Google for Education

Över 40 sätt att använda betalutgåvorna av Google Workspace for Education

goo.gle/use-edu-workspace

Så här ska presentationen användas

Presentationen består av ett urval av de användningsfall 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 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 betalutgåvorna av 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 du kan uppfylla organisationens behov.

Google Workspace for Education Plus

Här ingår Education Standard, Teaching and Learning Upgrade och andra funktioner som bara finns i Plus.

Education Plus ger elever, lärare, utbildningsledare och IT-administratörer en **allt-i-ett-lösning** för utbildningsteknik och lättanvända verktyg för **avancerad säkerhet och bättre insikter, samt berikad undervisning och inlärning**.

Google Workspace for Education Standard

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

Teaching and Learning Upgrade

Förbättrade undervisnings- och inlärningsverktyg gör det enklare att undervisa på ett sätt som ger inverkan eftersom inlärningen blir mer anpassad. Det förbättrar effektiviteten i klassrummet och gör det möjligt att undervisa och lära var som helst.

Innehållsförteckning

Avancerade säkerhets- och insiktsfunktioner

Säkerhetsöversikten

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

Sidan Säkerhetsstatus

- Metodtips för säkerhet
- Rekommendationer för utsatta områden

Utredningsverktyget

- Otillåtet material som delas
- Filer som delas av misstag
- E-post med nätfiske och skadlig programvara
- Stoppa skadliga aktörer
- Mer detaljerade säkerhetsinsikter
- Förhindra möten som inte kontrolleras

Domänhantering och -kontroll

- Skanna Gmail-bilagor för att upptäcka hot
- Skapa översikter och rapporter om användning
- Hitta filer enklare
- Organiserade interna dokument
- Fylla i avdelningsgrupper automatiskt
- Skapa en målgrupp för intern fildelning
- Begränsa fildelning
- Begränsningar för Workspace-appen
- Hantera lagringsutrymme
- Dataregleringar
- Riktlinjer för anslag
- Hantera ändpunktsenheter
- Hantera Windows-enheter
- Anpassade inställningar för Windows-enheter
- Automatisera uppdateringar till Windows-enheter
- Dra nytta av kryptering på klientsidan

Innehållsförteckning

Förbättrade undervisnings- och inlärningsfunktioner

Google Classroom

- Hantera åtkomst till Classroom-tillägg
- Integrera engagerande innehåll i Classroom
- Skapa klasser i stor skala

Plagiatrapporter

- Sök efter plagiat med plagiatrapporter
- Utför plagiatkontroll genom att jämföra med tidigare elevinlämningar
- Ge eleverna möjlighet att lära sig av plagiat

Dokument, Kalkylark och Presentationer

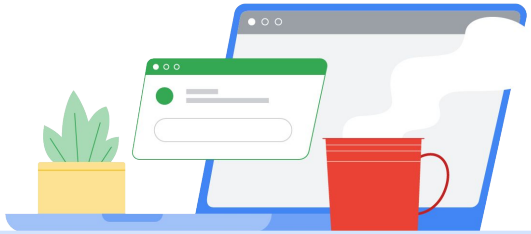
- Godkänna interna dokument

Google Meet

- Spela in möten
- Hänvisa till det som har tagits upp under lektioner
- Undanröja språkbarriärer
- Sända samlingar och skolevenemang
- Ställa frågor
- Samla in åsikter
- Små elevgrupper
- Kontrollera närvaron

Avancerade säkerhets- och insiktsfunktioner

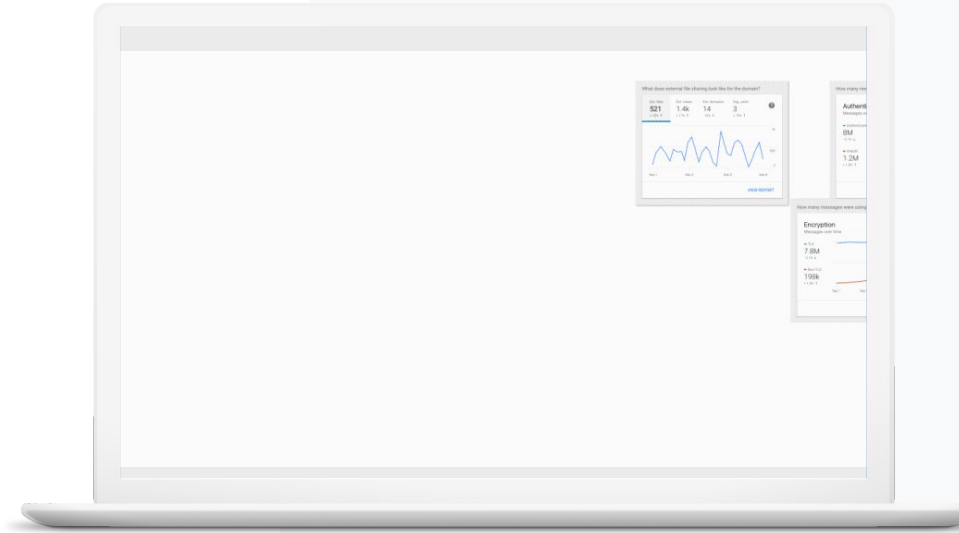
Få större kontroll över hela domänen med hjälp av proaktiva säkerhetsverktyg som ger skydd mot hot, gör det möjligt att analysera säkerhetsincidenter och skyddar elevernas och lärarnas data.



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

“

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

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

Stegvisa anvisningar

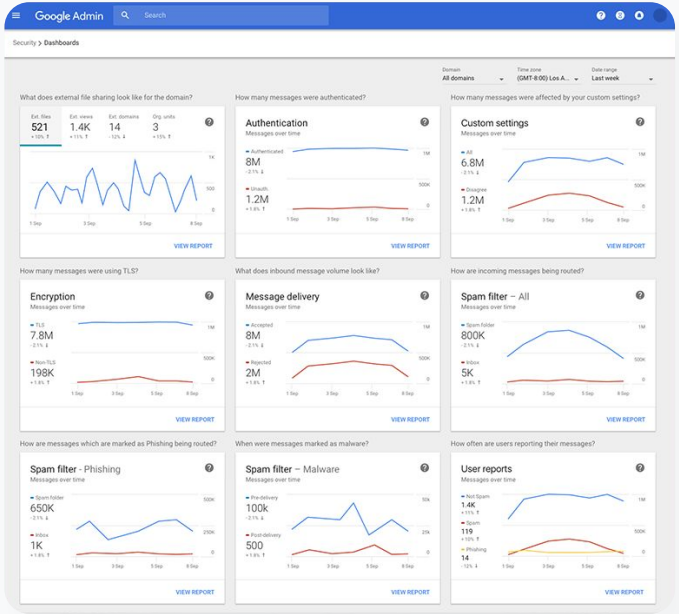
Relevant dokumentation i hjälpcentret

- Om säkerhetsöversikten

Så här gör du: Översikten

Så här visar du säkerhetsöversikten:

- 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.”

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 angiven tidsperiod

Stegvisa anvisningar

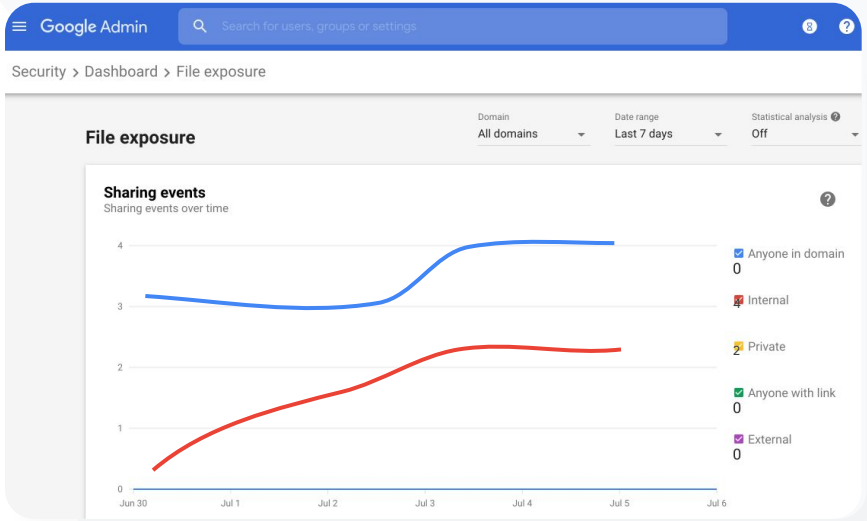
Relevant dokumentation i hjälpcentret

- Kom igång med sidan Säkerhetsstatus

Så här gör du: Extern fildelning

Så här visar du rapporten Filexponering:

- 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

Appar från tredje part

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

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

Stegvisa anvisningar

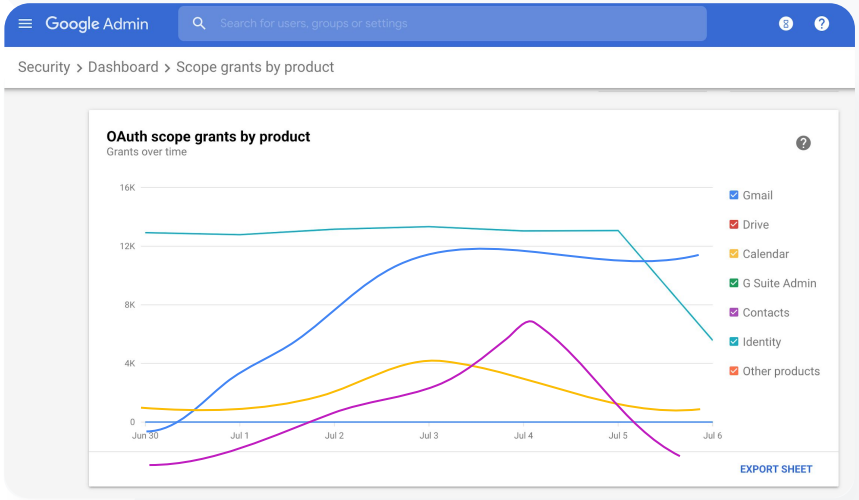
Relevant dokumentation i hjälpcentret

- Rapport över aktivitet för OAuth-beviljande

Så här gör du: Appar från tredje part

Så här visar du rapporten över aktivitet för OAuth-beviljanden:

- 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
- Vill du filtrera informationen klickar du på **App**, **Omfattning** eller **Användare**
- Vill du skapa en kalkylarksrapport ska du klicka på **Exportera kalkylark**



Relevant dokumentation i hjälpcentret

- Rapport över aktivitet för OAuth-beviljande

“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 hen utsattes för.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Hur markerar användarna sin e-post?
- Användarrapporter

Försök till nätfiske

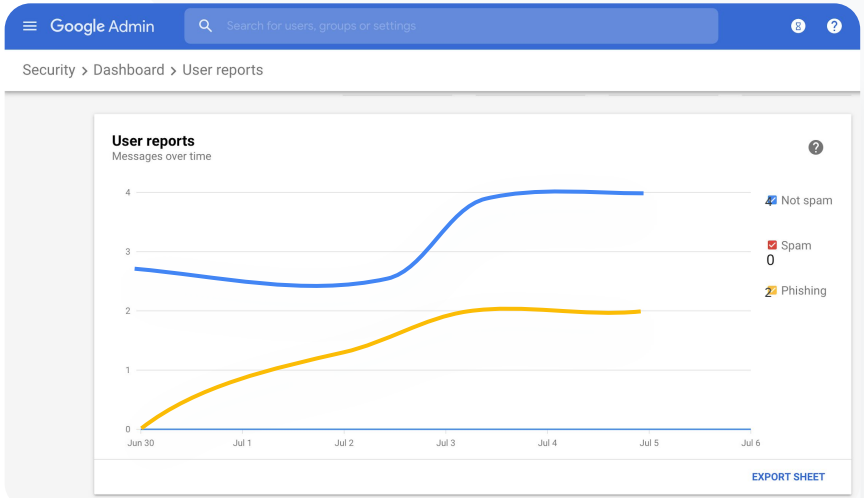
I **panelen Användarrapporter** i **säkerhetsöversikten** kan du se meddelanden som har flaggats som nätfiske eller skräppost under en viss tidsperiod. Du kan visa information om e-postmeddelanden som har flaggats som nätfiske, till exempel dess mottagare och hur många gånger det har öppnats.

- Med användarrapporter kan du se hur användarna markerar sina meddelanden, som skräppost, inte skräppost eller nätfiske, under en viss tidsperiod
- Du kan anpassa diagrammet så det endast visar information om vissa typer av meddelanden, till exempel om meddelandena skickades internt eller extern, enligt ett datumintervall, och så vidare

Så här gör du: Försök till nätfiske

Så här visar du panelen Användarrapporter:

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



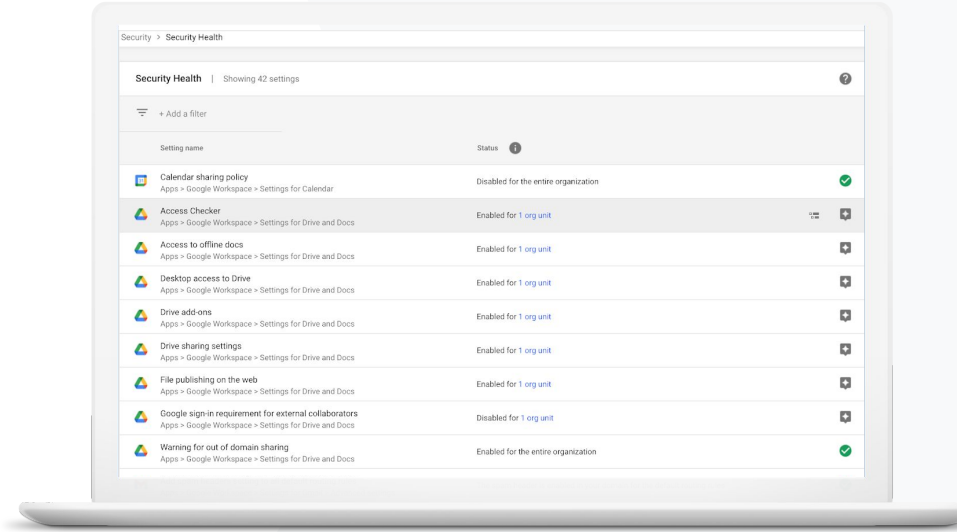
Relevant dokumentation i hjälpcentret

- 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

Metodtips för säkerhet	Stegvisa anvisningar
Rekommendationer för utsatta områden	Stegvisa anvisningar

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

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

Stegvisa anvisningar

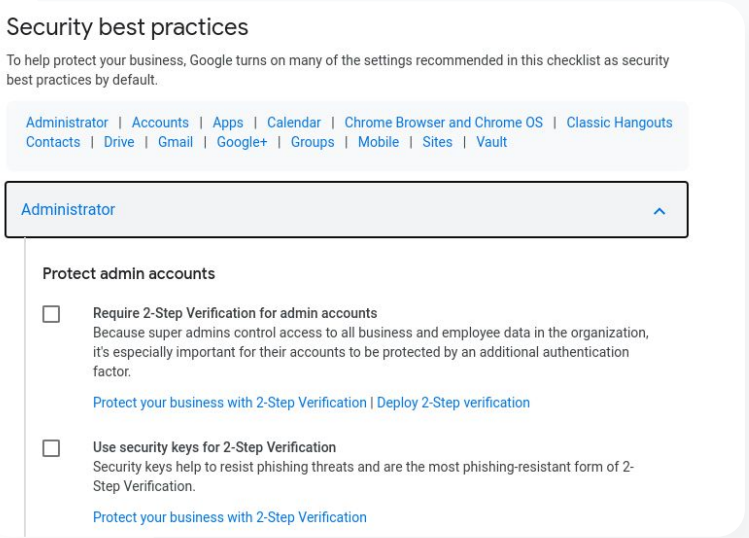
Relevant dokumentation i hjälpcentret

- Kom igång med sidan Säkerhetsstatus

Så här gör du: Checklista med metodtips för säkerhet

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

- **Administratör:** Skydda administratörskonton
- **Konton:** 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



Relevant dokumentation i hjälpcentret

- Övervaka status för dina säkerhetsinställningar

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

Rekommendationer för utsatta områden

På sidan **Säkerhetsstatus** kan du granska säkerhetskonfigurationen 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
- Läsa ytterligare information och supportartiklar om rekommendationerna

Stegvisa anvisningar

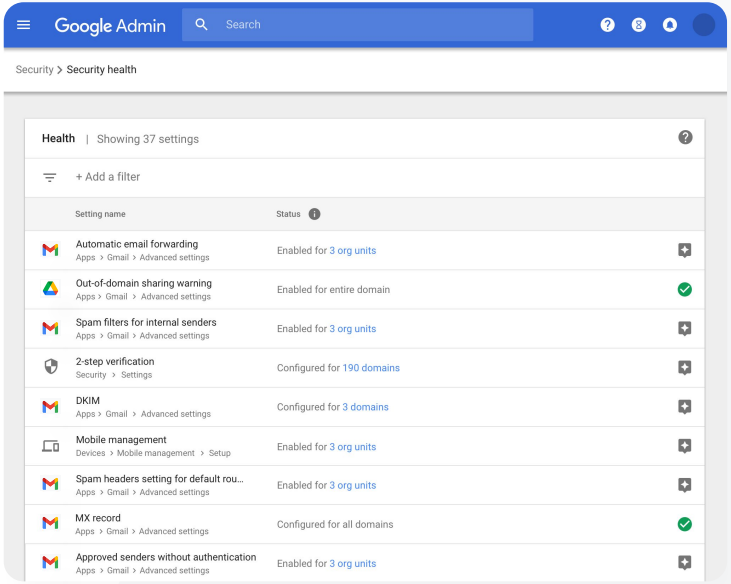
Relevant dokumentation i hjälpcentret

- 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 ikonen visas mer information och anvisningar



Relevant dokumentation i hjälpcentret

- Kom igång med sidan Säkerhetsstatus

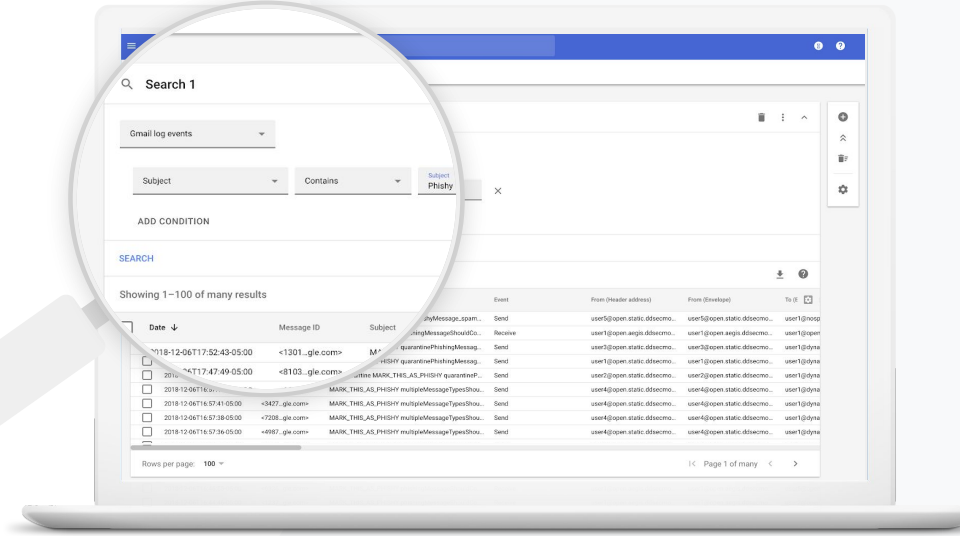
Utredningsverktyget

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
Mer detaljerade säkerhetsinsikter	Stegvisa anvisningar
Förhindra möten som inte kontrolleras	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

Relevant dokumentation i hjälpcentret

- Villkor för logghändelser för Drive
- Åtgärder för logghändelser för Drive

Otillåtet material som delas

Logghändelser för Drive i **utredningsverktyget** kan göra det enklare att hitta, spåra och isolera eller radera oönskade filer på domänen. Med logghändelsedata för Drive kan du

- söka efter dokument utifrån namn, aktör, ägare med mera
- vidta åtgärder genom att ändra filbehörigheterna eller radera filen
- söka i innehåll som användare skapar i Google Workspace och innehåll som de laddar upp på Drive
- 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

“

En fil har av misstag delats med en grupp som INTE ska ha åtkomst till den.

Jag vill ta bort deras åtkomst till den.”

Filer som delas av misstag

Logghändelser för Drive i **utredningsverktyget** kan göra det enklare att hitta och lösa fildelningsproblem. Med händelsedata i Drive-loggar kan du

- 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

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Kör en sökning i utredningsverktyget
- Vidta åtgärder baserat på sökresultat

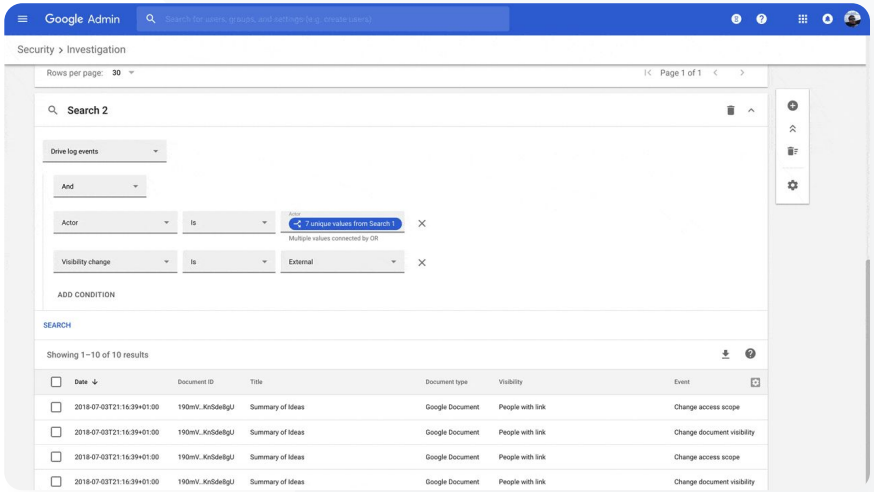
Så här gör du: Logghändelser för Drive

Så här undersöker du logghändelser för Drive:

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

Så här vidtar du åtgärder:

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



Relevant dokumentation i hjälpcentret

- Kör en sökning i utredningsverktyget
- Vidta åtgärder baserat på sökresultat

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

> 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

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

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
- Visa VirusTotal-rapporter

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
- Genomsöka e-postbilagor och få detaljerad data om hotkontext och anseende med VirusTotal-rapporter
- Vidta åtgärder genom att markera meddelanden som skräppost eller nätfiske, skicka dem till en viss inkorg eller till karantän eller radera dem

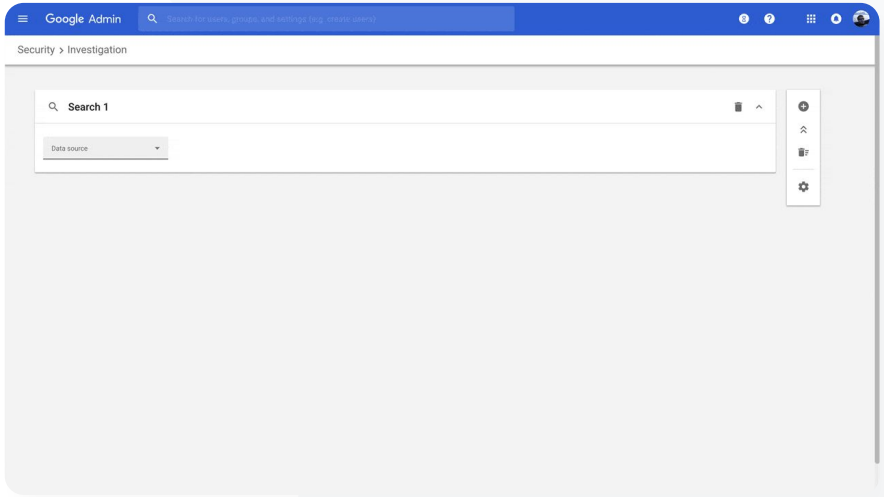
Så här gör du: Gmail-loggar

Så här går du igenom Gmail-loggar:

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

Så här vidtar du åtgärder:

- Välj den relevanta filen i sökresultatet
- Klicka på **Åtgärder**
- Välj **Radera meddelandet 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 kan jag stoppa det här?”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Söka efter och utreda händelser i användarloggen
- Skapa aktivitetsregler med utredningsverktyget

Stoppa skadliga aktörer

Med **användarloggen** i **utredningsverktyget** kan du

- identifiera och utreda försök att kapa användarkonton i organisationen
- kontrollera vilka tvåstegsmetoder som användarna i organisationen använder
- läsa 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

Så här gör du: Stoppa skadliga aktörer

Så här undersöker du logghändelser för användare:

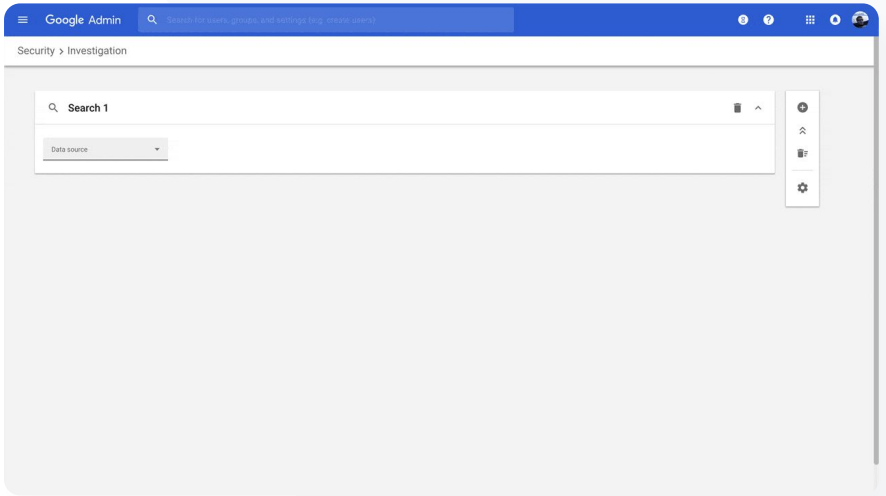
- Logga in på **administratörskonsolen**
- Klicka på **Säkerhet** > **Utredningsverktyg**
- Välj **Logghändelser för användare**
- Klicka på **Lägg till villkor** > **Sök**

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

En av våra lärare har berättat att en bifogad fil i Gmail ser misstänkt ut.

Kan IT-personalen avgöra om filen är ett säkerhetshot?”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Kör en sökning i utredningsverktyget
- Visa VirusTotal-rapporter från utredningsverktyget

Få djupare säkerhetsinsikter

VirusTotal-rapporter innehåller mer information om resultatet av en säkerhetsutredning. Det finns bland annat en omfattande översikt som administratörer kan utgå från när de ska kontrollera säkerheten för en specifik domän, filbilaga, IP-adress eller webbadress baserat på crowdsourcade insikter.

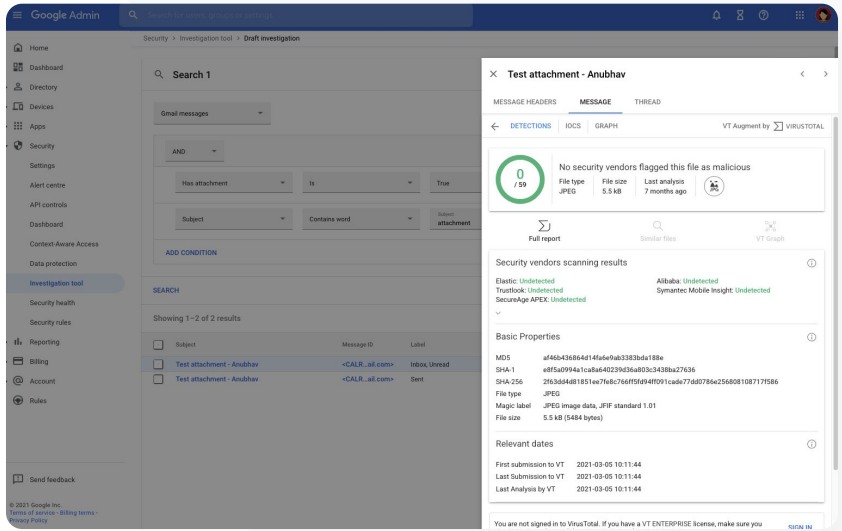
- Få ytterligare säkerhetsinsikter om logghändelser för Gmail och Chrome
- Analysera misstänkta filer, webbadresser, domäner och IP-adresser
- Få crowdsourcad information om varför en bilaga eller webbplats kanske betraktas som riskabel
- Få hjälp med att fatta beslut när du tar itu med säkerhetsfrågor

Så här gör du: Få djupare säkerhetsinsikter

Så här visar du VirusTotal-rapporter om Gmail:

- Logga in på **administratörskonsolen**
- Klicka på **Säkerhet** > **Säkerhetscenter** > **Utredningsverktyg**
- Välj **Gmail-meddelanden**
- Klicka på **Lägg till villkor** > **Har bilaga**
- Klicka på **meddelande-id:t** eller **ämneslänken** bland sökresultaten
- Klicka på någon av flikarna **Meddelande** eller **Tråd** på sidopanelen
- Välj **Visa VirusTotal-rapport**

Administratörer kan också visa VirusTotal-rapporter om Chrome. Följ bara anvisningarna ovan och välj **Logghändelser för Chrome** i utredningsverktyget.



Relevant dokumentation i hjälpcentret

- Visa VirusTotal-rapporter från utredningsverktyget

Elever stannar kvar i Google Meet-samtal efter att lektionen är slut. Jag behöver kunna avsluta Meet-samtalet för alla så det inte stör undervisningen.”

Förhindra virtuella möten som inte kontrolleras

Google Workspace-administratörer kan använda åtgärden **Avsluta möte för alla** i utredningsverktyget för att ta bort alla användare från ett möte i organisationen. Mötesvärdar kan även göra detta för enskilda Google Meet-samtal.

- Mötet avslutas för alla användare som är med för närvarande, även de som är i smågrupper
- Det förhindrar att någon deltar i framtida förekomster av mötet utan att värden är närvarande

Stegvisa anvisningar

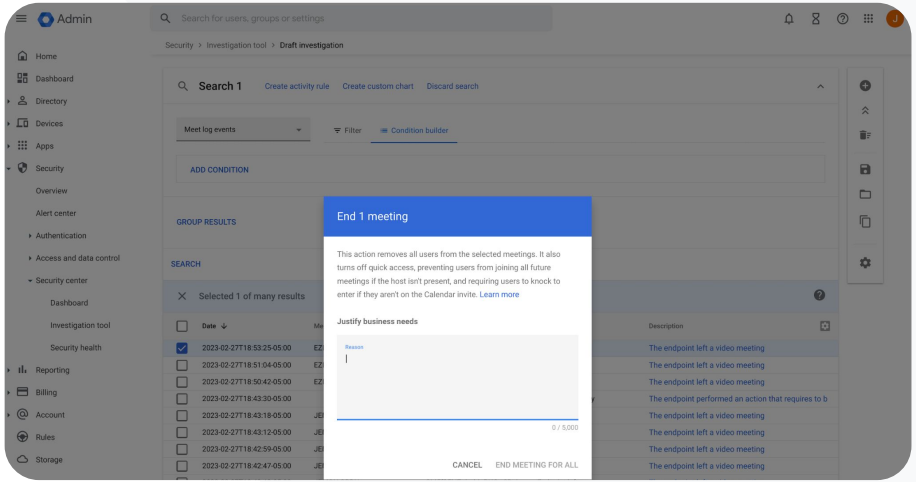
Relevant dokumentation i hjälpcentret

- Avsluta möten med hjälp av utredningsverktyget

Så här gör du: Förhindra virtuella möten som inte kontrolleras

Så här avslutar du ett möte för alla användare med hjälp av utredningsverktyget:

- Logga in på **administratörskonsolen**
- Klicka på **Säkerhet** > **Säkerhetscenter** > **Utredningsverktyg**
- Välj **Logghändelser för Meet**
- Klicka på **Sök**. I sökresultaten visas en lista med logghändelser för Meet
- Markera rutorna för de möten som du vill avsluta för alla användare
- Välj **Åtgärder**
- Klicka på **Avsluta mötet för alla**



Relevant dokumentation i hjälpcentret

- Avsluta möten med hjälp av utredningsverktyget

Domänhantering och -kontroll

Administratörer har åtkomst till avancerade verktyg i Google Workspace så de kan hantera organisationens data, ställa in kontroller, övervaka användning och göra det enklare att efterleva utbildningsstandarder.

Användningsområden

Skanna G-mailbilagor för att upptäcka hot

Skapa översikter och rapporter om användning — Stegvisa anvisningar

Hitta filer enklare — Stegvisa anvisningar

Organisera interna dokument — Stegvisa anvisningar

Fylla i avdelningsgrupper automatiskt — Stegvisa anvisningar

Skapa målgrupper för intern fildelning — Stegvisa anvisningar

Begränsa fildelning — Stegvisa anvisningar

Begränsningar för Workspace-appen — Stegvisa anvisningar

Hantera lagringsutrymme — Stegvisa anvisningar

Datareglerингar — Stegvisa anvisningar

Riktlinjer för anslag — Stegvisa anvisningar

Hantera ändpunktsenheter — Stegvisa anvisningar

Hantera Windows-enheter — Stegvisa anvisningar

Anpassade inställningar för Windows-enheter — Stegvisa anvisningar

Automatisera uppdateringar till Windows-enheter — Stegvisa anvisningar

Dra nytta av kryptering på klientsidan — Stegvisa anvisningar

“

Hur kan jag bättre skydda min domän mot noll-dagars skadlig kod och utpressningsvirus?”

Skanna Gmail-bilagor för att upptäcka hot

E-postbilagor kan innehålla skadlig programvara. För att upptäcka dessa hot kan Gmail skanna eller använda funktioner i Säkerhetssandlåda. Bilagor som identifierats som hot skickas till skräppostmappen.

- Upptäck skadlig programvara genom att virtuellt “starta upp” den i en privat, säker sandlådemiljö och analysera bieffekterna för att avgöra om det finns skadliga funktioner
- Skanna Microsoft Word, PowerPoint, PDF, zip-filer, och mer
- Aktivera skanning för hela domänen, eller skapa regler för genomsökningarna baserade på specifika faktorer som avsändare, domän och mer

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Skapa regler för att upptäcka skadliga bilagor

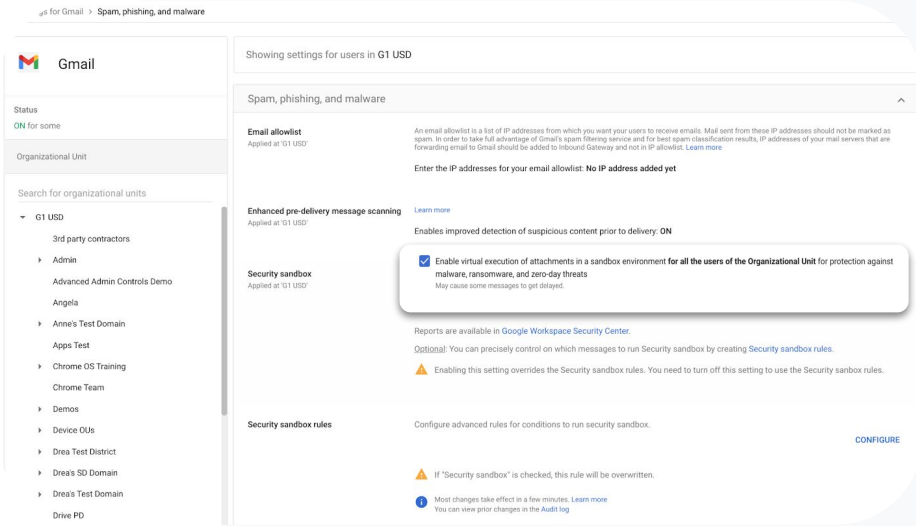
Så här gör du: Skanna Gmail-bilagor för att upptäcka hot

Så fungerar det

E-postbilagor öppnas upp i en sandlåda några minuter innan e-postmeddelandet levereras, vilket ger ett extra säkerhetslager.

Hur man skannar samtliga bilagor i säkerhetssandlådan:

- Logga in på din **administratörskonsol**
- Klicka på **Meny** > **Appar** > **Google Workspace** > **Gmail** > **Skräppost, Nätfiske, och Skadlig programvara**
- Välj en organisationsenhet eller tillämpa inställningar för hela din domän
- Skrolla till **Säkerhetssandlåda** under **Skräppost, Nätfiske, och Skadlig programvara**
- Markera rutan **Aktivera virtuell kontroll av bilagor i en sandboxmiljö**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Skapa regler för att upptäcka skadliga bilagor

Hur kan jag få koll på hur Classroom används i min domän?”

Skapa översikter och rapporter om användning

Med **mallen för BigQuery Export och Looker Studio**, analysverktyg som Looker Studio och visualiseringspartner från tredje part som är integrerade i BigQuery kan administratörer skapa anpassade instrumentpaneler och rapporter som bygger på aktivitetsloggarna från Classroom.

- Exportera loggdata för Classroom från administratörskonsolen till BigQuery och Looker Studio
- Visa snabbt användningsrapporter för hela domänen. Ta reda på vem som tog bort en elev från en klass, vem som arkiverade en klass ett visst datum och annat
- Förstå allmänna trender och agera snabbare med anpassningsbara översiktsmallar i Looker Studio

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Konfigurera en mall för BigQuery Export och Data Studio

Så här gör du: Skapa översikter och rapporter om användning

01 Skapa och exportera ett BigQuery-projekt:

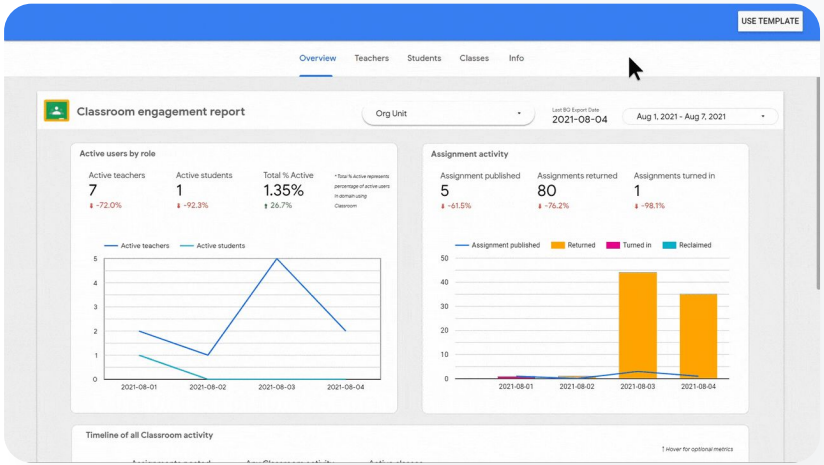
- Logga in på console.cloud.google.com > **Skapa ett nytt projekt**
- Logga in på admin.google.com > **Rapporter** > **BigQuery Export**
- Klicka på **Cloud BigQuery-projektet** > ge datasetet ett namn > **Spara**

02 Lägg till BigQuery-exporten i Looker Studio:

- Logga in i Looker Studio > **Skapa** > **Datakälla**
- Välj **BigQuery** > **Mina projekt**. Klicka på det projekt som du har skapat och sedan på **Aktivitet**
- Markera rutan under **Partitionerad tabell** och klicka på **Anslut**

03 Skapa en Looker Studio-översikt:

- Öppna mallen och välj **Använd mall**
- Under **Ny datakälla** väljer du datakälla för **aktivitet**
- Klicka på **Kopiera rapport**



Relevant dokumentation i hjälpcentret

- Konfigurera en mall för BigQuery Export och Data Studio

Jag försöker hitta medgivanden angående en utflykt som vårdnadshavare har skickat in via Gmail, Chat och Dokument.

Hur hittar jag de här filerna i min domän?”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Guide om Google Cloud Search
- Aktivera eller inaktivera Cloud Search för användare

Hitta filer enklare

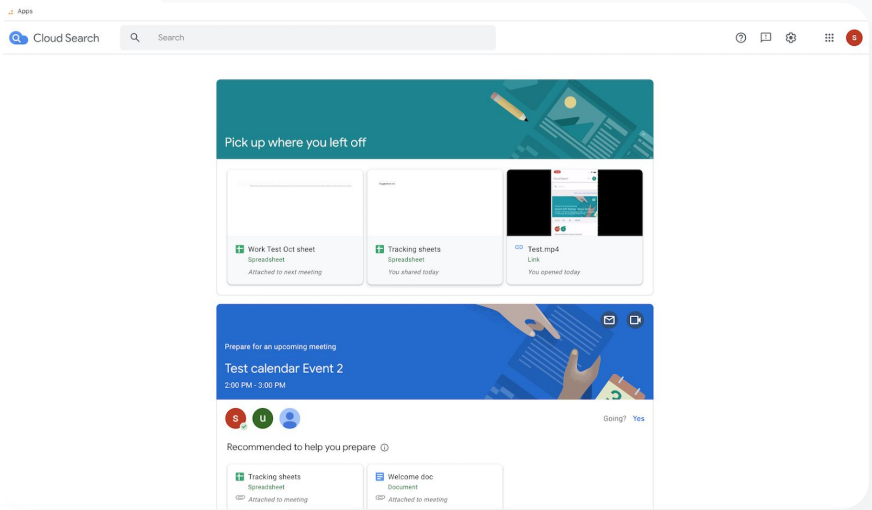
Med Google Cloud Search kan pedagoger på skolan snabbt hitta innehåll i Google Workspace och appar från tredje part.

- Hitta den information som du behöver, var du än är, på din laptop, mobiltelefon eller surfplatta
- Sök i Google Workspace-appar som Drive, Kontakter, Gmail och datakällor från tredje part

Så här gör du: Hitta filer enklare

Aktivera Cloud Search för användare:

- Logga in på **administratörskonsolen** > **Meny** > **Appar** > **Google**
- Klicka på **Tjänststatus**
- Om du vill aktivera eller inaktivera en tjänst för alla inom organisationen klickar du **På för alla** eller **Av för alla**
- Klicka på **Spara**
- Vill du aktivera en tjänst för en grupp av användare inom en organisationsenhet eller i olika organisationsenheter väljer du en **åtkomstgrupp**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Guide om Google Cloud Search
- Aktivera eller inaktivera Cloud Search för användare

> Jag vill lägga till känslighetsetiketter på skolans filer för att kunna uppfylla krav på efterlevnad, förhindra missbruk och organisera filerna bättre.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Hantera Drive-etiketter

Organisera dokument i domänen

Drive-etiketter gör det enklare för användare att hitta, organisera och tillämpa policyer i hela domänen. Administratörer kan skapa och hantera Drive-etiketter och på så sätt förhindra att filer används på fel sätt och se till att elevdata uppfyller krav på efterlevnad.

- Etiketter består av metadata som kan göra det enklare att organisera känsliga utbildningsfiler som utbildningsplaner och efterlevnadsdokument
- Endast administratörer kan skapa, definiera strukturer och publicera etiketter. Användare i organisationen kan tillämpa etiketter på de filer de redigerar och ange fältvärden
- Drive-etiketter kan användas som en del av automatiserat förebyggande av dataförlust

Så här gör du: Organisera dokument i domänen

Så fungerar det

Google Drive innehåller märkta etiketter (en visuell indikator) och standardetiketter som gör det enklare att organisera filer i domänen.

Så här aktiverar du Drive-etiketter för skolan:

- Logga in på **administratörskonsolen**
- Klicka på **Meny** > **Appar** > **Google Workspace** > **Drive och Dokument**
- Välj **Etiketter**
- **Aktivera** eller **inaktivera** etiketter
- Klicka på **Spara**

Relevant dokumentation i hjälpcentret

- Hantera Drive-etiketter

Hur kan jag automatisera gruppmedlemskap så att nya pedagoger som börjar på skolan läggs till i e-postlistan med pedagoger?”

Fylla i avdelningsgrupper automatiskt

Med **dynamiska grupper** kan administratörer uppdatera gruppmedlemskap för hela skolan med anpassade villkor.

- Skapa dynamiska grupper där medlemskap hanteras automatiskt
- Grupper hålls uppdaterade enligt en medlemskapsfråga som du skapar
- Använd dynamiska grupper som
  - e-post- och distributionslistor
  - modererade grupper och gemensamma inkorgar
  - säkerhetsgrupper

Stegvisa anvisningar

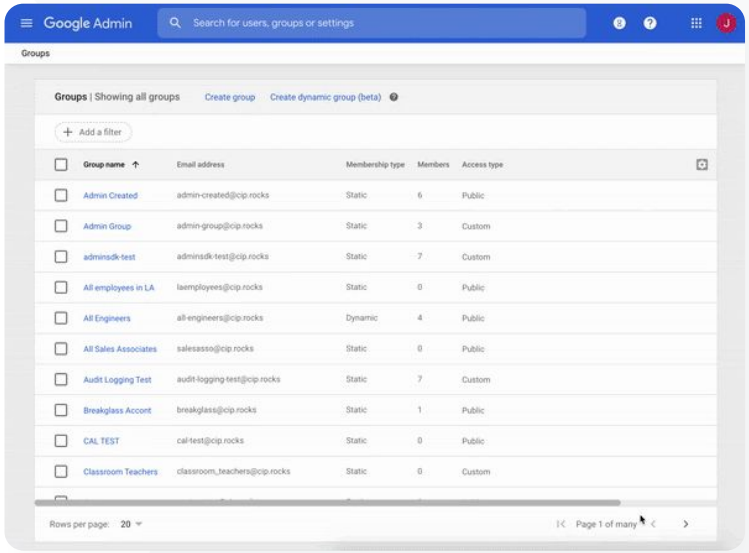
Relevant dokumentation i hjälpcentret

- Hantera medlemskap automatiskt med dynamiska grupper

Så här gör du: Fylla i grupper automatiskt

Skapa en dynamisk grupp:

- Logga in på **administratörskonsolen** och öppna **Meny** > **Katalog** > **Grupper**
- Klicka på **Skapa dynamisk grupp**
- Skapa medlemskapsfrågan med följande:
  - Villkorslista: Villkor som ska användas för medlemskapet, d.v.s. Avdelning
  - Värdefält: Det värde som du vill använda
- Ange följande uppgifter:
  - Namn: Identifierar gruppen i listor och meddelanden
  - Beskrivning: Gruppens syfte
  - E-postadress för gruppen: Den e-postadress som används för gruppen
- Klicka på **Spara**
- Klicka på **Klar**



Relevant dokumentation i hjälpcentret

- Hantera medlemskap automatiskt med dynamiska grupper

“Personalen delar ibland dokument med hela organisationen av misstag, och därmed utsätts känslig data för risker. Hur kan jag begränsa delningen så att de bara kan dela till en mindre, mer relevant grupp?”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Om målgrupper
- Metodtips för att distribuera till en målgrupp
- Skapa en målgrupp

Skapa målgrupper för intern fildelning

Inställningarna för **Målgrupp** kan bidra till att förbättra säkerheten för organisationens data eftersom risken för att användarna råkar överdela filer minskar.

- Se till att filer delas med rätt personer, som ett visst team eller en viss avdelning
- Målgrupper är grupper med människor som administratörer kan rekommendera att användare delar sina objekt med
- Administratörer kan lägga till målgrupper i delningsinställningarna för användare och på så sätt uppmuntra till att de delar med en mer specifik målgrupp
- Finns i Google Drive, Dokument och Chat

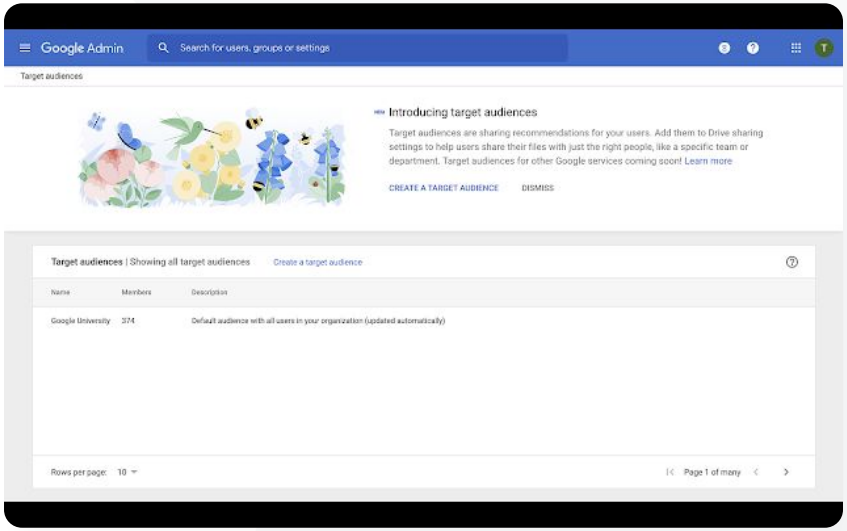
Så här gör du: Skapa målgrupper för intern fildelning

Så fungerar det

När du skapat en målgrupp kan du lägga till medlemmar och tillämpa målgruppen på Google Drive för att göra den tillgänglig i användarnas delningsinställningar. Du kan till exempel göra så att en medarbetare kan se målgruppen All personal när hen delar Drive-filer.

Så här aktiverar du Drive-etiketter för skolan:

- Logga in på **administratörskonsolen** och öppna **Meny** > **Katalog** > **Målgrupper**
- Klicka på **Skapa målgrupp**
- Under **Namn** skriver du in ett namn på målgruppen
- Välj **Lägg till medlemmar** och lägg till de medlemmar som du vill ha med
- Klicka på **Klar**



Relevant dokumentation i hjälpcentret

- Om målgrupper
- Metodtips för att distribuera till en målgrupp
- Skapa en målgrupp

Hur förhindrar jag att gymnasieeleverna delar dokument med grundskoleeleverna?”

Begränsa fildelning

Förtroenderegler för Drive ger administratörer möjlighet att ange regler så att de kan styra vem som har åtkomst till filer på Google Drive. Det skyddar skolans data. Policyer kan gälla för enskilda användare, grupper, organisationsenheter och domäner.

- Skydda känsliga uppgifter och upprätthåll efterlevnad av branschstandarder och förordningar.
- Begränsa intern och/eller extern domändelning. Administratörer kan skapa en förtroenderegel som gör att elever endast kan dela Drive-filer inom organisationen.
- När Förtroenderegler är aktiverat visas det i stället för Delningsalternativ bland administratörsreglagen i Google Drive.

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Skapa och hantera förtroenderegler för Drive-delning

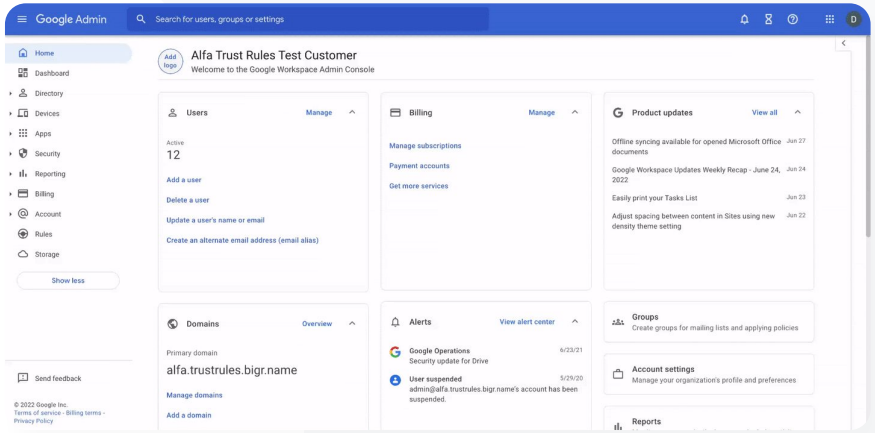
Så här gör du: Begränsa fildelning

Aktivera förtroenderegler för Drive:

- Logga in på **administratörskonsolen** och öppna **Meny** > **Regler**
- På kortet **Samarbeta säkert** högst upp på sidan klickar du på **Aktivera förtroenderegler**
- Din uppgiftslista öppnas automatiskt och visar förloppet för aktivering av förtroenderegler

Administratörer kan skapa en förtroenderegel, visa och ändra information om förtroenderegler, ta bort en förtroenderegel och visa logghändelser för förtroenderegler.

Titta i hjälpcentret för administratörer. Där finns stegvisa anvisningar om hur du hanterar förtroenderegler.



Relevant dokumentation i hjälpcentret

- Skapa och hantera förtroenderegler för Drive-delning

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

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Översikt över kontextkänslig åtkomst
- Tilldela kontextkänsliga åtkomstnivåer för appar

Begränsningar för Google Workspace-appen

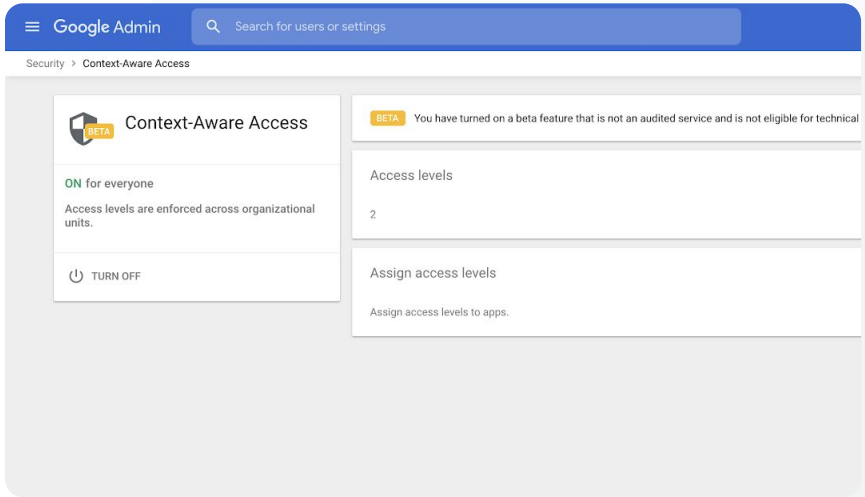
Med hjälp av **Kontextkänslig åtkomst** kan du skapa detaljerade policyer för åtkomstkontroll i **Google Workspace-appar och SAML-appar från tredje part** (Security Assertion Markup Language) baserat på attribut som användaridentitet, plats, enhetens säkerhetsstatus och IP-adress. Du kan till och med begränsa åtkomsten till appar utanför nätverket.

- Du kan tillämpa principer för kontextkänslig åtkomst till Google Workspace for Education-tjänsterna
- Begränsa åtkomst till Workspace-appar på skolägda enheter, ange att man bara kan öppna Drive om en enhet med användarutrymme är krypterad och annat

Så här gör du: Begränsa användningen av Google Workspace-appar

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 den app som 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

Hantera lagringen för domänen

Skolor med Google Workspace for Education har en baskvot på 100 TB gemensamt lagringsutrymme. Det är tillräckligt för ungefär 100 miljoner dokument, 8 miljoner presentationer eller 400 000 timmar med video. **Hantera det gemensamma Drive-lagringsutrymmet** så skolan säkert använder det på ett effektivt sätt.

Jag vill införa en ny lagringshanteringsplan för min domän.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Lagringsguide för administratörer
- Förstå tillgänglighet och användning av lagringsutrymme
- Frigöra eller skaffa mer lagringsutrymme
- Ange lagringsgränser

Använd administratörsverktyg, rapporter och loggar för att

- förstå hur mycket lagringsutrymme du använder
- ange lagringsgränser
- hitta de konton som använder en oproportionerligt stor mängd lagringsutrymme

I Teaching and Learning Upgrade och Education Plus finns möjligheten till större lagringsutrymme utöver baskvoten. Man kan:

- lägga till 100 GB i det delade utrymmet per licens med Teaching and Learning Upgrade
- lägga till 20 GB i det delade utrymmet per licens med Education Plus

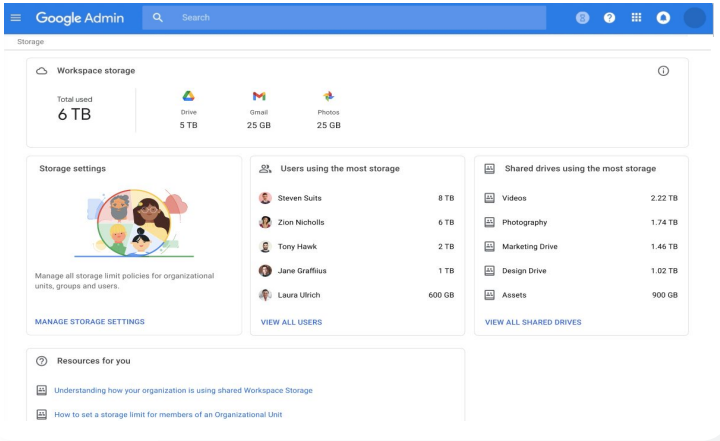
Så här gör du: Hantera lagringen för domänen

Ta reda på hur mycket utrymme respektive användare använder:

- Logga in på **administratörskonsolen** och öppna **Meny** > **Lagringsutrymme**
- Visa hur mycket lagringsutrymme organisationen och användarna använder

Ange lagringsgränser:

- Öppna **administratörskonsolen** > **Meny** > **Lagringsutrymme**
- I **Lagringsinställningar** klickar du på **Hantera**
- Klicka på **Lagringsgräns för användare** och välj den enhet som gränsen ska gälla för:
  - Organisationsenhet: Klicka på **organisationsenheten**
  - Grupp: Klicka på **Grupper**, klicka på **sökfältet** och ange **namnet på gruppen**. Klicka sedan på **gruppen**
- Välj **På** och **ange mängden lagringsutrymme**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Lagringsguide för administratörer
- Förstå tillgänglighet och användning av lagringsutrymme
- Frigöra eller skaffa mer lagringsutrymme
- Ange lagringsgränser

“Min elev-, lärar- och personaldata måste lagras i EU på grund av gällande datalagstiftning.”

Dataregleringar

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

- Education Plus- och Education Standard-användare kan välja en dataregion för några av användarna och andra dataregioner för särskilda avdelningar samt visa dataregioners flyttförlopp
- 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

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Välja en geografisk plats för din data

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

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 dataregionpolicy eftersom användarna utanför den region där deras data lagras i vissa fall kan uppleva latens

Stegvisa anvisningar

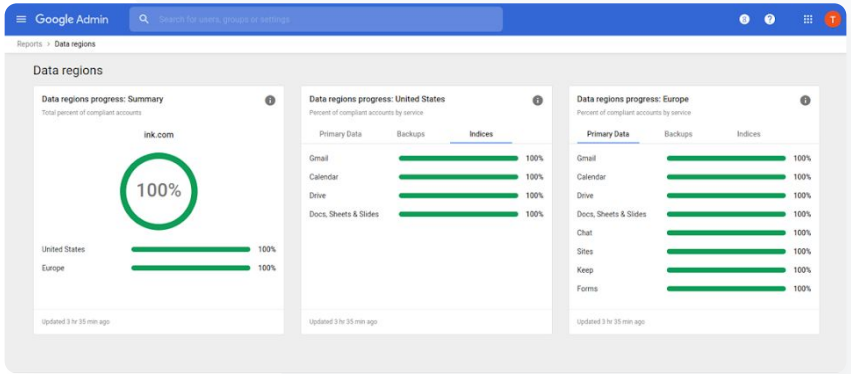
Relevant dokumentation i hjälpcentret

- Välja en geografisk plats för din data

Så här gör du: Dataregleringar

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**



Relevant dokumentation i hjälpcentret

- Välja en geografisk plats för din data

Hantera ändpunktsenheter

Med **hantering av Enterprise-ändpunkt** 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

> 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

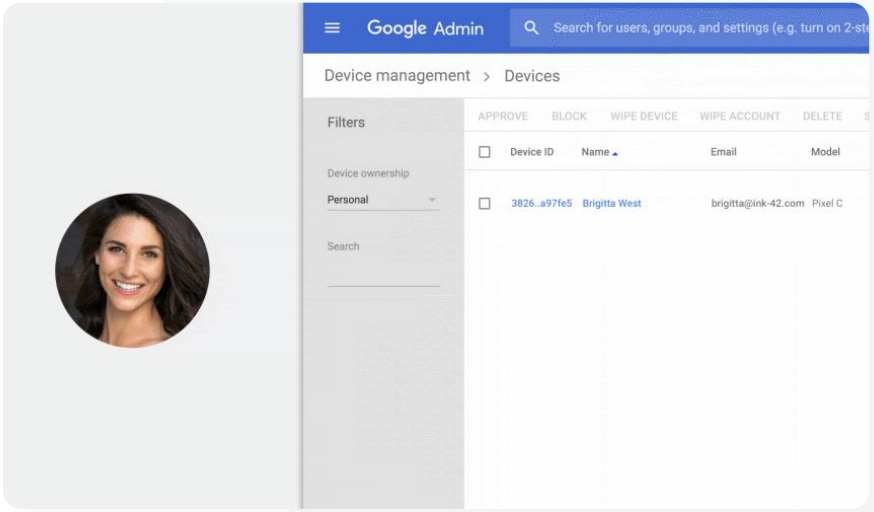
Relevant dokumentation i hjälpcentret

- Hantera enheter med Googles ändpunktshantering
- Konfigurera avancerad mobilhantering

Så här gör du: Hantera ändpunktsenheter

För avancerad mobilhantering:

- Logga in på **administratörskonsolen**
- Öppna **administratörskonsolen** > **Enheter**
- Klicka på **Inställningar** till vänster > **Universella inställningar**
- Klicka på **Allmänt** > **Mobilhantering**
- Vill du att inställningarna ska gälla alla väljer du organisationsenheten på den högsta nivån. Välj annars en underordnad organisationsenhet
- Välj **avancerat**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Hantera enheter med Googles ändpunktshantering
- Konfigurera avancerad mobilhantering

Hantera Microsoft Windows-enheter

Hantera och skydda skolans Windows 10-enheter i administratörskonsolen, precis på samma sätt som med Android-, iOS-, Chrome- och Jamboard-enheter.

- Aktivera enkel inloggning så att användare enklare kan komma åt Google Workspace på sina Windows 10-enheter
- Se till att de enheter som används för att komma åt Google Workspace är uppdaterade och skyddade, och upprätthåller efterlevnadsstandarder genom att hantera enheter i administratörskonsolen
- Rensa en enhet, distribuera uppdateringar av enhetskonfigurationer och annat till Windows 10-enheter från molnet

“Några av mina pedagoger använder Windows 10-enheter. Hur kan jag hantera alla skolans enheter på samma plats?”

Stegvisa anvisningar

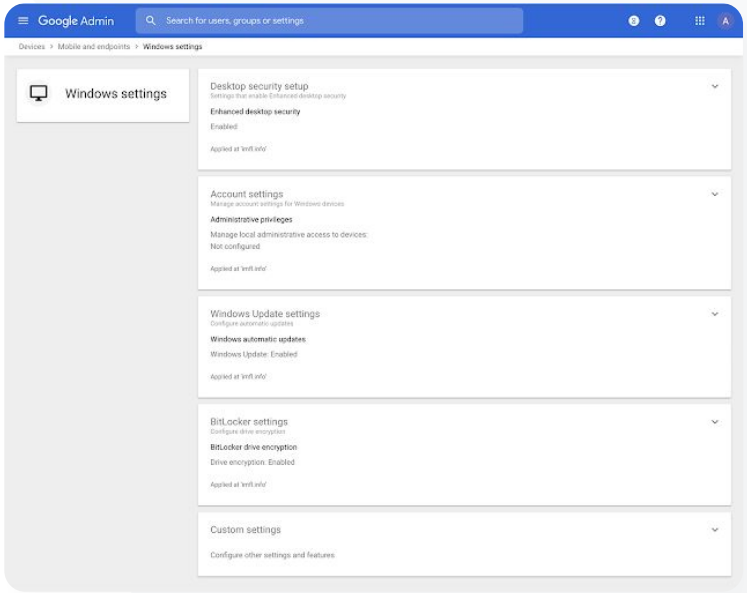
Relevant dokumentation i hjälpcentret

- Aktivera Windows-enhetshantering
- Registrera en enhet i Windows-enhetshantering

Så här gör du: Hantera Microsoft Windows-enheter

Aktivera Windows-enhetshantering:

- Öppna **administratörskonsolen** och navigera till **Meny** > **Enheter** > **Mobila och ändpunkter** > **Inställningar** > **Windows-inställningar**
- Välj **Konfigurering av Windows-hantering**
- Vill du att inställningen ska gälla alla väljer du organisationsenheten på den högsta nivån
- Välj **Aktiverad** bredvid **Windows-enhetshantering**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Aktivera Windows-enhetshantering
- Registrera en enhet i Windows-enhetshantering

Hur kan jag konfigurera wifi-profiler på mina Windows 10-enheter?”

Anpassade inställningar för Windows 10-enheter

Administratörer kan lägga till anpassade inställningar till sina enheter med hjälp av Googles hantering av Windows-enheter.

- Kontrollera anpassade enhetsinställningar via administratörskonsolen
- Tillämpa inställningar för:
  - Enhetshantering
  - Säkerhet
  - Maskinvara och nätverk
  - Programvara
  - Integritet

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

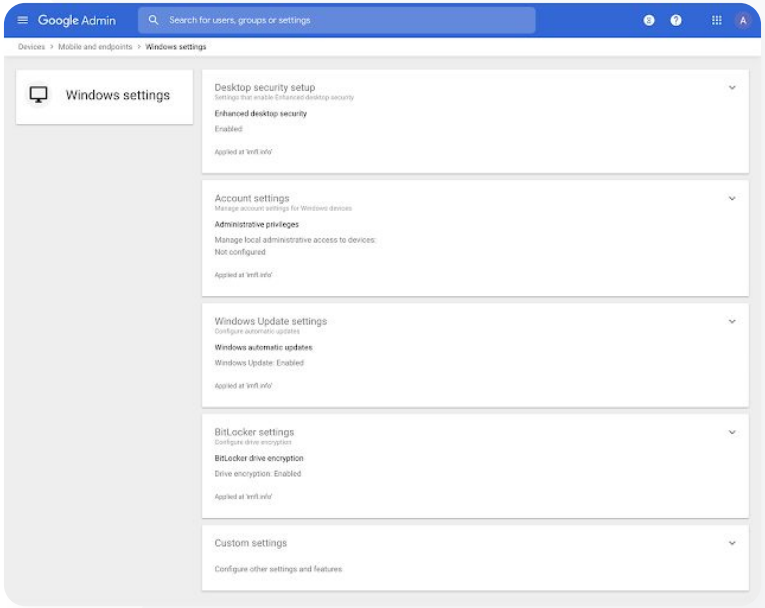
- Vanliga anpassade inställningar
- Lägg till anpassade inställningar

Så här gör du: Anpassade inställningar för Windows 10-enheter

Lägg till en ny anpassad inställning:

- Öppna **administratörskonsolen** och navigera till **Meny** > **Enheter** > **Mobila och ändpunkter** > **Inställningar** > **Windows-inställningar**
- Välj **Anpassade inställningar**
- Klicka på **Lägg till en anpassad inställningar** och fyll i de fält som krävs
- Klicka på **Nästa**
- Välj en **organisationsenhet** som inställningen ska gälla för
- Klicka på **Använd**

Observera att Google inte tillhandahåller teknisk support eller ansvarar för produkter och inställningar från tredje part.



Relevant dokumentation i hjälpcentret

- Vanliga anpassade inställningar
- Lägg till anpassade inställningar

“

Jag vill se till att våra Windows 10-enheter får de senaste uppdateringarna.”

Automatisera uppdateringar för Windows 10-enheter

Ange hur och när skolans Windows 10-enheter får säkerhetsuppdateringar och andra viktiga nedladdningar via Windows automatiska uppdateringstjänst.

- Ställ in aviseringar om att ladda ned uppdateringar från kontrollpanelen för Windows Update, ange timmar då omstarter efter uppdateringar inte ska schemaläggas och annat
- Tillämpa inställningar för hela skolan eller specifika organisationsenheter
- Det kan ta upp till 24 timmar att införa ändringar, men det går oftast snabbare

Stegvisa anvisningar

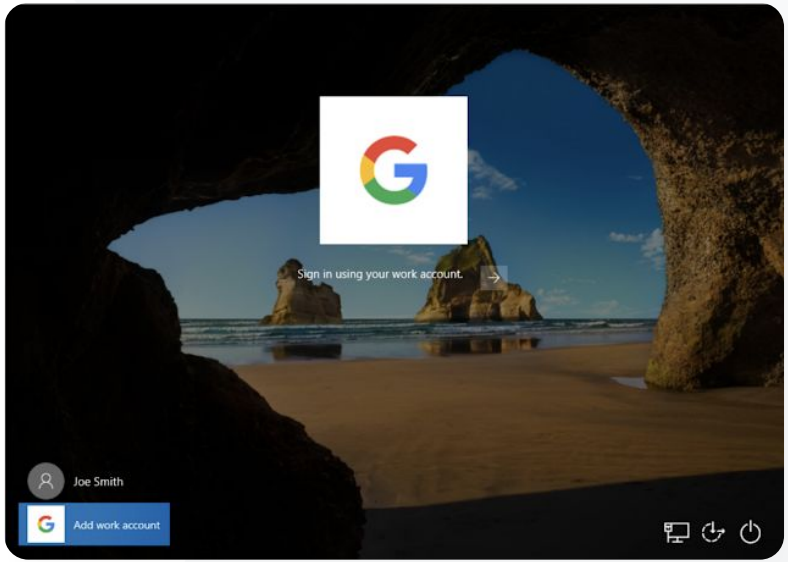
Relevant dokumentation i hjälpcentret

- Hantera automatiska uppdateringar

Så här gör du: Automatisera uppdateringar för Windows 10-enheter

Konfigurera uppdateringar:

- Öppna **administratörskonsolen** och navigera till **Meny** > **Enheter** > **Mobila och ändpunkter** > **Inställningar** > **Windows-inställningar**
- Välj **Inställningar för Windows Update** > **Aktiverad**
- Välj **Aktiverad** bredvid **Windows-enhetshantering**
- Ställ in alternativen nedan och andra:
  - Godkänn uppdateringar för Microsoft-appar
  - Beteende vid automatisk uppdatering
  - Automatisera uppdateringsfrekvens
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Hantera automatiska uppdateringar

“Jag vet att Google har de högsta standarderna när det gäller datakryptering, men jag vill kunna kontrollera krypteringsnycklarna för vårt universitets immateriella egendom och forskning.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Om kryptering på klientsidan

Dra nytta av kryptering på klientsidan

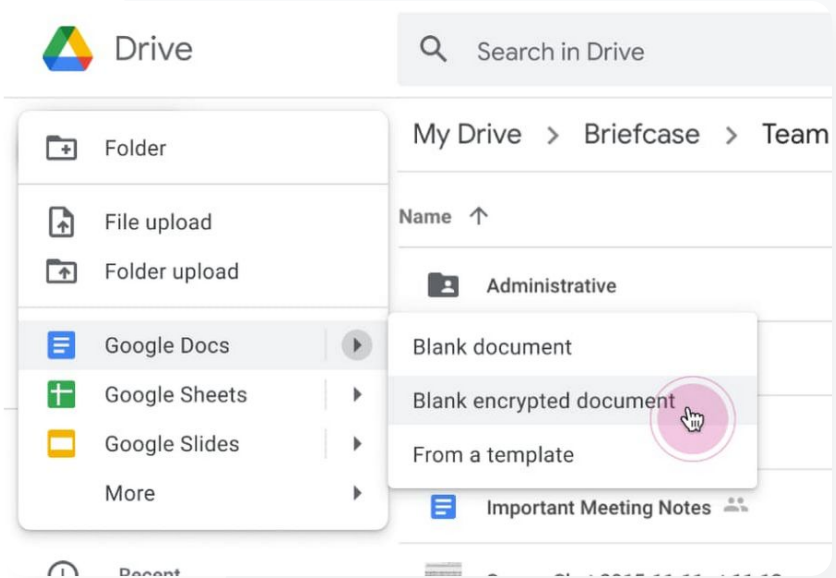
Google Workspace använder redan de senaste kryptografiska standarderna för att kryptera all data i vila och under överföring mellan sina anläggningar. Med **kryptering på klientsidan** har administratörer direkt kontroll över krypteringsnycklar och den identitetsleverantör som används för att komma åt de nycklarna.

- Använd dina egna krypteringsnycklar till att kryptera känslig data, som skolans immateriella egendom
- Innehållskryptering hanteras i webbläsaren innan data skickas eller lagras i Googles molnbaserade lagringsutrymme
- Välj vilka användare som kan skapa krypterat innehåll på klientsidan och dela det internt eller externt

Så här gör du: Dra nytta av kryptering på klientsidan

Konfigurera kryptering på klientsidan (CSE):

- Konfigurera en krypteringsnyckeltjänst
  - Skydda din data med nyckelhanterings- och kontrollfunktioner genom att skapa en nyckeltjänst
- Anslut Google Workspace till den externa nyckeltjänsten
  - Lägg till och hantera nyckeltjänster för kryptering på klientsidan genom att lägga in webbadressen för nyckeltjänsten i administratörskonsolen
- Tilldela organisationsenheter eller grupper nyckeltjänsten
  - Tilldela en nyckeltjänst som standard för hela organisationen
- Anslut Google Workspace till din identitetsleverantör
  - Anslut till identitetsleverantören (IdP) för kryptering på klientsidan så kan du verifiera användares idententiteter innan du låter dem kryptera innehåll eller komma åt krypterat innehåll
- Aktivera kryptering på klientsidan för användare
  - Aktivera kryptering på klientsidan så att organisationsenheter eller grupper med användare som behöver skapa krypterat innehåll på klientsidan kan göra det

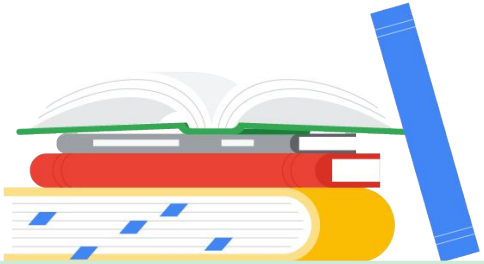


Relevant dokumentation i hjälpcentret

- Om kryptering på klientsidan

Undervisnings- och inlärningsfunktioner

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

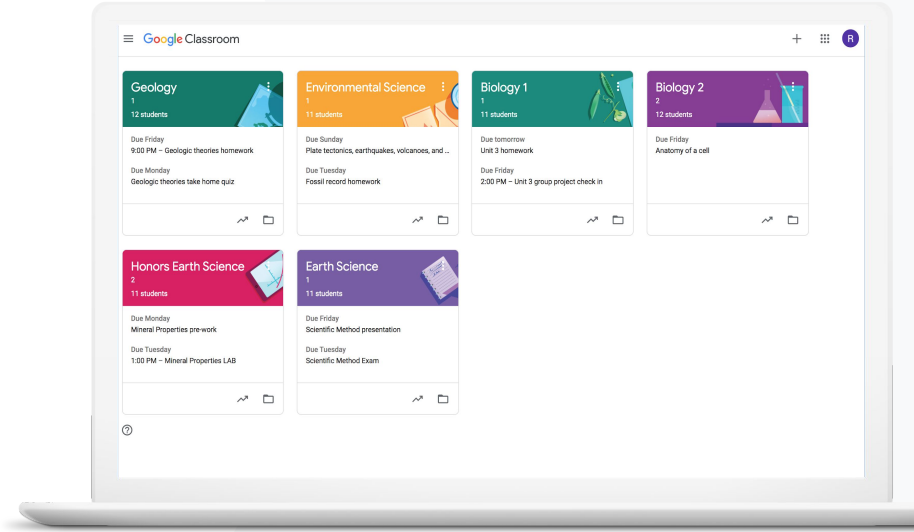


- Google Classroom
- Plagiatrapporter
- Dokument, Kalkylark och Presentationer
- Google Meet

Google Classroom

Vad är detta?

Google Classroom är den centrala platsen för undervisning och inlärning. Med betalfunktionerna i Classroom får man alla klassverktyg samlade på en och samma plats. Pedagoger kan komma åt sina favoritverktyg direkt i Classroom och hålla klasslistor synkroniserade med externa system.



Användningsområden

Hantera åtkomst till Classroom-tillägg	Stegvisa anvisningar
Integrera engagerande innehåll i Classroom	Stegvisa anvisningar
Skapa klasser i stor skala	Stegvisa anvisningar

“

Jag önskar att jag på något sätt kunde ge pedagogerna åtkomst till sina favoritverktyg för utbildningsteknik med enkel inloggning.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Hantera Google Workspace Marketplace-appar
- Använda tillägg i Classroom
- Hantera Marketplace-appar på godkännandelistan
- Distribuera en Marketplace-app till användare
- Classroom-tillägg [guiden Komma igång för administratörer (på engelska)]

Hantera åtkomst till Classroom-tillägg

Bestäm vilka utbildningsappar från tredje part som skolan kan öppna med en **godkännandelista för domänen**. Gör så att pedagoger enkelt kan installera tillägg och använda dem till elevernas hemuppgifter med bara några klick.

- Skapa en godkännandelista för domänen så att det är bestämt vilka tredjepartsappar pedagoger kan installera från Google Workspace Marketplace
- Förbättra inlärningen med fler utbildningsappar. Pedagoger kan tilldela, granska och betygsätta direkt i Google Classroom
- Google Workspace Marketplace innehåller Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Arts & Culture, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora, Wordwall med flera

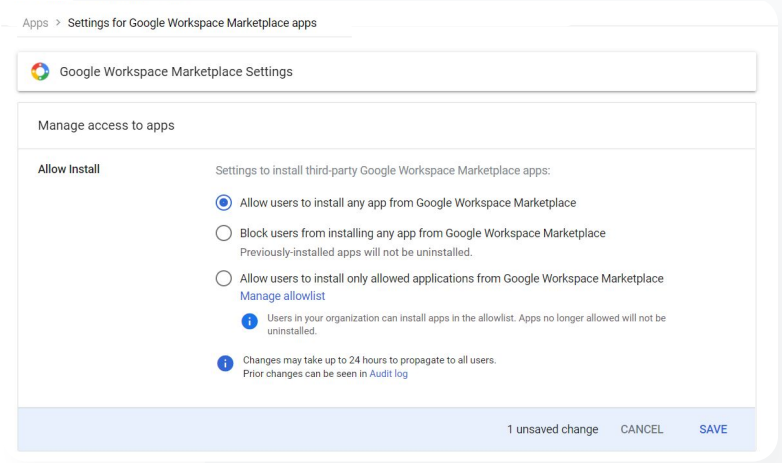
Så här gör du: Hantera åtkomst till Classroom-tillägg

Hantera åtkomst till tillägg med en godkännandelista för domänen:

- I administratörskonsolen väljer du **Meny** > **Google Workspace Marketplace-appar** > **Applista**
- Välj **Godkännandelista**
- Ange namnet på det tillägg du vill ha eller sök efter det
- Klicka på **Välj** och se till att **Tillåt användarna att installera den här appen** är markerat
- Klicka på **Fortsätt** och **Slutför**

Ge tillägg åtkomst till din godkännandelista:

- I administratörskonsolen väljer du **Meny** > **Google Workspace Marketplace-appar** > **Applista**
- Markera det tillägg som du vill distribuera
- Under **Användaråtkomst** klickar du på **Visa organisationsenheter och grupper**
- Välj mellan att göra det **tillgängligt för alla** eller begränsa åtkomsten till **vissa grupper** eller **organisationsenheter**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Hantera Google Workspace Marketplace-appar
- Använda tillägg i Classroom
- Hantera Marketplace-appar på godkännandelistan
- Distribuera en Marketplace-app till användare
- Classroom-tillägg [guiden Komma igång för administratörer (på engelska)]

> Jag vill tilldela mina elever ett Kahoot!-inlärningsspel och även betygsätta det utan att stänga Google Classroom.”

Integrera engagerande innehåll i Classroom

Med **tillägg för Classroom** kan pedagoger dela engagerande aktiviteter och innehåll med klassen genom att lägga till tillägg i uppgifter, frågor, material eller meddelanden i Classroom.

- Ge pedagogerna och eleverna åtkomst till sina favoritverktyg, t.ex. Kahoot!, Nearpod och Pear Deck, utan att stänga Classroom
- Med tillägg behöver inte eleverna hantera flera olika lösenord eller navigera till externa webbplatser
- Betygsätt och granska elevernas arbeten via tillägg, direkt i Classroom

Stegvisa anvisningar

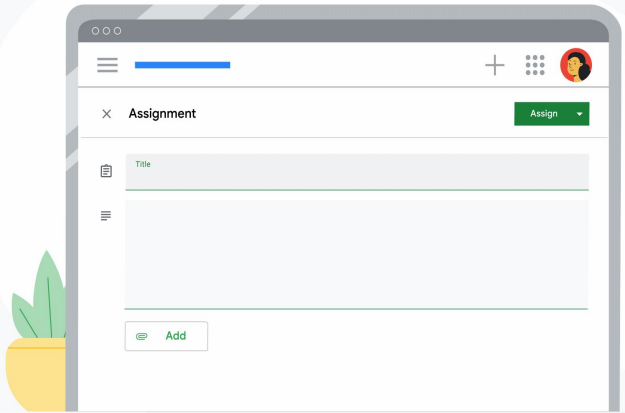
Relevant dokumentation i hjälpcentret

- Använda tillägg i Classroom
- Classroom-tillägg [guiden Komma igång för lärare (på engelska)]

Så här gör du: Integrera engagerande innehåll i Classroom

Så här lägger du till tillägg i uppgifter, quiz och frågor:

- Logga in på Classroom-kontot på **classroom.google.com**
- Välj den aktuella klassen i listan och välj **Klassuppgifter**
- Välj **Skapa** och välj vad du vill skapa
- Ange titel och anvisningar
- Under **Tillägg** väljer du det tillägg du vill använda
- Välj **Tilldela**



Så här lägger du till tillägg i ett meddelande:

- På sidan **Flöde** för klassen väljer du **Berätta något för klassen**
- Skriv in ditt meddelande
- Under **Tillägg** väljer du det tillägg du vill använda
- Välj **Lägg upp**

Relevant dokumentation i hjälpcentret

- Använda tillägg i Classroom
- Classroom-tillägg [guiden Komma igång för lärare (på engelska)]

“Jag behöver kunna skapa klasser automatiskt och hantera klasslistor i Google Classroom.”

Skapa klasser i stor skala

Import av SIS-klasslistor och Clever gör det möjligt att skapa klasser automatiskt och hålla klasslistor synkroniserade med skolans system för elevinformation.

- Det är tillgängligt för K-12-distrikt i USA och Kanada där man använder Education Plus
- Administratörer kan importera klasslistor till Google Classroom från systemet med elevinformation och sedan automatiskt skapa klasser
- Automatisera och hantera smidigt klasslistor i Google Classroom

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Komma igång med import av klasslistor från SIS
- Konfigurera import av SIS-klasslistor via Clever

Så här gör du: Skapa klasser i stor skala

Så här konfigurerar du import av klasslistor från SIS:

- Konfigurera synkronisering av klasslistor i Google Classroom inom Clever
- Distriktadministratören i Clever och den avancerade administratören i Google Workspace kan följa de stegvisa anvisningarna i Clever

Om distriktet inte har ett Clever-konto:

- Skapa ett Clever-konto

Om distriktet har ett Clever-konto:

- Begär import av klasslistor på Clever-översikten

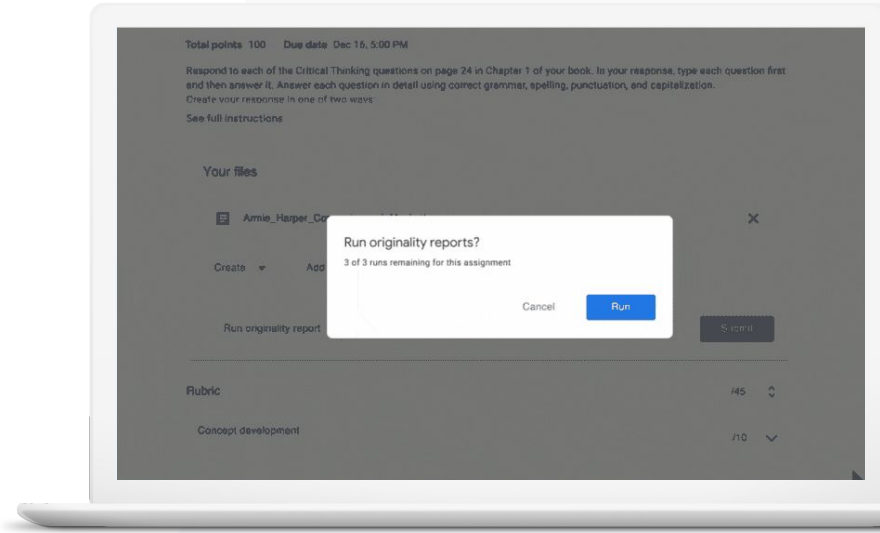
Relevant dokumentation i hjälpcentret

- Konfigurera import av SIS-klasslistor via Clever

Plagiatrapporter

Vad är detta?

Med plagiatrapporter kan pedagoger och elever kontrollera att arbeten inte innehåller plagiat. Med hjälp av Google Sök kan man jämföra elevers arbeten mot miljardtals webbsidor och fler än 40 miljoner böcker. Betalfunktionerna för plagiatrapporter ger obegränsad åtkomst så att pedagoger kan genomsöka elevers inlämningar och jämföra dem med gamla inlämningar på en skolägd lagringsplats.



Användningsområden

Söka efter plagiat	Stegvisa anvisningar
Utför plagiatkontroll genom att jämföra med tidigare elevinlämningar	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.”

Söka efter plagiat

Lärare kan kontrollera om elevernas arbeten innehåller plagiat med hjälp av **plagiatrapporter**. Rapporten länkar till källor som identifieras och flaggar text som inte citerats.

- Kör plagiatrapporter i Dokument, Presentationer och Microsoft Word-dokument.
- Pedagoger som använder Teaching and Learning Upgrade eller Education Plus har
  - obegränsad åtkomst till plagiatrapporter
  - möjlighet att jämföra elevers arbeten med tidigare inlämningar på en skolägd lagringsplats

Du äger alltid din data. Det är vårt ansvar att se till att den hålls privat och skyddas.

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Aktivera plagiatrapporter
- Plagiatrapporter och integritet

Så här gör du: Söka efter plagiat

Aktivera plagiatrapporter för en uppgift i Classroom:

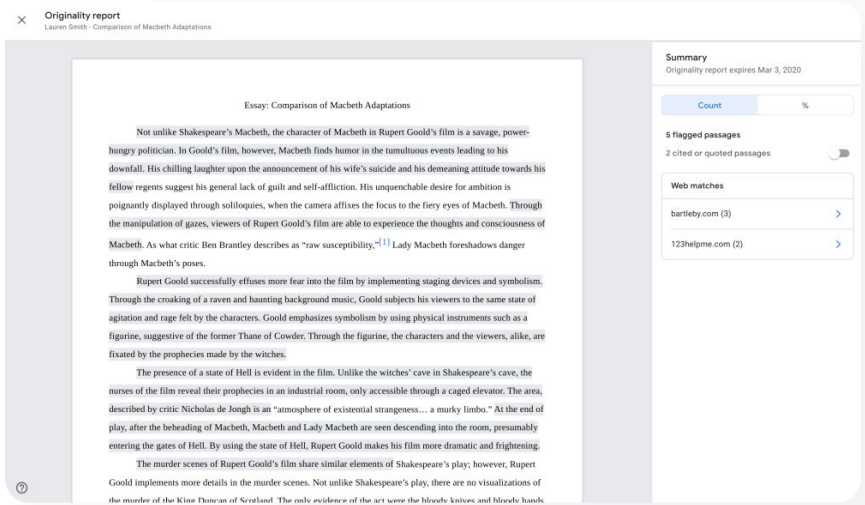
- Logga in på Classroom-kontot på **classroom.google.com**
- Välj den aktuella klassen i listan och välj **Klassuppgifter**
- Välj **Skapa** > **Hemuppgift**
- Markera kryssrutan bredvid **Plagiatrapporter** för att aktivera funktionen

Köra en plagiatrapport på en elevuppgift:

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

Aktivera plagiatrapporter för en uppgift i lärplattformen:

- Logga in på din **lärplattform**
- Välj den relevanta **kursen**
- Skapa en uppgift och välj **Google Uppgifter**
- Markera kryssrutan **Aktivera plagiatrapporter**



Relevant dokumentation i hjälpcentret

- Classroom: Aktivera plagiatrapporter
- Google Uppgifter: Aktivera plagiatrapporter

“Hur kan jag göra det möjligt för lärare att kontrollera om elevers arbeten innehåller plagiat genom att jämföra dem mot gamla elevarbeten?”

Utför plagiatkontroll genom att jämföra med tidigare elevinlämningar

Skolmatchningar i plagiatrapporter ger pedagoger möjlighet att jämföra elevarbeten med gamla inlämningar. Inlämningarna genomsöks och jämförs med elevarbeten på skolans privata lagringsplats.

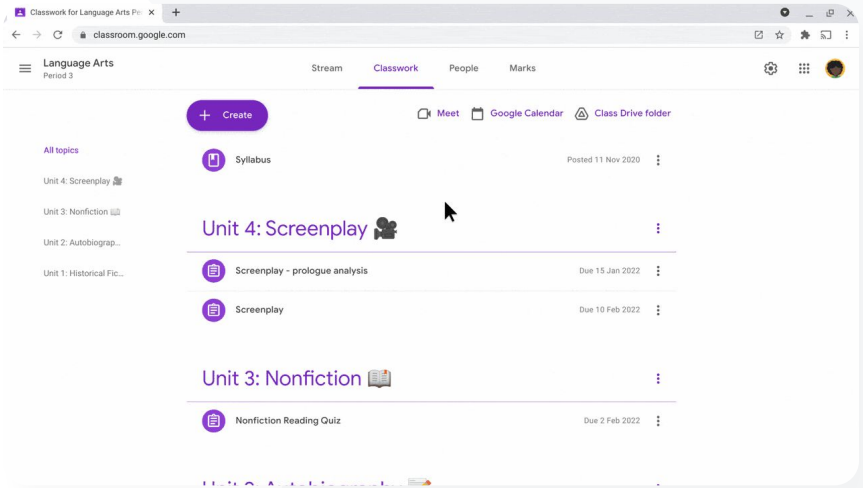
- Jämför matchningar med aktuella och gamla elevarbeten så att du kan upptäcka plagiat med Teaching and Learning Upgrade eller Education Plus
- Elevarbeten kan tryggt lagras och läggas in på den privata, skolägda lagringsplatsen som är tillgänglig för hela domänen

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Aktivera plagiatrapporter
- Aktivera skolmatchningar för plagiatrapporter i Classroom

Så här gör du: Utför plagiatkontroll genom att jämföra med tidigare elevinlämningar



Så här aktiverar du skolmatchningar för plagiatrapporter:

- I administratörskonsolen väljer du **Meny** > **Appar** > **Tilläggstjänster från Google** > **Classroom**
- Välj **lärarens organisationsenhet**
- Klicka på **Plagiatrapporter** och markera kryssrutan **Aktivera skolmatchning i plagiatrapporter**
- Klicka på **Spara**

Relevant dokumentation i hjälpcentret

- Aktivera skolmatchningar för plagiatrapporter i Classroom

“Jag vill lära mina elever hur man citerar källor på rätt sätt.”

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 plagiatrapporter jämförs elevernas arbeten 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 använda 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.

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

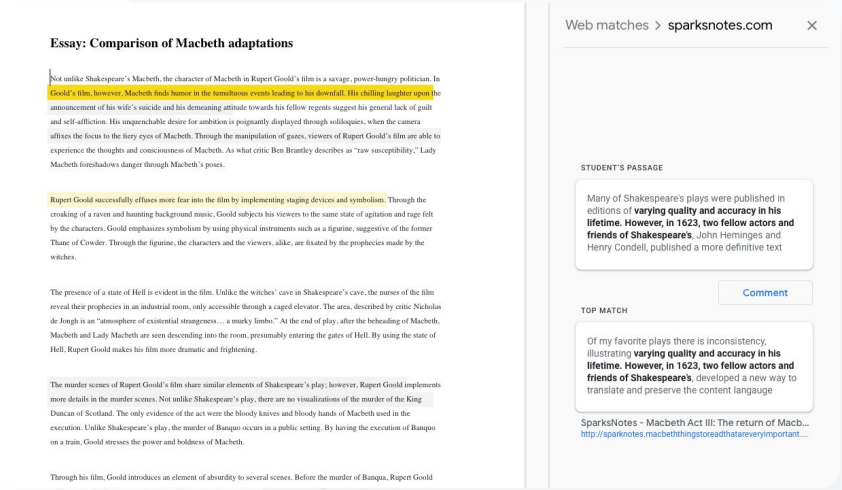
- Köra en plagiatrapport på en uppgift

Så här gör du: Ge eleverna möjlighet att lära sig av plagiat

Så här kan elever köra plagiatrapporter i Classroom:

- 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

Elever kan köra plagiatrapporter på lärplattformen med hjälp av Google Uppgifter



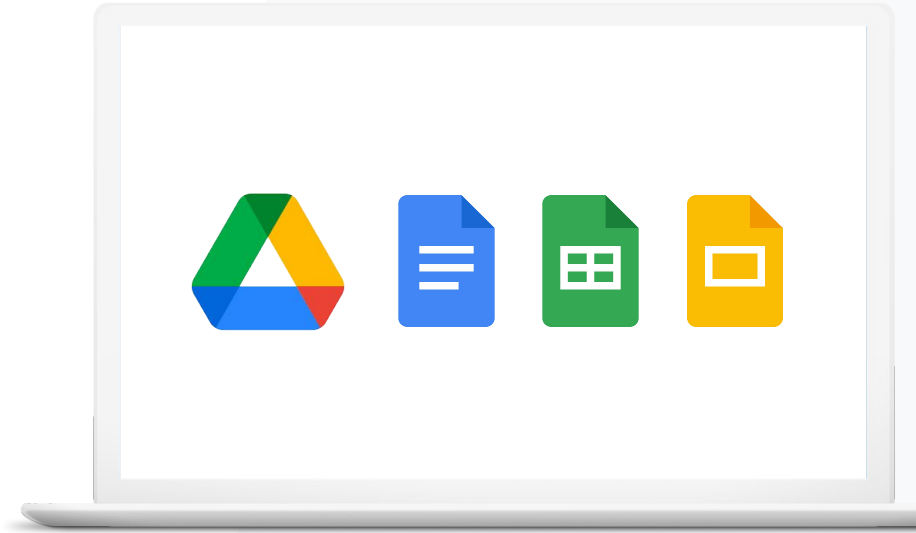
Relevant dokumentation i hjälpcentret

- Köra en plagiatrapport i Classroom
- Köra en plagiatrapport på lärplattformen

Dokument, Kalkylark och Presentationer

Vad är detta?

Med Dokument, Kalkylark och Presentationer kan alla på skolan samarbeta, skapa tillsammans, granska och redigera samtidigt och i realtid. Med betalfunktionerna i Education Plus kan pedagoger och administratörer sätta upp en godkännandeprocess för interna dokument på skolan.



Användningsområden

Godkänna interna dokument — Stegvisa anvisningar

Institutionen för naturkunskap håller på att ta fram en ny läroplan.

Hur kan de se till att förslaget på den nya läroplanen godkänns av alla ledare?”

Godkänna interna dokument

Med **Godkännanden** kan de olika skolgrupperna skicka dokument i Google Drive via en formell godkännandeprocess.

- Granskare kan godkänna, avvisa eller ge feedback på dokument direkt i Drive, Dokument och andra appar i Google Workspace
- Godkännare följer en länk till dokumentet där de kan granska, lämna kommentarer och avvisa eller godkänna det
- Hantera godkännanden för avtal eller nyanställda, godkänna ändringar för dokument innan de publiceras och annat

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Hantera godkännanden

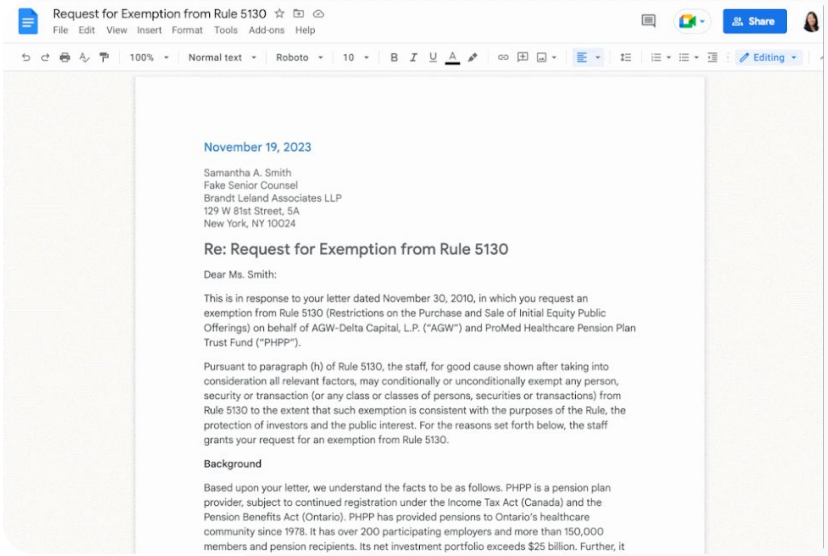
Så här gör du: Godkänna interna dokument

Så fungerar det

Administratörer kan styra hur användare och filer deltar i godkännandeprocessen.

Så här hanterar du godkännanden:

- Logga in på **administratörskonsolen** och öppna **Meny** > **Appar** > **Google Workspace** > **Drive och Dokument**
- Klicka på **Godkännanden**
- Vill du att inställningen ska gälla för alla väljer du ett barns **organisationsenhet** eller en **konfigurationsgrupp**
- Klicka på **Spara**



Relevant dokumentation i hjälpcentret

- Hantera godkännanden

Google Meet

Vad är detta?

De avancerade funktionerna i Google Meet är bland annat livestreaming, smågrupper, större möten, mötesinspelningar, liveöversatt textning och annat.

Användningsområden

Spela in möten	Stegvisa anvisningar	Ställa frågor	Stegvisa anvisningar
Hänvisa till det som har tagits upp under lektioner	Stegvisa anvisningar	Samla in åsikter	Stegvisa anvisningar
Undanröja språkbarriärer	Stegvisa anvisningar	Små elevgrupper	Stegvisa anvisningar
Sända samlingar och skolevenemang	Stegvisa anvisningar	Kontrollera närvaron	Stegvisa anvisningar

“

Vår skola har stora fortbildningsklasser med undervisning online. Vi behöver spela in lektionerna åt pedagoger som inte kan vara med.”

Spela in möten

Med Teaching and Learning Upgrade och Education Plus kan pedagoger spela in lektioner, lärarmöten, fortbildningstillfällen och annat. Möten sparas automatiskt på Drive.

- Inspelningar sparas på mötesarrangörens Drive. Se efter att det finns tillräckligt med utrymme på din Drive innan du spelar in
- Vi rekommenderar att IT-administratören aktiverar inspelning för enbart fakultet och personal

Stegvisa anvisningar

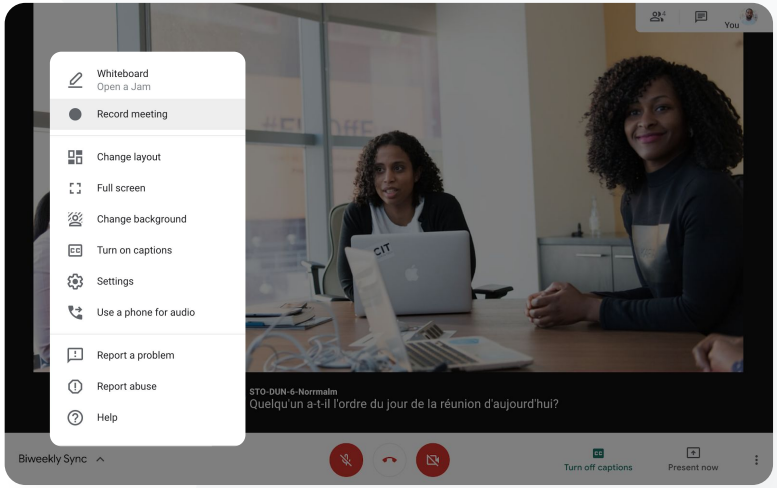
Relevant dokumentation i hjälpcentret

- Spela in ett videomöte

Så här gör du: Spela in möten

Så här startar du en inspelning:

- Starta eller gå med i ett möte i **Google Meet**
- Klicka på **Aktiviteter** > **Inspelning**
- Välj **Starta inspelning**
- I fönstret som öppnas klickar du på **Starta**
- En röd prick visas nere till höger på skärmen. Det betyder att ett möte spelas in
- En videofil med mötet sparas automatiskt i Drive



Relevant dokumentation i hjälpcentret

- Spela in ett videomöte

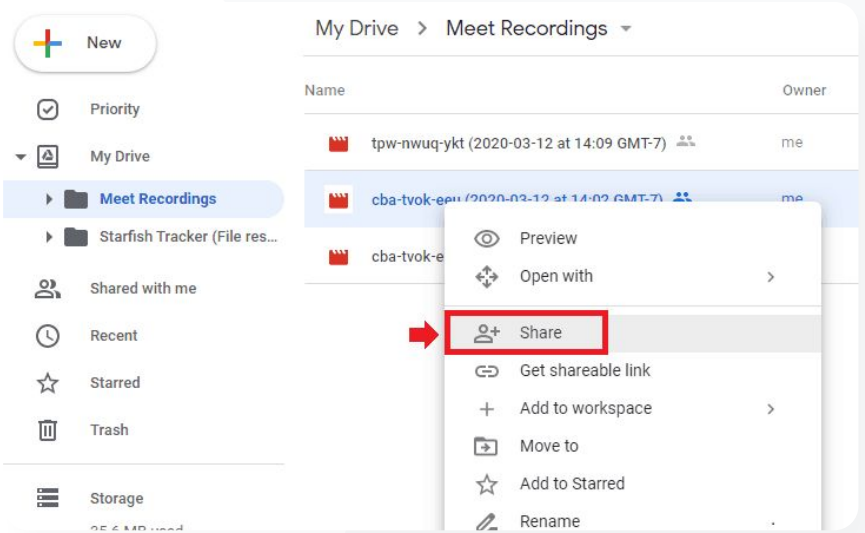
Så här gör du: Visa och dela inspelningar

Så här startar du en inspelning:

- Välj filen
- Klicka på ikonen för **Dela**
- **Lägg till** godkända tittare

ELLER

- 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
- Vill du 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

“Hur kan jag transkribera en virtuell klass så elever kan gå igenom begrepp senare?”

Hänvisa till det som har tagits upp under lektioner

Med transkribering av möten kan pedagoger automatiskt transkribera lektioner och diskussioner så elever enklare kan gå igenom olika begrepp igen. Transkriptioner registrerar närvaro och det står vem som sagt vad under ett möte.

- Det är tillgängligt på engelska för Google Meet-användare som använder en dator
- Administratörer kan aktivera transkribering för skolgrupperna
- Transkriptioner sparas automatiskt på mötesvärdens Drive
- När mötestranskriptioner är aktiverade visas en symbol för transkriptioner högst upp till vänster för alla som deltar i mötet
- Transkriptioner innehåller de ord som sagts under ett möte. Vill du ha en transkription av chattmeddelanden får du i stället spela in mötet

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Använda transkribering i Google Meet
- Aktivera eller inaktivera transkribering

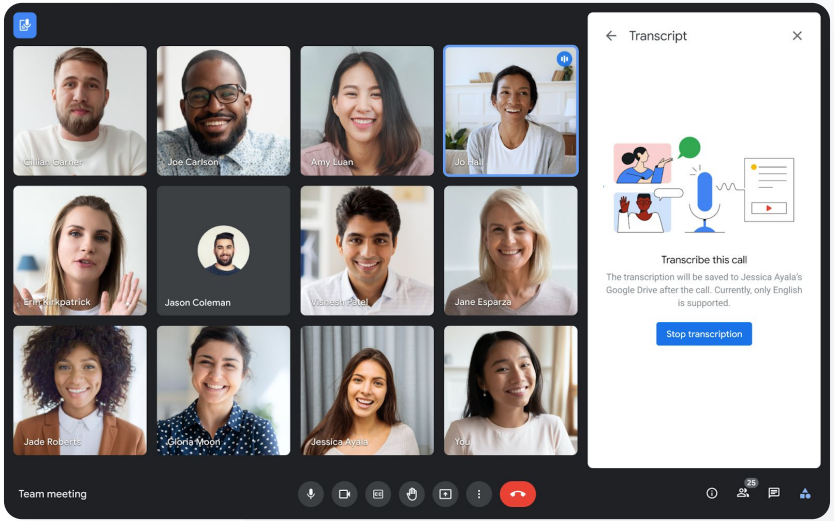
Så här gör du: Hänvisa till det som har tagits upp under lektioner

Så här aktiverar du transkriptioner i Google Meet:

- Välj ikonen för **Aktiviteter** nere till höger när du är i ett möte
- Klicka på **Transkriptioner** > **Starta transkription** > **Starta**

Så här stoppar du transkriptioner i Google Meet:

- Välj symbolen **Aktiviteter** > **Transkriptioner** > **Stoppa transkription** > **Stoppa**



Relevant dokumentation i hjälpcentret

- Använda transkribering i Google Meet
- Aktivera eller inaktivera transkribering

Vi håller virtuella föräldramöten, och ibland är föräldrar som talar ett annat språk med.

Hur kan jag göra möten inkluderande och se till att alla förstår?”

Undanröja språkbarriärer

Översatt textning gör möten mer inkluderande eftersom språkbarriärer tas bort. När mötesdeltagare får information på sina föredragna språk får alla samma chans att förstå, lära och samarbeta.

- Pedagoger kan interagera med elever, föräldrar och intressenter i samhället som talar andra språk
- Använd översatt textning när du ska översätta till eller från engelska, franska, tyska, portugisiska eller spanska
- Det är också möjligt att översätta från engelska till japanska, mandarin eller svenska

Stegvisa anvisningar

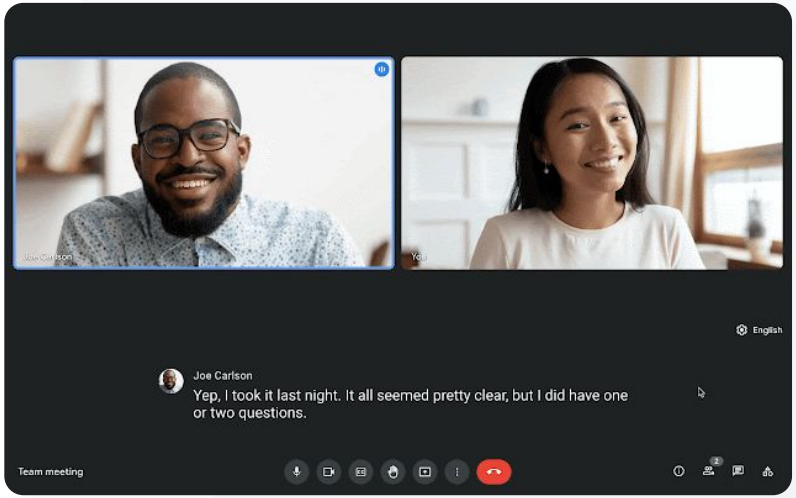
Relevant dokumentation i hjälpcentret

- Använda översatt textning i Google Meet

Så här gör du: Undanröja språkbarriärer

Så här aktiverar du översatt textning:

- När du har ett möte igång visas **Fler alternativ** längst ned på skärmen. Klicka där och sedan på **Inställningar** > **Textning**
- Aktivera **Textning**
- Välj **språk för mötet**
- Aktivera **Översatt textning**
- Välj **språk att översätta till**



Relevant dokumentation i hjälpcentret

- Använda översatt textning i Google Meet

Sända samlingar, skolhändelser och möten

Livestreama till upp till 10 000 tittare med Teaching and Learning Upgrade och upp till 100 000 tittare 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.

- Bestäm hur många du vill livestreama för. Välj om streamen ska
  - visas endast för användare i organisationen (i domänen)
  - delas med andra betrodda Google Workspace-domäner
  - kunna ses på YouTube
- Vi rekommenderar att IT-administratören aktiverar livestreaming för enbart fakultet och personal
- Om en användare inte kan delta i livestreamen kan hen titta på den när mötet är avslutat
- Lägg till textning, omröstningar och frågestunder i en livestream för att göra den mer inkluderande och engagerande

> “Vi behöver kunna livestreama våra personal- och fakultetsmöten till en stor grupp berörda parter och föräldrar.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Aktivera eller inaktivera livestreaming för Meet
- Livestreama ett videomöte

Så här gör du: Sända samlingar, skolhändelser och möten

Så här skapar du en livestreamhändelse:

- Öppna **Google Kalender**
- Välj **+ Skapa** > **Fler alternativ**
- Lägg till händelseinformation såsom datum, tid och beskrivning
- Lägg till deltagare som kan delta i videomötet fullt ut, vilket innebär att andra kan se och höra dem och att de kan presentera
- 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 som tillåts enligt betallicensen genom att klicka på **Kopiera** och sedan dela webbadressen till livestreamen
- Välj **Spara**
- Streamingen startar inte automatiskt. Under mötet ska du välja **Mer** > **Starta streaming**

Relevant dokumentation i hjälpcentret

- Aktivera eller inaktivera livestreaming för Meet
- Livestreama ett videomöte

“

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

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 moderatorn en frågerapport automatiskt till sin e-postadress

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Ställa frågor till deltagarna i Google Meet

Så här gör du: Ställa frågor

Ställ 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 moderatorerna **en rapport via e-post**
- Öppna e-postmeddelandet och 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.”

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

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Genomföra omröstningar i Google Meet

Så här gör du: Samla in åsikter

Skapa en omröstning:

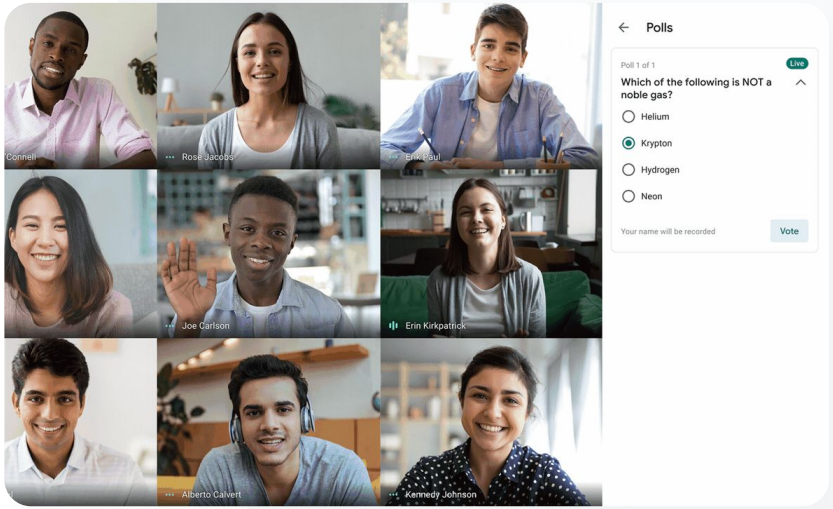
- Välj **ikonen för Aktiviteter** uppe till höger i ett möte > **Omröstning**
- Välj **Starta en omröstning**
- Skriv en fråga
- Välj **Starta** eller **Spara**

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 moderatorerna **en rapport via e-post**
- Öppna e-postmeddelandet > välj **den bifogade rapporten**



Relevant dokumentation i hjälpcentret

- Genomföra omröstningar i Google Meet

“

Ibland har vi elever som studerar hemifrån. När vi jobbar i små grupper behöver jag enkelt kunna skapa smågrupper utifrån redan bestämda grupper.”

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Använda smågrupper i Google Meet

Små elevgrupper

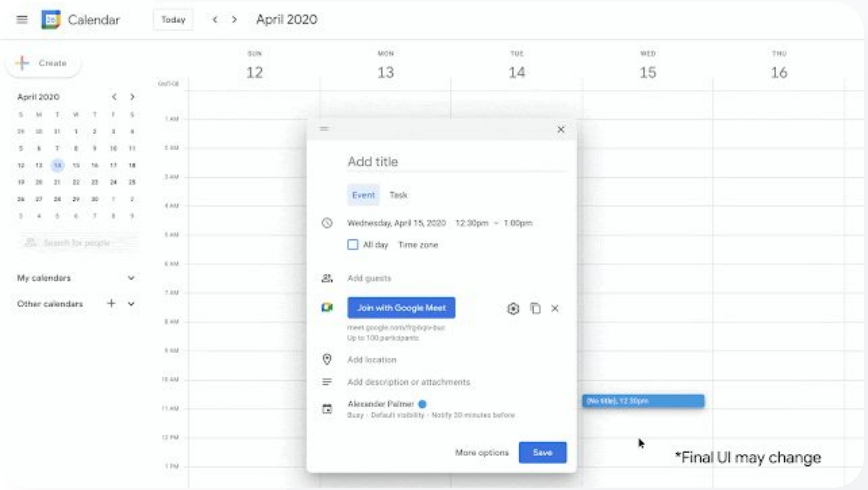
Med funktionen för smågrupper kan pedagoger dela in eleverna i mindre grupper under **virtuell undervisning, hybridundervisning eller undervisning på plats.** Smågrupper måste startas av moderatorer under ett videosamtal på en dator.

- Det går att skapa smågrupper i förväg när man skapar en händelse. Man kan också göra det medan mötet pågår
- 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

Så här gör du: Skapa små elevgrupper

Skapa smågrupper före mötet:

- Skapa en ny händelse i Google Kalender
- Klicka på **Lägg till videokonferenser i Google Meet**
- Lägg till deltagare. Välj sedan **Ändra konferensinställningar**
- Klicka på **Smågrupper**
- Välj antal smågrupper. Gör sedan något av följande:
  - Dra deltagarna till olika rum
  - Skriv namnen direkt i ett rum
  - Klicka på **Blanda** för att blanda grupperna
- Klicka på **Spara**



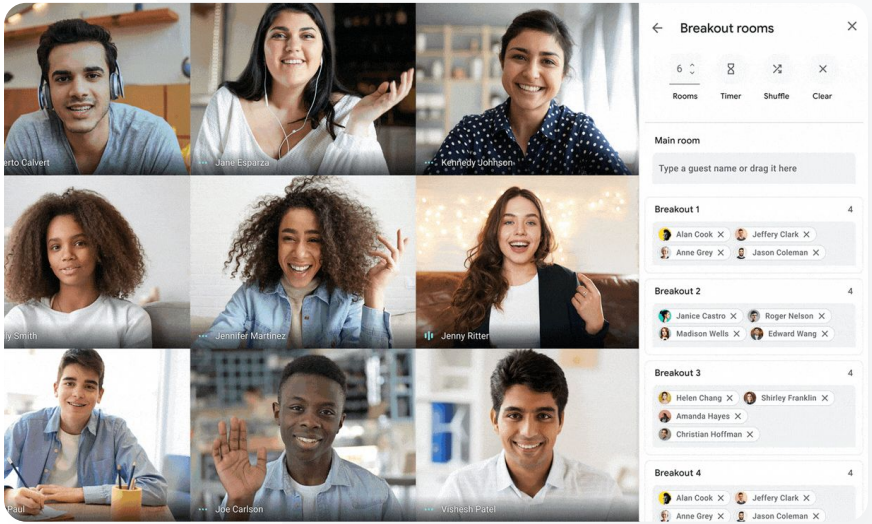
Relevant dokumentation i hjälpcentret

- Använda smågrupper i Google Meet

Så här gör du: Skapa små elevgrupper

Skapa smågrupper under mötet:

- Starta ett videosamtal
- Välj **ikonen för Aktiviteter** uppe till höger > **Smågrupper**
- **Välj antalet smågrupper** som du behöver i panelen Smågrupper
- 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.”

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 med hjälp av livestreamingrapporter
- Moderatorer kan aktivera eller inaktivera närvarospårning och livestreamingrapporter i mötet eller via händelsen i Kalender

Stegvisa anvisningar

Relevant dokumentation i hjälpcentret

- Spåra närvaro i Google Meet

Så här gör du: Kontrollera närvaron

Så här kontrollerar du närvaron i ett möte:

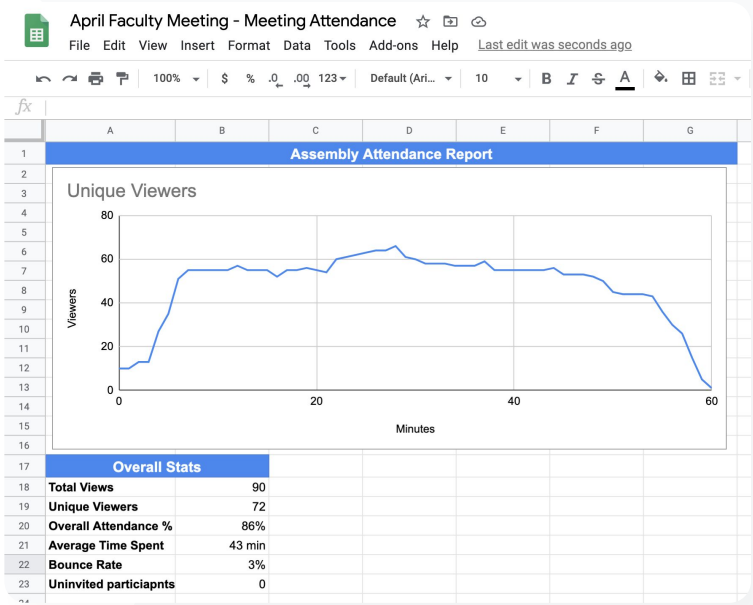
- Starta ett videosamtal
- Välj **menyikonen** längst ned
- Välj **Inställningar** > **Värdkontroller**
- Aktivera eller inaktivera **Närvarospårning**

Så här kontrollerar du närvaron i Kalender:

- **Aktivera Google Meet-konferenser** i en Kalender-händelse
- Välj **Inställningar** till höger
- Markera kryssrutan bredvid **Närvarospårning** > klicka på **Spara**

Få en närvarorapport:

- Efter mötet får moderatorn **rapporten via e-post**
- Öppna e-postmeddelandet och välj den **bifogade rapporten**



Relevant dokumentation i hjälpcentret

- Spåra närvaro i Google Meet

Tack