Google for Education

40+ måter å bruke Google Workspace for Education på (betalte utgaver)

goo.gle/use-edu-workspace

Slik bruker du denne samlingen

Denne samlingen er et utvalg av populære bruksmønstre som er tilgjengelige hvis du bruker en av de **betalte utgavene av Google Workspace for Education**. Disse verktøyene kan bidra til **bedre datasikkerhet, økt effektivitet for lærere, større engasjement blant elevene, bedre samarbeid for hele skolen** med mer.

Samlingen er organisert etter **funksjon**, etterfulgt av **vanlige bruksmønstre** og en enkel **veiledning** i bruk av funksjonen. Gå gjennom hele samlingen og se hvor mye du kan gjøre med de betalte utgavene av Google Workspace for Education.

Google Workspace for Education (betalte utgaver)

Med tre betalte utgaver av Google Workspace for Education får du flere valgmuligheter, mer kontroll og større fleksibilitet for å dekke organisasjonens behov.

Google Workspace for Education Plus

Inkluderer Education Standard, Teaching and Learning Upgrade og andre funksjoner som er eksklusive for Plus.

Med Education Plus får elever, lærere, utdanningsledere og IT-administratorer **undervisningsverktøy i en alt-i-ett-løsning** med brukervennlige verktøy for **avansert sikkerhet og statistikk samt bedre undervisning og læring**.

Google Workspace for Education Standard

Avanserte sikkerhets- og statistikkverktøy bidrar til å redusere risikoer og bekjempe trusler med bedre synlighet og styring i hele læringsmiljøet.

Teaching and Learning Upgrade

Bedre undervisnings- og læringsverktøy bidrar til at undervisningen blir mer virkningsfull med mer personlig tilpasset læring, effektive klasserom og mulighet for undervisning og læring uansett hvor man er.

Innhold

Avanserte sikkerhets- og statistikkfunksjoner

Sikkerhetsoversikten

- Mengden nettsøppel
- Ekstern fildeling
- Apper fra tredjeparter
- Forsøk på nettfisking

Side for sikkerhetstilstand

- Anbefalte fremgangsmåter for sikkerhet
- Anbefalinger for risikoområder

Undersøkelsesverktøyet

- Deling av støtende materiale
- Utilsiktet deling av filer
- E-poster med nettfisking og skadelig programvare
- Stopp useriøse aktører
- Mer omfattende sikkerhetsstatistikk
- Forhindre møter uten tilsyn

Domeneadministrasjon og -kontroller

- Skan Gmail-vedlegg etter trusler
- Opprett bruksoversikter og -rapporter
- Finn filer enklere
- Organiserte interne dokumenter
- Fyll inn avdelingsgrupper automatisk
- Opprett målgruppe for intern fildeling
- Begrens fildeling
- Begrensninger for apper i Workspace
- Lagringsadministrasjon
- Regelverk for data
- Regler for tilskudd
- Administrer endepunktenheter
- Administrer Windows-enheter
- Egendefinerte innstillinger for Windows-enheter
- Automatiser oppdateringer av Windows-enheter
- Dra nytte av kryptering på klientsiden

Innhold

Bedre undervisnings- og læringsfunksjoner

Google Classroom

- Administrer tilgang til Classroom-tillegg
- Integrer engasjerende innhold i Classroom
- Opprett kurs i stor skala

Plagiatrapporter

- Se etter plagiering med plagiatrapporter
- Sjekk originaliteten opp mot tidligere elevarbeid
- Gjør plagiatkontroll om til en mulighet for læring

Dokumenter, Regneark og Presentasjoner

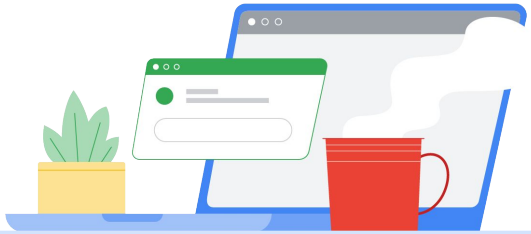
- Godkjenn interne dokumenter

Google Meet

- Ta opp møter
- Henvis til klassediskusjoner
- Fjern språkbarrierer
- Kringkast samlinger og skolearrangementer
- Still spørsmål
- Innsamling av innspill
- Små elevgrupper
- Sporing av deltakelse

Avanserte sikkerhets- og statistikkfunksjoner

Få mer kontroll over domenet ditt med proaktive sikkerhetsverktøy som beskytter mot trusler, analyserer sikkerhetshendelser og ivaretar elev- og personaldata.

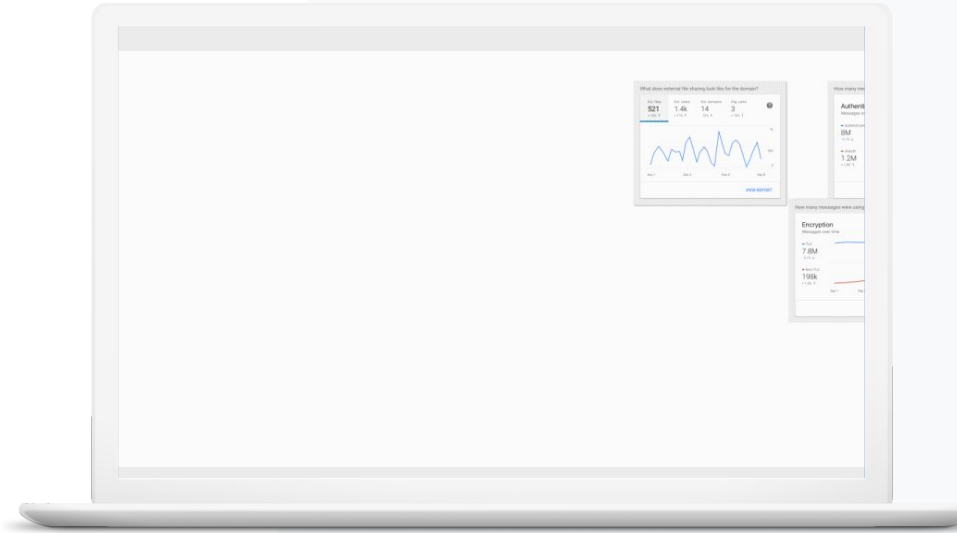


- Sikkerhetsoversikten
- Side for sikkerhetstilstand
- Undersøkelsesverktøyet
- Domeneadministrasjon og -kontroller

Sikkerhetsoversikten

Hva er dette?

Bruk sikkerhetsoversikten til å få oversikt over alle sikkerhetsrapportene dine. Som standard viser hvert panel sikkerhetsrapporter med data fra de siste 7 dagene. Du kan tilpasse oversikten til å vise data fra i dag, i går, denne uken, forrige uke, denne måneden, forrige måned eller for flere dager siden (opptil 180 dager).



Bruksmønstre

Mengden nettsøppel	Trinnvis veiledning
Ekstern fildeling	Trinnvis veiledning
Apper fra tredjeparter	Trinnvis veiledning
Forsøk på nettfisking	Trinnvis veiledning

“

Jeg vil redusere antallet overflødige og unødvendige e-poster og samtidig redusere mengden sikkerhetstrusler for skolen.”

Mengden nettsøppel

Med **sikkerhetsoversikten** får du en visuell representasjon av aktiviteten i Google Workspace for Education-miljøet ditt, inkludert

- nettsøppel
- mistenkelige vedlegg
- nettfishing
- og mye mer
- skadelig programvare

Trinnvis veiledning

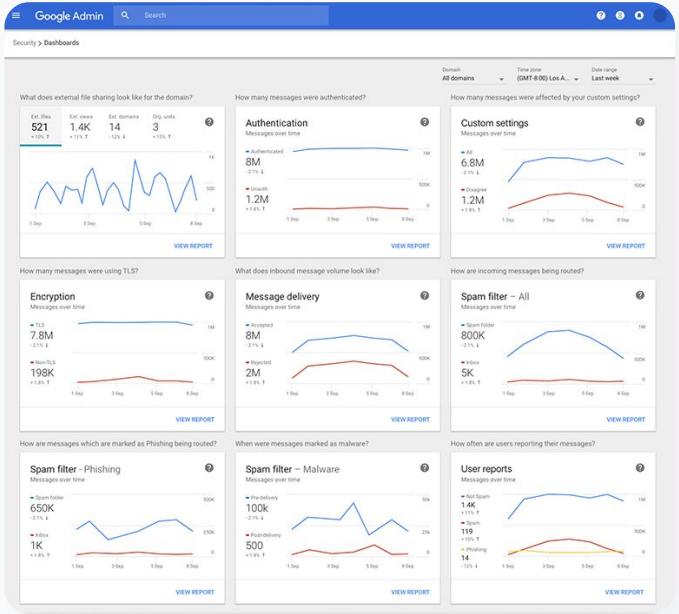
Relevant dokumentasjon i brukerstøtten

- Om sikkerhetsoversikten

Veiledning: Oversiktens struktur

Slik bruker du sikkerhetsoversikten:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Oversikt**
- Fra sikkerhetsoversikten kan du se nærmere på data, eksportere data til Regneark eller andre verktøy fra tredjeparter eller starte undersøkelser med undersøkelsesverktøyet



Relevant dokumentasjon i brukerstøtten

- Om sikkerhetsoversikten

Ekstern fildeling

Jeg vil se aktivitet om ekstern fildeling for å forhindre at sensitive data deles med tredjeparter.”

Bruk **fileksponeringsrapporten** fra **sikkerhetsoversikten** til å se verdier for ekstern fildeling for domenet ditt, inkludert

- antall delingshendelser til brukere utenfor domenet i en bestemt tidsperiode
- hvor mange ganger en ekstern fil er sett i en bestemt tidsperiode

Trinnvis veiledning

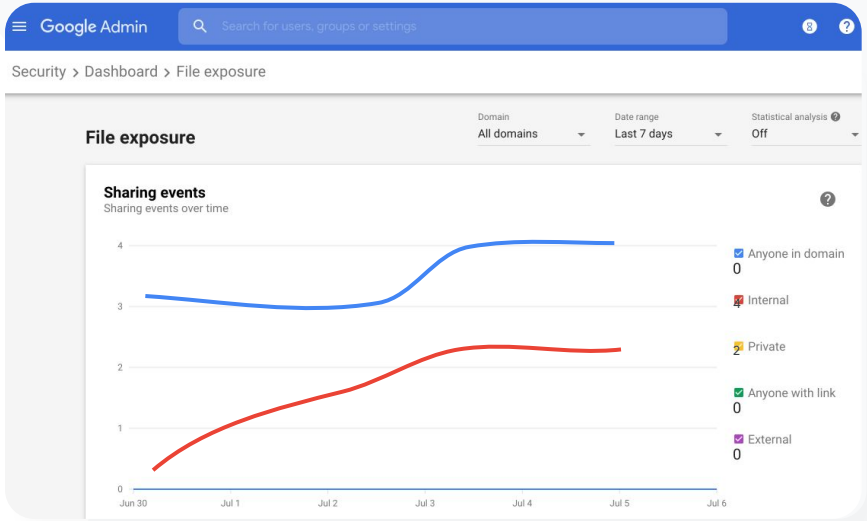
Relevant dokumentasjon i brukerstøtten

- Kom i gang med siden for sikkerhetstilstand

Veiledning: Ekstern fildeling

Slik kan du se fileksponeringsrapporten:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Oversikt**
- I panelet **«Hvordan ser den eksterne delingen ut for domenet?»** klikker du på **Se rapporten** nederst til høyre



Relevant dokumentasjon i brukerstøtten

- Om sikkerhetsoversikten
- Fileksponeringsrapport

Apper fra tredjeparter

Bruk **aktivitetsrapporten om OAuth-tilgang** fra **sikkerhetsoversikten** til å holde øye med hvilke apper fra tredjeparter som er koblet til domenet ditt, og hvilke data de har tilgang til.

- OAuth gir tjenester fra tredjeparter tilgang til brukeres kontoinformasjon uten å avsløre brukernes passord. Det kan være lurt å begrense hvilke tredjepartsapper som har tilgang.
- Bruk panelet for OAuth-tilgangsaktivitet til å holde øye med tilgangsaktivitet basert på app, omfang eller bruker og til å oppdatere tilgangstillatelser.

> Jeg vil se tredjepartsappene som har tilgang til data på domenet mitt.”

Trinnvis veiledning

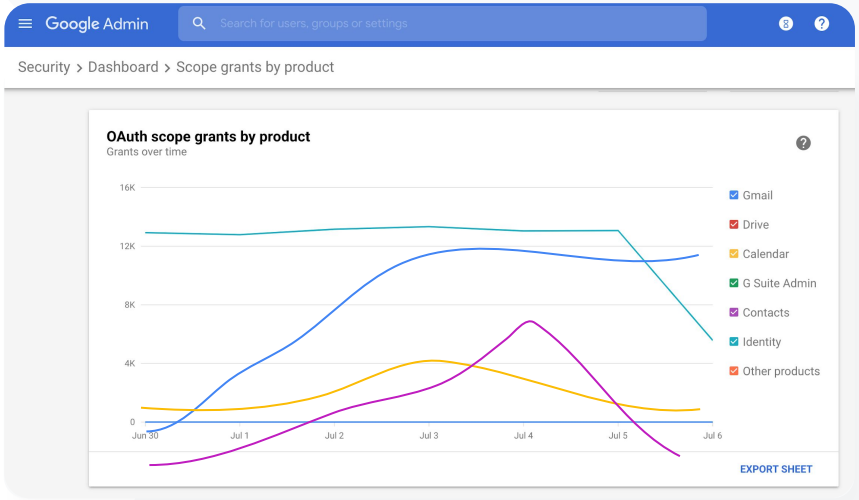
Relevant dokumentasjon i brukerstøtten

- Aktivitetsrapport om OAuth-tilgang

Veiledning: Apper fra tredjeparter

Slik bruker du aktivitetsrapporten om OAuth-tilgang:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Oversikt**
- Nederst klikker du på **Se rapporten**
- Du kan se aktivitet knyttet til OAuth-tilgang etter produkt (app), omfang eller bruker
- For å filtrere informasjonen klikker du på **App**, **Omfang** eller **Bruker**
- For å generere en regnearkrapport klikker du på **Eksporter regneark.**



Relevant dokumentasjon i brukerstøtten

- Aktivitetsrapport om OAuth-tilgang

“Brukere har rapportert et forsøk på nettfisking. Jeg vil kunne spore når nettfiskings-e-posten ble mottatt, nøyaktig hva slags e-post brukerne har mottatt, og hva slags risiko de var utsatt for.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Slik merker brukerne e-postene sine
- Brukerrapporter

Forsøk på nettfisking

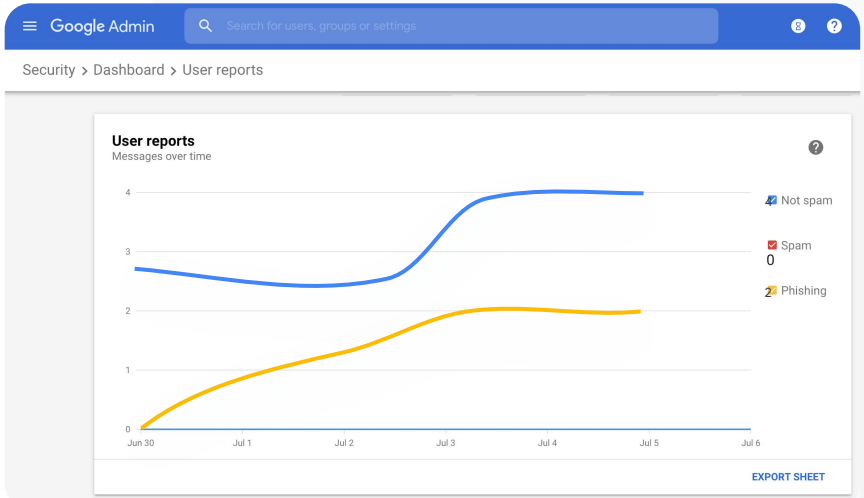
Med **panelet for brukerrapporter** i **sikkerhetsoversikten** kan du se meldinger som er merket som nettfisking eller søppelpost i en bestemt tidsperiode. Du kan se informasjon om e-poster merket som nettfisking, for eksempel mottakere og hvor mange ganger de er åpnet.

- Med brukerrapporter kan du se hvordan brukere merker e-postene sine – enten som søppelpost, ikke søppelpost eller nettfisking – i en bestemt tidsperiode.
- Du kan tilpasse diagrammet slik at du kun ser informasjon om bestemte typer e-poster – for eksempel om e-postene ble sendt internt eller eksternt, etter datoperiode osv.

Veiledning: Forsøk på nettfisking

Slik bruker du panelet for brukerrapporter:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Oversikt**
- Nederst til høyre i **panelet for brukerrapporter** klikker du på **Se rapporten**



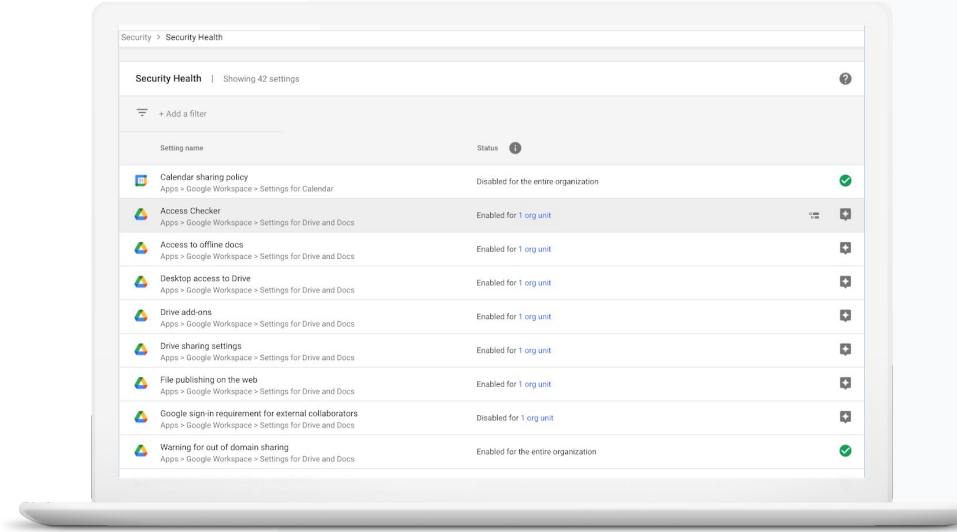
Relevant dokumentasjon i brukerstøtten

- Om sikkerhetsoversikten
- Fileksponeringsrapport

Sikkerhetstilstand

Hva er dette?

På siden for sikkerhetstilstand får du en omfattende oversikt over sikkerhetsstatusen for Google Workspace-miljøet ditt, og du kan sammenligne konfigurasjonene dine med anbefalinger fra Google for å beskytte organisasjonen proaktivt.



Bruksmønstre

Anbefalte fremgangsmåter for sikkerhet — Trinnvis veiledning

Anbefalinger for risikoområder — Trinnvis veiledning

“Fortell meg hvor jeg finner anbefalte fremgangsmåter for oppretting av sikkerhetsregler.”

Anbefalte fremgangsmåter for sikkerhet

Åpne siden for sikkerhetstilstand for å få anbefalte fremgangsmåter om sikkerhetsregler med

- anbefalinger for potensielle risikoområder på domenet ditt
- anbefalinger om optimale innstillinger for sikkerhet
- direktelinker til innstillingene
- mer informasjon og brukerstøtteartikler

Trinnvis veiledning

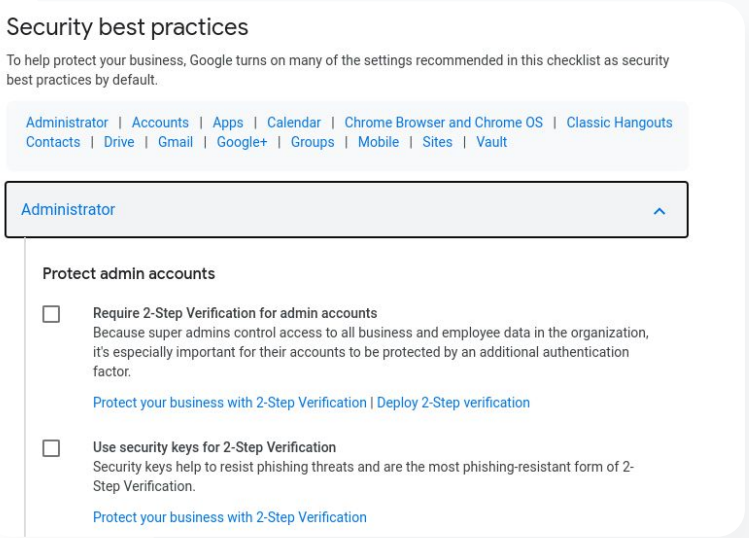
Relevant dokumentasjon i brukerstøtten

- Kom i gang med siden for sikkerhetstilstand

Veiledning: Sjekkliste med anbefalte fremgangsmåter for sikkerhet

For å bidra til å beskytte organisasjonen din slår Google som standard på mange av de anbefalte innstillingene i denne sjekklisten, i tråd med de anbefalte fremgangsmåtene for sikkerhet. Vi anbefaler at du ser nærmere på dem som er markert nedenfor.

- **Administrator:** Beskytt administratorkontoer
- **Kontoer:** Bidra til å forebygge og løse problemer knyttet til kontoer med sikkerhetsbrudd
- **Apper:** Gjennomgå tredjeparters tilgang til kjernetjenester.
- **Kalender:** Begrens ekstern kalenderdeling
- **Disk:** Begrens deling og samarbeid utenfor domenet ditt
- **Gmail:** Konfigurer autentisering og infrastruktur
- **Arkiv:** Kontroller, revider og sikre Arkiv-kontoer



Relevant dokumentasjon i brukerstøtten

- Følg med på tilstanden til sikkerhetsinnstillingene dine

“Jeg vil ha en forståelig oversikt over sikkerhetsinnstillingene for domenet mitt med praktiske anbefalinger for håndtering av potensielle risikoområder.”

Anbefalinger for risikoområder

På siden for **sikkerhetstilstand** ser du en oversikt over sikkerhetskonfigurasjonene dine og anbefalte endringer. På siden for sikkerhetstilstand kan du

- raskt identifisere potensielle risikoområder på domenet ditt
- få anbefalinger om optimale innstillinger for sikkerhet
- finne mer informasjon og brukerstøtteartikler om anbefalingene

Trinnvis veiledning

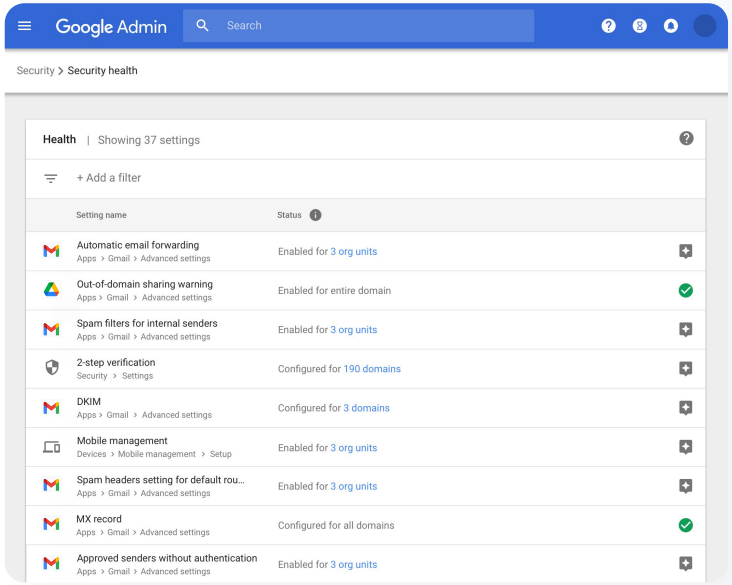
Relevant dokumentasjon i brukerstøtten

- Kom i gang med siden for sikkerhetstilstand

Veiledning: Sikkerhetsanbefalinger

Slik ser du anbefalinger:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Sikkerhetstilstand**
- Se statusinnstillingene i kolonnen lengst til høyre
  - Et grønt hakemerke indikerer en trygg innstilling
  - Et grått ikon indikerer at du anbefales å ta en titt på innstillingen. Klikk på ikonet for å se detaljer og en veiledning



Relevant dokumentasjon i brukerstøtten

- Kom i gang med siden for sikkerhetstilstand

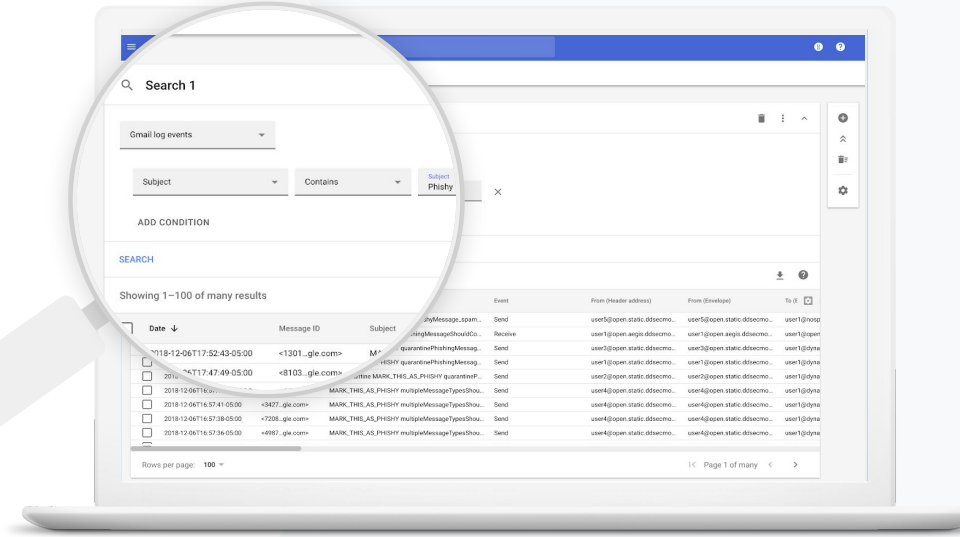
Undersøkelsesverktøyet

Hva er dette?

Bruk undersøkelsesverktøyet til å identifisere, kategorisere og håndtere sikkerhets- og personvernproblemer på domenet ditt.

Bruksmønstre

Deling av støtende materiale	Trinnvis veiledning
Utilsiktet deling av filer	Trinnvis veiledning
Kategorisering av e-poster	Trinnvis veiledning
E-poster med nettfisking eller skadelig programvare	Trinnvis veiledning
Stopp useriøse aktører	Trinnvis veiledning
Mer omfattende sikkerhetsstatistikk	Trinnvis veiledning
Forhindre møter uten tilsyn	Trinnvis veiledning



Jeg vet at en fil med støtende materiale blir delt. Jeg vil vite hvem som opprettet den, når den ble opprettet, hvem som har delt den med hvem, hvem som har redigert den, og jeg vil slette den."

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Betingelser for logghendelser i Disk
- Handlinger knyttet til logghendelser i Disk

Deling av støtende materiale

Logghendelser for Disk i **undersøkelsesverktøyet** kan brukes til å finne, spore og isolere eller slette uønskede filer på domenet. Med tilgang til logghendelsesdata for Disk kan du gjøre dette:

- søke etter dokumenter basert på navn, aktør, eier med mer
- gjennomføre tiltak ved å endre filtillatelser eller slette filen
- søke i innhold som brukere oppretter i Google Workspace, og innhold de laster opp til Disk
- se all logginformasjon tilknyttet dokumentet:
  - opprettelsesdato
  - hvem som eier det, hvem som har sett det, og hvem som har redigert det
  - når det ble delt

“En fil ble utilsiktet delt med en gruppe som IKKE skal ha tilgang til den.

Jeg vil fjerne gruppens tilgang.”

Utilsiktet deling av filer

Logghendelser i Disk i **undersøkelsesverktøyet** kan brukes til å spore og løse problemer med fildeling. Med tilgang til logghendelsesdata i Disk kan du gjøre dette:

- søke etter dokumenter basert på navn, aktør, eier med mer
- se all logginformasjon som er tilknyttet dokumentet, inkludert hvem som har sett det, og når det ble delt
- gjennomføre tiltak ved å endre tillatelser og slå av nedlasting, utskrift og kopiering

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Kjør et søk i undersøkelsesverktøyet
- Gjennomfør tiltak basert på søkeresultater

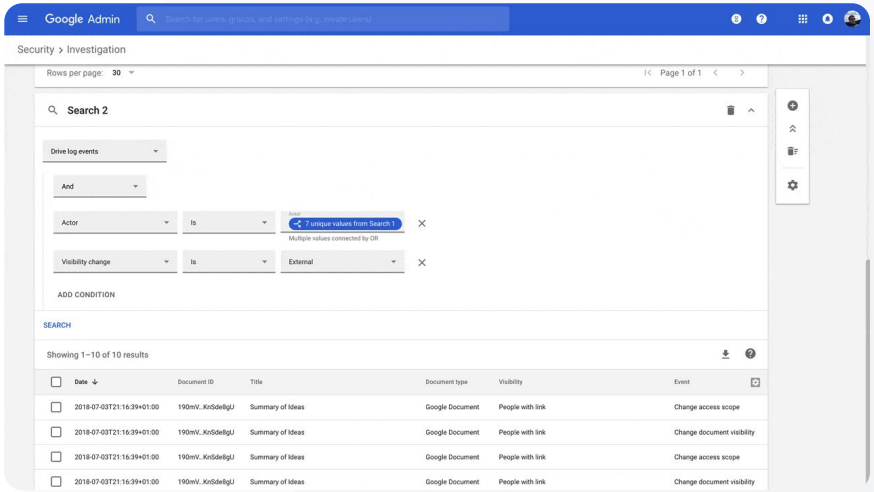
Veiledning: Logghendelser i Disk

Slik undersøker du logghendelser i Disk:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Undersøkelsesverktøy**
- Velg **Logghendelser i Disk**
- Klikk på **Legg til en betingelse** > **Søk**

Slik gjennomfører du tiltak

- Velg den relevante filen i søkeresultatene
- Klikk på **Handlinger** > **Revider filtillatelser** for å åpne Tillatelser-siden
- Klikk på **Personer** for å se hvem som har tilgang.
- Klikk på **Linker** for å se eller endre innstillingene for linkdeling for de valgte filene
- Klikk på **Ventende endringer** for å gå gjennom endringene før du lagrer



Relevant dokumentasjon i brukerstøtten

- Kjør et søk i undersøkelsesverktøyet
- Gjennomfør tiltak basert på søkeresultater

> Noen har sendt en e-post som IKKE skulle vært sendt. Vi vil vite hvem den er sendt til, om mottakerne har åpnet den, om de har svart, og vi vil slette e-posten. Jeg vil også vite hva innholdet i e-posten er.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Betingelser for Gmail-logger og Gmail-meldinger
- Handlinger for Gmail-meldinger og logghendelser i Gmail
- Fremgangsmåte for å se innhold i e-poster

Kategorisering av e-poster

Gmail-loggene i **undersøkelsesverktøyet** kan brukes til å identifisere og håndtere farlige eller støtende e-poster på domenet ditt. Ved hjelp av Gmail-loggene kan du gjøre dette:

- søke etter spesifikke e-poster etter emne, meldings-ID, vedlegg, avsender med mer
- se e-postdetaljer, inkludert forfatter, mottaker, åpning og videresending
- gjennomføre tiltak basert på søkeresultater – tiltak for Gmail-meldinger kan omfatte sletting, gjenoppretting, merking som søppelpost eller nettfisking, sending til innboksen og sending til karantene

“

En e-post med nettfisking eller skadelig programvare ble sendt til brukerne. Vi vil se om brukerne har klikket på linken i e-posten eller lastet ned vedlegget, siden dette potensielt kan utsette brukerne og domenet vårt for risiko.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Betingelser for Gmail-logger og Gmail-meldinger
- Handlinger for Gmail-meldinger og logghendelser i Gmail
- Fremgangsmåte for å se innhold i e-poster
- Se VirusTotal-rapporter

E-poster med nettfisking og skadelig programvare

Ved hjelp av **undersøkelsesverktøyet**, spesielt **Gmail-loggene**, kan du finne og isolere skadelige e-poster på domenet ditt. Ved hjelp av Gmail-loggene kan du gjøre dette:

- søke i e-postmeldinger etter spesifikt innhold, inkludert vedlegg
- se informasjon om bestemte e-poster, inkludert mottakere og åpning
- se e-poster og tråder, og avgjøre om de er skadelige
- skanne e-postvedlegg for å finne detaljerte data om trusselkontekst og omdømme med VirusTotal-rapporter
- gjennomføre tiltak ved å merke e-poster som søppelpost eller nettfisking, sende dem til bestemte innbokser, sette dem i karantene eller slette dem

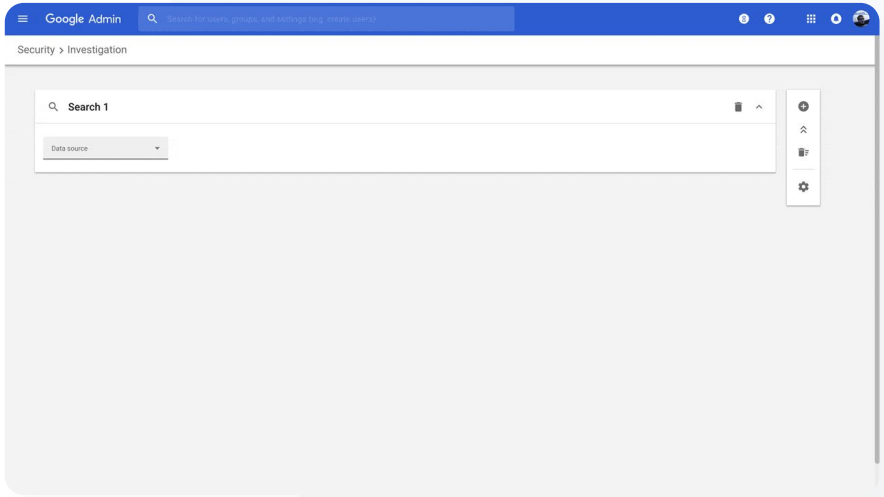
Veiledning: Gmail-logger

Slik undersøker du Gmail-logger:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Undersøkelsesverktøy**
- Velg **Logghendelser i Gmail** ELLER **Gmail-meldinger**
- Klikk på **Legg til en betingelse** > **Søk**

Slik gjennomfører du tiltak

- Velg den relevante filen i søkeresultatene
- Klikk på **Handlinger**
- Velg **Slett meldingen fra innboksen til eieren**
- For å bekrefte handlingen klikker du på Se nederst på siden
- I **Resultat**-kolonnen kan du se statusen for handlingen



Relevant dokumentasjon i brukerstøtten

- Betingelser for Gmail-logger og Gmail-meldinger
- Handlinger for Gmail-meldinger og logghendelser i Gmail
- Fremgangsmåte for å se innhold i e-poster

“Ondsinnede aktører går konsekvent etter høyprofilerte brukere på domenet mitt, mens jeg kjemper for å stoppe dem.

Hvordan kan jeg stoppe dette?”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Søk etter og undersøk logghendelser for brukere
- Opprett aktivitetsregler med undersøkelsesverktøyet

Stopp ondsinnede aktører

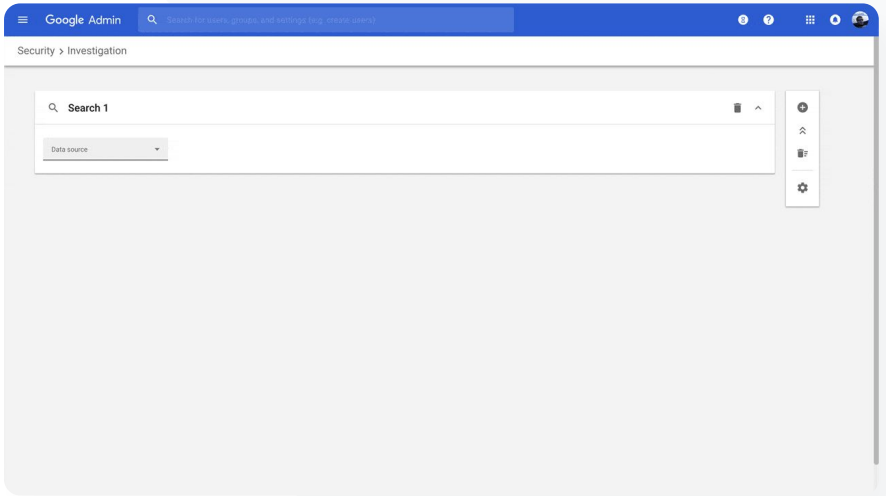
Med **brukerloggen** i **undersøkelsesverktøyet** kan du gjøre dette:

- identifisere og undersøke forsøk på å kapre brukerkontoer i organisasjonen din
- holde øye med hvilke metoder for totrinnsbekreftelse som brukes i organisasjonen
- finne ut mer om mislykkede påloggingsforsøk gjort av brukere i organisasjonen
- opprette aktivitetsregler med undersøkelsesverktøyet: Blokker automatisk meldinger og andre skadelige aktiviteter fra bestemte aktører
- beskytte høyprofilerte brukere enda bedre med Avansert beskyttelse-programmet
- gjenopprette eller utestenge brukere

Veiledning: Stopp ondsinnede aktører

Slik undersøker du en logghendelse for en bruker:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Undersøkelsesverktøy**
- Velg **Logghendelser for brukere**
- Klikk på **Legg til en betingelse** > **Søk**



Slik gjenoppretter eller utestenger du brukere

- I søkeresultatene velger du én eller flere brukere
- Klikk på rullegardinmenyen **Handlinger**
- Klikk på **Gjenopprett brukeren** eller **Utesteng brukeren**

Slik ser du informasjon om bestemte brukere

- På søkeresultatsiden velger du kun én bruker
- I rullegardinmenyen HANDLINGER klikker du på **Se detaljer**

Relevant dokumentasjon i brukerstøtten

- Søk etter og undersøk logghendelser for brukere

“

En av lærerne våre rapporterte en mistenkelig vedleggsfil i Gmail.

Hvordan kan IT-avdelingen finne ut om filen utgjør en sikkerhetstrussel?”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Kjør et søk i undersøkelsesverktøyet
- Se VirusTotal-rapporter fra undersøkelsesverktøyet

Få mer omfattende sikkerhetsstatistikk

VirusTotal-rapporter inneholder mer detaljerte resultater av en sikkerhetsundersøkelse med en omfattende oversikt. Dermed kan administratorer sjekke sikkerheten for bestemte domener, filvedlegg, IP-adresser og nettadresser basert på statistikk fra crowdsourcing.

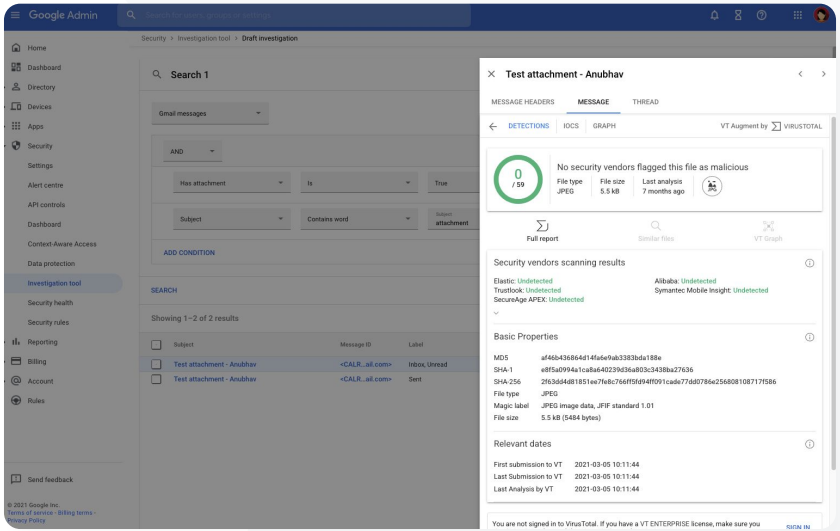
- Få ekstra sikkerhetsstatistikk for logghendelser i Gmail og Chrome
- Analyser mistenkelige filer, nettadresser, domener og IP-adresser
- Få tilgang til informasjon hentet fra crowdsourcing om hvorfor et vedlegg eller nettsted vurderes som usikkert
- Få hjelp med beslutningstakingen når du adresserer sikkerhetsproblemer

Veiledning: Få mer omfattende sikkerhetsstatistikk

Slik bruker du VirusTotal-rapporter knyttet til Gmail:

- Logg på **administrasjonskonsollen.**
- Klikk på **Sikkerhet** > **Sikkerhetssenter** > **Undersøkelsesverktøy.**
- Velg **Gmail-meldinger.**
- Klikk på **Legg til en betingelse** > **Har vedlegg.**
- I søkeresultatene klikker du på **meldings-ID-en** eller **emnelinken**
- I sidepanelet klikker du på **Melding**- eller **Trussel**-fanen
- Velg **Se VirusTotal-rapport**

Administratorer kan også se VirusTotal-rapporter knyttet til Chrome. Følg veiledningen ovenfor og velg **Chrome-logghendelser** i undersøkelsesverktøyet.



Relevant dokumentasjon i brukerstøtten

- Se VirusTotal-rapporter fra undersøkelsesverktøyet

“Elevene blir værende i Google Meet-samtaler etter at timen er avsluttet. Jeg trenger en metode for å avslutte Meet-samtalen for alle, slik at vi unngår forstyrrelser i undervisningen.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Bruk undersøkelsesverktøyet til å avslutte møter

Forhindre virtuelle møter uten tilsyn

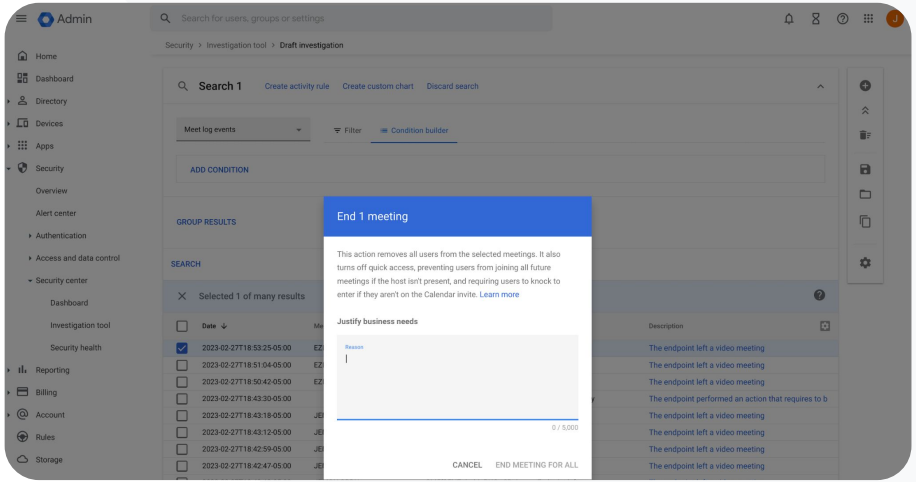
Google Workspace-administratorer kan bruke **Avslutt møtet for alle**-handlingen i undersøkelsesverktøyet for å fjerne alle brukere fra et møte i organisasjonen. Møteverter kan også gjøre dette i individuelle Google Meet-samtaler.

- Møtet avsluttes for alle brukere som deltar på møtet, inkludert brukerne i grupperom.
- Brukerne hindres i å delta i fremtidige tilfeller av møtet uten at verten er til stede.

Veiledning: Forhindre virtuelle møter uten tilsyn

Slik bruker du undersøkelsesverktøyet til å avslutte møter for alle brukere:

- Logg på **administrasjonskonsollen**
- Klikk på **Sikkerhet** > **Sikkerhetssenter** > **Undersøkelsesverktøy**
- Velg **Logghendelser i Meet**
- Klikk på **Søk** > en liste over logghendelsene i Meet vises i søkeresultatene
- Merk av i boksene for møtene du vil avslutte for alle brukere
- Velg **Handlinger**
- Klikk på **Avslutt møtet for alle**



Relevant dokumentasjon i brukerstøtten

- Bruk undersøkelsesverktøyet til å avslutte møter

Domeneadministrasjon og -kontroller

Administratorer har tilgang til avanserte Google Workspace-verktøy som kan brukes til å administrere organisasjonens data, konfigurere kontroller, overvåke bruk og overholde standarder for utdanning.

Bruksmønstre

Skan Gmail-vedlegg etter trusler	Trinnvis veiledning
Opprett bruksoversikter og -rapporter	Trinnvis veiledning
Finn filer enklere	Trinnvis veiledning
Organiser interne dokumenter	Trinnvis veiledning
Fyll inn avdelingsgrupper automatisk	Trinnvis veiledning
Opprett målgrupper for intern fildeling	Trinnvis veiledning
Begrens fildeling	Trinnvis veiledning
Begrensninger for apper i Workspace	Trinnvis veiledning
Lagringsadministrasjon	Trinnvis veiledning
Regelverk for data	Trinnvis veiledning
Regler for tilskudd	Trinnvis veiledning
Administrer endepunktenheter	Trinnvis veiledning
Administrer Windows-enheter	Trinnvis veiledning
Egendefinerte innstillinger for Windows-enheter	Trinnvis veiledning
Automatiser oppdateringer av Windows-enheter	Trinnvis veiledning
Dra nytte av kryptering på klientsiden	Trinnvis veiledning

“Hvordan kan jeg beskytte domenet mitt bedre mot nulldagssårbarhet overfor skadelig programvare og løsepenge-angrep?”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Lag regler for å oppdage skadelige vedlegg

Skan Gmail-vedlegg for trusler

Vedlegg til e-poster kan inneholde skadelig programvare. For å identifisere disse truslene, kan Gmail skanne vedleggene eller kjøre dem i en sikkerhets-sandkasse. Vedlegg som identifiseres som trusler, blir sendt til Søppelpost-mappen.

- Oppdag skadelig programvare ved å “bruke det” virtuelt i et avgrenset, sikkert sandkasse-miljø, og analyser bivirkningene for å avgjøre om det har skadelig oppførsel
- Skan Microsoft Word, PowerPoint, PDF, zip-filer og mer
- Muliggjør skanning for hele domenet, eller opprett skanneregler basert på spesifikke forhold som avsender, domene og mer

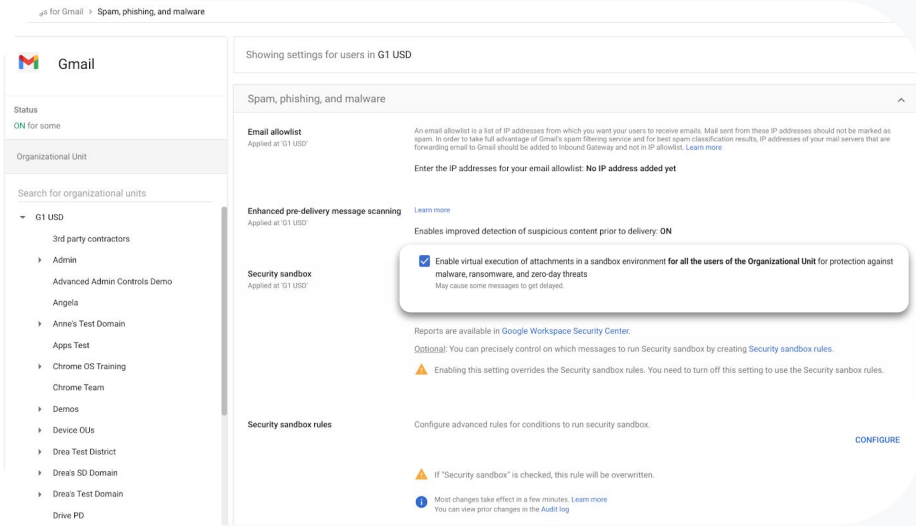
Veiledning: Skan Gmail-vedlegg for trusler

Slik fungerer det

Vedlegg til e-poster detoneres i en sandkasse minutter før den leveres. Det gir et ekstra lag med sikkerhet.

Slik kan du skanne alle vedlegg i en sikkerhets-sandkasse

- Logg på **administrasjonskonsollen**
- Klikk på **Meny** > **Apper** > **Google Workspace** > **Gmail** > **spam, nettfisking, og skadelig programvare**
- Velg en organisasjonsenhet eller innfør innstillingene på hele domenet
- Bla til **Sikkerhets-sandkasse** under **spam, nettfisking og skadelig programvare**
- Klikk på **Slå på virtuell åpning av vedlegg i et sandkassemiljø**-boksen
- Klikk på **Lagre**



Relevant dokumentasjon i brukerstøtten

- Lag regler for å oppdage skadelige vedlegg

“Hvordan får jeg innsikt i Classroom-bruken på domenet mitt?”

Opprett bruksoversikter og -rapporter

Med **BigQuery Export og Looker Studio-mal** kan administratorer bruke Classroom-aktivitetslogger til å opprette egendefinerte oversikter og rapporter med statistikkverktøy som Looker Studio og tredjeparts visualiseringspartnere integrert i BigQuery.

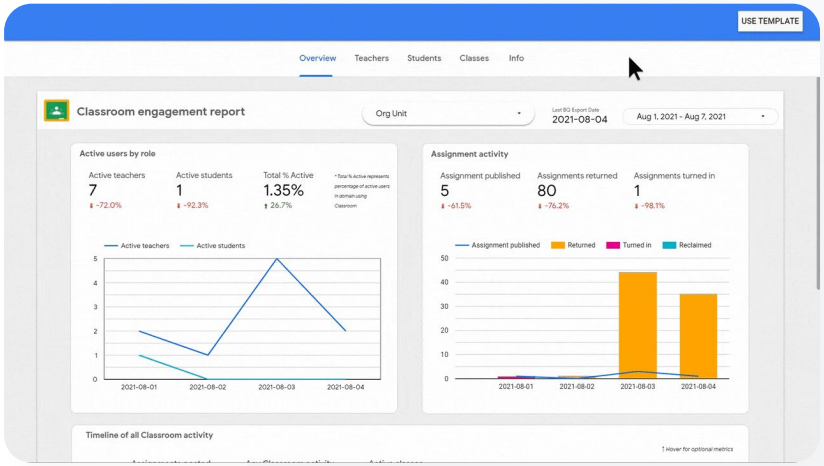
- Eksporter Classroom-loggdata fra administrasjonskonsollen til BigQuery og Looker Studio.
- Se rapporter om bruk og bruksfrekvens over hele domenet på et øyeblikk. Finn ut hvem som fjernet en elev fra et kurs, hvem som arkiverte et kurs på en bestemt dato, med mer.
- Med tilpassbare oversiktsmaler for Looker Studio kan du få innsikt i overordnede trender og iverksette tiltak raskere.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Konfigurer BigQuery-eksport og Looker Studio-mal

Veiledning: Opprett bruksoversikter og -rapporter



01 Opprett og eksporter et BigQuery-prosjekt

- Logg på console.cloud.google.com > **Opprett et nytt prosjekt**
- Logg på admin.google.com > **Rapporter** > **BigQuery Export**
- Klikk på **Cloud BigQuery-prosjekt** > gi datasettet et navn > **Lagre**

02 Legg til BigQuery-eksporten i Looker Studio

- Logg på Looker Studio > **Opprett** > **Datakilde**
- Velg **BigQuery** > **Mine prosjekter** klikk på prosjektet du opprettet > > **Aktivitet**
- Merk av i boksen under **Partisjonert tabell** > klikk på **Koble til**

03 Opprett en Looker Studio-oversikt

- Åpne malen > velg **Bruk mal**
- Under **Ny datakilde** velger du **aktivitet** som datakilde
- Klikk på **Kopier rapport**

Relevant dokumentasjon i brukerstøtten

- Konfigurer BigQuery-eksport og Looker Studio-mal

“Jeg må finne samtykkeskjemaer for en utflukt som foreldrene har sendt inn via Gmail, Chat og Dokumenter.

Hvordan finner jeg disse filene i domenet?”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Veiledning for Google Cloud Search
- Slå av eller på Cloud Search for brukerne

Finn filer enklere

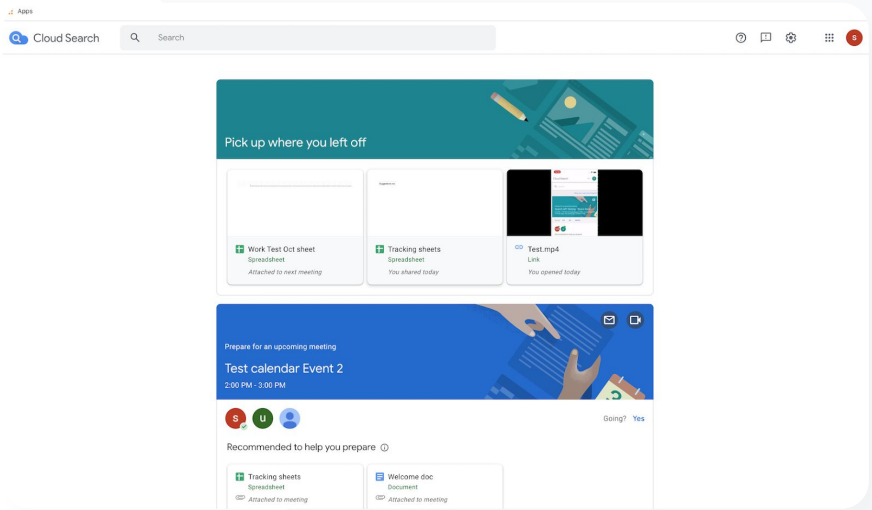
Med Google Cloud Search kan lærerne på institusjonen din raskt finne innhold i Google Workspace og tredjepartsapper.

- Finn informasjonen du trenger uansett hvor du er, med en laptop, en mobiltelefon eller et nettbrett.
- Søk i Google Workspace-apper som Disk, Kontakter, Gmail, samt tredjeparts datakilder.

Veiledning: Finn filer enklere

Slå på Cloud Search for brukerne

- Logg på **administrasjonskonsollen** > gå til **Meny** > **Apper** > **Google Workspace**.
- Klikk på **Tjenestestatus**.
- Hvis du skal slå av eller på en tjeneste for alle i organisasjonen, klikker du på **På for alle** eller **Av for alle**.
- Klikk på **Lagre**.
- Hvis du skal slå på en tjeneste for en gruppe brukere på tvers av eller innenfor organisasjonsenheter, velger du en **tilgangsgruppe**.
- Klikk på **Lagre**.



Relevant dokumentasjon i brukerstøtten

- Veiledning for Google Cloud Search
- Slå av eller på Cloud Search for brukerne

“Jeg vil sette følsomhetsetiketter på institusjonens filer for å innfri krav om overholdelse av regler, forhindre uriktig bruk og organisere filene bedre.”

Organiser dokumentene i domene ditt

Disk-etiketter gjør det enklere for brukerne å finne, organisere og implementere regler på domenet sitt. Administratorer kan opprette og administrere Disk-etiketter for å forhindre misbruk av filer og sørge for at elevdataene innfrir regelkravene.

- Etiketter er metadata som kan brukes til å organisere sensitive institusjonsfiler, for eksempel tilpassede undervisningsplaner, DOD eller reglementsdokumenter.
- Det er kun administratorer som kan opprette, definere strukturer for og publisere etiketter. Brukerne i organisasjonen din kan sette etiketter på filene de redigerer, og de kan angi feltverdiene.
- Disk-etiketter kan brukes til å støtte opp under automatisert forebygging av datatap.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Administrer Disk-etiketter

Veiledning: Organiser dokumentene i domene ditt

Slik fungerer det

I Google Disk finner du etiketter med merke (en visuell indikator) og standardetiketter som du kan bruke til å organisere filene i domenet ditt.

Slik slår du på Disk-etiketter for institusjonen din:

- Logg på **administrasjonskonsollen.**
- Klikk på **Meny** > **Apper** > **Google Workspace** > **Disk og Dokumenter.**
- Velg **Etiketter.**
- Slå etiketter **av** eller **på.**
- Klikk på **Lagre.**

Relevant dokumentasjon i brukerstøtten

- Administrer Disk-etiketter

“Hvordan kan jeg automatisere gruppemedlemskap slik at hver gang en ny lærer starter på institusjonen vår, legges vedkommende til i e-postlisten min for lærere?”

Fyll inn avdelingsgrupper automatisk

Med **dynamiske grupper** kan administratorer oppdatere gruppemedlemskap for hele skolen med tilpassede kriterier.

- Opprett dynamiske grupper som administrerer medlemskap automatisk.
- Hold gruppene oppdatert basert på medlemskapssøk du oppretter.
- Bruk dynamiske grupper som
  - e-post- og distribusjonslister
  - modererte grupper og samarbeidsinnbokser
  - sikkerhetsgrupper

Trinnvis veiledning

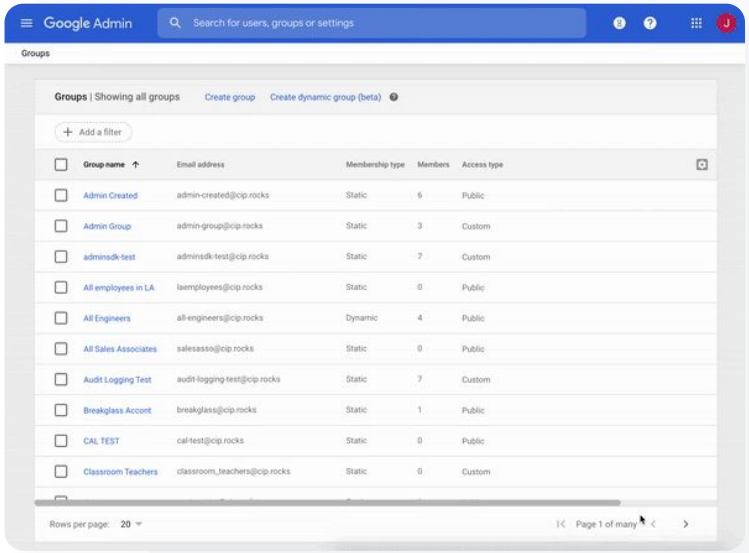
Relevant dokumentasjon i brukerstøtten

- Administrer medlemskap automatisk med dynamiske grupper

Veiledning: Fyll inn grupper automatisk

Opprett en dynamisk gruppe

- Logg på **administrasjonskonsollen** > gå til **Meny** > **Katalog** > **Grupper.**
- Klikk på **Opprett en dynamisk gruppe**
- Bygg opp medlemskapsøket i følgende:
  - listen over betingelser: kriterier for medlemskap, f.eks. avdeling
  - verdifeltet: verdien du vil bruke
- Angi denne informasjonen:
  - navn: dette identifiserer gruppen i lister og meldinger
  - beskrivelse: formålet med gruppen
  - gruppe-e-post: e-postadressen som brukes for gruppen
- Klikk på **Lagre.**
- Klikk på **Ferdig.**



Relevant dokumentasjon i brukerstøtten

- Administrer medlemskap automatisk med dynamiske grupper

“De ansatte deler utilsiktet dokumenter med hele organisasjonen, noe som utsetter sensitive data for risiko. Hvordan kan jeg begrense delingen deres til en mindre, mer relevant gruppe?”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Om målgrupper
- Anbefalte fremgangsmåter for implementering av målgrupper
- Opprett en målgruppe

Opprett målgrupper for intern fildeling

Med innstillingene for **målgrupper** kan du forbedre sikkerheten for organisasjonens data ved å redusere risikoen for at brukerne utilsiktet deler filer med for mange personer.

- Sikre at filene kun deles med de rette personene, for eksempel bestemte team eller avdelinger.
- Målgrupper er grupper med personer som administratorer kan anbefale at brukere deler elementer med.
- Administratorer kan legge til målgrupper i brukernes delingsinnstillinger for å oppfordre til deling med en mer spesifikk målgruppe.
- Tilgjengelig i Google Disk, Dokumenter og Chat.

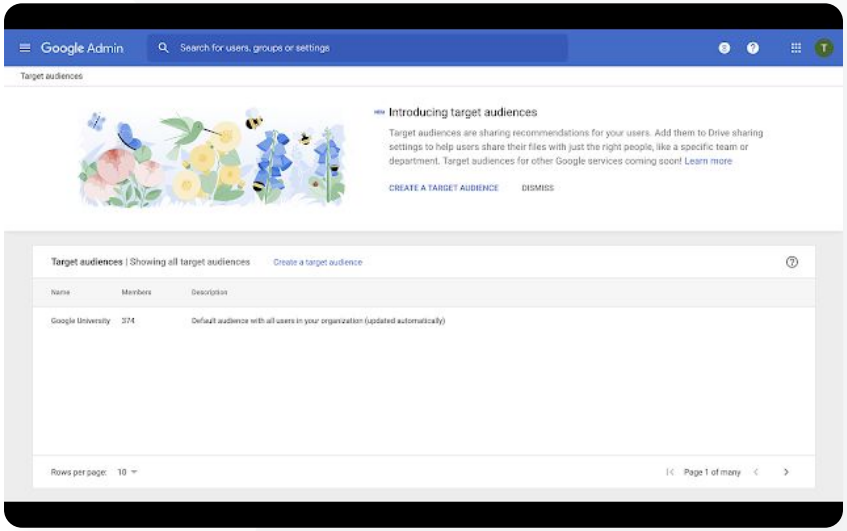
Veiledning: Opprett målgrupper for intern fildeling

Slik fungerer det

Når du har opprettet en målgruppe, kan du legge til medlemmer og bruke målgrupper i Google Disk for å gjøre den tilgjengelig i brukernes delingsinnstillinger. Du kan for eksempel sørge for at de ansatte ser målgruppen «Alle ansatte» når de deler Disk-filer.

Slik slår du på Disk-etiketter for institusjonen din:

- Logg på **administrasjonskonsollen** > gå til **Meny** > **Katalog** > **Målgrupper.**
- Klikk på **Opprett målgruppe.**
- Under **Navn** skriver du inn et navn for målgruppen.
- Velg **Legg til medlemmer** > legg til de medlemmene du ønsker.
- Klikk på **Ferdig.**



Relevant dokumentasjon i brukerstøtten

- Om målgrupper
- Anbefalte fremgangsmåter for implementering av målgrupper
- Opprett en målgruppe

“Hvordan kan jeg forhindre at ungdomsskoleelevene deler dokumenter med barneskoleelevene?”

Begrens fildeling

Med klareringsreglene for Disk kan administratorer angi regler for å kontrollere hvem som får tilgang til Google Disk-filer, for å beskytte institusjonelle data. Retningslinjene kan gjelde for individuelle brukere, grupper, organisasjonsenheter og domener.

- Beskytt sensitiv informasjon og overhold bransjestandarder og forordninger.
- Begrens intern og/eller ekstern domenedeling. Administratorer kan opprette en klareringsregel for å bare tillate at elevene deler Disk-filer innad i organisasjonen.
- Når klareringsreglene er aktivert, erstatter de de eksisterende delingsalternativene i administratorkontrollene for Google Disk.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Opprett og administrer klareringsregler for Disk-deling

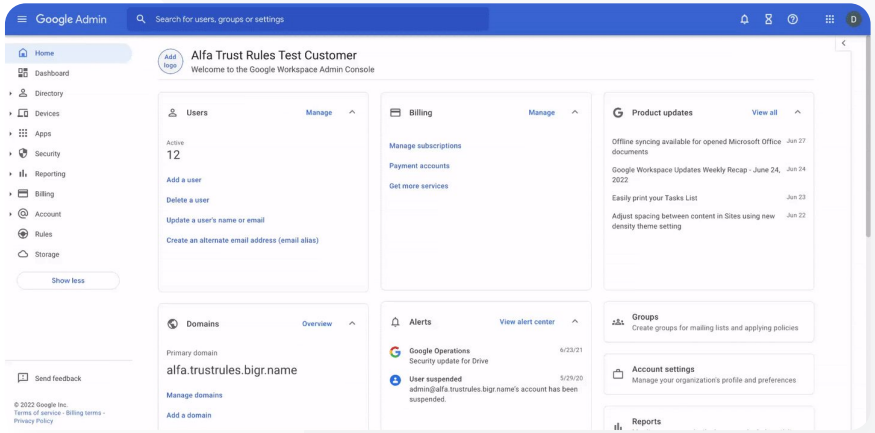
Veiledning: Begrens fildeling

Slå på klareringsregler for Disk

- Logg på **administrasjonskonsollen** > gå til **Meny** > **Regler.**
- Gå til **Samarbeid på en trygg måte**-kortet øverst på siden og klikk på **Slå på klareringsregler.**
- Oppgavelistene dine åpnes automatisk og viser fremdriften for aktiveringen av klareringsregler.

Administratorer kan opprette og slette klareringsregler, se og endre detaljene dem samt følge med på logghendelser.

Gå til brukerstøtten for administratorer for å se en trinnvis veiledning for administrering av klareringsregler.



Relevant dokumentasjon i brukerstøtten

- Opprett og administrer klareringsregler for Disk-deling

Appbegrensninger i Google Workspace

Med **kontekstsensitiv tilgang** kan du opprette detaljerte regler for tilgangskontroll for **Google Workspace- og tredjeparts SAML-apper** (Security Assertion Markup Language) basert på attributter som brukeridentitet, posisjon, enhetens sikkerhetsstatus og IP-adresse. I tillegg kan du begrense tilgangen til apper utenfor nettverket.

- Du kan bruke regler for kontekstsensitiv tilgang for kjernetjenestene i Google Workspace for Education.
- Du kan for eksempel begrense tilgangen til Workspace-apper fra enheter som er utstedt av institusjonen, eller bare gi tilgang til Disk hvis brukerlagringsenheten er kryptert.

> “Jeg vil begrense tilgangen til bestemte apper for brukere når de er tilkoblet nettverket vårt.”

Trinnvis veiledning

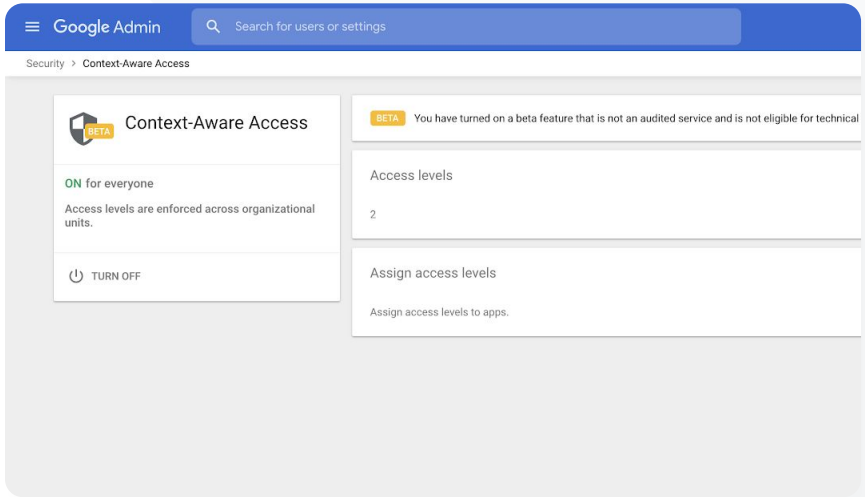
Relevant dokumentasjon i brukerstøtten

- Oversikt over kontekstsensitiv tilgang
- Tilordne apper nivåer for kontekstsensitiv tilgang

Veiledning: Begrens appbruken i Google Workspace

Slik bruker du kontekstsensitiv tilgang

- Logg på **administrasjonskonsollen.**
- Velg **Sikkerhet** > **Kontekstsensitiv tilgang** > **Tilordne.**
- Velg **Tilordne tilgangsnivåer** for å se listen over apper.
- Velg en **organisasjonsenhet eller konfigurasjonsgruppe** for å sortere listen.
- Velg **Tilordne** ved siden av appen du vil endre tilordning for.
- Velg ett eller flere tilgangsnivåer.
- Opprett flere nivåer hvis du vil at brukerne skal oppfylle flere betingelser.
- Klikk på **Lagre.**



Relevant dokumentasjon i brukerstøtten

- Oversikt over kontekstsensitiv tilgang
- Tilordne apper nivåer for kontekstsensitiv tilgang

“Jeg vil implementere en ny plan for lagringsbehandling på domenet mitt.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Lagringsveiledning for administratorer
- Få innsikt i tilgjengelig lagringsplass og bruk
- Frigjør eller få mer plass
- Angi lagringsgrenser

Administrer lagring på domenet ditt

Institusjoner med Google Workspace for Education har en grunnkvote på 100 TB felles lagringsplass. Det er nok lagringsplass til ca. drøye 100 millioner dokumenter, 8 millioner presentasjoner eller 400 000 timer med video. **Administrer felles Disk-lagring** for å sikre at institusjonen din bruker lagringsplassen effektivt.

Med administratorverktøy, rapporter og logger kan du gjøre dette:

- få oversikt over hvor mye lagringsplass du bruker
- angi lagringsgrenser
- identifisere kontoer som bruker urimelig mye lagringsplass

Med Teaching and Learning Upgrade og Education Plus får du ekstra lagringsplass i tillegg til grunnkvoten

- Med Teaching and Learning Upgrade får du 100 GB ekstra delt lagringsplass per lisens.
- Med Education Plus får du 20 GB ekstra delt lagringsplass per lisens.

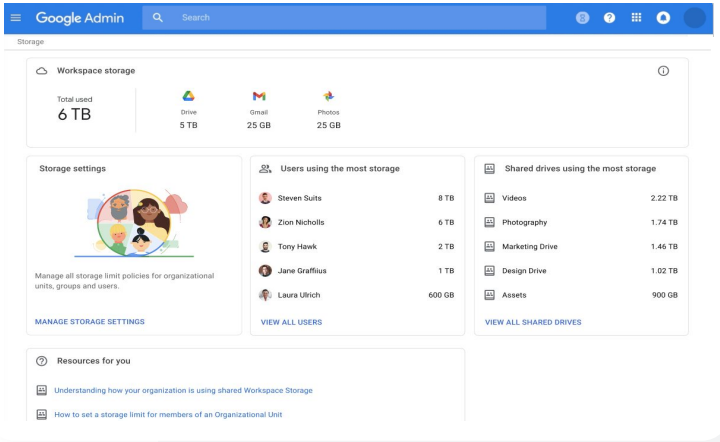
Veiledning: Administrer lagring på domenet ditt

Finn ut hvor mye lagringsplass de enkelte brukerne bruker

- Logg på **administrasjonskonsollen** > gå til **Meny** > **Lagring.**
- Vis bruken av lagringsplass etter organisasjon og bruker.

Angi lagringsgrenser

- Gå til **administrasjonskonsollen** > **Meny** > **Lagring.**
- I **Innstillinger for lagring** klikker du på **Administrer**
- Klikk på **Lagringsgrense for brukere** > velg enheten du skal angi en grense for:
  - Organisasjonsenhet: Klikk på **organisasjonsenheten.**
  - Gruppe: Klikk på **Grupper** > Klikk på **søkefeltet** > skriv inn **navnet på gruppen** > klikk på **gruppen.**
- Velg **På** og **angi mengden lagringsplass.**
- Klikk på **Lagre.**



Relevant dokumentasjon i brukerstøtten

- Lagringsveiledning for administratorer
- Få innsikt i tilgjengelig lagringsplass og bruk
- Frigjør eller få mer plass
- Angi lagringsgrenser

> Dataene til elever, ansatte og lærere må forbli i EU i henhold til gjeldende lov og rett."

Regelverk for data

Som administrator kan du velge å lagre data på et bestemt geografisk sted, enten i USA eller Storbritannia/Europa, ved å bruke **innstillinger for dataregioner**.

- Education Plus- og Education Standard-brukere kan velge én dataregion for noen av brukerne, eller forskjellige dataregioner for bestemte avdelinger, og se fremdriften etter som data flyttes mellom regioner.
- Legg til brukere i organisasjonsenheter for å gruppere dem etter avdeling, eller legg dem til i konfigurasjonsgrupper for å samle brukere innad eller på tvers av avdelinger.
- Brukere som ikke har Education Standard- eller Education Plus-lisenser, dekkes ikke av innstillinger for dataregioner.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Velg en geografisk posisjon for dataene dine

“Forskningen til de ansatte må forbli i USA på grunn av gjeldende regler for tilskudd.”

Regler for tilskudd

Som administrator kan du velge å lagre forskningsdata på et bestemt geografisk sted (enten i USA eller Storbritannia/Europa) ved å bruke en **innstilling for dataregioner**.

- Innstillinger for dataregioner dekker inaktive primærdata (inkludert sikkerhetskopier) for de fleste kjernetjenestene i Google Workspace for Education, som står oppført her.
- Tenk over innvirkningene før du angir innstillinger for dataregioner, siden brukere utenfor regionen der dataene oppbevares, kan oppleve lengre tidsforsinkelser i noen tilfeller.

Trinnvis veiledning

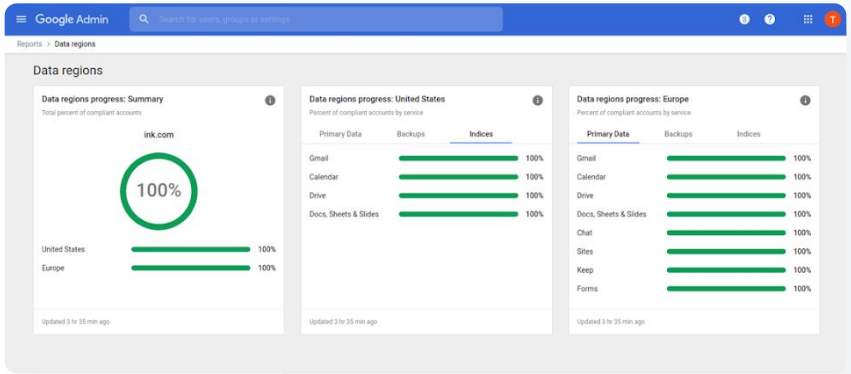
Relevant dokumentasjon i brukerstøtten

- Velg en geografisk posisjon for dataene dine

Veiledning: Regelverk for data

Slik definerer du dataregioner

- Logg på **administrasjonskonsollen.**
  - Merk: Du må være logget på som superadmin.
- Klikk på **Bedriftsprofil** > **Vis mer** > **Dataregioner.**
- Velg **organisasjonsenheten eller konfigurasjonsgruppen** du vil begrense til en region, eller velg hele kolonnen for å inkludere alle enheter og grupper.
- Velg regionen din, for eksempel **Ingen preferanse, USA, Europa.**
- Klikk på **Lagre.**



Relevant dokumentasjon i brukerstøtten

- Velg en geografisk posisjon for dataene dine

Administrer endepunktenheter

Ved å bruke **administrering av endepunkter for bedrifter** kan du få mer kontroll over organisasjonens data via mobilenheter. Begrens funksjoner på mobilenheter, gjør enhetskryptering obligatorisk, administrer apper på Android-enheter, iPhone og iPad, og slett data fra enheter.

- Du kan godkjenne, blokkere, oppheve blokkeringen av eller slette enheter via administrasjonskonsollen.
- Hvis noen mister en enhet eller slutter på skolen, kan du viske ut brukerens konto, profil – eller til og med alle data – fra den spesifikke administrerte modulenheten. Slike data er fortsatt tilgjengelige på datamaskiner og i nettlesere.

> Jeg trenger en metode for å administrere og implementere regler på alle typer enheter i skoleregionen – ikke bare Chromebook, men også enheter med iOS, Windows 10 osv. – spesielt hvis en av dem blir utsatt for sikkerhetsbrudd.”

Trinnvis veiledning

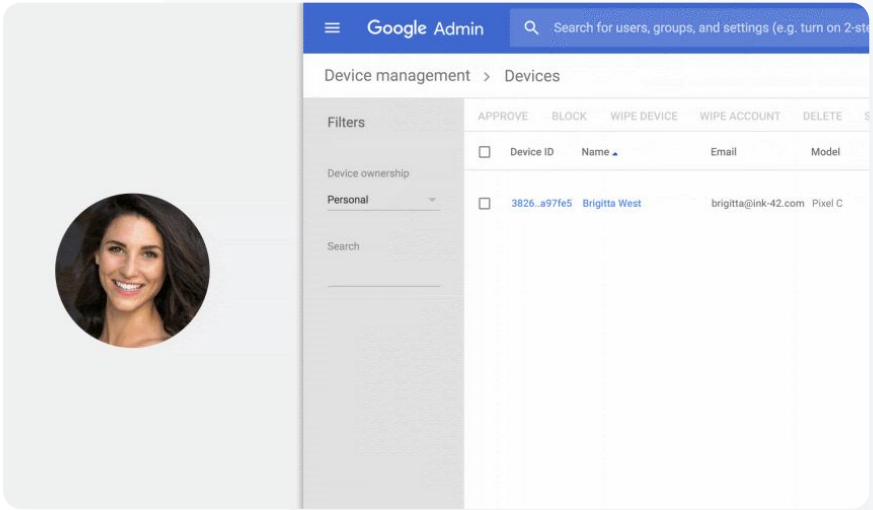
Relevant dokumentasjon i brukerstøtten

- Administrer enheter med administrering av endepunkter for Google
- Konfigurer avansert administrering av mobilenheter

Veiledning: Administrer endepunktenheter

Fremgangsmåte for avansert administrering av mobilenheter

- Logg på **administrasjonskonsollen**
- Gå til **Administrasjonskonsoll** > **Enheter**
- Til venstre klikker du på **Innstillinger** > **Universelle innstillinger**
- Klikk på **Generelt** > **Administrering av mobilenheter**
- Hvis du skal implementere disse innstillingene for alle, må den øverste organisasjonsenheten være avmerket. Hvis ikke velger du en underordnet organisasjonsenhet
- Velg **Avansert**
- Klikk på **Lagre**



Relevant dokumentasjon i brukerstøtten

- Administrer enheter med administrering av endepunkter for Google
- Konfigurer avansert administrering av mobilenheter

Administrer Microsoft Windows-enheter

Administrer og sikre Windows 10-enhetene til institusjonen via administrasjonskonsollen, akkurat som du gjør for Android-, iOS-, Chrome- og Jamboard-enheter.

> Noen av lærerne mine bruker Windows 10-enheter. Hvordan kan jeg administrere alle enhetene til institusjonen på samme sted?"

- Slå på global pålogging, slik at det blir enklere for brukerne å få tilgang til Google Workspace på Windows 10-enheter
- Sørg for at alle enheter med tilgang til Google Workspace er oppdaterte, sikre og i tråd med standardene ved å administrere enhetene i administrasjonskonsollen
- Du kan viske ut Windows 10-enheter og sende konfigurasjonsoppdateringer med mer til dem fra nettskyen

Trinnvis veiledning

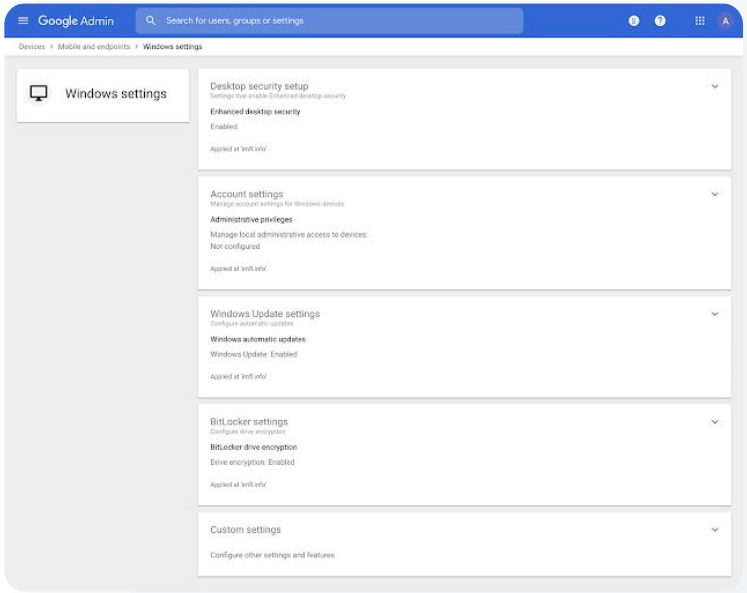
Relevant dokumentasjon i brukerstøtten

- Slå på Administrering av Windows-enheter
- Registrer enheter for Windows-enhetsadministrering

Veiledning: Administrer Microsoft Windows-enheter

Slå på Administrering av Windows-enheter

- I **administrasjonskonsollen** går du til **Meny** > **Enheter** > **Mobilenheter og endepunkter** > **Innstillinger** > **Windows-innstillinger**
- Velg **Konfigurering av Windows-administrering**
- Hvis du skal implementere denne innstillingen for alle, må den øverste organisasjonsenheten være avmerket
- Ved siden av **Administrering av Windows-enheter** velger du **Aktivert**
- Klikk på **Lagre**



Relevant dokumentasjon i brukerstøtten

- Slå på Administrering av Windows-enheter
- Registrer enheter for Windows-enhetsadministrering

“Hvordan kan jeg konfigurere wifi-profiler på Windows 10-enhetene mine?”

Egendefinerte innstillinger for Windows 10-enheter

Med Googles administrering av Windows-enheter kan administratorer legge til egendefinerte innstillinger i enhetsflåten sin.

- Kontroller egendefinerte innstillinger fra administrasjonskonsollen
- Legg til innstillinger for følgende:
  - administrering av enheter
  - sikkerhet
  - maskinvare og nettverk
  - programvare
  - personvern

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

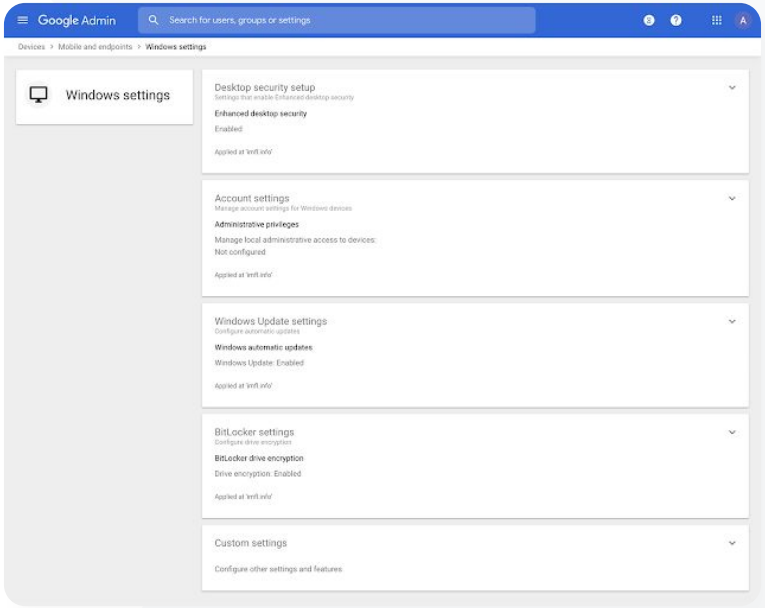
- Vanlige egendefinerte innstillinger
- Legg til egendefinerte innstillinger

Veiledning: Egendefinerte innstillinger for Windows 10-enheter

Legg til en ny egendefinert innstilling

- I **administrasjonskonsollen** går du til **Meny** > **Enheter** > **Mobilenheter og endepunkter** > **Innstillinger** > **Windows-innstillinger**
- Velg **Egendefinerte innstillinger**
- Klikk på **Legg til en egendefinert innstilling** > og fyll ut de nødvendige feltene
- Klikk på **Neste**
- Velg **organisasjonsenheten** som innstillingen skal gjelde for
- Klikk på **Bruk**

Vær oppmerksom på at Google ikke tilbyr teknisk støtte for tredjepartsprodukter eller -innstillinger, og heller ikke tar ansvar for disse.



Relevant dokumentasjon i brukerstøtten

- Vanlige egendefinerte innstillinger
- Legg til egendefinerte innstillinger

“Jeg vil sikre at Windows 10-enhetene i enhetsflåten min får de nyeste oppdateringene.”

Automatiser oppdateringer for Windows 10-enheter

Angi når og hvordan institusjonens Windows 10-enheter mottar sikkerhetsoppdateringer og andre viktige nedlastinger via den automatiske oppdateringstjenesten til Windows.

- Konfigurer varsler om nedlasting av oppdateringer fra Windows Update-kontrollpanelet, angi tidsperioder der omstart etter oppdatering ikke skal forekomme, og mye mer
- Legg til innstillinger for hele institusjonen eller for bestemte organisasjonsenheter
- Det kan ta opptil 24 timer før endringene trer i kraft, men som regel går det mye kjappere

Trinnvis veiledning

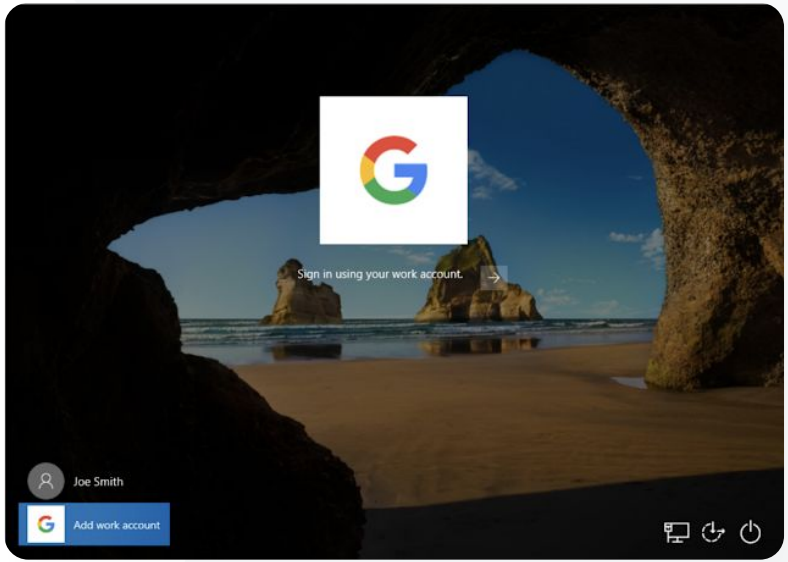
Relevant dokumentasjon i brukerstøtten

- Administrer automatiske oppdateringer

Veiledning: Automatiser oppdateringer for Windows 10-enheter

Konfigurer oppdateringer

- I **administrasjonskonsollen** går du til **Meny** > **Enheter** > **Mobilenheter og endepunkter** > **Innstillinger** > **Windows-innstillinger**
- Velg **Innstillinger for Windows Update** > **Aktivert**
- Ved siden av **Administrering av Windows-enheter** velger du **Aktivert**
- Konfigurer alternativene nedenfor, blant annet disse:
  - Godta oppdateringer for Microsoft-apper
  - Atferd for automatiske oppdateringer
  - Frekvens for automatiske oppdateringer
- Klikk på **Lagre**



Relevant dokumentasjon i brukerstøtten

- Administrer automatiske oppdateringer

“Jeg vet at Google overholder de høyeste standardene for datakryptering, men jeg ønsker å kontrollere krypteringsnøklene for universitetets åndsverk og stipendforskning.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Om kryptering på klientsiden

Dra nytte av kryptering på klientsiden

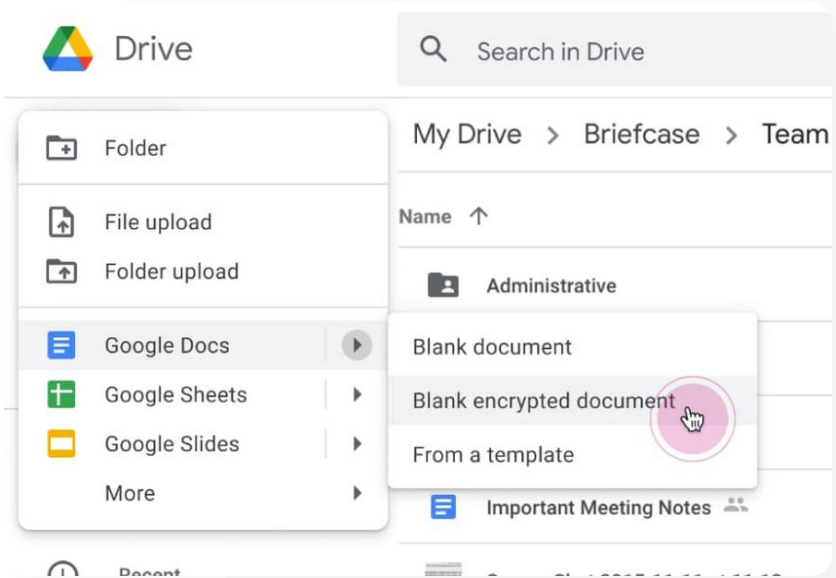
Google Workspace bruker allerede de nyeste kryptografiske standardene til å kryptere alle inaktive data og data under overføring mellom egne tjenere. Med **kryptering på klientsiden** kan administratorer ta direkte kontroll over krypteringsnøklene og identitetsleverandøren som brukes for å få tilgang til disse nøklene.

- Bruk dine egne krypteringsnøkler til å kryptere sensitive data, for eksempel institusjonens åndsverk
- Innholdskrypteringen foregår i nettleseren din før dataene overføres eller lagres på Googles skybaserte lagringsplass
- Velg hvilke brukere som kan opprette innhold som krypteres på klientsiden, og som kan dele det internt eller eksternt

Veiledning: Dra nytte av kryptering på klientsiden

Konfigurer kryptering på klientsiden

- Konfigurer krypteringsnøkkeltjenesten din
  - Beskytt dataene dine med nøkkeladministrasjon og kontrollfunksjoner ved å opprette en nøkkeltjeneste
- Koble Google Workspace til den eksterne nøkkeltjenesten
  - Legg til og administrer nøkkeltjenester for kryptering på klientsiden ved å inkludere nettadressen for nøkkeltjenestene i administrasjonskonsollen
- Tilordne nøkkeltjenesten til organisasjonsenheter eller grupper
  - Angi én nøkkeltjeneste som standardtjenesten for hele insitusjonen
- Koble Google Workspace til identitetsleverandøren din
  - Koble til identitetsleverandøren for kryptering på klientsiden for å bekrefte identiteten til brukerne før de kan kryptere innhold eller få tilgang til kryptert innhold
- Slå på kryptering på klientsiden
  - Slå på kryptering på klientsiden, slik at organisasjonsenheter eller grupper av brukere som trenger det, kan opprette innhold som krypteres på klientsiden

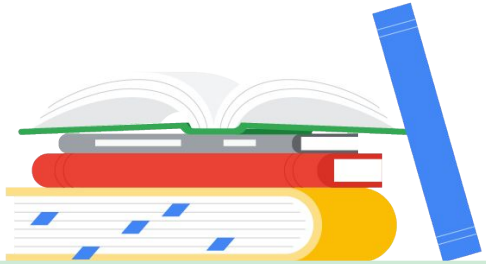


Relevant dokumentasjon i brukerstøtten

- Om kryptering på klientsiden

Undervisnings- og læringsfunksjoner

Gi lærerne tilgang til flere funksjoner i det digitale læringsmiljøet med engasjerende undervisningsressurser, verktøy som fremmer faglig integritet og avansert videokommunikasjon.

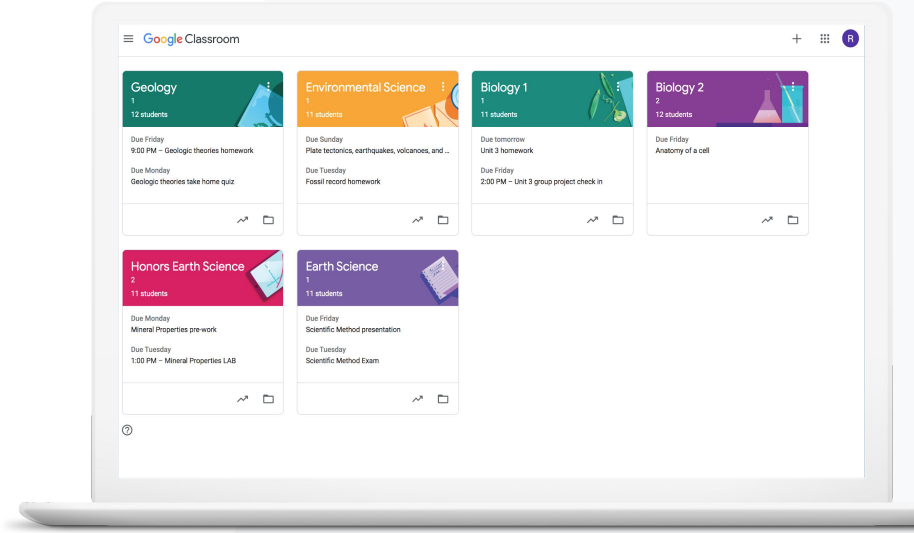


- Google Classroom
- Plagiatrapporter
- Dokumenter, Regneark og Presentasjoner
- Google Meet

Google Classroom

Hva er dette?

Google Classroom er et sentralt sted for undervisning og læring. De betalte funksjonene i Classroom gjør det enklere å samle kursverktøyene på ett sted. Lærerne får direkte tilgang til favorittverktøyene sine i Classroom, og kan synkronisere klasselistene med eksterne systemer.



Bruksmønstre

Administrer tilgang til Classroom-tillegg	Trinnvis veiledning
Integrer engasjerende innhold i Classroom	Trinnvis veiledning
Opprett kurs i stor skala	Trinnvis veiledning

> Jeg skulle ønske jeg kunne gi lærerne tilgang til undervisningsverktøyene de foretrekker, med global pålogging. ”

Administrer tilgang til Classroom-tillegg

Bestem hvilke utdanningsapper fra tredjeparter som skal være tilgjengelige for institusjonen din, med en **godkjenningsliste for domener.** Gjør det enkelt for lærerne å installere tillegg og inkludere dem i elevenes oppgaver med noen få klikk.

- Opprett en godkjenningsliste for domenet for å bestemme hvilke tredjepartsapper lærerne kan installere fra Google Workspace Marketplace
- Gi elevene bedre læringsutbytte med flere utdanningsapper. Lærerne kan tildele, vurdere og sette karakterer på oppgaver direkte i Google Classroom
- Google Workspace Marketplace inkluderer Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Arts & Culture, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora, Wordwall med mer

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Administrer Google Workspace Marketplace-apper
- Bruk tillegg i Classroom
- Administrer Marketplace-appene på godkjenningslisten din
- Distribuer Marketplace-apper til brukerne
  - Classroom-tillegg [Startveiledning for lærere]

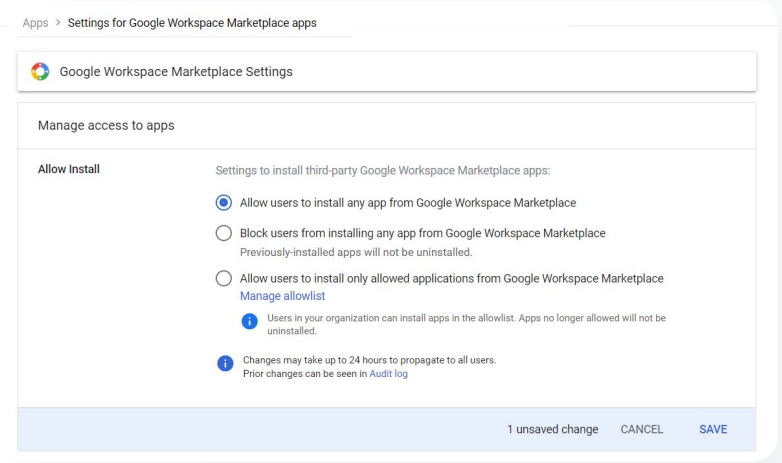
Veiledning: Administrer tilgang til Classroom-tillegg

Administrer tilgang til tillegg med en godkjenningsliste for domener

- I administrasjonskonsollen velger du **Meny** > **Google Workspace Marketplace-apper** > **App-liste**
- Velg **Sett apper på godkjenningslisten**
- Skriv inn navnet på eller søk etter tillegget du ønsker
- Klikk på **Velg** og kontroller at **Tillat at brukere installerer denne appen** er merket av
- Klikk på **Fortsett** og **Fullfør**

Gi tilgang til tillegg for ønsket godkjenningsliste

- I administrasjonskonsollen velger du **Meny** > **Google Workspace Marketplace-apper** > **App-liste**
- Velg tillegget du ønsker å distribuere
- Under **Brukertilgang** klikker du på **Se organisasjonsenheter og grupper**
- Du kan velge å gi **tilgang til alle** eller å begrense tilgangen til **utvalgte grupper** eller **organisasjonsenheter**
- Klikk på **Lagre**



Relevant dokumentasjon i brukerstøtten

- Administrer Google Workspace Marketplace-apper
- Bruk tillegg i Classroom
- Administrer Marketplace-appene på godkjenningslisten din
- Distribuer Marketplace-apper til brukerne
- Classroom-tillegg [Startveiledning for lærere]

“Jeg ønsker å tildele et pedagogisk Kahoot!-spill til elevene mine og sette karakterer uten å forlate Google Classroom.”

Integrer engasjerende innhold i Classroom

Med **Classroom-tillegg** kan lærere dele engasjerende aktiviteter og innhold med elevene sine ved å legge ved tillegg i oppgaver, spørsmål, materialer og kunngjøringer i Classroom.

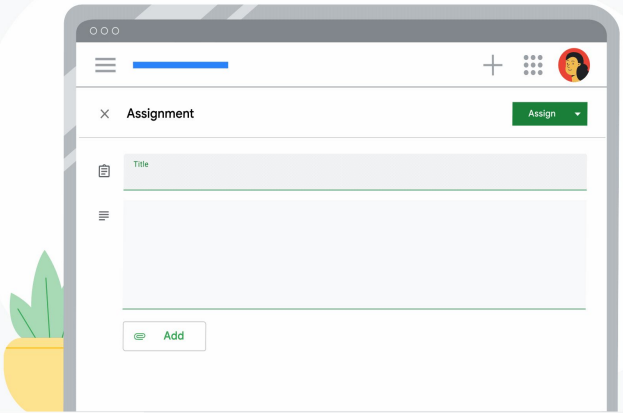
- Gi lærere og elever mulighet til å bruke favorittverktøy, for eksempel Kahoot!, Nearpod og Pear Deck, uten å gå ut av Classroom
- Med tillegg slipper elevene å holde styr på flere passord eller å gå til eksterne nettsteder
- Vurder og gjennomgå elevarbeid fra tillegg – direkte i Classroom

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Bruk tillegg i Classroom
- Classroom-tillegg [Startveiledning for lærere]

Veiledning: Integrer engasjerende innhold i Classroom



Slik legger du ved tillegg i en oppgave, en quiz eller et spørsmål:

- Logg på Classroom-kontoen din på **classroom.google.com**
- Velg det relevante kurset fra listen, og velg **Kursarbeid**
- Velg **Opprett** > velg hva du vil opprette
- Skriv inn en tittel og en veiledning
- Under **Tillegg** velger du tillegget du vil bruke
- Velg **Tildel**

Slik legger du ved tillegg i en kunngjøring:

- På **Strøm**-siden for kurset velger du **Kunngjør noe til kurset ditt**
- Skriv inn kunngjøringen
- Under **Tillegg** velger du tillegget du vil bruke
- Velg **Legg ut**

Relevant dokumentasjon i brukerstøtten

- Bruk tillegg i Classroom
- Classroom-tillegg [Startveiledning for lærere]

> Jeg trenger en metode for å automatisere oppsettet av kurs og administrere klasselister i Google Classroom.»

Opprett kurs i stor skala

Import av klasselister fra systemer for elevinformasjon gjør det mulig å opprette kurs automatisk og synkronisere klasselister med skolens system for elevinformasjon via Clever.

- Tilgjengelig for grunnskoler og videregående skoler i USA og Canada med Education Plus
- Administratorer kan importere klasselister fra skolens system for elevinformasjon til Google Classroom for å konfigurere kurs automatisk
- Automatiser og administrer klasselister sømløst i Google Classroom

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Kom i gang med import av klasselister fra systemer for elevinformasjon
- Konfigurer import av klasselister fra systemer for elevinformasjon via Clever

Veiledning: Opprett kurs i stor skala

Slik konfigurerer du import av klasselister fra systemer for elevinformasjon:

- Konfigurer synkronisering av Google Classroom-klasselister i Clever
- Distriktsadministratoren i Clever og superadministratoren i Google Workspace kan følge den trinnvise veiledningen fra Clever

Gjør følgende hvis skoledistriktet ditt ikke har noen Clever-konto:

- Opprett en Clever-konto

Gjør følgende hvis skoledistriktet ditt har en Clever-konto:

- Be om import av klasselister på Clever-oversikten

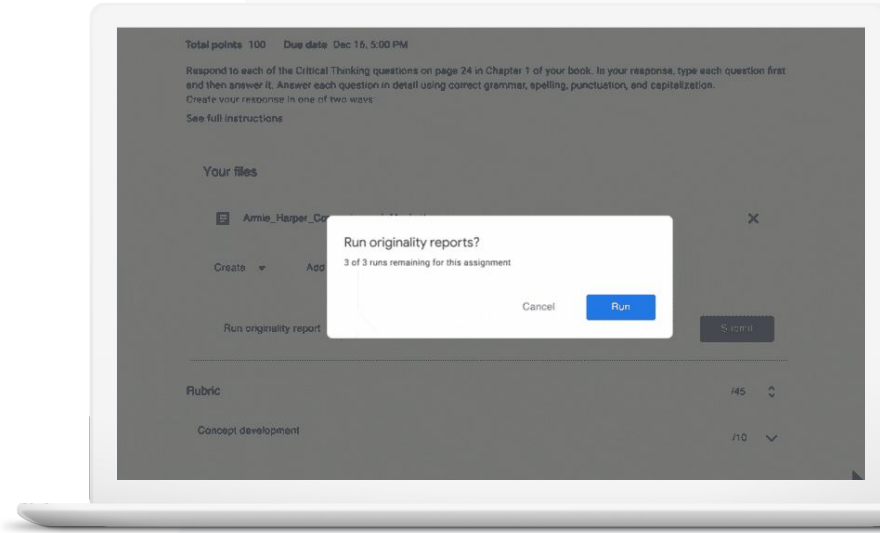
Relevant dokumentasjon i brukerstøtten

- Konfigurer import av klasselister fra systemer for elevinformasjon via Clever

Plagiatrapporter

Hva er dette?

Plagiatrapporter gjør det mulig for lærere og elever å sjekke om arbeid er autentisk ved å bruke Google Søk til å sammenligne elevarbeid med milliarder av nettsider og mer enn 40 millioner bøker. De betalte funksjonene for plagiatrapporter gir ubegrenset tilgang, slik at lærerne kan sammenligne elevenes innleveringer opp mot et repositorium med eldre elevarbeid som eies av skolen.



Bruksmønstre

Se etter plagiering	Trinnvis veiledning
Sjekk originaliteten opp mot tidligere elevarbeid	Trinnvis veiledning
Gjør plagiatkontroll om til en mulighet for læring	Trinnvis veiledning

“Jeg vil se etter plagiering eller ufullstendige kildehenvisninger i elevenes arbeid.”

Se etter plagiering

Lærere kan sjekke om elevenes arbeid er autentisk, ved hjelp av **plagiatrapporter**. Rapporten genererer linker til gjenkjente kilder og merker tekst der kildehenvisning mangler.

- Kjør plagiatrapporter opp mot Dokumenter, Presentasjoner og Microsoft Word-dokumenter.
- Lærere som bruker Teaching and Learning Upgrade eller Education Plus, får dette:
  - ubegrenset tilgang til plagiatrapporter
  - muligheten til å sammenligne fellestrekk mellom elever opp mot et repositorium med eldre elevarbeid som eies av skolen

Du eier alltid dataene dine — det er vårt ansvar å beskytte dem.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Slå på plagiatrapporter
- Plagiatrapporter og personvern

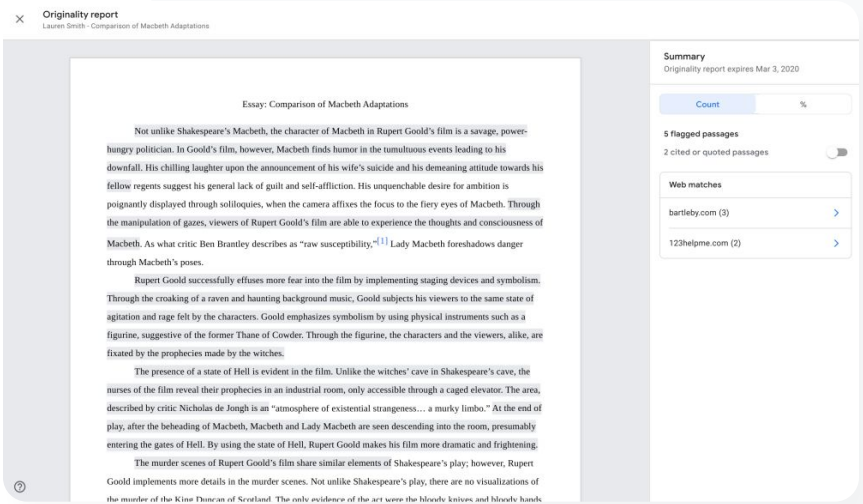
Veiledning: Se etter plagiering

Slå på plagiatrapporter for en oppgave i Classroom

- Logg på Classroom-kontoen din på **classroom.google.com**
- Velg det relevante kurset fra listen, og velg **Kursarbeid**
- Velg **Opprett** > **Oppgave**
- Merk av i boksen ved siden av **Plagiatrapporter** for å slå dette på

Kjør plagiatrapporter på elevarbeid

- Velg den aktuelle elevens fil fra listen, og klikk for å åpne filen i retteverktøyet
- Under elevens oppgave klikker du på **Se etter plagiering**



Slå på plagiatrapporter for en oppgave i læringsplattformen din

- Logg på **læringsplattformen din**
- Velg det relevante **kurset**
- Opprett en oppgave > Velg **Google Oppgaver**
- Merk av i boksen **Slå på plagiatrapporter**

Relevant dokumentasjon i brukerstøtten

- Classroom: Slå på plagiatrapporter
- Google Oppgaver: Slå på plagiatrapporter

“

Hvordan kan jeg gi lærerne mulighet til å sammenligne elevenes arbeid med elevarbeid fra tidligere år for å avdekke plagiering?”

Sjekk originaliteten opp mot tidligere elevarbeid

Samsvar fra skolen i plagiatrapporter gir lærerne muligheten til å sammenligne elevarbeid med tidligere innleveringer ved å gjennomsøke elevens oppgaver opp mot institusjonens private repositorium med elevarbeid.

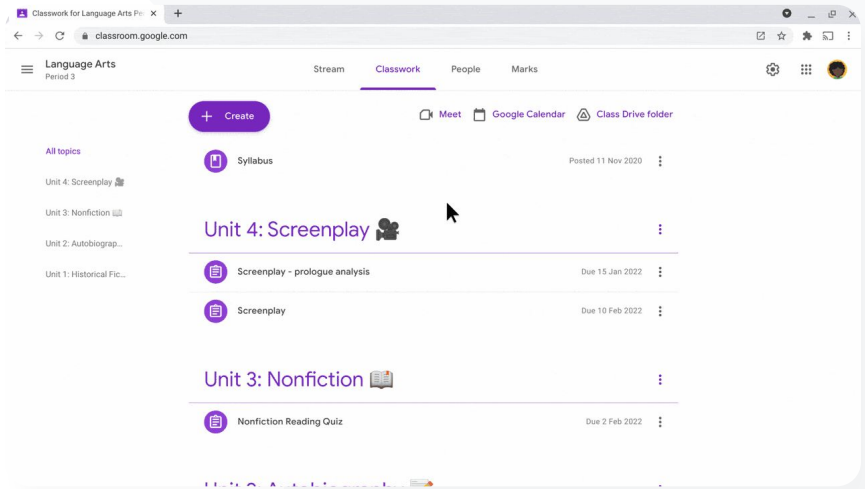
- Sammenlign fellestrekk mellom elever med nytt og eldre elevarbeid for å avdekke plagiering ved hjelp av Teaching and Learning Upgrade eller Education Plus
- Elevarbeid kan lagres trygt og etterfylles i skolens private, domenedekkende repositorium

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Slå på plagiatrapporter
- Slå på samsvar fra skolen for plagiatrapporter i Classroom

Veiledning: Sjekk originaliteten opp mot tidligere elevarbeid



Slik slår du på samsvar fra skolen i plagiatrapporter:

- I administrasjonskonsollen velger du **Meny** > **Apper** > **Tilleggstjenester fra Google** > **Classroom**
- Velg **lærernes organisasjonsenhet**
- Klikk på **Plagiatrapporter** > merk av i boksen **Slå på samsvar fra skolen i plagiatrapporter**
- Klikk på **Lagre**

Relevant dokumentasjon i brukerstøtten

- Slå på samsvar fra skolen for plagiatrapporter i Classroom

“Jeg ønsker at elevene mine skal få muligheten til å lære hvordan de bruker kildehenvisninger på riktig måte.”

Gjør plagiatkontroll om til en mulighet for læring

Elever kan finne innhold uten kildehenvisninger samt utilsiktet plagiering før de leverer inn arbeid, ved å kjøre en **plagiatrapport** opptil tre ganger per oppgave. Med plagiatrapporter sammenlignes elevenes arbeid med ulike kilder, og tekst uten kildehenvisning blir flagget. På den måten kan de få ny innsikt, rette opp i feil og trygt levere inn arbeidet sitt.

- I både Teaching and Learning Upgrade og Education Plus kan lærere bruke plagiatrapporter så ofte de vil, mens i Education Fundamentals kan de bare slå på denne funksjonen fem ganger per kurs.
- Når du har levert inn arbeid, kjører Classroom automatisk en rapport som bare læreren kan se. Hvis du trekker tilbake en oppgave og leverer den på nytt, kjører Classroom en ny plagiatrapport for læreren.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

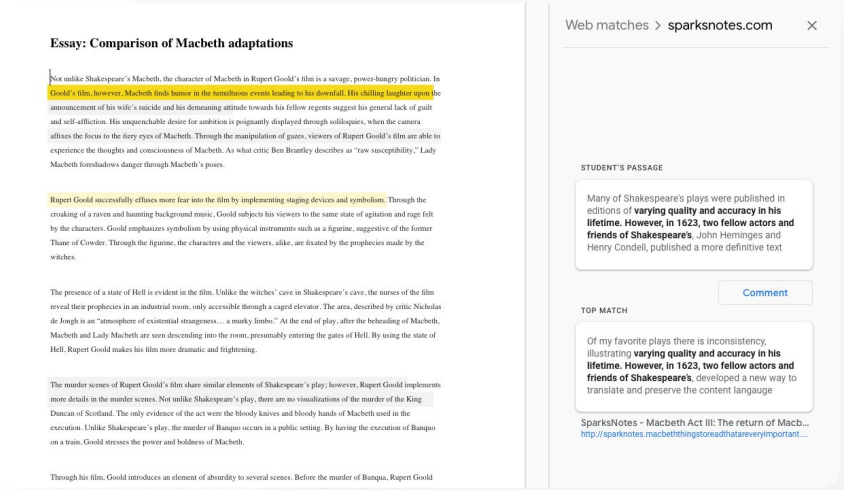
- Kjør plagiatrapporter på arbeidet ditt

Veiledning: Gjør plagiatkontroll om til en mulighet for læring

Slik kan elevene kjøre plagiatrapporter i Classroom:

- Logg på Classroom-kontoen din på classroom.google.com.
- Velg det relevante kurset fra listen, og velg **Kursarbeid**
- Velg den relevante oppgaven fra listen, og klikk på **Se oppgaven**
- Gå til **Arbeidet ditt** og velg å **laste opp** eller **opprette en fil**
- Ved siden av **Plagiatrapporter** klikker du på **Kjør**
- For å åpne rapporten klikker du på **Se plagiatrapporten** under navnet på oppgavefilen
- For å endre flaggede tekststykker og sørge for at de har riktige kildehenvisninger klikker du på **Rediger** nederst

Elevene kan kjøre plagiatrapporter på læringsplattformen sin ved hjelp av Google Oppgaver.



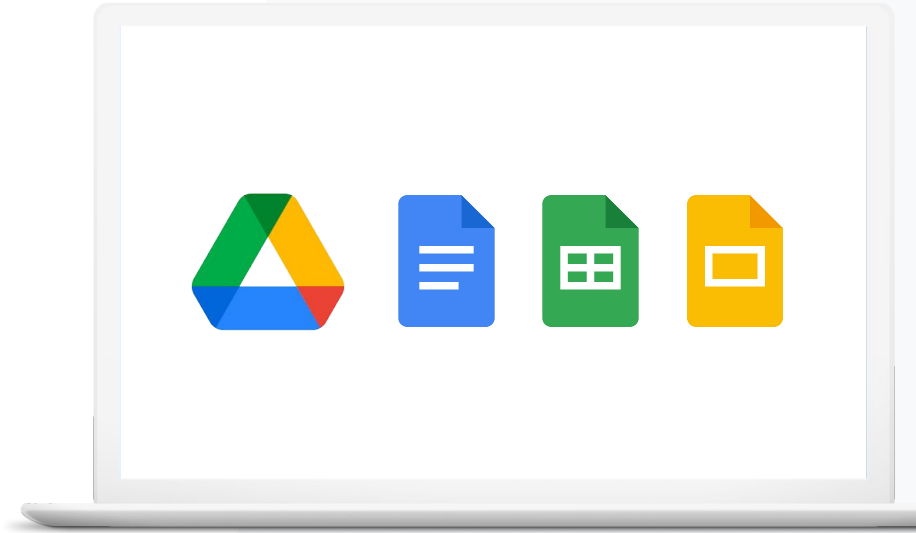
Relevant dokumentasjon i brukerstøtten

- Kjør plagiatrapporter i Classroom
- Kjør plagiatrapporter på læringsplattformen din

Dokumenter, Regneark og Presentasjoner

Hva er dette?

Med Dokumenter, Regneark og Presentasjoner kan skolefellesskapet samarbeide, skape, gjennomgå og redigere samtidig i sanntid. Med betalte funksjoner i Education Plus kan lærere og administratorer innføre en godkjenningsprosess for intern dokumentasjon på institusjonen.



Bruksmønstre

Godkjenn interne dokumenter — Trinnvis veiledning

“

Naturfagsavdelingen er i ferd med å utvikle et nytt pensum.

Hvordan kan de sikre at pensumforslaget deres godkjennes av alle avdelingslederne?”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Administrer godkjenninger

Godkjenn interne dokumenter

Med **godkjenninger** kan skolefellesskapet sende dokumenter i Google Disk gjennom en formell godkjenningsprosess.

- Brukere som gjennomgår dokumentene, kan godkjenne, avvise eller gi tilbakemeldinger på dem direkte i Disk, Dokumenter og andre Google Workspace-apper
- Godkjennerne følger en link til dokumentet. Her kan de gjennomgå dokumentet, legge inn kommentarer og avvise eller godkjenne dokumentet
- Administrer godkjenninger for kontrakter eller nyansettelser, godkjenn endringer for dokumenter før publisering, med mer

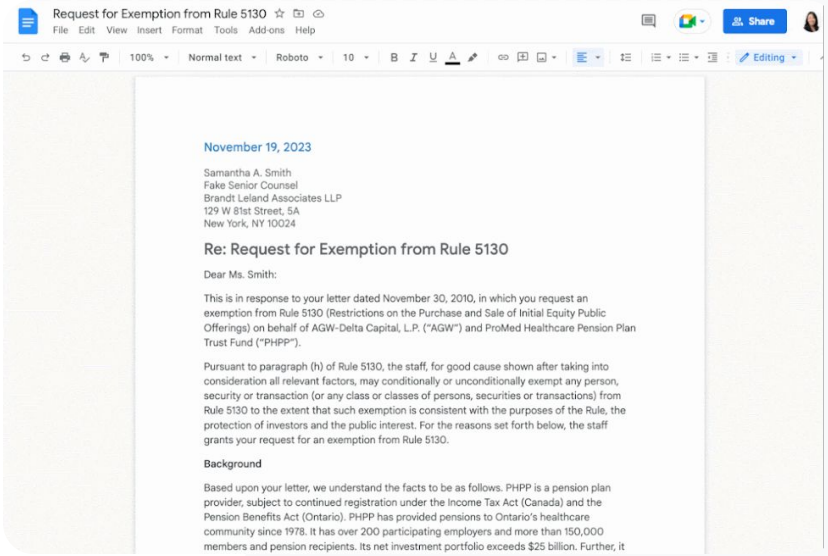
Veiledning: Godkjenn interne dokumenter

Slik fungerer det

Administratorer kan kontrollere hvordan brukere og filer inngår i godkjenningsprosessen.

Slik administrerer du godkjenninger:

- Logg på **administrasjonskonsollen** > gå til **Meny** > **Apper** > **Google Workspace** > **Disk og Dokumenter**
- Klikk på **Godkjenninger**
- Hvis du skal implementere innstillingen for alle, velger du en underordnet **organisasjonsenhet** eller en **konfigurasjonsgruppe**
- Klikk på **Lagre**



Relevant dokumentasjon i brukerstøtten

- Administrer godkjenninger

Google Meet

Hva er dette?

Blant de avanserte funksjonene i Google Meet finner du direktesending, grupperom, større møter, møteopptak og direkteoversatt teksting.

Bruksmønstre

Ta opp møter	Trinnvis veiledning	Still spørsmål	Trinnvis veiledning
Henvis til klassediskusjoner	Trinnvis veiledning	Innsamling av innspill	Trinnvis veiledning
Fjern språkbarrierer	Trinnvis veiledning	Små elevgrupper	Trinnvis veiledning
Kringkast samlinger og skolearrangementer	Trinnvis veiledning	Sporing av deltakelse	Trinnvis veiledning

Ta opp møter

Med Teaching and Learning Upgrade og Education Plus kan lærerne ta opp leksjoner, personalmøter, kurs for faglig utvikling med mer. Møtene lagres automatisk i Disk.

- Opptak lagres i møtearrangørens Disk. Sjekk at du har nok plass på Disk før opptaket
- Vi anbefaler at IT-administratorene kun gir personale og lærere muligheten til å ta opp

> Institusjonen vår tilbyr store nettkurs for faglig utvikling, og vi ønsker å ta opp disse for lærerne som ikke kan delta.”

Trinnvis veiledning

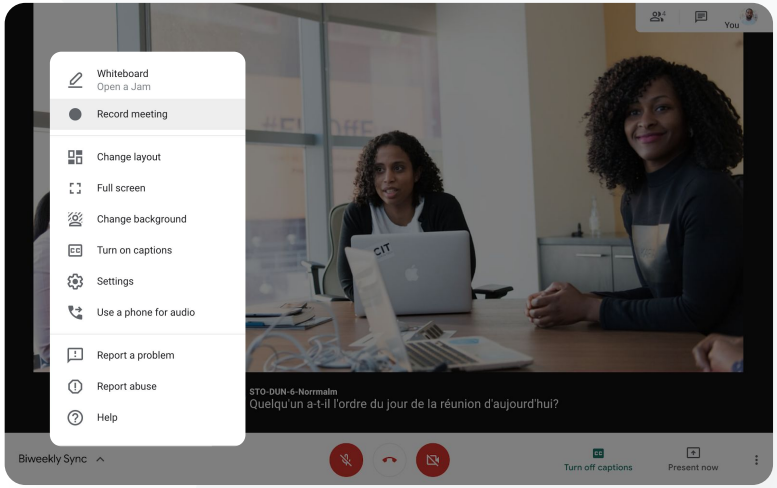
Relevant dokumentasjon i brukerstøtten

- Ta opp videomøter

Veiledning: Ta opp møter

Slik starter du et opptak:

- Start eller bli med i et møte i **Google Meet**
- Klikk på **Aktiviteter** > **Opptak**
- Velg **Start opptak**
- I vinduene som åpnes, klikker du på **Start**
- En rød prikk vises nederst til høyre på skjermen for å indikere at møtet tas opp
- En videofil av møtet lagres automatisk i Disk



Relevant dokumentasjon i brukerstøtten

- Ta opp videomøter

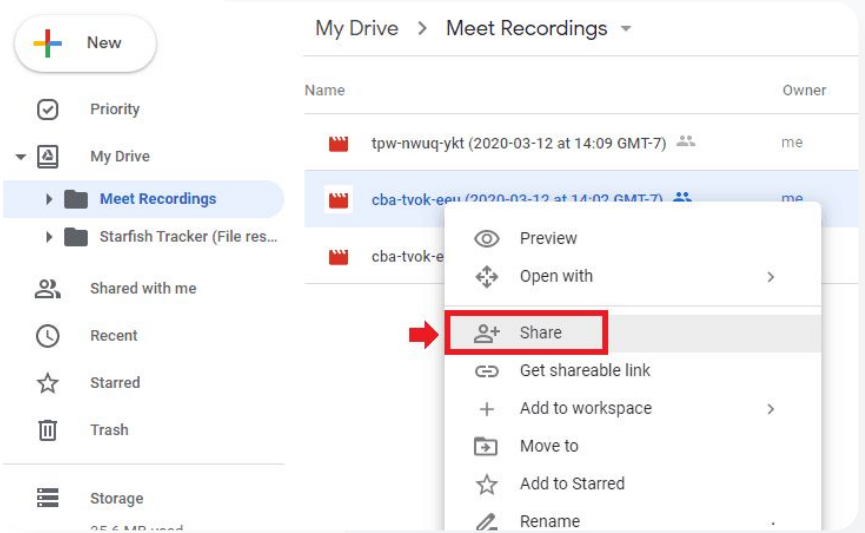
Veiledning: Se og del opptak

Slik starter du et opptak:

- Velg filen
- Klikk på **deleikonet**
- **Legg til** godkjente tilskuere

ELLER

- Velg **linkikonet**
- **Lim inn** linken i en e-post eller chatmelding



Slik laster du ned opptak

- Velg filen
- Klikk på **Mer**-ikonet > Last ned
- **Dobbeltklikk** på den nedlastede filen for å spille den av

Slik spiller du av opptak fra Disk

- I Disk dobbeltklikker du på en opptaksfil for å spille den av. «Behandles fortsatt» vises frem til opptaket kan spilles av på nettet
- For å legge til et opptak i Min disk velger du filen og klikker på **Legg til i Min disk**

Relevant dokumentasjon i brukerstøtten

- Ta opp videomøter

“Hvordan kan jeg transkribere et virtuelt kurs, slik at elevene kan gå gjennom konseptene igjen senere?”

Henvis til klassediskusjoner

Med møtetranskripsjoner kan lærere filme leksjoner og klassediskusjoner automatisk, slik at det blir enklere for elevene å gå gjennom konseptene igjen ved en senere anledning. Transkripsjonene viser hvem som deltok på møtet, og hvem som sa hva.

- Tilgjengelig på engelsk for Google Meet-brukere med stasjonær eller bærbar datamaskin.
- Administratorer kan slå på transkripsjon for skolefellesskapet sitt.
- Transkripsjoner lagres automatisk i møtevertens Disk.
- Når møtetranskripsjon er slått på, vises et transkripsjonsikon øverst til venstre, for alle som deltar på møtet.
- Transkripsjoner inneholder ordene som blir sagt under et møte. Hvis du vil ha en transkripsjon av chatmeldinger, må du ta opp møtet.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Bruk transkripsjon med Google Meet
- Slå transkripsjon på eller av

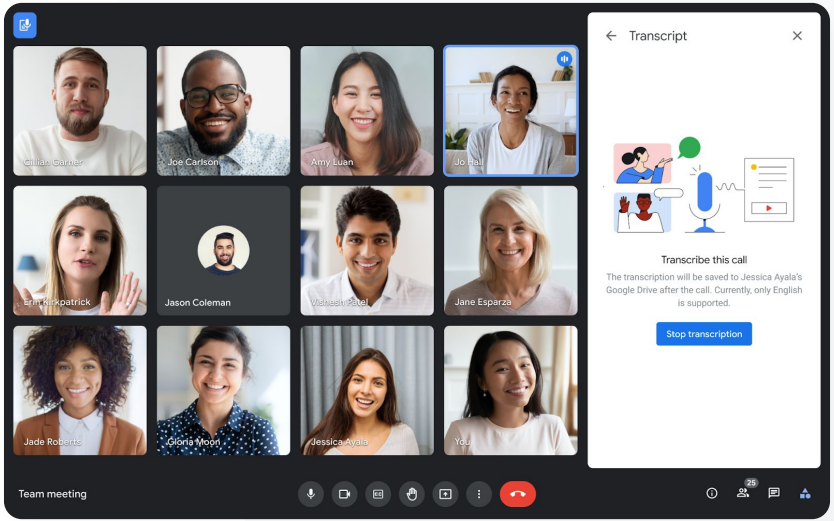
Veiledning: Henvis til klassediskusjoner

Slik slår du på transkripsjoner i Google Meet:

- Under et møte velger du **aktivitetsikonet** nederst til høyre
- Klikk på **Transkripsjoner** > **Start transkriberingen** > **Start**

Slik stopper du transkripsjoner i Google Meet:

- Velg **aktivitetsikonet** > **Transkripsjoner** > **Stopp transkriberingen** > **Stopp**



Relevant dokumentasjon i brukerstøtten

- Bruk transkripsjon med Google Meet
- Slå transkripsjon på eller av

“

Vi avholder virtuelle foreldremøter, men noen ganger snakker ikke alle samme språk.

Hvordan kan jeg gjøre møtene inkluderende og fjerne språkbarrierene?”

Fjern språkbarrierer

Oversatt teksting gjør møtene mer inkluderende ved å fjerne eventuelle språkbarrierer. Når møtedeltakerne får innholdet presentert på det språket de ønsker, får alle like muligheter til informasjonsdeling, læring og samarbeid.

- Lærere kan kommunisere med elever, foreldre og interessenter i fellesskapet som snakker et annet språk
- Bruk oversatt teksting til å oversette engelsk til fransk, tysk, portugisisk og spansk, eller omvendt
- Du kan også oversette engelsk til japansk, mandarin og svensk

Trinnvis veiledning

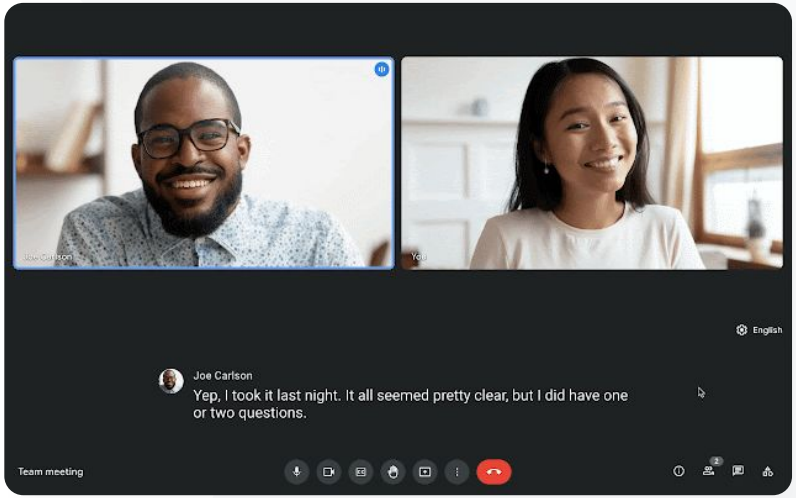
Relevant dokumentasjon i brukerstøtten

- Bruk oversatt teksting i Google Meet

Veiledning: Fjern språkbarrierer

Slik slår du på oversatt teksting:

- Under et møte klikker du på **Flere alternativer** nederst på skjermen > **Innstillinger** > **Teksting**
- Slå på **teksting**
- Velg **språket som snakkes på møtet**
- Slå på **oversatt teksting**
- Velg **språket du vil oversette til**



Relevant dokumentasjon i brukerstøtten

- Bruk oversatt teksting i Google Meet

> Vi må ha muligheten til å direktesende personal- og lærermøter til en stor gruppe interessenter og til foreldre.”

Kringkast samlinger, skolearrangementer og møter

Direktesend til opptil 10 000 seere med Teaching and Learning Upgrade og opptil 100 000 seere med Education Plus. Deltakere kan bli med ved å velge linken til direktesendingen i e-posten fra arrangøren eller i kalenderinvitasjonen.

- Bestem hvor mange direktesendingen skal deles med. Angi om sendingen
  - bare skal være synlig for brukere i organisasjonen (på domenet)
  - skal deles med andre klarerte Google Workspace-domener
  - skal kunne sees på YouTube
- Vi anbefaler at IT-administratorene kun gir personale og lærere muligheten til å slå på direktesending
- Hvis en bruker går glipp av direktesendingen, kan hen få tilgang til opptaket av møtet etter at det er ferdig
- Legg til teksting, avstemninger samt spørsmål og svar i direktesendingen for å gjøre den mer inkluderende og engasjerende

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Slå direktesendinger på eller av for Meet
- Direktesend et videomøte

Veiledning: Kringkast samlinger, skolearrangementer og møter

Slik oppretter du en direktesendingsaktivitet:

- Åpne **Google Kalender**
- Velg **+ Opprett** > **Aktivitet** > **Flere alternativer**
- Legg til informasjon om aktiviteten, for eksempel datoen, klokkeslettet og en beskrivelse
- Legg til deltakere som kan delta fullt ut på videomøtet, dvs. deltakere som kan ses, høres og presentere
- Klikk på **Legg til en Google Meet-videokonferanse** > **Meet**
- Ved siden av Bli med via Google Meet velger du **nedoverpilen** og deretter **Legg til direktesending**
- For å invitere så mange personer som er tillatt med den betalte utgaven din, kan du klikke på **Kopiér** og dele nettadressen til direktesendingen
- Velg **Lagre**
- Strømmingen starter ikke automatisk. I møtet velger du **Mer** > **Start strømmingen**

Relevant dokumentasjon i brukerstøtten

- Slå direktesendinger på eller av for Meet
- Direktesend et videomøte

“Jeg trenger en rask løsning for å stille spørsmål, teste elevenes kunnskap og samhandle med klassen for å holde dem engasjert.”

Still spørsmål

Bruk **Spørsmål og svar**-funksjonen i Google Meet for å engasjere elevene og gjøre timene mer interaktive. Lærere får en enda mer detaljert rapport om alle spørsmålene og svarene når den virtuelle timen er over.

- Moderatorer kan stille så mange spørsmål som nødvendig. De kan også filtrere eller sortere spørsmål, merke dem som besvarte samt skjule eller prioritere spørsmål
- Etter hvert møte der det stilles spørsmål, sendes en spørsmålsrapport automatisk til moderatoren via e-post

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Still spørsmål til møtedeltakere i Google Meet

Veiledning: Still spørsmål

Still et spørsmål

- Øverst til høyre i et møte velger du **aktivitetsikonet** > **Spørsmål** (for å slå på Spørsmål og svar velger du **Slå på Spørsmål og svar**)
- For å stille spørsmål klikker du på **Still et spørsmål** nederst til høyre
- **Skriv inn spørsmålene dine** > velg **Legg ut**

Se spørsmålsrapporten

- Etter et møte får moderatorene tilsendt **en spørsmålsrapport på e-post**
- Åpne e-posten > klikk på **rapportvedlegget**

Relevant dokumentasjon i brukerstøtten

- Still spørsmål til møtedeltakere i Google Meet

“Jeg trenger en enkel løsning for å samle inn innspill fra elever og andre lærere mens jeg underviser eller holder personalmøter.”

Innsamling av innspill

Den som planlegger eller starter et virtuelt møte, kan opprette en **avstemning** for møtedeltakerne. Med denne funksjonen kan du samle inn informasjon raskt fra alle elevene eller deltakerne i et møte.

- Moderatorer kan lagre avstemninger som de senere kan legge ut i et møte. De lagres under Avstemninger-delen i virtuelle møter.
- Etter møtet får moderatoren en e-post med en rapport om avstemningsresultatene.

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Hold avstemninger i Google Meet

Veiledning: Samle inn innspill

Lag avstemninger

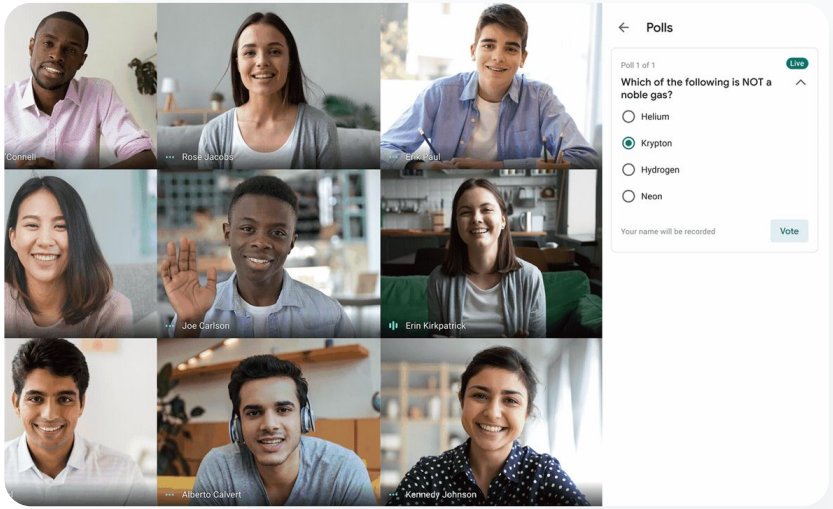
- Øverst til høyre i et møte velger du **aktivitetsikonet** > **Avstemning**
- Velg **Start en avstemning**
- Skriv inn spørsmål
- Velg **Start** eller **Lagre**

Moderer avstemninger

- Øverst til høyre i et møte velger du **aktivitetsikonet** > **Avstemning**
- Hvis du vil la deltakerne se resultatene av en avstemning i sanntid, går du til **Vis resultatene til alle** og **slår på bryteren**
- For å lukke en avstemning og forhindre flere svar, klikker du på **Avslutt avstemningen**
- For å slette en avstemning permanent, velger du **Slett-ikonet**

Se på avstemningsrapporter

- Etter et møte får moderatorene tilsendt **en rapport på e-post**
- Åpne e-posten > velg **rapportvedlegget**



Relevant dokumentasjon i brukerstøtten

- Hold avstemninger i Google Meet

“Noen ganger har vi elever som deltar i undervisningen hjemmefra. Når vi gjør arbeid i små grupper, må jeg enkelt kunne opprette grupperom basert på grupper som er angitt på forhånd.”

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Bruk grupperom i Google Meet

Små elevgrupper

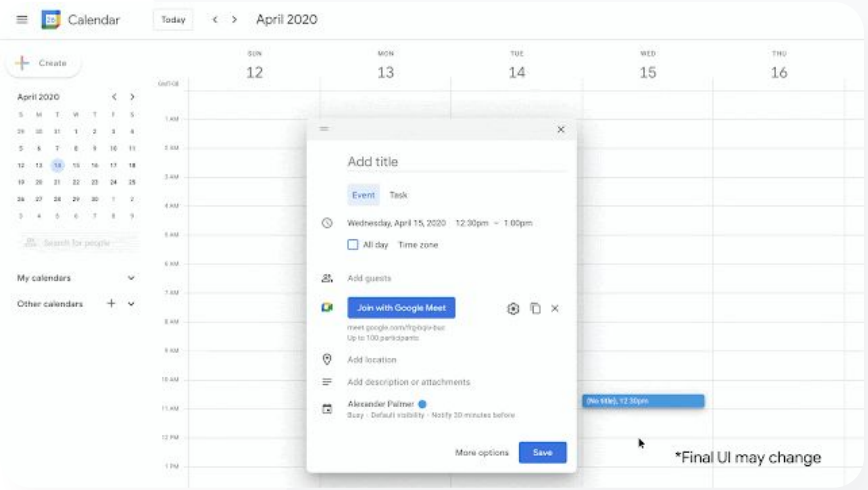
Lærere kan bruke grupperom til å dele elevene inn i mindre grupper når de har virtuell undervisning, **hybridundervisning eller undervisning ansikt til ansikt**. Grupperom må startes av moderatorer i løpet av en videosamtale via en datamaskin.

- Grupperom kan lages på forhånd når et arrangement opprettes, eller mens et møte pågår
- Opprett opptil 100 grupperom per virtuelle møte
- Lærere kan enkelt gå mellom grupperom for å hjelpe til når det trengs
- Administratorer kan velge at bare lærere eller ansatte kan opprette grupperom

Veiledning: Opprett små elevgrupper

Opprett grupperom før møtet

- Opprett en ny aktivitet i Google Kalender
- Klikk på **Legg til en Google Meet-videokonferanse**
- Legg til deltakere > velg **Endre konferanseinnstillingene**
- Klikk på **Grupperom**
- Velg antallet grupperom, og gjør ett av følgende:
  - Dra deltakere til forskjellige rom
  - Skriv inn navn direkte i et rom
  - Klikk på **Fordel tilfeldig** for å fordele deltakere tilfeldig i gruppene
- Klikk på **Lagre**



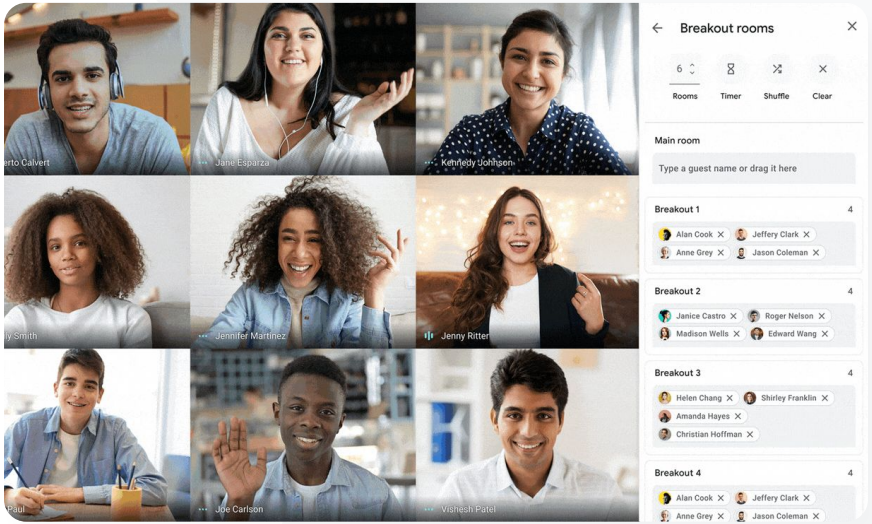
Relevant dokumentasjon i brukerstøtten

- Bruk grupperom i Google Meet

Veiledning: Opprett små elevgrupper

Opprett grupperom under møtet

- Start en videosamtale
- Øverst til høyre velger du **aktivitetsikonet** > **Grupperom**
- I panelet for grupperom **velger du hvor mange grupperom** du trenger
- Elevene fordeles deretter i rommene, men moderatorene kan flytte personer manuelt til andre rom hvis det er nødvendig
- Nederst til høyre klikker du på **Åpne** rom



Svar på spørsmål i ulike grupperom

- Moderatoren får et varsel nede på skjermen når en deltaker ber om hjelp. Velg Bli med for å bli med i den aktuelle deltakerens grupperom.

Relevant dokumentasjon i brukerstøtten

- Bruk grupperom i Google Meet

“

Vi har problemer med å holde oversikt over hvem som deltar i kurs på nettet. Jeg trenger en enkel løsning for å rapportere deltakelsen i kursene på hele domenet.”

Sporing av deltakelse

Oppmøteregistrering oppretter automatisk en rapport om deltakelse for alle møter med fem eller flere deltakere. Rapportene viser hvem som deltok på møtet, deltakernes e-postadresser og hvor lenge de deltok i den virtuelle timen.

- Du kan spore deltakelse på direktesendte aktiviteter med rapporter om direktesendinger
- Moderatorer kan slå oppmøteregistrering og rapporter om direktesendinger av og på i møter og via kalenderaktiviteten

Trinnvis veiledning

Relevant dokumentasjon i brukerstøtten

- Spor deltakelse i Google Meet

Veiledning: Sporing av deltakelse

Slik registrerer du oppmøte i et møte:

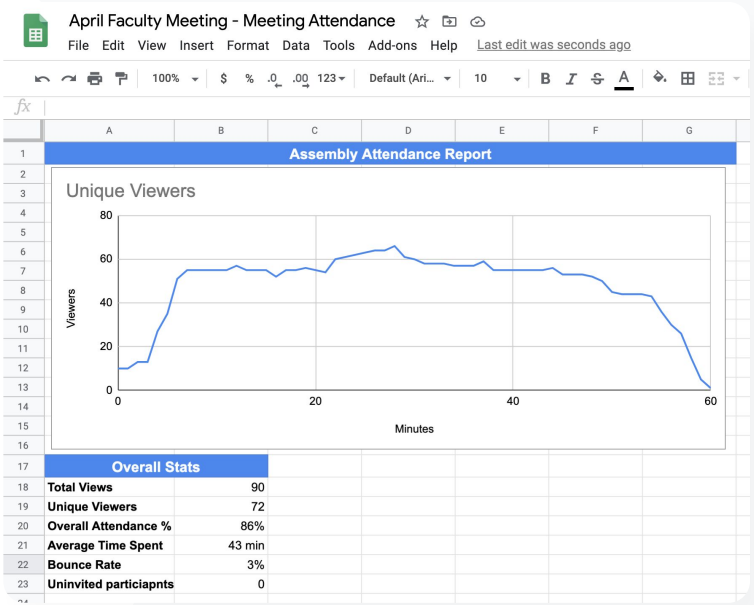
- Start en videosamtale
- Nederst velger du **menyikonet**
- Velg **innstillingsikonet** > **Vertskontroller**
- Slå **Oppmøteregistrering** på eller av

Slik registrerer du oppmøte i Kalender:

- **Slå på Google Meet-konferanser** fra en kalenderaktivitet
- Til høyre velger du **innstillingsikonet**
- Velg boksen ved siden av **Oppmøteregistrering** > klikk på **Lagre**

Få rapporten om deltakelse

- Etter et møte får moderatoren tilsendt **en rapport på e-post**
- Åpne e-posten > velg **rapportvedlegget**



Relevant dokumentasjon i brukerstøtten

- Spor deltakelse i Google Meet

Takk