Google for Education

40 e più modi per utilizzare le versioni a pagamento di Google Workspace for Education

goo.gle/use-edu-workspace

Come utilizzare questa presentazione

Questa presentazione include una selezione di casi d'uso popolari disponibili per chi utilizza una delle **versioni a pagamento di Google Workspace for Education**. Gli strumenti descritti contribuiscono ad aumentare **la sicurezza dei dati, l'efficienza degli insegnanti, il coinvolgimento degli studenti** e **la collaborazione a livello dell'intera scuola**, solo per fare alcuni esempi.

La presentazione è organizzata per **funzionalità**. Per ognuna di queste vengono riportati di volta in volta **casi d'uso comuni** e semplici **istruzioni** per il relativo utilizzo. Leggi l'intera presentazione per scoprire tutto quello che le versioni a pagamento di Google Workspace for Education ti consentono di fare.

Le versioni a pagamento di Google Workspace for Education

Le tre versioni a pagamento di Google Workspace for Education ti consentono di usufruire di una scelta più ampia, di più opzioni di controllo e di un maggiore livello di flessibilità per soddisfare le esigenze della tua organizzazione.

Google Workspace for Education Plus

Include Education Standard, Teaching and Learning Upgrade e altre funzionalità esclusive della versione Plus.

Education Plus mette a disposizione di studenti, insegnanti, dirigenti scolastici e amministratori IT una soluzione di tecnologia educativa **all-in-one** che offre strumenti di facile utilizzo **per approfondimenti e sicurezza di livello avanzato oltre a esperienze di apprendimento e insegnamento.**

Google Workspace for Education Standard

Gli strumenti avanzati di sicurezza e approfondimento aiutano a ridurre i rischi e ad attenuare le minacce attraverso un livello più elevato di visibilità e controllo nell'intero ambiente di apprendimento.

Teaching and Learning Upgrade

Gli strumenti ottimizzati per l'insegnamento e l'apprendimento offrono un vantaggio didattico poiché rendono l'apprendimento più personalizzato, creano efficienza in classe e consentono di insegnare e apprendere in qualsiasi luogo.

Sommario

Funzionalità avanzate di sicurezza e approfondimento

Dashboard per la sicurezza

- Volume di spam
- Condivisione esterna dei file
- Applicazioni di terze parti
- Tentativo di phishing

Stato della sicurezza

- Best practice per la sicurezza
- Consigli per le aree a rischio

Strumento di indagine

- Condivisione di materiale illecito
- Condivisione accidentale di file
- Gestione delle email
- Email di phishing e malware
- Blocco dei malintenzionati
- Approfondimenti più dettagliati sulla sicurezza
- Eliminazione delle riunioni senza supervisione

Gestione e controllo del dominio

- Scansione degli allegati Gmail per il rilevamento delle minacce
- Creazione di dashboard e report sull'utilizzo
- Migliore reperimento dei file
- Organizzazione dei documenti interni
- Creazione automatica dei gruppi del reparto
- Creazione dei segmenti di pubblico per la condivisione interna dei file
- Limitazione della condivisione dei file
- Limitazione delle app di Workspace
- Gestione dello spazio di archiviazione nel dominio
- Normative sui dati
- Normative sulle sovvenzioni
- Gestione dei dispositivi endpoint
- Gestione dei dispositivi Windows
- Impostazioni personalizzate per i dispositivi Windows 10
- Automazione degli aggiornamenti dei dispositivi Windows 10
- Utilizzo della crittografia lato client

Sommario

Funzionalità ottimizzate di insegnamento e apprendimento

Google Classroom

- Gestione dell'accesso ai componenti aggiuntivi di Classroom
- Integrazione di contenuti coinvolgenti in Classroom
- Creazione di corsi su vasta scala

Report sull'originalità

- Analisi per rilevare casi di plagio con i report sull'originalità
- Verifica dell'originalità sulla base dei precedenti lavori degli studenti
- Rilevamento dei casi di plagio come opportunità di apprendimento

Documenti, Fogli e Presentazioni

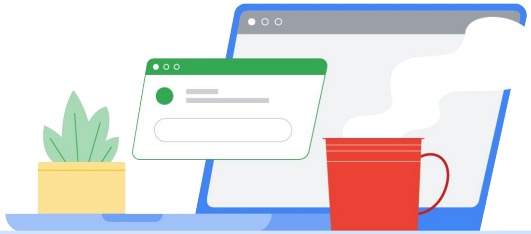
- Approvazione della documentazione interna

Google Meet

- Registrazione delle riunioni
- Consultazione di quanto discusso in classe
- Eliminazione delle barriere linguistiche
- Trasmissione di assemblee, riunioni ed eventi scolastici
- Possibilità di fare domande
- Raccolta di opinioni
- Piccoli gruppi di studenti
- Monitoraggio delle partecipazioni

Funzionalità avanzate di sicurezza e approfondimento

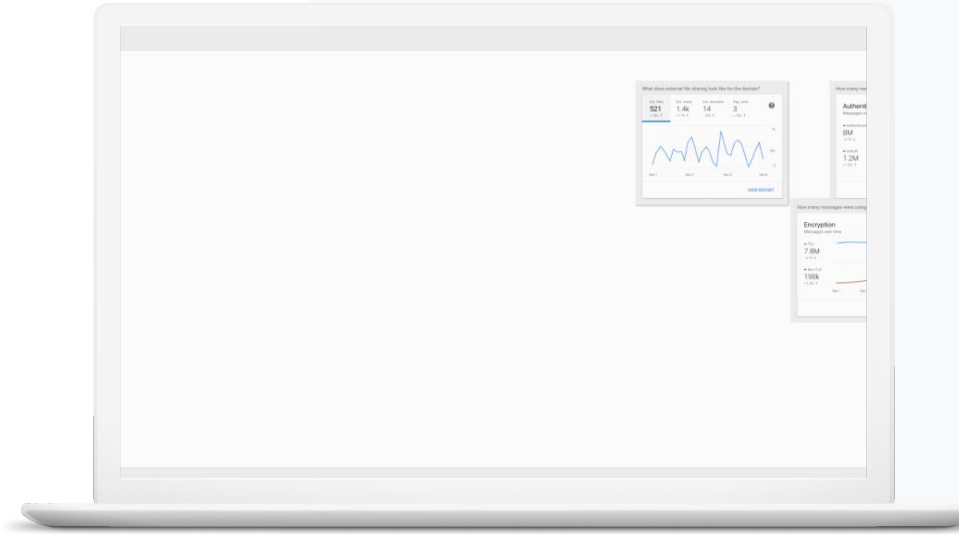
Controlla meglio il tuo dominio grazie a strumenti di sicurezza proattivi che ti consentono di difenderti dalle minacce, di analizzare gli incidenti di sicurezza e di proteggere i dati degli studenti e del corpo docenti.



Dashboard per la sicurezza

Di cosa si tratta?

Utilizza la dashboard per la sicurezza per visualizzare una panoramica dei vari report sulla sicurezza. Per impostazione predefinita, ciascun riquadro del report di sicurezza visualizza i dati relativi agli ultimi sette giorni. Puoi personalizzare la dashboard in modo da visualizzare i dati relativi a: Oggi, Ieri, Questa settimana, Ultima settimana, Questo mese, Mese scorso o Numero di giorni precedenti (fino a 180).



Casi d'uso

Volume di spam	Istruzioni passo passo
Condivisione esterna dei file	Istruzioni passo passo
Applicazioni di terze parti	Istruzioni passo passo
Tentativo di phishing	Istruzioni passo passo

“Voglio essere in grado di controllare le email eccessive e non necessarie e ridurre allo stesso tempo le minacce per la mia scuola.”

Volume di spam

La **dashboard per la sicurezza** fornisce una rappresentazione visiva delle attività svolte nel tuo ambiente Google Workspace for Education, ad esempio:

- Spam
- Phishing
- Malware
- Allegati sospetti
- Altre attività

Istruzioni passo passo

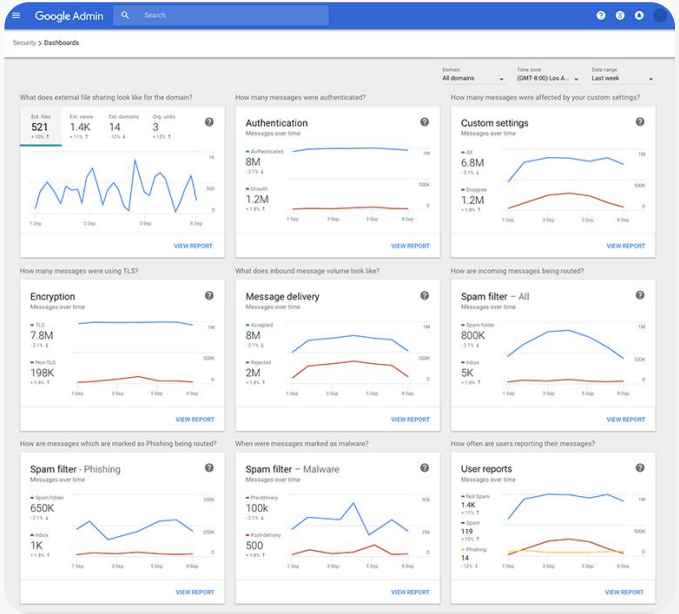
Documentazione pertinente del Centro assistenza

- Informazioni sulla dashboard per la sicurezza

Istruzioni: panoramica della dashboard

Come visualizzare la dashboard per la sicurezza

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Dashboard**
- Dalla dashboard per la sicurezza puoi analizzare i dati, esportare i dati in Fogli o in uno strumento di terze parti oppure lanciare un'indagine nello strumento di indagine



Documentazione pertinente del Centro assistenza

- Informazioni sulla dashboard per la sicurezza

“Voglio prendere visione delle attività di condivisione esterna dei file per evitare che dati sensibili vengano condivisi con terze parti.”

Condivisione esterna dei file

Utilizza il **report Esposizione file** disponibile nella **dashboard per la sicurezza** per consultare una serie di metriche relative alla condivisione file all'esterno del tuo dominio, tra cui ad esempio:

- Numero di eventi di condivisione con utenti esterni al dominio relativi a un periodo di tempo specifico.
- Numero di visualizzazioni ricevute da un file esterno in un determinato periodo di tempo.

Istruzioni passo passo

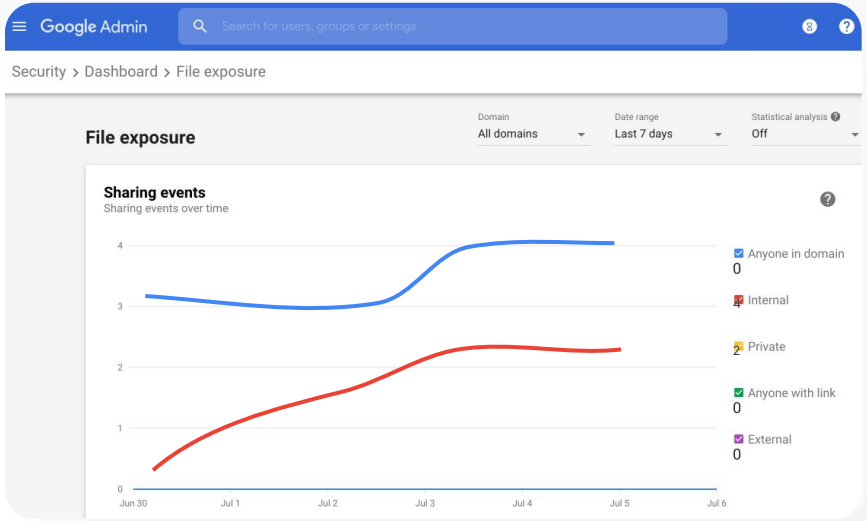
Documentazione pertinente del Centro assistenza

- Inizia a usare la pagina Stato della sicurezza

Istruzioni: condivisione esterna dei file

Come visualizzare il report Esposizione file

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Dashboard**
- Nel riquadro intitolato "**Qual è lo stato della condivisione di file esterna nel dominio?**", fai clic su **Visualizza report** nell'angolo in basso a destra



Documentazione pertinente del Centro assistenza

- Informazioni sulla dashboard per la sicurezza
- Report Esposizione file

Applicazioni di terze parti

Utilizza il **report Attività di autorizzazione con OAuth** disponibile nella **dashboard per la sicurezza** per tenere sotto controllo le applicazioni di terze parti collegate al tuo dominio e i dati a cui hanno accesso.

- Tramite le autorizzazioni con OAuth, si consente a servizi di terze parti di accedere ai dati dell'account di un utente senza dover rendere nota la sua password. È consigliabile limitare le app di terze parti che dispongono dell'accesso.
- Utilizza il riquadro Attività di autorizzazione con OAuth per monitorare le attività di autorizzazione in base ad app, ambito o utente e aggiornare le autorizzazioni concesse.

> “Voglio sapere quali applicazioni di terze parti hanno accesso ai dati del mio dominio.”

Istruzioni passo passo

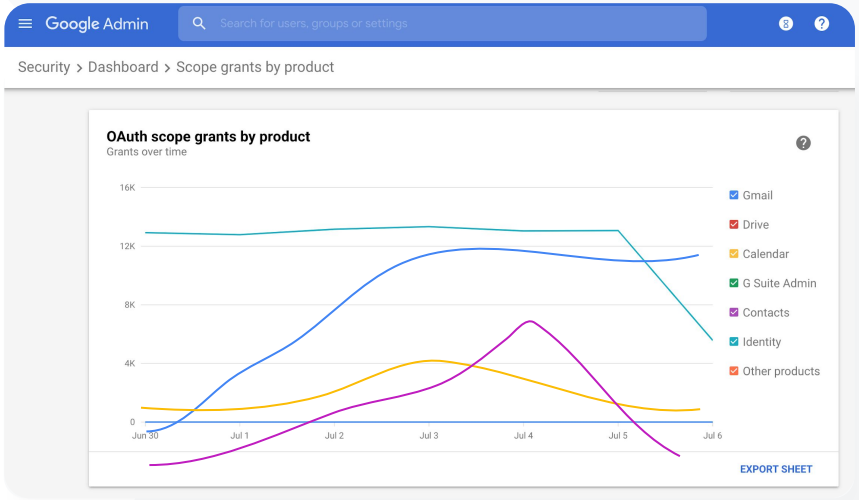
Documentazione pertinente del Centro assistenza

- Report Attività di autorizzazione con OAuth

Istruzioni: applicazioni di terze parti

Come visualizzare il report Attività di autenticazione OAuth

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Dashboard**
- In basso, fai clic su **Visualizza report**
- Puoi visualizzare le attività di autorizzazione con OAuth in base a prodotto (app), ambito o utente
- Per filtrare le informazioni, fai clic su **Applicazione**, **Ambito** o **Utente**
- Per generare un report in formato foglio di lavoro, fai clic su **Esporta foglio**



Documentazione pertinente del Centro assistenza

- Report Attività di autorizzazione con OAuth

“Gli utenti hanno segnalato un tentativo di phishing. Voglio essere in grado di risalire al momento in cui l'email di phishing è arrivata, in cosa consisteva esattamente l'email ricevuta dall'utente e quali rischi comportava.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- In che modo gli utenti contrassegnano le email
- Report utenti

Tentativo di phishing

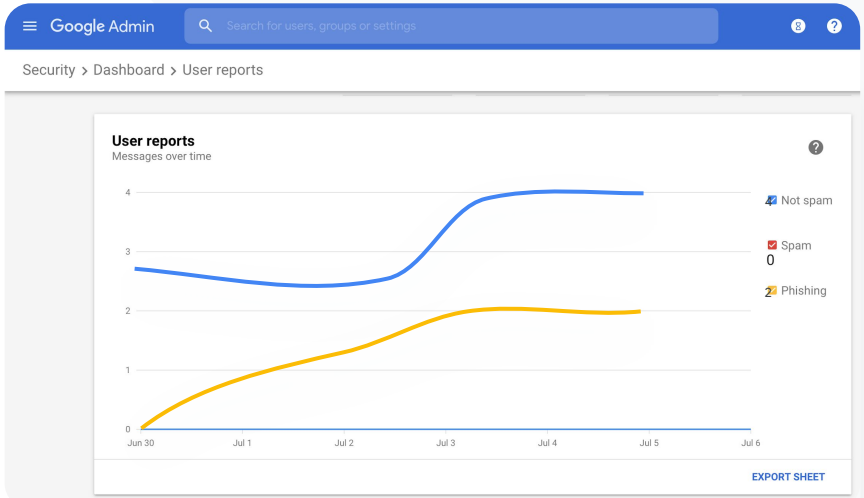
Nel **riquadro Report utenti** della **dashboard per la sicurezza** puoi visualizzare i messaggi che sono stati segnalati come phishing o spam in un determinato periodo di tempo. Puoi visualizzare alcune informazioni sulle email segnalate come phishing, ad esempio i relativi destinatari e le aperture.

- Il riquadro Report utenti mostra come gli utenti contrassegnano i messaggi, ad esempio spam, non spam o phishing, durante un intervallo di tempo specifico.
- Puoi personalizzare il grafico in modo che fornisca i dettagli soltanto su alcuni tipi di messaggi, ad esempio quelli inviati internamente o esternamente, in un intervallo di date e così via.

Istruzioni: tentativo di phishing

Come visualizzare il riquadro Report utenti

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Dashboard**
- Nell'angolo in basso a destra del **riquadro Report utenti**, fai clic su **Visualizza report**



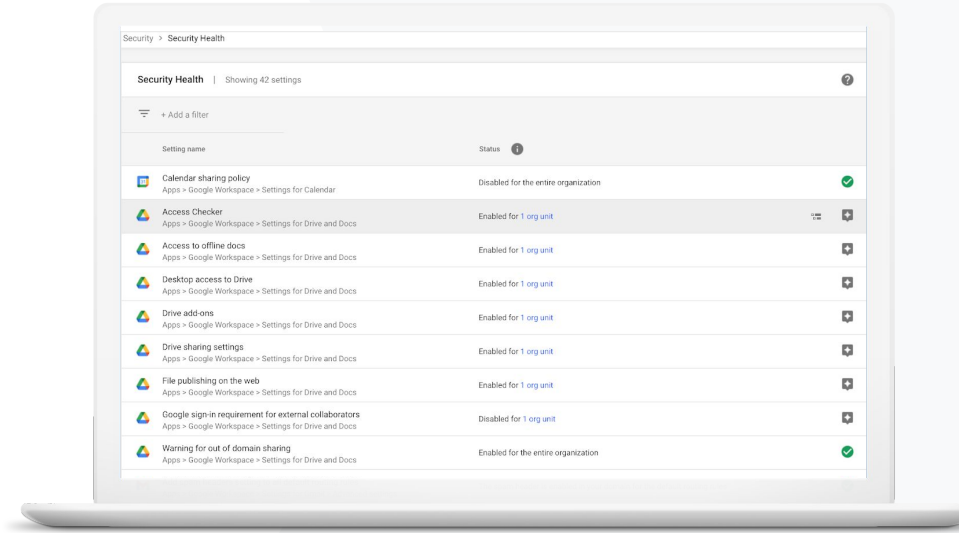
Documentazione pertinente del Centro assistenza

- Informazioni sulla dashboard per la sicurezza
- Report Esposizione file

Stato della sicurezza

Di cosa si tratta?

La pagina Stato della sicurezza fornisce una panoramica completa del livello di sicurezza del tuo ambiente Google Workspace e ti consente di confrontare le tue configurazioni con i consigli di Google per proteggere in modo proattivo la tua organizzazione.



Casi d'uso

Best practice per la sicurezza — Istruzioni passo passo

Consigli per le aree a rischio — Istruzioni passo passo

“Vorrei sapere dove posso trovare best practice o consigli su come configurare i criteri di sicurezza.”

Best practice per la sicurezza

Apri la pagina Stato della sicurezza per accedere a best practice sui criteri di sicurezza con:

- Consigli per le aree del tuo dominio potenzialmente a rischio
- Consigli sulle impostazioni ottimali per una sicurezza più efficace
- Link diretti alle impostazioni
- Informazioni aggiuntive e articoli di assistenza

Istruzioni passo passo

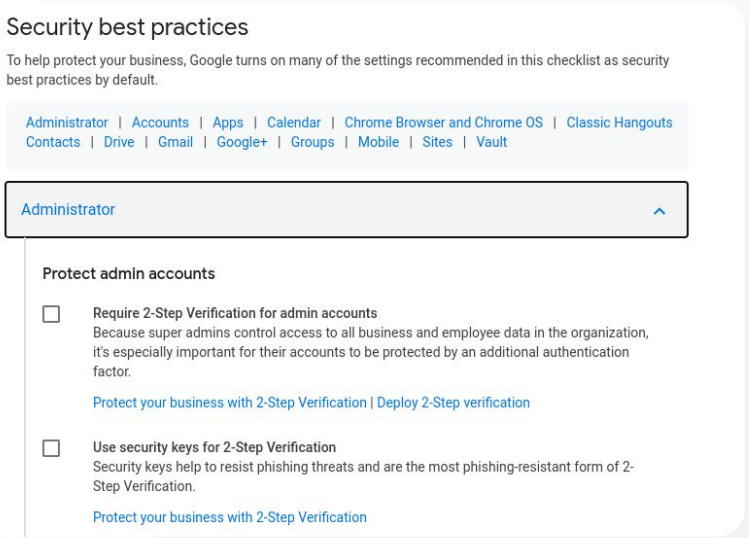
Documentazione pertinente del Centro assistenza

- Inizia a usare la pagina Stato della sicurezza

Istruzioni: elenco di controllo delle best practice per la sicurezza

Per contribuire a proteggere la tua organizzazione, Google attiva per impostazione predefinita molte delle impostazioni consigliate in questo elenco di controllo come best practice per la sicurezza. Ti consigliamo di esaminare in maggiore dettaglio quelle messe in evidenza di seguito.

- **Amministratore:** proteggere gli account amministratore
- **Account:** prevenire e sanare le compromissioni degli account
- **Applicazioni:** rivedere l'accesso di terze parti ai servizi principali
- **Calendar:** limitare la condivisione esterna dei calendari
- **Drive:** limitare la condivisione e la collaborazione all'esterno del dominio
- **Gmail:** configurare l'autenticazione e l'infrastruttura
- **Vault:** esaminare, controllare e proteggere gli account Vault



Documentazione pertinente del Centro assistenza

- Monitorare lo stato delle impostazioni di sicurezza

“Voglio avere un'istantanea immediata delle impostazioni di sicurezza del mio dominio, con consigli concreti sui provvedimenti da adottare per le aree potenzialmente a rischio.”

Consigli per le aree a rischio

La pagina **Stato della sicurezza** passa in rassegna la tua configurazione di sicurezza e segnala le modifiche consigliate. In questa pagina puoi:

- Identificare rapidamente le aree del tuo dominio potenzialmente a rischio
- Ricevere consigli sulle impostazioni ottimali per una sicurezza più efficace
- Leggere informazioni aggiuntive e articoli di assistenza in merito ai consigli

Istruzioni passo passo

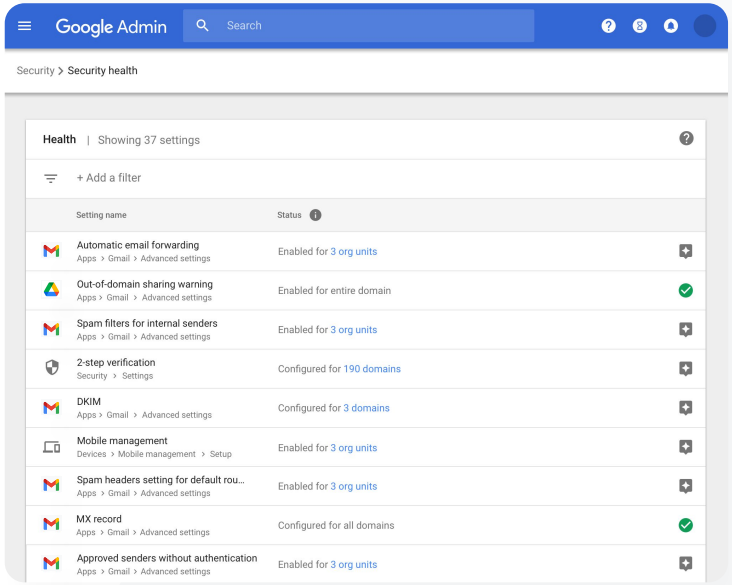
Documentazione pertinente del Centro assistenza

- Inizia a usare la pagina Stato della sicurezza

Istruzioni: consigli per la sicurezza

Come visualizzare i consigli

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Stato della sicurezza**
- Visualizza le impostazioni relative allo stato nella colonna più a destra
  - Il segno di spunta verde indica che l'impostazione è sicura
  - L'icona di colore grigio indica la presenza di un consiglio relativo all'impostazione: fai clic sull'icona per aprire dettagli e istruzioni



Documentazione pertinente del Centro assistenza

- Inizia a usare la pagina Stato della sicurezza

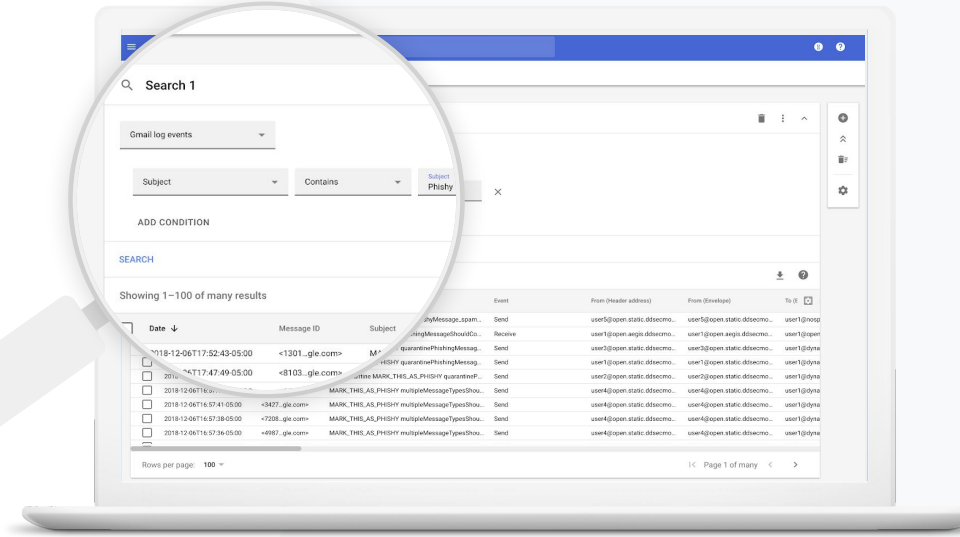
Strumento di indagine

Di cosa si tratta?

Utilizza lo strumento di indagine per identificare, assegnare una priorità e intervenire in merito a problemi di sicurezza e privacy nel tuo dominio.

Casi d'uso

Condivisione di materiale illecito	Istruzioni passo passo
Condivisione accidentale di file	Istruzioni passo passo
Gestione delle email	Istruzioni passo passo
Email di phishing/malware	Istruzioni passo passo
Blocco dei malintenzionati	Istruzioni passo passo
Approfondimenti più dettagliati sulla sicurezza	Istruzioni passo passo
Eliminazione delle riunioni senza supervisione	Istruzioni passo passo



“So che c'è un file contenente materiale illecito che viene condiviso. Voglio sapere chi lo ha creato, quando è stato creato, chi lo ha condiviso con chi e chi lo ha modificato. Inoltre, voglio eliminarlo.”

Condivisione di materiale illecito

Gli eventi del log di Drive disponibili nello **strumento di indagine** possono aiutarti a trovare, monitorare e isolare o eliminare i file indesiderati nel tuo dominio. Grazie all'accesso ai Dati degli eventi del log di Drive puoi:

- Cercare i documenti in base a nome, attore, proprietario e altro
- Prendere provvedimenti eliminando il file o modificando le relative autorizzazioni
- Cercare i contenuti che gli utenti creano in Google Workspace e quelli che caricano su Drive
- Visualizzare tutte le informazioni di log correlate al documento in questione
  - Data di creazione
  - Chi è il proprietario, chi ne ha preso visione e chi lo ha modificato
  - Quando è stato condiviso

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Condizioni per gli eventi dei log di Drive
- Azioni per gli eventi del log di Drive

“Un file è stato condiviso per errore con un gruppo che NON dovrebbe avervi accesso.

Voglio rimuovere l'accesso a questi utenti.”

Condivisione accidentale di file

Gli eventi del log di Drive nello **strumento di indagine** possono aiutarti a monitorare e risolvere i problemi di condivisione dei file. Grazie all'accesso ai Dati degli eventi del log di Drive puoi:

- Cercare i documenti in base a nome, attore, proprietario e così via
- Visualizzare tutte le informazioni di log correlate al documento in questione, ad esempio chi ne ha preso visione e quando è stato condiviso
- Prendere provvedimenti modificando le autorizzazioni e disattivando le opzioni di download, stampa e copia

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Eseguire una ricerca nello strumento di indagine
- Adottare azioni basate sui risultati della ricerca

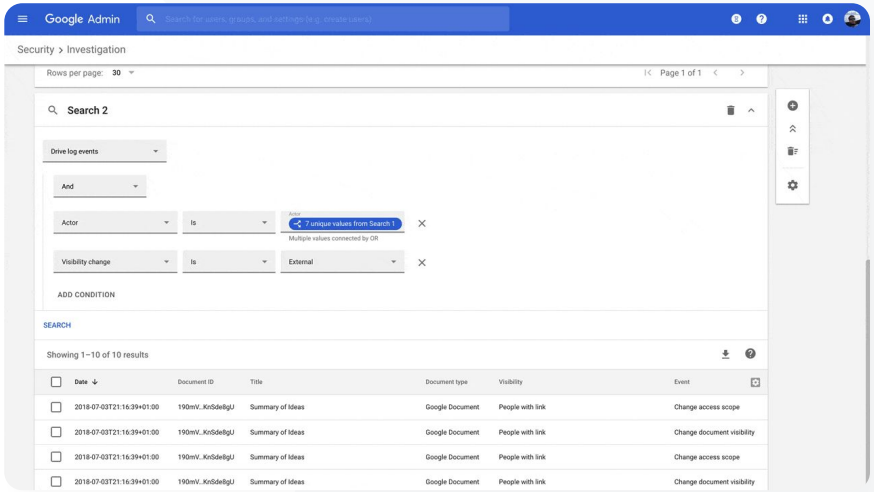
Istruzioni: eventi del log di Drive

Come si effettuano indagini negli eventi del log di Drive

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Strumento di indagine**
- Seleziona **Eventi del log di Drive**
- Fai clic su **Aggiungi condizione** > **Cerca**

Come intervenire

- Seleziona il file pertinente nei risultati di ricerca
- Fai clic su **Azioni** > **Autorizzazioni file per il controllo** per aprire la pagina Autorizzazioni
- Fai clic su **Persone** per vedere chi ha accesso
- Fai clic su **Link** per visualizzare o modificare le impostazioni di condivisione tramite link per i file selezionati
- Fai clic su **Modifiche in sospeso** per esaminare le modifiche prima di salvare



Documentazione pertinente del Centro assistenza

- Eseguire una ricerca nello strumento di indagine
- Adottare azioni basate sui risultati della ricerca

“Qualcuno ha inviato un'email che NON avrebbe dovuto essere spedita. Voglio sapere a chi l'hanno mandata e se i destinatari l'hanno aperta e hanno risposto. Infine, voglio eliminarla. Voglio anche conoscere i contenuti dell'email.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Condizioni per i log di Gmail e i messaggi di Gmail
- Azioni per i messaggi di Gmail e gli eventi dei log di Gmail
- Procedura per poter visualizzare i contenuti di un'email

Gestione delle email

I **log di Gmail** disponibili nello **strumento di indagine** possono aiutarti a identificare le email pericolose o illecite nel tuo dominio e a prendere i necessari provvedimenti. L'accesso ai log di Gmail ti consente di:

- Cercare specifiche email in base a oggetto, ID messaggio, allegato, mittente e altri criteri simili
- Visualizzare i dettagli delle email, tra cui autore, destinatario, aperture e inoltri
- Intervenire in funzione dei risultati di ricerca: ad esempio puoi eliminare i messaggi di Gmail, ripristinarli, contrassegnarli come spam o phishing, inviarli a Posta in arrivo e metterli in quarantena

“

È stata inviata un'email di phishing o malware agli utenti. Vogliamo vedere se gli utenti hanno fatto clic sul link contenuto nell'email o scaricato l'allegato, in quanto queste azioni possono potenzialmente esporre a rischi gli utenti e il nostro dominio.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Condizioni per i log di Gmail e i messaggi di Gmail
- Azioni per i messaggi di Gmail e gli eventi dei log di Gmail
- Procedura per poter visualizzare i contenuti di un'email
- Visualizzare i report di VirusTotal

Email di phishing e malware

Aprire lo **strumento di indagine**, e nello specifico i **log di Gmail**, può essere utile per trovare e isolare le email dannose all'interno del dominio. L'accesso ai log di Gmail ti consente di:

- Cercare i messaggi email in base a specifici contenuti, allegati compresi
- Visualizzare le informazioni relative a email specifiche, tra cui i destinatari e le aperture
- Visualizzare i messaggi e i thread per determinare se sono dannosi
- Analizzare gli allegati delle email per trovare il contesto dettagliato della minaccia e i dati di reputazione con i report di VirusTotal
- Adottare provvedimenti contrassegnando i messaggi come spam o phishing, inviarli a una specifica Posta in arrivo, metterli in quarantena o eliminarli

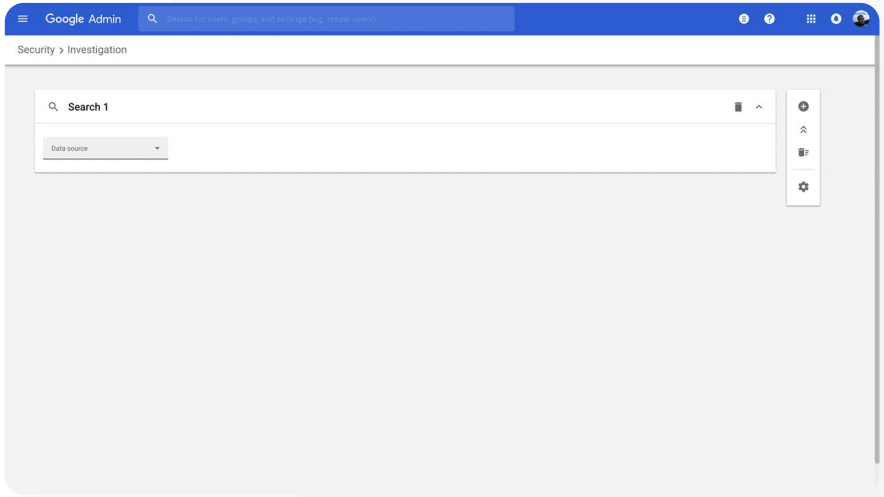
Istruzioni: log di Gmail

Come eseguire indagini nei log di Gmail

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Strumento di indagine**
- Seleziona **Eventi del log di Gmail** OPPURE **Messaggi Gmail**
- Fai clic su **Aggiungi condizione** > **Cerca**

Come intervenire

- Seleziona il file pertinente nei risultati di ricerca
- Fai clic su **Azioni**
- Seleziona **Elimina messaggio dalla Posta in arrivo**
- Per confermare l'azione, fai clic su Visualizza in fondo alla pagina
- Nella colonna **Risultato** potrai visualizzare lo stato dell'azione



Documentazione pertinente del Centro assistenza

- Condizioni per i log di Gmail e i messaggi di Gmail
- Azioni per i messaggi di Gmail e gli eventi dei log di Gmail
- Procedura per poter visualizzare i contenuti di un'email

“Un malintenzionato prende costantemente di mira gli utenti di alto profilo del mio dominio e non riesco in alcun modo a beccarlo.

Come posso fermarlo?”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Cercare e analizzare gli eventi del log utente
- Creare regole di attività con lo strumento di indagine

Blocco dei malintenzionati

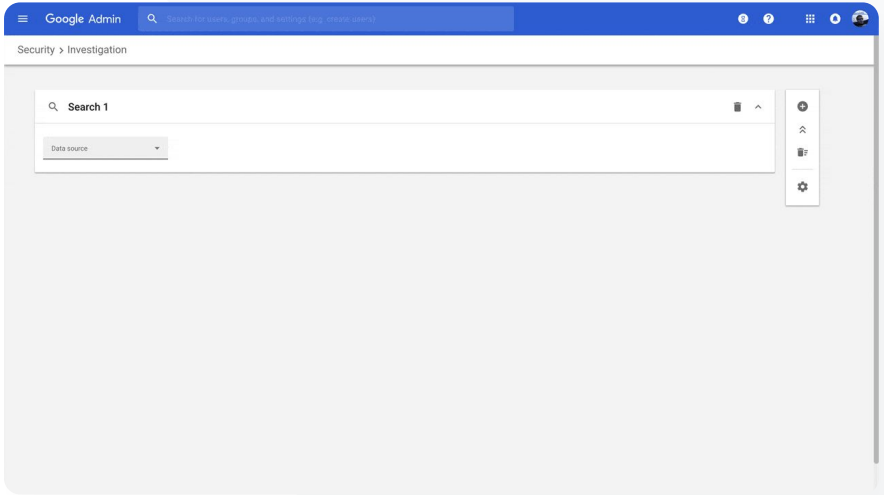
Il **log utente** presente nello **strumento di indagine** ti può aiutare a:

- Identificare e analizzare i tentativi da parte di utenti malintenzionati di assumere il controllo degli account utente dell'organizzazione
- Monitorare i metodi di verifica in due passaggi utilizzati dagli utenti della tua organizzazione
- Ottenere maggiori informazioni sui tentativi di accesso non riusciti da parte di utenti della tua organizzazione
- Creare regole di attività con lo strumento di indagine: bloccare automaticamente i messaggi e altre attività dannose di determinati attori
- Garantire una protezione più efficace agli utenti di alto profilo con il programma di protezione avanzata
- Ripristinare o sospendere utenti

Istruzioni: blocco dei malintenzionati

Come eseguire indagini negli eventi del log utente

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Strumento di indagine**
- Seleziona **Eventi dei log utente**
- Fai clic su **Aggiungi condizione** > **Cerca**



Come ripristinare o sospendere utenti

- Dai risultati di ricerca, seleziona uno o più utenti
- Fai clic sul menu a discesa **Azioni**
- Fai clic su **Ripristina utente** o **Sospendi utente**

Come visualizzare i dettagli relativi a uno specifico utente

- Dalla pagina dei risultati di ricerca, seleziona un solo utente
- Dal menu a discesa AZIONI, fai clic su **Visualizza dettagli**

Documentazione pertinente del Centro assistenza

- Cercare e analizzare gli eventi del log utente

Uno dei nostri insegnanti ha segnalato un file allegato in Gmail che sembrava sospetto.

C'è un modo affinché il reparto IT stabilisca se il file è una minaccia per la sicurezza?”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Eseguire una ricerca nello strumento di indagine
- Visualizzare i report di VirusTotal dallo strumento di indagine

Approfondimenti più dettagliati sulla sicurezza

I report di VirusTotal espandono i risultati di un'indagine sulla sicurezza fornendo una panoramica completa, che permette agli amministratori di verificare la sicurezza di un particolare dominio, file allegato, indirizzo IP o URL sulla base di informazioni provenienti da crowdsourcing.

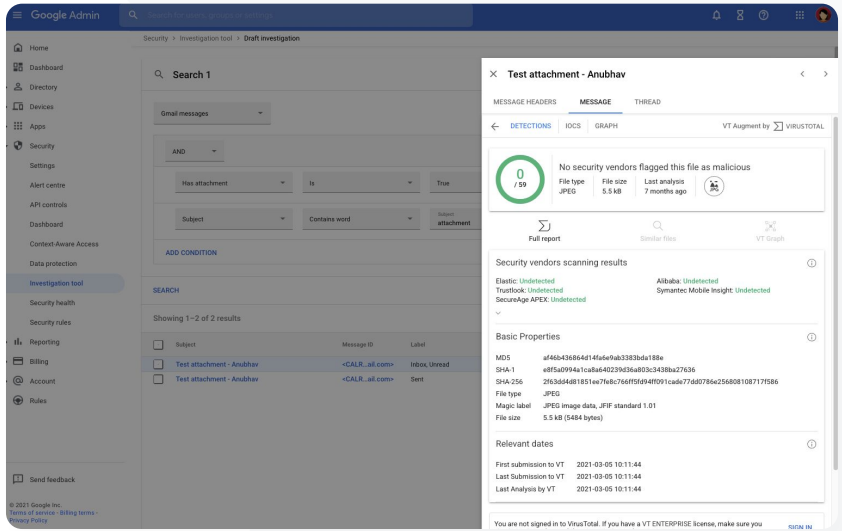
- Ulteriori informazioni importanti sulla sicurezza relative agli eventi dei log di Gmail e di Chrome
- Analisi di file, URL, domini e indirizzi IP sospetti
- Dettagli in crowdsourcing sul motivo per cui un allegato o un sito web potrebbero essere considerati rischiosi
- Assistenza nel processo decisionale mirato alla risoluzione dei problemi di sicurezza

Istruzioni: approfondimenti più dettagliati sulla sicurezza

Come si visualizzano i report di VirusTotal relativi a Gmail

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Centro sicurezza** > **Strumento di indagine**
- Scegli **Messaggi Gmail**
- Fai clic su **Aggiungi condizione** > **Con allegato**
- Nei risultati della ricerca, fai clic sul link **ID messaggio** o **Oggetto**
- Dal riquadro laterale, fai clic sulla scheda **Messaggio** o **Thread**
- Seleziona **Visualizza il report di VirusTotal**

Gli amministratori possono visualizzare anche i report di VirusTotal relativi a Chrome. Basta seguire le istruzioni qui sopra e selezionare **Eventi del log di Chrome** nello strumento di indagine.



Documentazione pertinente del Centro assistenza

- Visualizzare i report di VirusTotal dallo strumento di indagine

“Gli studenti rimangono nelle chiamate di Google Meet anche dopo il termine delle lezioni. Ho bisogno di fare in modo che le chiamate di Meet terminino per tutti affinché non si creino singhiozzi nella didattica.”

Eliminazione delle riunioni virtuali senza supervisione

Gli amministratori di Google Workspace possono utilizzare l'azione **Termina riunione per tutti** nello strumento di indagine per rimuovere tutti gli utenti da qualsiasi riunione all'interno dell'organizzazione. Anche gli organizzatori delle riunioni hanno questa possibilità per la singola chiamata di Google Meet.

- La riunione terminerà per tutti gli utenti che partecipano in quel momento, inclusi quelli dei gruppi di lavoro associati
- Questa azione impedisce anche a chiunque di partecipare alle istanze future di quella riunione in assenza dell'organizzatore

Istruzioni passo passo

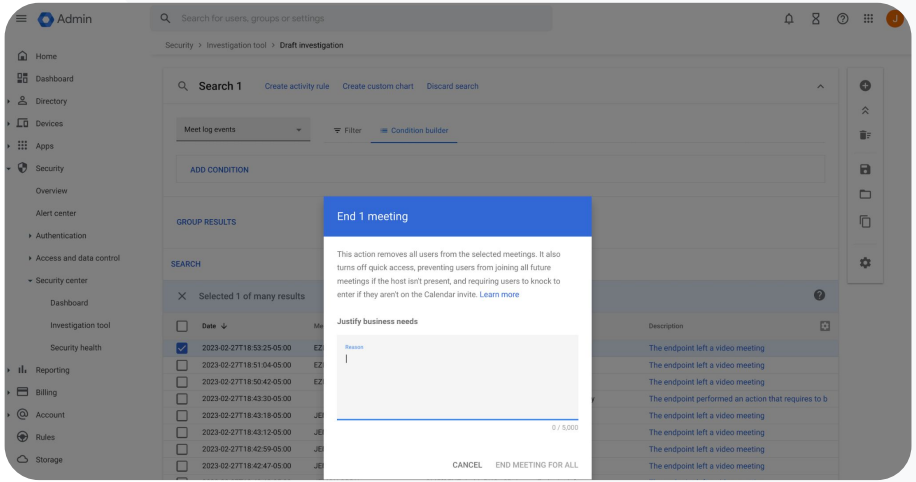
Documentazione pertinente del Centro assistenza

- Utilizzare lo strumento di indagine per terminare le riunioni

Istruzioni: eliminazione delle riunioni virtuali senza supervisione

Come utilizzare lo strumento di indagine per terminare una riunione per tutti gli utenti

- Accedi alla **Console di amministrazione**
- Fai clic su **Sicurezza** > **Centro sicurezza** > **Strumento di indagine**
- Seleziona **Eventi del log di Meet**
- Fai clic su **Cerca** > Nei risultati di ricerca verrà visualizzato un elenco di eventi del log di Meet
- Seleziona le caselle corrispondenti alle riunioni che vuoi terminare per tutti gli utenti
- Seleziona **Azioni**
- Fai clic su **Termina riunione per tutti**



Documentazione pertinente del Centro assistenza

- Utilizzare lo strumento di indagine per terminare le riunioni

Gestione e controllo del dominio

Gli amministratori hanno accesso agli strumenti avanzati di Google Workspace per gestire i dati della propria organizzazione, impostare controlli, monitorare l'utilizzo e garantire la conformità agli standard didattici.

Casi d'uso

Scansione degli allegati Gmail per il rilevamento delle minacce	Istruzioni passo passo
Creazione di dashboard e report sull'utilizzo	Istruzioni passo passo
Migliore reperimento dei file	Istruzioni passo passo
Organizzazione dei documenti interni	Istruzioni passo passo
Creazione automatica dei gruppi del reparto	Istruzioni passo passo
Creazione dei segmenti di pubblico per la condivisione interna dei file	Istruzioni passo passo
Limitazione della condivisione dei file	Istruzioni passo passo
Limitazione alle app di Workspace	Istruzioni passo passo
Gestione dello spazio di archiviazione	Istruzioni passo passo
Normative sui dati	Istruzioni passo passo
Normative sulle sovvenzioni	Istruzioni passo passo
Gestione dei dispositivi endpoint	Istruzioni passo passo
Gestione dei dispositivi Windows	Istruzioni passo passo
Impostazioni personalizzate per i dispositivi Windows 10	Istruzioni passo passo
Automazione degli aggiornamenti dei dispositivi Windows 10	Istruzioni passo passo
Utilizzo della crittografia lato client	Istruzioni passo passo

“Come posso garantire una migliore protezione del mio dominio contro le minacce costituite dai malware zero-day e dai ransomware?”

Scansione degli allegati Gmail per il rilevamento delle minacce

Gli allegati email possono includere software dannosi. Per identificare queste minacce, Gmail può sottoporre a scansione o eseguire gli allegati nella Sandbox per la sicurezza. Gli allegati identificati come minacce vengono inviati alla cartella Spam.

- Rilevare malware eseguendolo virtualmente in una Sandbox sicura e privata, in modo da analizzare gli effetti nocivi e determinare quali comportamenti dannosi può eseguire
- Eseguire la scansione di file Microsoft Word, PowerPoint, PDF, ZIP e altri
- Attivare la scansione per l'intero dominio o creare regole di scansione in base a condizioni specifiche come mittente, dominio e altro

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Configurare le regole per rilevare gli allegati dannosi

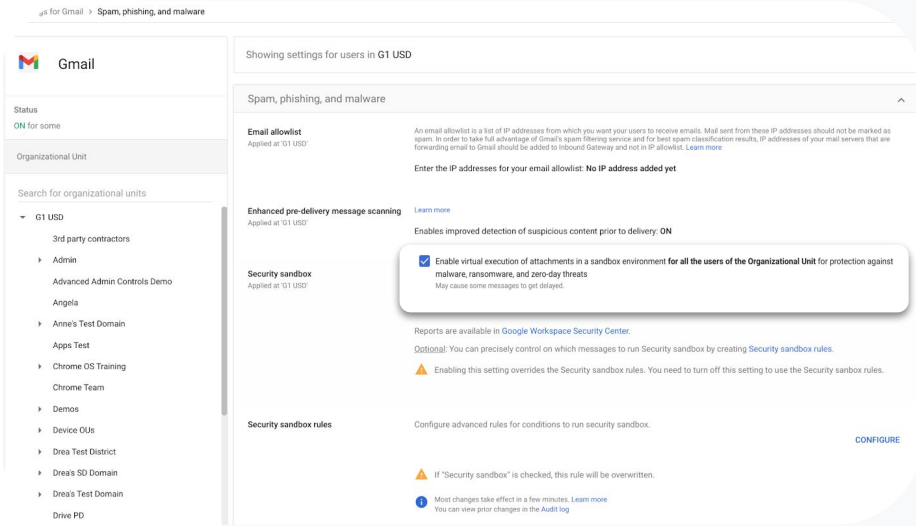
Istruzioni: scansione degli allegati Gmail per il rilevamento delle minacce

Come funziona

Il processo di detonazione in una sandbox, a cui gli allegati sono sottoposti prima che l'email venga recapitata, garantisce un ulteriore livello di sicurezza.

Come eseguire la scansione di tutti gli allegati in Sandbox per la sicurezza

- Accedi alla **Console di amministrazione**
- Fai clic su **Menu** > **App** > **Google Workspace** > **Gmail** > **Spam, phishing e malware**
- Seleziona l'unità organizzativa oppure applica le impostazioni all'intero dominio
- Scorri fino a **Sandbox per la sicurezza** nella sezione **Spam, phishing e malware**
- Seleziona la casella **Attiva l'esecuzione virtuale degli allegati in un ambiente sandbox**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Configurare le regole per rilevare gli allegati dannosi

“In che modo posso comprendere l'utilizzo di Classroom all'interno del dominio?”

Creazione di dashboard e report sull'utilizzo

Con **BigQuery Export e il modello di Looker Studio**, gli amministratori possono utilizzare i log delle attività di Classrooms per creare dashboard e report personalizzati con strumenti di analisi come Looker Studio e partner di visualizzazione terzi integrati in BigQuery.

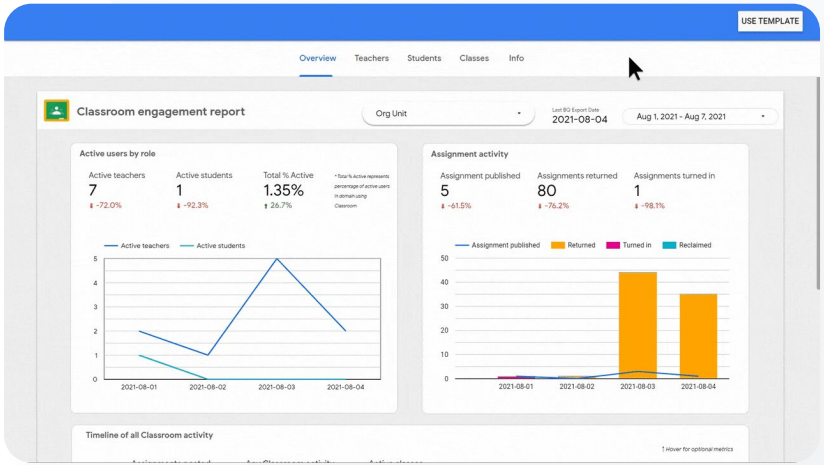
- Esporta i dati del log di Classroom dalla Console di amministrazione in BigQuery e Looker Studio
- Visualizza rapidamente i report sull'utilizzo e sull'adozione in tutto il dominio. Individua chi ha rimosso uno studente da un corso, chi ha archiviato un corso in una determinata data e altro ancora
- Grazie ai modelli di dashboard personalizzabili di Looker Studio, comprendi le tendenze generali e agisci più rapidamente

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Configurare BigQuery Export e il modello di Data Studio

Istruzioni: creazione di dashboard e report sull'utilizzo



01 Imposta ed esporta un progetto BigQuery

- Accedi a console.cloud.google.com > **Crea un nuovo progetto**
- Accedi ad admin.google.com > **Report** > **BigQuery Export**
- Fai clic sul **progetto BigQuery sul cloud** > Dai un nome al set di dati > **Salva**

02 Aggiungi la tua esportazione di BigQuery a Looker Studio

- Accedi a Looker Studio > **Crea** > **Origine dati**
- Seleziona **il connettore BigQuery** > **I miei progetti** > Fai clic sul progetto che hai creato > **Attività**
- Seleziona la casella alla voce **Tabella partizionata** > Fai clic su **Connetti**

03 Crea una dashboard di Looker Studio

- Apri il modello > Seleziona **Usa modello**
- Alla voce **Nuova origine dati**, scegli **Attività**
- Fai clic su **Copia report**

Documentazione pertinente del Centro assistenza

- Configurare BigQuery Export e il modello di Data Studio

Devo rintracciare i moduli di autorizzazione per le gite che le famiglie hanno inviato tramite Gmail, Chat e Documenti.

Come trovo questi file nel dominio?”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Guida a Google Cloud Search
- Attivare o disattivare Cloud Search per gli utenti

Migliore reperimento dei file

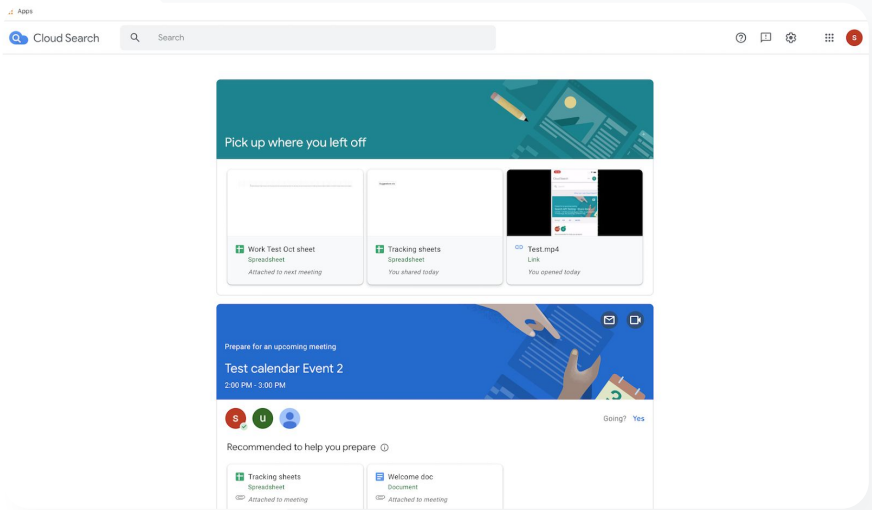
Con Google Cloud Search, gli insegnanti del tuo istituto possono trovare rapidamente i contenuti all'interno di Google Workspace e delle app di terze parti.

- Trova le informazioni di cui hai bisogno, ovunque tu sia, utilizzando il tuo laptop, cellulare o tablet
- Cerca nelle app di Google Workspace, come Drive, Contatti, Gmail, e nelle origini dati di terze parti

Istruzioni: migliore reperimento dei file

Attivare Cloud Search per gli utenti

- Accedi alla **Console di amministrazione** > Vai a **Menu** > **App** > **Google**
- Fai clic su **Stato del servizio**
- Per attivare o disattivare un servizio per tutti gli utenti dell'organizzazione, fai clic su **ON per tutti** oppure **OFF per tutti**
- Fai clic su **Salva**
- Per attivare un servizio per un insieme di utenti all'interno di una o tutte le unità organizzative, seleziona un **gruppo di accesso**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Guida a Google Cloud Search
- Attivare o disattivare Cloud Search per gli utenti

> Voglio applicare etichette “Sensibilità” ai file del mio istituto per allinearmi ai requisiti di conformità, prevenire l'uso improprio e migliorare l'organizzazione dei file.”

Organizzazione dei documenti interni

Le etichette di Drive aiutano gli utenti a trovare, organizzare e applicare norme in tutto il dominio. Gli amministratori possono creare e gestire le etichette di Drive per impedire l'uso improprio dei file e garantire che i dati degli studenti soddisfino i requisiti di conformità.

- Le etichette sono metadati che possono aiutare a organizzare file didattici sensibili come programmi individuali, documenti di istruzione militare o documenti di conformità
- Solo gli amministratori possono creare e pubblicare etichette e definirne le strutture. Gli utenti della tua organizzazione possono applicare etichette ai file che possono modificare, nonché impostare i valori dei campi
- Le etichette di Drive possono essere utilizzate a supporto della Prevenzione della perdita di dati automatica

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Gestire le etichette di Drive

Istruzioni: organizzazione dei documenti interni

Come funziona

Google Drive offre etichette con badge (un indicatore visivo) e standard per aiutarti a organizzare i file nel dominio.

Come attivare le etichette di Drive per il tuo istituto

- Accedi alla **Console di amministrazione**
- Fai clic su **Menu** > **App** > **Google Workspace** > **Drive e Documenti**
- Seleziona **Etichette**
- **Attiva** o **disattiva** le etichette.
- Fai clic su **Salva**

Documentazione pertinente del Centro assistenza

- Gestire le etichette di Drive

“Come posso automatizzare l'iscrizione a un gruppo affinché ogni volta che un nuovo docente si unisce al nostro istituto venga incluso nella mia lista mailing list ‘docenti’?”

Creazione automatica dei gruppi del reparto

I gruppi dinamici consentono agli amministratori di aggiornare l'appartenenza a gruppi a livello scolastico con criteri personalizzati.

- Crea gruppi dinamici che gestiscono automaticamente l'appartenenza
- Tieni aggiornati i gruppi in base a una query di appartenenza creata da te
- Utilizza i gruppi dinamici come:
  - Mailing list ed elenchi di distribuzione
  - Gruppi moderati e caselle di posta collaborative
  - Gruppi di sicurezza

Istruzioni passo passo

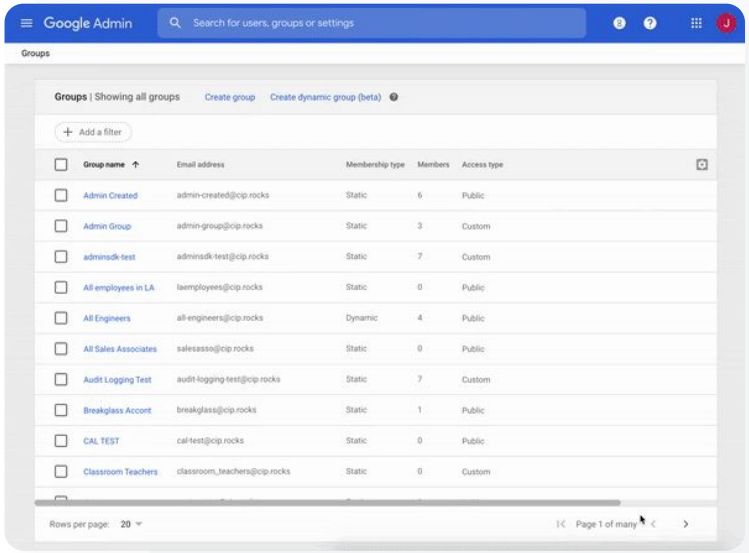
Documentazione pertinente del Centro assistenza

- Gestire l'appartenenza automaticamente con i gruppi dinamici

Istruzioni: creazione automatica dei gruppi del reparto

Creare un gruppo dinamico

- Accedi alla **Console di amministrazione** > Vai a **Menu** > **Directory** > **Gruppi**
- Fai clic su **Crea gruppo dinamico**
- Crea la tua query di appartenenza con:
  - Elenco delle condizioni: i criteri da usare per l'appartenenza, ad esempio "Reparto"
  - Campo Valore: il valore che vuoi utilizzare
- Inserisci le seguenti informazioni:
  - Nome: identifica il gruppo negli elenchi e nei messaggi
  - Descrizione: lo scopo del gruppo
  - Email del gruppo: l'indirizzo email usato per il gruppo
- Fai clic su **Salva**
- Fai clic su **Fine**



Documentazione pertinente del Centro assistenza

- Gestire l'appartenenza automaticamente con i gruppi dinamici

Il mio staff condivide accidentalmente documenti con tutta l'organizzazione, mettendo a rischio i dati sensibili. Come faccio a limitare la condivisione a un gruppo più piccolo e più pertinente?”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Informazioni sui segmenti di pubblico di destinazione
- Best practice per l'implementazione di un pubblico di destinazione
- Creare un pubblico di destinazione

Creazione dei segmenti di pubblico per la condivisione interna dei file

Le impostazioni del **pubblico di destinazione** aiutano a migliorare la sicurezza dei dati della tua organizzazione riducendo la possibilità che gli utenti condividano accidentalmente i file.

- Assicurati che i file vengano condivisi solo con le persone giuste, come un team o un reparto specifico
- I segmenti di pubblico di destinazione sono gruppi di persone che gli amministratori possono consigliare agli utenti per la condivisione dei propri file
- Gli amministratori possono aggiungere segmenti di pubblico di destinazione alle impostazioni di condivisione degli utenti per incoraggiare la condivisione con un pubblico più specifico
- Sono disponibili in Google Drive, Documenti e Chat

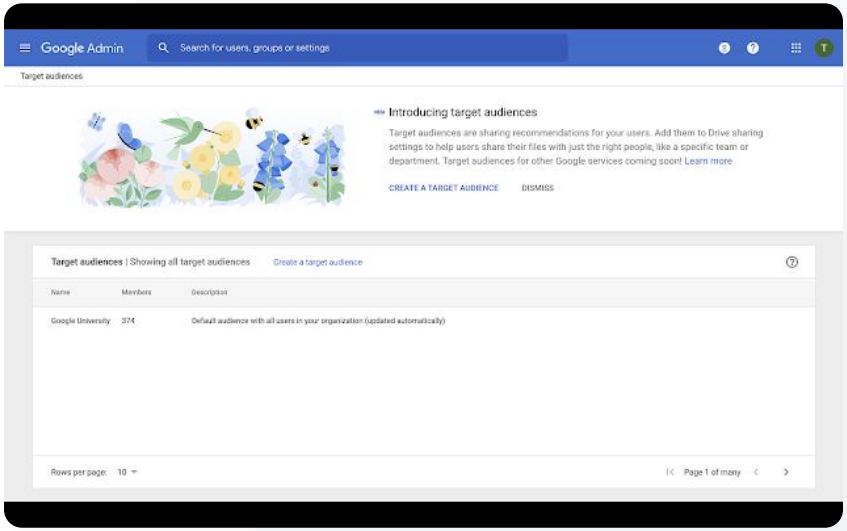
Istruzioni: creazione dei segmenti di pubblico per la condivisione interna dei file

Come funziona

Dopo aver creato un segmento di pubblico di destinazione, puoi aggiungere i membri e applicarlo a Google Drive per renderlo disponibile nelle impostazioni di condivisione degli utenti. Ad esempio, puoi consentire a un membro dello staff di vedere il segmento di pubblico di destinazione "Tutto lo staff" durante la condivisione di file di Drive.

Come attivare le etichette di Drive nell'istituto

- Accedi alla **Console di amministrazione** > Vai a **Menu** > **Directory** > Pubblico di destinazione
- Fai clic su **Crea segmento di pubblico di destinazione**
- Alla voce **Nome**, inserisci il nome del segmento di pubblico di destinazione
- Seleziona **Aggiungi membri** > Includi i membri che vuoi
- Fai clic su **Fine**



Documentazione pertinente del Centro assistenza

- Informazioni sui segmenti di pubblico di destinazione
- Best practice per l'implementazione di un pubblico di destinazione
- Creare un pubblico di destinazione

“Come posso impedire ai miei studenti di scuola secondaria di condividere documenti con gli studenti della scuola primaria?”

Limitazione della condivisione dei file

Le **regole di attendibilità di Drive** consentono agli amministratori di impostare regole per controllare chi può accedere ai file di Google Drive che aiutano a garantire la privacy dei dati dell'istituto. I criteri possono essere applicati a singoli utenti, gruppi, unità organizzative e domini.

- Proteggi le informazioni sensibili e mantieni la conformità con gli standard e le normative del settore
- Limita la condivisione interna o esterna al dominio: gli amministratori possono creare una regola di attendibilità per consentire agli studenti di condividere file di Drive solo all'interno dell'organizzazione
- Le "regole di attendibilità", una volta abilitate, sostituiscono le "Opzioni di condivisione" presenti nei controlli di amministrazione di Google Drive

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Creare e gestire le regole di attendibilità per la condivisione di Drive

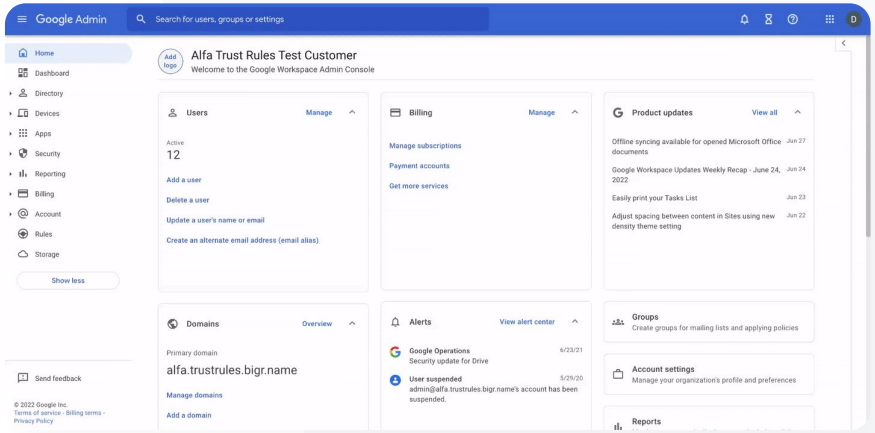
Istruzioni: limitazione della condivisione dei file

Attivare le regola di attendibilità di Drive

- Accedi alla **Console di amministrazione** > Vai a **Menu** > **Regole**
- Nella scheda **Collabora in sicurezza** nella parte superiore della pagina, fai clic su **Attiva le regole di attendibilità**
- Si apre automaticamente l'elenco Attività, che mostra lo stato di avanzamento dell'attivazione delle regole di attendibilità

Gli amministratori possono creare una regola di attendibilità, visualizzarne e modificarne i dettagli, eliminarla e visualizzarne gli eventi del log.

Visita il Centro assistenza per amministratori per istruzioni dettagliate sulla gestione delle regole di attendibilità



Documentazione pertinente del Centro assistenza

- Creare e gestire le regole di attendibilità per la condivisione di Drive

“Voglio limitare l'accesso a determinate app quando gli utenti si trovano nella rete.”

Limitazioni delle app di Google Workspace

Con l'**accesso sensibile al contesto**, puoi creare criteri di sicurezza per il controllo granulare degli accessi a **Google Workspace e alle app SAML (Security Assertion Markup Language) di terze parti** in base ad attributi come l'identità dell'utente, la località, lo stato della sicurezza del dispositivo e l'indirizzo IP. Puoi persino limitare l'accesso alle app dall'esterno della rete.

- Puoi applicare i criteri di accesso sensibile al contesto ai servizi principali di Google Workspace for Education
- Ad esempio, puoi limitare l'accesso alle app di Workspace dai dispositivi forniti dall'istituto o accedere a Drive solo se il dispositivo di archiviazione di un utente è criptato

Istruzioni passo passo

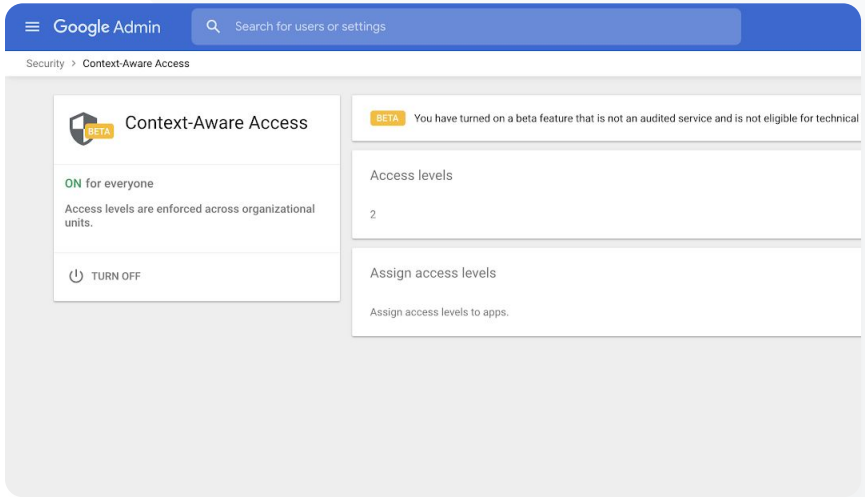
Documentazione pertinente del Centro assistenza

- Panoramica dell'accesso sensibile al contesto
- Assegnare i livelli di accesso sensibile al contesto alle app

Istruzioni: limitazione dell'utilizzo delle app di Google Workspace

Come utilizzare l'accesso sensibile al contesto

- Accedi alla **Console di amministrazione**
- Seleziona **Sicurezza** > **Accesso sensibile al contesto** > **Assegna**
- Seleziona **Assegna livelli di accesso** per visualizzare il tuo elenco di app
- Seleziona **un'unità organizzativa o un gruppo di configurazione** per ordinare l'elenco
- Seleziona **Assegna** in corrispondenza dell'app da modificare
- Seleziona uno o più livelli di accesso
- Crea più livelli se vuoi che gli utenti soddisfino più di una condizione
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Panoramica dell'accesso sensibile al contesto
- Assegnare i livelli di accesso sensibile al contesto alle app

“Voglio implementare un nuovo piano di gestione dell'archiviazione nel mio dominio.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Guida allo spazio di archiviazione per gli amministratori
- Comprendere la disponibilità e l'utilizzo dello spazio di archiviazione
- Liberare o acquistare altro spazio di archiviazione
- Impostare limiti

Gestione dello spazio di archiviazione nel dominio

Gli istituti che usano Google Workspace for Education dispongono di una base di 100 TB di spazio di archiviazione in pool, sufficiente per circa oltre 100 milioni di documenti, 8 milioni di presentazioni o 400.000 ore di video. **Gestisci lo spazio di archiviazione in pool di Drive** per fare in modo che l'istituto utilizzi lo spazio di archiviazione in modo efficace.

Utilizza gli strumenti di amministrazione, i report e i log per:

- Sapere quanto spazio di archiviazione è in uso
- Impostare limiti
- Individuare gli account che usano una quantità sproporzionata di spazio

Teaching and Learning Upgrade ed Education Plus offrono ulteriore spazio di archiviazione oltre a quello di base fornito

- Aggiungi 100 GB al pool condiviso per licenza con Teaching and Learning Upgrade
- Aggiungi 20 GB al pool condiviso per licenza con Education Plus

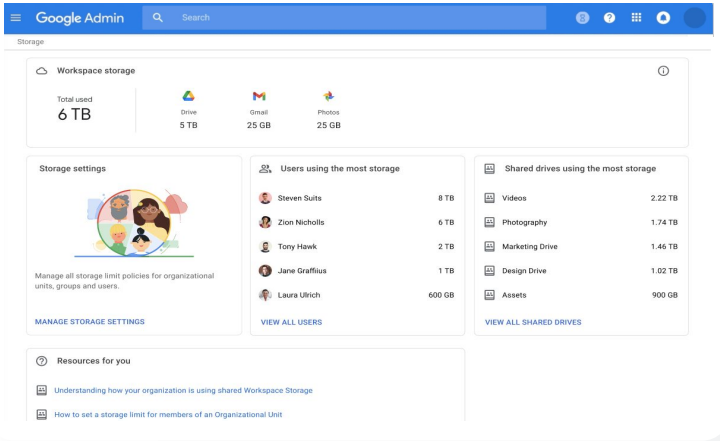
Istruzioni: gestione dello spazio di archiviazione nel dominio

Stabilire l'utilizzo dello spazio di archiviazione in base al singolo utente

- Accedi alla **Console di amministrazione** > Vai a **Menu** > **Spazio di archiviazione**
- Visualizza l'utilizzo dello spazio di archiviazione in base ad organizzazione e utente

Impostare limiti

- Nella **Console di amministrazione**, vai a **Menu** > **Spazio di archiviazione**
- Nella sezione **Impostazioni spazio di archiviazione**, fai clic su **Gestione**
- Fai clic su **Limite di spazio di archiviazione dell'utente** > Seleziona l'entità cui applicare il limite:
  - Unità organizzativa - Fai clic su quella che vuoi selezionare
  - Gruppo - Fai clic su **Gruppi** > Fai clic sul **campo della ricerca** > Inserisci il **nome del gruppo** > Fai clic sul **gruppo**
- Seleziona **On** e **imposta la quantità di spazio di archiviazione**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Guida allo spazio di archiviazione per gli amministratori
- Comprendere la disponibilità e l'utilizzo dello spazio di archiviazione
- Liberare o acquistare altro spazio di archiviazione
- Impostare limiti

Normative sui dati

In qualità di amministratore, puoi scegliere di archiviare i dati in una specifica area geografica (Stati Uniti o Europa/Regno Unito) utilizzando un **criterio per la regione di dati**.

- Gli utenti Education Plus ed Education Standard possono scegliere una regione di dati per alcuni utenti o regioni di dati diverse per reparti specifici e visualizzarne l'avanzamento degli spostamenti
- Inserisci gli utenti in un'unità organizzativa per applicare l'impostazione in base al reparto, oppure in un gruppo di configurazione per applicare l'impostazione a utenti che appartengono a uno o più reparti
- I criteri per le regioni di dati non si applicano agli utenti privi di una licenza Education Standard o Education Plus

“I dati degli studenti e del personale (docente e non docente) devono rimanere nell'Unione Europea per ottemperare alle normative.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Scegliere un’area geografica per i propri dati

“Le ricerche del corpo docente devono rimanere negli Stati Uniti per ottemperare a normative sulle sovvenzioni.”

Normative sulle sovvenzioni

In qualità di amministratore, puoi scegliere di archiviare le ricerche condotte dal tuo corpo docente in una specifica area geografica (Stati Uniti o Europa) utilizzando un **criterio per la regione di dati**.

- I criteri per le regioni di dati coprono i principali dati at-rest (inclusi i backup) per la maggior parte dei servizi principali di Google Workspace for Education, elencati qui
- Valuta i pro e contro prima di impostare un criterio per la regione di dati, in quanto gli utenti che si trovano al di fuori dell'area geografica in cui sono ospitati i loro dati potrebbero riscontrare una latenza maggiore in determinate circostanze

Istruzioni passo passo

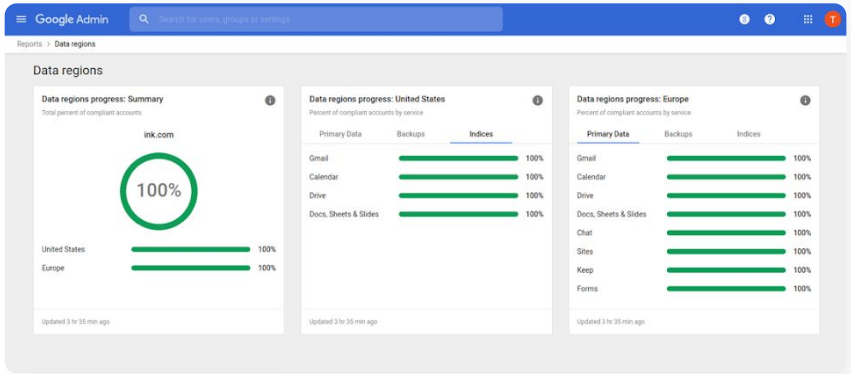
Documentazione pertinente del Centro assistenza

- Scegliere un'area geografica per i propri dati

Istruzioni: normative sui dati

Come definire le regioni di dati

- Accedi alla **Console di amministrazione**
  - Nota: è necessario effettuare l'accesso come super amministratore
- Fai clic su **Profilo aziendale** > **Mostra di più** > **Regioni di dati**
- Seleziona **l'unità organizzativa o il gruppo di configurazione** che vuoi limitare a una regione oppure seleziona l'intera colonna per includere tutte le unità e tutti i gruppi
- Seleziona la tua regione, scegliendo un'opzione tra **Nessuna preferenza, Stati Uniti, Europa**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Scegliere un'area geografica per i propri dati

Gestione dei dispositivi endpoint

Utilizzare la **gestione degli endpoint aziendali** è un modo per avere più controllo sui dati dell'organizzazione tramite i dispositivi mobili. Puoi limitare le funzionalità dei dispositivi mobili, richiedere la crittografia dei dispositivi, gestire le app sui dispositivi Android oppure su iPhone e iPad e persino cancellare i dati da un dispositivo.

- Puoi approvare, bloccare, sbloccare o eliminare dei dispositivi dalla Console di amministrazione
- Se un utente smarrisce un dispositivo o lascia la scuola, puoi cancellare il suo account, il suo profilo o addirittura tutti i dati da quel determinato dispositivo gestito. Questi dati rimarranno comunque disponibili da computer o browser web

> “Ho bisogno di un modo per gestire tutti i tipi di dispositivi in uso nel distretto (iOS, Windows 10 ecc.), non solo i Chromebook, e inviare loro i criteri, soprattutto nel caso in cui uno sia stato compromesso.”

Istruzioni passo passo

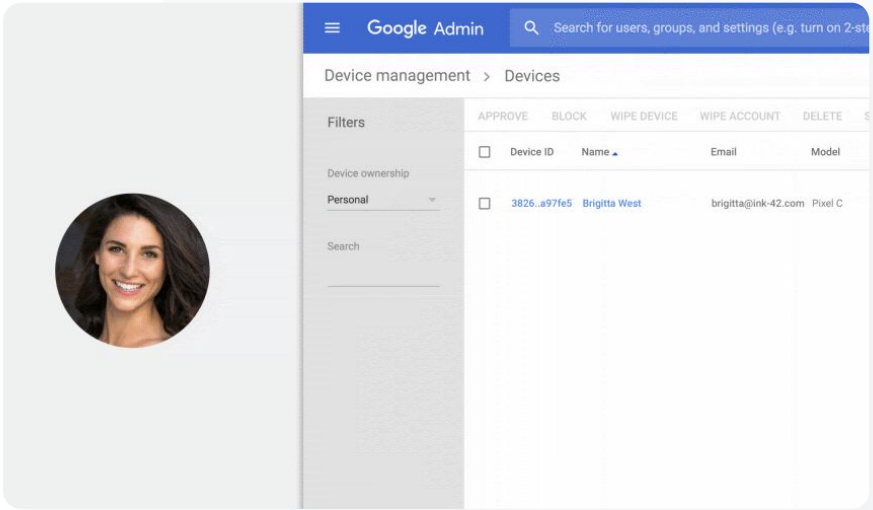
Documentazione pertinente del Centro assistenza

- Gestire i dispositivi con la Gestione degli endpoint Google
- Configurare la gestione avanzata dei dispositivi mobili

Istruzioni: gestione dei dispositivi endpoint

Come attivare gestione dei dispositivi mobili avanzata

- Accedi alla **Console di amministrazione**
- Dalla **Console di amministrazione** > **Dispositivi** > **Dispositivi mobili ed endpoint**
- A sinistra, fai clic su **Impostazioni** > **Impostazioni universali**
- Fai clic su **Generali** > **Gestione dispositivi mobili**
- Per applicare l'impostazione a tutti, lascia selezionata l'unità organizzativa di primo livello, altrimenti seleziona un'unità organizzativa secondaria
- Seleziona **Avanzata**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Gestire i dispositivi con la Gestione degli endpoint Google
- Configurare la gestione avanzata dei dispositivi mobili

“Alcuni miei docenti usano dispositivi dotati di Windows 10. Come faccio a gestire in modo centralizzato tutti i dispositivi del mio istituto?”

Gestione dei dispositivi Microsoft Windows

Gestisci e proteggi i dispositivi Windows 10 del tuo istituto tramite la Console di amministrazione, proprio come fai per i dispositivi Android, iOS, Chrome e Jamboard.

- Abilita il Single Sign-On in modo che gli utenti possano accedere più facilmente a Google Workspace sui dispositivi Windows 10
- Assicurati che i dispositivi utilizzati per accedere a Google Workspace siano aggiornati, protetti e adeguati agli standard di conformità, grazie alla gestione dei dispositivi nella Console di amministrazione
- Cancella i dati, esegui il push degli aggiornamenti della configurazione ed esegui altre operazioni sui dispositivi Windows 10 dal cloud

Istruzioni passo passo

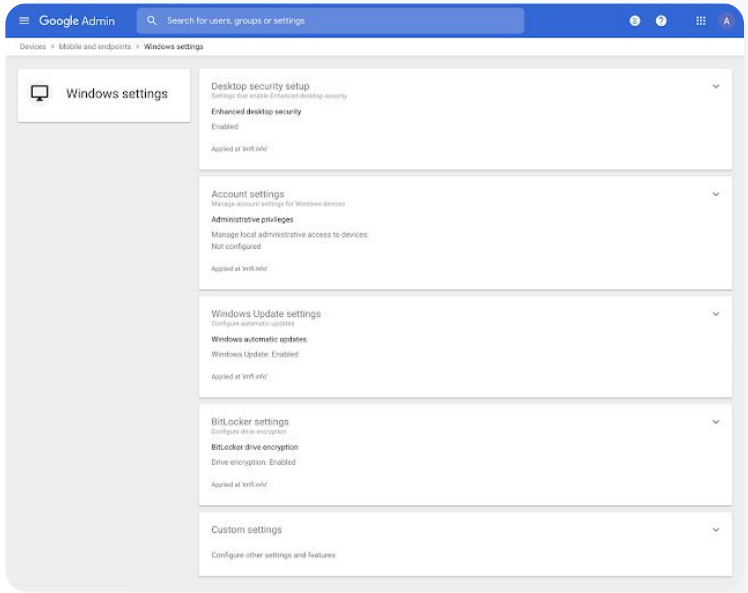
Documentazione pertinente del Centro assistenza

- Attivare la gestione dei dispositivi Windows
- Registrare un dispositivo nella gestione dei dispositivi Windows

Istruzioni: gestione dei dispositivi Microsoft Windows

Attivare la gestione dei dispositivi Windows

- Nella **Console di amministrazione**, vai a **Menu** > **Dispositivi** > **Dispositivi mobili ed endpoint** > **Impostazioni** > **Impostazioni di Windows**
- Seleziona **Configurazione di Gestione Windows**
- Per applicare l'impostazione a tutti, lascia selezionata l'unità organizzativa di primo livello
- Accanto a **Gestione dei dispositivi Windows**, seleziona **Abilitata**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Attivare la gestione dei dispositivi Windows
- Registrare un dispositivo nella gestione dei dispositivi Windows

Come si configurano i profili Wi-Fi sui miei dispositivi Windows 10?”

Impostazioni personalizzate per i dispositivi Windows 10

Utilizzando la gestione dei dispositivi Windows di Google, gli amministratori possono aggiungere impostazioni personalizzate al parco di dispositivi.

- Gestisci le impostazioni personalizzate del dispositivo dalla Console di amministrazione
- Applica le impostazioni a:
  - Gestione dispositivi
  - Sicurezza
  - Hardware e rete
  - Software
  - Privacy

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

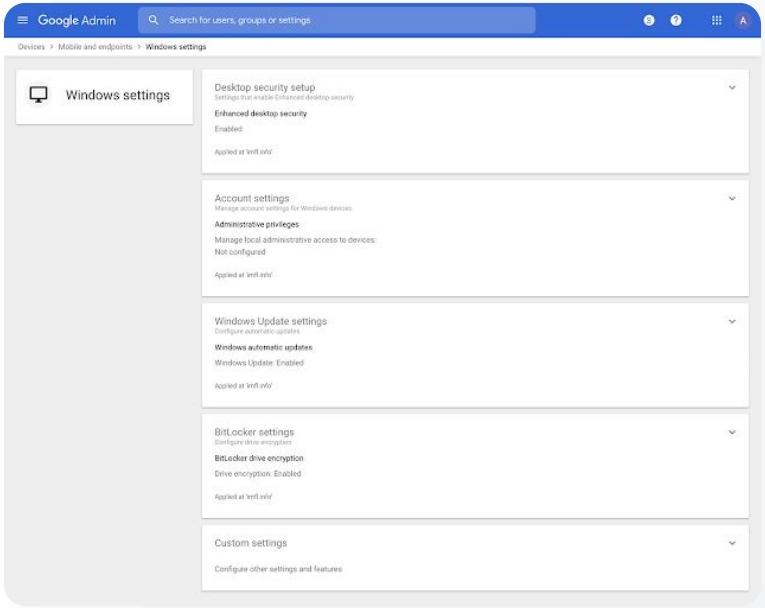
- Impostazioni personalizzate comuni
- Aggiungere impostazioni personalizzate

Istruzioni: impostazioni personalizzate per i dispositivi Windows 10

Aggiungere una nuova impostazione personalizzata

- Nella **Console di amministrazione**, vai a **Menu** > **Dispositivi** > **Dispositivi mobili ed endpoint** > **Impostazioni** > **Impostazioni di Windows**
- Seleziona **Impostazioni personalizzate**
- Fai clic su **Aggiungi un'impostazione personalizzata** > Compila i campi richiesti
- Fai clic su **Avanti**
- Scegli l'**unità organizzativa** cui applicare le impostazioni
- Fai clic su **Applica**

Tieni presente che Google non fornisce assistenza tecnica e né è responsabile per prodotti o impostazioni di terze parti.



Documentazione pertinente del Centro assistenza

- Impostazioni personalizzate comuni
- Aggiungere impostazioni personalizzate

“Voglio assicurarmi che il mio parco di dispositivi Windows 10 riceva gli aggiornamenti più recenti.”

Automazione degli aggiornamenti dei dispositivi Windows 10

Stabilisci come e quando i dispositivi Windows 10 del tuo istituto riceveranno gli aggiornamenti della sicurezza e altri importanti download tramite il servizio di aggiornamento automatico di Windows.

- Imposta notifiche per scaricare gli aggiornamenti dal pannello di controllo di Windows Update, imposta gli orari in cui non pianificare i riavvii degli aggiornamenti e molto altro
- Applica le impostazioni all'intero istituto o a unità organizzative specifiche
- Le modifiche possono richiedere fino a 24 ore, ma in genere sono più rapide

Istruzioni passo passo

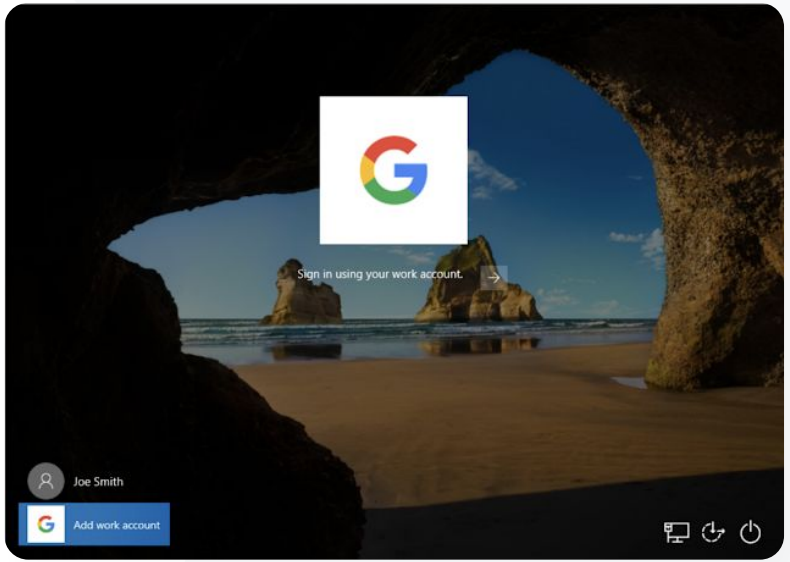
Documentazione pertinente del Centro assistenza

- Gestire gli aggiornamenti automatici

Istruzioni: automazione degli aggiornamenti dei dispositivi Windows 10

Configurare gli aggiornamenti

- Nella **Console di amministrazione**, vai a **Menu** > **Dispositivi** > **Dispositivi mobili ed endpoint** > **Impostazioni** > **Impostazioni di Windows**
- Seleziona **Impostazioni di Windows Update** > **Abilitate**
- Accanto a **Gestione dei dispositivi Windows**, seleziona **Abilitata**
- Configura le seguenti opzioni, tra le altre:
  - Accetta gli aggiornamenti per le applicazioni Microsoft
  - Comportamento aggiornamenti automatici
  - Automazione della frequenza di aggiornamento
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Gestire gli aggiornamenti automatici

“So che Google rispetta gli standard più elevati per quanto riguarda la crittografia dei dati, ma voglio gestire le chiavi di crittografia per la proprietà intellettuale della nostra università e finanziare la ricerca.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Informazioni sulla crittografia lato client

Utilizzo della crittografia lato client

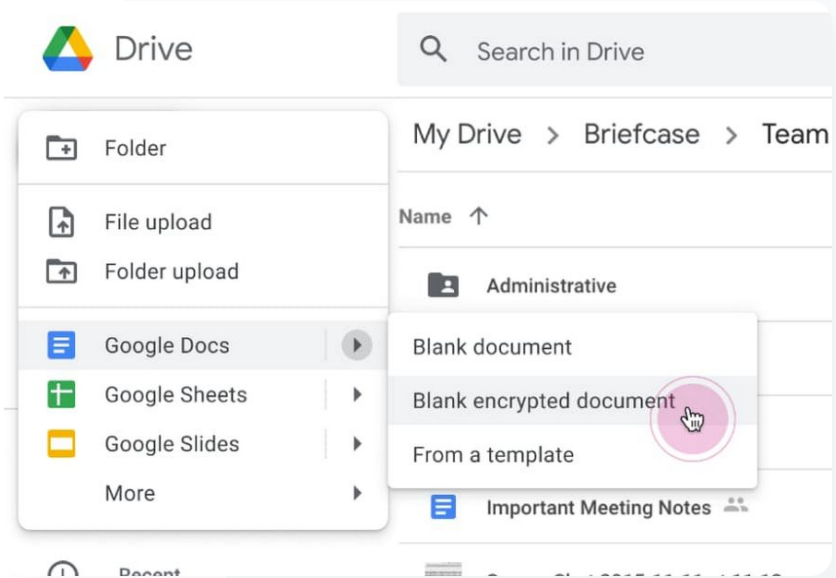
Google Workspace utilizza già i più recenti standard crittografici per criptare tutti i dati at-rest e in transito tra le proprie strutture. Con la **crittografia lato client**, gli amministratori hanno il controllo diretto delle chiavi di crittografia e del provider di identità utilizzato per accedere alle chiavi.

- Usa le tue chiavi di crittografia per crittografare i dati sensibili, come la proprietà intellettuale del tuo istituto
- La crittografia dei contenuti viene gestita nel browser prima che i dati siano trasmessi o salvati nello spazio di archiviazione basato su cloud di Google
- Scegli quali utenti possono creare contenuti criptati sul lato client e condividerli internamente o esternamente

Istruzioni: utilizzo della crittografia lato client

Configurare la crittografia lato client

- Configura il servizio chiavi di crittografia
  - Proteggi i tuoi dati con funzionalità di gestione e controllo delle chiavi creando il tuo servizio chiavi
- Connetti Google Workspace al tuo servizio chiavi esterno
  - Aggiungi e gestisci i servizi chiavi per la crittografia lato client includendo l'URL del servizio chiavi nella Console di amministrazione
- Assegna il servizio chiavi a unità organizzative o gruppi
  - Assegna un servizio chiavi come predefinito per l'intero istituto
- Connetti Google Workspace al tuo provider di identità
  - Stabilisci la connessione al tuo provider di identità per la crittografia lato client al fine di verificare l'identità degli utenti prima di consentire loro di criptare contenuti o di accedervi
- Attiva la crittografia lato client per gli utenti
  - Attiva la crittografia lato client per abilitare le unità organizzative o i gruppi per gli utenti che devono creare contenuti crittografati lato client

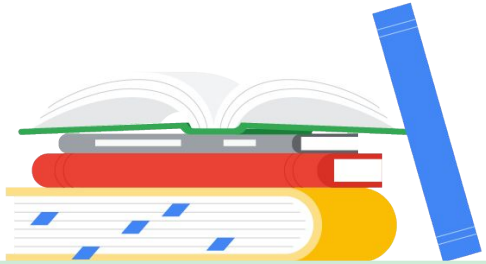


Documentazione pertinente del Centro assistenza

- Informazioni sulla crittografia lato client

Funzionalità di insegnamento e apprendimento

Permetti ai docenti di accedere a funzionalità aggiuntive nel tuo ambiente di apprendimento digitale. Potranno così usufruire di esperienze in classe più significative, strumenti a sostegno dell'integrità accademica e comunicazione video avanzata.

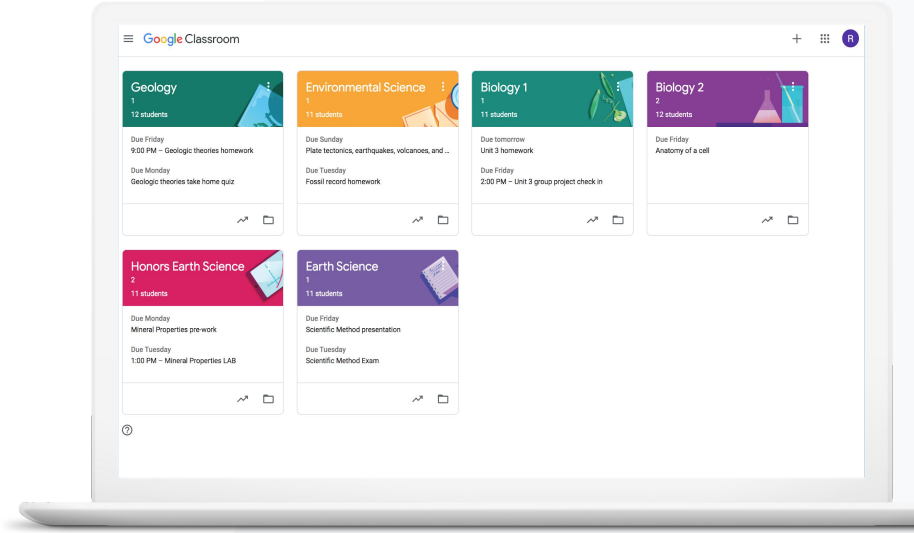


- Google Classroom
- Report sull'originalità
- Documenti, Fogli e Presentazioni
- Google Meet

Google Classroom

Di cosa si tratta?

Google Classroom è il punto di riferimento centralizzato per l'insegnamento e l'apprendimento. Le funzionalità a pagamento di Classroom aiutano a riunire gli strumenti della classe in un unico posto. I docenti possono accedere ai loro strumenti preferiti direttamente in Classroom e mantenere gli elenchi dei corsi sincronizzati con i sistemi esterni.



Casi d'uso

Gestione dell'accesso ai componenti aggiuntivi di Classroom	Istruzioni passo passo
Integrazione di contenuti coinvolgenti in Classroom	Istruzioni passo passo
Creazione di corsi su vasta scala	Istruzioni passo passo

> Vorrei che ci fosse un modo per fornire accesso Single Sign-On agli strumenti di tecnologia educativa preferiti dai miei insegnanti. ”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Gestire le app del Google Workspace Marketplace
- Utilizzare componenti aggiuntivi in Classroom
- Gestire le app del Marketplace inserite nella lista consentita
- Distribuire un'app del Marketplace agli utenti
- Componenti aggiuntivi di Classroom: guida introduttiva per gli amministratori

Gestione dell'accesso ai componenti aggiuntivi di Classroom

Stabilisci a quali app didattiche di terze parti può accedere il tuo istituto con una **lista consentita di domini**. Consenti agli insegnanti di installare facilmente i componenti aggiuntivi e di includerli nei compiti degli studenti in pochi clic.

- Crea una lista consentita nel tuo dominio per stabilire quali app di terze parti possono essere installate dai docenti tramite Google Workspace Marketplace
- Sostieni i risultati didattici con app educative supplementari. Gli insegnanti possono assegnare, rivedere e valutare i compiti direttamente all'interno di Google Classroom
- Google Workspace Marketplace comprende diversi componenti aggiuntivi

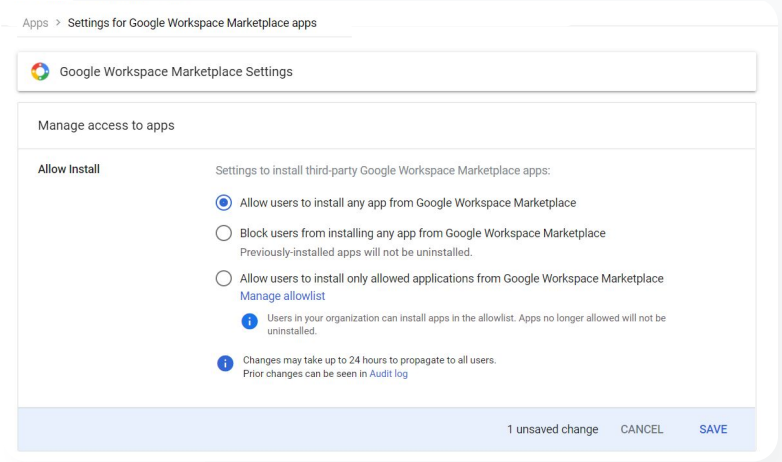
Istruzioni: gestione dell'accesso ai componenti aggiuntivi di Classroom

Gestire l'accesso ai componenti aggiuntivi con una lista consentita del dominio

- Nella Console di amministrazione, seleziona **Menu** > App di Google Workspace Marketplace > **Elenco di app**
- Seleziona **Includi app nella lista consentita**
- Inserisci il nome del tuo componente aggiuntivo desiderato o cercalo
- Fai clic su **Seleziona** e assicurati che l'opzione **Consenti agli utenti di installare questa app** sia selezionata
- Fai clic su **Continua** e **Fine**

Concedere accesso ai componenti aggiuntivi alla lista consentita desiderata

- Nella Console di amministrazione, seleziona **Menu** > App di Google Workspace Marketplace > **Elenco di app**
- Selezionare il componente aggiuntivo da distribuire
- Alla voce **Accesso utenti**, fai clic su **Visualizza unità organizzative e gruppi**
- Scegli **Disponibile per tutti** oppure limita l'accesso a **gruppi selezionati** o **unità organizzative**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Gestire le app del Google Workspace Marketplace
- Utilizzare componenti aggiuntivi in Classroom
- Gestire le app del Marketplace inserite nella lista consentita
- Distribuire un'app del Marketplace agli utenti
- Componenti aggiuntivi di Classroom: guide introduttive per gli amministratori

“Voglio assegnare e valutare un gioco educativo ai miei studenti senza uscire da Google Classroom.”

Integrazione di contenuti coinvolgenti in Classroom

Con i **componenti aggiuntivi di Classroom**, gli insegnanti possono condividere attività e contenuti coinvolgenti con la classe allegando componenti aggiuntivi a compiti, domande, materiali o annunci all'interno di Classroom.

- Consenti a insegnanti e studenti di usare i loro strumenti preferiti
- Grazie ai componenti aggiuntivi, non serve costringere gli studenti a gestire più password o visitare siti web esterni
- Rivedi e valuta i lavori degli studenti dai componenti aggiuntivi, direttamente all'interno di Classroom

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Utilizzare componenti aggiuntivi in Classroom
- Componenti aggiuntivi di Classroom: guida introduttiva per i docenti

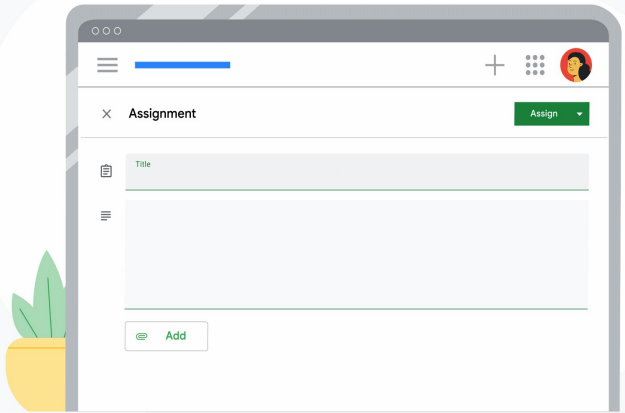
Istruzioni: integrazione di contenuti coinvolgenti in Classroom

Come allegare componenti aggiuntivi a un compito, un quiz o una domanda

- Accedi al tuo account Classroom alla pagina **classroom.google.com**
- Dopo aver selezionato il corso pertinente dall'elenco, scegli **Lavori del corso**
- Seleziona **Crea** > Scegli cosa vuoi creare
- Inserisci il titolo e le istruzioni
- In **Componenti aggiuntivi**, scegli quello da utilizzare
- Seleziona **Assegna**

Come allegare i componenti aggiuntivi a un annuncio

- All'interno della pagina **Stream** del corso, seleziona **Pubblica un annuncio per il tuo corso**
- Inserisci l'annuncio
- In **Componenti aggiuntivi**, scegli quello da utilizzare
- Seleziona **Pubblica**



Documentazione pertinente del Centro assistenza

- Utilizzare componenti aggiuntivi in Classroom
- Componenti aggiuntivi di Classroom: guide introduttive per i docenti

“

Ho bisogno di un modo per automatizzare la configurazione dei corsi e gestire gli elenchi degli studenti in Google Classroom.”

Creazione di corsi su vasta scala

L'importazione dell'elenco degli studenti del SIS consente la creazione automatica dei corsi e, grazie a Clever, tiene gli elenchi dei corsi sincronizzati con il sistema informatico per gli studenti (SIS) della tua scuola.

- È disponibile per i distretti di istruzione primaria e secondaria negli Stati Uniti e in Canada che usano Education Plus
- Gli amministratori possono importare gli elenchi dei corsi dal SIS in Google Classroom per configurare automaticamente i corsi
- Automatizza e gestisci senza problemi gli elenchi di corsi in Google Classroom

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Iniziare a utilizzare l'importazione dell'elenco degli studenti del SIS
- Configurare l'importazione dell'elenco degli studenti del SIS tramite Clever

Istruzioni: creazione di corsi su vasta scala

Come configurare l'importazione dell'elenco degli studenti del SIS

- Configura la sincronizzazione dell'elenco degli studenti di Google Classroom con Clever
- L'amministratore del tuo distretto su Clever e il super amministratore di Google Workspace possono seguire le istruzioni dettagliate di Clever

Se il tuo distretto non dispone di un account Clever:

- Crea un account Clever

Se invece il tuo distretto dispone di un account Clever:

- Richiedi l'importazione dell'elenco degli studenti all'interno della dashboard di Clever

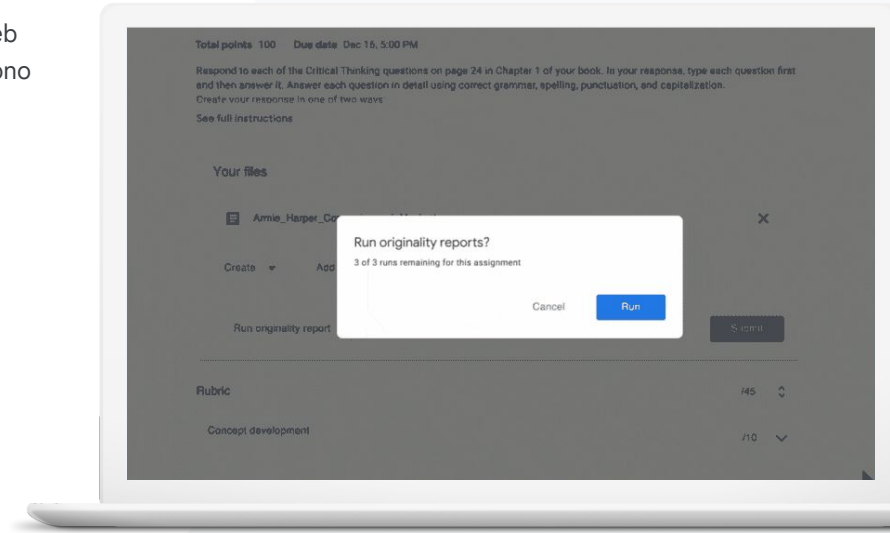
Documentazione pertinente del Centro assistenza

- Configurare l'importazione dell'elenco degli studenti del SIS tramite Clever

Report sull'originalità

Di cosa si tratta?

I report sull'originalità consentono a docenti e studenti di verificare l'autenticità del lavoro utilizzando la Ricerca Google per confrontare i compiti con miliardi di pagine web e oltre 40 milioni di libri. Le funzionalità a pagamento dei report sull'originalità forniscono un accesso illimitato grazie al quale i docenti possono analizzare i contributi degli studenti rispetto a un archivio di proprietà della scuola dei lavori precedenti.



Casi d'uso

Analisi per rilevare casi di plagio con i report sull'originalità	Istruzioni passo passo
Verifica dell'originalità sulla base dei precedenti lavori degli studenti	Istruzioni passo passo
Rilevamento dei casi di plagio come opportunità di apprendimento	Istruzioni passo passo

“Voglio controllare i lavori dei miei studenti per individuare eventuali plagi o citazioni scorrette.”

Analisi per rilevare casi di plagio con i report sull'originalità

Gli insegnanti possono verificare l'autenticità dei lavori consegnati dai propri studenti utilizzando i **report sull'originalità**. Il report fornisce link alle fonti rilevate e segnala le eventuali citazioni omesse.

- Esegui report sull'originalità rispetto a Documenti, Presentazioni e documenti di Microsoft Word.
- I docenti che usano Teaching and Learning Upgrade o Education Plus ottengono:
  - Accesso illimitato ai report sull'originalità
  - Confronto delle corrispondenze tra studenti con un archivio scolastico dei lavori consegnati in precedenza

I dati restano di tua proprietà: è nostra responsabilità proteggerli e mantenerli privati.

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Attivare i report sull'originalità
- Report sull'originalità e privacy

Istruzioni: analisi per rilevare casi di plagio con i report sull'originalità

Attivare i report sull'originalità per un compito in Classroom

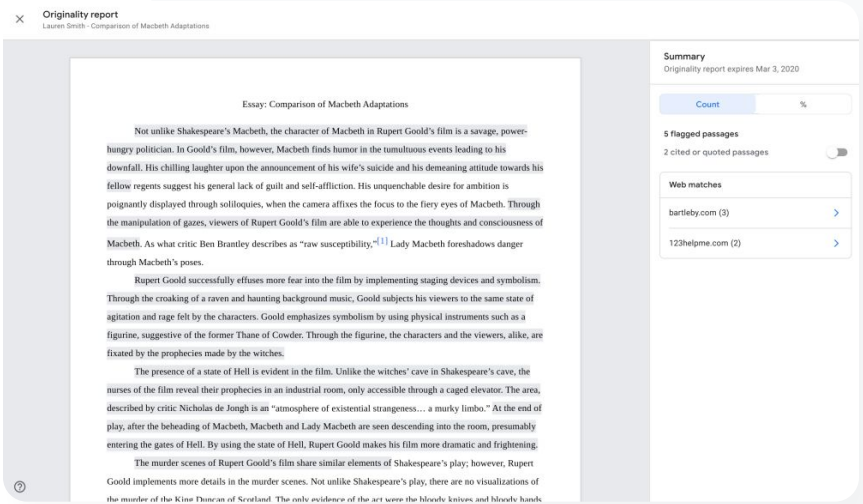
- Accedi al tuo account Classroom alla pagina **classroom.google.com**
- Dopo aver selezionato il corso pertinente dall'elenco, scegli **Lavori del corso**
- Seleziona **Crea** > **Compito**
- Seleziona la casella accanto a **Report sull'originalità** per attivare la funzionalità

Eseguire un report sull'originalità relativo al lavoro dello studente

- Seleziona il file pertinente dello studente dall'elenco e fai clic sul file per aprirlo nello strumento di valutazione
- Sotto il compito dello studente, fai clic su **Esegui controllo anti-plagio (originalità)**

Attivare i report sull'originalità per un compito all'interno dell'SGA

- Accedi al tuo **sistema di gestione dell'apprendimento (SGA)**
- Seleziona il **corso** pertinente
- Crea un compito > Seleziona **Google Compiti**
- Seleziona la casella **Abilita i rapporti sull'originalità**



Documentazione pertinente del Centro assistenza

- Classroom: Attivare i report sull'originalità
- Google Compiti: Attivare i report sull'originalità

“Come posso consentire agli insegnanti di confrontare il lavoro di uno studente con quello degli studenti degli anni passati per rilevare plagi?”

Verifica dell'originalità sulla base dei precedenti lavori degli studenti

Le corrispondenze in documenti della scuola dei report sull'originalità consentono ai docenti di confrontare il lavoro dello studente con i compiti consegnati in passato analizzandolo rispetto all'archivio privato dei compiti dell'istituto.

- Confronta le corrispondenze tra studenti con i lavori attuali e consegnati in precedenza da altri alunni per rilevare casi di plagio, grazie a Teaching and Learning Upgrade o Education Plus
- Il lavoro dello studente può essere archiviato in modo sicuro e integrato nel corpus privato di proprietà della scuola a livello di dominio

Istruzioni passo passo

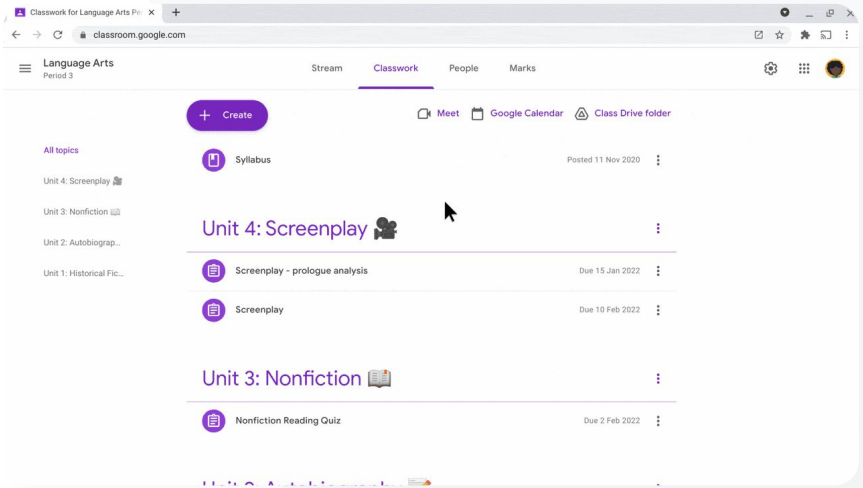
Documentazione pertinente del Centro assistenza

- Attivare i report sull'originalità
- Attivare le corrispondenze in documenti della scuola per i report sull'originalità in Classroom

Istruzioni: verifica dell'originalità sulla base dei precedenti lavori degli studenti

Come attivare le corrispondenze in documenti della scuola per i report sull'originalità

- Nella Console di amministrazione, seleziona **Menu** > **App** > **Servizi Google aggiuntivi** > **Classroom**
- Seleziona l'**unità organizzativa del docente**
- Fai clic su **Report sull'originalità** > Seleziona la casella **Abilita le corrispondenze in documenti della scuola nei report sull'originalità**
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Attivare le corrispondenze in documenti della scuola per i report sull'originalità in Classroom

“Voglio offrire ai miei studenti un'opportunità per apprendere come citare correttamente le loro fonti.”

Rilevamento dei casi di plagio come opportunità di apprendimento

Gli studenti hanno la possibilità di identificare i contenuti privi di citazioni e i plagi non intenzionali prima di consegnare il proprio lavoro eseguendo fino a tre **report sull'originalità** per compito. I report sull'originalità mettono a confronto il lavoro degli studenti con svariate fonti e segnalano il testo sprovvisto di citazioni. In questo modo, gli studenti hanno l'opportunità di imparare, correggere gli errori e consegnare i propri compiti senza preoccupazioni.

- Nelle versioni Teaching and Learning Upgrade ed Education Plus, i docenti possono usare i report sull'originalità tutte le volte che vogliono, mentre Education Fundamentals dà loro la possibilità di attivare questa funzionalità per un massimo di cinque volte per corso
- Alla consegna di un lavoro, Classroom esegue automaticamente un report visualizzabile solo dall'insegnante. Se si annulla la consegna di un compito e poi lo si invia di nuovo, Classroom esegue un altro report sull'originalità per l'insegnante

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

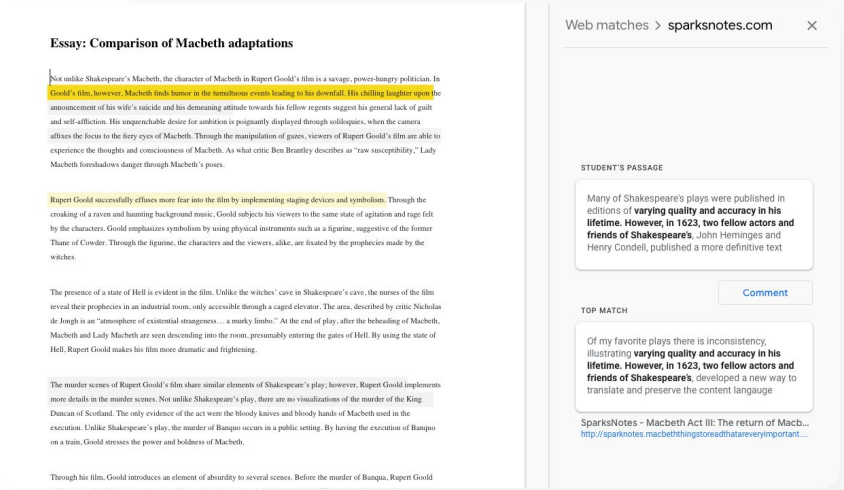
- Eseguire un report sull'originalità relativo al proprio lavoro

Istruzioni: rilevamento dei casi di plagio come opportunità di apprendimento

Come gli studenti possono eseguire un report sull'originalità in Classroom

- Accedi al tuo account Classroom alla pagina classroom.google.com
- Dopo aver selezionato il corso pertinente dall'elenco, scegli **Lavori del corso**
- Seleziona il compito pertinente dall'elenco e fai clic su **Visualizza compito**
- In **Il tuo lavoro**, seleziona **Carica** o **Crea il file**
- Accanto a **Report sull'originalità**, fai clic su **Esegui**
- Per aprire il report, fai clic su **Visualizza report sull'originalità** sotto il nome del file del compito
- Per rivedere il compito al fine di riscrivere o citare correttamente i passaggi segnalati, fai clic su **Modifica** in basso

Gli studenti possono eseguire report sull'originalità all'interno dell'SGA usando Google Compiti



Documentazione pertinente del Centro assistenza

- Eseguire un report sull'originalità in Classroom
- Eseguire un report sull'originalità nell'SGA

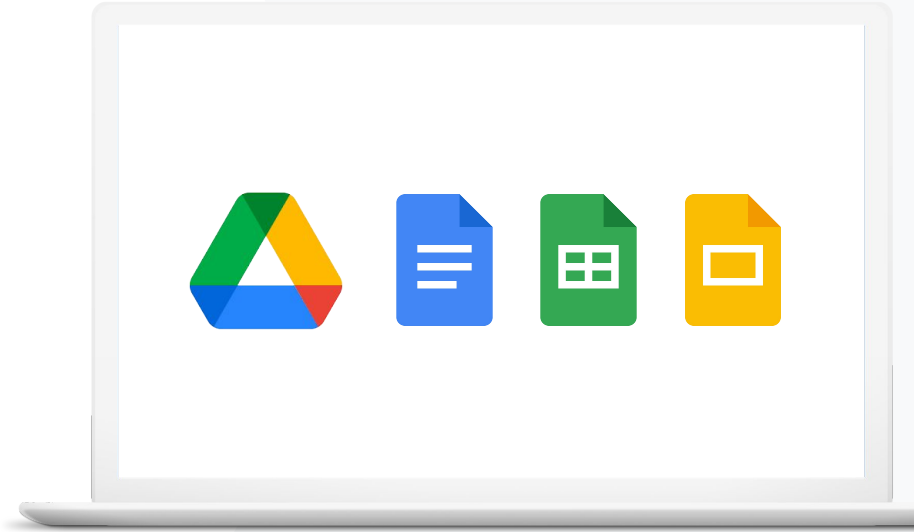
Documenti, Fogli e Presentazioni

Di cosa si tratta?

Documenti, Fogli e Presentazioni consentono alle comunità scolastiche di collaborare, creare, esaminare e modificare contemporaneamente in tempo reale. Le funzionalità a pagamento in Education Plus consentono a docenti e amministratori di istituire un processo di approvazione per la documentazione interna in tutto l'istituto.

Casi d'uso

Approvazione della documentazione interna — Istruzioni passo passo



Il dipartimento di scienze sta preparando un nuovo programma.

Come possono far sì che la loro proposta sia approvata da tutti i capi di dipartimento?”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Gestire le approvazioni

Approvazione della documentazione interna

Grazie alle **Approvazioni**, la comunità scolastica può inviare documenti su Google Drive per sottoporli a un processo di approvazione formale.

- I revisori possono approvare o rifiutare i documenti oppure lasciare un feedback al loro interno, il tutto direttamente da Drive, Documenti e altre app di Google Workspace
- Gli approvatori possono rivedere i contenuti seguendo il link al documento, lasciare commenti e rifiutarlo o approvarlo
- Gestisci l'approvazione di un contratto o una nuova assunzione, delle modifiche a un documento prima della pubblicazione e altro

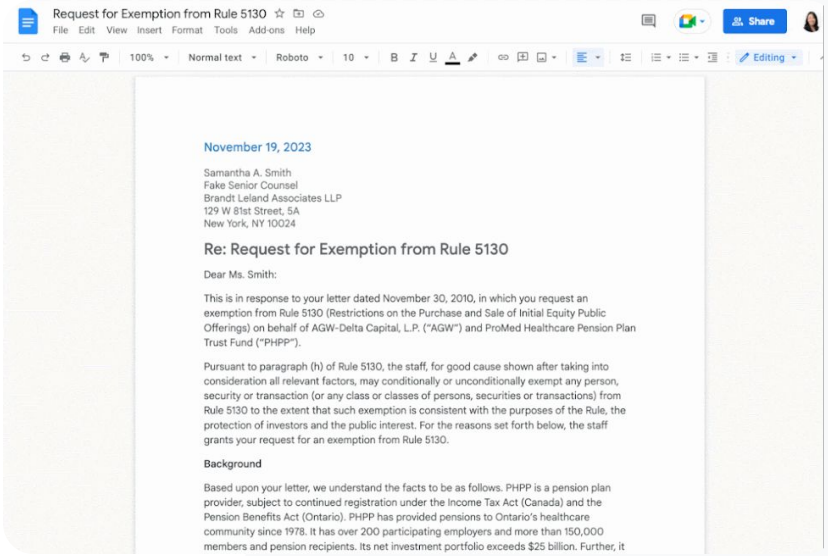
Istruzioni: approvazione della documentazione interna

Come funziona

Gli amministratori possono gestire la modalità in cui utenti e file prendono parte al processo di approvazione.

Come gestire le approvazioni

- Accedi alla **Console di amministrazione** > Vai a **Menu** > **App** > **Google Workspace** > **Drive e Documenti**
- Fai clic su **Approvazioni**
- Per applicare l'impostazione a tutti, seleziona un'**unità organizzativa** o un **gruppo di configurazione** secondari
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Gestire le approvazioni

Google Meet

Di cosa si tratta?

Le funzionalità avanzate di Google Meet includono live streaming, gruppi di lavoro, riunioni con un numero maggiore di partecipanti, registrazione delle riunioni, sottotitoli codificati con traduzione dal vivo e altro.

Casi d'uso

Registrazione delle riunioni	Istruzioni passo passo	Possibilità di fare domande	Istruzioni passo passo
Consultazione di quanto discusso in classe	Istruzioni passo passo	Raccolta di opinioni	Istruzioni passo passo
Eliminazione delle barriere linguistiche	Istruzioni passo passo	Piccoli gruppi di studenti	Istruzioni passo passo
Trasmissione di assemblee, riunioni ed eventi scolastici	Istruzioni passo passo	Monitoraggio delle partecipazioni	Istruzioni passo passo

“Il nostro istituto offre grandi corsi di sviluppo professionale online che dobbiamo registrare per i docenti che non possono essere presenti.”

Registrazione delle riunioni

Con Teaching and Learning Upgrade e Education Plus, i docenti possono registrare lezioni, riunioni di docenti, corsi di sviluppo professionale e altro ancora. Le riunioni vengono salvate automaticamente su Drive.

- Le registrazioni vengono salvate nel Drive dell'organizzatore della riunione. Prima di registrare, accertati che ci sia spazio a sufficienza sul tuo Drive
- È consigliabile che gli amministratori IT abilitino la registrazione solo per il personale docente e amministrativo

Istruzioni passo passo

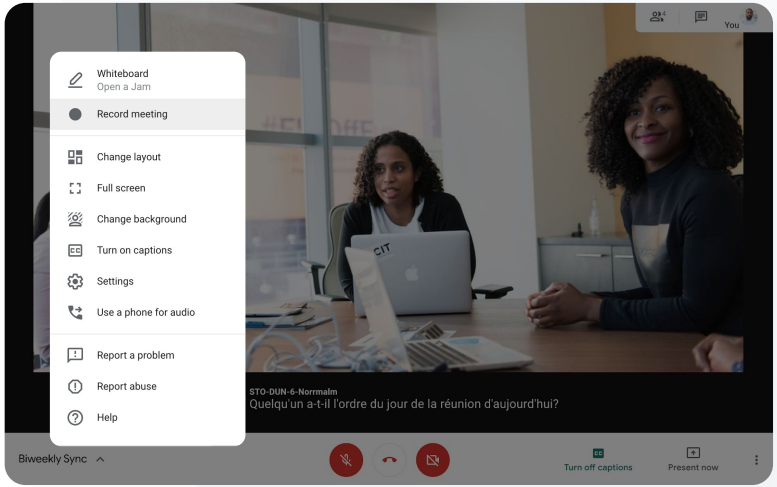
Documentazione pertinente del Centro assistenza

Registrare una riunione video

Istruzioni: registrazione delle riunioni

Come avviare una registrazione

- Avvia o partecipa a una riunione in **Google Meet**
- Fai clic su **Attività** > **Registrazione**
- Seleziona **Avvia registrazione**
- Nella finestra che si apre, fai clic su **Avvia**
- Nell'angolo in alto a sinistra dello schermo apparirà un punto rosso a indicare che è in corso la registrazione della riunione
- Un file con il video della riunione verrà salvato automaticamente nel tuo Drive



Documentazione pertinente del Centro assistenza

- Registrare una riunione video

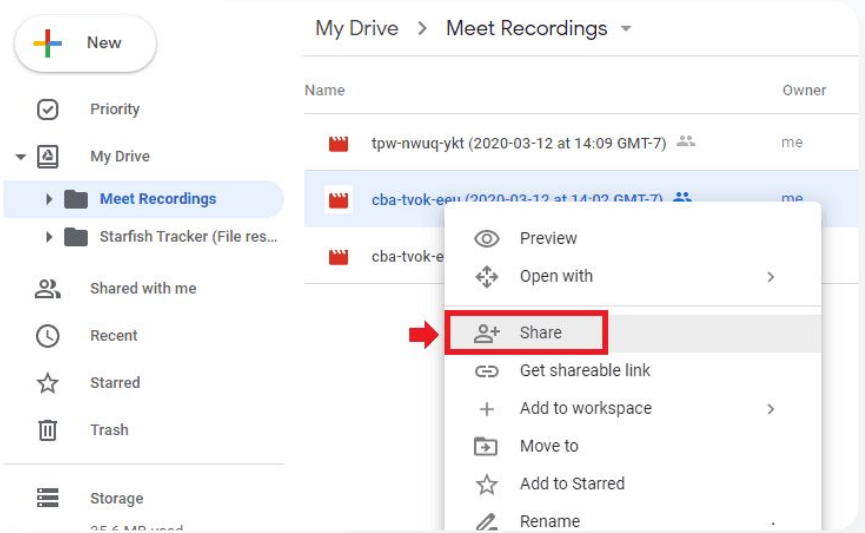
Istruzioni: visualizzazione e condivisione delle registrazioni

Come avviare una registrazione

- Seleziona il file
- Fai clic sull'icona di **condivisione**
- **Aggiungi i** visualizzatori approvati

Oppure

- Seleziona l'icona del **link**
- **Incolla** il link in un'email o in un messaggio di chat



Come scaricare una registrazione

- Seleziona il file
- Fai clic sull'icona **Altro** > Scarica
- **Fai doppio clic** sul file scaricato per riprodurlo

Come riprodurre la registrazione da Drive

- In Drive, fai doppio clic sul file della registrazione per riprodurla; finché il file non è pronto per essere guardato online, viene visualizzato il messaggio "Elaborazione ancora in corso"
- Per aggiungere una registrazione al tuo Drive, seleziona il file e fai clic su **Aggiungi a Il mio Drive**

Documentazione pertinente del Centro assistenza

- Registrare una riunione video

“Come faccio a trascrivere un corso virtuale affinché gli studenti possano consultarne il contenuto in un secondo momento?”

Consultazione di quanto discusso in classe

Con le trascrizioni delle riunioni, i docenti possono acquisire automaticamente la lezione e la discussione in classe, rendendo facile per gli studenti rivedere i concetti. Le trascrizioni tengono traccia della partecipazione e mostrano chi ha detto cosa in una riunione.

- Disponibili in inglese per gli utenti di Google Meet su computer o laptop
- Gli amministratori possono attivare le trascrizioni per la comunità scolastica
- Le trascrizioni vengono salvate automaticamente sul Drive di chi ha organizzato la riunione
- Quando le trascrizioni della riunione sono attive, viene visualizzata un'icona Trascrizioni in alto a sinistra per tutti i partecipanti alla riunione
- Le trascrizioni contengono quanto detto a voce in una riunione: per ottenere una trascrizione dei messaggi della chat, registra la riunione

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Usare le trascrizioni con Google Meet
- Attivare o disattivare la trascrizione

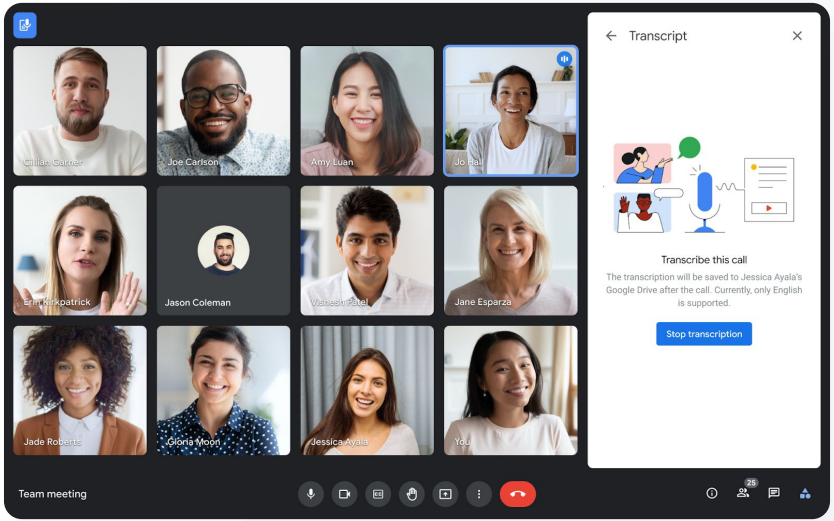
Istruzioni: consultazione di quanto discusso in classe

Attivare le trascrizioni in Google Meet

- In una riunione, nell'angolo in alto a destra, seleziona l'icona **Attività**
- Fai clic su **Trascrizioni** > **Avvia trascrizione** > **Avvia**

Come interrompere le trascrizioni in Google Meet

- Seleziona l'icona **Attività** > **Trascrizioni** > **Interrompi trascrizione** > **Interrompi**



Documentazione pertinente del Centro assistenza

- Usare le trascrizioni con Google Meet
- Attivare o disattivare la trascrizione

Organizziamo conferenze virtuali famiglie/insegnanti, ma a volte non parliamo tutti la stessa lingua.

Come faccio a rendere inclusive le riunioni e superare le barriere linguistiche?”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Utilizzare i sottotitoli codificati tradotti in Google Meet

Eliminazione delle barriere linguistiche

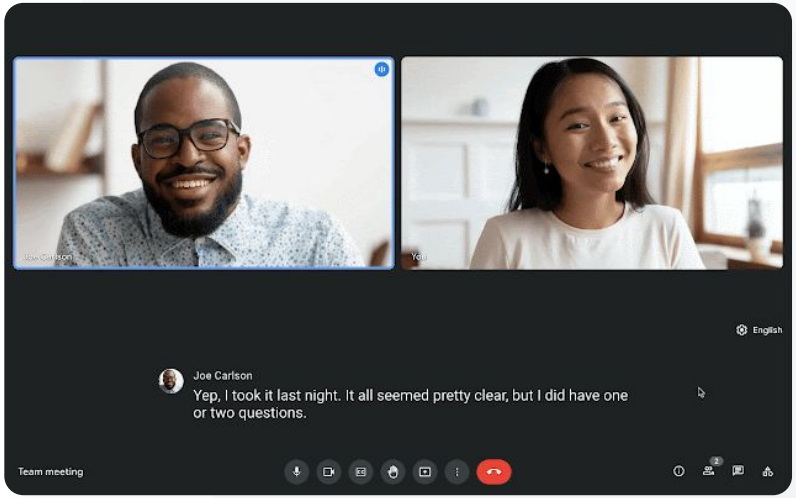
I sottotitoli codificati tradotti rendono più inclusive le riunioni eliminando le barriere della competenza linguistica. Se i partecipanti alla riunione dispongono di contenuti nella loro lingua preferita, si bilancia la condivisione delle informazioni, l'apprendimento e la collaborazione.

- I docenti possono interagire con studenti, famiglie e parti interessate della comunità che parlano una lingua diversa
- Utilizza i sottotitoli codificati per tradurre nelle seguenti lingue dall'inglese o viceversa: francese, tedesco, portoghese o spagnolo
- Oppure traduci dall'inglese in giapponese, mandarino o svedese

Istruzioni: eliminazione delle barriere linguistiche

Come attivare i sottotitoli codificati tradotti

- Durante una riunione, in basso a destra nello schermo, fai clic su **Altre opzioni** > **Impostazioni** > **Sottotitoli codificati**
- Attiva **Sottotitoli codificati**
- Seleziona la **Lingua della riunione**
- Attiva **Sottotitoli tradotti**
- Seleziona la **lingua di destinazione**



Documentazione pertinente del Centro assistenza

- Utilizzare i sottotitoli codificati tradotti in Google Meet

> Vogliamo avere la possibilità di trasmettere in live streaming le riunioni del personale e dei docenti affinché possa assistere un numero nutrito di persone coinvolte e genitori.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Attivare o disattivare il live streaming per Meet
- Trasmettere una riunione video in live streaming

Trasmissione di assemblee, riunioni ed eventi scolastici

Trasmetti in live streaming per un massimo di 10.000 spettatori con Teaching and Learning Upgrade e per un massimo di 100.000 spettatori con Education Plus. Per partecipare, gli utenti possono selezionare il link al live streaming fornito dall'organizzatore in un'email o con un invito di Calendar.

- Stabilisci in che misura verrà condiviso il tuo live streaming, cioè se sarà:
  - Visibile solo agli utenti all'interno della tua organizzazione (nel dominio)
  - Condivisibile con altri domini affidabili di Google Workspace
  - Disponibile su YouTube
- È consigliabile che gli amministratori IT abilitino il live streaming solo per il personale docente e amministrativo
- Se un utente non può essere presente per il live streaming, potrà guardarlo in un momento successivo una volta terminata la riunione
- Aggiungi sottotitoli codificati, sondaggi e domande e risposte a un live streaming per aumentare l'inclusività e il coinvolgimento

Istruzioni: trasmissione di assemblee, riunioni ed eventi scolastici

Come si crea un evento in live streaming

- Apri **Google Calendar**
- Seleziona **+ Crea** > **Altre opzioni**
- Aggiungi i dettagli dell'evento, ad esempio la data, l'ora e la descrizione
- Aggiungi gli utenti che possono partecipare alla riunione video con tutti i diritti di accesso, ovvero che potranno essere visti, sentiti e avranno la possibilità di presentare
- Fai clic su **Aggiungi videoconferenza di Google Meet** > **Meet**
- Accanto a Partecipa con Google Meet, seleziona la **Freccia giù**, quindi **Aggiungi live streaming**
- Per invitare il numero massimo di singoli utenti consentito dalla versione a pagamento di cui disponi, fai clic su **Copia** e condividi l'URL del live streaming
- Seleziona **Salva**
- Lo streaming non si avvia automaticamente: durante la riunione, seleziona **Altro** > **Avvia streaming**

Documentazione pertinente del Centro assistenza

- Attivare o disattivare il live streaming per Meet
- Trasmettere una riunione video in live streaming

Possibilità di fare domande

Utilizza la funzionalità **Domande e risposte** di Google Meet per tenere vivo l'interesse degli studenti e rendere il corso più interattivo. Al termine della lezione virtuale, gli insegnanti riceveranno un report dettagliato con tutte le domande e le risposte.

- Non c'è alcun limite al numero di domande che possono porre i moderatori. Inoltre, questi ultimi possono anche filtrare o ordinare le domande, contrassegnarle come risolte, nasconderle o assegnare la priorità a determinate domande
- Al termine di ogni riunione in cui sono state attivate le domande, il moderatore riceverà automaticamente via email un report sulle domande fatte

> “Mi serve un modo rapido per fare delle domande, verificare le conoscenze degli studenti e interagire con la classe in modo da mantenere alto l'interesse di tutti.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Fare domande ai partecipanti in Google Meet

Istruzioni: possibilità di fare domande

Fare una domanda

- In una riunione, nell'angolo in alto a destra, seleziona l'**icona Attività** > **Domande** (per attivare Domande e risposte, seleziona **Attiva Domande e risposte**)
- Per porre una domanda, fai clic su **Fai una domanda** nell'angolo in basso a destra
- **Inserisci le tue domande** > Seleziona **Pubblica**

Visualizzare il report relativo alle domande

- Dopo una riunione, il moderatore riceve un'**email con il report sulle domande**
- Apri l'email > Fai clic sul **report in allegato**

Documentazione pertinente del Centro assistenza

- Fare domande ai partecipanti in Google Meet

Raccolta di opinioni

Chi programma o avvia una riunione virtuale può creare un **sondaggio** per i partecipanti della riunione. Questa funzionalità consente di aggregare in modo rapido e stimolante le informazioni fornite da tutti gli studenti o i partecipanti di una riunione.

- I moderatori possono salvare un sondaggio in modo da pubblicarlo in un momento successivo durante una riunione. I sondaggi vengono salvati nella pratica sezione Sondaggi all'interno delle riunioni virtuali
- Al termine della riunione, un report con i risultati del sondaggio viene inviato automaticamente al moderatore via email

> “Ho bisogno di un modo semplice per raccogliere feedback dagli studenti e dai miei colleghi quando tengo un corso o una riunione del personale.”

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Condurre sondaggi in Google Meet

Istruzioni: raccolta di opinioni

Creare un sondaggio

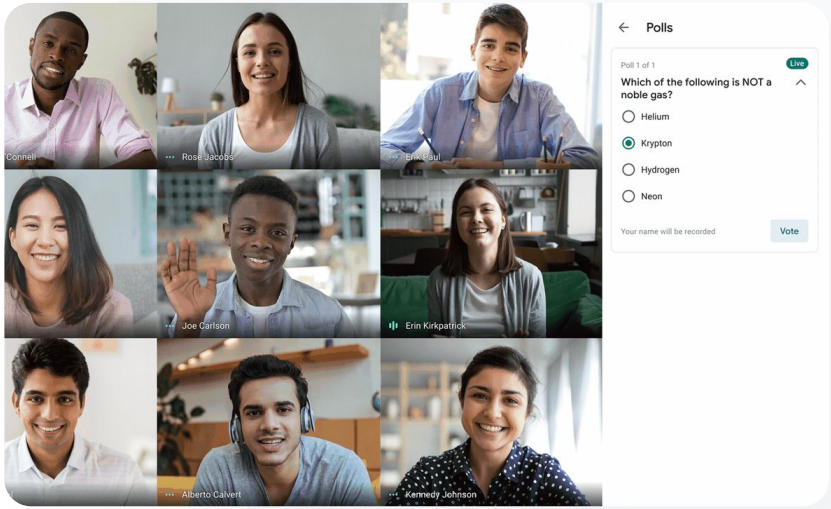
- Nell'angolo in alto a destra di una riunione, seleziona l'**icona Attività** > **Sondaggio**
- Seleziona **Avvia un sondaggio**
- Inserisci una domanda
- Seleziona **Lancia** o **Salva**

Moderare un sondaggio

- In una riunione, nell'angolo in alto a destra, seleziona l'**icona Attività** > **Sondaggio**
- Per consentire ai partecipanti di visualizzare in tempo reale i risultati di un sondaggio, accanto a **Mostra i risultati a tutti**, seleziona l'**opzione On**
- Per chiudere un sondaggio e non consentire altre risposte, fai clic su **Termina il sondaggio**
- Per eliminare definitivamente un sondaggio, seleziona l'**icona Elimina**

Visualizzare un report su un sondaggio

- Dopo una riunione, il moderatore riceve un'**email con il report**
- Apri l'email > Seleziona il **report in allegato**



Documentazione pertinente del Centro assistenza

- Condurre sondaggi in Google Meet

“A volte abbiamo studenti in didattica a distanza. Quando lavoriamo in piccoli gruppi, ho bisogno di un modo per creare facilmente gruppi di lavoro basati su categorie predefinite.”

Piccoli gruppi di studenti

I docenti possono utilizzare i gruppi di lavoro per suddividere gli studenti in piccoli gruppi durante le lezioni virtuali, **in presenza o ibride**. I gruppi di lavoro devono essere avviati dai moderatori durante una videochiamata su un computer.

- I gruppi di lavoro possono essere definiti in anticipo durante la creazione di un evento o mentre è in corso una riunione
- È possibile creare fino a 100 gruppi di lavoro per riunione virtuale
- Gli insegnanti possono passare facilmente da un gruppo di lavoro all'altro per aiutare i singoli gruppi in base alle necessità
- Gli amministratori possono fare in modo che solo i membri del personale docente e amministrativo abbiano la facoltà di creare gruppi di lavoro

Istruzioni passo passo

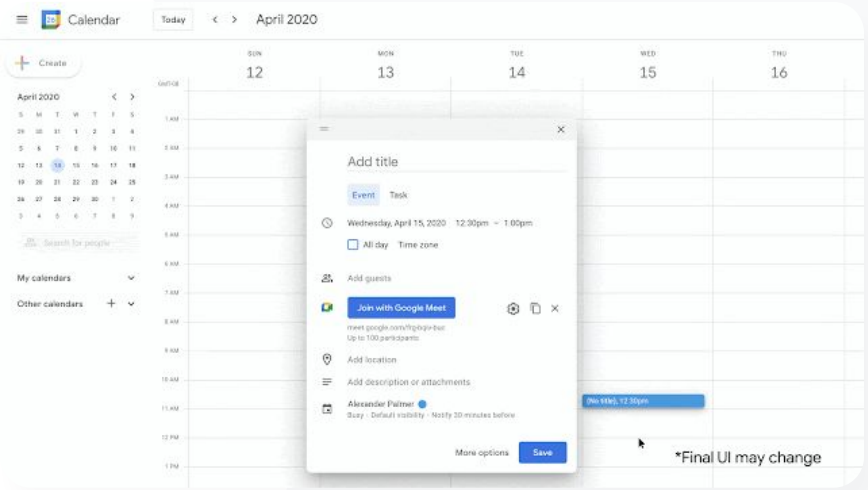
Documentazione pertinente del Centro assistenza

- Utilizzare i gruppi di lavoro in Google Meet

Istruzioni: creazione di piccoli gruppi di studenti

Creare i gruppi di lavoro prima della riunione

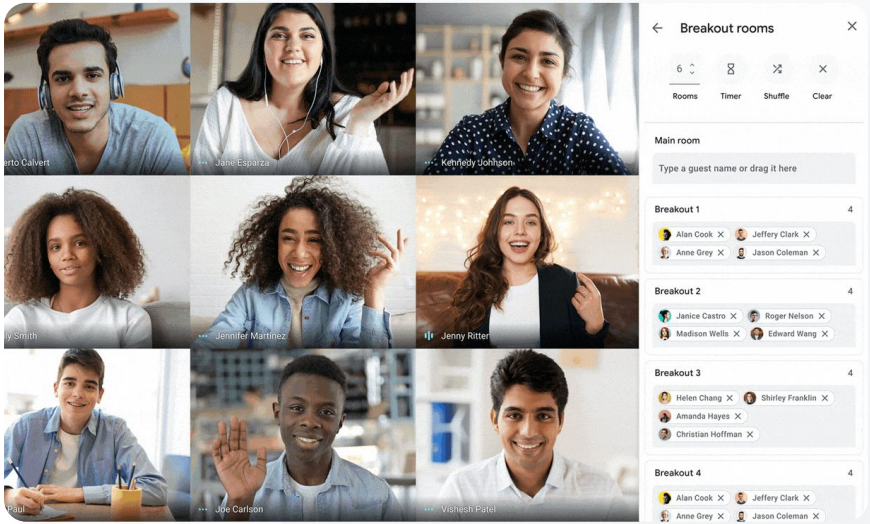
- Crea un nuovo evento in Google Calendar
- Fai clic su **Aggiungi videoconferenza di Google Meet**
- Aggiungi i partecipanti > Seleziona **Modifica le impostazioni della conferenza**
- Fai clic su **Gruppi di lavoro**
- Scegli il numero di gruppi di lavoro e seleziona una delle seguenti opzioni:
  - Trascina i partecipanti in stanze virtuali diverse
  - Inserisci i nomi direttamente in una stanza virtuale
  - Fai clic su **Distribuisci casualmente** per mescolare i gruppi
- Fai clic su **Salva**



Documentazione pertinente del Centro assistenza

- Utilizzare i gruppi di lavoro in Google Meet

Istruzioni: creazione di piccoli gruppi di studenti



Creare gruppi di lavoro durante la riunione

- Avvia una videochiamata
- In alto a destra, seleziona l'**icona Attività** > **Gruppi di lavoro**
- Nel riquadro Gruppi di lavoro, **scegli il numero di gruppi** di cui hai bisogno
- Gli studenti vengono quindi distribuiti tra i gruppi, ma i moderatori hanno la possibilità di spostarli in gruppi diversi all'occorrenza
- In basso a destra, fai clic su **Apri** gruppi di lavoro

Rispondere alle domande poste in altri gruppi di lavoro

- Quando un partecipante chiede aiuto, in fondo allo schermo del moderatore viene visualizzata una notifica: seleziona Partecipa per accedere al gruppo di lavoro del partecipante interessato

Documentazione pertinente del Centro assistenza

- Utilizzare i gruppi di lavoro in Google Meet

“Abbiamo qualche difficoltà a tenere traccia di chi partecipa ai corsi online. Ho bisogno di una soluzione semplice per registrare le partecipazioni ai corsi nell'intero dominio.”

Monitoraggio delle partecipazioni

Il monitoraggio delle partecipazioni mette a disposizione un report sulla partecipazione creato in modo automatico per tutte le riunioni con cinque o più partecipanti. Nei report viene riportato l'elenco dei partecipanti alla chiamata, con le rispettive email e il tempo per cui hanno seguito il corso virtuale.

- Puoi monitorare le partecipazioni durante i live streaming con gli appositi report
- I moderatori possono attivare e disattivare i report sul monitoraggio delle partecipazioni e i report relativi ai live streaming direttamente da una riunione o dall'evento nel calendario

Istruzioni passo passo

Documentazione pertinente del Centro assistenza

- Monitorare le partecipazioni in Google Meet

Istruzioni: monitoraggio delle partecipazioni

Come monitorare la partecipazione all'interno di una riunione

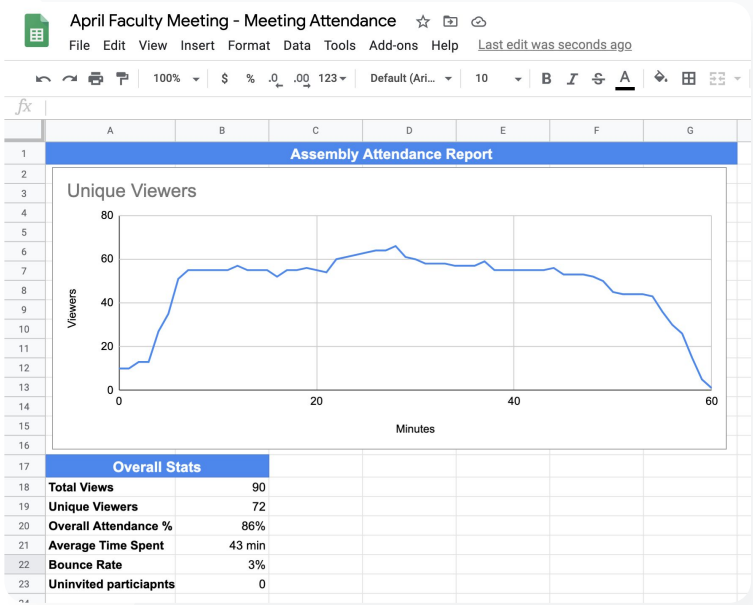
- Avvia una videochiamata
- In basso, seleziona l'**icona del menu**
- Seleziona l'**icona delle impostazioni** > **Controlli dell'organizzatore**
- Attiva o disattiva **Monitoraggio delle partecipazioni**

Come monitorare la partecipazione in Calendar

- **Attiva la conferenza di Google Meet** da un evento nel calendario
- A destra, seleziona l'**icona delle impostazioni**
- Seleziona la casella accanto a **Monitoraggio delle partecipazioni** > Fai clic su **Salva**

Ricevere il report sulla partecipazione

- Dopo una riunione, il moderatore riceve un'**email con il report**
- Apri l'email > Seleziona il **report in allegato**



Documentazione pertinente del Centro assistenza

- Monitorare le partecipazioni in Google Meet

Grazie