Google for Education

Over 40 måder at bruge betalingsudgaverne af Google Workspace for Education på

goo.gle/use-edu-workspace

Sådan bruges diasshowet

Dette diasshow indeholder et udvalg af de mest populære eksempler på brug, der er tilgængelige, hvis du anvender en af **betalingsudgaverne af Google Workspace for Education**. Disse værktøjer kan være med til at forbedre **datasikkerheden, undervisernes effektivitet, elevernes engagement, samarbejdet på hele skolen** og meget mere.

Diasshowet er organiseret efter **funktion** efterfulgt af **almindelige eksempler på brug** samt enkle **vejledninger** i brugen af funktionen. Gennemgå hele diasshowet, og se, hvor meget du kan gøre med betalte udgaver af Google Workspace for Education.

Betalingsudgaver af Google Workspace for Education

Få flere valgmuligheder, mere kontrol og fleksibilitet til at opfylde din organisations behov med tre betalingsudgaver af Google Workspace for Education.

Google Workspace for Education Plus

Omfatter Education Standard, Teaching and Learning Upgrade og flere funktioner, der kun gælder for Plus.

Education Plus styrker elever, undervisere, uddannelsesledere og it-administratorer med en uddannelsesteknologisk **universalløsning** med brugervenlige værktøjer, der giver **avanceret sikkerhed og indsigt samt beriget undervisning og læring**.

Google Workspace for Education Standard

Avancerede sikkerhedsværktøjer og avanceret indsigt hjælper med at reducere risici og undgå trusler med øget synlighed og kontrol i hele dit læringsmiljø.

Teaching and Learning Upgrade

Forbedrede værktøjer til undervisning og læring er med til at forbedre undervisningens gennemslagskraft ved at gøre læring mere personlig, skabe effektiv undervisning og muliggøre undervisning og læring, uanset hvor man er.

Indholdsfortegnelse

Avancerede sikkerhedsværktøjer og avanceret indsigt

Kontrolpanel for sikkerhed

- Spammængde
- Ekstern fildeling
- Tredjepartsapps
- Forsøg på phishing

Siden Sikkerhedstilstand

- Optimale løsninger for sikkerhed
- Anbefalinger vedrørende risikoområder

Undersøgelsesværktøj

- Deling af krænkende materiale
- Utilsigtet deling af filer
- Phishing og malware i mails
- Stop skadelige aktører
- Større indsigt i sikkerhed
- Undgå møder uden opsyn

Domæneadministration og -styring

- Scan Gmail-vedhæftninger for trusler
- Opret brugskontrolpaneler og brugsrapporter
- Find filer nemmere
- Organiserede interne dokumenter
- Udfyld afdelingsgrupper automatisk
- Opret målgrupper til intern fildeling
- Begræns fildeling
- Begrænsninger for Workspace-appen
- Administrer lagerplads
- Datalovgivning
- Regler for tilskud
- Administrer slutpunktsenheder
- Administrer Windows-enheder
- Tilpassede indstillinger for Windows-enheder
- Automatisér Windows-enhedsopdateringer
- Brug kryptering på klientsiden

Indholdsfortegnelse

Forbedrede undervisnings- og læringsmuligheder

Google Classroom

- Administrer adgang til Classroom-tilføjelser
- Integrer engagerende indhold i Classroom
- Opret hold i stor skala

Originalitetsrapporter

- Scan for plagiering med originalitetsrapporter
- Tjek originalitet i forhold til tidligere elevopgaver
- Gør registrering af plagiering til en mulighed for at lære

Docs, Sheets og Slides

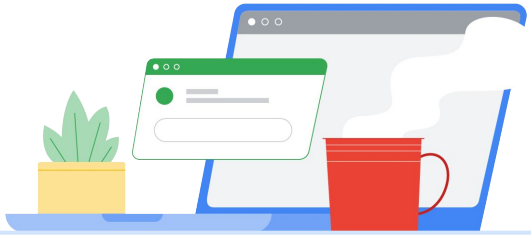
- Godkend interne dokumenter

Google Meet

- Optage møder
- Henvis til det, der blev talt om i timen
- Fjern sprogbarrierer
- Send fællessamlinger og skoleevents
- Stil spørgsmål
- Indsamling af output
- Små elevgrupper
- Registrering af deltagelse

Avancerede sikkerhedsværktøjer og avanceret indsigt

Få mere kontrol på hele dit domæne med proaktive sikkerhedsværktøjer, der hjælper dig med at forsvare dig mod trusler, analysere sikkerhedshændelser og beskytte elevernes og undervisernes data.

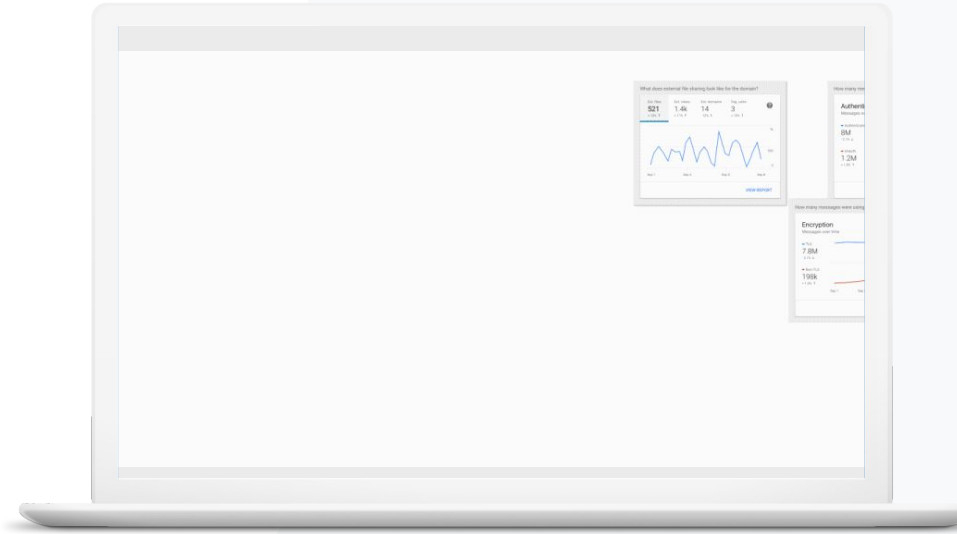


- Kontrolpanel for sikkerhed
- Siden Sikkerhedstilstand
- Undersøgelsesværktøj
- Domæneadministration og -styring

Kontrolpanel for sikkerhed

Hvad er det?

Brug kontrolpanelet for sikkerhed til at se en oversigt over forskellige sikkerhedsrapporter. De enkelte paneler med sikkerhedsrapporter viser som standard data fra de seneste syv dage. Du kan tilpasse kontrolpanelet for at se data fra i dag, i går, denne uge, sidste uge, denne måned, sidste måned eller nogle dage siden (op til 180 dage).



Eksempler på brug

Spammængde	Detaljeret vejledning
Ekstern fildeling	Detaljeret vejledning
Tredjepartsapps	Detaljeret vejledning
Forsøg på phishing	Detaljeret vejledning

Jeg vil gerne undgå for mange og unødvendige mails og samtidigt reducere antallet af trusler mod sikkerheden for min skole."

Spammængde

Kontrolpanelet for sikkerhed giver en visuel repræsentation af aktiviteten i hele dit Google Workspace for Education-miljø, herunder:

- Spam
- Phishing
- Malware
- Mistænkelige vedhæftede filer
- Og meget andet

Detaljeret vejledning

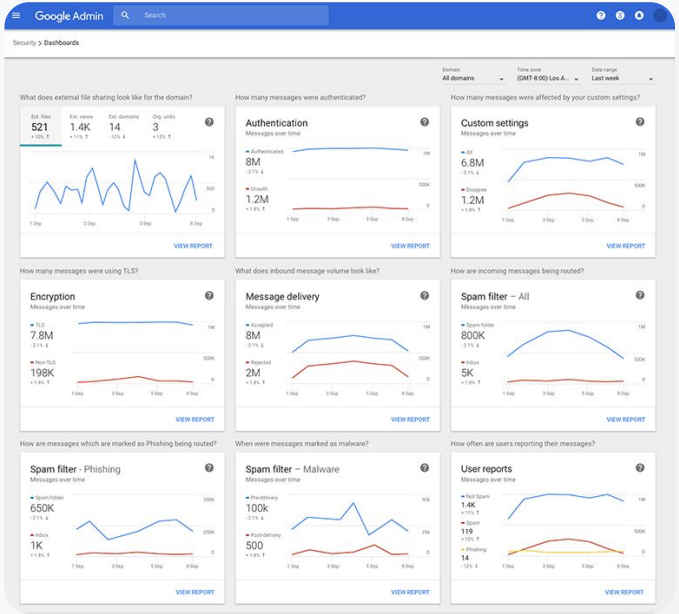
Relevant dokumentation i Hjælp

- Om kontrolpanelet for sikkerhed

Vejledning: Oversigt over kontrolpanel

Sådan ser du kontrolpanelet for sikkerhed

- Log ind på **Administrationskonsol**
- Klik på **Sikkerhed** > **Kontrolpanel**
- I kontrolpanelet for sikkerhed kan du se detaljerede oplysninger, eksportere data til Sheets eller et værktøj fra en tredjepart eller starte en undersøgelse i undersøgelsesværktøjet



Relevant dokumentation i Hjælp

- Om kontrolpanelet for sikkerhed

Jeg vil gerne se ekstern fildelingsaktivitet for at forhindre, at følsomme oplysninger deles med tredjeparter."

Ekstern fildeling

Brug **rapporten om fileksponering** fra **kontrolpanelet for sikkerhed** til at se metrics for ekstern fildeling for dit domæne, herunder:

- Antal delingshændelser til brugere uden for dit domæne i et angivet tidsrum.
- Antal visninger, en ekstern fil har haft i løbet af et bestemt tidsrum.

Detaljeret vejledning

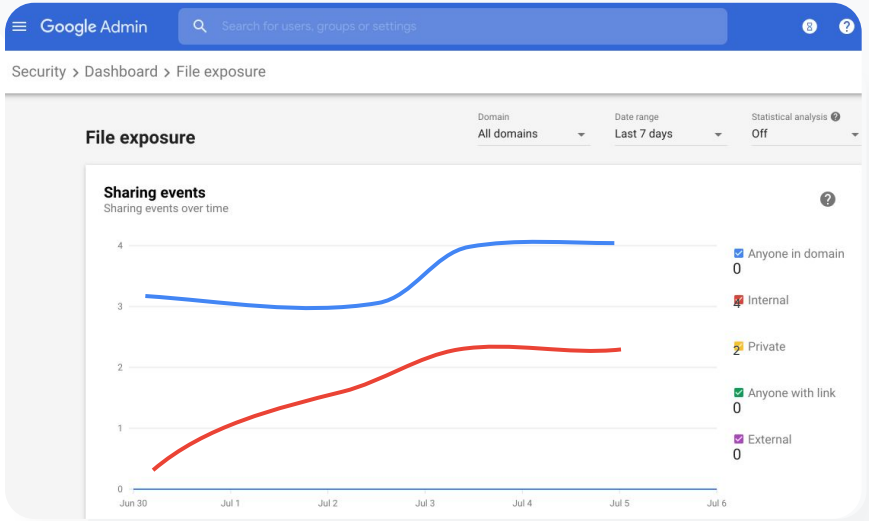
Relevant dokumentation i Hjælp

- Kom godt i gang med siden Sikkerhedstilstand

Vejledning: Ekstern fildeling

Sådan ser du rapporten om fileksponering

- Log ind på **Administrationskonsol.**
- Klik på **Sikkerhed** > **Kontrolpanel**
- I panelet med titlen "**Hvordan ser ekstern fildeling ud for domænet?**" skal du klikke på **Se rapport** nederst til højre



Relevant dokumentation i Hjælp

- Om kontrolpanelet for sikkerhed
- Rapport om fileksponering

"Jeg vil gerne se, hvilke tredjepartsapps der har adgang til mit domænes data."

Tredjepartsapps

Brug **rapporten om OAuth-tildelingsaktivitet** fra **kontrolpanelet for sikkerhed** til at holde øje med, hvilke tredjepartsapps der har forbindelse til dit domæne, og hvilke data de har adgang til.

- OAuth giver tredjepartstjenester adgangstilladelse til en brugers kontooplysninger uden at afsløre brugerens adgangskode. Det kan være en god idé at begrænse, hvilke tredjepartsapps der har adgang.
- Brug panelet OAuth-tildelingsaktivitet til at overvåge tildelingsaktivitet efter app, omfang eller bruger og til at opdatere tildelte tilladelser.

Detaljeret vejledning

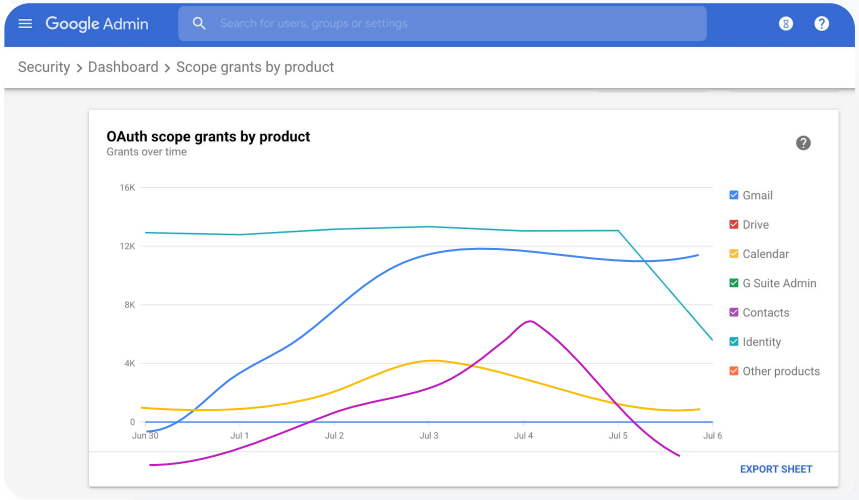
Relevant dokumentation i Hjælp

- Rapport om OAuth-tildelingsaktivitet

Vejledning: Tredjepartsapps

Sådan ser du rapporten om OAuth-tildelingsaktivitet

- Log ind på **Administrationskonsol**
- Klik på **Sikkerhed** > **Kontrolpanel**
- Klik på **Se rapport nederst**
- Du kan se OAuth-tildelingsaktivitet efter produkt (app), omfang eller bruger
- Hvis du vil filtrere oplysningerne, skal du klikke på **App**, **Omfang** eller **Bruger**
- Du kan generere rapporten i et regneark ved at klikke på **Eksportér regneark**



Relevant dokumentation i Hjælp

- Rapport om OAuth-tildelingsaktivitet

Nogle brugere har rapporteret et forsøg på phishing. Jeg vil gerne se, hvornår phishingmailen blev modtaget, hvad det præcis var for en mail, min bruger modtog, og hvilken risiko brugeren blev udsat for."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Sådan markerer brugere deres mails
- Brugerrapporter

Forsøg på phishing

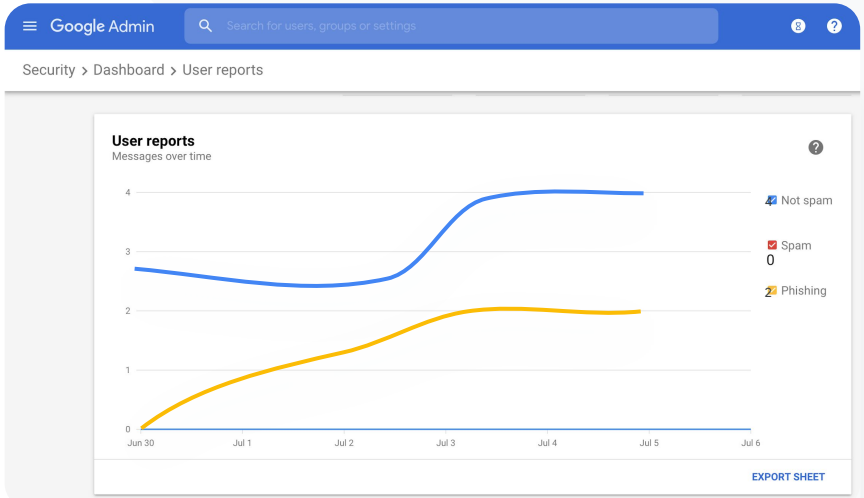
Panelet Brugerrapporter i **kontrolpanelet for sikkerhed** giver dig mulighed for at se meddelelser, der blev rapporteret som phishing eller spam inden for et bestemt tidsrum. Du kan se oplysninger om mails, der er rapporteret som phishing, f.eks. modtagere og antal åbninger.

- Brugerrapporter giver dig mulighed for at se, hvordan brugerne markerer deres meddelelser – f.eks. som spam, ikke spam eller phishing – inden for et bestemt tidsrum.
- Du kan tilpasse grafen for kun at få oplysninger om visse typer meddelelser. Det kan f.eks. være, hvorvidt meddelelserne blev sendt internt eller eksternt, efter datointerval osv.

Vejledning: Forsøg på phishing

Sådan ser du panelet Brugerrapporter

- Log ind på **Administrationskonsol**
- Klik på **Sikkerhed** > **Kontrolpanel**
- Nederst til højre på **panelet Brugerrapporter** skal du klikke på **Se rapport**



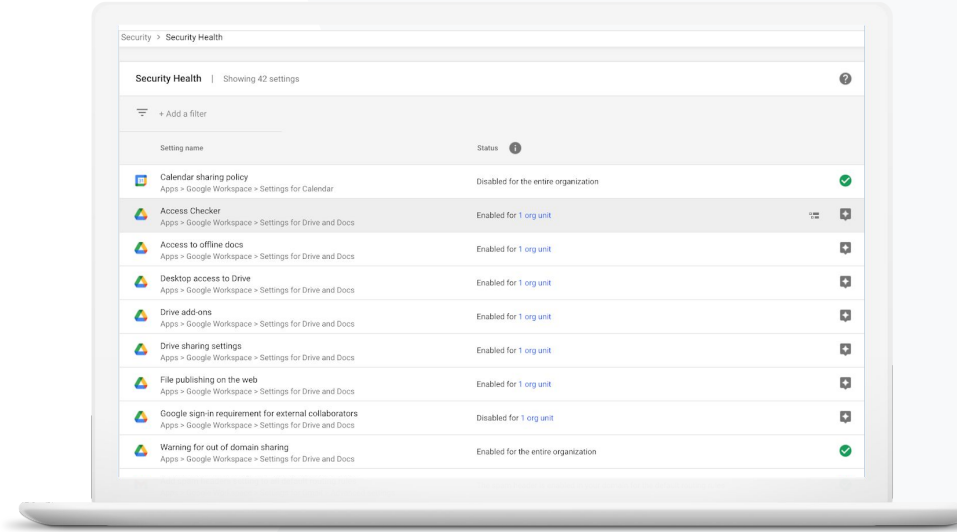
Relevant dokumentation i Hjælp

- Om kontrolpanelet for sikkerhed
- Rapport om fileksponering

Sikkerhedstilstand

Hvad er det?

Siden Sikkerhedstilstand indeholder en omfattende oversigt over sikkerhedsniveauet for dit Google Workspace-miljø, hvor du kan sammenligne dine konfigurationer med anbefalinger fra Google for proaktivt at beskytte din organisation.



Eksempler på brug

Optimale løsninger for sikkerhed	Detaljeret vejledning
Anbefalinger vedrørende risikoområder	Detaljeret vejledning

"Giv mig forslag til optimale løsninger eller anbefalinger vedrørende konfiguration af sikkerhedspolitikker."

Optimale løsninger for sikkerhed

Åbn siden Sikkerhedstilstand for at se optimale løsninger for sikkerhedspolitikker med:

- Anbefalinger vedrørende potentielle risikoområder på dit domæne
- Anbefalinger om optimale indstillinger for at øge effektiviteten af beskyttelsen
- Direkte links til indstillingerne
- Yderligere oplysninger og supportartikler

Detaljeret vejledning

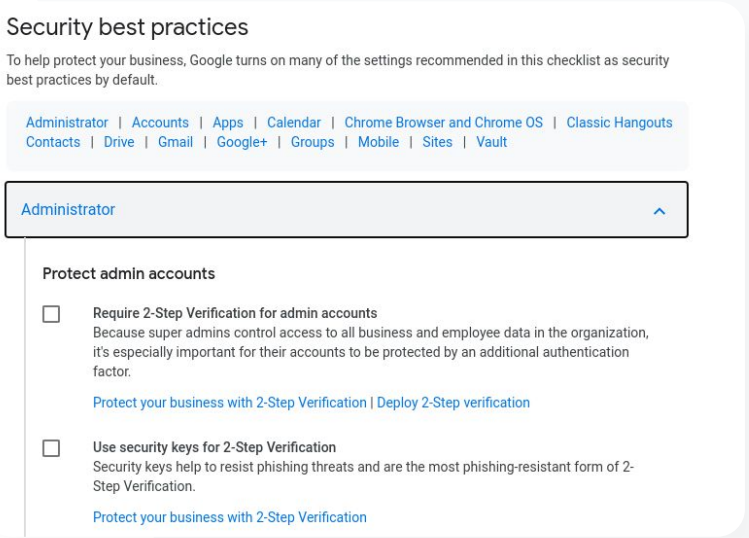
Relevant dokumentation i Hjælp

- Kom godt i gang med siden Sikkerhedstilstand

Vejledning: Tjekliste for optimale løsninger for sikkerhed

Google aktiverer som standard mange af de indstillinger, der anbefales på tjeklisten som optimale løsninger for sikkerhed, for at hjælpe med at beskytte din organisation. Vi anbefaler, at du ser nærmere på dem, der er fremhævet nedenfor.

- **Administrator:** Beskyt administratorkonti
- **Konti:** Hjælp med at forhindre og afhjælpe kompromitterede konti
- **Apps:** Gennemgå tredjeparters adgang til kernetjenester
- **Kalender:** Begræns ekstern deling af kalendere
- **Drev:** Begræns deling og samarbejde uden for dit domæne
- **Gmail:** Konfigurer godkendelse og infrastruktur
- **Vault:** Administrer, gennemgå og beskyt Vault-konti



Relevant dokumentation i Hjælp

- Overvåg tilstanden af dine sikkerhedsindstillinger

"Jeg vil gerne have et sammenfattet øjebliksbillede af sikkerhedsindstillingerne for mit domæne med handlingsrettede anbefalinger, så jeg kan gøre noget ved potentielle risikoområder."

Anbefalinger vedrørende risikoområder

Siden **Sikkerhedstilstand** gennemgår din sikkerhedskonfiguration og rapporterer anbefalede ændringer. På siden Sikkerhedstilstand kan du gøre følgende:

- Hurtigt identificere områder med potentielle risici på dit domæne
- Få anbefalinger om optimale indstillinger for at øge effektiviteten af din beskyttelse
- Læse yderligere oplysninger og supportartikler om anbefalingerne

Detaljeret vejledning

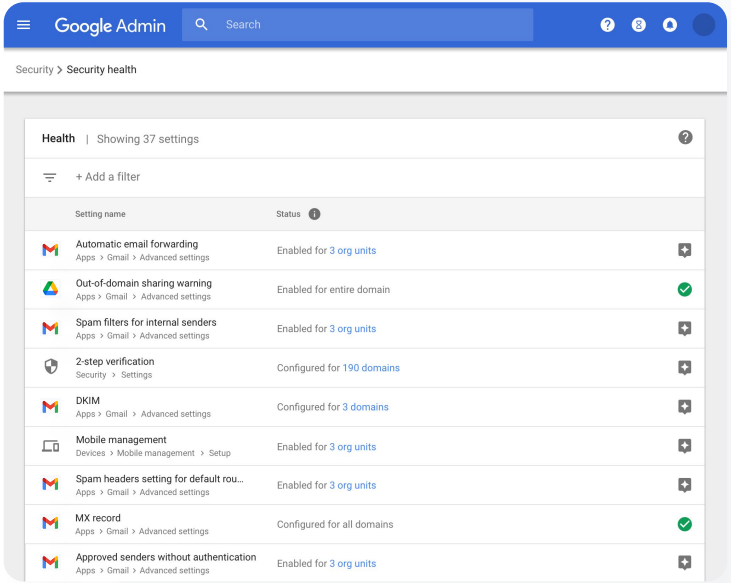
Relevant dokumentation i Hjælp

- Kom godt i gang med siden Sikkerhedstilstand

Vejledning: Sikkerhedsanbefalinger

Sådan ser du anbefalinger

- Log ind på **Administrationskonsol**
- Klik på **Sikkerhed** > **Sikkerhedstilstand**
- Se statusindstillingerne i kolonnen yderst til højre
  - Et grønt flueben angiver en sikker indstilling
  - Et gråt ikon angiver en anbefaling om at undersøge indstillingen nærmere. Klik på ikonet for at åbne info og vejledninger



Relevant dokumentation i Hjælp

- Kom godt i gang med siden Sikkerhedstilstand

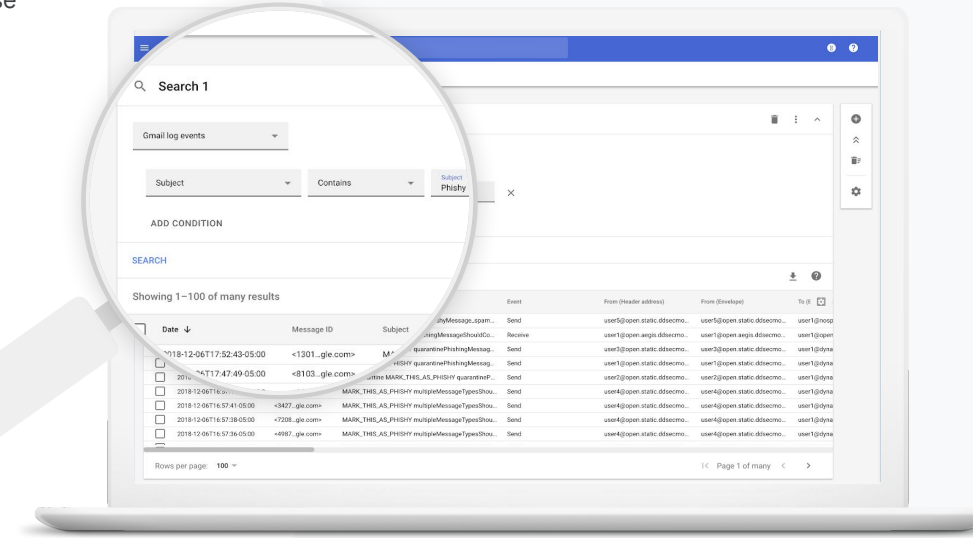
Undersøgelsesværktøj

Hvad er det?

Brug undersøgelsesværktøjet til at identificere, rangere og reagere i forbindelse med sikkerheds- og privatlivsrelaterede problemer på dit domæne.

Eksempler på brug

Deling af krænkende materiale	Detaljeret vejledning
Utilsigtet fildeling	Detaljeret vejledning
Rangering af mail	Detaljeret vejledning
Phishing/malware i mails	Detaljeret vejledning
Stop skadelige aktører	Detaljeret vejledning
Større indsigt i sikkerhed	Detaljeret vejledning
Undgå møder uden opsyn	Detaljeret vejledning



"Jeg ved, at der er en fil med krænkende materiale, som bliver delt. Jeg vil gerne vide, hvem der har oprettet den, hvornår den blev oprettet, hvem der har delt den med hvem, hvem der har redigeret den, og jeg vil gerne slette den."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Betingelser for loghændelser i Drev
- Handlinger for loghændelser i Drev

Deling af krænkende materiale

Loghændelser i Drev i undersøgelsesværktøjet kan hjælpe dig med at finde, registrere og isolere eller slette uønskede filer på dit domæne. Når du tilgår Loghændelser i Drev, kan du:

- Søge efter dokumenter efter navn, aktør, ejer osv.
- Træffe foranstaltninger ved at ændre filtilladelserne eller slette filen
- Søge efter indhold, som brugere opretter i Google Workspace, og indhold, de uploader til Drev
- Se alle logoplysninger om det pågældende dokument
  - Oprettelsesdato
  - Hvem er ejeren, hvem har set det, og hvem har redigeret det
  - Hvornår blev det delt

En fil blev utilsigtet delt med en gruppe, som ikke skulle have adgang til den.

Jeg vil fjerne gruppens adgang til den.

Utilsigtet delte filer

Loghændelser i Drev i **undersøgelsesværktøjet** kan hjælpe dig med at spore og løse problemer med fildeling. Når du tilgår Loghændelser i Drev, kan du:

- Søge efter dokumenter efter navn, aktør, ejer osv.
- Se alle logoplysninger om det pågældende dokument, bl.a. hvem der har set det, og hvornår det blev delt
- Træffe foranstaltninger ved at ændre tilladelserne og deaktivere download, udskrivning og kopiering

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Køre en søgning i undersøgelsesværktøjet
- Træffe foranstaltninger baseret på søgeresultaterne

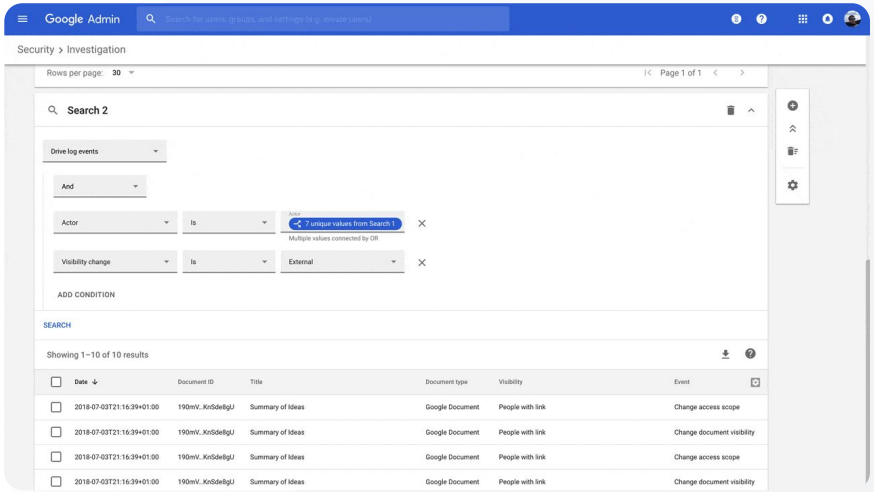
Vejledning: Loghændelser i Drev

Sådan undersøger du loghændelser i Drev

- Log ind på **Administrationskonsol.**
- Klik på **Sikkerhed** > **Undersøgelsesværktøj**
- Vælg **Loghændelser i Drev**
- Klik på **Tilføj betingelse** > **Søg**

Sådan træffer du foranstaltninger

- Vælg den relevante fil i søgeresultaterne
- Klik på **Handlinger** > **Revisionsfiltilladelser** for at åbne siden Tilladelser
- Klik på **Personer** for at se, hvem der har adgang
- Klik på **Links** for at se eller ændre indstillingerne for linkdeling for de valgte filer
- Klik på **Afventende ændringer** for at gennemgå dine ændringer, inden du gemmer



Relevant dokumentation i Hjælp

- Kør en søgning i undersøgelsesværktøjet
- Træffe foranstaltninger baseret på søgeresultaterne

“

En bruger har sendt en mail, der ikke skulle være sendt. Vi vil gerne vide, hvem brugeren har sendt den til, om modtagerne har åbnet den, om de har besvaret den, og vi vil gerne slette mailen. Jeg vil også gerne kende indholdet i mailen."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Betingelser for Gmail-logs og Gmail-meddelelser
- Handlinger for Gmail-meddelelser og loghændelser i Gmail
- Vejledning til at se indholdet i en mail

Rangering af mail

Gmail-loggerne i **undersøgelsesværktøjet** kan hjælpe dig med at identificere og reagere på farlige eller krænkende mails på dit domæne. Når du tilgår dine Gmail-logs, kan du gøre følgende:

- Søge efter bestemte mails efter emne, meddelelses-id, vedhæftet fil, afsender og lignende
- Se mailoplysninger som f.eks. forfatter, modtager, antal åbninger og videresendelser.
- Træffe foranstaltninger baseret på søgeresultaterne. Handlinger på Gmail-meddelelser omfatter sletning, gendannelse, markering som spam eller phishing, send til indbakken og send til karantæne.

"Der blev sendt en mail med phishing eller malware til brugerne. Vi vil gerne se, om brugerne har klikket på linket i mailen eller downloadet den vedhæftede fil. Hvis de har, kan det volde skade for brugerne og vores domæne."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Betingelser for Gmail-logs og Gmail-meddelelser
- Handlinger for Gmail-meddelelser og loghændelser i Gmail
- Vejledning til at se indholdet i en mail
- Se VirusTotal-rapporter

Phishing og malware i mails

Undersøgelsesværktøjet og især **Gmail-loggerne** kan hjælpe dig med at finde og isolere skadelige mails på dit domæne. Når du tilgår dine Gmail-logs, kan du gøre følgende:

- Søge i mailmeddelelser efter bestemt indhold, heriblandt vedhæftede filer
- Se oplysninger om bestemte mails, bl.a. modtagere og antal åbninger
- Se meddelelserne og tråden for at fastslå, om de er skadelige
- Scan vedhæftede filer i mails for at få detaljer om trusselskontekst og omdømmedata med VirusTotal-rapporter
- Træf foranstaltninger ved at markere meddelelserne som spam eller phishing, sende dem til en bestemt indbakke eller i karantæne eller at slette dem

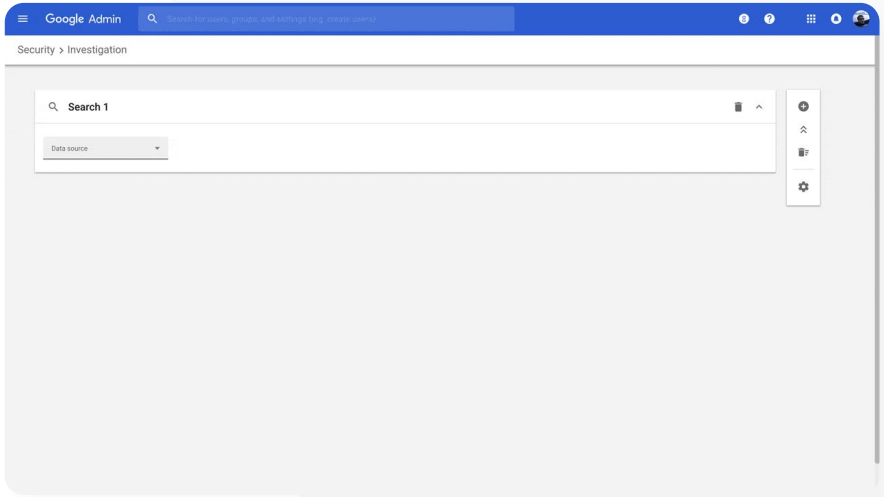
Vejledning: Gmail-logs

Sådan undersøger du Gmail-logs

- Log ind på **Administrationskonsol.**
- Klik på **Sikkerhed** > **Undersøgelsesværktøj**
- Vælg **Loghændelser i Gmail** eller **Gmail-meddelelser**
- Klik på **Tilføj betingelse** > **Søg**

Sådan træffer du foranstaltninger

- Vælg den relevante fil i søgeresultaterne
- Klik på **Handlinger**
- Vælg **Slet meddelelse fra indbakke**
- Hvis du vil bekræfte handlingen, skal du klikke på Vis nederst på siden
- Du kan se status for handlingen i kolonnen **Resultat**



Relevant dokumentation i Hjælp

- Betingelser for Gmail-logs og Gmail-meddelelser
- Handlinger for Gmail-meddelelser og loghændelser i Gmail
- Vejledning til at se indholdet i en mail

"En ondsindet aktør går konstant efter højtprofilerede brugere på mit domæne, og hver gang jeg forsøger at forhindre et angreb, dukker der et nyt op som et nyt muldvarpeskud i en græsplæne.

Hvordan stopper jeg det?"

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Søg efter og undersøg loghændelser for brugere
- Opret aktivitetsregler i undersøgelsesværktøjet

Stop skadelige aktører

Brugerloggen i **undersøgelsesværktøjet** kan hjælpe dig med at:

- Identificere og undersøge forsøg på at kapre brugerkonti i din organisation
- Holde øje med, hvilke totrinsmetoder brugerne i din organisation anvender
- Få flere oplysninger om mislykkede loginforsøg for brugere i din organisation
- Oprette aktivitetsregler i undersøgelsesværktøjet: Bloker automatisk meddelelser og anden skadelig aktivitet fra bestemte aktører
- Beskytte højtprofilerede brugere yderligere ved hjælp af programmet Avanceret beskyttelse
- Gendanne eller suspendere brugere

Vejledning: Stop skadelige aktører

Sådan undersøger du loghændelser for brugere

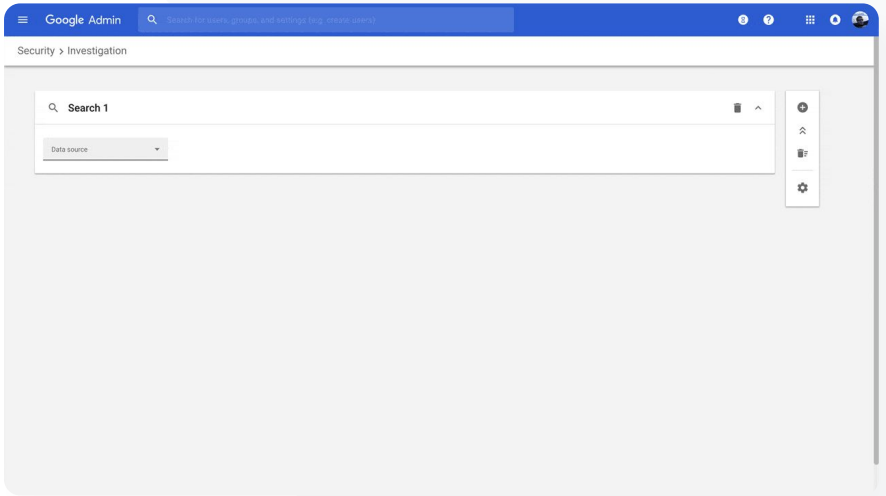
- Log ind på **Administrationskonsol.**
- Klik på **Sikkerhed** > **Undersøgelsesværktøj**
- Vælg **Loghændelser for bruger**
- Klik på **Tilføj betingelse** > **Søg**

Sådan gendanner eller suspenderer du brugere

- Vælg en eller flere brugere i søgeresultaterne
- Klik på rullemenuen **Handlinger**
- Klik på **Gendan bruger** eller **Suspender bruger**

Sådan ser du oplysninger om en bestemt bruger

- Vælg kun én bruger på siden med søgeresultaterne
- I rullemenuen Handlinger skal du klikke på **Se info**



Relevant dokumentation i Hjælp

- Søg efter og undersøg loghændelser for brugere

"En af vores undervisere har rapporteret, at en vedhæftet fil ser mistænkelig ud i Gmail.

Hvordan kan IT afgøre, om filen udgør en sikkerhedstrussel?"

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Kør en søgning i undersøgelsesværktøjet
- Se VirusTotal-rapporter fra undersøgelsesværktøjet

Få mere indsigt i sikkerhed

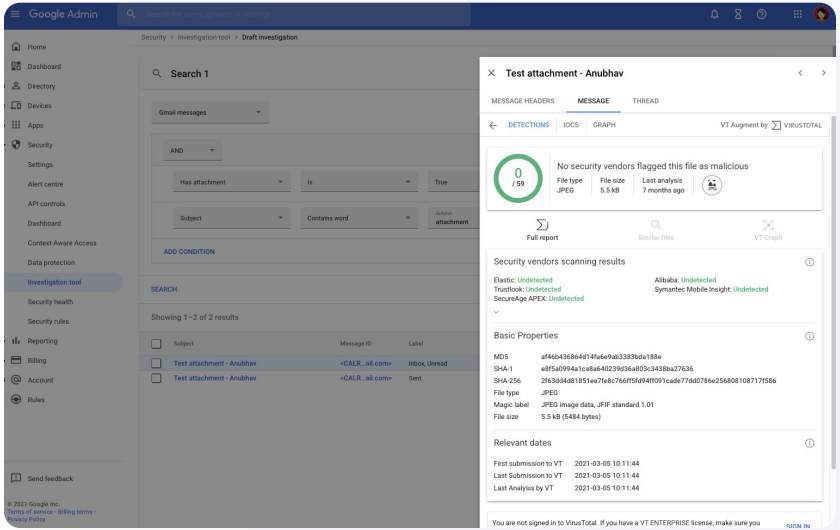
VirusTotal-rapporter udvider resultaterne af en sikkerhedsundersøgelse ved at indeholde en omfattende oversigt, hvilket giver administratorer mulighed for at kontrollere sikkerheden for et bestemt domæne, en vedhæftet fil, IP-adresse eller webadresse baseret på crowd-sourcet indsigt.

- Få yderligere sikkerhedsindsigt i loghændelser i Gmail og Chrome
- Analysér mistænkelige filer, webadresser, domæner og IP-adresser
- Få adgang til crowdsourcede oplysninger om, hvorfor en vedhæftet fil eller et website kan være risikabel
- Få hjælp til beslutningstagning, når du skal løse problemer med sikkerheden

Vejledning: Få mere indsigt i sikkerhed

Sådan ser du VirusTotal-rapporter, der er relateret til Gmail

- Log ind på **Administrationskonsol**
- Klik på **Sikkerhed** > **Sikkerhedscenter** > **Undersøgelsesværktøj**
- Vælg **Gmail-meddelelser**
- Klik på **Tilføj betingelse** > **Indeholder vedhæftede filer**
- Fra søgeresultater skal du klikke på **Meddelelses-id** eller **Emnelink**
- Fra sidepanelet skal du klikke på fanen **Meddelelse** eller **Tråd**
- Vælg **Se VirusTotal-rapport**



Administratorer kan også se VirusTotal-rapporter, der er relateret til Chrome. Du skal blot følge vejledningen ovenfor og vælge **Loghændelser i Chrome** i undersøgelsesværktøjet.

Relevant dokumentation i Hjælp

- Se VirusTotal-rapporter fra undersøgelsesværktøjet

Eleverne bliver hængende på Google Meet-opkald, når undervisningen er slut. Jeg har brug for en måde at afslutte Meet-opkald for alle for at forhindre afbrydelser i undervisningen."

Undgå ikke-styrede virtuelle møder

Google Workspace-administratorer kan bruge **Afslut møde for alle** i undersøgelsesværktøjet for at fjerne alle brugere fra et møde i organisationen. Mødeværter har samme mulighed for individuelle Google Meet-opkald.

- Mødet afsluttes for alle brugere i mødet, også personer i grupperum.
- Forhindrer enhver fra at deltage i kommende forekomster af mødet, uden at værten er til stede.

Detaljeret vejledning

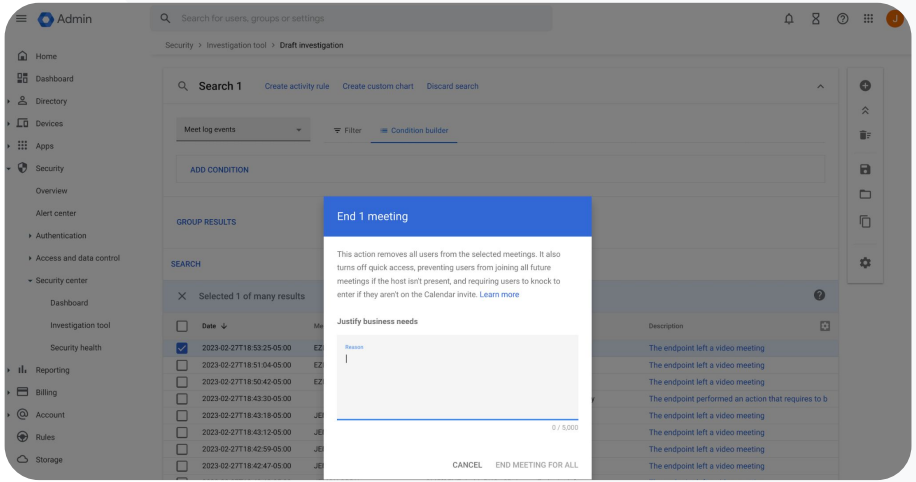
Relevant dokumentation i Hjælp

- Brug undersøgelsesværktøjet til at afslutte møder

Vejledning: Undgå ikke-styrede virtuelle møder

Sådan bruger du undersøgelsesværktøjet til at afslutte et møde for alle brugere

- Log ind på **Administrationskonsol**
- Klik på **Sikkerhed** > **Sikkerhedscenter** > **Undersøgelsesværktøj**
- Vælg **Loghændelser i Meet**
- Klik på **Søgning** > I søgeresultaterne får du vist en liste over Loghændelser i Meet
- Markér afkrydsningsfelterne ud for de møder, du vil afslutte for alle brugere
- Vælg **Handlinger**
- Klik på **Afslut møde for alle**



Relevant dokumentation i Hjælp

- Brug undersøgelsesværktøjet til at afslutte møder

Domæneadministration og -styring

Administratorer har adgang til avancerede værktøjer i Google Workspace, så de kan administrere organisationens data, konfigurere indstillinger, overvåge brug og hjælpe med at overholde uddannelsesrelaterede standarder.

Eksempler på brug

Scan Gmail-vedhæftninger for trusler	Detaljeret vejledning
Opret brugskontrolpaneler og brugsrapporter	Detaljeret vejledning
Find filer nemmere	Detaljeret vejledning
Organiser interne dokumenter	Detaljeret vejledning
Udfyld afdelingsgrupper automatisk	Detaljeret vejledning
Opret målgrupper til intern fildeling	Detaljeret vejledning
Begræns fildeling	Detaljeret vejledning
Begrænsninger for Workspace-appen	Detaljeret vejledning
Administrer lagerplads	Detaljeret vejledning
Datalovgivning	Detaljeret vejledning
Regler for tilskud	Detaljeret vejledning
Administrer slutpunktsenheder	Detaljeret vejledning
Administrer Windows-enheder	Detaljeret vejledning
Tilpassede indstillinger for Windows-enheder	Detaljeret vejledning
Automatisér Windows-enhedsopdateringer	Detaljeret vejledning
Brug kryptering på klientsiden	Detaljeret vejledning

“Hvordan kan jeg bedre beskytte mit domæne mod zero-day malware og ransomware-trusler?”

Scan Gmail-vedhæftninger for trusler

Vedhæftede filer i e-mails kan indeholde skadelig software. For at identificere disse trusler kan Gmail scanne eller åbne vedhæftede filer i Security Sandbox. Vedhæftede filer, der identificeres som trusler, sendes til Spam-mappen.

- Opdag malware ved at køre den i et privat, sikkert sandbox-miljø og analysere virkningerne for at identificere ondsindet adfærd
- Scan Microsoft Word-, PowerPoint-, PDF- og zip-filer med mere
- Aktivér scanning for hele domænet, eller opret scanningsregler baseret på specifikke forhold såsom afsender, domæne med mere

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Opsæt regler for at opdage skadelige vedhæftede filer

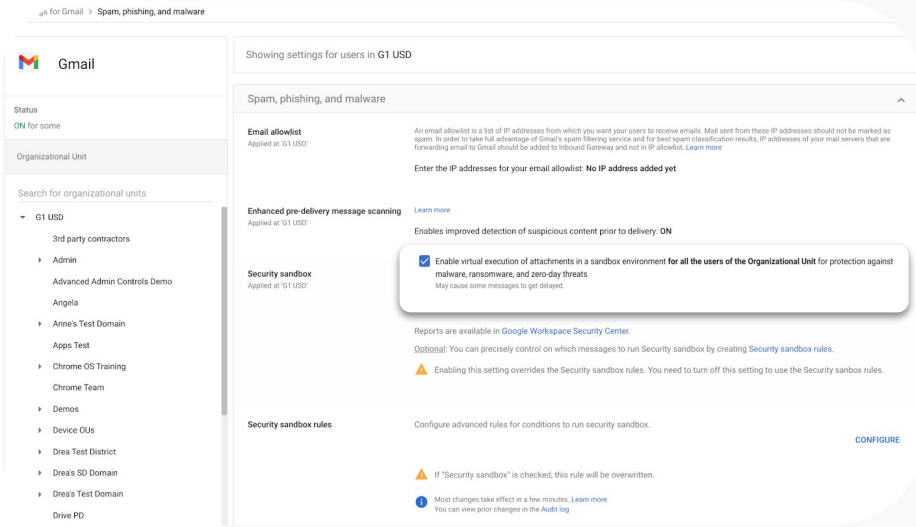
Vejledning: Scan Gmail-vedhæftninger for trusler

Sådan gør du

Vedhæftede filer i e-mails åbnes i en sandbox få minutter før levering af e-mailen, og dermed opnås et ekstra lag af sikkerhed.

Sådan scanner du alle vedhæftede filer i Security Sandbox

- Log ind i din **Administrationskonsol**
- Klik **Menu** > **Apps** > **Google Workspace** > **Gmail** > **Spam, Phishing og Malware**
- Vælg en organisationsenhed, eller anvend indstillinger på tværs af dit domæne
- Rul til **Security Sandbox** under **Spam, Phishing og Malware**
- Marker afkrydsningsfeltet **Aktiver virtuel åbning af vedhæftede filer i sandbox-miljø**
- Klik **Gem**



Relevant dokumentation i Hjælp

- Opsæt regler for at opdage skadelige vedhæftede filer

Hvordan kan jeg forstå brugen af Classroom på mit domæne?"

Opret brugskontrolpaneler og brugsrapporter

Med **BigQuery Export og Looker Studio-skabelon** kan administratorer bruge logfiler for aktivitet i Classroom til at oprette tilpassede kontrolpaneler og rapporter med analyseværktøjer som f.eks. Looker Studio og tredjepartsvisualiseringspartnere, der er integreret i BigQuery.

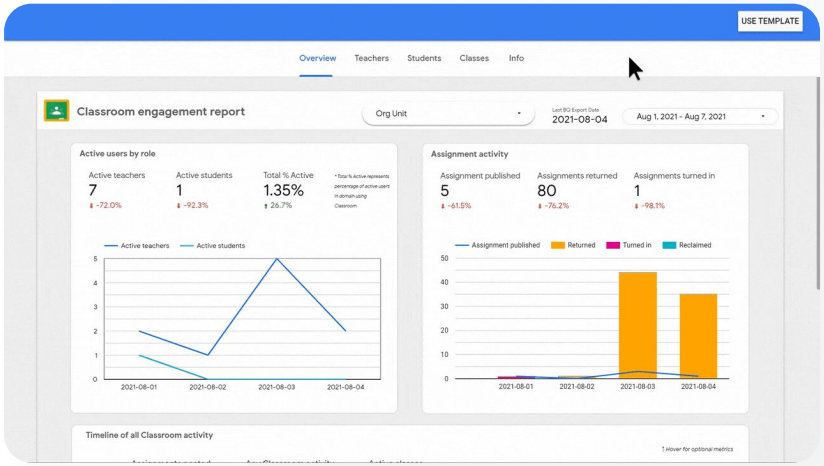
- Eksportere Classroom-logdata fra Administrationskonsol til BigQuery og Looker Studio.
- Se brugs- og indførelsesrapporter hurtigt på hele dit domæne. Se, hvem der fjernede en elev fra et hold, hvem der arkiverede et hold på en bestemt dato, og mere.
- Med tilpassede Looker Studio-kontrolpanelskabeloner kan du få indsigt i overordnede trends og reagere hurtigere.

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Konfigurer en BigQuery-eksport og en Data Studio-skabelon

Vejledning: Opret brugskontrolpaneler og brugsrapporter



1. Konfigurere og eksportere et BigQuery-projekt

- Log ind på console.cloud.google.com > **Opret et nyt projekt**
- Log ind på admin.google.com > **Rapporter** > **BigQuery Export**
- Klik på **Cloud BigQuery-projekt** > Angiv navnet for dit datasæt > **Gem**

2. Tilføj din BigQuery-eksport i Looker Studio

- Log ind på Looker Studio > **Opret** > **Datakilde**
- Vælg **BigQuery-connector** > **Mine projekter** > klik på det projekt, du har oprettet > **Aktivitet**
- Markér afkrydsningsfeltet under **Partitionstabel** > Klik på **Opret forbindelse**

3. Oprette et kontrolpanel i Looker Studio

- Åbn skabelonen > vælg **Brug skabelon**
- Under **Ny datakilde** skal du vælge **Aktivitet** datakilde
- Klik på **Kopiér rapport**

Relevant dokumentation i Hjælp

- Konfigurer en BigQuery-eksport og en Data Studio-skabelon

Jeg har brug for at finde de skriftlige tilladelser til en skoleudflugt, som forældre har indsendt via Gmail, Chat og Docs.

Hvordan finder jeg disse filer på mit domæne?"

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Vejledning til Google Cloud Search
- Slå Cloud Search til eller fra for brugere

Find filer nemmere

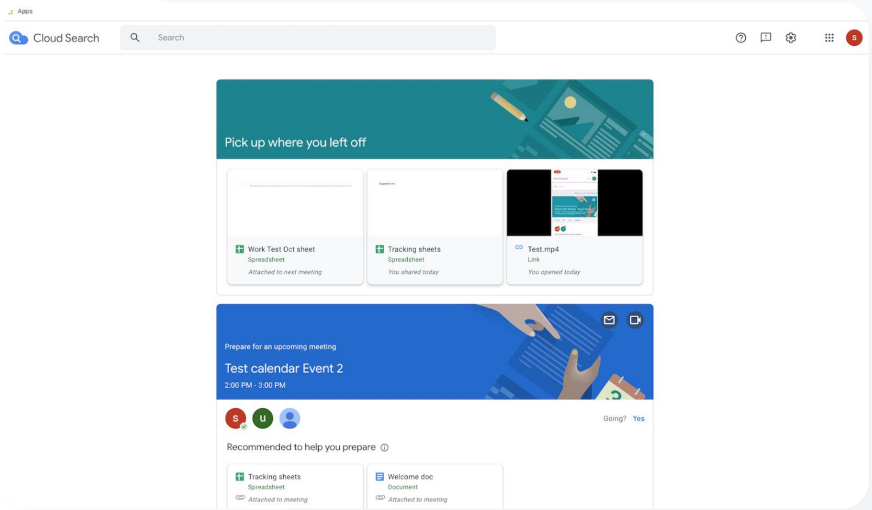
Med Google Cloud Search kan underviserne i din organisation hurtigt finde indhold i hele Google Workspace og apps fra tredjeparter.

- Find de oplysninger, du har brug for, fra et hvilket som helst sted, med din bærbare computer, din mobiltelefon eller tablet.
- Søg i Google Workspace-appsene, f.eks. Drev, Kontakter, Gmail og kilder fra tredjeparter

Vejledning: Find filer nemmere

Aktivér Cloud Search for brugere

- Log ind på **Administrationskonsol** > Gå til **Menu** > **Apps** > **Google**
- Klik på **Tjenestestatus**
- Hvis du vil slå en tjeneste til eller fra for alle i din organisation, skal du klikke på **Slået til for alle** eller **Slået fra for alle**
- Klik på **Gem**
- Hvis du vil aktivere en tjeneste for en gruppe brugere på tværs af eller i organisationsenheder, skal du vælge en **Adgangsgruppe**.
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Vejledning til Google Cloud Search
- Slå Cloud Search til eller fra for brugere

"Jeg vil anvende følsomhedsetiketter til min uddannelsesinstitutions filer, så de ensrettes og overholder gældende regler, forhindrer misbrug og forbedrer filorganisering."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Administrer Drev-etiketter

Organiser dokumenter på dit domæne

Drevetiketter hjælper brugere med at finde, organisere og anvende politikker på hele deres domæne. Administratorer kan oprette og administrere drevetiketter for at forhindre filmisbrug og sikre, at elevdata overholder de gældende regler.

- Etiketter er metadata, der kan hjælpe med at organisere følsomme uddannelsesfiler som f.eks. individuelle læringsprogrammer, DOD-dokumenter og overholdelsesdokumenter.
- Kun administratorer kan oprette, definere strukturer og offentliggøre etiketter. Brugerne i din organisation kan anvende etiketter til de filer, de redigerer, og kan angive feltværdier.
- Drev-etiketter kan bruges til at støtte automatiseret Forebyggelse af datatab.

Vejledning: Organiser dokumenter på dit domæne

Sådan fungerer det

Google Drev tilbyder badgeetiketter (en visuel indikator) og standardetiketter, som hjælper dig med at organisere filer på dit domæne.

Sådan aktiverer du Drev-etiketter for din uddannelsesinstitution

- Log ind på **Administrationskonsol**
- Klik på **Menu** > **Apps** > **Google Workspace** > **Drev og Docs**
- Vælg **Etiketter**
- Slå etiketter **til** eller **fra**
- Klik på **Gem**

Relevant dokumentation i Hjælp

- Administrer Drev-etiketter

Hvordan kan jeg automatisere gruppemedlemskab, så alle nye undervisere bliver inkluderet på min "underviser"-mailliste?"

Udfyld afdelingsgrupper automatisk

Dynamiske grupper gør det muligt for administratorer at opdatere gruppemedlemskab på hele skolen med tilpassede kriterier.

- Opret dynamiske grupper, der administrerer medlemskaber automatisk
- Holder grupperne opdaterede på grundlag af en medlemskabsforespørgsel, du opretter.
- Brug dynamiske grupper som
  - Mail- og distributionslister
  - Modererede grupper og fællesindbakker
  - Sikkerhedsgrupper

Detaljeret vejledning

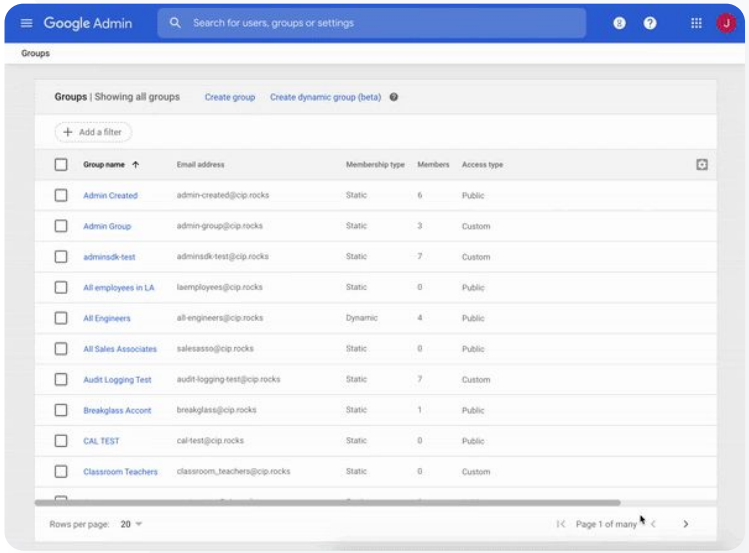
Relevant dokumentation i Hjælp

- Administrer medlemskab automatisk ved hjælp af dynamiske grupper

Vejledning: Udfyld grupper automatisk

Opret en dynamisk gruppe

- Log ind på **Administrationskonsol** > Gå til **Menu** > **Indeks** > **Grupper**
- Klik på **Opret dynamisk gruppe**
- Opret din forespørgsel om medlemskab i:
  - Liste over betingelser: Kriterier, der skal bruges til medlemskab, f.eks. afdeling
  - Værdifelt: Den værdi, du vil bruge.
- Angiv følgende oplysninger:
  - Navn: Identificerer gruppen på lister og i meddelelser
  - Beskrivelse: Formålet med gruppen
  - Gruppemail: Gruppens mailadresse
- Klik på **Gem**
- Klik på **Udfør**



Relevant dokumentation i Hjælp

- Administrer medlemskab automatisk ved hjælp af dynamiske grupper

"Mine undervisere deler utilsigtet dokumenter med hele organisationen og bringer dermed følsomme oplysninger i fare. Hvordan kan jeg begrænse det, de deler, til en mindre og mere relevant gruppe?"

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Om målgrupper
- De bedste fremgangsmåder til implementering af en målgruppe
- Opret en målgruppe

Opret målgrupper til intern fildeling

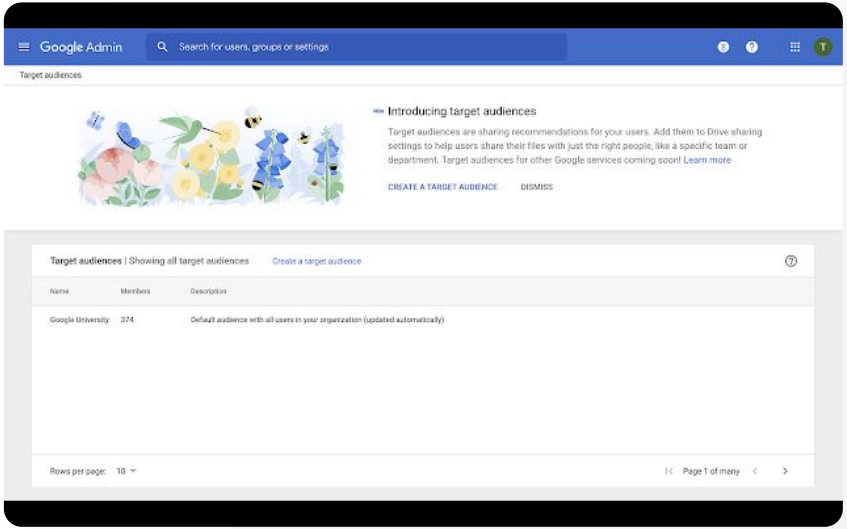
Målgruppeindstillinger hjælper med at forbedre sikkerheden af organisationens data ved at mindske muligheden for, at brugere utilsigtet deler for mange filer.

- Sørger for, at filer deles med de rette modtagere, f.eks. et specifikt team eller afdeling
- Målgrupper er grupper af brugere, som administratorer kan anbefale, at brugerne deler deres elementer med
- Administratorer kan tilføje målgrupper til brugeres delingsindstillinger for at tilskynde til deling med en mere specifik målgruppe
- Tilgængelig i Google Drev, Docs og Chat

Vejledning: Opret målgrupper til intern fildeling

Sådan fungerer det

Når du har oprettet en målgruppe, kan du tilføje medlemmer og anvende Målgrupper på Google Drev for at gøre den tilgængelig i brugernes delingsindstillinger. Du kan f.eks. gøre det muligt for en medarbejder at se en "Personale-målgruppe", når vedkommende deler Drevfiler.



Sådan aktiverer du Drev-etiketter for din uddannelsesinstitution

- Log ind på **Administrationskonsol** > gå til **Menu** > **Indeks** > **Målgrupper**
- Klik på **Opret målgruppe**
- Under **Navn** skal du angive et navn for målgruppen
- Vælg **Tilføj medlemmer** > inkluder de medlemmer, du vil
- Klik på **Udfør**

Relevant dokumentation i Hjælp

- Om målgrupper
- De bedste fremgangsmåder til implementering af en målgruppe
- Opret en målgruppe

Hvordan forhindrer jeg, at elever fra ældre årgange deler dokumenter med yngre elever?"

Begræns fildeling

Tillidsregler på Drev gør det muligt for administratorer at indstille regler for at kontrollere, hvem der får adgang til Google Drev-filer, så uddannelsesinstitutionens data holdes sikre. Politikker kan omfatte individuelle brugere, grupper, organisationsenheder og domæner.

- Beskyt følsomme oplysninger, og overhold branchestandarder og regler.
- Begræns intern og/eller ekstern deling af domænet. Administratorer kan oprette en tillidsregel, så det kun er studerende, der kan dele Drevfiler i din organisation
- Når "Tillidsregler" er aktiveret, erstatter de de eksisterende "Delingsindstillinger" i administratorkontroller til Google Drev.

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Opret og administrer tillidsregler for Drev-deling

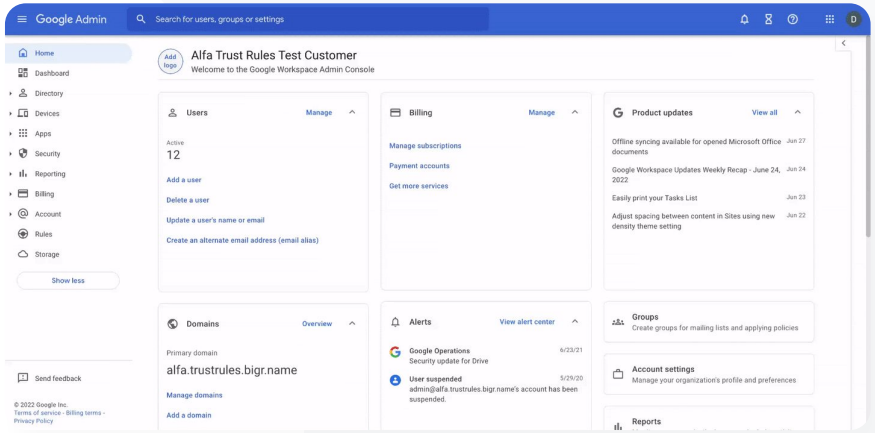
Vejledning: Begræns fildeling

Aktivér tillidsregler i Drev

- Log ind på **Administrationskonsol** > gå til **Menu** > **Regler**
- I kortet **Samarbejd sikkert** øverst på siden skal du klikke på **Aktivér tillidsregler**
- Dine Opgavelister åbnes automatisk og viser status for aktivering af tillidsregler

Administratorer kan oprette tillidsregler, se og redigere oplysninger om tillidsregler, slette tillidsregler og se loghændelser for tillidsregler.

Gå til Hjælp til Google Apps Admin for at få en trinvis vejledning til at administrere tillidsregler



Relevant dokumentation i Hjælp

- Opret og administrer tillidsregler for Drev-deling

Jeg vil gerne begrænse adgangen til bestemte apps, når brugerne er på vores netværk."

Appbegrænsninger for Google Workspace

Ved hjælp af **Kontekstbevidst adgangskontrol** kan du oprette granulerede politikker for adgangskontrol for appsene **Google Workspace og tredjeparten SAML** (Security Assertion Markup Language) baseret på attributter som f.eks. brugeridentitet, lokation, enhedens sikkerhedsstatus og IP-adresse. Du kan endda begrænse adgangen til apps uden for netværket.

- Du kan anvende politikker for kontekstbevidst adgangskontrol på kernetjenesterne i Google Workspace for Education
- Du kan f.eks. begrænse adgangen til Workspace-apps fra enheder, der er udstedt af uddannelsesinstitutionen, eller begrænse adgangen til Drev til krypterede brugerlagerenheder.

Detaljeret vejledning

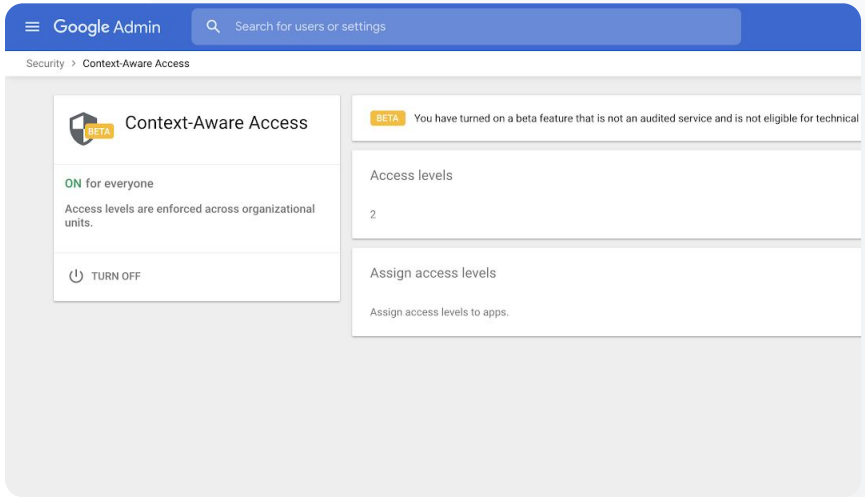
Relevant dokumentation i Hjælp

- Oversigt over kontekstbevidst adgangskontrol
- Tildel niveauer for kontekstbevidst adgangskontrol til apps

Vejledning: Begræns brugen af Google Workspace-appen

Sådan bruger du kontekstbevidst adgangskontrol

- Log ind på **Administrationskonsol**
- Vælg **Sikkerhed** > **Kontekstbevidst adgangskontrol** > **Tildel**
- Vælg **Tildel adgangsniveauer** for at se din liste over apps
- Vælg en **organisationsenhed eller konfigurationsgruppe** for at sortere listen
- Vælg **Tildel** ud for den app, du vil justere
- Vælg et eller flere adgangsniveauer
- Opret flere niveauer, hvis brugerne skal opfylde mere end én betingelse
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Oversigt over kontekstbevidst adgangskontrol
- Tildel niveauer for kontekstbevidst adgangskontrol til apps

Administrer lagerplads for dit domæne

Jeg vil implementere en ny lageradministratorplan på mit domæne."

Uddannelsesinstitutioner med Google Workspace for Education har som udgangspunkt 100 TB fælles lagerplads, hvilket er nok lagerplads til over ca. 100 millioner dokumenter, 8 millioner præsentationer eller 400.000 timers video. **Administrer fælles Drev-lagerplads** for at sikre, at din uddannelsesinstitution bruger lagerpladsen effektivt.

Brug administratorværktøjer, rapporter og logfiler til at:

- Se, hvor meget lagerplads du bruger
- Angive lagergrænser
- Identificere konti, der bruger uforholdsmæssigt meget lagerplads

Teaching and Learning Upgrade og Education Plus tilbyder yderligere lagerkapacitet oven i den medfølgende lagerplads

- Tilføj 100 GB til den fælles lagerplads pr. licens med Teaching and Learning Upgrade
- Tilføj 20 GB til den fælles lagerplads pr. licens med Education Plus

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Vejledning til lagerplads for administratorer
- Forstå tilgængeligheden af lagerplads og forbrug
- Frigør plads eller få mere lagerplads
- Angive lagergrænser

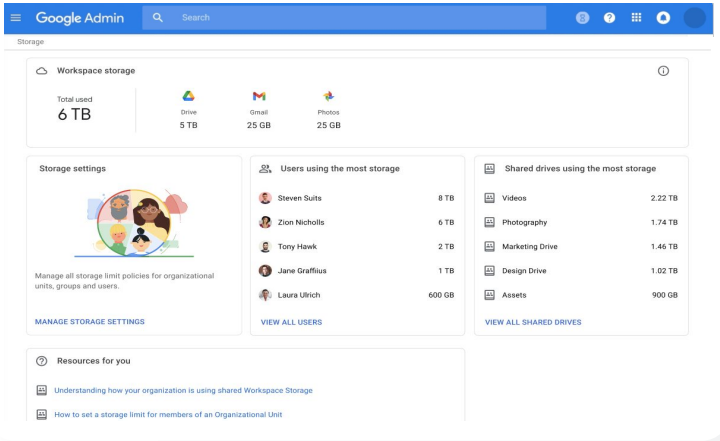
Vejledning: Administrer lagerplads for dit domæne

Identificer lagerforbrug efter bruger

- Log ind på **Administrationskonsol** > Gå til **Menu** > **Lagerplads**
- Se lagerforbrug efter organisation og bruger

Angive lagergrænser

- I **Administrationskonsol** > **Menu** > **Lagerplads**
- I **indstillingerne for lagerplads** skal du klikke på **Administrer**
- Klik på **Grænse for brugeres lagerplads** > vælg den enhed, du vil angive en grænse for:
  - Organisationsenhed: Klik på **organisationsenhed**
  - Gruppe: Klik på **Grupper** > Klik på **søgefeltet** > angiv **gruppens navn** > klik på **gruppen**
- Vælg **Aktivér**, og **angiv lagerplads**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Vejledning til lagerplads for administratorer
- Forstå tilgængeligheden af lagerplads og forbrug
- Frigør plads eller få mere lagerplads
- Angive lagergrænser

"Mine data vedrørende elever, undervisere og personale skal blive i EU på grund af lovgivningen."

Datalovgivning

Som administrator kan du vælge at opbevare data på en bestemt geografisk lokation enten i USA eller Storbritannien/Europa ved hjælp af en **politik for dataregion**.

- Brugere af Education Plus og Education Standard kan vælge én dataregion for nogle af brugerne eller forskellige dataregioner for bestemte afdelinger og se fremskridt for flytning af dataregioner.
- Placer brugere i en organisationsenhed for at konfigurere indstillingen efter afdeling, eller placer dem i en konfigurationsgruppe for at konfigurere indstillingen for brugere på tværs af eller internt i afdelinger.
- Brugere, som ikke er tildelt en licens til Education Standard eller Education Plus, er ikke omfattet af politikker for dataregioner.

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Vælg et geografisk område for dine data

"Mine underviseres forskning skal blive i USA på grund af reglerne for tilskud."

Regler for tilskud

Som administrator kan du vælge at opbevare dine underviseres forskning på en bestemt geografisk lokation (USA eller Europa) ved hjælp af en **politik for dataregion**.

- Politikker for dataregion dækker de primære inaktive data (herunder sikkerhedskopier) for de fleste kernetjenester i Google Workspace for Education, som kan ses her
- Overvej fordelene og ulemperne, inden du angiver en politik for dataregion, da brugere uden for den region, hvor deres data opbevares, i nogle tilfælde kan opleve længere forsinkelse.

Detaljeret vejledning

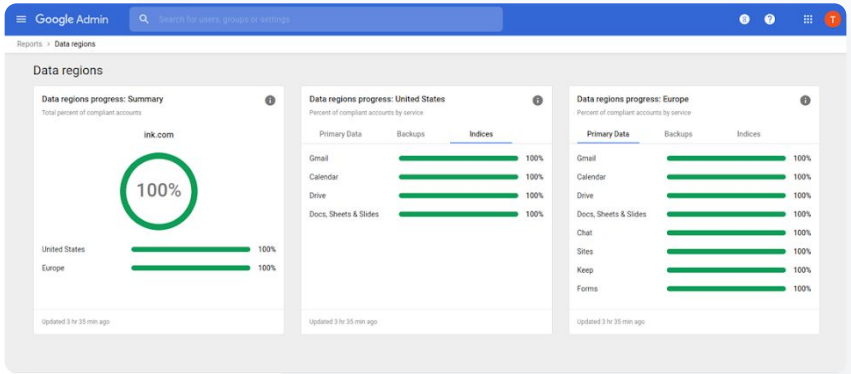
Relevant dokumentation i Hjælp

- Vælg et geografisk område for dine data

Vejledning: Datalovgivning

Sådan definerer du dataregioner

- Log ind på **Administrationskonsol**
  - Bemærk! Du skal være logget ind som superadministrator
- Klik på **Virksomhedsprofil** > **Vis mere** > **Dataregioner**
- Vælg den **organisationsenhed eller konfigurationsgruppe**, du vil begrænse til en region, eller vælg hele kolonnen for at medtage alle enheder og grupper
- Vælg en region. Valgmulighederne er **Ingen præference, USA, Europa**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Vælg et geografisk område for dine data

> Jeg har brug for en metode til at administrere og overføre politikker til alle typer enheder i hele mit distrikt – iOS, Windows 10 osv. og ikke kun Chromebooks – især hvis en af dem er kompromitteret."

Administrer slutpunktsenheder

Du kan bruge **administration af slutpunkter for virksomheder** til at få større kontrol over din organisations data via mobilenheder. Begræns funktionerne på mobilenheder, kræv enhedskryptering, administrer apps på Android-enheder eller iPhones og iPads, og ryd data på en enhed.

- Du kan godkende, blokere, fjerne blokeringen fra eller slette enheder via Administrationskonsol.
- Hvis en bruger mister en enhed eller udmeldes af skolen, kan du rydde en brugers konto, vedkommendes profil eller alle data fra den pågældende administrerede modulenhed. Disse data vil stadig være tilgængelige via en computer eller webbrowser.

Detaljeret vejledning

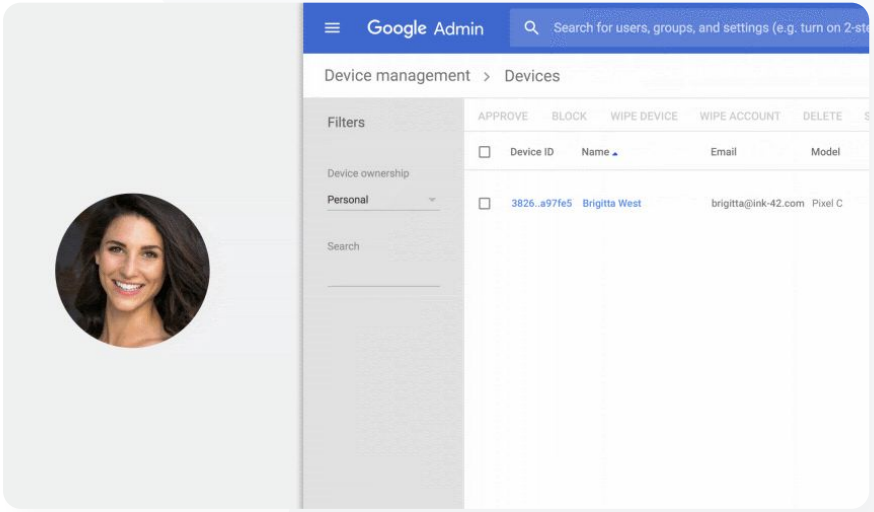
Relevant dokumentation i Hjælp

- Administrer enheder med Google-slutpunktsadministration
- Konfigurer avanceret mobiladministration

Vejledning: Administrer slutpunktsenheder

Sådan bruger du avanceret mobiladministration

- Log ind på **Administrationskonsol**
- Gå til **Administrationskonsol** > **Enheder**
- Til venstre skal du klikke på **Indstillinger** > **Universelle indstillinger**
- Klik på **Generelt** > **Mobiladministration**
- Hvis indstillingerne skal gælde for alle, skal du sørge for, at den øverste organisationsenhed er valgt. Hvis ikke, skal du vælge en underordnet organisationsenhed.
- Vælg **Avanceret**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Administrer enheder med Google-slutpunktsadministration
- Konfigurer avanceret mobiladministration

"Nogle af mine undervisere bruger Windows 10-enheder. Hvordan kan jeg administrere alle uddannelsesinstitutionens enheder på samme sted?"

Administrer Microsoft Windows-enheder

Administrer og beskyt din uddannelsesinstitutions Windows 10-enheder via Administrationskonsol, ligesom du gør for Android-, iOS-, Chrome- og Jamboard-enheder.

- Aktivér Single Sign-On, så brugerne nemmere kan få adgang til Google Workspace på deres Windows 10-enheder
- Sørg for, at enheder, der bruges til at få adgang til Google Workspace, er opdaterede, sikre og overholder standarderne ved at administrere enheder i Administrationskonsol
- Slet en enhed, send enhedskonfigurationsopdateringer og mere til Windows 10-enheder fra skyen

Detaljeret vejledning

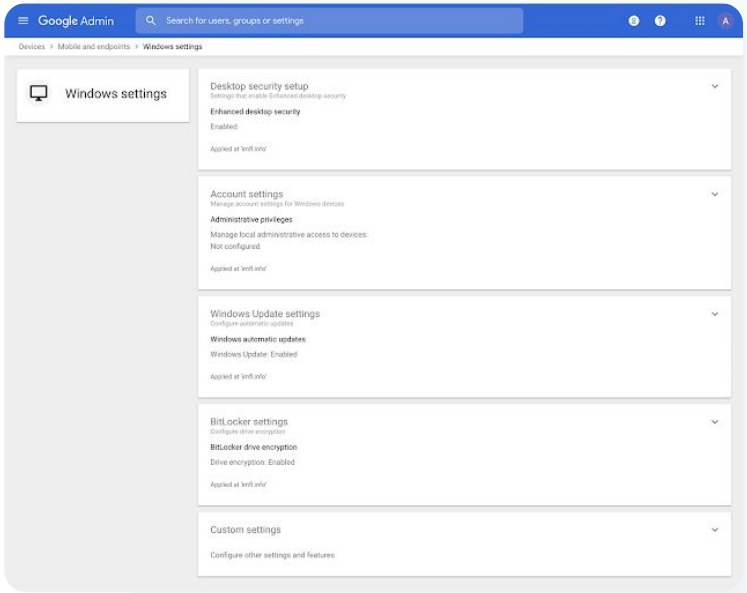
Relevant dokumentation i Hjælp

- Aktivér Administration af Windows-enheder
- Tilmeld en enhed til Windows-enhedsadministration

Vejledning: Administrer Microsoft Windows-enheder

Aktivér Administration af Windows-enheder

- I **Administrationskonsol** skal du gå til **Menu** > **Enheder** > **Mobil og slutpunkter** > **Indstillinger** > **Windows-indstillinger**
- Vælg **Konfiguration af Windows-administration**
- Hvis indstillingen skal gælde for alle, skal du sørge for, at den øverste organisationsenhed er valgt
- Ud for **Aktivering af Windows-enhed** skal du vælge **Aktiveret**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Aktivér Administration af Windows-enheder
- Tilmeld en enhed til Windows-enhedsadministration

Hvordan konfigurerer jeg Wi-Fi-profiler på mine Windows 10-enheder?"

Tilpassede indstillinger for Windows 10-enheder

Med Googles administration af Windows-enheder kan administratorer tilføje fælles indstillinger til deres flådes enheder.

- Administrer fælles enhedsindstillinger fra Administrationskonsol
- Anvend indstillinger på:
  - Administration af enheder
  - Sikkerhed
  - Hardware og netværk
  - Software
  - Privatliv

Detaljeret vejledning

Relevant dokumentation i Hjælp

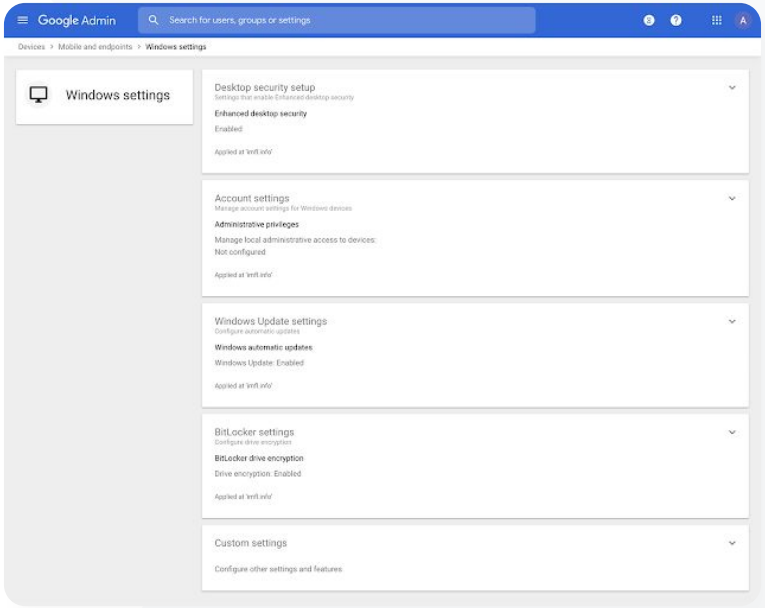
- Fælles tilpassede indstillinger
- Tilføj tilpassede indstillinger

Vejledning: Tilpassede indstillinger for Windows 10-enheder

Tilføj en ny tilpasset indstilling

- I **Administrationskonsol** skal du gå til **Menu** > **Enheder** > **Mobil og slutpunkter** > **Indstillinger** > **Windows-indstillinger**
- Vælg **Tilpassede indstillinger**
- Klik på **Tilføj en tilpasset indstilling** > og udfyld felterne
- Klik på **Næste**
- Vælg den **organisationsenhed**, du vil anvende indstillingen på
- Klik på **Anvend**

Bemærk, at Google ikke yder teknisk support og ikke har ansvaret for produkter eller indstillinger fra tredjeparter.



Relevant dokumentation i Hjælp

- Fælles tilpassede indstillinger
- Tilføj tilpassede indstillinger

"Jeg vil sikre, at Windows 10-enhederne i min flåde modtager de seneste opdateringer."

Automatiser opdateringer til Windows 10-enheder

Angiv, hvordan og hvornår din uddannelsesinstitutions Windows 10-enheder skal modtage sikkerhedsopdateringer og andre vigtige downloads via den automatiske opdateringstjeneste fra Windows.

- Konfigurer notifikationer til at downloade opdateringer fra Windows Update-kontrolpanelet, angiv tidspunkter, hvor der ikke skal genstartes efter opdateringer, og meget mere
- Implementer indstillinger for hele din uddannelsesinstitution eller specifikke organisationsenheder
- Der kan gå op til 24 timer, før ændringerne træder i kraft, men typisk sker det hurtigere

Detaljeret vejledning

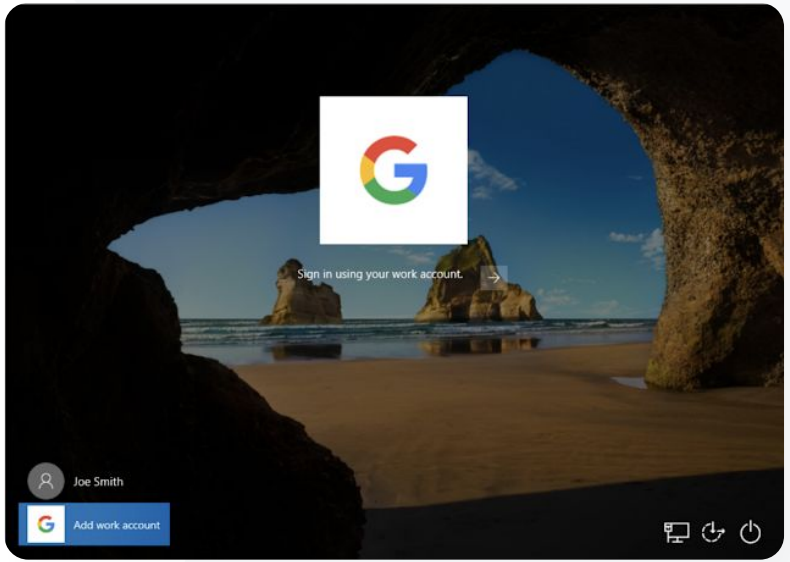
Relevant dokumentation i Hjælp

- Administrer automatiske opdateringer

Vejledning: Automatiser opdateringer til Windows 10-enheder

Konfigurer opdateringer

- I **Administrationskonsol** skal du gå til **Menu** > **Enheder** > **Mobil og slutpunkter** > **Indstillinger** > **Windows-indstillinger**
- Vælg **Indstillinger for Windows Update** > **Aktiveret**
- Ud for **Aktivering af Windows-enhed** skal du vælge **Aktiveret**
- Konfigurer valgmulighederne nedenfor bl.a.:
  - Acceptér opdateringer til Microsoft-apps
  - Adfærd for automatisk opdatering
  - Automatiser opdateringsfrekvens
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Administrer automatiske opdateringer

Jeg ved, at Google har de højeste standarder med hensyn til datakryptering, men jeg vil gerne styre krypteringsnøglerne til vores universitets intellektuelle ejendom og fondsstøttede forskning."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Om kryptering på klientsiden

Brug kryptering på klientsiden

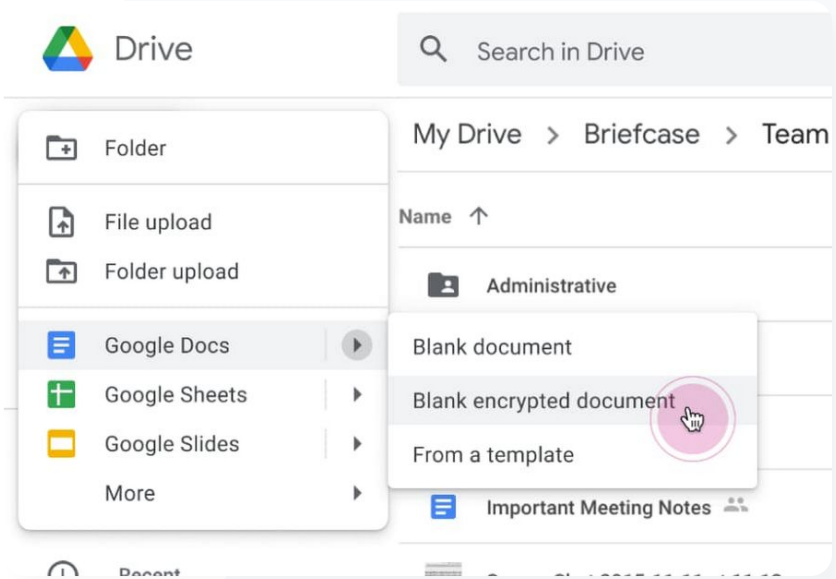
Google Workspace bruger allerede de nyeste kryptografiske standarder til at kryptere alle data under opbevaring og under overførsel mellem deres faciliteter. Med **kryptering på klientsiden** har administratorer direkte kontrol over krypteringsnøglerne og den identitsudbyder, som bliver anvendt til at få adgang til disse nøgler.

- Brug dine egne krypteringsnøgler til at kryptere følsomme oplysninger, som f.eks. din uddannelsesinstitutions intellektuelle ejendom
- Indholdskryptering behandles i din browser, før der overføres eller gemmes data i Googles skybaserede lager
- Vælg, hvilke brugere der kan oprette krypteret indhold på klientsiden, og del det internt eller eksternt

Vejledning: Brug kryptering på klientsiden

Konfigurer kryptering på klientsiden (CSE)

- Konfigurer din nøgletjeneste til kryptering
  - Beskyt dine data med administration af nøgler, og kontrollér funktioner ved at oprette din nøgletjeneste
- Forbind Google Workspace til din eksterne nøgletjeneste
  - Tilføj og administrer nøgletjenester for kryptering på klientsiden ved at inkludere webadressen for nøgletjenester i Administrationskonsol
- Tildel din nøgletjeneste til organisationsenheder eller -grupper
  - Tildel en nøgletjeneste som standard for hele institutionen
- Forbind Google Workspace til din IdP
  - Opret forbindelse til din identitetsudbyder (IdP) for kryptering på klientsiden for at verificere identiteten på brugere, før du tillader dem at kryptere indhold eller få adgang til krypteret indhold
- Aktivér CSE for brugere
  - Aktivér kryptering på klientsiden for at aktivere organisationsenheder eller grupper med brugere, som skal kunne oprette indhold med kryptering på klientsiden

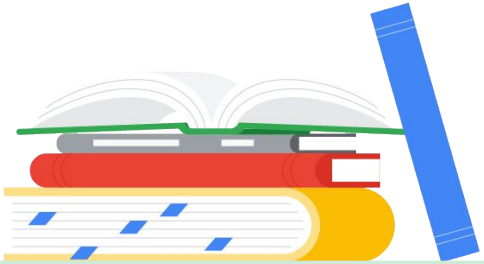


Relevant dokumentation i Hjælp

- Om kryptering på klientsiden

Undervisnings- og læringsmuligheder

Udstyr dine undervisere med yderligere funktioner i dit digitale læringsmiljø med forbedrede holdoplevelser, værktøjer, der underbygger akademisk redelighed, og forbedret videokommunikation.

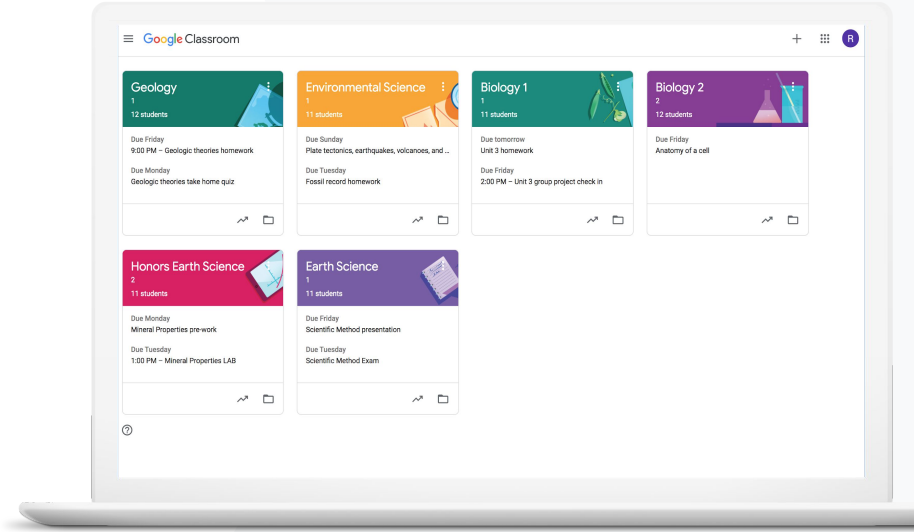


- Google Classroom
- Originalitetsrapporter
- Docs, Sheets og Slides
- Google Meet

Google Classroom

Hvad er det?

Google Classroom er dit centrale sted til undervisning og læring. Betalingsfunktionerne i Classroom samler holdets værktøjer på ét sted. Undervisere får adgang til deres yndlingsværktøjer direkte i Classroom og kan sørge for, at holdlister er synkroniserede med eksterne systemer.



Eksempler på brug

Administrer adgang til Classroom-tilføjelser	Detaljeret vejledning
Integrer engagerende indhold i Classroom	Detaljeret vejledning
Opret hold i stor skala	Detaljeret vejledning

"Jeg ville ønske, at jeg kunne give mine undervisere Single Sign-On-adgang til deres foretrukne uddannelsesteknologiske værktøjer."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Administrer Google Workspace Marketplace-apps
- Brug tilføjelser i Classroom
- Administrer Marketplace-apps på din tilladelsesliste
- Distribuer en Marketplace-app til brugerne
- Classroom-tilføjelser [Getting Started Guide for Admins]

Administrer adgang til Classroom-tilføjelser

Bestem, hvilke læringsapps fra tredjeparter din uddannelsesinstitution skal have adgang til, med en **domænetilladelsesliste**. Gør det muligt for undervisere nemt at installere tilføjelser og inkludere dem i elevopgaver med bare et par klik.

- Opret en tilladelsesliste på hele dit domæne for at bestemme, hvilke tredjepartsapps som undervisere kan installere fra Google Workspace Marketplace.
- Støt læringsudbyttet med supplerende læringsapps. Undervisere kan tildele, gennemgå og give karakterer direkte i Google Classroom.
- Google Workspace Marketplace omfatter Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Arts & Culture, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora, Wordwall og flere.

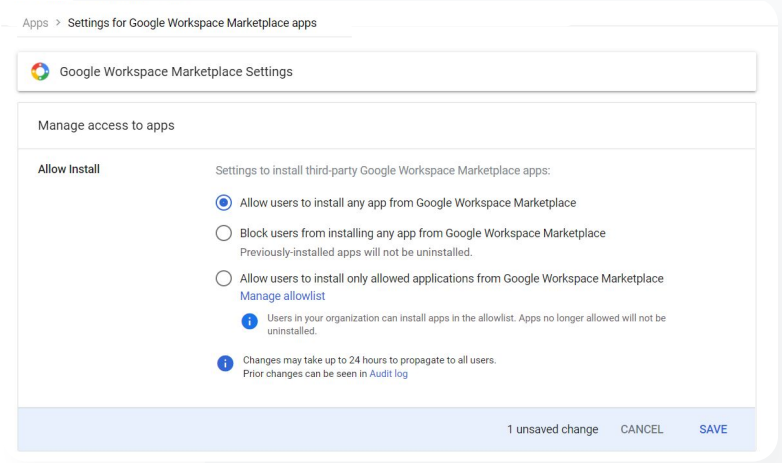
Vejledning: Administrer adgang til Classroom-tilføjelser

Administrer adgang til tilføjelser med en domænetilladelsesliste

- I Administrationskonsol skal du vælge **Menu** > **Google Workspace Marketplace-apps** > **Appliste**
- Vælg **Sæt app på tilladelseslisten**
- Angiv navnet på din ønskede tilføjelse, eller søg efter den
- Klik på **Vælg**, og sørg for, at **Tillad, at brugerne installerer denne app** er valgt
- Klik på **Fortsæt**, og **Udfør**

Giv adgang til tilføjelser til din ønskede tilladelsesliste

- I Administrationskonsol skal du vælge **Menu** > **Google Workspace Marketplace-apps** > **Appliste**
- Vælg den tilføjelse, du vil distribuere
- Under **Brugeradgang** skal du klikke på **Se organisationsenhed og grupper**
- Vælg mellem **tilgængelig for alle**, eller juster adgangen til **udvalgte grupper** eller **organisationsenheder**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Administrer Google Workspace Marketplace-apps
- Brug tilføjelser i Classroom
- Administrer Marketplace-apps på din tilladelsesliste
- Distribuer en Marketplace-app til brugerne
- Classroom-tilføjelser [Getting Started Guide for Admins]

> Jeg vil gerne tildele og bedømme et lærerigt Kahoot!-spil til mine elever uden at forlade Google Classroom."

Integrer engagerende indhold i Classroom

Med **Classroom-tilføjelser** kan undervisere dele engagerende aktiviteter og indhold med deres hold ved at vedhæfte tilføjelser til opgaver, spørgsmål, materiale eller meddelelser i Classroom.

- Giv undervisere og elever mulighed for at bruge deres yndlingsværktøjer som bl.a. Kahoot!, Nearpod og Pear Deck uden at forlade Classroom
- Med tilføjelser slipper eleverne for at holde styr på flere adgangskoder eller navigere på eksterne websites
- Giv karakterer og gennemgå elevopgaver fra tilføjelser, direkte i Classroom

Detaljeret vejledning

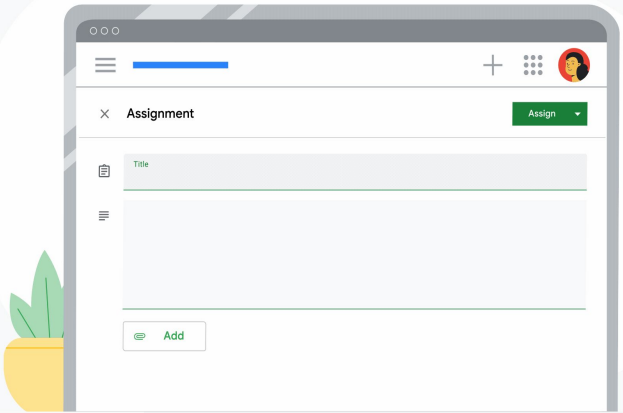
Relevant dokumentation i Hjælp

- Brug tilføjelser i Classroom
- Classroom-tilføjelser [Getting Started Guide for Teachers]

Vejledning: Integrer engagerende indhold i Classroom

Sådan vedhæfter du tilføjelser til opgaver, tests eller spørgsmål

- Log ind på din Classroom-konto på **classroom.google.com**
- Vælg det relevante hold på listen, og vælg **Ressourcer**
- Vælg **Opret** > vælg, hvad du vil oprette
- Angiv en titel, og udfyld en vejledning
- Under **Tilføjelser** skal du vælge den tilføjelse, du vil bruge
- Vælg **Tildel**



Sådan vedhæfter du tilføjelser til en meddelelse

- Under dit hold skal du vælge siden **Stream** og dernæst **Send en meddelelse til dit hold**
- Skriv din meddelelse
- Under **Tilføjelser** skal du vælge den tilføjelse, du vil bruge
- Vælg **Opslag**

Relevant dokumentation i Hjælp

- Brug tilføjelser i Classroom
- Classroom-tilføjelser [Getting Started Guide for Teachers]

Jeg har brug for at automatisere konfigurationen af hold og administrere holdlister i Google Classroom."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Kom godt i gang med import af holdlister fra et elevadministrationssystem
- Konfigurer import af holdlister fra et elevadministrationssystem via Clever

Opret hold i stor skala

Importering af holdlister fra et elevadministrationssystem gør det muligt at oprette hold automatisk og holder dine holdlister synkroniserede med skolens elevadministrationssystem (SIS) med Clever.

- Tilgængeligt for grundskoler og ungdomsuddannelser i USA og Canada via Education Plus
- Administratorer kan importere holdlister fra dit elevadministrationssystem til Google Classroom for automatisk at konfigurere hold
- Automatiser og administrer holdlister i Google Classroom nemt

Vejledning: Opret hold i stor skala

Sådan konfigurerer du import af holdlister fra et elevadministrationssystem

- Konfigurer synkronisering af holdlister i Google Classroom i Clever
- Din distriktsadministrator i Clever og din superadministrator i Google Workspace kan følge den trinvise vejledning i Clever

Hvis dit distrikt ikke har en Clever-konto:

- Opret en Clever-konto

Hvis dit distrikt har en Clever-konto:

- Anmod om import af holdlister i dit Clever-kontrolpanel

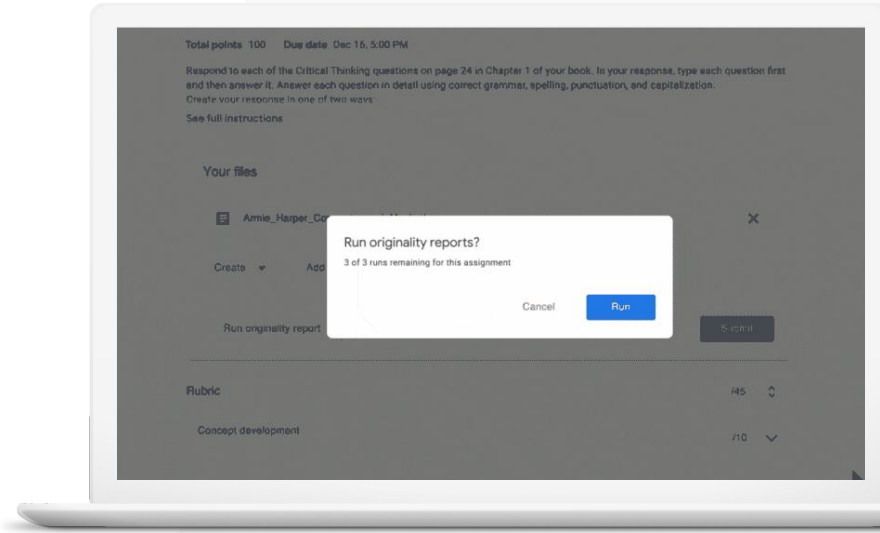
Relevant dokumentation i Hjælp

- Konfigurer import af holdlister fra et elevadministrationssystem via Clever

Originalitetsrapporter

Hvad er det?

Originalitetsrapporter gør det muligt for undervisere og elever at tjekke originaliteten af opgaver ved hjælp af Google Søgning, som sammenligner elevopgaver med flere hundrede milliarder websider og over 40 millioner bøger. De betalte funktioner i originalitetsrapporter giver ubegrænset adgang, så undervisere kan scanne elevernes indsendte opgaver i forhold til tidligere skoleopgaver, som ejes af skolen.



Eksempler på brug

Scan for plagiering	Detaljeret vejledning
Tjek originalitet i forhold til tidligere elevopgaver	Detaljeret vejledning
Gør registrering af plagiering til en mulighed for at lære	Detaljeret vejledning

"Jeg vil gerne tjekke mine elevers opgaver for plagiering og forkerte henvisninger."

Scan for plagiering

Undervisere kan tjekke originaliteten af elevernes opgaver ved hjælp af **originalitetsrapporter**. Rapporten linker til registrerede kilder og markerer tekst, der ikke er citeret.

- Kør originalitetsrapporter i forhold til Docs, Slides og Microsoft Word-dokumenter.
- Undervisere med Teaching and Learning Upgrade eller Education Plus får:
  - Ubegrænset adgang til originalitetsrapporter
  - Sammenlign indbyrdes matches mellem elever ved hjælp af et skoleejet lager med tidligere indsendte opgaver.

Du ejer altid dine egne data – det er vores ansvar at beskytte dem.

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Aktivér originalitetsrapporter
- Originalitetsrapporter og privatliv

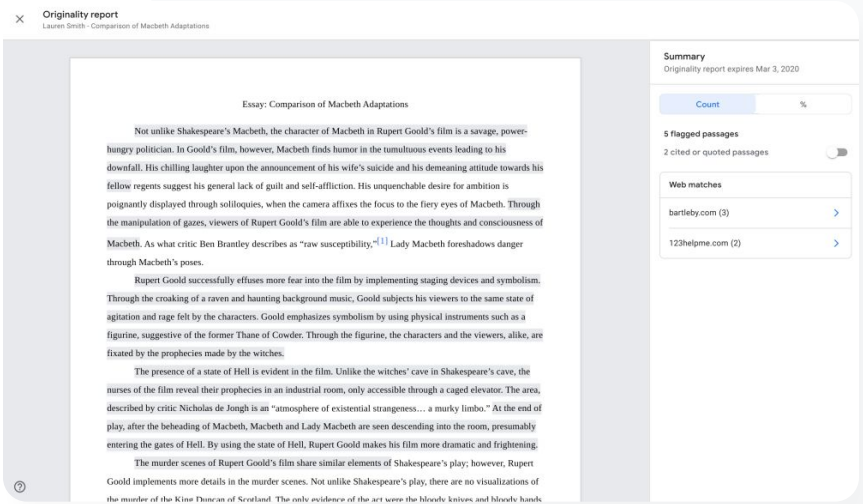
Vejledning: Scan for plagiering

Aktivér originalitetsrapporter i forbindelse med opgaver i Classroom

- Log ind på din Classroom-konto på **classroom.google.com**
- Vælg det relevante hold på listen, og vælg **Ressourcer**
- Vælg **Opret** > **Opgave**
- Markér afkrydsningsfeltet ud for **originalitetsrapporter** for at aktivere funktionen

Kør originalitetsrapporter på elevopgaver

- Vælg den relevante elevs fil på listen, og klik for at åbne filen i bedømmelsesværktøjet
- Klik på **Tjek originalitet under elevens opgave**



Aktivér originalitetsrapporter for en opgave i dit undervisningssystem

- Log ind på dit **Undervisningssystem**
- Vælg det relevante **kursus**
- Opret en opgave > vælg **Google Opgaver**
- Markér afkrydsningsfeltet **Aktivér originalitetsrapporter**

Relevant dokumentation i Hjælp

- Classroom: Aktivér originalitetsrapporter
- Google Opgaver: Aktivér originalitetsrapporter

Hvordan kan jeg gøre det muligt for undervisere at undersøge elevers opgaver for plagiering ved at sammenligne med tidligere elevopgaver?"

Tjek originalitet i forhold til tidligere elevopgaver

Skolematches i originalitetsrapporter gør det muligt for undervisere at sammenligne elevopgaver med tidligere elevopgaver ved at scanne elevopgaver i forhold til din uddannelsesinstitutions private lager med elevopgaver.

- Sammenlign matches mellem elever i forhold til aktuelle og tidligere elevopgaver for at registrere plagiering med Teaching and Learning Upgrade eller Education Plus
- Elevopgaver kan gemmes sikkert og udfyldes i dit private, skoleejede lager på domænet.

Detaljeret vejledning

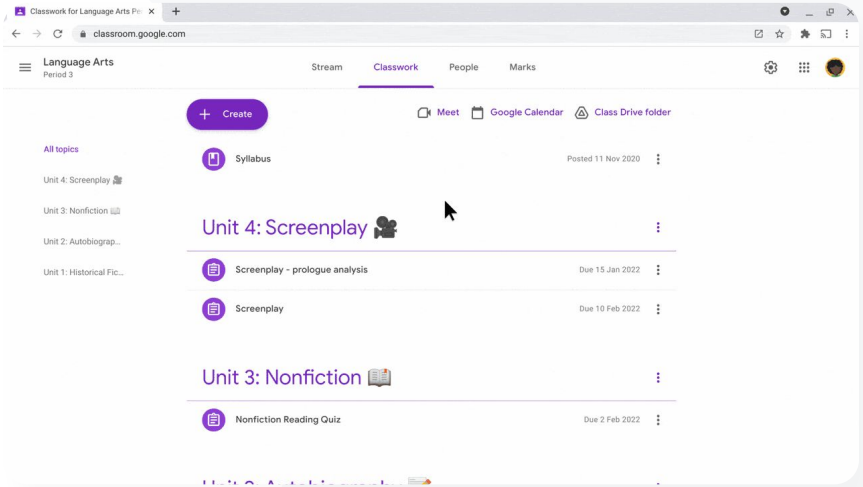
Relevant dokumentation i Hjælp

- Aktivér originalitetsrapporter
- Aktivér skolematches for originalitetsrapporter i Classroom

Vejledning: Tjek originalitet i forhold til tidligere elevopgaver

Sådan aktiverer du skolematches for originalitetsrapporter

- I Administrationskonsol skal du vælge **Menu** > **Apps** > **Yderligere Google-tjenester** > **Classroom**
- Vælg **organisationsenheden med undervisere**
- Klik på **Originalitetsrapporter** > markér afkrydsningsfeltet **Aktivér undersøgelse af originalitetsrapporter for match i et andet dokument fra skolen**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Aktivér skolematches for originalitetsrapporter i Classroom

"Jeg vil gerne give mine elever muligheden for at lære, hvordan de citerer deres kilder korrekt."

Gør registrering af plagiering til en mulighed for at lære

Eleverne kan identificere utilsigtet plagiering og indhold, der ikke er citeret, inden de afleverer deres opgaver. Dette kan de gøre ved hjælp af en **originalitetsrapport**, som kan køres op til tre gange pr. opgave. Originalitetsrapporter sammenligner elevopgaver med forskellige kilder og rapporterer tekst, der ikke er citeret, så eleverne får mulighed for at lære, rette fejl og aflevere deres lektier med selvtillid.

- I Teaching and Learning Upgrade og Education Plus kan underviserne aktivere originalitetsrapporter så mange gange, de vil, mens de kun kan aktivere denne funktion fem gange pr. hold i Education Fundamentals.
- Når opgaven er afleveret, kører Classroom automatisk en rapport, som kun underviseren kan se. Hvis du annullerer afleveringen af en opgave og derefter afleverer den igen, kører Classroom en ny originalitetsrapport til underviseren.

Detaljeret vejledning

Relevant dokumentation i Hjælp

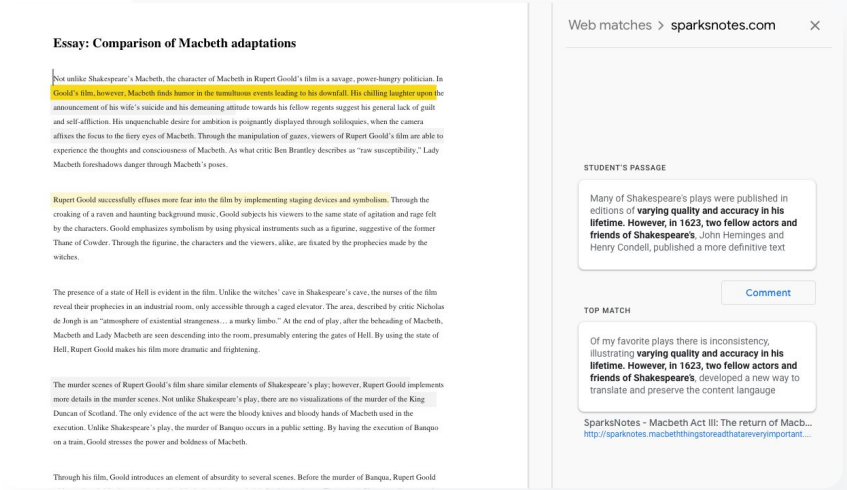
- Kør en originalitetsrapport på din opgave

Vejledning: Gør beskyttelse mod plagiering til en mulighed for at lære

Sådan kører elever originalitetsrapporter i Classroom

- Log ind på din Classroom-konto på classroom.google.com
- Vælg det relevante hold på listen, og vælg **Ressourcer**
- Vælg den relevante opgave på listen, og klik på **Se opgave**
- Under **Dine opgaver** skal du vælge **Upload** eller **oprette en fil**
- Ud for **Originalitetsrapporter** skal du klikke på **Kør**
- Hvis du vil åbne rapporten, skal du klikke på **Se originalitetsrapport** under navnet på opgavefilen
- Hvis du vil revidere opgaven for at omskrive eller citere rapporterede tekststykker korrekt, skal du klikke på **Rediger** nederst

Elever kan køre originalitetsrapporter i deres undervisningssystem ved hjælp af Google Assignments.



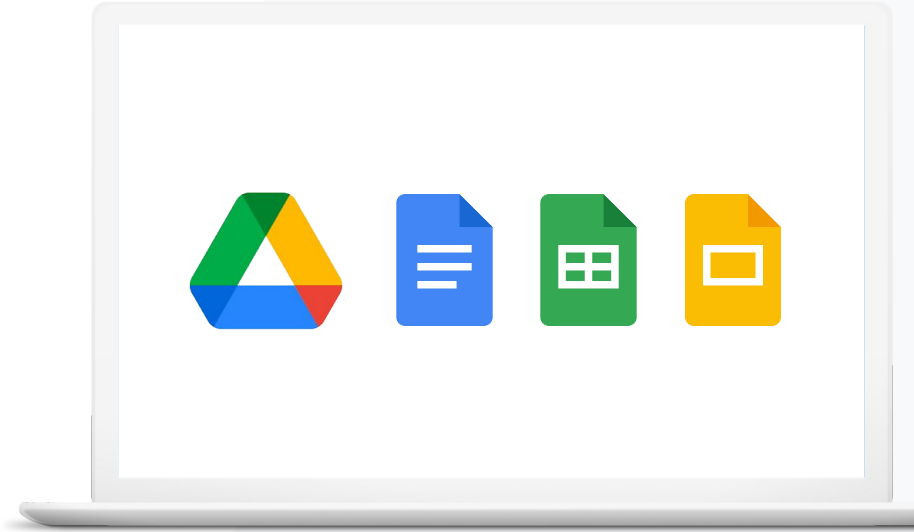
Relevant dokumentation i Hjælp

- Kør en originalitetsrapport i Classroom
- Kør en originalitetsrapport i dit undervisningssystem

Docs, Sheets og Slides

Hvad er det?

Med Docs, Sheets og Slides kan alle på skolen samarbejde om, oprette, gennemse og redigere dokumenter på samme tid i realtid. Betalte funktioner i Education Plus gør det muligt for undervisere og administratorer at foretage en godkendelsesproces af intern dokumentation i hele uddannelsesinstitutionen.



Eksempler på brug

Godkend interne dokumenter — Detaljeret vejledning

Afdelingen for naturfag er ved udvikle et nyt pensum.

Hvordan sørger de for, at deres pensumforslag godkendes af alle institutledere?"

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Administrer godkendelser

Godkend interne dokumenter

Med **Godkendelser** kan hele skolen sende dokumenter i Google Drev via en formel godkendelsesproces.

- Godkendere kan godkende, afvise eller give feedback på dokumenterne direkte i Drev, Docs og andre Google Workspace-apps
- Godkenderne følger et link til dokumentet, hvor de kan gennemgå, skrive kommentarer og afvise eller godkende det
- Du kan administrere en godkendelse af en kontrakt eller nyansættelse, godkende ændringer af et dokument før udgivelse og mere

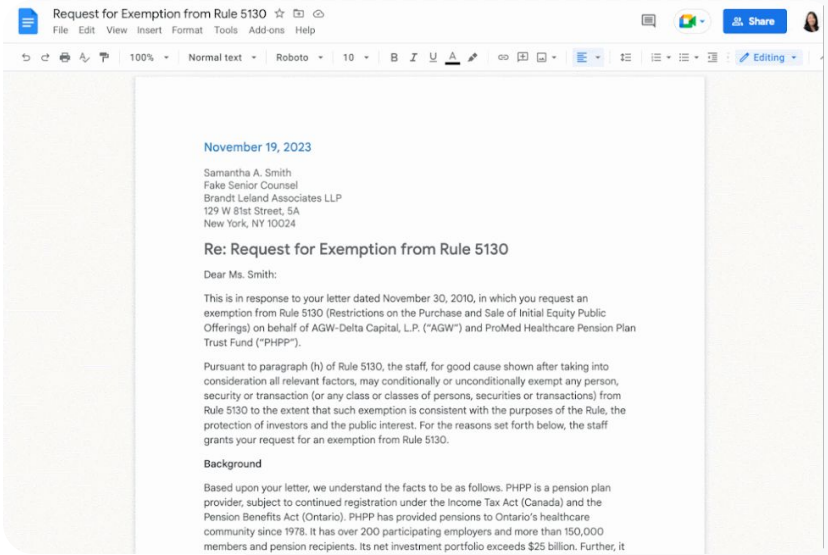
Vejledning: Godkend interne dokumenter

Sådan fungerer det

Administratorer kan styre, hvordan brugere og filer indgår i godkendelsesprocessen.

Sådan administrerer du godkendelser

- Log ind på **Administrationskonsol** > gå til **Menu** > **Apps** > **Google Workspace** > **Drev og Docs**
- Klik på **Godkendelser**
- Vælg en underordnet **organisationsenhed** eller en **konfigurationsgruppe**
- Klik på **Gem**



Relevant dokumentation i Hjælp

- Administrer godkendelser

Google Meet

Hvad er det?

De avancerede funktioner i Google Meet omfatter livestreaming, grupperum, større møder, mødeoptagelser, liveoversatte undertekster og mere.

Eksempler på brug

Optage møder	Detaljeret vejledning	Stil spørgsmål	Detaljeret vejledning
Henvis til det, der blev talt om i timen	Detaljeret vejledning	Indsamling af input	Detaljeret vejledning
Fjern sprogbarrierer	Detaljeret vejledning	Små elevgrupper	Detaljeret vejledning
Send fællessamlinger og skoleevents	Detaljeret vejledning	Registrering af deltagelse	Detaljeret vejledning

"Vores uddannelsesinstitution tilbyder store onlinekurser i faglig udvikling, som vi har brug for at optage til undervisere, som ikke kan deltage."

Optage møder

Med Teaching and Learning Upgrade og Education Plus kan undervisere optage lektioner, fakultetsmøder, faglige udviklingskurser og mere. Møderne gemmes automatisk i Drev.

- Optagelserne gemmes i mødearrangørens Drev. Før du optager, skal du sørge for, at der er nok plads på dit Drev
- Det anbefales, at it-administratorer kun aktiverer optagelse for undervisere og andet personale

Detaljeret vejledning

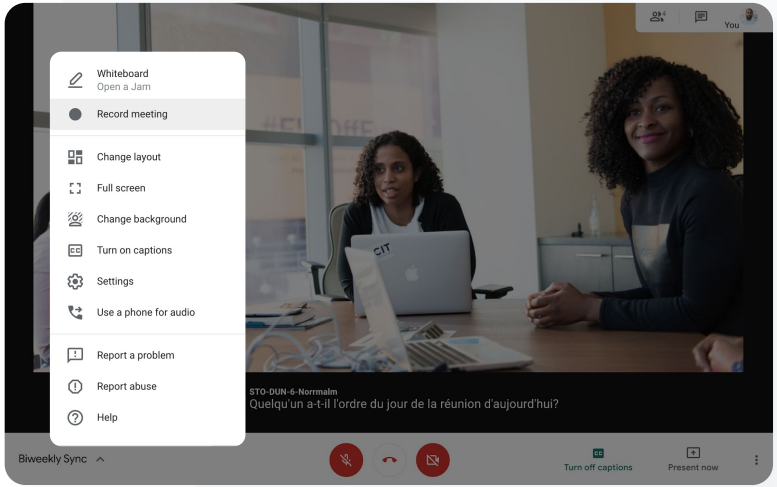
Relevant dokumentation i Hjælp

- Optag et videomøde

Vejledning: Optage møder

Sådan starter du en optagelse

- Start eller deltag i et møde i **Google Meet**
- Klik på **Aktiviteter** > **Optagelse**
- Vælg **Start optagelse**
- I vinduet, der åbnes, skal du klikke på **Start**
- Der vises en rød prik øverst til højre på skærmen for at angive, at et møde optages
- En videofil af mødet gemmes automatisk i dit Drev



Relevant dokumentation i Hjælp

- Optag et videomøde

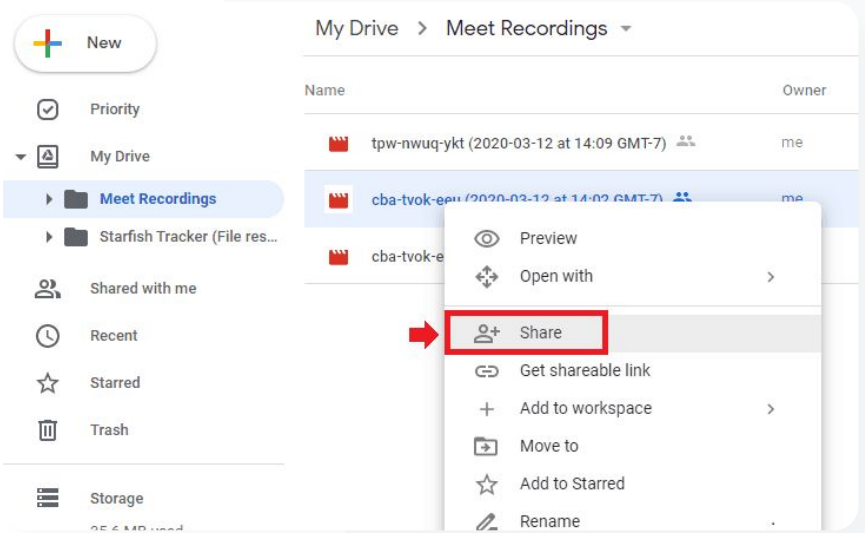
Vejledning: Se og del optagelser

Sådan starter du en optagelse

- Vælg filen
- Klik på ikonet **Del**
- **Tilføj** godkendte seere

ELLER

- Vælg ikonet **Link**
- **Indsæt** linket i en mail eller chatbesked



Sådan downloader du en optagelse

- Vælg filen
- Klik på ikonet **Mere** > Download
- **Dobbeltklik** på filen, der kan downloades, for at afspille den

Sådan afspiller du optagelsen fra Drev

- Dobbeltklik på optagelsesfilen i Drev for at afspille den. "Behandlingen er stadig i gang" vises, indtil filen er klar til visning online
- Du kan føje en optagelse til Drev ved at vælge filen og klikke på **Føj til Mit drev**

Relevant dokumentation i Hjælp

- Optag et videomøde

"Hvordan transskriberer jeg virtuel undervisning, så eleverne kan gennemgå begreber senere?"

Henvis til det, der blev talt om i timen

Med mødetransskriptioner kan undervisere automatisk fastholde deres lektion og diskussionen på holdet, hvilket gør det lettere for elever at genbesøge begreber. Transskriptioner registrerer mødedeltagelse og viser, hvem der sagde hvad på et møde.

- Tilgængelig på engelsk for brugere af Google Meet på en stationær eller bærbar computer.
- Administratorer kan aktivere transskription for hele skolen.
- Transskriptioner gemmes automatisk på mødeværtens Drev.
- Når mødetransskriptioner er aktiveret, vises ikonet Transskriptioner øverst til venstre til alle i mødet.
- Transskriptioner indeholder de talte ord fra et møde. Hvis du gerne vil have en transskription af chatbeskeder, skal du optage dit møde.

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Brug transskription med Google Meet
- Slå transskription til eller fra

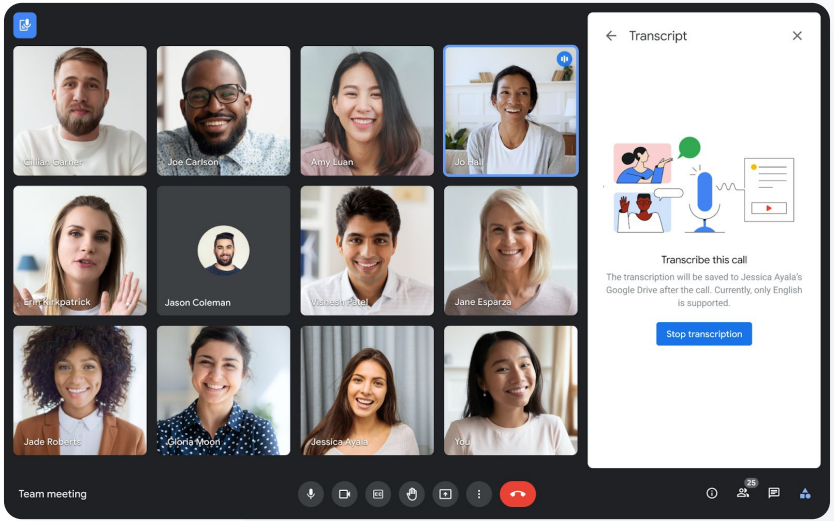
Vejledning: Henvis til det, der blev talt om i timen

Sådan aktiverer du transskription i Google Meet

- Nederst til højre i et møde skal du vælge ikonet **Aktiviteter**
- Klik på **Transskriptioner** > **Start transskription** > **Start**

Sådan stopper du transskriptioner i Google Meet

- Vælg **ikonet Aktiviteter** > **Transskriptioner** > **Stop transskription** > **Stop**



Relevant dokumentation i Hjælp

- Brug transskription med Google Meet
- Slå transskription til eller fra

"Vi afholder forældremøder virtuelt, men nogle gange taler vi ikke alle det samme sprog.

Hvordan gør jeg møder inkluderende og overvinder sprogbarrierer?"

Fjern sprogbarrierer

Oversatte undertekster gør møder mere inkluderende ved at fjerne sproglige barrierer. Når mødedeltagere bruger indhold på deres foretrukne sprog, hjælper det med at give alle lige adgang til informationsdeling, læring og samarbejde.

- Undervisere kan interagere med elever, forældre og interessenter, som taler et andet sprog
- Brug oversatte undertekster til at oversætte engelsk til eller fra fransk, tysk, portugisisk eller spansk
- Eller oversæt engelsk til japansk, mandarin eller svensk

Detaljeret vejledning

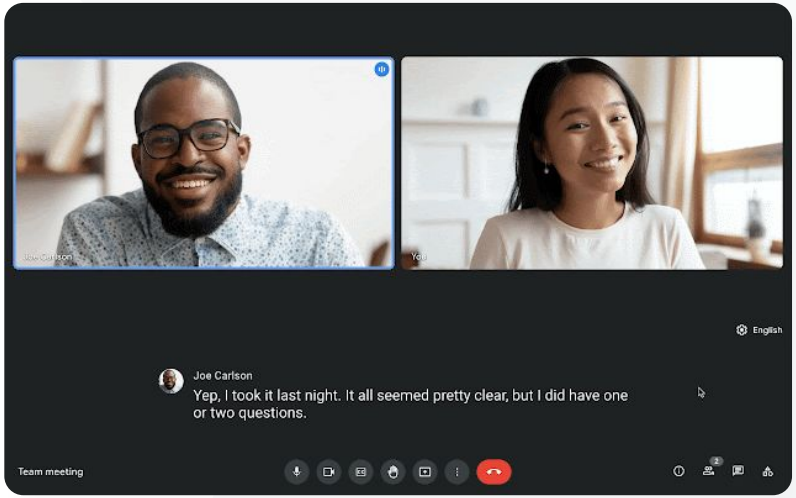
Relevant dokumentation i Hjælp

- Brug oversatte undertekster i Google Meet

Vejledning: Fjern sprogbarrierer

Sådan aktiverer du oversatte undertekster

- Når du er i et møde, skal du nederst på skærmen klikke på **Flere valgmuligheder** > **Indstillinger** > **Undertekster**
- Slå **Undertekster til**
- Vælg **Mødesprog**
- Aktivér Oversatte undertekster.
- Vælg det **sprog, der skal oversættes til**



Relevant dokumentation i Hjælp

- Brug oversatte undertekster i Google Meet

"Vi har brug for at kunne livestreame vores personale- og lærermøder til en bred gruppe af andre interessenter og forældre."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Slå livestreaming til eller fra for Meet
- Livestream et videomøde

Send fællessamlinger, skolebegivenheder og møder

Livestream til op til 10.000 brugere med Teaching and Learning Upgrade og til op til 100.000 brugere med Education Plus. Deltagerne kan oprette forbindelse ved at vælge linket til livestreaming, som arrangøren har angivet i en mail eller invitation i Kalender.

- Afgør, hvor bredt din livestream skal deles. Vælg, om streamen skal:
  - Være synlig kun for brugere i din organisation (på domænet)
  - Deles med andre pålidelige Google Workspace-domæner
  - Kunne ses med YouTube
- Det anbefales, at it-administratorer kun aktiverer livestreaming for undervisere og andet personale
- Hvis brugerne går glip af livestreamen, kan de få adgang til optagelsen, når mødet er afsluttet
- Tilføj undertekster, afstemninger og Spørgsmål og svar til en livestream for at øge inklusionen og engagementet

Vejledning: Send fællessamlinger, skolebegivenheder og møder

Sådan opretter du en livestreamingbegivenhed

- Åbn **Google Kalender**
- Vælg **Opret** > **Flere valgmuligheder**
- Tilføj oplysninger om begivenheden, f.eks. dato, klokkeslæt og beskrivelse
- Tilføj deltagere, som kan deltage fuldt ud i videomødet, hvilket betyder, at de kan ses, høres og kan præsentere
- Klik på **Tilføj videomøde** > **Meet**
- Ud for Deltag via Meet skal du vælge **menupilen** og derefter **Tilføj livestream**
- Hvis du vil invitere så mange enkeltpersoner, som din betalingsudgave tillader, skal du klikke på **Kopiér** og derefter dele webadressen til livestreamen
- Vælg **Gem**
- Streamingen starter ikke automatisk. Når mødet er i gang, skal du vælge **Mere** > **Start streaming**

Relevant dokumentation i Hjælp

- Slå livestreaming til eller fra for Meet
- Livestream et videomøde

"Jeg vil gerne have mulighed for hurtigt at stille spørgsmål, måle, hvor meget eleverne har lært, og interagere med holdet for at holde dem engageret."

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Stil spørgsmål til deltagere i Google Meet

Stil spørgsmål

Brug funktionen **Spørgsmål og svar** i Google Meet som hjælp til at holde eleverne engageret og gøre undervisningen mere interaktiv. Underviserne får en detaljeret rapport over alle spørgsmålene og svarene, når den virtuelle lektion er slut.

- Moderatorer kan stille så mange spørgsmål som nødvendigt. De kan filtrere eller sortere spørgsmål, markere dem som besvaret og skjule eller prioritere spørgsmål.
- Efter hvert møde, hvor spørgsmål er aktiveret, sendes der automatisk en spørgsmålsrapport via mail til moderatoren.

Vejledning: Stil spørgsmål

Stil et spørgsmål

- Under et møde skal du vælge **ikonet Aktiviteter** øverst til højre > **Spørgsmål**. (Du aktiverer Spørgsmål og svar ved at vælge **Aktivér Spørgsmål og svar**)
- Du kan stille et spørgsmål ved at klikke på **Stil et spørgsmål** nederst til højre
- **Skriv dine spørgsmål** > vælg **Send**

Se spørgsmålsrapporten

- Når mødet er slut, modtager moderatorerne en **mail med en spørgsmålsrapport**
- Åbn mailen > klik på den **vedhæftede rapport**

Relevant dokumentation i Hjælp

- Stil spørgsmål til deltagere i Google Meet

"Jeg har brug for en nem løsning til at samle input fra både elever og andre undervisere, mens jeg underviser eller holder møde med personalet."

Indsamling af input

Den bruger, som har planlagt eller starter et virtuelt møde, kan oprette en **afstemning** for deltagerne i et møde. Denne funktion hjælper med at samle oplysninger fra alle eleverne eller deltagerne i et møde på en hurtig og engagerende måde.

- Moderatorer kan gemme en afstemning, som skal slås op på et senere tidspunkt under et møde. Den gemmes i sektionen Afstemninger i et virtuelt møde.
- Efter mødet sendes der automatisk en rapport med resultatet af afstemningen via mail til moderatoren.

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Afhold afstemninger i Google Meet

Vejledning: Indsaml input

Opret en afstemning

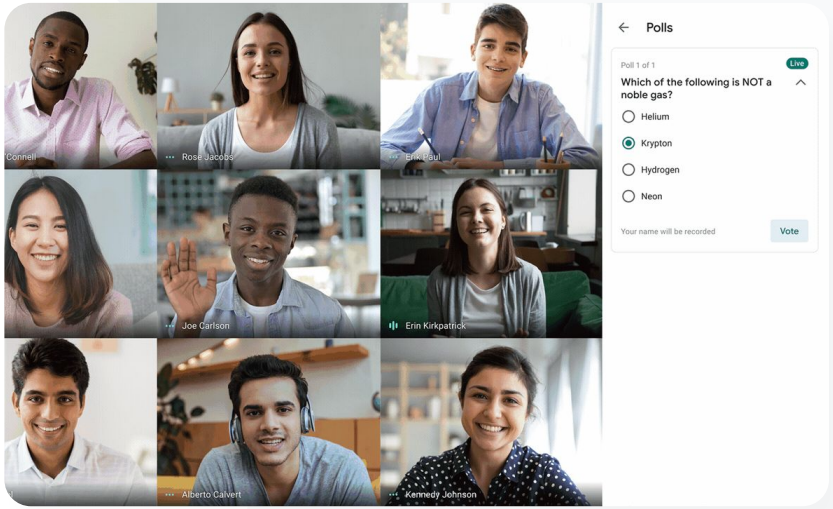
- Øverst til højre i et møde skal du vælge **ikonet Aktiviteter** > **Afstemning**
- Vælg **Start en afstemning**
- Angiv et spørgsmål
- Vælg **Start** eller **Gem**

Moderer en afstemning

- Øverst til højre i et møde skal du vælge **ikonet Aktiviteter** > **Afstemning**
- Hvis du vil give deltagerne mulighed for at se resultatet af en afstemning i realtid, skal du slå kontakten **til** ud for **Vis resultaterne til alle deltagere**
- Du kan lukke en afstemning og forhindre, at der bliver afgivet stemmer, ved at klikke på **Luk afstemningen**
- Hvis du vil slette en afstemning permanent, skal du vælge **ikonet Slet**

Se en rapport over afstemninger

- Når mødet er slut, modtager moderatorerne en **mail med en rapport**
- Åbn mailen > vælg den **vedhæftede rapport**



Relevant dokumentation i Hjælp

- Afhold afstemninger i Google Meet

“

Nogle gange følger eleverne undervisningen hjemmefra. Når vi arbejder i små grupper, har jeg brug for en måde, hvorpå jeg nemt kan oprette grupperum baseret på foruddefinerede grupper".

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Brug grupperum i Google Meet:

Små elevgrupper

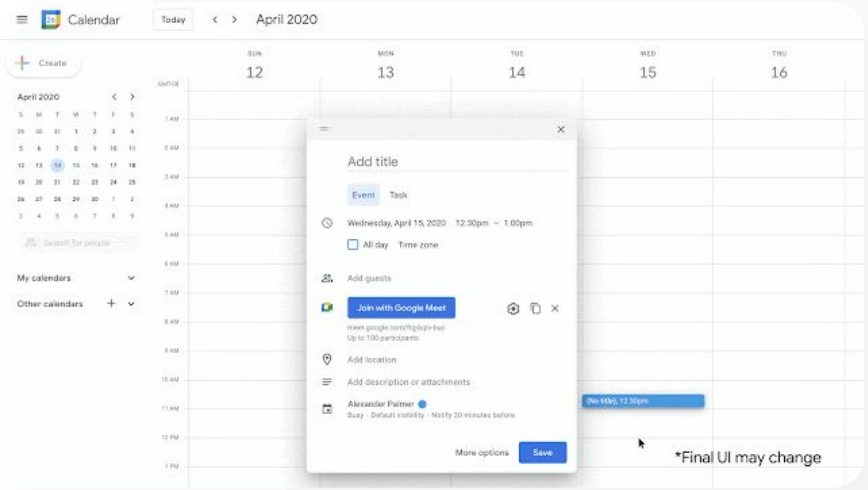
Undervisere kan bruge grupperum til at opdele eleverne i mindre grupper under virtuel, **hybrid eller personlig undervisning**. Grupperum kan kun startes af moderatorer under et videoopkald på en computer.

- Grupperum kan oprettes på forhånd, når du opretter en begivenhed, eller mens mødet er i gang
- Opret op til 100 grupperum pr. virtuelt møde
- Underviseren kan nemt gå fra det ene grupperum til det andet for at hjælpe grupperne efter behov
- Administratorer kan sikre, at kun undervisere eller personale kan oprette grupperum

Vejledning: Opret små elevgrupper

Opret grupperum forud for mødet

- Opret en ny begivenhed i Google Kalender
- Klik på **Tilføj Google Meet-videomøde**
- Tilføj deltagere > Vælg **Skift mødeindstillinger**
- Klik på **Grupperum**
- Vælg antallet af grupperum, og vælg en af følgende muligheder:
  - Træk deltagerne til forskellige rum
  - Angiv navne direkte i et rum
  - Klik på **Bland** for at blande grupperne
- Klik på **Gem**



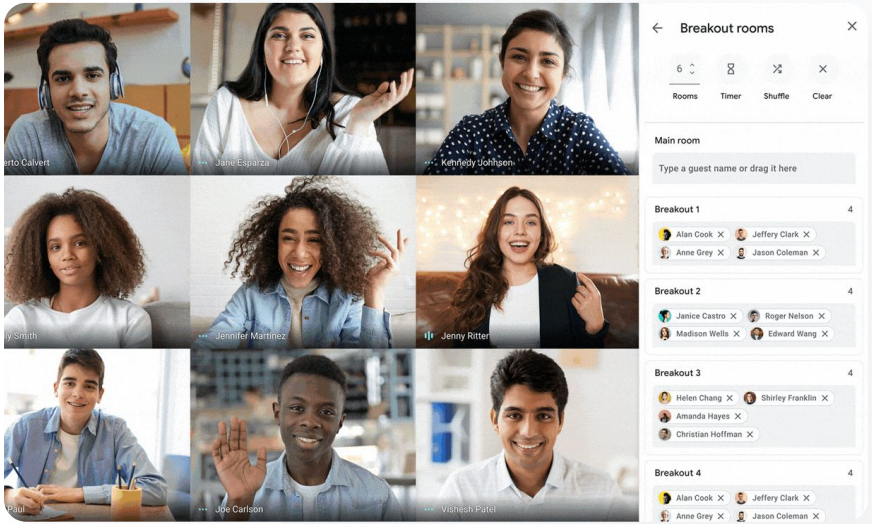
Relevant dokumentation i Hjælp

- Brug grupperum i Google Meet:

Vejledning: Opret små elevgrupper

Opret grupperum under mødet

- Start et videoopkald
- Øverst til højre skal du vælge **ikonet Aktiviteter** > **Grupperum**
- I panelet Grupperum **kan du vælge, hvor mange grupperum** du har brug for
- Eleverne fordeles derefter i rummene, men moderatorer kan manuelt flytte dem til andre rum, hvis det er nødvendigt
- Klik på **Åbn** rummene nederst til højre



Besvar spørgsmål i forskellige grupperum

- Der vises en notifikation nederst på moderatorens skærm, når deltagerne beder om hjælp. Vælg Deltag for at deltage i den pågældende deltagers grupperum

Relevant dokumentation i Hjælp

- Brug grupperum i Google Meet:

"Vi har problemer med at holde styr på, hvem der deltager i onlinelektioner. Jeg har brug for en nem løsning til at rapportere om deltagelse for lektioner på hele mit domæne."

Registrering af deltagelse

Deltagelsesregistrering leverer en automatisk deltagelsesrapport for alle møder med mindst fem deltagere. Rapporterne viser, hvem der har deltaget i opkaldet, deltagernes mails, og hvor længe de havde forbindelse til den virtuelle lektion.

- Du kan registrere deltagelse under livestreamede begivenheder med livestreamrapporter
- Moderatorer kan aktivere og deaktivere deltagelsesregistrering og livestreamrapporter i et møde eller via kalenderbegivenheden

Detaljeret vejledning

Relevant dokumentation i Hjælp

- Registrer deltagelse i Google Meet

Vejledning: Registrering af deltagelse

Sådan registrerer du deltagelse under et møde

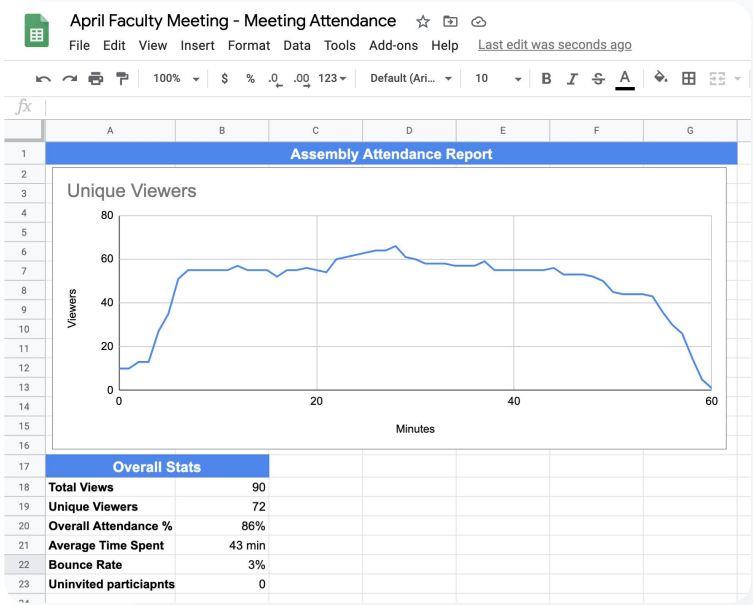
- Start et videoopkald
- Vælg **menuikonet nederst**
- Vælg **ikonet Indstillinger** > **Værtsfunktioner**
- Slå **Deltagelsesregistrering** til eller fra

Sådan registrerer du deltagelse i Kalender

- **Aktivér møder i Google Meet** via en kalenderbegivenhed
- Vælg **ikonet Indstillinger til højre**
- Markér feltet ud for **Deltagelsesregistrering** > klik på **Gem**

Hent deltagelsesrapporten

- Når mødet er slut, modtager moderatoren **en mail med en rapport**
- Åbn mailen > vælg den **vedhæftede rapport**



Relevant dokumentation i Hjælp

- Registrer deltagelse i Google Meet

Tak