and Learning Upgrade en Education Plus bieden extra opslagcapaciteit bovenop de standaard opslagruimte:

- 100 GB extra in de gecombineerde opslag per licentie voor de Teaching and Learning Upgrade
- 20 GB extra in de gecombineerde opslag per licentie voor Education Plus

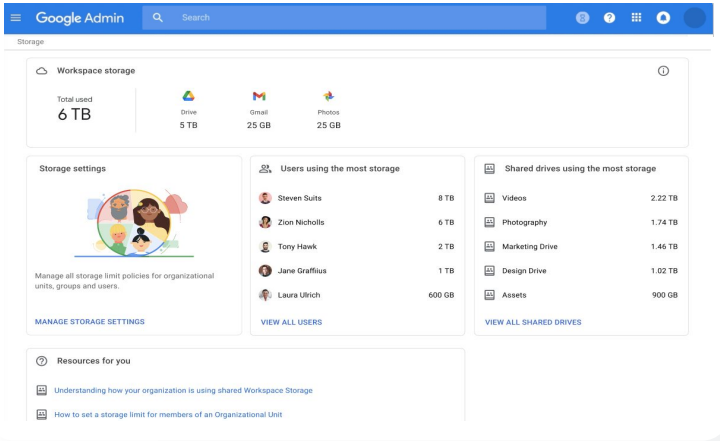
Instructies: Opslag beheren in je domein

Gebruik van opslag vaststellen per gebruiker

- Log in bij de **Beheerdersconsole** > ga naar **Menu** > **Opslag**
- Bekijk het gebruik van opslag per organisatie en gebruiker

Opslaglimieten instellen

- Ga naar de **Beheerdersconsole** > **Menu** > **Opslag**
- Ga naar **Instellingen voor opslag** en klik op **Beheren**
- Klik op **Opslaglimiet voor gebruikers** > selecteer waaraan je een limiet wilt stellen:
  - Organisatie-eenheid: klik op de **organisatie-eenheid**
  - Groep: klik op **Groepen** > klik op het **zoekveld** > vul de **naam van de groep** in > klik op de **groep**
- Selecteer **Aan** en **stel de hoeveelheid opslag in**
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Opslaggids voor beheerders
- Over de beschikbaarheid en het gebruik van opslag
- Opslag vrijmaken of meer opslag kopen
- Opslaglimieten instellen

Gegevensregelgeving

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

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

- Met Education Plus en Education Standard kun je een bepaalde gegevensregio kiezen voor bepaalde gebruikers. Ook kun je voor verschillende afdelingen verschillende gegevensregio's kiezen en bekijken welke verplaatsingen er binnen gegevensregio's zijn.
- 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.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Een geografische locatie kiezen voor je gegevens

"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 for Education-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

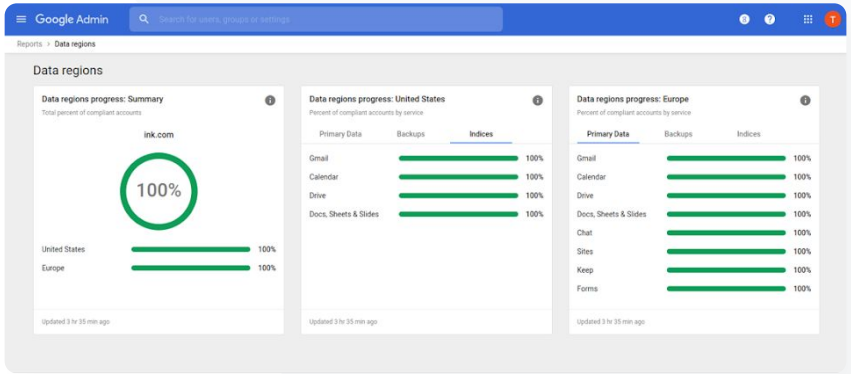
Relevante Helpcentrum-documentatie

- Een geografische locatie kiezen voor je gegevens

Instructies: Gegevensregelgeving

Gegevensregio's bepalen

- Log in bij de **Beheerdersconsole**
  - Opmerking: Je moet ingelogd zijn als hoofdbeheerder
- Klik op **Bedrijfsprofiel** > **Meer tonen** > **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

Eindpuntapparaten beheren

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

- In de Beheerdersconsole kun je apparaten goedkeuren, blokkeren, deblokkeren of verwijderen.
- 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 bereik en niet alleen op Chromebooks, vooral als een apparaat is gehackt."

Stapsgewijze instructies

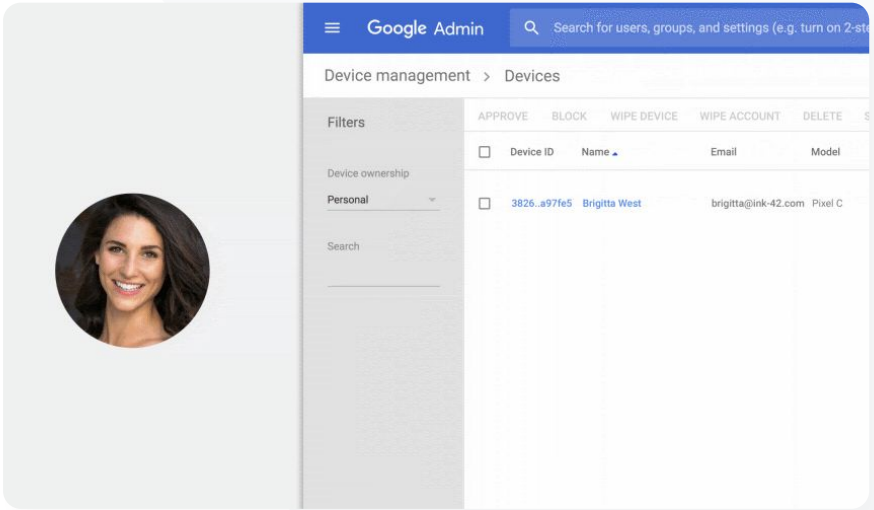
Relevante Helpcentrum-documentatie

- Apparaten beheren met Google-eindpuntbeheer
- Geavanceerd mobiel beheer instellen

Instructies: Eindpuntapparaten beheren

Geavanceerd mobiel beheer gebruiken

- Log in bij de **Beheerdersconsole**
- Ga in de **Beheerdersconsole** naar **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 instellingen voor iedereen gelden. Selecteer anders een onderliggende organisatie-eenheid
- Selecteer **Geavanceerd**
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Apparaten beheren met Google-eindpuntbeheer
- Geavanceerd mobiel beheer instellen

Sommige docenten gebruiken een apparaat met Windows 10. Hoe kan ik op één plek alle apparaten van mijn onderwijsinstelling beheren?"

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Windows-apparaatbeheer aanzetten
- Een apparaat inschrijven voor Windows-apparaatbeheer

Microsoft Windows-apparaten beheren

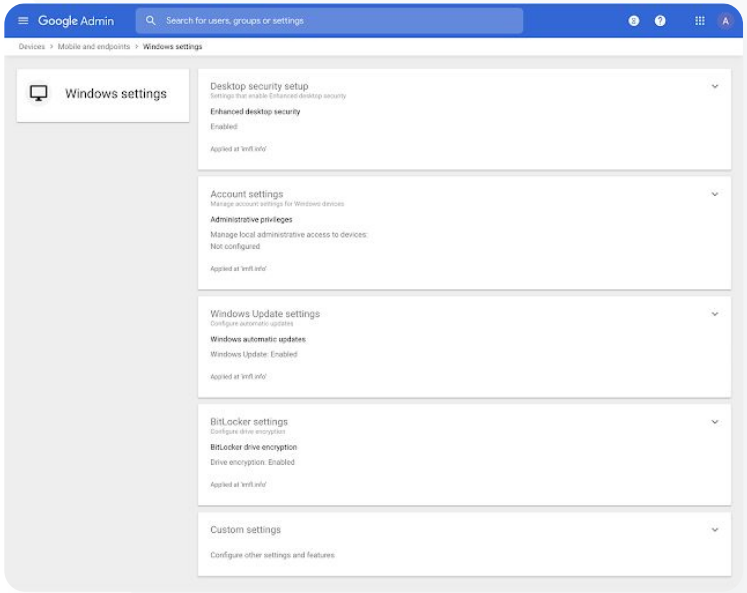
Apparaten met Windows 10 kun je net als Android-, iOS-, Chrome- en Jamboard-apparaten beheren en beveiligen via de Beheerdersconsole.

- Stel single sign-on in, zodat gebruikers makkelijker toegang hebben tot Google Workspace op hun Windows 10-apparaten
- Beheer apparaten waarop je Google Workspace gebruikt in de Beheerdersconsole, zodat ze worden geüpdatet en beveiligd en voldoen aan de regels
- Via de cloud kun je onder andere een apparaat met Windows 10 wissen of updates voor apparaatconfiguratie afdwingen

Instructies: Microsoft Windows-apparaten beheren

Windows-apparaatbeheer aanzetten

- Ga in de **Beheerdersconsole** naar **Menu** > **Apparaten** > **Mobiel en eindpunten** > **Instellingen** > **Windows-instellingen**
- Selecteer **Instellen van Windows-beheer**
- Laat de organisatie-eenheid op het hoogste niveau staan als je wilt dat de instelling voor iedereen geldt
- Selecteer **Aangezet** naast **Windows-apparaatbeheer**
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Windows-apparaatbeheer aanzetten
- Een apparaat inschrijven voor Windows-apparaatbeheer

Hoe stel je wifi-profielen in op Windows 10-apparaten?"

Aangepaste instellingen voor Windows 10-apparaten

Met Windows-apparaatbeheer van Google kunnen beheerders aangepaste instellingen toevoegen aan hun apparaten.

- Beheer aangepaste apparaatinstellingen vanuit de Beheerdersconsole
- Pas instellingen toe op:
  - Apparaatbeheer
  - Beveiliging
  - Hardware en netwerk
  - Software
  - Privacy

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

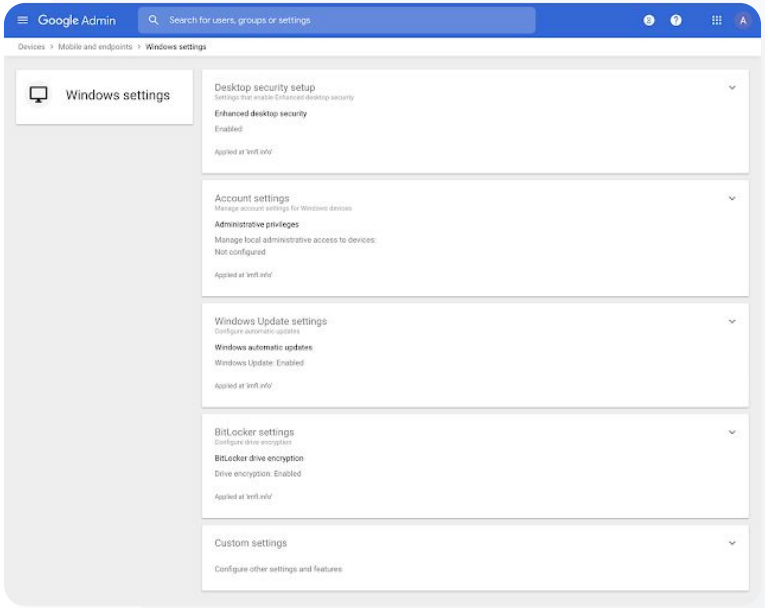
- Veelgebruikte aangepaste instellingen
- Aangepaste instellingen toevoegen

Instructies: Aangepaste instellingen voor Windows 10-apparaten

Een nieuwe aangepaste instelling toevoegen

- Ga in de **Beheerdersconsole** naar **Menu** > **Apparaten** > **Mobiel en eindpunten** > **Instellingen** > **Windows-instellingen**
- Selecteer **Aangepaste instellingen**
- Klik op **Een aangepaste instelling toevoegen** en vul de gevraagde velden in
- Klik op **Volgende**
- Kies de **organisatie-eenheid** waarop je de instelling wilt toepassen
- Klik op **Toepassen**

Houd er rekening mee dat Google geen technische support biedt voor producten en instellingen van derden en dat Google daar geen verantwoordelijkheid voor neemt.



Relevante Helpcentrum-documentatie

- Veelgebruikte aangepaste instellingen
- Aangepaste instellingen toevoegen

Ik wil ervoor zorgen dat onze Windows 10-apparaten altijd de nieuwste updates krijgen."

Updates automatiseren op Windows 10-apparaten

Je kunt instellen hoe en wanneer Windows 10-apparaten beveiligingsupdates en andere belangrijke downloads via de Windows-service voor automatische updates krijgen.

- Bij de instellingen van Windows Update kun je onder andere meldingen instellen om updates te downloaden en tijden inplannen waarop apparaten niet opnieuw opstarten voor een update
- Pas instellingen toe op de hele onderwijsinstelling of op specifieke organisatie-eenheden
- Wijzigingen verwerken kan tot 24 uur duren, maar meestal gaat het sneller

Stapsgewijze instructies

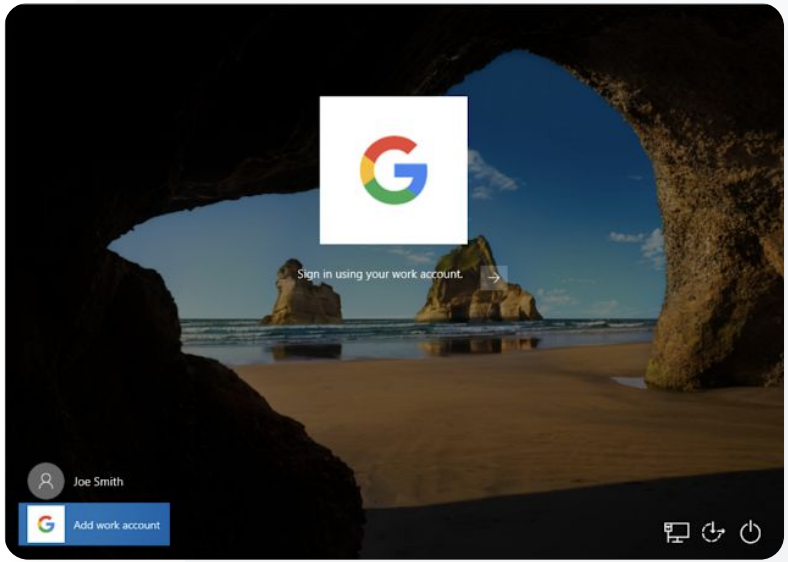
Relevante Helpcentrum-documentatie

- Automatische updates beheren

Instructies: Updates automatiseren op Windows 10-apparaten

Updates configureren

- Ga in de **Beheerdersconsole** naar **Menu** > **Apparaten** > **Mobiel en eindpunten** > **Instellingen** > **Windows-instellingen**
- Selecteer **Instellingen voor Windows Update** > **Aangezet**
- Selecteer **Aangezet** naast **Windows-apparaatbeheer**
- Stel onder andere deze opties in:
  - Updates voor Microsoft-apps accepteren
  - Gedrag van automatische updates
  - Frequentie van automatische updates
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Automatische updates beheren

> Ik weet dat Google de strengste normen voor gegevensversleuteling heeft, maar ik wil de encryptiesleutels van het intellectueel eigendom en onderzoek van onze universiteit zelf beheren."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Over versleuteling aan de clientzijde

Versleuteling aan de clientzijde gebruiken

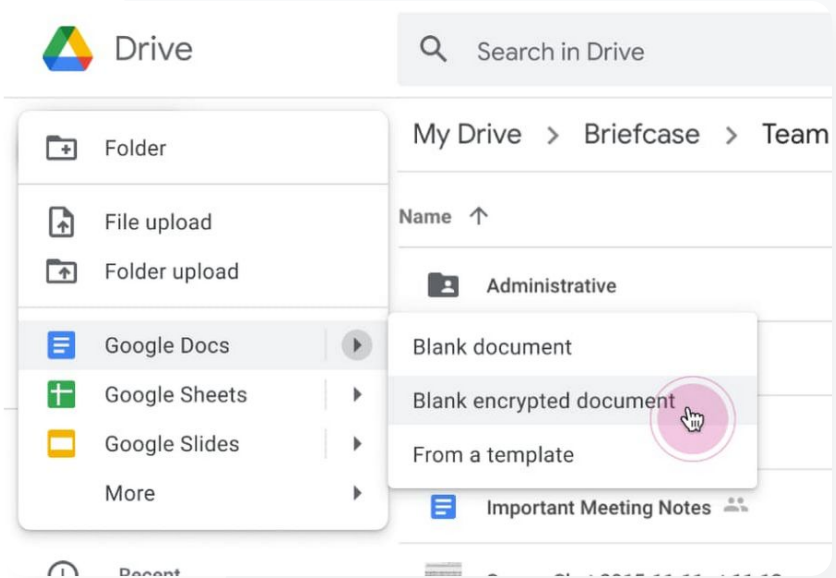
Google Workspace maakt al gebruik van de nieuwste cryptografische standaarden om alle 'data at rest' en 'data in transit' tussen faciliteiten te versleutelen. Met **versleuteling aan de clientzijde** hebben beheerders rechtstreeks controle over encryptiesleutels en welke identiteitsprovider er wordt gebruikt om toegang te krijgen tot die sleutels.

- Gebruik je eigen sleutels voor het coderen van gevoelige gegevens, zoals het intellectueel eigendom van je onderwijsinstelling
- Content wordt in de browser versleuteld, voordat gegevens worden verstuurd of opgeslagen in cloudopslag van Google
- Kies welke gebruikers content met versleuteling aan de clientzijde kunnen maken en deze intern of extern kunnen delen

Instructies: Versleuteling aan de clientzijde gebruiken

Versleuteling aan de clientzijde (VCZ) instellen

- Stel de service voor versleutelingssleutels in
  - Bescherm gegevens via sleutelbeheer en andere beheerfuncties door een sleutelservice te maken
- Koppel Google Workspace aan je externe sleutelservice
  - Voeg sleutelservices toe en beheer deze voor versleuteling aan de clientzijde door de sleutelservice-URL op te nemen in de Beheerdersconsole
- Wijs de sleutelservice toe aan organisatie-eenheden of groepen
  - Wijs één sleutelservice toe als de standaardservice voor de hele onderwijsinstelling
- Koppel Google Workspace aan je IdP
  - Maak een koppeling met je identiteitsprovider (IdP) voor versleuteling aan de clientzijde om de identiteit van gebruikers te verifiëren voordat je ze toestemming geeft content te versleutelen of versleutelde content te openen
- Zet VCZ aan voor gebruikers
  - Zet versleuteling aan de clientzijde aan voor organisatie-eenheden of groepen die content met versleuteling aan de clientzijde moeten kunnen maken

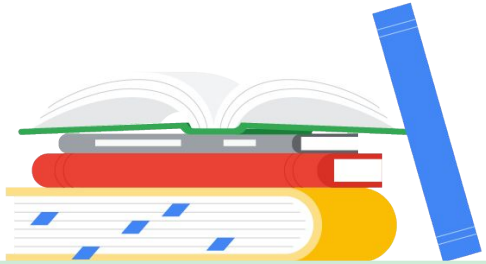


Relevante Helpcentrum-documentatie

- Over versleuteling aan de clientzijde

Functies voor lesgeven en leren

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

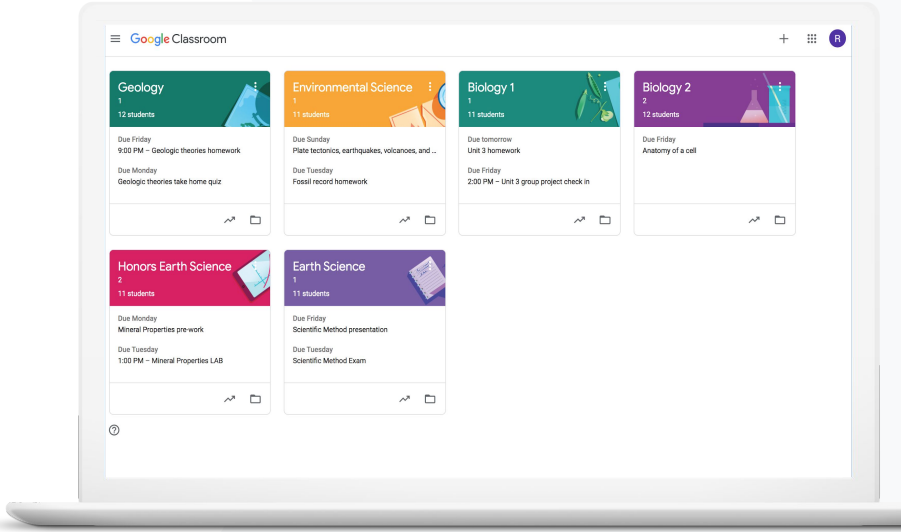


- Google Classroom
- Originaliteitsrapporten
- Documenten, Spreadsheets en Presentaties
- Google Meet

Google Classroom

Wat is het?

Google Classroom is een centrale plek voor lesgeven en leren. Met de betaalde functies van Classroom worden handige tools voor lesgroepen bij elkaar gebracht. Docenten kunnen hun favoriete tools kiezen in Classroom en lesgroeplijsten synchroniseren met externe systemen.



Toepassingen

Toegang tot Classroom-add-ons beheren	Stapsgewijze instructies
Aantrekkelijke content integreren in Classroom	Stapsgewijze instructies
Lesgroepen op schaal maken	Stapsgewijze instructies

“

Ik zou graag toegang via single sign-on willen instellen voor de favoriete edtech-tools van de docenten. "

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Google Workspace Marketplace-apps beheren
- Add-ons gebruiken in Classroom
- Marketplace-apps op de toelatingslijst beheren
- Een Marketplace-app distribueren naar gebruikers
- Add-ons voor Classroom [Handleiding Aan de slag voor beheerders]

Toegang tot Classroom-add-ons beheren

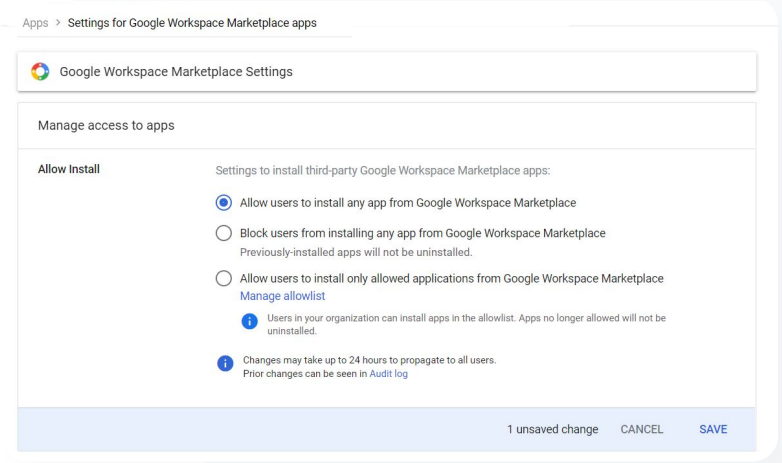
Bepaal met een **toelatingslijst voor je domein** tot welke onderwijs-apps van derden je onderwijsinstelling toegang kan hebben. Geef docenten de mogelijkheid om met een paar klikken add-ons te installeren en in opdrachten voor leerlingen op te nemen.

- Maak een toelatingslijst voor je domein om te bepalen welke apps van derden docenten mogen installeren vanuit de Google Workspace Marketplace.
- Gebruik aanvullende onderwijs-apps voor betere leerresultaten. Docenten kunnen binnen Google Classroom opdrachten toewijzen, nakijken en een cijfer geven.
- In de Google Workspace Marketplace vind je onder meer Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Arts & Culture, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora en Wordwall.

Instructies: Toegang tot Classroom-add-ons beheren

Toegang tot add-ons beheren met een toelatingslijst voor je domein

- Selecteer in de Beheerdersconsole **Menu** > **Google Workspace Marketplace-apps** > **Lijst met apps**
- Selecteer **App op toelatingslijst zetten**
- Vul de naam van de gewenste add-on in of zoek ernaar
- Klik op **Selecteren** en zorg dat **Gebruikers toestaan deze app te installeren** is geselecteerd
- Klik op **Doorgaan** en dan op **Voltooien**



Add-ons toegang verlenen tot een toelatingslijst

- Selecteer in de Beheerdersconsole **Menu** > **Google Workspace Marketplace-apps** > **Lijst met apps**
- Selecteer de add-on die je wilt distribueren
- Klik onder **Gebruikerstoegang** op **Organisatie-eenheden en groepen bekijken**
- Kies **Beschikbaar voor iedereen** of beperk de toegang door specifieke **groepen** of **organisatie-eenheden** te selecteren
- Klik op **Opslaan**

Relevante Helpcentrum-documentatie

- Google Workspace Marketplace-apps beheren
- Add-ons gebruiken in Classroom
- Marketplace-apps op de toelatingslijst beheren
- Een Marketplace-app distribueren naar gebruikers
- Add-ons voor Classroom [Handleiding Aan de slag voor beheerders]

> Ik wil met Kahoot! mijn leerlingen een educatieve game laten doen en deze nakijken zonder Google Classroom te verlaten."

Aantrekkelijke content integreren in Classroom

Via **Classroom-add-ons** kunnen docenten interactieve activiteiten en aantrekkelijke content delen met de lesgroep. Ze kunnen binnen Classroom add-ons toevoegen aan opdrachten, vragen, lesmateriaal of mededelingen.

- Bied docenten en leerlingen de mogelijkheid om hun favoriete tools te gebruiken, zoals Kahoot!, Nearpod en Pear Deck. Dit alles gewoon in Classroom
- Met add-ons hoeven leerlingen niet meerdere wachtwoorden te beheren of externe websites te gebruiken
- Gebruik add-ons om het werk van leerlingen na te kijken en cijfers te geven, rechtstreeks in Classroom

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Add-ons gebruiken in Classroom
- Add-ons voor Classroom [Handleiding Aan de slag voor docenten]

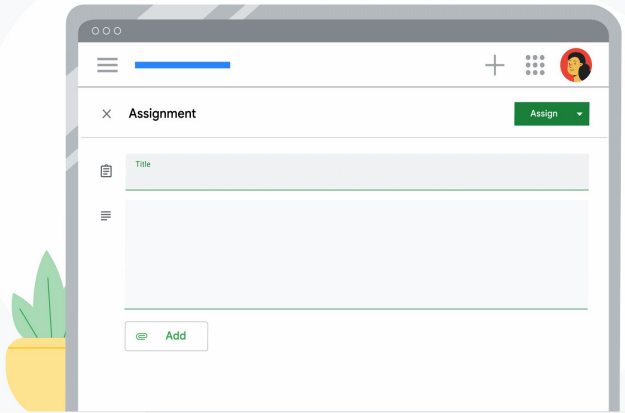
Instructies: Aantrekkelijke content integreren in Classroom

Add-ons toevoegen aan een opdracht, toets of vraag

- Log in op je Classroom-account via **classroom.google.com**
- Selecteer de relevante lesgroep uit de lijst en kies **Schoolwerk**
- Selecteer **Maken** en kies wat je wilt maken
- Vul een titel en instructies in
- Kies bij **Add-ons** de add-on die je wilt gebruiken
- Selecteer **Toewijzen**

Add-ons toevoegen aan een mededeling

- Ga naar de pagina **Updates** van de lesgroep en selecteer **Doe een mededeling aan je lesgroep**
- Voer de mededeling in
- Kies bij **Add-ons** de add-on die je wilt gebruiken
- Selecteer **Posten**



Relevante Helpcentrum-documentatie

- Add-ons gebruiken in Classroom
- Add-ons voor Classroom [Handleiding Aan de slag voor docenten]

Ik wil het samenstellen van lesgroepen en het beheer van klassenlijsten automatiseren in Google Classroom."

Lesgroepen op schaal maken

Door klassenlijsten uit het LIS te importeren kun je via Clever automatisch lesgroepen maken en deze gesynchroniseerd houden met het leerlinginformatiesysteem (LIS) van je school.

- Beschikbaar bij Education Plus voor het basis- en middelbaar onderwijs in de VS en Canada
- Beheerders kunnen klassenlijst uit je LIS importeren in Google Classroom om automatisch lesgroepen samen te stellen
- Automatiseer en beheer naadloos lesgroeplijsten in Google Classroom

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Aan de slag met het importeren van klassenlijsten naar het LIS
- Klassenlijsten importeren uit het LIS instellen via Clever

Instructies: Lesgroepen op schaal maken

Het importeren van klassenlijsten uit je LIS instellen

- Synchronisatie van klassenlijsten in Google Classroom met Clever instellen
- De schoolleider in Clever en de hoofdbeheerder in Google Workspace kunnen de stapsgewijze instructies van Clever volgen

Als je schooldistrict geen Clever-account heeft:

- Maak een Clever-account

Als je schooldistrict wel een Clever-account heeft:

- Vraag een klassenlijstimport aan in je Clever-dashboard

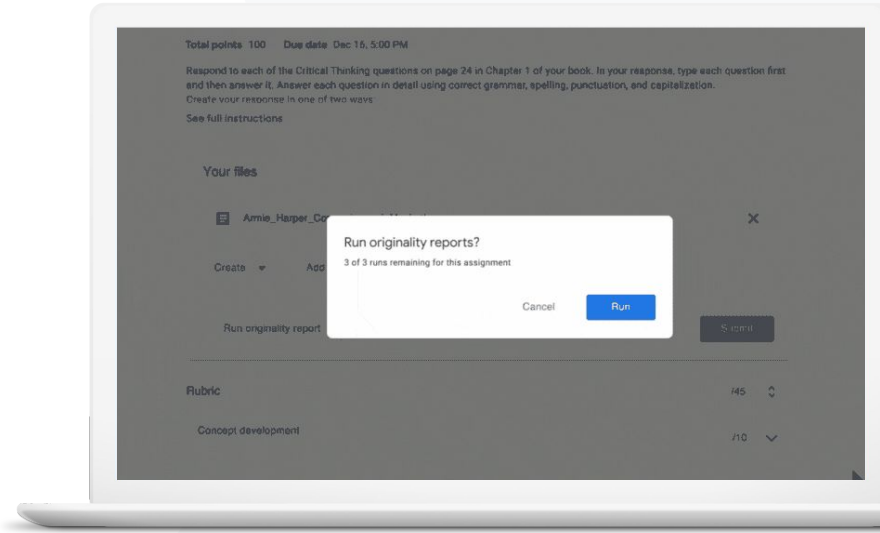
Relevante Helpcentrum-documentatie

- Klassenlijsten importeren uit het LIS instellen via Clever

Originaliteitsrapporten

Wat is het?

Met originaliteitsrapporten kunnen docenten en leerlingen nagaan of werk authentiek is. Via Google Zoeken wordt het werk van een leerling vergeleken met miljarden webpagina's en meer dan 40 miljoen boeken. Bij de betaalde versie heb je onbeperkt toegang tot originaliteitsrapporten en kunnen docenten het werk van leerlingen vergelijken met eerder werk dat de school heeft opgeslagen.



Toepassingen

Scannen op plagiaat	Stapsgewijze instructies
Originaliteit vergelijken met eerder werk van leerlingen	Stapsgewijze instructies
Plagiaatcontroles als leermoment	Stapsgewijze instructies

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

Scannen op plagiaat

Docenten kunnen de authenticiteit van het werk van leerlingen checken met **originaliteitsrapporten**. Het rapport bevat links naar gevonden bronnen en markeert niet-geciteerde tekst.

- Maak originaliteitsrapporten voor documenten in Documenten, Presentaties en Microsoft Word.

- Docenten hebben deze voordelen met de Teaching and Learning Upgrade of Education Plus:
  - Onbeperkte toegang tot originaliteitsrapporten
  - Overeenkomsten zoeken tussen het werk van leerlingen en eerder ingeleverd werk dat de school heeft opgeslagen

Gegevens blijven bezit van de school. Wij zorgen ervoor dat ze privé en beveiligd zijn.

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Originaliteitsrapporten aanzetten
- Originaliteitsrapporten en privacy

Instructies: Scannen op plagiaat

Originaliteitsrapporten aanzetten voor opdrachten in Classroom

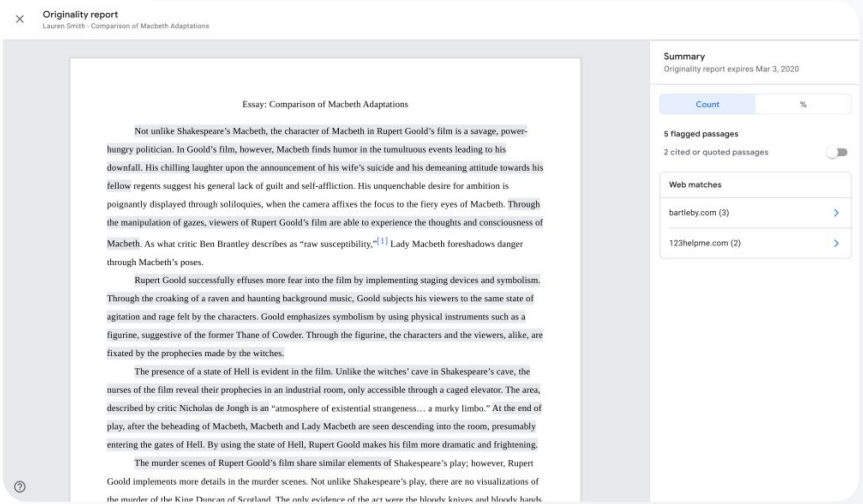
- Log in op je Classroom-account via **classroom.google.com**
- Selecteer de relevante lesgroep uit de lijst en kies **Schoolwerk**
- Selecteer **Maken** > **Opdracht**
- Vink het vakje naast **Originaliteitsrapporten** aan om de functie aan te zetten

Een originaliteitsrapport maken voor werk van leerlingen

- Selecteer het relevante 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**

Originaliteitsrapporten aanzetten voor opdrachten in je LBS

- Log in bij je **leerbeheersysteem**
- Selecteer het relevante **vak**
- Maak een opdracht en selecteer **Google Opdrachten**
- Vink het vakje aan voor **Originaliteitsrapporten aanzetten**



Relevante Helpcentrum-documentatie

- Classroom: Originaliteitsrapporten aanzetten
- Google Opdrachten: Originaliteitsrapporten aanzetten

Hoe zorg ik ervoor dat docenten het werk van een leerling kunnen scannen op plagiaat van werk van leerlingen uit de afgelopen jaren?"

Originaliteit vergelijken met eerder werk van leerlingen

Met **Schoolovereenkomsten** voor originaliteitsrapporten kunnen docenten het werk van leerlingen vergelijken met eerder ingeleverd werk van leerlingen door in het privéarchief van je onderwijsinstelling daarop te scannen.

- Met de Teaching and Learning Upgrade of met Education Plus kun je het werk van leerlingen vergelijken met ander werk dat nu of al eerder is ingeleverd, zodat je plagiaat kunt opsporen.
- Het werk van leerlingen kun je beveiligd opslaan en aanvullen in een privéarchief voor het hele domein van de school.

Stapsgewijze instructies

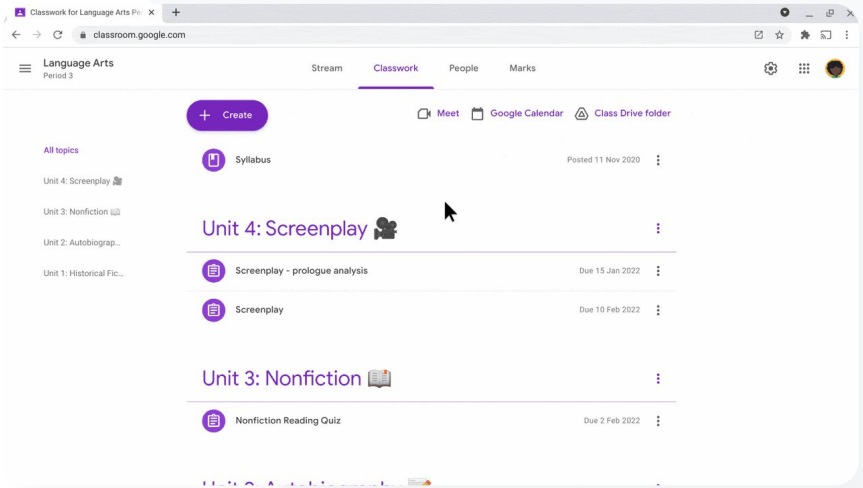
Relevante Helpcentrum-documentatie

- Originaliteitsrapporten aanzetten
- Schoolovereenkomsten aanzetten voor originaliteitsrapporten in Classroom

Instructies: Originaliteit vergelijken met eerder werk van leerlingen

Schoolovereenkomsten aanzetten voor originaliteitsrapporten

- Selecteer in de Beheerdersconsole **Menu** > **Apps** > **Aanvullende Google-services** > **Classroom**
- Selecteer de **organisatie-eenheid van de docent**
- Klik op **Originaliteitsrapporten** en vink **Schoolovereenkomsten voor originaliteitsrapporten aanzetten** aan
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Schoolovereenkomsten aanzetten voor originaliteitsrapporten in Classroom

"Ik wil mijn leerlingen leren hoe ze bronnen op de juiste manier citeren."

Plagiaatcontroles als leermoment

Leerlingen kunnen content zonder citaat en onbedoeld plagiaat opsporen, voordat ze hun werk inleveren door een **originaliteitsrapport** uit te voeren. Dit kunnen ze 3 keer per opdracht doen. In originaliteitsrapporten wordt het werk van leerlingen vergeleken met verschillende bronnen. Tekst zonder citaat wordt gemarkeerd, zodat ze hiervan 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 zo vaak gebruiken 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

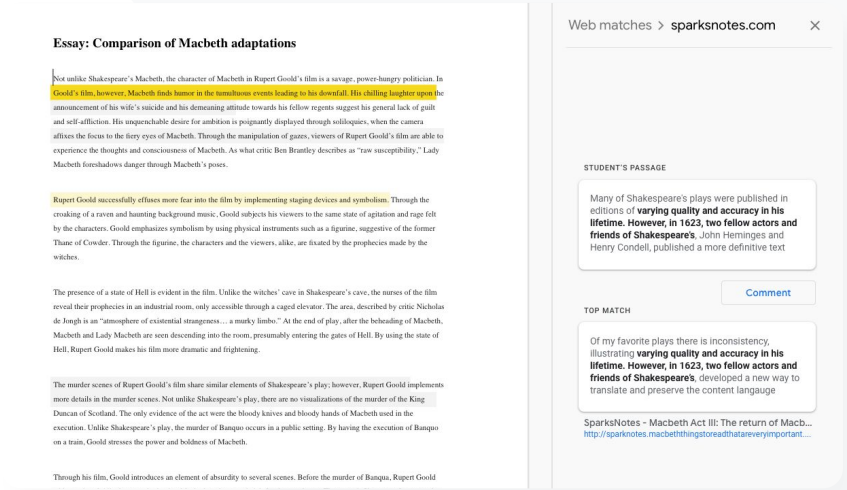
- Een originaliteitsrapport laten maken voor je werk

Instructies: Plagiaatbescherming als leermoment

Hoe leerlingen originaliteitsrapporten kunnen maken in Classroom

- 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 **maak een bestand**
- 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

Leerlingen kunnen met Google Opdrachten originaliteitsrapporten maken binnen het LBS.



Relevante Helpcentrum-documentatie

- Een originaliteitsrapport maken in Classroom
- Een originaliteitsrapport in je LBS

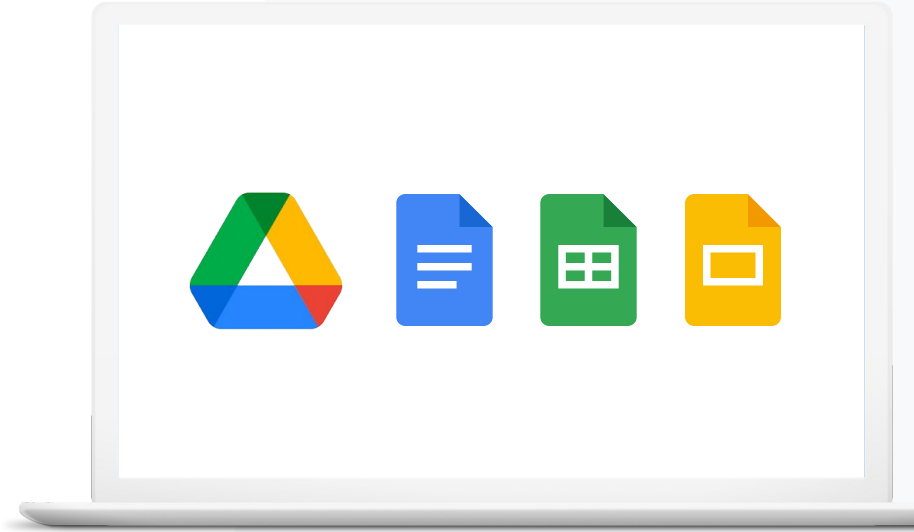
Documenten, Spreadsheets en Presentaties

Wat is het?

Met Documenten, Spreadsheets en Presentaties kunnen scholen tegelijk en in realtime samenwerken, samen iets nieuws maken, werk beoordelen en bewerken. Met de betaalde functies van Education Plus kunnen docenten en beheerders een goedkeuringsproces voor interne documentatie invoeren in je onderwijsinstelling.

Use cases

Interne documenten goedkeuren — Stapsgewijze instructies



Onze afdeling natuurwetenschappen ontwikkelt een nieuw lesprogramma.

Hoe zorgen ze ervoor dat het voorgestelde lesprogramma door alle afdelingshoofden wordt goedgekeurd?"

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Goedkeuringen beheren

Interne documenten goedkeuren

Met **goedkeuringen** kan je school documenten in Google Drive naar een formeel goedkeuringsproces sturen.

- Goedkeurders kunnen deze documenten goedkeuren, afwijzen of er feedback op geven, allemaal rechtstreeks vanuit Drive, Documenten en andere Google Workspace-apps
- Goedkeurders volgen een link naar het document en kunnen het daarna beoordelen, er reacties in plaatsen en het uiteindelijk afwijzen of goedkeuren
- Je kunt onder andere goedkeuringen beheren voor een contract- of een nieuwe werknemer, of wijzigingen in een document goedkeuren, voordat het wordt gepubliceerd

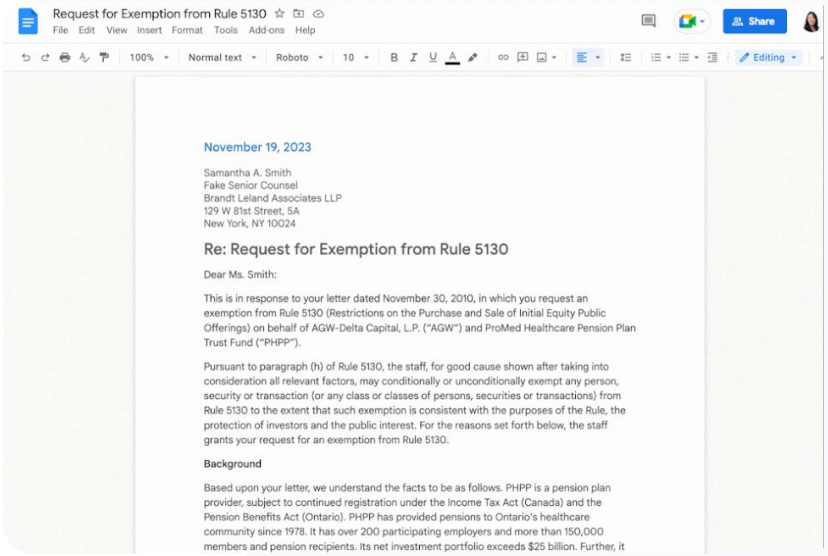
Instructies: Interne documenten goedkeuren

Hoe het werkt

Beheerders kunnen bepalen welke rol gebruikers en bestanden spelen in het goedkeuringsproces.

Goedkeuringen beheren

- Log in bij de **Beheerdersconsole** > ga naar **Menu** > **Apps** > **Google Workspace** > **Drive en Documenten**
- Klik op **Goedkeuringen**
- Selecteer een onderliggende **organisatie-eenheid** of een **configuratiegroep** als je wilt dat de instelling voor iedereen geldt
- Klik op **Opslaan**



Relevante Helpcentrum-documentatie

- Goedkeuringen beheren

Google Meet

Wat is het?

De geavanceerde functies van Google Meet zijn onder andere livestreamen, breakoutruimtes, grotere vergaderingen, opnamen van vergaderingen en live vertaalde ondertiteling.

Toepassingen

Vergaderingen opnemen — Stapsgewijze instructies	Vragen stellen — Stapsgewijze instructies
Verwijzen naar wat in de les is besproken — Stapsgewijze instructies	Input verzamelen — Stapsgewijze instructies
Taalbarrières wegnemen — Stapsgewijze instructies	Kleine leerlinggroepen — Stapsgewijze instructies
Bijeenkomsten en evenementen op school uitzenden — Stapsgewijze instructies	Deelname bijhouden — Stapsgewijze instructies

“

Onze onderwijsinstelling biedt grote online lessen voor professionele ontwikkeling aan die we moeten opnemen voor docenten die niet aanwezig kunnen zijn."

Vergaderingen opnemen

Met de Teaching and Learning Upgrade en Education Plus kunnen docenten opnamen maken van bijvoorbeeld lessen, stafvergaderingen en trainingen voor professionele ontwikkeling. Opnamen worden automatisch opgeslagen in Drive.

- Opnamen worden opgeslagen in de Drive van de organisator van de vergadering. Zorg voorafgaand aan de opname voor genoeg ruimte in je Drive.
- We raden IT-beheerders aan om opnamen alleen aan te zetten voor docenten en andere medewerkers.

Stapsgewijze instructies

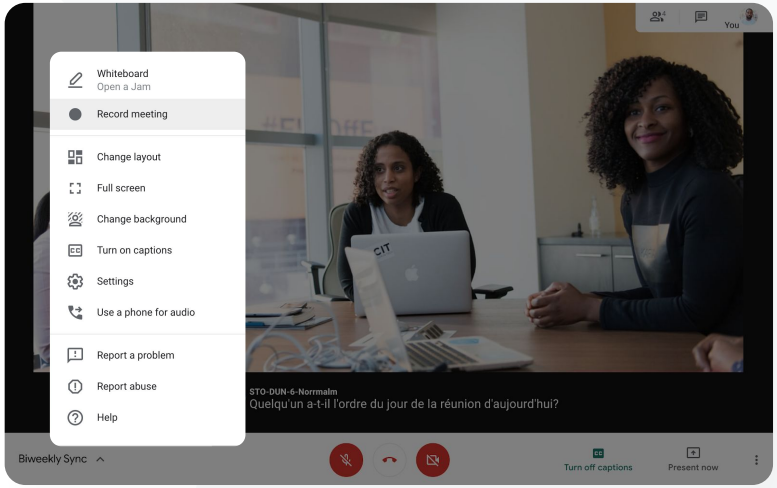
Relevante Helpcentrum-documentatie

- Een videovergadering opnemen

Instructies: Vergaderingen opnemen

Een opname starten

- Start of neem deel aan een vergadering in **Google Meet**
- Klik op **Activiteiten** > **Opnemen**
- Selecteer **Opname starten**
- Klik op **Starten** in het venster dat verschijnt
- Er verschijnt rechtsonder een rode stip 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

- Een videovergadering opnemen

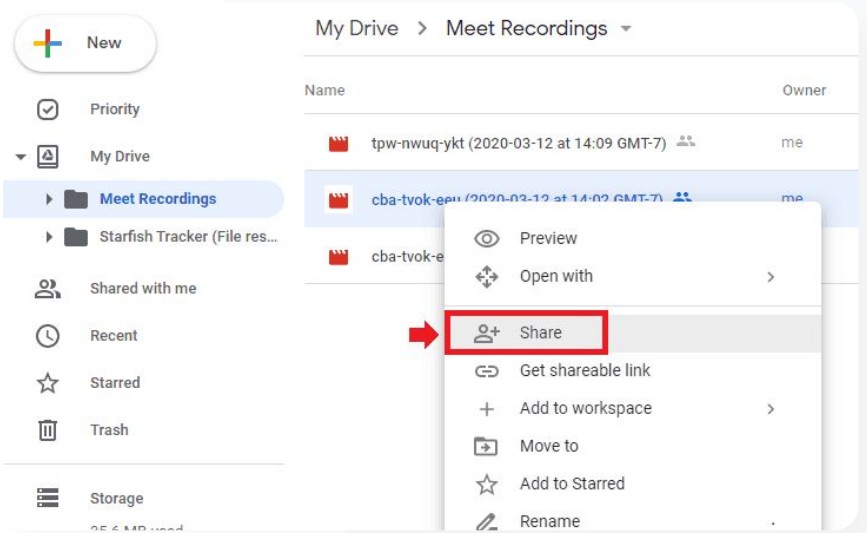
Instructies: Opnamen bekijken en delen

Een opname delen

- Selecteer het bestand
- Klik op het icoon **Delen**
- **Voeg kijkers toe** die zijn goedgekeurd

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 downloadbare bestand om het af te spelen

De opname afspelen vanuit Drive

- Dubbelklik in Drive op de opname om deze af te spelen. 'Wordt nog verwerkt' wordt getoond totdat 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

"Hoe kan ik een transcript van een virtuele les maken, zodat leerlingen deze later kunnen bestuderen?"

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Transcript maken met Google Meet
- Transcriptie aan- of uitzetten

Verwijzen naar wat in de les is besproken

Docenten kunnen hun les en wat in de les wordt gezegd automatisch vastleggen, zodat leerlingen de hoofdconcepten makkelijker kunnen terugvinden. In transcripten staat wie de vergadering heeft bijgewoond en wie wat heeft gezegd.

- Beschikbaar in het Engels voor Google Meet-gebruikers met een computer of laptop.
- Beheerders kunnen transcriptie aanzetten voor hun school.
- Transcripten worden automatisch opgeslagen in de Drive van de host van de vergadering.
- Als transcriptie is aangezet, verschijnt er voor iedereen in de vergadering linksboven een transcripticoon.
- Transcripten geven weer wat er in een vergadering is gezegd. Als je een transcript wilt van chatberichten, moet je je vergadering opnemen.

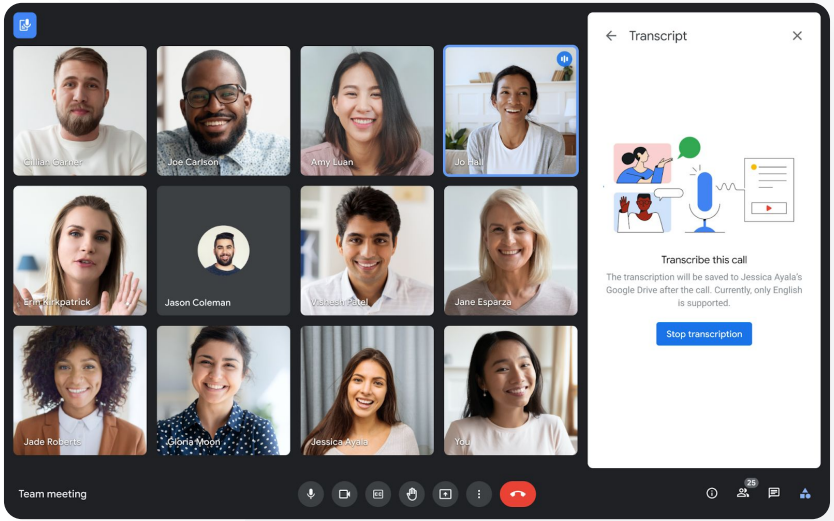
Instructies: Verwijzen naar wat in de les is besproken

Transcripten aanzetten in Google Meet

- Selecteer rechtsonder in een vergadering het **activiteitenicoon**
- Klik op **Transcripten** > **Transcriptie starten** > **Starten**

Transcriptie stoppen in Google Meet

- Selecteer het **activiteitenicoon** > **Transcripten** > **Transcriptie stoppen** > **Stoppen**



Relevante Helpcentrum-documentatie

- Transcript maken met Google Meet
- Transcriptie aan- of uitzetten

"We organiseren virtuele videovergaderingen met ouders/docenten, maar soms spreken we niet allemaal dezelfde taal.

Hoe kan ik taalbarrières wegnemen en vergaderingen inclusiever maken?"

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Vertaalde ondertiteling gebruiken in Google Meet

Taalbarrières wegnemen

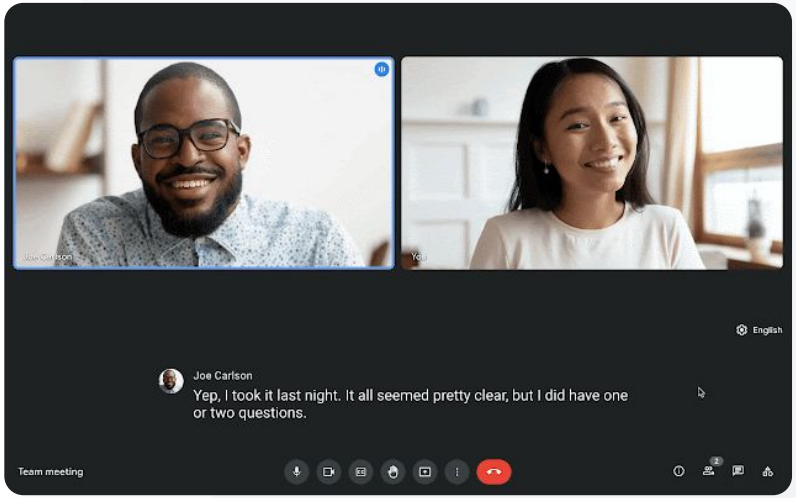
Vertaalde ondertiteling maakt vergaderingen inclusiever, omdat taalbarrières worden weggenomen. Als deelnemers content in hun voorkeurstaal krijgen, is informatie delen, leren en samenwerken voor iedereen toegankelijker.

- Docenten kunnen interactie hebben met leerlingen, ouders en andere stakeholders die een andere taal spreken
- Gebruik vertaalde ondertiteling om Engels te vertalen naar Frans, Duits, Portugees of Spaans of andersom
- Of vertaal Engels naar Japans, Mandarijn of Zweeds

Instructies: Taalbarrières wegnemen

Vertaalde ondertiteling aanzetten

- Klik tijdens een vergadering onderin het scherm op **Meer opties** > **Instellingen** > **Ondertiteling**
- Zet **Ondertiteling** aan
- Selecteer de **taal van de vergadering**
- Zet **Vertaalde ondertiteling** aan
- Selecteer de **taal waarnaar je wilt vertalen**



Relevante Helpcentrum-documentatie

- Vertaalde ondertiteling gebruiken in Google Meet

"We moeten onze vergaderingen kunnen livestreamen voor een brede groep stakeholders en ouders."

Bijeenkomsten, evenementen en vergaderingen uitzenden

Livestream naar tot wel 10.000 kijkers met de Teaching and Learning Upgrade en naar tot wel 100.000 kijkers met Education Plus. Kijkers kunnen deelnemen door te klikken op de link van de livestream. De organisator deelt deze in een e-mail of via de Agenda-uitnodiging.

- Bepaal hoe breed je livestream wordt gedeeld. Kies hoe toegankelijk de stream is:
  - Alleen zichtbaar voor gebruikers in je organisatie (in je domein)
  - Gedeeld met andere vertrouwde Google Workspace-domeinen
  - Te bekijken op YouTube
- We raden IT-beheerders aan om livestreaming alleen aan te zetten voor docenten en andere medewerkers
- Als een gebruiker de livestream mist, kan deze de opname bekijken nadat de vergadering is beëindigd
- Voeg aan een livestream ondertiteling, polls en vragen en antwoorden toe om deze inclusiever te maken en meer betrokkenheid te krijgen

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Livestreaming aan- of uitzetten voor Meet
- Een videovergadering livestreamen

Instructies: Bijeenkomsten, evenementen en vergaderingen uitzenden

Een livestream maken

- Open **Google Agenda**
- Selecteer + Maken **Afspraak** > **Meer opties**
- Vul de afspraakgegevens in, zoals de datum, tijd en beschrijving
- Voeg mensen toe die volledig aan de videovergadering kunnen deelnemen. Dit houdt in dat anderen ze kunnen zien en horen, en dat ze kunnen presenteren
- Klik op **Google Meet-videovergadering toevoegen** > **Meet**
- Selecteer naast Deelnemen via Google Meet de **pijl-omlaag** en dan **Livestream toevoegen**
- Als je het maximale aantal personen wilt uitnodigen dat is toegestaan met je betaalde versie, klik je op **Kopiëren** en deel je de URL van de livestream
- Selecteer **Opslaan**
- Livestreams worden niet automatisch gestart. Selecteer tijdens de vergadering **Meer** > **Streamen starten**

Relevante Helpcentrum-documentatie

- Livestreaming aan- of uitzetten voor Meet
- Een videovergadering livestreamen

Vragen stellen

Gebruik de **Q&A**-functie 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.

- Moderators kunnen zo veel 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.

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

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Deelnemers vragen stellen in Google Meet

Instructies: Vragen stellen

Een vraag stellen

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

Vragenrapport bekijken

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

Relevante Helpcentrum-documentatie

- Deelnemers vragen stellen in Google Meet

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

Input verzamelen

Degene die een virtuele vergadering heeft gepland of start, kan een **poll** maken voor 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. Polls 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: Input verzamelen

Een poll maken

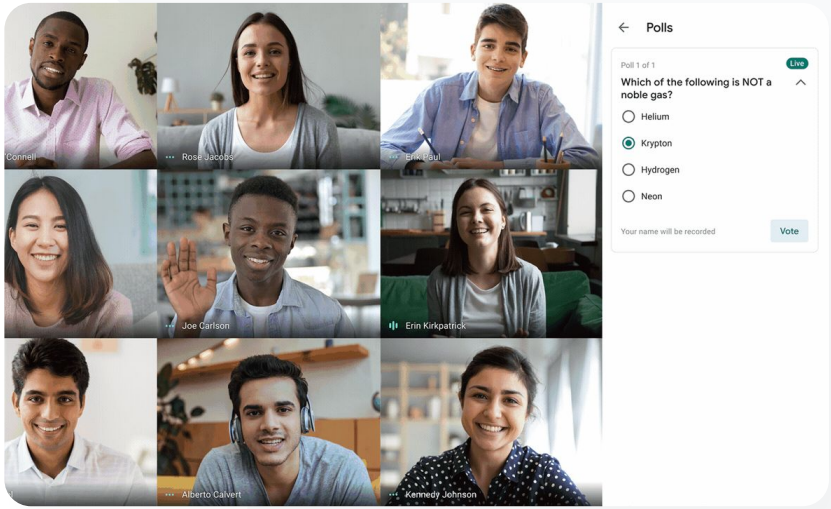
- Klik rechtsboven in een vergadering op het **activiteitenicoon** > **Poll**
- Kies **Poll starten**
- Geef een vraag op
- Selecteer **Starten** of **Opslaan**

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 het rapport**
- Open de e-mail en selecteer het **rapport in de bijlage**



Relevante Helpcentrum-documentatie

- Polls uitvoeren in Google Meet

"Soms hebben we leerlingen die vanuit huis leren. Ik heb een manier nodig om bij kleine groepsopdrachten makkelijk breakoutruimtes te kunnen maken op basis van vooraf gedefinieerde groepen."

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Breakoutruimtes gebruiken in Google Meet

Kleine leerlinggroepen

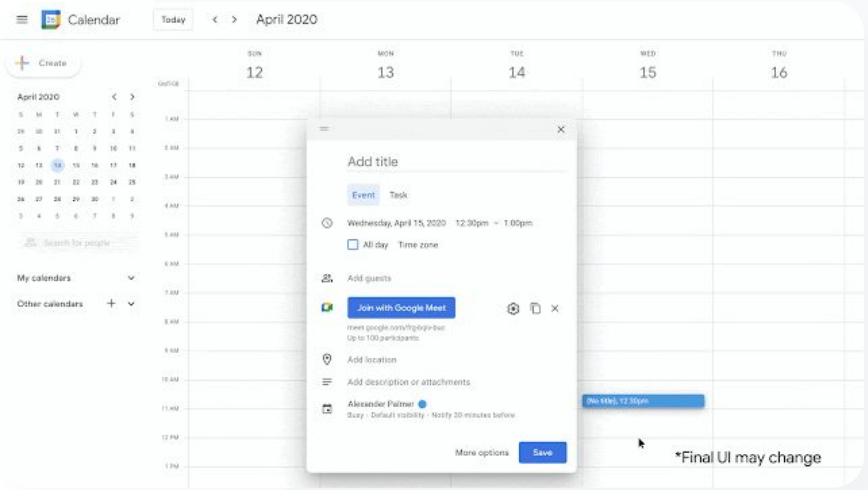
Docenten kunnen breakoutruimtes gebruiken om leerlingen in kleinere groepen te verdelen tijdens virtuele, **hybride of fysieke lessen**. Breakoutruimtes moeten door moderators worden gestart tijdens een videogesprek op een computer.

- Je kunt breakoutruimtes vooraf maken (als je een afspraak plant) of tijdens de vergadering.
- 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.

Instructies: Kleine groepen leerlingen maken

Breakoutruimtes maken vóór de vergadering

- Maak een nieuwe afspraak in Google Agenda
- Klik op **Google Meet-videovergadering toevoegen**
- Voeg deelnemers toe en selecteer **Instellingen voor vergadering wijzigen**
- Klik op **Breakoutruimtes**
- Kies het aantal breakoutruimtes en ga op een van deze manieren verder:
  - Sleep deelnemers naar verschillende ruimtes
  - Vul namen rechtstreeks in een ruimte in
  - Klik op **Shuffle** om de groepen willekeurig in te delen
- Klik op **Opslaan**



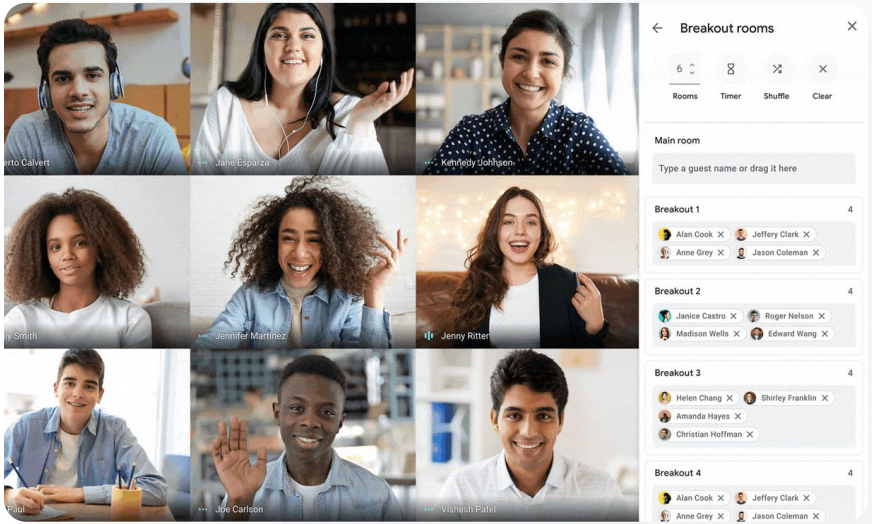
Relevante Helpcentrum-documentatie

- Breakoutruimtes gebruiken in Google Meet

Instructies: Kleine groepen leerlingen maken

Breakoutruimtes maken tijdens de vergadering

- Videogesprek starten
- Selecteer rechtsboven het **activiteitenicoon** > **Breakoutruimtes**
- Kies in het deelvenster Breakoutruimtes **hoeveel breakoutruimtes** je nodig hebt
- Leerlingen worden daarna verdeeld over de ruimtes, maar de moderators kunnen mensen indien nodig verplaatsen naar een andere ruimte
- Klik rechtsonder op **Ruimtes openen**



Vragen beantwoorden in verschillende breakoutruimtes

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

Relevante Helpcentrum-documentatie

- Breakoutruimtes gebruiken in Google Meet

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

Deelname bijhouden

Deelname bijhouden geeft je een automatisch deelnamerapport voor elke vergadering met vijf of meer deelnemers. De rapporten tonen wie er heeft deelgenomen aan het gesprek, de e-mailadressen van de deelnemers en hoelang ze hebben meegedaan aan de virtuele les.

- 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

Stapsgewijze instructies

Relevante Helpcentrum-documentatie

- Deelname bijhouden in Google Meet

Instructies: Deelname bijhouden

Deelname bijhouden in een vergadering

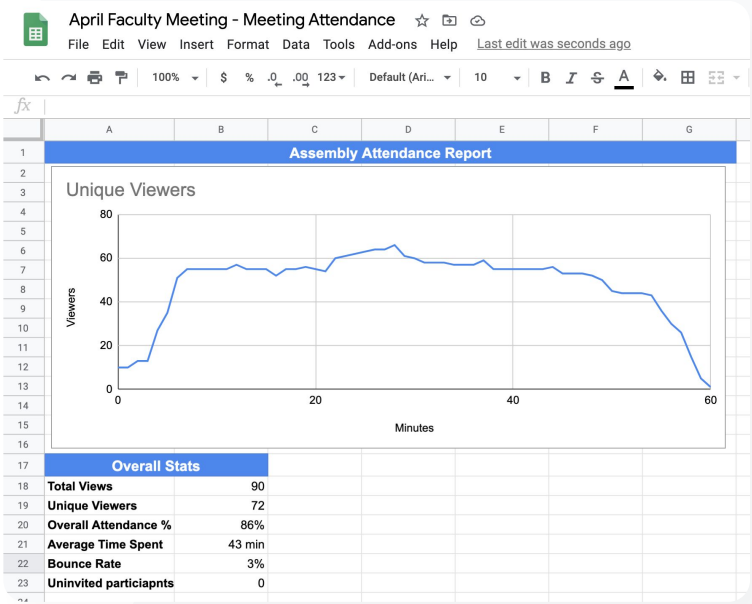
- Videogesprek starten
- Selecteer onderaan het **menu-icoon**
- Klik op het **instellingenicoon** > **Opties voor host**
- Zet **Deelname bijhouden** aan of uit

Deelname bijhouden in Agenda

- **Zet Google Meet-vergaderingen aan** vanuit een Agenda-afspraak
- Selecteer rechts het **instellingenicoon**
- Vink het vakje aan naast **Deelname bijhouden** en klik op **Opslaan**

Het deelnamerapport downloaden

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



Relevante Helpcentrum-documentatie

- Deelname bijhouden in Google Meet

Bedankt