

Google for Education

Över 30 sätt att använda betalutgåvorna av Google Workspace for Education

goo.gle/use-edu-workspace



Så här ska presentationen användas

Denna presentation består av ett urval av de mest populära användningsfallen som är tillgängliga om du använder någon av **betalutgåvorna av Google Workspace for Education**. Med dessa verktyg kan du öka **datasäkerheten, lärarnas effektivitet, elevernas engagemang, samarbetet i skolan** och mycket annat.

Presentationen är ordnad efter **funktion**, följt av **vanliga användningsfall** och enkla **anvisningar** om hur man använder funktionen. Gå igenom hela presentationen och se allt som går att göra med Google Workspace for Education.

Betalutgåvor av Google Workspace for Education

Med de tre betalutgåvorna av Google Workspace for Education får du fler val, större kontroll och mer flexibilitet så att du kan uppfylla organisationens behov.



Google Workspace for Education Standard

Avancerade säkerhets- och analysverktyg som hjälper dig att minska riskerna och undvika hot genom bättre synlighet och kontroll i hela utbildningsmiljön.



Teaching and Learning Upgrade

Med förbättrade verktyg för lärare är det möjligt att stärka kommunikationen och undervisningsupplevelsen och uppmuntra till akademisk integritet.



Google Workspace for Education Plus

En omfattande lösning med alla funktionerna i Education Standard och Teaching and Learning Upgrade och som dessutom ger den mest effektiva och enhetliga undervisningsmiljön för hela skolan.

Innehållsförteckning



Säkerhets- och analysverktyg

Verktyg i Education Standard och Education Plus

Utredningsverktyget

- Otillåtet material som delas
- Filer som delas av misstag
- Utvärdering av e-post
- E-post med nätfiske och skadlig programvara
- Stoppa skadliga aktörer

Säkerhetsöversikten

- Mängden skräppost
- Extern fildelning
- Appar från tredje part
- Försök till nätfiske

Säkerhetsstatus

- Rekommendationer för utsatta områden
- Få uppdateringar om rekommenderade metoder
- Metodtips för säkerhet
- Öka säkerheten för en växande skola

Avancerade administratörskontroller

- Lagstiftning gällande data
- Riktlinjer för anslag
- Appbegränsningar
- Hantera mobila enheter
- Migrera data

Innehållsförteckning



Undervisnings- och inlärningsverktyg

Verktyg i Teaching and Learning Upgrade och Education Plus

Plagiatrapporter

- Söka efter plagiat
- Ge eleverna möjlighet att lära sig av plagiat

Google Meet

- Säkra videomöten
- Öka säkerheten under videokonferenser
- Spela in lektioner
- Spela in lärarmöten
- Missade lektioner
- Livestreama möten
- Livestreama evenemang på skolan
- Ställa frågor
- Samla in åsikter
- Små elevgrupper
- Kontrollera närvaron



Säkerhets- och analysverktyg

Få större kontroll över hela domänen med hjälp av proaktiva säkerhetsverktyg som ger skydd mot hot, gör det möjligt att analysera säkerhetshändelser och skyddar elevernas och lärarnas data.



[Utredningsverktyget](#)



[Säkerhetsöversikten](#)



[Sidan Säkerhetsstatus](#)



[Avancerade administratörskontroller](#)

Utredningsverktyget

Vad är detta?

Med hjälp av utredningsverktyget kan du identifiera, utvärdera och vidta åtgärder för problemen med säkerhet och integritet på domänen.

Användningsområden

Otillåtet material som delas



[Stegvisa anvisningar](#)

Filer som delas av misstag



[Stegvisa anvisningar](#)

Utvärdering av e-post



[Stegvisa anvisningar](#)

E-post med nätfiske/skadlig programvara

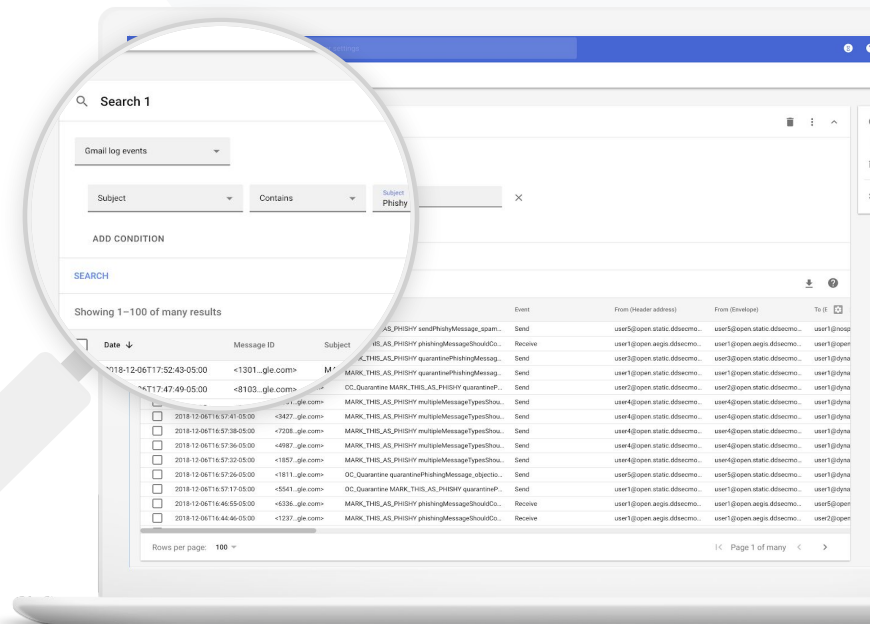


[Stegvisa anvisningar](#)

Stoppa skadliga aktörer



[Stegvisa anvisningar](#)





”

Jag vet att en fil med otillåtet material delas. Jag vill veta vem som har skapat den, när den skapades, vem som har delat den med vem, vem som har redigerat den och sedan vill jag radera den.”

[Stegvisa anvisningar](#)

Otillåtet material som delas

Med Drive-loggar i utredningsverktyget kan du hitta, spåra och isolera eller radera oönskade filer på domänen. Du kan göra följande med åtkomst till [Drive-loggar](#):

- ✓ Söka efter dokument utifrån namn, aktör, ägare och liknande.
- ✓ Visa all logginformation som är kopplad till dokumentet.
 - Datum då det skapades.
 - Vem som äger det, vem som är öppnat det och vem som har redigerat det.
 - När det delades.
- ✓ Vidta åtgärder genom att ändra filbehörigheterna eller radera filen.

[🔗](#) Relevant dokumentation i hjälpcentret

[Villkor för logghändelser för Drive](#)

[Åtgärder för logghändelser för Drive](#)



”

En fil har av misstag delats med en grupp som INTE ska ha åtkomst till den. Jag vill ta bort deras åtkomst till den.”

[Stegvisa anvisningar](#)

Filer som delas av misstag

Med Drive-loggar i utredningsverktyget kan du spåra och åtgärda problem med delade filer. Du kan göra följande med åtkomst till [Drive-loggar](#):

- ✓ Söka efter dokument utifrån namn, aktör, ägare och liknande.
- ✓ Visa all logginformation som är kopplad till dokumentet, till exempel vem som har öppnat det och när det har delats.
- ✓ Vidta åtgärder genom att ändra filbehörigheterna och inaktivera nedladdning, utskrift och kopiering.

[🔗](#) Relevant dokumentation i hjälpcentret

[Villkor för logghändelser för Drive](#)

[Åtgärder för logghändelser för Drive](#)



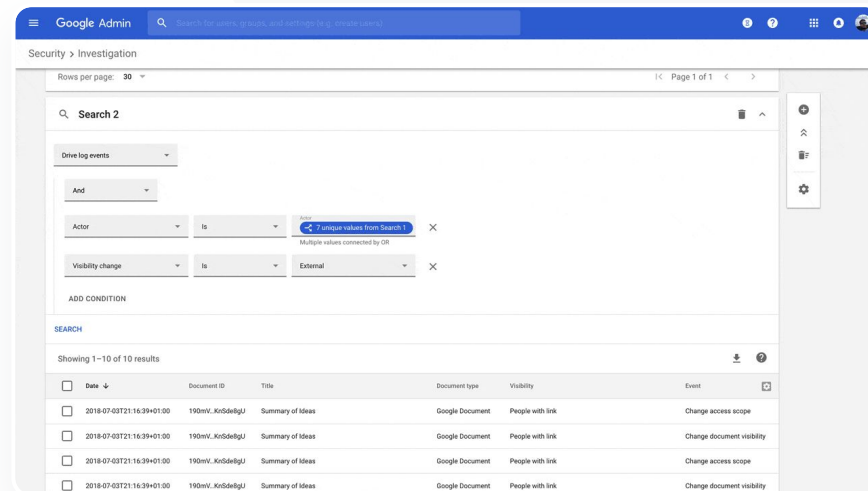
Så här gör du: Logghändelser för Drive

Så här utreder du

- Logga in på administratörskonsolen.
- Klicka på Säkerhet > Utredningsverktyget.
- Välj Logghändelser för Drive.
- Klicka på Lägg till villkor > Sök.

Så här vidtar du åtgärder

- Välj de relevanta filerna i sökresultatet.
- Klicka på Åtgärder > Granska filbehörigheter för att öppna sidan Behörigheter.
- Klicka på Personer för att se vilka som har åtkomst.
- Klicka på Länkar för att visa eller ändra inställningarna för länkelning för de valda filerna.
- Klicka på Väntande ändringar för att granska ändringarna innan du sparar.



Security > Investigation

Rows per page: 30 Page 1 of 1

Search 2

Drive log events

And

Actor is 7 Active users from Search 1

Visibility change is External

ADD CONDITION

SEARCH

Showing 1–10 of 10 results

<input type="checkbox"/>	Date ↓	Document ID	Title	Document type	Visibility	Event
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrSd6lGJ	Summary of Ideas	Google Document	People with link	Change access scope
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrSd6lGJ	Summary of Ideas	Google Document	People with link	Change document visibility
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrSd6lGJ	Summary of Ideas	Google Document	People with link	Change access scope
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrSd6lGJ	Summary of Ideas	Google Document	People with link	Change document visibility

 [Relevant dokumentation i hjälpcentret](#)

[Villkor för logghändelser för Drive](#)

[Åtgärder för logghändelser för Drive](#)



”

Någon har skickat ett e-postmeddelande som INTE borde ha skickats.

Vi vill veta vem personen har skickat meddelandet till, om mottagarna har öppnar det, om de har svarat och sedan vill vi radera e-postmeddelandet. Jag vill även veta vad e-postmeddelandet innehåller.”

[Stegvisa anvisningar](#)

Utvärdering av e-post

Med Gmail-loggar i utredningsverktyget kan du identifiera och vidta åtgärder mot farliga eller otillåtna e-postmeddelanden inom domänen. Du kan göra följande med åtkomst till Gmail-loggar:

- ✓ Söka efter specifika e-postmeddelanden utifrån ämne, meddelande-id, bilagor, avsändare och liknande.
- ✓ Visa information om e-postmeddelandet, till exempel vem som skrev det, mottagare och hur många gånger det har öppnats och vidarebefordrats.
- ✓ Vidta åtgärder baserat på sökresultat. Du kan till exempel radera Gmail-meddelanden, återställa dem, markera dem som skräppost eller nätfiske, skicka dem till inkorgen och placera dem i karantän.

 [Relevant dokumentation i hjälpcentret](#)

[Villkor för Gmail-loggar och Gmail-meddelanden](#)

[Åtgärder för Gmail-meddelanden och logghändelser för Gmail](#)

[Så här visar du innehållet i ett e-postmeddelande](#)



”

Ett e-postmeddelande med nätfiske eller skadlig programvara har skickats till användarna. Vi vill se om användare har klickat på länken i e-postmeddelandet eller laddat ned bilagan eftersom dessa åtgärder kan utsätta användarna och domänen för fara.”

[Stegvisa anvisningar](#)

E-post med nätfiske och skadlig programvara

Genom att öppna utredningsverktyget, mer specifikt Gmail-loggarna, kan du hitta och isolera skadliga e-postmeddelanden inom domänen. Du kan göra följande med åtkomst till Gmail-loggar:

- ✓ Söka efter specifikt innehåll, till exempel bilagor, i e-postmeddelanden.
- ✓ Visa information om specifika e-postmeddelanden, till exempel mottagare och hur många gånger det har öppnats.
- ✓ Visa meddelanden och tråden för att avgöra om de är skadliga.
- ✓ Vidta åtgärder, till exempel markera meddelanden som skräppost eller nätfiske, skicka dem till en viss inkorg eller till karantän, eller radera dem.

 [Relevant dokumentation i hjälpcentret](#)

[Villkor för Gmail-loggar och Gmail-meddelanden](#)

[Åtgärder för Gmail-meddelanden och logghändelser för Gmail](#)

[Så här visar du innehållet i ett e-postmeddelande](#)



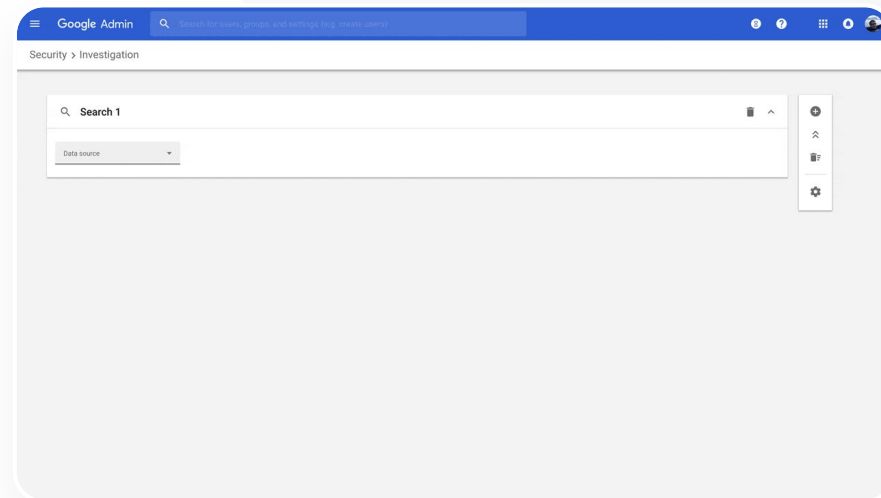
Så här gör du: Gmail-loggar

Så här utreder du

- Logga in på administratörskonsolen.
- Klicka på Säkerhet > Utredningsverktyget.
- Välj Logghändelser för Gmail ELLER Gmail-meddelanden.
- Klicka på Lägg till villkor > Sök.

Så här vidtar du åtgärder

- Välj de relevanta meddelandena i sökresultatet.
- Klicka på Åtgärder.
- Välj Radera meddelandet från inkorgen.
- Klicka på Radera från inkorgen.
- Bekräfta åtgärden genom att klicka på Visa längst ned på sidan.
- I kolumnen Resultat kan du visa statusen för åtgärden.



[↪ Relevant dokumentation i hjälpcentret](#)

[Villkor för Gmail-loggar och Gmail-meddelanden](#)

[Åtgärder för Gmail-meddelanden och logghändelser för Gmail](#)

[Så här visar du innehållet i ett e-postmeddelande](#)



”

En skadlig aktör riktar ständigt in sig på högprofilerade användare på domänen och så fort jag blir av med en dyker en annan upp. Hur får jag bukt på problemet?”

[Stegvisa anvisningar](#)

Stoppa skadliga aktörer

Med användarloggen i utredningsverktyget kan du göra följande:

- ✓ Identifiera och utreda försök att kapa användarkonton i organisationen.
- ✓ Kontrollera vilka metoder för tvåstegsverifiering som användarna i organisationen använder.
- ✓ Läs mer om misslyckade inloggningsförsök från användare i organisationen.
- ✓ [Skapa aktivitetsregler med utredningsverktyget](#): Blockera automatiskt meddelanden och andra skadliga aktiviteter från specifika aktörer.
- ✓ Skydda högprofilerade användare ytterligare med [programmet Avancerat skydd](#).
- ✓ Återställa eller stänga av användare.

 [Relevant dokumentation i hjälpcentret](#)

[Söka efter och utreda händelser i användarloggen](#)

[Skapa aktivitetsregler med utredningsverktyget](#)



Så här gör du: Logghändelser för användare

Så här utreder du

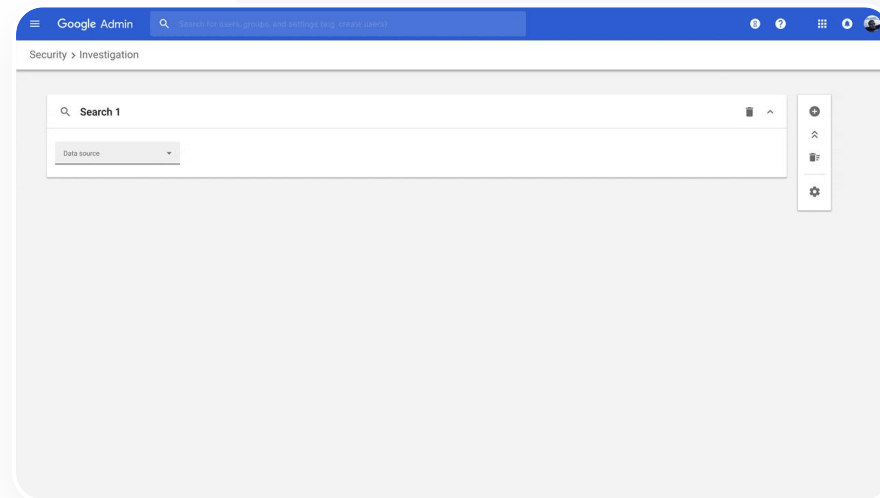
- Logga in på administratörskonsolen.
- Klicka på Säkerhet > Utredningsverktyget.
- Välj Logghändelser för användare.
- Klicka på Lägg till villkor > Sök.

Så här återställer eller stänger du av användare

- Välj en eller flera användare i sökresultatet.
- Klicka på rullgardinsmenyn Åtgärder.
- Klicka på Återställ användare eller Stäng av användare.

Så här visar du information om en specifik användare

- Välj enbart en användare på sökresultatsidan.
- På rullgardinsmenyn ÅTGÄRDER klickar du på Visa information.



[↪](#) Relevant dokumentation i hjälpcentret

[Söka efter och utreda händelser i användarloggen](#)

Säkerhetsöversikten

Vad är detta?

I säkerhetsöversikten kan du få en översikt över de olika säkerhetsrapporterna. Som standard visar varje ruta i säkerhetsrapporten data från de senaste sju dagarna. Anpassa översikten för att visa data från i dag, i går, den här veckan, förra veckan, den här månaden, förra månaden eller ett visst antal dagar sedan (upp till 180 dagar).

Användningsområden

Mängden skräppost



[Stegvisa anvisningar](#)

Extern fildelning



[Stegvisa anvisningar](#)

Appar från tredje part

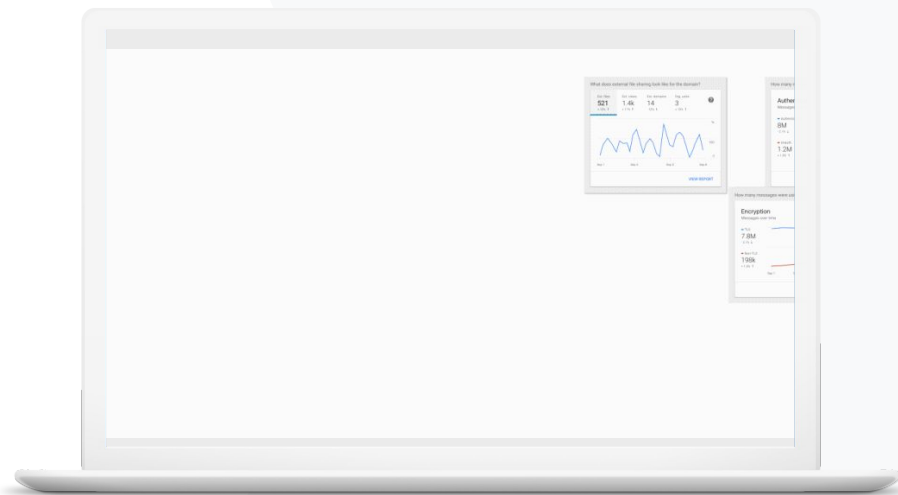


[Stegvisa anvisningar](#)

Försök till nätfiske



[Stegvisa anvisningar](#)





Mängden skräppost

I säkerhetsöversikten får du en visuell återgivning av aktiviteten i Google Workspace for Education, till exempel:

- ✓ Skräppost
- ✓ Misstänkta bilagor
- ✓ Nätfiske
- ✓ Med mera
- ✓ Skadlig programvara

 [Relevant dokumentation i hjälpcentret](#)

[Om säkerhetsöversikten](#)



Jag vill kunna styra över stora mängder eller onödiga e-postmeddelanden samtidigt som jag minskar säkerhetshoten för skolan.”

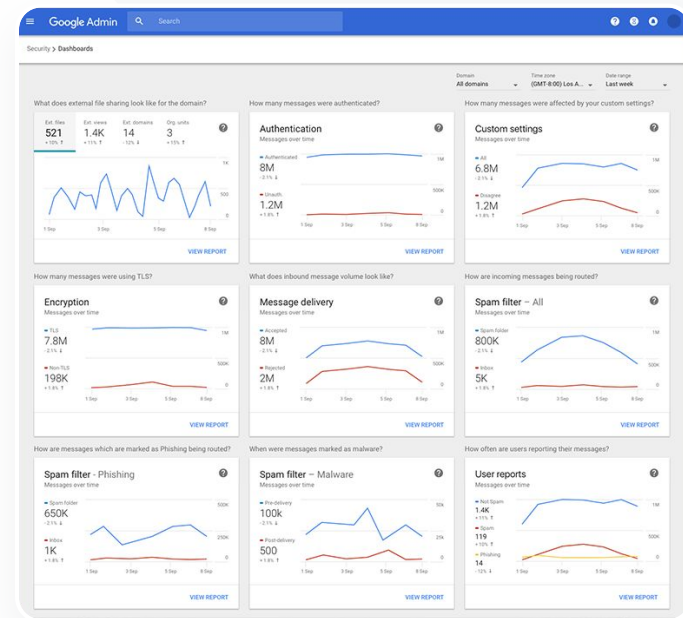
[Stegvisa anvisningar](#)



Så här gör du: Översikten

Så här visar du översikten

- Logga in på **administratörskonsolen**.
- Klicka på **Säkerhet > Översikt**.
- Via säkerhetsöversikten kan du granska data, exportera data till Kalkylark eller ett verktyg från tredje part eller starta en utredning i utredningsverktyget.



[Relevant dokumentation i hjälpcentret](#)

[Om säkerhetsöversikten](#)



”

Jag vill se vilka filer som delas externt för att förhindra att känsliga uppgifter delas med tredje part.”

[Stegvisa anvisningar](#)

Extern fildelning

Med rapporten Filexponering i säkerhetsöversikten kan du se mätvärden om extern fildelning för domänen, till exempel:

- ✓ Antalet delningshändelser till användare utanför domänen under en viss tidsperiod.
- ✓ Antalet visningar av en extern fil som mottogs under en viss tidsperiod.

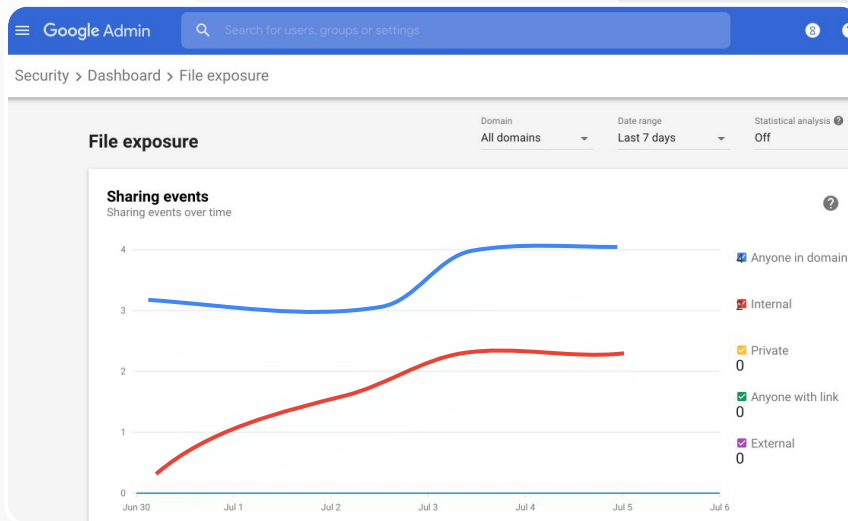
[🔗](#) Relevant dokumentation i hjälpcentret

[Kom igång med sidan Säkerhetsstatus](#)

Så här gör du: Rapporten Filexponering

Så här visar du rapporten

- Logga in på administratörskonsolen.
- Klicka på Säkerhet > Översikt.
- I panelen Hur ser extern fildelning ut för domänen? klickar du på Visa rapport nere till höger.



[🔗](#) Relevant dokumentation i hjälpcentret

[Om säkerhetsöversikten Rapporten
Filexponering](#)



”

Jag vill se vilka appar från tredje part som har åtkomst till domänens data.”

[Stegvisa anvisningar](#)

Appar från tredje part

Med rapporten över aktivitet för OAuth-beviljande i säkerhetsöversikten kan du hålla koll på vilka appar från tredje part som är anslutna till domänen och vilken data de har åtkomst till.

- ✓ Med OAuth får tjänster från tredje part åtkomst till en användares kontouppgifter utan att användarens lösenord exponeras. Det kan vara bra att begränsa vilka appar från tredje part som har åtkomst.
- ✓ Med aktivitetspanelen för OAuth-beviljande kan du hålla koll på vilka appar som beviljas, i vilken omfattning, för vilka användare och uppdatera behörigheterna.

[🔗](#) Relevant dokumentation i hjälpcentret

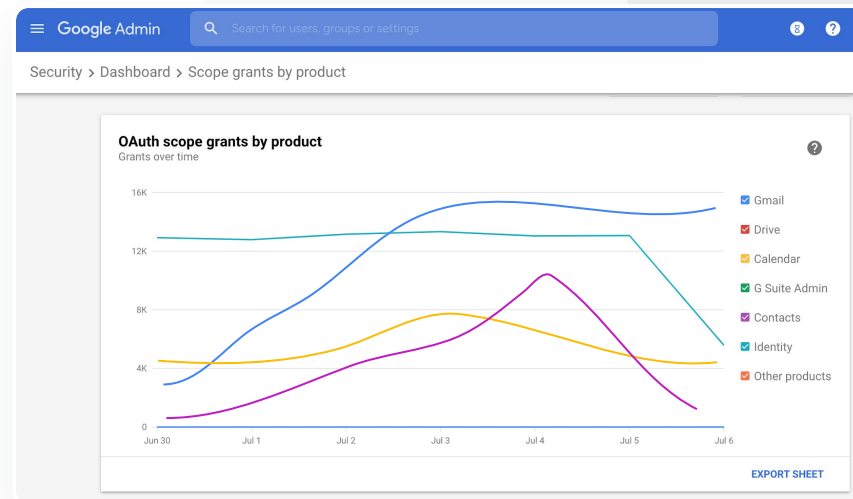
[Rapport över aktivitet för OAuth-beviljande i app](#)



Så här gör du: Rapport över aktivitet för OAuth-beviljande i app

Så här visar du rapporten

- Logga in på administratörskonsolen.
- Klicka på Säkerhet > Översikt.
- Klicka på Visa rapport längst ned.
- Du kan visa aktiviteten för OAuth-beviljande efter produkt (app), omfattning eller användare.
- Om du vill filtrera informationen klickar du på App, Omfattning eller Användare.
- Om du vill skapa en kalkylarsrapport klickar du på Exportera kalkylark.



[Relevant dokumentation i hjälpcentret](#)

[Rapport över aktivitet för OAuth-beviljande i app](#)



Användare har rapporterat ett försök till nätfiske. Jag vill kunna kontrollera när e-postmeddelandet med nätfiske mottogs, exakt vilket e-postmeddelande som mottagaren fick och vilken risk han eller hon utsattes för.”

[Stegvisa anvisningar](#)

Försök till nätfiske

I panelen **Användarrapporter** i säkerhetsöversikten kan du se meddelanden som har flaggats som nätfiske eller skräppost under en viss tidsperiod. Du kan visa information om e-postmeddelanden som har flaggats som nätfiske, till exempel dess mottagare och hur många gånger det har öppnats.



Med användarrapporter kan du se hur användarna markerar sina meddelanden (till exempel som skräppost, inte skräppost eller nätfiske) under en viss tidsperiod.



Du kan anpassa diagrammet så att det endast visar information om vissa typer av meddelanden, till exempel om meddelandet skickades internt eller extern, enligt ett datumintervall, och så vidare.



Relevant dokumentation i hjälpcentret

[Hur markerar användarna sin e-post?](#)

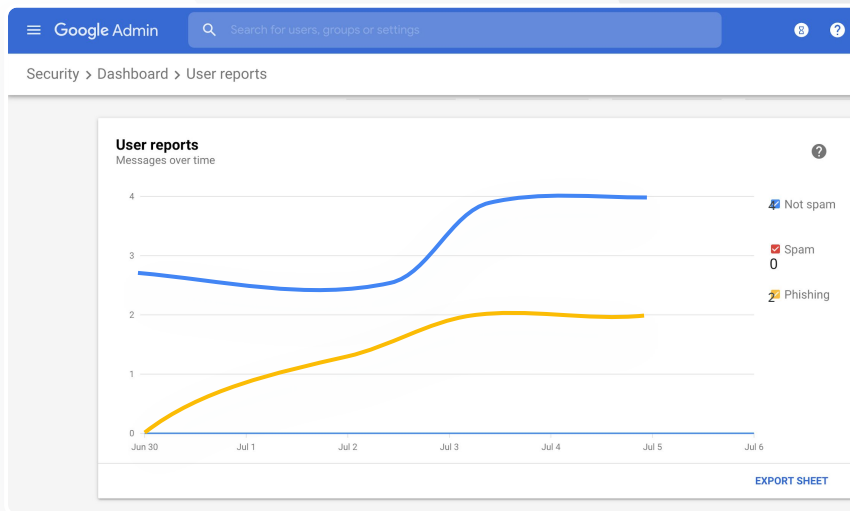
[Användarrapporter](#)



Så här gör du: Panelen Användarrapporter

Så här visar du rapporten

- Logga in på administratörskonsolen.
- Klicka på Säkerhet > Översikt.
- Klicka på Visa rapport nere till höger i panelen Användarrapporter.



[🔗](#) Relevant dokumentation i hjälpcentret

[Om säkerhetsöversikten](#) [Rapporten](#)
[Filexponering](#)

Säkerhetsstatus

Vad är detta?

På sidan Säkerhetsstatus får du en omfattande översikt över säkerhetsstatusen för Google Workspace-miljön och kan jämföra konfigurationerna med rekommendationer från Google för att proaktivt skydda organisationen.

Användningsområden

[Rekommendationer för utsatta områden](#)



[Stegvisa anvisningar](#)

[Få uppdateringar om rekommenderade metoder](#)



[Stegvisa anvisningar](#)

[Metodtips för säkerhet](#)

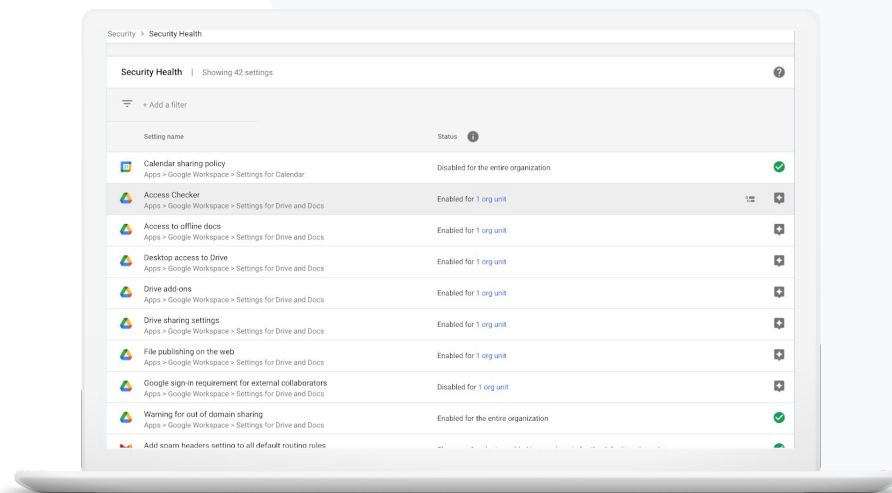


[Stegvisa anvisningar](#)

[Öka säkerheten för en växande skola](#)



[Stegvisa anvisningar](#)





”

Jag vill ha en enkel översiktsbild över domänens säkerhetsinställningar med konkreta rekommendationer om hur jag åtgärdar potentiella riskområden.”

[Stegvisa anvisningar](#)

Rekommendationer för utsatta områden

På sidan **Säkerhetsstatus** kan du granska säkerhetskfigurationen och se rekommenderade ändringar. Du kan göra följande på sidan **Säkerhetsstatus**:

- ✓ Identifiera snabbt potentiella riskområden på domänen.
- ✓ Få rekommendationer om de bästa inställningarna för att öka säkerhetens effektivitet.
- ✓ Läs ytterligare information och supportartiklar om rekommendationerna.

[🔗](#) Relevant dokumentation i hjälpcentret

[Kom igång med sidan Säkerhetsstatus](#)



”

Jag hanterar domänen, men jag vet inte det jag inte vet. Hjälp mig att se till att allt är skyddat av de rätta inställningarna.”

[Stegvisa anvisningar](#)

Få uppdateringar om rekommenderade metoder

På sidan **Säkerhetsstatus** kan du granska säkerhetskonfigurationen och se rekommenderade ändringar. Du kan få följande på sidan **Säkerhetsstatus**:

- ✓ Rekommendationer för potentiella riskområden på domänen.
- ✓ Rekommendationer om de bästa inställningarna för att öka säkerhetens effektivitet.
- ✓ Ytterligare information och hjälpartiklar.

 [Relevant dokumentation i hjälpcentret](#)

[Kom igång med sidan Säkerhetsstatus](#)



”

Visa var jag kan hitta metodtips eller rekommendationer om hur jag konfigurerar säkerhetsprinciper.”

[Stegvisa anvisningar](#)

Metodtips för säkerhet

På sidan Säkerhetsstatus kan du få metodtips om säkerhetsprinciper med följande:

- ✓ Rekommendationer för potentiella riskområden på domänen.
- ✓ Rekommendationer om de bästa inställningarna för att öka säkerhetens effektivitet.
- ✓ Direktlänkar till inställningar.
- ✓ Ytterligare information och hjälpartiklar.

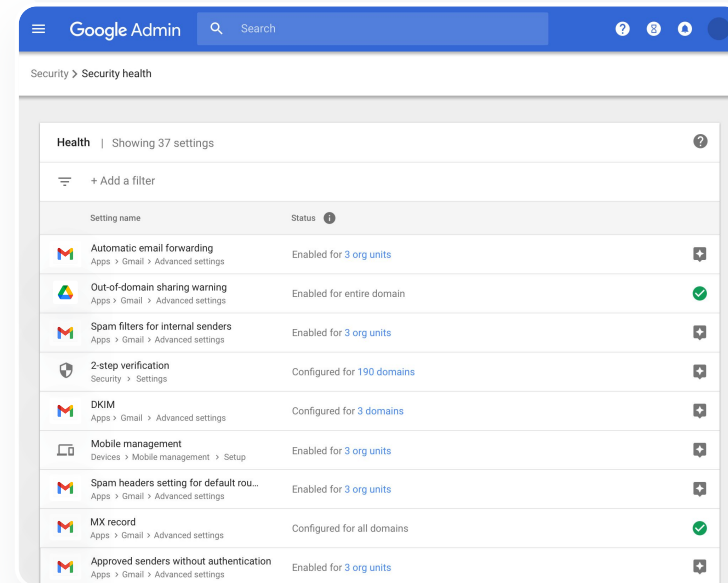
 [Relevant dokumentation i hjälpcentret](#)

[Kom igång med sidan Säkerhetsstatus](#)

Så här gör du: Säkerhetsrekommendationer

Så här visar du rekommendationer

- Logga in på administratörskonsolen.
- Klicka på **Säkerhet > Säkerhetsstatus**.
- Visa statusinställningarna i kolumnen längst till höger.
 - En grön bockmarkering visas om en inställning är säker.
 - En grå ikon visas om du bör kontrollera inställningen. Om du klickar på ikonerna visas mer information och anvisningar.



 Relevant dokumentation i hjälpcentret

[Kom igång med sidan Säkerhetsstatus](#)



”

Jag vill försäkra mig om att skolan är så skyddad som möjligt när vår personalstyrka utökas och vi får fler elever.”

[Stegvisa anvisningar](#)

Öka säkerheten för en växande skola

IT-administratörer bör följa de här [säkerhetsrutinerna](#) för att stärka säkerheten och integriteten för företagsinformation. Använd en eller flera inställningar i Googles administratörskonsol för att införa varje rutin i denna checklista.

- ✓ Rekommendationer för att förhindra att konton utsätts för intrång och åtgärda obehörig åtkomst.
- ✓ Anvisningar om hur du begränsar delning och samarbete utanför domänen.
- ✓ Funktioner för granskning av tredje parts åtkomst till tjänster.

 [Relevant dokumentation i hjälpcentret](#)

[Checklista för säkerhetsåtgärder för medelstora och stora organisationer](#)



Så här gör du: Checklista för säkerhet

I syfte att skydda organisationen har Google som standard aktiverat många av de rekommenderade inställningarna i den här checklistan. Vi rekommenderar att du tar en närmare titt på de som är markerade nedan.

- **Administratör:** Skydda administratörskonton
- **Användarkonton:** Förhindra att konton utsätts för intrång och åtgärda obehörig åtkomst
- **Appar:** Granska åtkomst till tjänster för tredje part
- **Kalender:** Begränsa extern kalenderdelning
- **Drive:** Begränsa delning och samarbete utanför domänen
- **Gmail:** Konfigurera autentisering och infrastruktur
- **Arkiv:** Kontrollera, granska och skydda Arkiv-konton

Security best practices

To help protect your business, Google turns on many of the settings recommended in this checklist as security best practices by default.

[Administrator](#) | [Accounts](#) | [Apps](#) | [Calendar](#) | [Chrome Browser and Chrome OS](#) | [Classic Hangouts](#)
[Contacts](#) | [Drive](#) | [Gmail](#) | [Google+](#) | [Groups](#) | [Mobile](#) | [Sites](#) | [Vault](#)

Administrator

Protect admin accounts

- Require 2-Step Verification for admin accounts**
Because super admins control access to all business and employee data in the organization, it's especially important for their accounts to be protected by an additional authentication factor.
[Protect your business with 2-Step Verification](#) | [Deploy 2-Step verification](#)
- Use security keys for 2-Step Verification**
Security keys help to resist phishing threats and are the most phishing-resistant form of 2-Step Verification.
[Protect your business with 2-Step Verification](#)

 [Relevant dokumentation i hjälpcentret](#)

[Övervaka status för dina säkerhetsinställningar](#)



Avancerade administratörskontroller

Vad är detta?

Håll koll på och styr vilka användare och enheter som har åtkomst till domänen och data.

Användningsområden

Lagstiftning gällande data



[Stegvisa anvisningar](#)

Riktlinjer för anslag



[Stegvisa anvisningar](#)

Appbegränsningar



[Stegvisa anvisningar](#)

Hantera mobila enheter

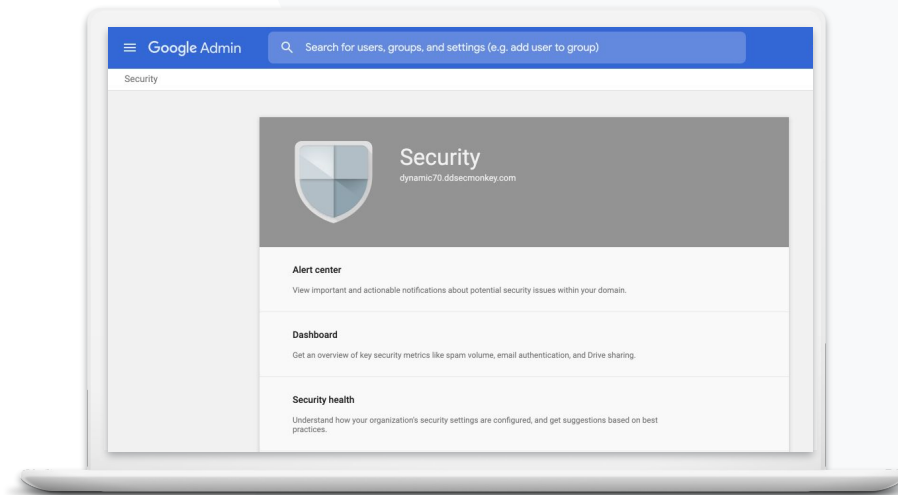


[Stegvisa anvisningar](#)

Migrera data



[Stegvisa anvisningar](#)





”

Data från elever, lärare
och personal måste lagras
i USA i enlighet med
gällande datalagstiftning.”

[Stegvisa anvisningar](#)

Lagstiftning gällande data

Som administratör kan du välja om data ska lagras på en specifik geografisk plats (antingen USA eller Förenade kungariket/Europa) med hjälp av en **dataregionspolicy**.

- ✓ Du kan välja en dataregion för vissa användare eller olika dataregioner för specifika avdelningar eller team.
- ✓ Samla användarna i en organisationsenhet (om inställningarna ska göras per avdelning) eller i en konfigurationsgrupp (om inställningarna ska gälla användare på olika avdelningar).
- ✓ Användare som inte har tilldelats en Education Standard- eller Education Plus-licens omfattas inte av dataregionspolicyer.



Relevant dokumentation i hjälpcentret

[Välja en geografisk plats för din data](#)

”

Fakultetens forskning måste lagras i USA på grund av föreskrifter för deras anslag.”

[Stegvisa anvisningar](#)

Riktlinjer för anslag

Som administratör kan du välja att lagra fakultetens forskning på en viss geografisk plats (antingen i USA eller Europa) genom att använda en **dataregionspolicy**.

- ✓ Dataregionspolicyer omfattar den primära vilande datan (inklusive säkerhetskopior) för de allra flesta Google Workspace for Education-tjänster som anges [här](#).
- ✓ Tänk igenom för- och nackdelarna innan du anger en dataregionspolicy eftersom användarna utanför den region där deras data lagras i vissa fall kan uppleva latens.

 [Relevant dokumentation i hjälpcentret](#)

[Välja en geografisk plats för din data](#)



Så här gör du: Dataregioner*

Så här anger du dataregioner

- Logga in på administratörskonsolen.
 - Obs! Du måste vara inloggad som avancerad administratör.
- Klicka på företagsprofilen > Visa mer > Dataregioner.
- Välj den organisationsenhet eller konfigurationsgrupp som du vill begränsa till en region eller markera hela kolumnen om du vill inkludera alla enheter och grupper.
- Välj ett alternativ, till exempel Ingen inställning, USA eller Europa.
- Klicka på Spara.

* Endast institutioner som har Education Standard eller Education Plus uppfyller villkoren för att lagra data i specifika regioner med funktionen för dataregioner.

[↪](#) Relevant dokumentation i hjälpcentret

[Välja en geografisk plats för din data](#)



Jag vill begränsa åtkomsten till specifika appar när användarna är anslutna till nätverket.”

[Stegvisa anvisningar](#)

Appbegränsningar

Med hjälp av Kontextkänslig åtkomst, kan du skapa detaljerade principer för åtkomstkontroll i webbappar baserat på attribut som användaridentitet, plats, enhetens säkerhetsstatus och IP-adress. Du kan till och med begränsa åtkomsten till appar utanför nätverket.

- ✓ Du kan tillämpa principer för kontextkänslig åtkomst till Google Workspace för Education-tjänsterna.
- ✓ Exempel: Om en användare loggar in på en Google Workspace-tjänst i skolan och går vidare till ett kafé kontrolleras en princip för kontextkänslig åtkomst för tjänsten igen när användaren byter plats.

[↔](#) Relevant dokumentation i hjälpcentret

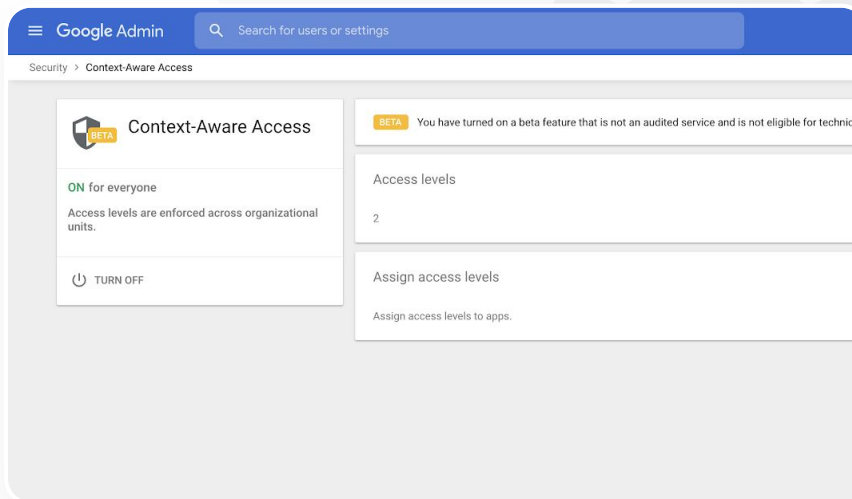
[Översikt över kontextkänslig åtkomst](#) [Tilldela kontextkänsliga åtkomstnivåer för appar](#)

* Endast institutioner som har Education Standard eller Education Plus uppfyller villkoren för tillämpning av kontextkänsliga principer.

Så här gör du: Kontextkänslig åtkomst

Så här använder du kontextkänslig åtkomst

- Logga in på administratörskonsolen.
- Välj **Säkerhet > Kontextkänslig åtkomst > Tilldela**.
- Välj **Tilldela åtkomstnivåer** för att se en lista över appar.
- Välj en organisationsenhet eller konfigurationsgrupp om du vill sortera listan.
- Välj **Tilldela** bredvid appen du vill ändra.
- Välj minst en åtkomstnivå.
- Du kan skapa flera nivåer om du vill att användarna ska uppfylla minst ett villkor.
- Klicka på **Spara**.



[↗](#) Relevant dokumentation i hjälpcentret

[Översikt över kontextkänslig åtkomst](#)

[Tilldela kontextkänsliga åtkomstnivåer för appar](#)

”

Jag måste kunna hantera och implementera principer på enheter med olika operativsystem, t.ex. iOS, och Windows 10, i hela distriktet och inte bara Chromebooks, särskilt om någon av enheterna utsätts för obehörig åtkomst.”

[Stegvisa anvisningar](#)

Hantera mobila enheter

Med avancerad mobilhantering får du större kontroll över organisationens data via mobila enheter. Du kan begränsa funktioner på mobila enheter, kräva enhetskryptering, hantera appar på Android-enheter eller iPhones och iPads och till och med rensa en enhet på data.

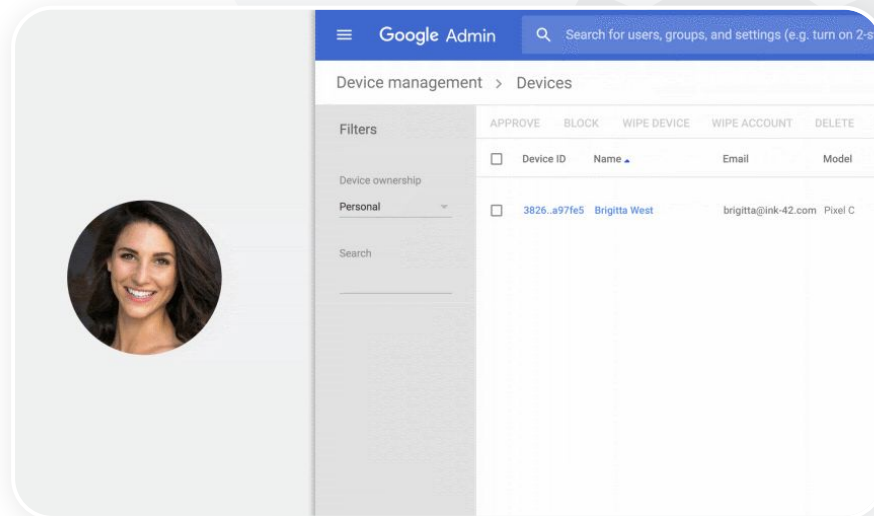
- ✓ Du kan godkänna, blockera, återaktivera eller radera enheter via administratörskonsolen.
- ✓ Om någon tappar bort en enhet eller avregistreras från skolan kan du rensa användarens konto, hans eller hennes profil eller all data från den specifika mobila enheten som hanteras. Denna data är fortfarande tillgänglig via en dator eller webbläsare.

 [Relevant dokumentation i hjälpcentret](#)
[Konfigurera avancerad mobilhantering](#)
[Godkänna, blockera, avblockera eller radera en enhet](#)
[Ta bort data från en enhet](#)

Så här gör du: Aktivera avancerad mobilhantering

Så här aktiverar du funktionen

- Logga in på administratörskonsolen.
- Öppna administratörskonsolen > Enheter.
- Klicka på Inställningar tillvänster > Universella inställningar.
- Klicka på Allmänt > Mobilhantering.
- Om du vill att inställningen ska gälla alla väljer du organisationsenheten på den högsta nivån. Välj annars en underordnad organisationsenhet.
- Välj Avancerat.
- Klicka på Spara.



➔ Relevant dokumentation i hjälpcentret

[Konfigurera avancerad mobilhantering](#)

[Godkänna, blockera, avblockera eller radera en enhet](#)

[Ta bort data från en enhet](#)



”

Vi ska byta till Google Workspace och måste migrera all data till den nya Google-miljön.”

[Stegvisa anvisningar](#)

Migrera data

I migreringsguiderna finns information om hur du flyttar all data för organisationen, till exempel e-post, kalendrar, kontakter, mappar, filer och behörigheter, till Google Workspace.

Data från färre än 1 000 användare

- ✓ Ta en titt i produktmatrisen för att få en uppfattning om vilken lösning som passar institutionen bäst.

[Läs mer](#)

Data från fler än 1 000 användare

- ✓ Använd Google Workspace Migrate för att försäkra dig om att stora mängder data migreras på ett effektivt sätt.

[Läs mer](#)

[↪ Relevant dokumentation i hjälpcentret](#)

[Migrera organisationens data till Google Workspace](#)

[Produktmatris för migrering av Google Workspace](#)

[Om Google Workspace Migrate](#)

[Installera och konfigurera Google Workspace Migrate](#)

Så här gör du: Google Workspace Migrate

Innan du börjar

Registrera dig för [betaversionen](#) och kontrollera att [systemkraven](#) har uppfyllts.

Så här gör du

1. Konfigurera Google Cloud Console

[Aktivera API:er](#)

[Skapa webbklient-id för OAuth](#)

[Skapa ett tjänstkonto för Google Workspace](#)

2. Konfigurera administratörskonsolen

[Konfigurera administratörsroller](#)

[Auktorisera klient-id:t](#)

3. Ladda ned och installera

[Ladda ned installationsprogrammen](#)

[Installera databaserna](#)

[Installera och konfigurera plattformen](#)

[Installera nodservrarna](#)

[\(Valfritt\) Konfigurera nodservern för användning av TLS](#)

4. Konfigurera migreringsprodukten

[Konfigurera krypteringsnyckeln](#)

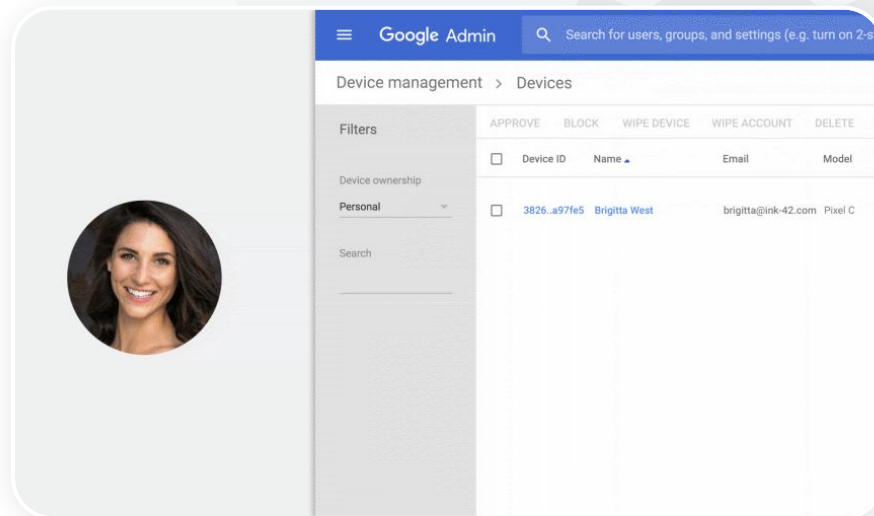
[Konfigurera databasinställningarna](#)

[Konfigurera adressen för återanrop](#)

[Lägg till nodservrarna](#)

[Skapa ett projekt](#)

Hjälp Kontakta en [Google Cloud Partner](#).



[Relevant dokumentation i hjälpcentret](#)

[Om Google Workspace Migrate](#)

[Installera och konfigurera Google Workspace Migrate](#)

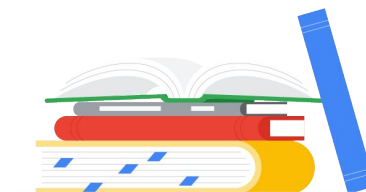
[Migrera organisationens data till Google Workspace](#)

[Produktmatris för migrering av Google Workspace](#)



Undervisnings- och inlärningsverktyg

Ge pedagogerna ytterligare möjligheter i den digitala undervisningsmiljön, t.ex. förbättrad videokommunikation, utökade klassfunktioner och verktyg för akademisk integritet.



[Plagiatrapporter](#)



[Google Meet](#)

Plagiatrapporter

Vad är detta?

Pedagoger och elever kan kontrollera att arbetet inte innehåller plagiat. Med hjälp av Google Sök jämförs elevens arbete med miljarder med webbsidor och miljontals böcker i plagiatrapporten. Plagiatrapporten innehåller länkar till webbsidor som upptäckts och flaggar text som inte citerats.

Användningsområden

[Söka efter plagiat](#)

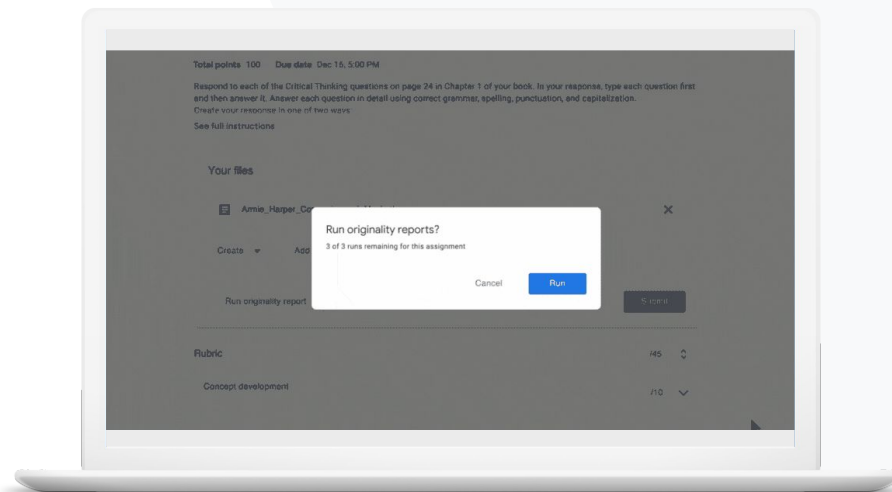


[Stegvisa anvisningar](#)

[Ge eleverna möjlighet att lära sig av plagiat](#)



[Stegvisa anvisningar](#)



”


Jag vill kontrollera om det finns plagiat eller saknade källhänvisningar i elevernas arbeten.

[Stegvisa anvisningar](#)

Söka efter plagiat

Lärare kan kontrollera om elevernas arbeten innehåller plagiat med hjälp av **plagiatrapporter**. Med hjälp av Google Sök jämförs elevens arbete med källmaterial från flera miljarder webbsidor och miljontals böcker i plagiatrapporten.

- ✓ Pedagoger med Teaching and Learning Upgrade eller Education Plus har obegränsad åtkomst till plagiatrapporter.
- ✓ Just nu är plagiatrapporter endast tillgängliga för
 - Google-konton som är inställda på engelska
 - arbeten som görs i Google Dokument
 - Google for Education-konton.

 [Relevant dokumentation i hjälpcentret](#)

[Aktivera plagiatrapporter](#)

Så här gör du: Efterkontroll av pedagog

Så här aktiverar du plagiatrapporter för en hemuppgift

- Logga in på Classroom-kontot på classroom.google.com.
- Välj den aktuella klassen i listan och välj Klassuppgifter.
- Välj Skapa > Hemuppgift.
- Markera kryssrutan bredvid Plagiatrapporter för att aktivera funktionen.

Så här aktiverar du plagiatrapporter för elevarbeten

- Välj filen för den aktuella eleven i listan och öppna den i betygsverktyget genom att klicka.
- Under elevens hemuppgift klickar du på Utför plagiatkontroll.

Originality report
Lizeth Smith - Comparison of Macbeth Adaptations

Essay: Comparison of Macbeth Adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth finds humor in the tumultuous events leading to his downfall. His chilling laughter upon the announcement of his wife's suicide and his demeaning attitude towards his fellow regents suggest his general lack of guilt and self-affliction. His unquenchable desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gazes, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility,"^[1] Lady Macbeth foreshadows danger through Macbeth's poses.

Rupert Goold successfully effuses more fear into the film by implementing staging devices and symbolism. Through the croaking of a raven and haunting background music, Goold subjects his viewers to the same state of agitation and rage felt by the characters. Goold emphasizes symbolism by using physical instruments such as a figurine, suggestive of the former Thane of Cowder. Through the figurine, the characters and the viewers, alike, are fixated by the prophecies made by the witches.

The presence of a state of Hell is evident in the film. Unlike the witches' cave in Shakespeare's play, the nurses of the film reveal their prophecies in an industrial room, only accessible through a caged elevator. The area, described by critic Nicholas de Jongh is an "atmosphere of existential strangeness... a murky limbo." At the end of play, after the beheading of Macbeth, Macbeth and Lady Macbeth are seen descending into the room, presumably entering the gates of Hell. By using the state of Hell, Rupert Goold makes his film more dramatic and frightening.

The murder scenes of Rupert Goold's film share similar elements of Shakespeare's play; however, Rupert Goold implements more details in the murder scenes. Not unlike Shakespeare's play, there are no visualizations of the murder of the King Duncan of Scotland. The only evidence of the act were the bloody knives and bloody hands

Summary
Originality report expires Mar 3, 2020

Count %

5 flagged passages
2 cited or quoted passages

Web matches

bartleby.com (3)	>
123helpme.com (2)	>

[Relevant dokumentation i hjälpcentret](#)

[Aktivera plagiatrapporter](#)

”

Jag vill ge eleverna möjlighet att kontrollera om deras arbeten innehåller plagiat och att lära sig genom att upptäcka fusk.

[Stegvisa anvisningar](#)

Ge eleverna möjlighet att lära sig av plagiat

Eleverna kan hitta innehåll utan källhänvisning och oavsiktligt plagiat innan de lämnar in sina arbeten genom att köra en **plagiatrapport** upp till tre gånger per hemuppgift. Med originalrapporter jämförs elevernas dokument med olika källor och text utan källhänvisningar flaggas. På så sätt får de möjlighet att lära sig, rätta till misstagen och lämna in skolarbeten utan att oroa sig.

- ✓ I Teaching and Learning Upgrade och Education Plus kan pedagoger aktivera plagiatrapporter så många gånger de vill. I Education Fundamentals kan de endast aktivera funktionen fem gånger per klass.
- ✓ När arbetena har lämnats in körs en rapport automatiskt i Classroom och bara läraren har tillgång till den. Om du ångrar en inlämning och sedan skickar in hemuppgiften igen körs en till plagiatrapport åt läraren i Classroom.

[🔗](#) Relevant dokumentation i hjälpcentret

[Köra en plagiatrapport på en uppgift](#)

Så här gör du: Förhandskontroll av eleverna

Så här kör elever plagiatrapporter

- Logga in på Classroom-kontot på classroom.google.com.
- Välj den aktuella klassen i listan och välj Klassuppgifter.
- Välj den aktuella hemuppgiften i listan och klicka på Visa hemuppgift.
- Under Ditt arbete väljer du Ladda upp eller Skapa fil.
- Bredvid Plagiatrapporter klickar du på Kör.
- Du öppnar rapporten genom att klicka på Visa plagiatrapport under hemuppgiftens namn.
- Om du vill granska hemuppgiften för att skriva om eller ange korrekta källhänvisningar för flaggade stycken klickar du på Redigera längst ned.

Essay: Comparison of Macbeth adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth first hovers in the limbo of a man torn between his ambition and his conscience. His chilling laughter upon the announcement of his wife's suicide and his denigrating attitude towards his fellow rebels suggest his general lack of guilt and self-affliction. His unrepentant desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gases, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility," Lady Macbeth foreshadows danger through Macbeth's poses.

Rupert Goold successfully effuses more fear into the film by implementing staging devices and symbolism. Through the croaking of a raven and haunting background music, Goold subjects his viewers to the same state of agitation and rage felt by the characters. Goold emphasizes symbolism by using physical instruments such as a figurine, suggestive of the former Thane of Cowdrie. Through the figurine, the characters and the viewers, alike, are fixated by the prophecies made by the witches.

The presence of a state of Hell is evident in the film. Unlike the witches' cave in Shakespeare's play, the nurses of the film reveal their prophecies in an industrial room, only accessible through a caged elevator. The area, described by critic Nicholas de Jongh is an "atmosphere of existential strangeness... a murky limbo." At the end of play, after the beheading of Macbeth, Macbeth and Lady Macbeth are seen descending into the room, presumably entering the gates of Hell. By using the state of Hell, Rupert Goold makes his film more dramatic and frightening.

The murder scenes of Rupert Goold's film share similar elements of Shakespeare's play; however, Rupert Goold implements more details in the murder scenes. Not unlike Shakespeare's play, there are no visualizations of the murder of the King Duncan of Scotland. The only evidence of the act were the bloody knives and bloody hands of Macbeth used in the execution. Unlike Shakespeare's play, the murder of Banquo occurs in a public setting. By having the execution of Banquo on a train, Goold stresses the power and boldness of Macbeth.

Through his film, Goold introduces an element of absurdity to several scenes. Before the murder of Banquo, Rupert Goold

Web matches > sparksnotes.com ✕

STUDENT'S PASSAGE

Many of Shakespeare's plays were published in editions of **varying quality and accuracy in his lifetime. However, in 1623, two fellow actors and friends of Shakespeare's**, John Heminges and Henry Condell, published a more definitive text

[Comment](#)

TOP MATCH

Of my favorite plays there is inconsistency, illustrating **varying quality and accuracy in his lifetime. However, in 1623, two fellow actors and friends of Shakespeare's**, developed a new way to translate and preserve the content language

SparksNotes - Macbeth Act III: The return of Macb...
<http://sparksnotes.macbethingstoreadthataveeryimportant...>

[↔](#) Relevant dokumentation i hjälpcentret

[Köra en plagiatrapport på en uppgift](#)



Vad är detta?

De avancerade funktionerna i Google Meet inkluderar bland annat livestreaming, smågrupper, mötesinspelningar som sparas i Drive, närvarorapporter och möten med upp till 250 deltagare.

Användningsområden

Säkra videomöten



[Stegvisa anvisningar](#)

Öka säkerheten under videokonferenser



[Stegvisa anvisningar](#)

Spela in lektioner



[Stegvisa anvisningar](#)

Spela in lärmöten



[Stegvisa anvisningar](#)

Missade lektioner



[Stegvisa anvisningar](#)

Livstreama möten



[Stegvisa anvisningar](#)

Livstreama evenemang på skolan



[Stegvisa anvisningar](#)

Ställa frågor



[Stegvisa anvisningar](#)

Samla in åsikter



[Stegvisa anvisningar](#)

Små elevgrupper



[Stegvisa anvisningar](#)

Kontrollera närvaron



[Stegvisa anvisningar](#)

Säkra videomöten

Med Google Meet kan skolor dra nytta av samma säkra infrastruktur, inbyggda skydd och globala nätverk som Google använder för att skydda sin information och säkerställa integriteten. Du kan lita på följande säkerhetsåtgärder i Google Meet:

- ✓ **Integritet och efterlevnad:** Följer strikta säkerhetsstandarder i syfte att skydda elevernas och skolans data
- ✓ **Kryptering:** Alla data från klient till Google krypteras
- ✓ **Åtgärder mot otillåten användning:** Ge moderatorn kontroll över närvaron och se till att bara de rätta personerna deltar
- ✓ **Säker implementering, åtkomst och styrning:** Flera försiktighetsåtgärder har införts i syfte se till att möten är privata och säkra
- ✓ **Åtgärder vid incidenter:** En viktig del av Googles övergripande säkerhets- och integritetsprogram och är avgörande för efterlevnad av globala integritetsföreskrifter
- ✓ **Tillförlitlighet:** En molnintegrerad infrastruktur i flera lager som har skapats för att kunna skalas och hantera stora öknings av användare
- ✓ **Bestäm vem som går med:** Förbättrade knackningar som gör det möjligt att hantera flera förfrågningar samtidigt och blockera knackningar när vissa kriterier har uppfyllts
- ✓ **Låsinställningar:** Moderatorerna kan styra vem som chattar, presenterar eller till och med pratar under ett virtuellt möte

[Stegvisa anvisningar](#)



Hur gör jag videokonferenser ännu säkrare för skolan?”

[Stegvisa anvisningar](#)

Öka säkerheten under videokonferenser

I Teaching and Learning Upgrade och Education Plus finns ytterligare funktioner som ska motverka otillåten användning, till exempel obligatoriskt godkännande av externa deltagare, förbättrade inställningar för moderering av möten och möten med namn som fungerar som ett skydd mot att avslutade möten återanvänds. När den sista deltagaren har lämnat kan deltagarna inte gå med igen. Eleverna kan inte gå med igen såvida läraren inte startar om mötet.

- ✓ Om ett möte har ett namn kan deltagarna inte gå med på nytt när den sista deltagaren har lämnat och den tiosiffriga möteskoden fungerar inte längre.
- ✓ Eleverna kan inte gå med på nytt förrän en lärare startar om mötet med namnet.
- ✓ Lärare kan avsluta mötet för alla deltagare, vilket gör att de inte kan stanna kvar efter att läraren har lämnat.

 [Relevant dokumentation i hjälpcentret](#)

[Säkerhet och integritet i Google Meet för undervisning](#) [Starta ett videomöte i Google Meet](#)

Så här gör du: Möten med namn

Så här skapar du ett möte med namn

- Använd en kort länk, till exempel `g.co/meet/[ANGE NAMN]`
- Öppna meet.google.com eller Google Meet-appen och ange mötets namn i fältet **Gå med i** eller **starta ett möte**

Så fungerar det

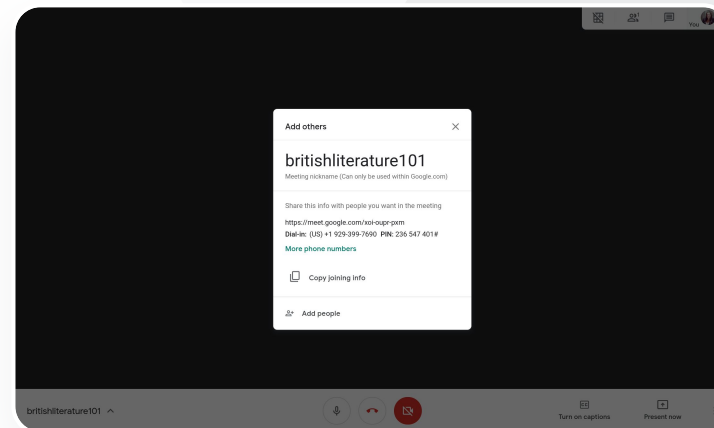
När läraren startar ett möte med ett namn skapas en tio tecken lång möteskod som tillfälligt kopplas till namnet.

När den sista personen har lämnat mötet eller när läraren avslutar mötet slutar den tillfälliga koden samt kopplingen mellan namnet och möteskoden att gälla.

Om eleverna inte har behörighet att skapa möten kan de inte använda namnet eller möteskoden.

Lärare kan återanvända mötesnamnet.

Då skapas en ny tillfällig möteskod som eleverna kan använda för att gå med i mötet igen.



[Relevant dokumentation i hjälpcentret](#)
[Säkerhet och integritet i Google Meet för undervisning](#)
[Starta ett videomöte i Google Meet](#)



Vår skola erbjuder stora onlinekurser som vi måste spela in för distansundervisning och för elever som inte kan delta.”

[Stegvisa anvisningar](#)

Spela in lektioner

Med Teaching and Learning Upgrade och Education Plus kan användarna spela in möten och automatiskt spara dem på Drive så länge det behövs. På så sätt är det enkelt att arkivera och dela lektioner, workshoppar och arbetsessioner.

- ✓ Om lärarna använder Classroom kan de skapa en unik länk för varje klass med hjälp av Google Meet-integreringen som visas i flödet i Classroom och på sidan Klassuppgifter.
- ✓ Länken ger möjlighet att låta varje klass hålla egna möten där både lärare och elever enkelt kan gå med.
- ✓ Spela smidigt in lektioner med hjälp av integreringen.

 [Relevant dokumentation i hjälpcentret](#)

[Konfigurera Google Meet för distansundervisning](#)



Vi anordnar regelbundet personalmöten online och alla möten måste spelas in. Dessutom skulle vi vilja spela in kurser för yrkesutveckling och styrelsemöten.”

[Stegvisa anvisningar](#)

Spela in lärarmöten

Med Teaching and Learning Upgrade och Education Plus sparas **inspelade videomöten** automatiskt i Drive så länge användaren behöver inspelningen. På så sätt är det enkelt att arkivera och dela möten, kurser för yrkesutveckling och styrelsemöten.

- ✓ Vi rekommenderar att IT-administratören aktiverar inspelning för enbart fakultet och personal.
- ✓ Du kan lägga till separata organisationsenheter för fakultet och elever och sedan tillämpa separata regler.
- ✓ Om du använder Classroom och har verifierade lärare kan du aktivera åtkomst för lärargruppen.

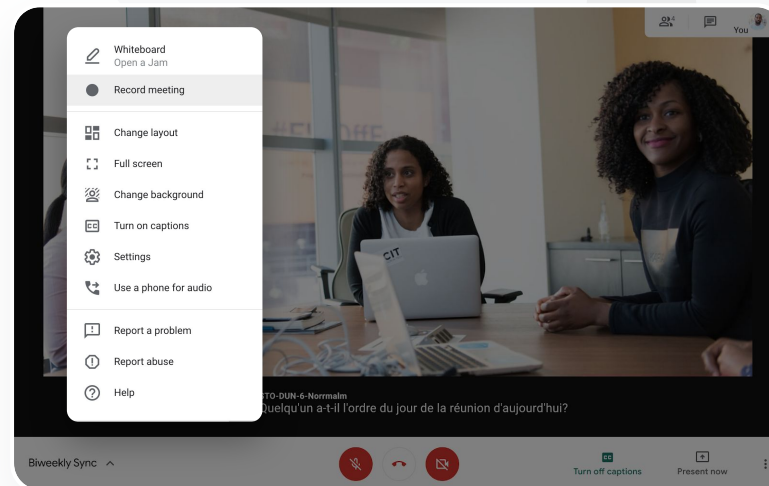
 [Relevant dokumentation i hjälpcentret](#)

[Konfigurera Google Meet för distansundervisning](#)

Så här gör du: Inspelningar

Så här spelar du in ett möte

- Öppna mötet via Kalender och välj Anslut via Google Meet.
- På bekräftelsesidan för möten ska du öppna alternativmenyn genom att välja de tre lodrätta punkterna nere till höger.
- Klicka på **spela in möte**. En röd prick visas nere till höger på skärmen för att visa att ett möte spelas in.
- En videofil med mötet sparas automatiskt i Drive.



[↗](#) Relevant dokumentation i hjälpcentret

[Konfigurera Google Meet för distansundervisning](#)



Jag vill titta på en
inspelad lektion från när
jag inte kunde delta.”

[Stegvisa anvisningar](#)

Missade lektioner

Alla användare har åtkomst till Drive-lagring på skolans domän och inspelningar av videomöten sparas automatiskt i mötesarrangörens Drive om du använder Teaching and Learning Upgrade och Education Plus. Om du vill titta på det inspelade mötet ber du arrangören om en länk till inspelningen eller öppnar den via Kalender-händelsen.

- ✓ Inspelningar sparas i mötesarrangörens Drive.
- ✓ Mötesdeltagare i samma organisationsenhet som mötesarrangören beviljas automatiskt åtkomst till inspelningen.
- ✓ Om mötesarrangören ändras skickas länken till inspelningen till den som ursprungligen skapade mötet.

 [Relevant dokumentation i hjälpcentret](#)

[Spela in ett videomöte](#)

Så här gör du: Visa och dela inspelningar

Så här delar du en inspelning

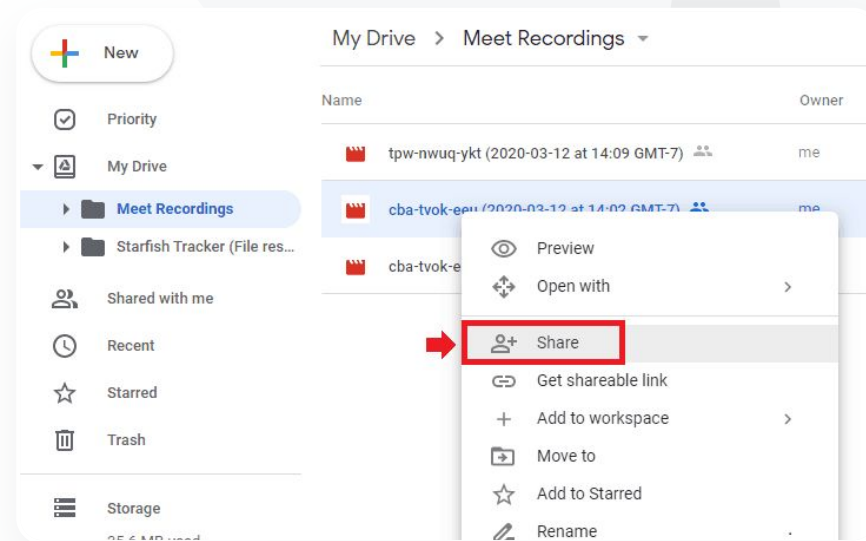
- Välj filen.
- Klicka på ikonen för Dela. **ELLER**
- Lägg till godkända tittare.
- Välj ikonen för Länk.
- Klistra in länken i ett e-postmeddelande eller ett meddelande i Chat.

Så här laddar du ned en inspelning

- Välj filen.
- Klicka på ikonen för Mer > Ladda ned.
- Spela upp filen genom att dubbelklicka på den.

Så här spelar du upp inspelningen i Drive

- Öppna Drive och dubbelklicka på filen med inspelningen när du vill spela upp den. Meddelandet Bearbetas fortfarande visas tills filen kan visas online.
- Om du vill lägga till en inspelning i din Drive markerar du filen och klickar på Lägg till på min enhet.



[Relevant dokumentation i hjälpcentret](#)

[Spela in ett videomöte](#)



Vi måste kunna livestreama våra personal- och fakultetsmöten till andra berörda parter och föräldrar.”

[Stegvisa anvisningar](#)

Livestreama möten

Livestreama till upp till 10 000 tittare på domänen med Teaching and Learning Upgrade och upp till 100 000 tittare på domänen med Education Plus. Deltagare kan gå med genom att välja länken till livestreamen som tillhandahålls av arrangören via e-post eller en inbjudan i Kalender. Prata med IT-administratören för att se till att du har behörighet att streama live.

- ✓ Vi rekommenderar att IT-administratören aktiverar livestreaming för enbart fakultet och personal.
- ✓ Vid stora evenemang kan du få en bättre upplevelse genom att streama live i stället för att användarna ansluter till ett interaktivt videomöte.
- ✓ Om en användare inte kan delta i livestreamen kan han eller hon titta på den när mötet är avslutat.

 [Relevant dokumentation i hjälpcentret](#)

[Konfigurera Google Meet för distansundervisning](#)



Vi gillar att livestreama idrottsevenemang och andra viktiga evenemang, som examensceremonin eller balen, för de som inte kan delta på plats.”

[Stegvisa anvisningar](#)

Livestreama evenemang på skolan

Sänd live till hela skolan med **livestreaming**. Välj bara länken för livestreamen som du får från arrangören via e-post eller Kalender-händelsen. Kontakta IT-administratören och se till att du har behörighet att streama live. Annars kan du [titta på inspelningen](#) när mötet är avslutat.

- ✓ Med livestreaming i Google Meet kan du få kontakt med alla som är engagerade i skolan genom att streama examensceremonier, idrottsevenemang eller föräldramöten live.
- ✓ Livestreama till upp till 10 000 tittare på domänen med Teaching and Learning Upgrade och upp till 100 000 tittare på domänen med Education Plus.

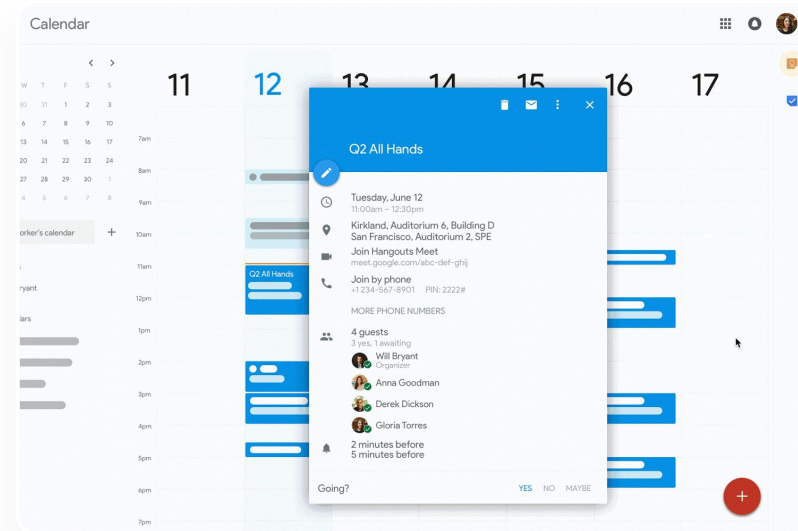
[🔗](#) Relevant dokumentation i hjälpcentret

[Konfigurera Google Meet för distansundervisning](#)

Så här gör du: Livestreaming

Så här ger du behörighet att streama live

- Öppna Google Kalender.
- Välj + Skapa > Fler alternativ.
- Lägg till händelseinformation såsom datum, tid och beskrivning.
- Lägg till upp till 250 gäster som kan delta i videomötet fullt ut, vilket innebär att andra kan se och höra dem och att de kan presentera. Det går att lägga till personer från andra organisationer.
- Klicka på **Lägg till Konferens > Meet**.
- Bredvid Gå med i Meet väljer du **nedåtpilen** och sedan **Lägg till livestream**.
- Du kan bjuda in så många personer på domänen som tillåts enligt betallicensen genom att klicka på **Kopiera** och sedan dela webbadressen till livestreamen i ett e-postmeddelande eller meddelande i Chat.
- Välj **Spara**.
- Streamingen startar inte automatiskt. Under mötet ska du välja **Mer > Starta streaming**.



[↗](#) Relevant dokumentation i hjälpcentret

[Konfigurera Google Meet för distansundervisning](#)

Obs! Enbart gäster i organisationen kan se livestreamen.

”

Jag behöver snabbt kunna ställa frågor, kontrollera vad eleverna kan och interagera med klassen för att engagera dem.”

[Stegvisa anvisningar](#)

Ställa frågor

Med funktionen **Frågor och svar** i Google Meet kan du se till att eleverna är engagerade och göra lektionen mer interaktiv. Pedagoger får till och med en detaljerad rapport över alla frågor och svar i slutet av den virtuella lektionen.

- ✓ Moderatorer kan ställa så många frågor de vill. De kan dessutom filtrera bort eller sortera frågor, markera dem som besvarade eller dölja eller prioritera dem.
- ✓ Efter varje möte där frågor var aktiverade får moderatoren en frågerapport automatiskt till sin e-postadress.

 [Relevant dokumentation i hjälpcentret](#)

[Ställa frågor till deltagarna i Google Meet](#)

Så här gör du: Frågor och svar

Ställa en fråga:

- Välj ikonen för Aktiviteter uppe till höger i ett möte > **Frågor (Aktivera Frågor och svar genom att välja Aktivera Frågor och svar)**
- Fråga något genom att klicka på **Ställ en fråga** nere till höger.
- **Skriv frågorna > välj Lägg upp.**

Visa frågerapporten:

- Efter mötet får moderatorn **en frågerapport via e-post.**
- Öppna e-postmeddelandet > klicka på **den bifogade rapporten.**



[↔](#) Relevant dokumentation i hjälpcentret

[Ställa frågor till deltagarna i Google Meet](#)



Jag behöver enkelt kunna samla in åsikter från både elever och andra pedagoger medan jag håller i en lektion eller ett personalmöte.”

[Stegvisa anvisningar](#)

Samla in åsikter

Den person som schemalade eller startade ett virtuellt möte kan skapa en **omröstning** för deltagarna i mötet. Med hjälp av den här funktionen går det att sammanställa information från alla elever eller deltagare i mötet på ett snabbt och engagerande sätt.

- ✓ Moderatorerna kan spara en omröstning och lägga upp den senare under mötet. Omröstningarna sparas i avsnittet Omröstningar i ett virtuellt möte.
- ✓ Efter mötet skickas en rapport med omröstningens resultat till moderatorns e-postadress.

 [Relevant dokumentation i hjälpcentret](#)

[Genomföra omröstningar i Google Meet](#)

Så här gör du: Genomföra omröstningar



Skapa en omröstning:

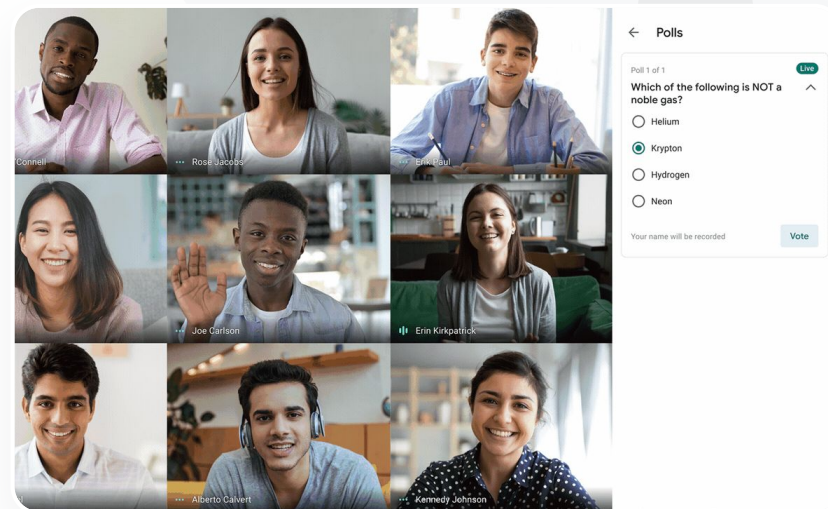
- Välj ikonen för Aktiviteter uppe till höger i ett möte > Omröstning.
- Välj Starta en omröstning.
- Skriv en fråga.
- Välj Starta eller Spara.

Moderera en omröstning:

- Välj ikonen för Aktiviteter uppe till höger i ett möte > Omröstning.
- Bredvid Visa resultatet för alla flyttar du reglaget till på om du vill låta deltagarna se resultatet i omröstningen.
- Stäng en omröstning och sluta tillåta svar genom att klicka på Avsluta omröstningen.
- Du kan radera en omröstning permanent genom att välja ikonen för Radera.

Visa en omröstningsrapport:

- Efter mötet får moderatorn en rapport via e-post.
- Öppna e-postmeddelandet > välj den bifogade rapporten.



[🔗](#) Relevant dokumentation i hjälpcentret

[Genomföra omröstningar i Google Meet](#)



Vi undervisar enbart på distans och måste enkelt kunna återskapa enkelheten i att dela in barnen i grupper, gå runt i rummet och lyssna, delta i diskussioner och enkelt kunna sammanföra gruppen igen.”

[Stegvisa anvisningar](#)

Små elevgrupper

Med funktionen **Smågrupper** kan pedagoger dela in eleverna i mindre grupper under virtuella lektioner. Smågrupper måste startas av moderatorer under ett videosamtal på en dator. Det går för närvarande inte att livestreama eller spela in smågrupper.

- ✓ Skapa upp till 100 smågrupper per virtuellt möte.
- ✓ Läraren kan enkelt hoppa mellan de olika smågrupperna när deltagarna behöver hjälp.
- ✓ Administratörerna kan se till att enbart fakultet eller personal kan skapa smågrupper.

 [Relevant dokumentation i hjälpcentret](#)

[Använda smågrupper i Google Meet](#)

Så här gör du: Skapa smågrupper

Så här skapar du smågrupper

- Starta ett videosamtal.
- Välj ikonen för **Aktiviteter uppe till höger > Smågrupper**.
- I panelen för smågrupper väljer du det antal smågrupper du behöver.
- Eleverna delas sedan in i de olika grupperna, men moderatorer kan manuellt flytta dem till olika grupper om det behövs.
- Klicka på **Öppna rum** nere till höger.

Svara på frågor i olika smågrupper

- Det visas en avisering längst ned på moderatorns skärm när deltagarna ber om hjälp. Välj **Gå med** för att gå med i deltagarens smågrupp.



[Relevant dokumentation i hjälpcentret](#)

[Använda smågrupper i Google Meet](#)



Det är svårt att hålla koll på vilka som deltar i lektionerna online. Jag måste enkelt kunna rapportera närvaron för klasser på hela domänen.

[Stegvisa anvisningar](#)

Kontrollera närvaron

Med **Närvarospårning** får du en automatisk närvarorapport för alla möten med minst fem deltagare. I rapporterna finns information om vem som deltog i samtalet, deltagarnas e-postadresser och hur länge de deltog i den virtuella lektionen.

- ✓ Du kan hålla koll på närvaron under livestreamade evenemang genom med hjälp av livestreamingrapporter.
- ✓ Moderatorer kan aktivera eller inaktivera närvarospårning och livestreamingrapporter i mötet eller via händelsen i Kalender.

 [Relevant dokumentation i hjälpcentret](#)

[Spåra närvaro i Google Meet](#)

Så här gör du: Närvarorapporter

Så här gör du i ett möte:

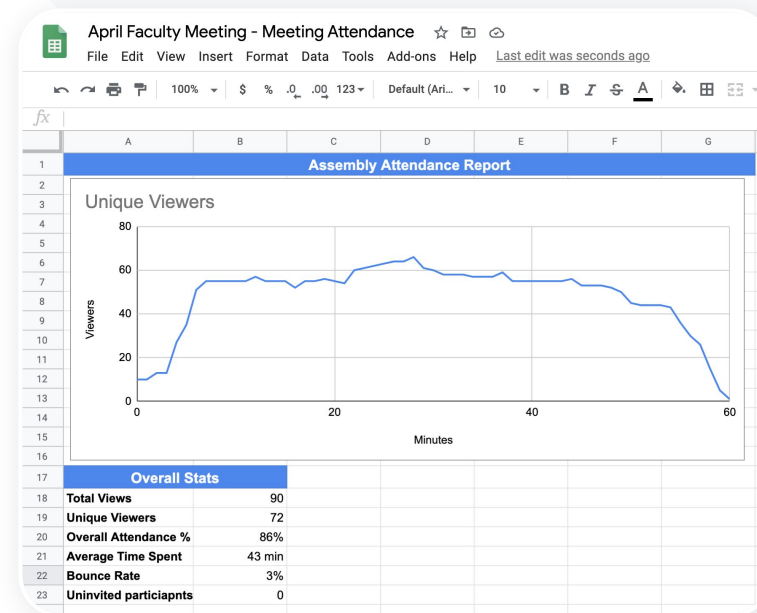
- Starta ett videosamtal.
- Välj menyikonen längst ned.
- Välj Inställningar > Värdkontroller.
- Aktivera eller inaktivera Närvarospårning.

Så här gör du i Kalender:

- Aktivera Google Meet-konferenser i en Kalender-händelse.
- Välj Inställningar till höger.
- Närvarospårning > på Spara.

Så här får du en närvarorapport:

- Efter mötet får moderatorn rapporten via e-post.
- Öppna e-postmeddelandet > välj den bifogade rapporten.



[🔗](#) Relevant dokumentation i hjälpcentret

[Spåra närvaro i Google Meet](#)

Tack