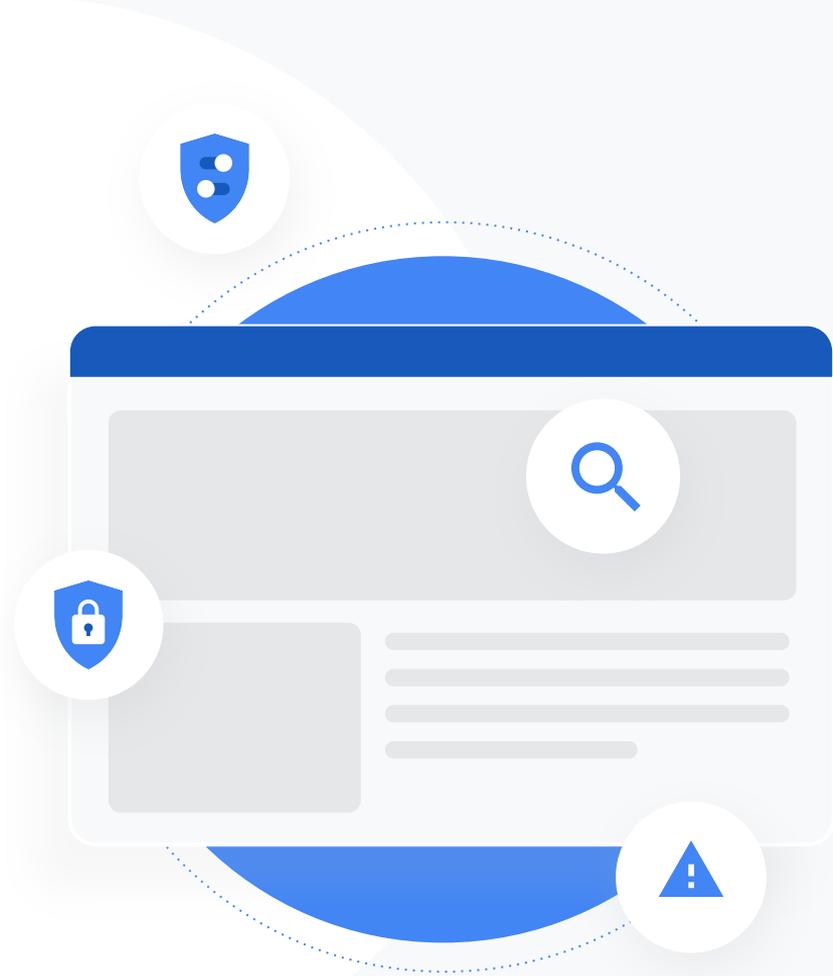


Google for Education

Mehr als 30 Tipps, wie Sie die kostenpflichtigen Versionen von Google Workspace for Education nutzen können

goo.gle/use-edu-workspace



So verwenden Sie diese Foliensammlung

In dieser Foliensammlung finden Sie eine Auswahl der beliebtesten Anwendungsfälle für die kostenpflichtigen Versionen von Google Workspace for Education. Die Tools können Sie dabei unterstützen, u. a. die **Datensicherheit**, die **Effizienz der Lehrkräfte**, die **Motivation der Schüler bzw. Studenten** sowie die **einrichtungsübergreifende Zusammenarbeit** zu verbessern.

Die Foliensammlung ist nach **Funktionen** sortiert. Zu jeder Funktion sind **häufige Anwendungsfälle** und einfache **Anleitungen** zur Verwendung der Funktion aufgeführt. Sehen Sie sich alle Folien an, um zu erfahren, welche Möglichkeiten Ihnen mit Google Workspace for Education zur Verfügung stehen.

Die kostenpflichtigen Versionen von Google Workspace for Education

Mit den folgenden drei kostenpflichtigen Versionen von Google Workspace for Education erhalten Sie vielfältige Optionen, mehr Einstellungsmöglichkeiten und zusätzliche Flexibilität, um den Anforderungen Ihrer Bildungseinrichtung gerecht zu werden.



Google Workspace for Education Standard

Erweiterte Sicherheits- und Analysetools bieten eine höhere Transparenz und eine bessere Steuerung Ihrer Lernumgebung, um Risiken zu senken und Bedrohungen zu mindern.



Teaching and Learning Upgrade

Mit den erweiterten Tools für **Lehrkräfte** bereichern Sie die Kommunikation und den Unterricht und fördern die akademische Integrität.



Google Workspace for Education Plus

Diese umfassende Lösung mit allen Funktionen von Education Standard und dem Teaching and Learning Upgrade stattet Ihre Bildungseinrichtung mit einer effektiven und einheitlichen Lernumgebung aus.

Inhaltsverzeichnis



Sicherheits- und Analysetools

Tools in Education Standard und Education Plus

Prüftool

- Missbräuchliche Inhalte, die in Ihrer Domain zirkulieren
- Versehentliche Freigabe von Dateien
- E-Mail-Voranalyse
- Phishing- und Malware-E-Mails
- Böswillige Akteure stoppen

Sicherheitsdashboard

- Spamvolumen
- Externe Dateifreigabe
- Drittanbieter-Anwendungen
- Phishing-Versuche

Sicherheitsstatus

- Empfehlungen für Risikobereiche
- Aktuelles zu Best Practices
- Best Practices für Sicherheit
- Mehr Sicherheit für eine wachsende Bildungseinrichtung

Erweiterte Steuerelemente für Administratoren

- Datenschutzgesetze
- Stipendienrichtlinien einhalten
- App-Zugriffsbeschränkungen
- Mobilgeräte verwalten
- Daten migrieren

Inhaltsverzeichnis



Tools zum Unterrichten und Lernen

Tools im Teaching and Learning Upgrade und in Education Plus

Plagiatsberichte

- Plagiate finden
- Plagiatsprüfungen als Anstoß zum Lernen

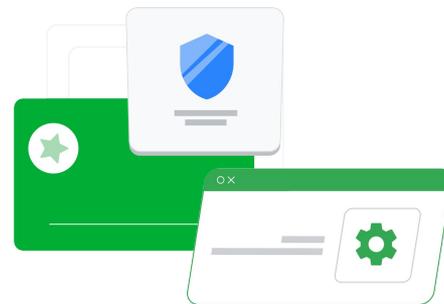
Google Meet

- Sichere Videokonferenzen
- Mehr Sicherheit bei Videokonferenzen
- Unterrichtseinheiten aufzeichnen
- Fakultätsbesprechungen aufzeichnen
- Verpasste Unterrichtseinheiten
- Livestreaming von Videokonferenzen
- Livestreaming von Schulveranstaltungen
- Fragen stellen
- Feedback sammeln
- Kleine Schüler-/Studentengruppen
- Teilnahme erfassen



Sicherheit- und Analysetools

Dank der proaktiven Sicherheitstools behalten Sie Ihre Domain noch besser im Blick. Die Funktionen bieten einen erhöhten Schutz gegen Bedrohungen und helfen Ihnen, sicherheitsrelevante Zwischenfälle zu analysieren und die Daten von Schülern oder Studenten sowie Lehrkräften zu schützen.



[Prüftool](#)



[Sicherheitsdashboard](#)



[Seite „Sicherheitsstatus“](#)



[Erweiterte Steuerelemente für Administratoren](#)



Prüftool

Beschreibung

Mit dem Prüftool können Sie Sicherheits- und Datenschutzprobleme in Ihrer Domain erkennen, beurteilen und Maßnahmen ergreifen.

Anwendungsfälle

Missbräuchliche Inhalte, die in Ihrer Domain zirkulieren



[Detaillierte Anleitung](#)

Versehentliche Freigabe von Dateien



[Detaillierte Anleitung](#)

E-Mail-Voranalyse



[Detaillierte Anleitung](#)

Phishing- und Malware-E-mails

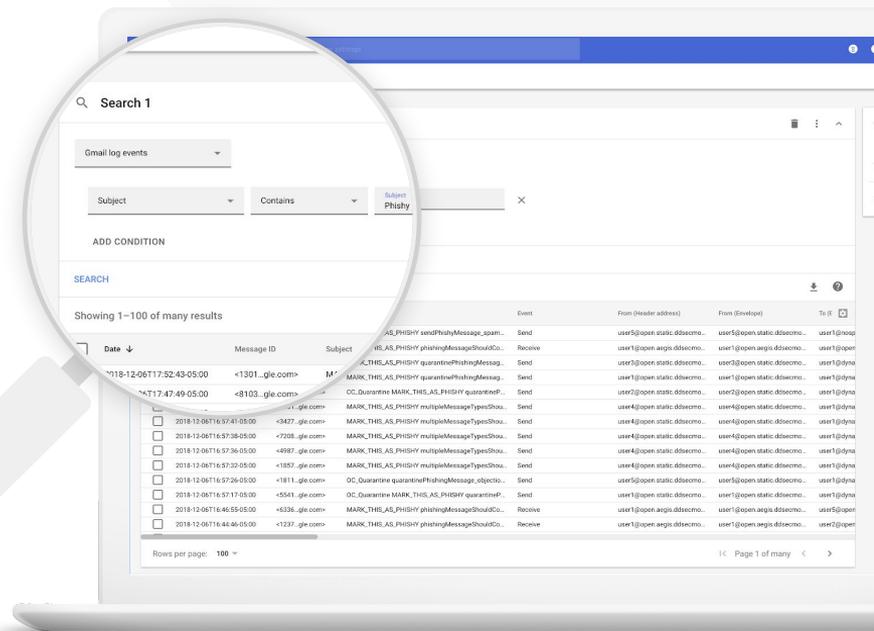


[Detaillierte Anleitung](#)

Böswillige Akteure stoppen



[Detaillierte Anleitung](#)



“

Ich weiß, dass gerade eine Datei im Umlauf ist, die missbräuchliches Material enthält. Ich möchte wissen, wer diese Datei wann erstellt hat, wer sie für wen freigegeben hat und von wem sie bearbeitet wurde – außerdem möchte ich sie löschen.“

[Detaillierte Anleitung](#)

Missbräuchliche Inhalte, die in Ihrer Domain zirkulieren

Drive-Protokolle im Prüftool unterstützen Sie dabei, unerwünschte Dateien in Ihrer Domain zu finden, nachzuverfolgen, zu isolieren oder zu löschen. Durch den Zugriff auf Ihre [Drive-Protokolle](#) können Sie:

- ✓ Dokumente mithilfe von Informationen wie Name, Akteur oder Eigentümer finden
- ✓ Alle Protokollinformationen im Zusammenhang mit einem bestimmten Dokument ansehen
 - Erstellungsdatum
 - Wem es gehört, wer es sich angesehen hat und durch wen es bearbeitet wurde
 - Wann es freigegeben wurde
- ✓ Maßnahmen ergreifen, indem Sie Dateiberechtigungen ändern oder die Datei löschen

[↗](#) Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Im Prüftool suchen](#) [Auf Grundlage von Suchergebnissen Aktionen durchführen](#)

Versehentliche Freigabe von Dateien

Drive-Protokolle im Prüftool unterstützen Sie dabei, Probleme bei der Dateifreigabe zu finden und zu lösen. Durch den Zugriff auf Ihre [Drive-Protokolle](#) können Sie:

- ✓ Dokumente mithilfe von Informationen wie Name, Akteur oder Eigentümer finden
- ✓ Alle Protokollinformationen im Zusammenhang mit einem bestimmten Dokument aufrufen, z. B. wer es sich angesehen hat und wann es freigegeben wurde
- ✓ Maßnahmen ergreifen, indem Sie Dateiberechtigungen ändern bzw. Funktionen wie Herunterladen, Drucken und Kopieren deaktivieren

 Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)

[Im Prüftool suchen](#) [Auf Grundlage von Suchergebnissen Aktionen durchführen](#)



Eine Datei wurde versehentlich an eine Gruppe freigegeben, die KEINEN Zugriff darauf haben sollte. Ich möchte diesen Zugriff entfernen.“

[Detaillierte Anleitung](#)

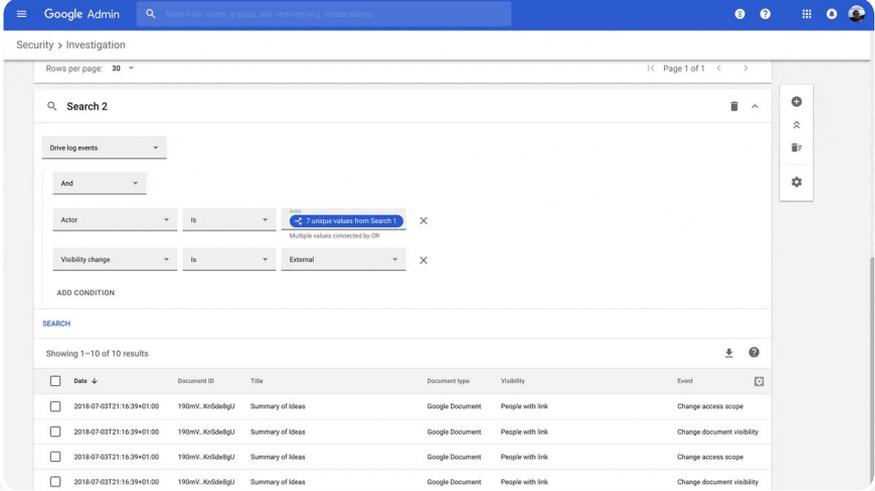
Anleitung: Drive-Protokollereignisse

Prüfung

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf Sicherheit > Prüftool.
- Wählen Sie Drive-Protokollereignisse aus.
- Klicken Sie auf Bedingung hinzufügen > Suchen.

Geeignete Maßnahmen

- Wählen Sie die betreffenden Dateien in den Suchergebnissen aus.
- Klicken Sie auf Aktionen > Dateiberechtigungen prüfen, um die Seite „Berechtigungen“ zu öffnen.
- Um zu sehen, wer Zugriff auf die jeweilige Datei hat, klicken Sie auf Personen.
- Wenn Sie die Einstellungen für die Linkfreigabe zu den ausgewählten Dateien aufrufen oder ändern möchten, klicken Sie auf Links.
- Wenn Sie die Änderungen vor dem Speichern noch einmal überprüfen möchten, klicken Sie auf Ausstehende Änderungen.



Security > Investigation

Rows per page: 30 Page 1 of 1

Search 2

Drive log events

And

Actor is 7 Alltags-Werte from Search 1

Visibility change is External

ADD CONDITION

SEARCH

Showing 1–10 of 10 results

<input type="checkbox"/>	Date	Document ID	Title	Document type	Visibility	Event
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrD6d6lGJ	Summary of Ideas	Google Document	People with link	Change access scope
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrD6d6lGJ	Summary of Ideas	Google Document	People with link	Change document visibility
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrD6d6lGJ	Summary of Ideas	Google Document	People with link	Change access scope
<input type="checkbox"/>	2018-07-03T21:16:39+01:00	190nv_KrD6d6lGJ	Summary of Ideas	Google Document	People with link	Change document visibility

[Weiterführende Informationen in der Google Workspace-Admin-Hilfe](#)

[Im Prüftool suchen](#)

[Auf Grundlage von Suchergebnissen](#)

[Aktionen durchführen](#)

“

Jemand hat eine E-Mail gesendet, die NICHT hätte versendet werden sollen. Wir möchten wissen, wer sie erhalten hat, ob sie geöffnet wurde und ob der Empfänger geantwortet hat. Außerdem möchten wir den Inhalt der E-Mail erfahren und sie anschließend löschen.“

[Detaillierte Anleitung](#)

E-Mail-Voranalyse

Die **Gmail-Protokolle** im Prüftool unterstützen Sie dabei, gefährliche oder missbräuchliche E-Mails innerhalb Ihrer Domain zu identifizieren und darauf zu reagieren. Durch den Zugriff auf Ihre Gmail-Protokolle können Sie:

- ✓ Bestimmte E-Mails über Informationen wie Betreff, Nachrichten-ID, Anhang oder Absender finden
- ✓ E-Mail-Informationen wie Autor, Empfänger und Weiterleitungen aufrufen und sehen, wer die Nachrichten geöffnet hat
- ✓ Auf Grundlage von Suchergebnissen Aktionen durchführen, z. B. Gmail-Nachrichten löschen, wiederherstellen, als Spam oder Phishing markieren, in den Posteingang verschieben oder unter Quarantäne stellen

 Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)

[Im Prüftool suchen](#)

[Auf Grundlage von Suchergebnissen Aktionen durchführen](#)

[Mit dem Prüftool Nachrichteninhalte in Gmail ansehen](#)

“

Eine Phishing- oder Malware-E-Mail wurde an einen oder mehrere Nutzer gesendet. Wir möchten sehen, ob jemand auf den Link in der E-Mail geklickt oder den Anhang heruntergeladen hat, da dies ein potenzielles Risiko für die Nutzer und unsere Domain bedeuten könnte.“

[Detaillierte Anleitung](#)

Phishing- und Malware-E-Mails

Mit dem **Prüftool**, insbesondere mit den **Gmail-Protokollen**, können Sie schädliche E-Mails innerhalb Ihrer Domain finden und isolieren. Durch den Zugriff auf Ihre Gmail-Protokolle können Sie:

- ✓ In E-Mails nach bestimmten Inhalten, einschließlich Anhängen, suchen
- ✓ Informationen zu bestimmten E-Mails aufrufen, z. B. wer der Empfänger war und wer sie geöffnet hat
- ✓ Die Nachrichten und den E-Mail-Thread aufrufen, um festzustellen, ob sie schädlich sind
- ✓ Maßnahmen ergreifen, z. B. Nachrichten als Spam oder Phishing markieren, sie in einen bestimmten Posteingang bzw. in Quarantäne verschieben oder sie löschen

[↗](#) Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Im Prüftool suchen](#)

[Auf Grundlage von Suchergebnissen Aktionen durchführen](#)

[Mit dem Prüftool Nachrichteninhalte in Gmail ansehen](#)

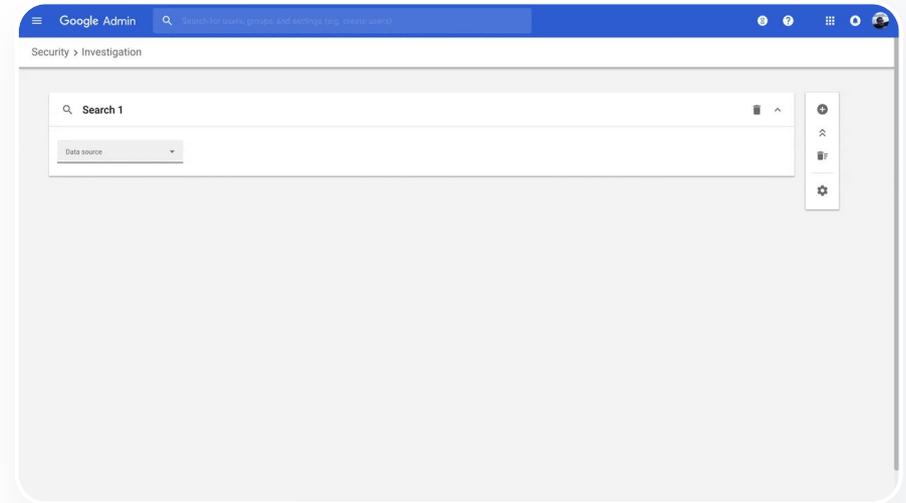
Anleitung: Gmail-Protokolle

Prüfung

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf **Sicherheit > Prüftool**.
- Wählen Sie **Gmail-Protokollereignisse** ODER **Gmail-Nachrichten** aus.
- Klicken Sie auf **Bedingung hinzufügen > Suchen**.

Geeignete Maßnahmen

- Wählen Sie die betreffenden Nachrichten in den Suchergebnissen aus.
- Klicken Sie auf **Aktionen**.
- Wählen Sie **Nachrichte aus dem Posteingang löschen** aus.
- Klicken Sie auf **Aus dem Posteingang löschen**.
- Um die Aktion zu überprüfen, klicken Sie unten auf der Seite auf **Ansehen**.
- In der **Ergebnisspalte** können Sie sich den Status der Aktion ansehen.



[➔ Weiterführende Informationen in der
Google Workspace-Admin-Hilfe](#)

[Im Prüftool suchen](#)

[Auf Grundlage von Suchergebnissen Aktionen durchführen](#)

[Mit dem Prüftool Nachrichteninhalte in Gmail ansehen](#)

“

Ein böswilliger Akteur hat es auf wichtige Nutzer innerhalb meiner Domain abgesehen, aber ich kriege ihn einfach nicht zu fassen. Wie kann ich dem ein Ende setzen?“

[Detaillierte Anleitung](#)

Böswillige Akteure stoppen

Mit dem Nutzerprotokoll im Prüftool können Sie:

- ✓ Manipulationsversuche von Nutzerkonten Ihrer Organisation identifizieren und prüfen
- ✓ Im Blick haben, welche Methoden der Bestätigung in zwei Schritten Nutzer in Ihrer Organisation verwenden
- ✓ Mehr über fehlgeschlagene Anmeldeversuche von Nutzern in Ihrer Organisation erfahren
- ✓ [Aktivitätsregeln erstellen und verwalten](#): Nachrichten und andere schädliche Aktivitäten bestimmter Akteure automatisch blockieren
- ✓ Wichtige Nutzer mit dem [erweiterten Sicherheitsprogramm noch besser schützen](#)
- ✓ Nutzer wiederherstellen oder sperren

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Nutzer-Protokollereignisse durchsuchen und prüfen](#)

[Aktivitätsregeln erstellen und verwalten](#)

Anleitung: Nutzer-Protokollereignisse

Prüfung

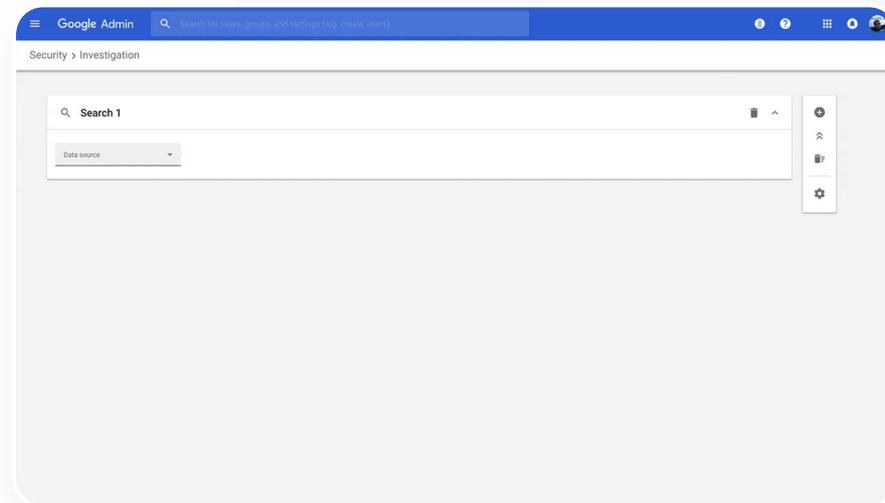
- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf Sicherheit > Prüftool.
- Wählen Sie Nutzer-Protokollereignisse aus.
- Klicken Sie auf Bedingung hinzufügen > Suchen.

Nutzer wiederherstellen oder sperren

- Wählen Sie aus den Suchergebnissen mindestens einen Nutzer aus.
- Klicken Sie auf das Drop-down-Menü Aktionen.
- Klicken Sie auf Nutzer wiederherstellen oder Nutzer sperren.

Informationen zu einem bestimmten Nutzer aufrufen

- Wählen Sie auf der Suchergebnisseite einen einzelnen Nutzer aus.
- Klicken Sie im Drop-down-Menü AKTIONEN auf Details ansehen.



 Weiterführende Informationen in der
Google Workspace-Admin-Hilfe
[Nutzer-Protokollereignisse durchsuchen und prüfen](#)

Sicherheitsdashboard

Beschreibung

Im Sicherheitsdashboard finden Sie eine Übersicht der verschiedenen Sicherheitsberichte. Standardmäßig sind in den einzelnen Berichten die Daten der letzten sieben Tage zu sehen. Sie können das Dashboard jedoch auch über die folgenden Optionen so anpassen, dass nur Daten für die entsprechenden Zeiträume angezeigt werden: „Heute“, „Gestern“, „Diese Woche“, „Letzte Woche“, „Aktueller Monat“, „Letzter Monat“ oder „Tage in der Vergangenheit (bis zu 180 Tage)“.

Anwendungsfälle

[Spamvolumen](#)



[Detaillierte Anleitung](#)

[Externe Dateifreigabe](#)



[Detaillierte Anleitung](#)

[Drittanbieter-Anwendungen](#)

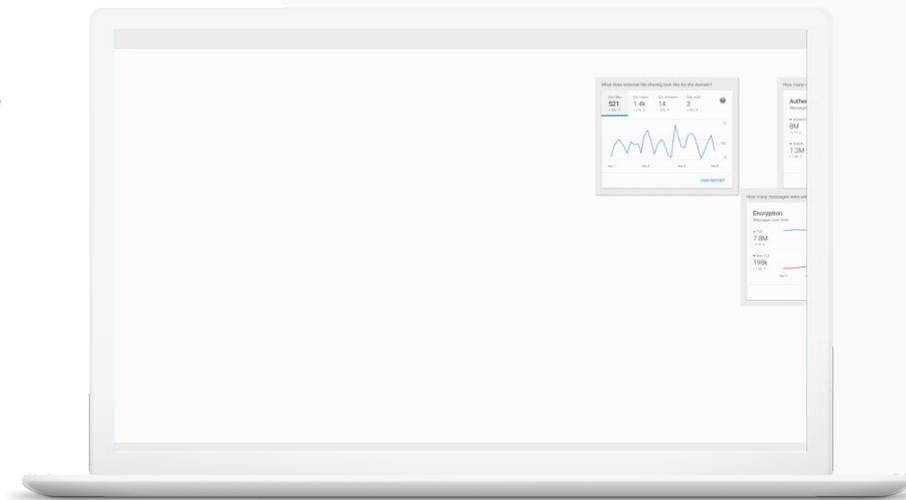


[Detaillierte Anleitung](#)

[Phishing-Versuche](#)



[Detaillierte Anleitung](#)





Spamvolumen

Im **Sicherheitsdashboard** sind die Aktivitäten in Ihrer Google Workspace for Education-Umgebung anschaulich aufbereitet, z. B. anhand von grafischen Darstellungen zu diesen Bereichen:

- ✓ Spam
- ✓ Verdächtige Anhänge
- ✓ Phishing
- ✓ Und mehr
- ✓ Malware

[↗](#) Weiterführende Informationen in der **Google Workspace-Admin-Hilfe**
[Sicherheitsdashboard verwenden](#)



Ich möchte Spam und unnötige E-Mails unter Kontrolle halten und meine Bildungseinrichtung besser vor Sicherheitsrisiken schützen.“

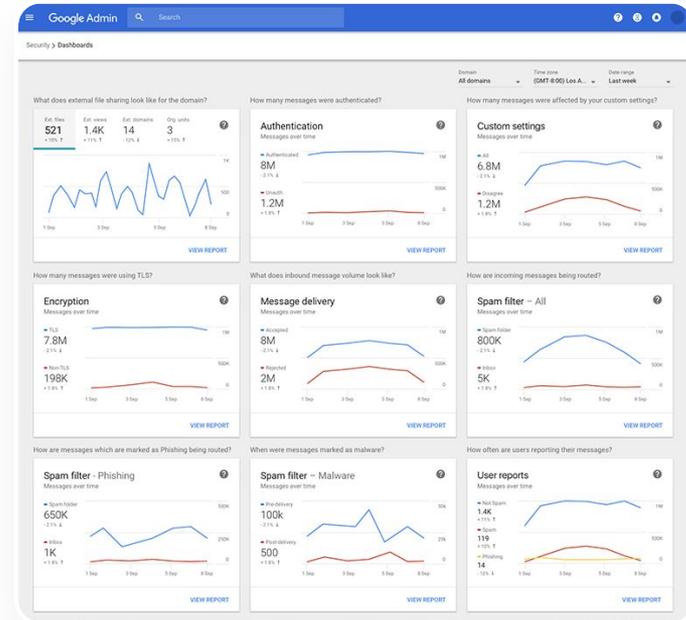
[Detaillierte Anleitung](#)



Anleitung: Dashboardübersicht

Dashboard aufrufen

- Melden Sie sich in der **Admin-Konsole** an.
- Klicken Sie auf **Sicherheit > Dashboard**.
- Suchen Sie im Sicherheitsdashboard nach Daten. Sie können sie dann in Google Tabellen oder Drittanbieter-Tools exportieren oder mit dem Prüftool untersuchen.



[Weiterführende Informationen in der Google Workspace-Admin-Hilfe Sicherheitsdashboard verwenden](#)



Externe Dateifreigabe

Mit dem Bericht „Dateisichtbarkeit“ aus dem Sicherheitsdashboard können Sie Messwerte für die externe Dateifreigabe Ihrer Domain ansehen, z. B.:

- ✓ Anzahl der Freigaben an Nutzer außerhalb Ihrer Domain in einem bestimmten Zeitraum
- ✓ Anzahl der Aufrufe einer extern freigegebenen Datei über einen bestimmten Zeitraum

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Die Funktionen der Seite „Sicherheitsstatus“](#)



Ich möchte sehen, wie viele Dateien außerhalb der Domain freigegeben und von externen Personen aufgerufen wurden, damit sensible Daten nicht versehentlich mit Dritten geteilt werden.“

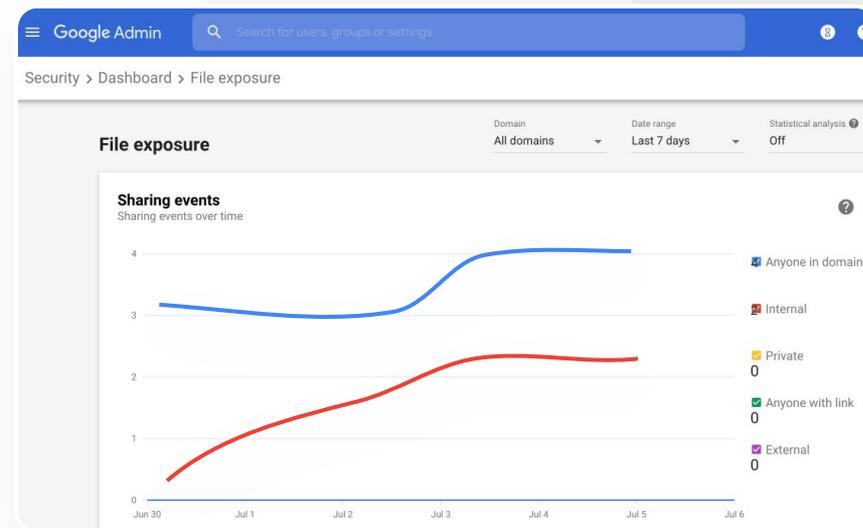
[Detaillierte Anleitung](#)



Anleitung: Bericht „Dateisichtbarkeit“

Bericht aufrufen

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf Sicherheit > Dashboard.
- Klicken Sie im Bereich mit dem Titel **Wie viele Dateien in der Domain wurden extern freigegeben?** in der rechten unteren Ecke auf **Bericht ansehen** .



 Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Sicherheitsdashboard verwenden Bericht
„Dateisichtbarkeit“](#)



Drittanbieter-Anwendungen

Mit dem Bericht „Änderungen der OAuth-Zustimmungen“ aus dem Sicherheitsdashboard können Sie im Blick behalten, welche Drittanbieter-Anwendungen mit Ihrer Domain verknüpft sind und auf welche Daten sie Zugriff haben.

- ✓ Über die OAuth-Zustimmung erhalten Drittanbieterdienste Zugriff auf Nutzerkontoinformationen, ohne dass Passwörter weitergegeben werden. Dabei können Sie den Zugriff auf bestimmte Drittanbieter-Apps einschränken.
- ✓ Im Bereich zu den OAuth-Zustimmungen sehen Sie alle Berechtigungen aufgelistet nach App, Umfang oder Nutzer und können sie bei Bedarf anpassen.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe
[Bericht „Änderungen der OAuth-Zustimmungen“](#)



Ich möchte sehen, welche Drittanbieter-Anwendungen Zugriff auf die Daten in meiner Domain haben.“

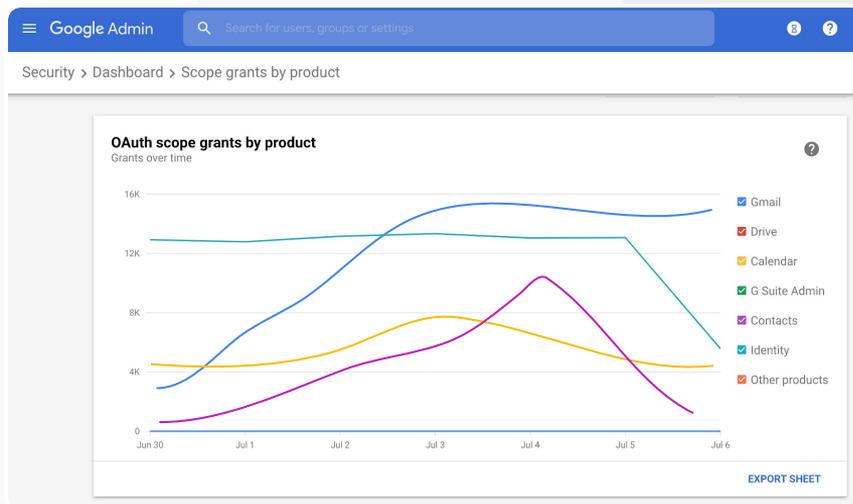
[Detaillierte Anleitung](#)



Anleitung: Bericht „Änderungen der OAuth-Zustimmungen“

Bericht aufrufen

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf **Sicherheit > Dashboard**.
- Klicken Sie unten auf **Bericht ansehen**.
- Im Bericht können Sie die OAuth-Zustimmung je nach Produkt (App), Umfang oder Nutzer aufrufen.
- Um die Informationen zu filtern, klicken Sie auf **App, Umfang** oder **Nutzer**.
- Um einen Bericht im Tabellenformat zu erstellen, klicken Sie auf **Als Tabelle exportieren**.



 [Weiterführende Informationen in der Google Workspace-Admin-Hilfe Bericht „Änderungen der OAuth-Zustimmungen“](#)



Phishing-Versuche

Im Bereich **Nutzerberichte** des **Sicherheitsdashboards** können Sie Nachrichten einsehen, die während eines bestimmten Zeitraums als Phishing oder Spam markiert wurden. Dabei können Sie sich Informationen zu diesen E-Mails anzeigen lassen, z. B. wer diese E-Mail empfangen und geöffnet hat.

- ✓ Im Bericht „Nutzerberichte“ erfahren Sie, welche Einstufungen die Nutzer in einem bestimmten Zeitraum für ihre Nachrichten verwendet haben, z. B. Spam, kein Spam oder Phishing.
- ✓ Sie können das Diagramm anpassen, um Informationen über bestimmte Nachrichtentypen abzurufen – z. B. intern oder extern gesendete Nachrichten oder solche aus einem bestimmten Zeitraum.

 Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)

[Wie markieren Nutzer ihre E-Mails?](#)

[Bericht „Nutzerberichte“](#)



Nutzer haben einen Phishing-Versuch gemeldet. Ich möchte nachsehen können, wann die Phishing-E-Mail eingegangen ist, wie sie ausgesehen hat und welchem Risiko meine Nutzer ausgesetzt waren.“

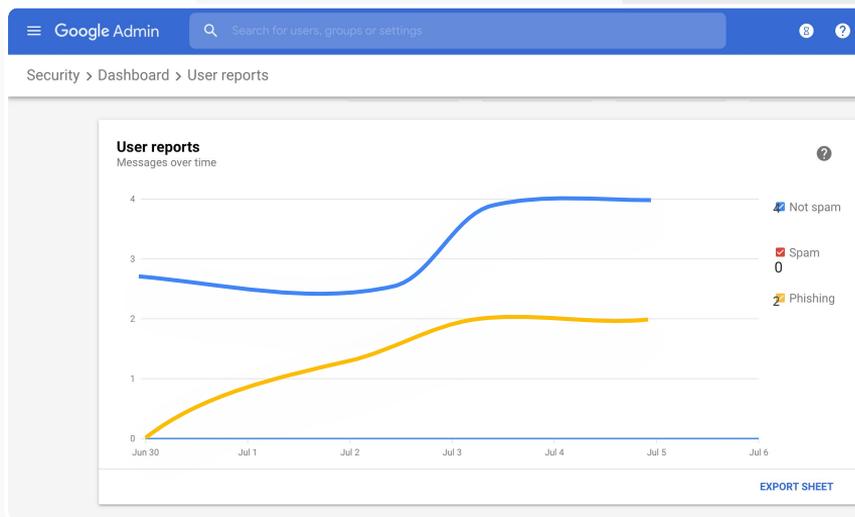
[Detaillierte Anleitung](#)



Anleitung: Bereich „Nutzerberichte“

Bericht aufrufen

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf Sicherheit > Dashboard.
- Klicken Sie im Bereich Nutzerberichte rechts unten auf Bericht ansehen.



[↗](#) Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#) [Sicherheitsdashboard verwenden Bericht „Dateisichtbarkeit“](#)

Sicherheitsstatus

Beschreibung

Auf der Seite „Sicherheitsstatus“ erhalten Sie eine umfassende Übersicht über den Sicherheitsstatus Ihrer Google Workspace-Umgebung. Sie können Ihre Konfigurationen mit den Empfehlungen von Google abgleichen und so Ihre Organisation proaktiv schützen.

Anwendungsfälle

[Empfehlungen für Risikobereiche](#)



[Detaillierte Anleitung](#)

[Aktuelles zu Best Practices](#)



[Detaillierte Anleitung](#)

[Best Practices für Sicherheit](#)

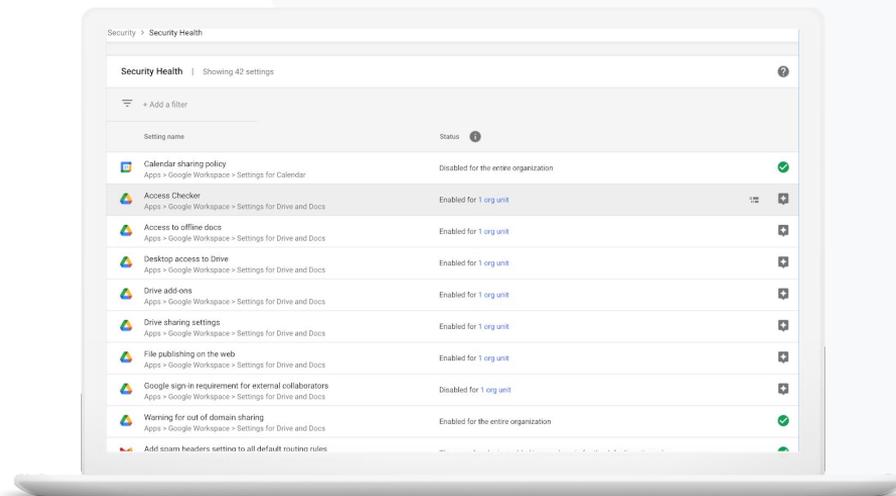


[Detaillierte Anleitung](#)

[Mehr Sicherheit für eine wachsende Bildungseinrichtung](#)



[Detaillierte Anleitung](#)





Ich wünsche mir eine übersichtliche Zusammenfassung der Sicherheitseinstellungen meiner Domain und möchte ausführbare Empfehlungen erhalten, um potenzielle Risiken zu vermeiden.“

[Detaillierte Anleitung](#)

Empfehlungen für Risikobereiche

Auf der Seite **Sicherheitsstatus** wird Ihre Sicherheitskonfiguration geprüft. Gegebenenfalls sehen Sie hier auch Änderungsvorschläge. Außerdem haben Sie folgende Möglichkeiten:

- ✓ Potenzielle Risikobereiche Ihrer Domain im Handumdrehen identifizieren
- ✓ Empfehlungen für optimale Einstellungen erhalten, um die Effektivität der Sicherheitskonfiguration zu verbessern
- ✓ Zusätzliche Informationen und Hilfeartikel zu den Empfehlungen erhalten

 Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)
[Die Funktionen der Seite „Sicherheitsstatus“](#)



“

Ich verwalte zwar unsere Domain, aber wenn ich etwas nicht sehe, kann ich auch nicht darauf reagieren. Daher würde ich gerne sicherstellen, dass alles ordnungsgemäß eingestellt und geschützt ist.“

[Detaillierte Anleitung](#)

Aktuelles zu Best Practices

Auf der Seite **Sicherheitsstatus** wird Ihre Sicherheitskonfiguration geprüft. Gegebenenfalls sehen Sie hier auch Änderungsvorschläge. Außerdem erhalten Sie hier Folgendes:

- ✓ Empfehlungen zu potenziellen Risikobereichen in Ihrer Domain
- ✓ Empfehlungen für optimale Einstellungen, um die Effektivität der Sicherheitskonfiguration zu verbessern
- ✓ Zusätzliche Informationen und Hilfeartikel

 Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)
[Die Funktionen der Seite „Sicherheitsstatus“](#)



Best Practices für Sicherheit

Auf der Seite „Sicherheitsstatus“ finden Sie die Best Practices für Sicherheitsrichtlinien, darunter:

- ✓ Empfehlungen zu potenziellen Risikobereichen in Ihrer Domain
- ✓ Empfehlungen für optimale Einstellungen, um die Effektivität der Sicherheitskonfiguration zu verbessern
- ✓ Direktlinks zu den Einstellungen
- ✓ Zusätzliche Informationen und Hilfeartikel

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Die Funktionen der Seite „Sicherheitsstatus“](#)



Wie lauten die Best Practices oder Empfehlungen für die Einrichtung von Sicherheitsrichtlinien?“

[Detaillierte Anleitung](#)



Sicherheitsstatus

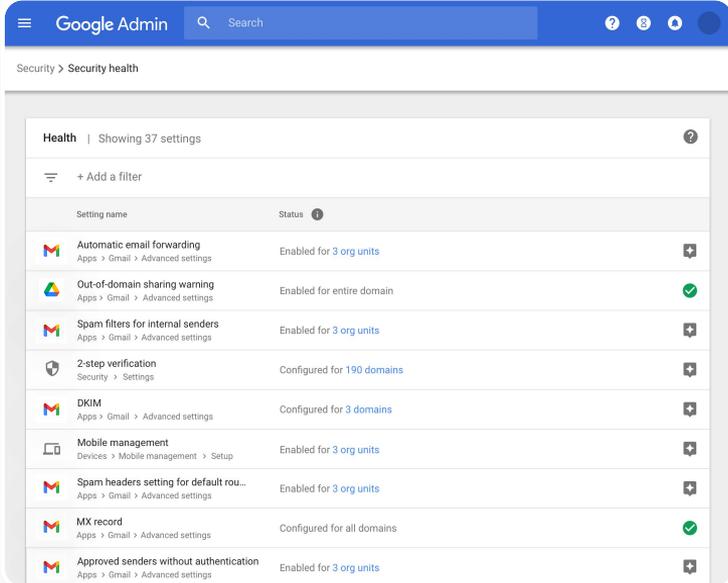


Sicherheits- und Analysetools

Anleitung: Sicherheitsempfehlungen

Empfehlungen ansehen

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf **Sicherheit > Sicherheitsstatus**.
- Den Status sehen Sie in der Spalte ganz rechts.
 - Ein grünes Häkchen bedeutet, dass eine Einstellung sicher ist.
 - Ein graues Symbol bedeutet, dass es für diese Einstellung eine Empfehlung gibt; klicken Sie auf das Symbol, um weitere Informationen und Anleitungen aufzurufen.



Health | Showing 37 settings

+ Add a filter

Setting name	Status
 Automatic email forwarding Apps > Gmail > Advanced settings	Enabled for 3 org units
 Out-of-domain sharing warning Apps > Gmail > Advanced settings	Enabled for entire domain
 Spam filters for internal senders Apps > Gmail > Advanced settings	Enabled for 3 org units
 2-step verification Security > Settings	Configured for 190 domains
 DKIM Apps > Gmail > Advanced settings	Configured for 3 domains
 Mobile management Devices > Mobile management > Setup	Enabled for 3 org units
 Spam headers setting for default rou... Apps > Gmail > Advanced settings	Enabled for 3 org units
 MX record Apps > Gmail > Advanced settings	Configured for all domains
 Approved senders without authentication Apps > Gmail > Advanced settings	Enabled for 3 org units

[↗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Die Funktionen der Seite „Sicherheitsstatus“](#)



“

Ich möchte sicherstellen,
dass meine wachsende
Bildungseinrichtung auch in
Zukunft so gut wie möglich
geschützt ist.“

[Detaillierte Anleitung](#)

Mehr Sicherheit für eine wachsende Bildungseinrichtung

Wenn sie die Daten der Bildungseinrichtung noch besser schützen möchten, sollten IT-Administratoren diesen [Best Practices für die Sicherheit](#) folgen. In der Admin-Konsole finden Sie verschiedene Einstellungen, mit denen sich die Best Practices in dieser Checkliste implementieren lassen.

- ✓ Empfehlungen, anhand derer Sie gehackte Konten leichter vermeiden und wiederherstellen können
- ✓ Anleitungen, wie sich Freigaben und die Zusammenarbeit außerhalb Ihrer Domain einschränken lassen
- ✓ Funktionen, mit denen Sie den Zugriff von Drittanbietern auf Hauptdienste überprüfen können

[↔](#) Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)
[Sicherheits-Checkliste für mittlere und große Unternehmen](#)



Anleitung: Sicherheits-Checkliste

Um Ihre Organisation noch besser zu schützen, wurden viele der in dieser Checkliste empfohlenen Einstellungen als Best Practices für die Sicherheit standardmäßig von Google aktiviert. Besonders die hier aufgelisteten Punkte sollten Sie sich genauer ansehen.

- **Administrator:** Administratorkonten schützen
- **Konten:** Gehackte Konten vermeiden und wiederherstellen
- **Apps:** Zugriff von Drittanbieter-Apps auf Hauptdienste prüfen
- **Kalender:** Externe Kalenderfreigabe einschränken
- **Drive:** Freigabe und Zusammenarbeit außerhalb Ihrer Domain einschränken
- **Gmail:** Authentifizierung und Infrastruktur einrichten
- **Vault:** Vault-Aktivitäten regelmäßig überprüfen

Security best practices

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

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

Administrator ^

Protect admin accounts

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

 Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Integrität der Sicherheitseinstellungen überwachen](#)

Erweiterte Steuerelemente für Administratoren

Beschreibung

Über die Steuerelemente für Administratoren behalten Sie den Überblick und können festlegen, welche Nutzer und Geräte Zugriff auf Ihre Domain und Ihre Daten haben.

Anwendungsfälle

[Datenschutzgesetze](#)



[Detaillierte Anleitung](#)

[Stipendienrichtlinien einhalten](#)



[Detaillierte Anleitung](#)

[App-Zugriffsbeschränkungen](#)



[Detaillierte Anleitung](#)

[Mobilgeräte verwalten](#)

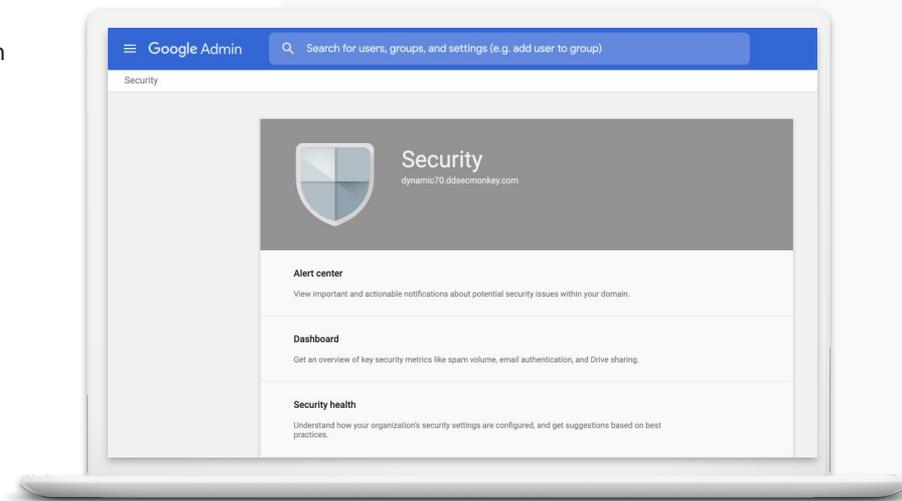


[Detaillierte Anleitung](#)

[Daten migrieren](#)



[Detaillierte Anleitung](#)





Datenschutzgesetze

Als Administrator können Sie mit einer **Richtlinie für Speicherorte** festlegen, dass Daten an einem bestimmten Ort gespeichert werden (USA oder Vereinigtes Königreich/Europa).

- ✓ Sie können bei Bedarf für bestimmte Nutzer einen Speicherort für Daten festlegen oder für bestimmte Abteilungen bzw. Teams unterschiedliche Speicherorte für Daten festlegen.
- ✓ Nutzer lassen sich in einer Organisationseinheit zusammenfassen, um den Speicherort für Daten auf Abteilungsebene auszuwählen. Alternativ können Sie sie auch einer Konfigurationsgruppe zuordnen, um einen Datenspeicherort für eine Gruppe von Nutzern aus verschiedenen Abteilungen oder innerhalb einer Abteilung festzulegen.
- ✓ Nutzer, denen keine Lizenz für Education Standard oder Education Plus zugewiesen wurde, werden von den Richtlinien für Speicherorte nicht abgedeckt.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Speicherorte für Daten: Standort für Ihre Daten auswählen](#)



Die Daten der Lernenden, des Lehrpersonals und der Mitarbeiter an meiner Bildungseinrichtung müssen laut Datenschutzgesetz in den USA bleiben.“

[Detaillierte Anleitung](#)



“

Laut Stipendienrichtlinien darf die gesamte Forschungsarbeit, die an meiner Fakultät geleistet wird, die USA nicht verlassen.“

[Detaillierte Anleitung](#)

Stipendienrichtlinien einhalten

Richtlinie für Speicherorte: Als Administrator können Sie festlegen, dass die Forschungsarbeit Ihrer Fakultät an einem bestimmten Ort gespeichert wird (USA oder Europa).

- ✓ Die Richtlinien für Speicherorte gelten für die primären ruhenden Daten (einschließlich Sicherungen) der meisten Hauptdienste von Google Workspace for Education, siehe [diese Liste](#).
- ✓ Beachten Sie beim Festlegen der Richtlinien für Speicherorte, dass Nutzer außerhalb der Region, in der ihre Daten gespeichert sind, in einigen Fällen unter Umständen eine höhere Latenz bemerken.



Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Speicherorte für Daten: Standort für Ihre Daten auswählen](#)



Anleitung: Speicherorte für Daten*

Speicherorte für Daten festlegen

- Melden Sie sich in der Admin-Konsole an.
 - Hinweis: Sie müssen als Super Admin angemeldet sein.
- Klicken Sie auf Unternehmensprofil > Mehr anzeigen > Speicherorte für Daten.
- Wählen Sie die Organisationseinheit oder Konfigurationsgruppe aus, die Sie auf einen Datenspeicherort beschränken wollen, oder markieren Sie die gesamte Spalte, um alle Einheiten und Gruppen auszuwählen.
- Wählen Sie den gewünschten Speicherort für Daten aus: „Keine Präferenz“, „USA“ oder „Europa“.
- Klicken Sie auf Speichern.

* Ausschließlich Institutionen, die Education Standard oder Education Plus nutzen, können ihre Daten mit der Funktion „Speicherorte für Daten“ in einer bestimmten Region speichern.

 Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Speicherorte für Daten: Standort für Ihre Daten auswählen](#)



App-Zugriffsbeschränkungen

Über die Einstellung **Kontextsensitiver Zugriff*** können Sie detaillierte Richtlinien für die Zugriffssteuerung auf Grundlage von Attributen wie Nutzer-ID, Standort, Sicherheitsstatus des Geräts oder IP-Adresse erstellen. Sie haben sogar die Möglichkeit, den Zugriff auf Apps außerhalb des Netzwerks einzuschränken.

- ✓ Die Richtlinien für den kontextsensitiven Zugriff lassen sich auf die Hauptdienste von Google Workspace for Education anwenden.
- ✓ Wenn sich beispielsweise ein Nutzer an seiner Einrichtung in einem Hauptdienst von Google Workspace anmeldet und dann in ein Café geht, wird eine Richtlinie ausgelöst, sobald er den Standort wechselt, und darüber der kontextsensitive Zugriff für diesen Dienst noch einmal geprüft.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Kontextsensitiver Zugriff](#)

[Apps kontextsensitive Zugriffsebenen zuweisen](#)



Ich möchte den Zugriff
auf bestimmte Apps
beschränken, wenn
Nutzer sich im Netzwerk
befinden.“

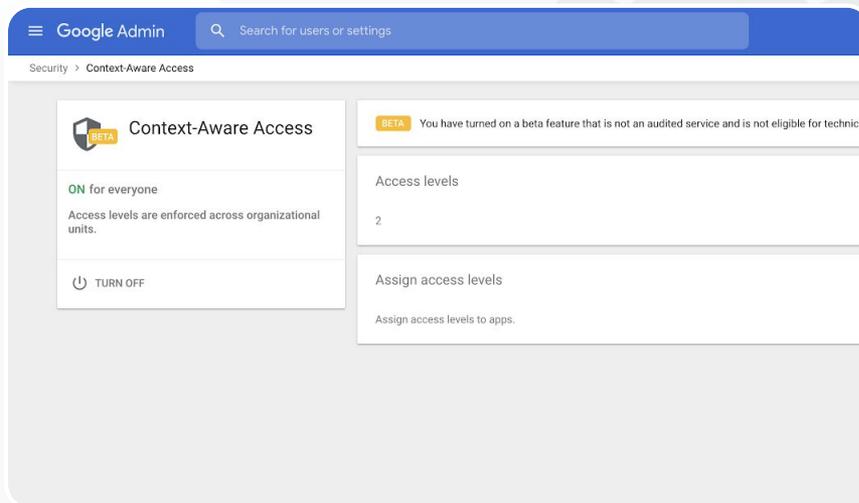
[Detaillierte Anleitung](#)

* Ausschließlich Institutionen, die Education Standard oder Education Plus nutzen, können kontextsensitive Richtlinien anwenden.

Anleitung: Kontextsensitiver Zugriff

Kontextsensitiven Zugriff nutzen

- Melden Sie sich in der Admin-Konsole an.
- Klicken Sie auf Sicherheit > Kontextsensitiver Zugriff > Zuweisen.
- Um eine Liste der Apps aufzurufen, wählen Sie **Zugriffsebenen zuweisen** aus.
- Wenn Sie die Liste sortieren möchten, wählen Sie eine **Organisationseinheit** oder **Konfigurationsgruppe** aus.
- Wählen Sie neben der App, die Sie anpassen möchten, **Zuweisen** aus.
- Wählen Sie eine oder mehrere Zugriffsebenen aus.
- Wenn Nutzer mehr als eine Bedingung erfüllen sollen, erstellen Sie mehrere Ebenen.
- Klicken Sie auf „Speichern“.



[↗](#) Weiterführende Informationen in der [Google Workspace-Admin-Hilfe](#)
[Kontextsensitiver Zugriff](#)
[Apps kontextsensitive Zugriffsebenen zuweisen](#)



Mobilgeräte verwalten

Mit der erweiterten **Mobilgeräteverwaltung** haben Sie mehr Einstellungsmöglichkeiten für die Daten Ihrer Organisation auf Mobilgeräten. Sie können Mobilgerätefunktionen einschränken, die Geräteverschlüsselung erzwingen, Apps auf Android- und iOS-Geräten wie iPhones und iPads verwalten sowie Daten von einem Gerät löschen.

- ✔ Sie können über die Admin-Konsole Geräte genehmigen, löschen, blockieren oder Blockierungen aufheben.
- ✔ Wenn ein Nutzer sein Gerät verloren oder die Institution verlassen hat, können Sie sein Konto, Profil oder alle Daten aus dem verwalteten Modul des Geräts löschen. Die Daten wären auf einem Computer oder über einen Webbrowser weiterhin verfügbar.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe
[Erweiterte Mobilgeräteverwaltung einrichten](#)
[Verwaltete Geräte genehmigen, löschen oder blockieren sowie Blockierungen aufheben](#)
[Unternehmensdaten von einem Gerät löschen](#)



Ich möchte in meinem Bereich Richtlinien auf jede Art von Gerät (z. B. iOS oder Windows 10) anwenden und für den gesamten Pool verwalten können – nicht nur für Chromebooks. Das gilt besonders bei gehackten Geräten.“

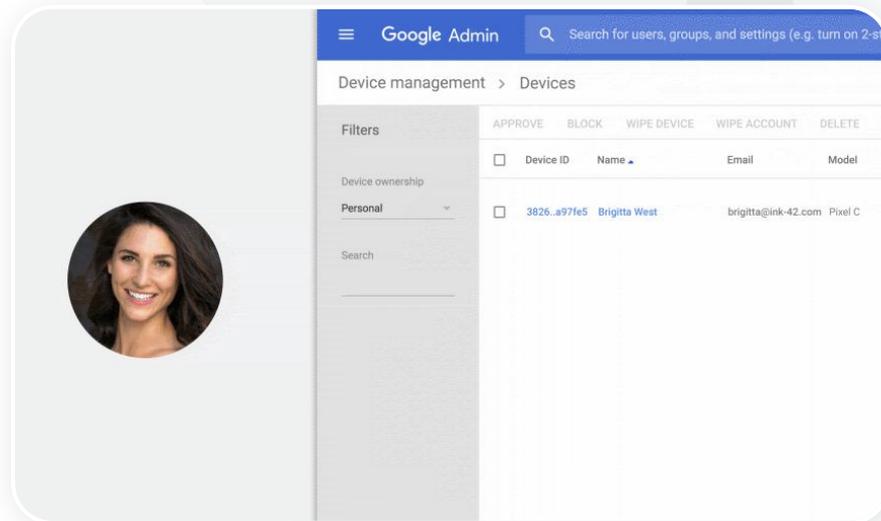
[Detaillierte Anleitung](#)



Anleitung: Erweiterte Mobilgeräteverwaltung aktivieren

Aktivierung

- Melden Sie sich in der Admin-Konsole an.
- Wählen Sie in der Admin-Konsole > Geräte aus.
- Klicken Sie links auf Einstellungen > Universelle Einstellungen.
- Klicken Sie auf Allgemein > Mobilgeräteverwaltung.
- Wenn die Einstellung für alle Nutzer gelten soll, verwenden Sie die oberste Organisationseinheit (bereits ausgewählt). Geben Sie andernfalls eine untergeordnete Organisationseinheit an.
- Wählen Sie Erweitert aus.
- Klicken Sie auf Speichern.



[↗](#) Weiterführende Informationen in der Google
Workspace-Admin-Hilfe

[Erweiterte Mobilgeräteverwaltung einrichten](#)
[Verwaltete Geräte genehmigen, löschen oder
blockieren sowie Blockierungen aufheben](#)
[Unternehmensdaten von einem Gerät löschen](#)



Daten migrieren

Mithilfe der **Migrationsanleitungen** können Sie alle Daten Ihrer Organisation ganz einfach zu Google Workspace migrieren – von E-Mails über Kalender und Kontakte bis hin zu Ordnern, Dateien und Berechtigungen.

Daten von < 1.000 Nutzern

- ✓ Die Produktmatrix gibt Ihnen einen guten Überblick darüber, welche Lösung sich am besten für Ihre Bildungseinrichtung eignet.

[Weitere Informationen](#)

Daten von > 1.000 Nutzern

- ✓ Mithilfe von Google Workspace Migrate können Sie sicherstellen, dass große Datenmengen effektiv migriert werden.

[Weitere Informationen](#)

[↗](#) Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Daten Ihrer Organisation in Google Workspace migrieren](#)
[Produktmatrix der Migrationstools für Google Workspace](#)
[Über Google Workspace Migrate](#)
[Google Workspace Migrate: Installation und Einrichtung](#)



Wir wechseln zu Google Workspace und müssen all unsere Daten in die neue Google-Umgebung migrieren.“

[Detaillierte Anleitung](#)

Anleitung: Google Workspace Migrate

Hinweis

Melden Sie sich für die [Betaversion](#) an und prüfen Sie, ob Sie die [Systemvoraussetzungen](#) erfüllen.

Anleitung

1. Google Cloud Console einrichten

[APIs aktivieren](#)

[OAuth-Webclient-ID erstellen](#)

[Google Workspace-Dienstkonto erstellen](#)

2. Admin-Konsole einrichten

[Administratorrollen einrichten](#)

[Client-ID autorisieren](#)

3. Herunterladen und installieren

[Installationsprogramme herunterladen](#)

[Datenbanken installieren](#)

[Plattform installieren und einrichten](#)

[Knotenserver installieren](#)

[Optionale Einrichtungsschritte für Knotenserver](#)

4. Migrationstool einrichten

[Verschlüsselungsschlüssel einrichten](#)

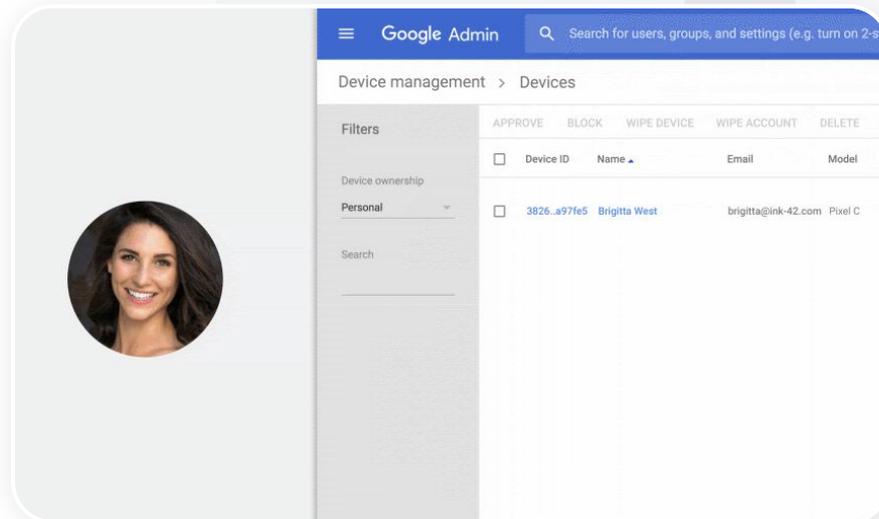
[Datenbankeinstellungen konfigurieren](#)

[Callback-Adresse konfigurieren](#)

[Knotenserver hinzufügen](#)

[Projekt erstellen](#)

Benötigen Sie Hilfe? Wenden Sie sich an einen [Google Cloud-Partner](#).



 Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Über Google Workspace Migrate](#)

[Google Workspace Migrate: Installation und Einrichtung](#)

[Daten Ihrer Organisation in Google Workspace migrieren](#)

[Produktmatrix der Migrationstools für Google Workspace](#)



Tools zum Unterrichten und Lernen

Dank erweiterten Funktionen für die digitale Lernumgebung sind Ihre Lehrkräfte besser ausgestattet, z. B. durch bessere Videokommunikation und mehr Interaktionsmöglichkeiten mit Lernenden sowie Tools zur Förderung der akademischen Integrität.



[Plagiatsberichte](#)



[Google Meet](#)

Plagiatsberichte

Beschreibung

Lehrkräfte und Lernende können Aufgaben auf Plagiate hin prüfen. Das Tool vergleicht Aufgaben von Kursteilnehmern mithilfe der Google-Suche mit Milliarden von Webseiten und Millionen von Büchern. Erkannte Webseiten werden dabei verlinkt und nicht als Zitat gekennzeichnete Textstellen markiert.

Anwendungsfälle

[Plagiate finden](#)

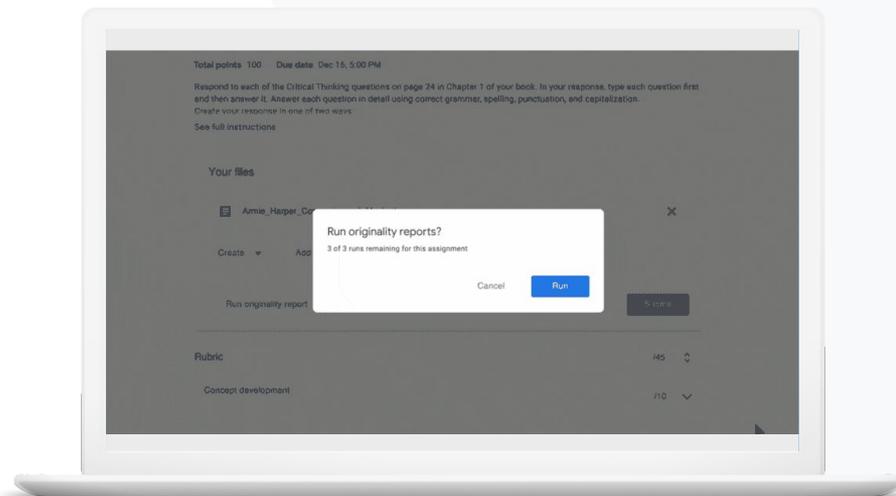


[Detaillierte Anleitung](#)

[Plagiatsprüfungen als
Anstoß zum Lernen](#)



[Detaillierte Anleitung](#)



Plagiate finden

Lehrkräfte können die akademische Integrität bei Aufgaben von Schülern oder Studenten mithilfe von **Plagiatsberichten** prüfen. Das Tool vergleicht Aufgaben von Lernenden mithilfe der Google-Suche mit Milliarden von Webseiten und Millionen von Büchern.

- ✓ Lehrkräfte, die das Teaching and Learning Upgrade oder Education Plus verwenden, haben unbeschränkten Zugriff auf Plagiatsberichte.
- ✓ Plagiatsberichte sind derzeit nur verfügbar für:
 - Google-Konten, für die als Sprache Englisch ausgewählt wurde
 - Aufgaben, die in Google Docs geschrieben wurden
 - Google for Education-Konten

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Plagiatsberichte aktivieren](#)



Ich möchte die Aufgaben meiner Lernenden auf Plagiate oder inkorrekte Zitate prüfen.“

[Detaillierte Anleitung](#)

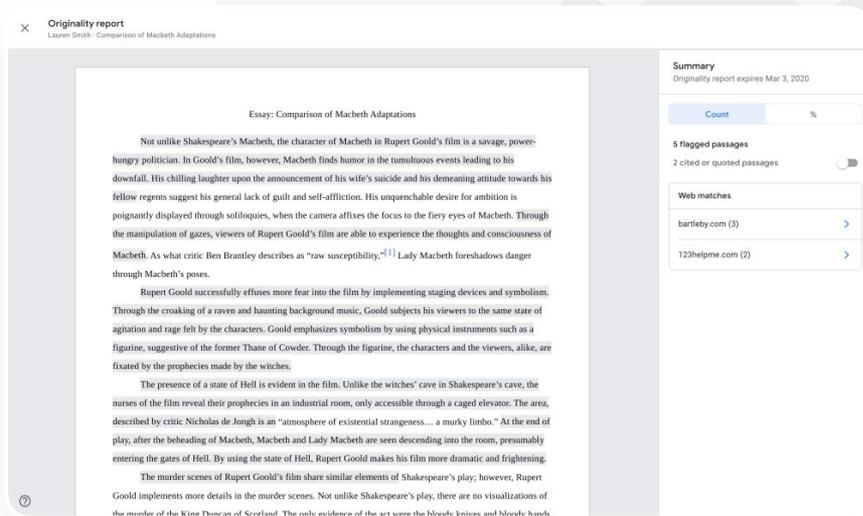
Anleitung: Nachkontrolle durch die Lehrkraft

Plagiatsberichte für eine Aufgabe aktivieren

- Melden Sie sich in Ihrem Classroom-Konto an:
classroom.google.com
- Wählen Sie die entsprechende Klasse aus der Liste aus und anschließend **Kursaufgaben**.
- Wählen Sie **Erstellen > Aufgabe** aus.
- Setzen Sie ein Häkchen bei **Plagiatsprüfung (Echtheit)**, um sie zu aktivieren.

Plagiatsprüfung durchführen

- Wählen Sie die Datei eines Schülers oder Studenten aus der Liste aus und klicken Sie darauf, um sie im Benotungstool zu öffnen.
- Klicken Sie unterhalb der Aufgabe des Lernenden auf **Plagiatsbericht erstellen**.



Originality report
Lizbeth Smith - Comparison of Macbeth Adaptations

Essay: Comparison of Macbeth Adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth finds humor in the tumultuous events leading to his downfall. His chilling laughter upon the announcement of his wife's suicide and his demeaning attitude towards his fellow regents suggest his general lack of guilt and self-affliction. His unquenchable desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gazes, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility,"¹¹ Lady Macbeth foreshadows danger through Macbeth's poses.

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

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

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

Summary
Originality report expires Mar 3, 2020

Count %

5 flagged passages
2 cited or quoted passages

Web matches

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

[↗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe
[Plagiatsberichte aktivieren](#)

Plagiatsprüfungen als Anstoß zum Lernen

Schüler und Studenten können einen **Plagiatsbericht** erstellen, um fehlende Zitatangaben und unbeabsichtigte Plagiate zu erkennen, bevor sie ihre Aufgaben einreichen – bis zu dreimal pro Aufgabe. Bei Plagiatsberichten werden die Dokumente mit zahlreichen Quellen abgeglichen und fehlende Zitatangaben markiert. So haben Lernende die Chance, sich zu verbessern, Fehler zu korrigieren und ihre Aufgaben mit Selbstvertrauen abzugeben.

- ✓ Sowohl im Teaching and Learning Upgrade als auch in Education Plus können Lehrkräfte Plagiatsberichte so oft aktivieren, wie sie möchten – in Education Fundamentals dagegen maximal bis zu fünfmal pro Klasse.
- ✓ Nachdem eine Aufgabe eingereicht wurde, erstellt Classroom ganz automatisch einen Bericht, den nur die Lehrkraft sehen kann. Wird eine Aufgabe zurückgezogen und noch einmal abgeben, wird in Classroom ein weiterer Plagiatsbericht für die Lehrkraft erstellt.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Plagiatsberichte erstellen](#)



Ich möchte, dass meine Schüler ihre Aufgaben auf Plagiate prüfen können, indem ich die ‚Schummelerkennung‘ als Anstoß zum Lernen nutze.“

[Detaillierte Anleitung](#)

Anleitung: Vorabprüfung durch den Lernenden

So können Schüler und Studenten Plagiatsberichte erstellen

- Im Classroom-Konto anmelden: classroom.google.com
- Die entsprechende Klasse aus der Liste und anschließend **Kursaufgaben** auswählen
- Die relevante Aufgabe aus der Liste auswählen und auf **Aufgabe ansehen** klicken
- Unter **Meine Aufgaben** eine Datei hochladen oder erstellen
- Neben **Plagiatsberichte auf Ausführen** klicken
- Um den Bericht zu öffnen, unter dem Dateinamen der Aufgabe auf **Plagiatsbericht ansehen** klicken
- Um die Aufgabe zu überarbeiten, unten auf **Bearbeiten** klicken

Essay: Comparison of Macbeth adaptations

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

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

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

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

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

Web matches > sparksnotes.com ✕

STUDENT'S PASSAGE

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

[Comment](#)

TOP MATCH

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

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

[↗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Plagiatsberichte erstellen](#)

Google Meet

Beschreibung

Die erweiterten Funktionen von Google Meet beinhalten u. a. Livestreaming, Breakouts, in Drive gespeicherte Aufzeichnungen von Videokonferenzen, Teilnahmeberichte und Videokonferenzen mit bis zu 250 Teilnehmern.

Anwendungsfälle

[Sichere Videokonferenzen](#)



[Detaillierte Anleitung](#)

[Mehr Sicherheit bei Videokonferenzen](#)



[Detaillierte Anleitung](#)

[Unterrichtseinheiten aufzeichnen](#)



[Detaillierte Anleitung](#)

[Fakultätsbesprechungen aufzeichnen](#)



[Detaillierte Anleitung](#)

[Verpasste Unterrichtseinheiten](#)



[Detaillierte Anleitung](#)

[Livestreaming von Videokonferenzen](#)



[Detaillierte Anleitung](#)

[Livestreaming von Schulveranstaltungen](#)



[Detaillierte Anleitung](#)

[Fragen stellen](#)



[Detaillierte Anleitung](#)

[Feedback sammeln](#)



[Detaillierte Anleitung](#)

[Kleine Schüler-/ Studentengruppen](#)



[Detaillierte Anleitung](#)

[Teilnahme erfassen](#)



[Detaillierte Anleitung](#)

Sichere Videokonferenzen

Mit Google Meet können Bildungseinrichtungen die gleiche sichere Infrastruktur, den gleichen integrierten Schutz und das gleiche globale Netzwerk nutzen, die Google zum Schutz Ihrer Daten und Ihrer Privatsphäre verwendet. Mit Google Meet profitieren Sie von den folgenden Sicherheitsmaßnahmen:

- ✓ **Datenschutz und Compliance:** Strenge Bildungsstandards für die Sicherheit von Lernenden und der Bildungseinrichtung
- ✓ **Verschlüsselung:** Alle Daten zwischen dem Client und Google sind verschlüsselt
- ✓ **Maßnahmen gegen Missbrauch:** Der Moderator kann die Teilnahme kontrollieren und sicherstellen, dass nur berechnigte Personen teilnehmen
- ✓ **Sichere Bereitstellung, geschützter Zugriff und sicherheitsbezogene Steuerelemente:** Dank mehrstufiger Sicherheitsvorkehrungen sind Videokonferenzen privat und sicher
- ✓ **Reaktion auf Vorfälle:** Bestandteil des allgemeinen Sicherheits- und Datenschutzprogramms von Google und der Schlüssel zur Einhaltung globaler Datenschutzbestimmungen
- ✓ **Zuverlässigkeit:** Eine mehrstufige cloudnative Infrastruktur, die auf Skalierbarkeit ausgelegt ist und flexibel auf Auslastungsspitzen reagieren kann
- ✓ **Teilnahmeüberblick behalten:** Verbesserte Anklopfunktion, z. B. die Verwaltung vieler Anfragen gleichzeitig oder das automatische Blockieren von Anfragen, die bestimmten Kriterien entsprechen
- ✓ **Sperrkontrollen:** Moderatoren können festlegen, wer während einer virtuellen Videokonferenz chatten, etwas präsentieren oder sprechen darf



Wie sicher ist Google Meet wirklich?“

[Detaillierte Anleitung](#)



Wie kann ich das Abhalten von Videokonferenzen für meine Bildungseinrichtung noch sicherer machen?“

[Detaillierte Anleitung](#)

Mehr Sicherheit bei Videokonferenzen

Das Teaching and Learning Upgrade und Education Plus beinhalten zusätzliche Maßnahmen gegen Missbrauch wie Genehmigungen für externe Teilnehmer, verbesserte Steuerelemente für die Moderation von Videokonferenzen sowie **Besprechungen mit Alias** – zum Schutz vor Wiederverwendung beendeter Videokonferenzen. Sobald der letzte Teilnehmer die Konferenz verlassen hat, kann niemand mehr daran teilnehmen. Schüler bzw. Studenten können erst dann wieder teilnehmen, wenn eine Lehrkraft diese Videokonferenz neu startet.

- ✓ Dank **Besprechungen mit Alias** kann niemand mehr an einer Konferenz teilnehmen, sobald der letzte Teilnehmer sie verlassen hat – auch der zehnstellige Besprechungscode wird danach ungültig.
- ✓ Schüler bzw. Studenten können erst dann wieder teilnehmen, wenn eine Lehrkraft diese Videokonferenz neu startet.
- ✓ Lehrkräfte können eine Videokonferenz für alle Teilnehmer beenden – so wird verhindert, dass jemand zurückbleibt, nachdem die Lehrkraft die Konferenz verlassen hat.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Sicherheit und Datenschutz in Meet für Bildungseinrichtungen](#)

[Google Meet-Videokonferenzen starten oder planen](#)

Anleitung: Besprechungen mit Alias

Besprechung mit Alias erstellen

- Verwenden Sie einen kurzen Link wie [g.co/meet/\[ALIAS EINGEBEN\]](https://g.co/meet/[ALIAS EINGEBEN])
- Öffnen Sie meet.google.com oder die mobile Meet-App und geben Sie im Feld **Besprechung starten oder beitreten** einen Alias für die Besprechung ein.

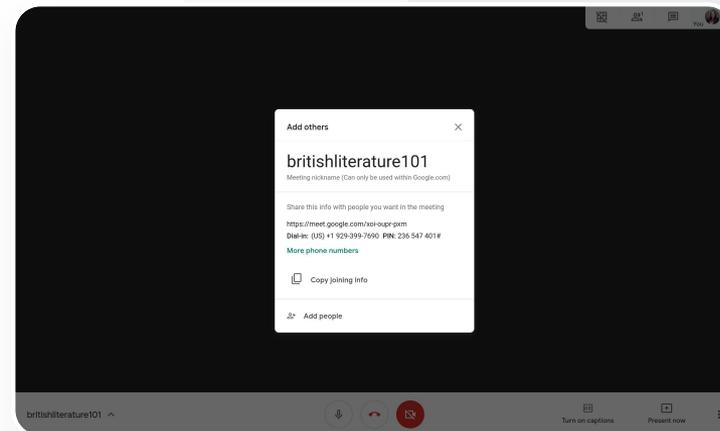
Funktionsweise

Wenn eine Lehrkraft eine Besprechung mit Alias startet, wird ein zehnstelliger Besprechungscode erstellt. Dieser ist vorübergehend mit dem Alias verknüpft.

Sobald die letzte Person die Videokonferenz verlassen oder die Lehrkraft sie beendet hat, laufen der vorübergehende Besprechungscode und die Verknüpfung zwischen dem Alias und dem Besprechungscode ab.

Wenn Schüler oder Studenten keine Berechtigung zum Erstellen von Videokonferenzen haben, können sie danach weder den Alias noch den Besprechungscode verwenden.

Lehrkräfte können den Alias wiederverwenden, wodurch ein neuer vorübergehender Besprechungscode erstellt wird. Dann können die Schüler und Studenten über den Alias wieder teilnehmen.



[↗](#) Weiterführende Informationen in der **Google Workspace-Admin-Hilfe**

[Sicherheit und Datenschutz in Meet für Bildungseinrichtungen](#)

[Google Meet-Videokonferenzen starten oder planen](#)



Unsere Einrichtung bietet große Onlinekurse an, die wir für den Fernunterricht oder für verhinderte Teilnehmer aufzeichnen müssen.“

[Detaillierte Anleitung](#)

Unterrichtseinheiten aufzeichnen

Mit dem Teaching and Learning Upgrade sowie Education Plus können Nutzer ihre Videokonferenzen **aufzeichnen** und sie automatisch und unbefristet in Google Drive speichern. So ist das Archivieren und Teilen von Lektionen, Workshops und Arbeitssitzungen kinderleicht.

- ✓ Sofern Classroom verwendet wird, können Lehrkräfte für jeden Kurs einen separaten Link zu Meet erstellen, der im Classroom-Stream und auf der Seite „Kursaufgaben“ zu sehen ist.
- ✓ Über diesen Link lassen sich im Kurs Videokonferenzen starten, die für Lehrkräfte und Schüler oder Studenten ganz leicht zugänglich sind.
- ✓ Mit dieser Integration lassen sich Lektionen nahtlos aufzeichnen.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Meet für den Fernunterricht nutzen](#)

Fakultätsbesprechungen aufzeichnen

Mit dem Teaching and Learning Upgrade sowie Education Plus werden **Aufzeichnungen** von Videokonferenzen automatisch in Google Drive gespeichert – und zwar so lange, wie der Nutzer sie benötigt. Damit wird das Archivieren und Teilen von Besprechungen, Kursen für die berufliche Weiterbildung sowie Vorstandssitzungen zum Kinderspiel.

- ✓ Es wird empfohlen, die Funktion zum Aufzeichnen ausschließlich für Mitglieder Ihrer Fakultät und Mitarbeiter zu aktivieren.
- ✓ Sie können jeweils eigene Organisationseinheiten für Lehrkräfte bzw. für Schüler und Studenten erstellen – dann legen Sie entsprechend unterschiedliche Zugriffsberechtigungen fest.
- ✓ Falls Sie Classroom nutzen, können Sie bestätigten Lehrkräften auch über Ihre Google Classroom-Gruppe Zugriff gewähren.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Meet für den Fernunterricht nutzen](#)



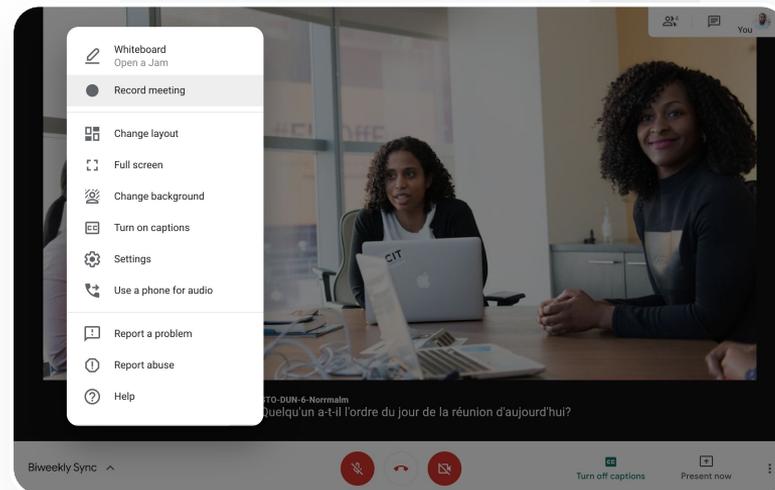
Wir halten regelmäßig Videokonferenzen mit unseren Mitarbeitern ab, die allesamt aufgezeichnet werden müssen. Außerdem möchten wir Kurse für die berufliche Weiterbildung und unsere Vorstandssitzungen aufzeichnen.“

[Detaillierte Anleitung](#)

Anleitung: Aufzeichnung

Eine Videokonferenz aufzeichnen

- Öffnen Sie die Videokonferenz aus Ihrem Kalender heraus und wählen Sie **Mit Google Meet teilnehmen** aus.
- Öffnen Sie auf der Bestätigungsseite für die Videokonferenz das **Optionsmenü**, indem Sie die drei vertikal angeordneten Punkte in der rechten unteren Ecke auswählen.
- Klicken Sie auf **Videokonferenz aufzeichnen**, woraufhin ein roter Punkt in der rechten unteren Ecke des Bildschirms erscheint; dieser zeigt an, dass die Konferenz nun aufgezeichnet wird.
- Eine Videodatei der Konferenz wird automatisch in Google Drive gespeichert.



[🔗 Weiterführende Informationen in der Google Workspace-Admin-Hilfe](#)

[Meet für den Fernunterricht nutzen](#)



Ich möchte eine
aufgezeichnete Lektion
von dem Tag ansehen, an
dem ich verhindert war.“

[Detaillierte Anleitung](#)

Verpasste Unterrichtseinheiten

Alle Nutzer haben Zugriff auf den Google Drive-Speicherplatz in der Domain der Bildungseinrichtung. Außerdem werden Aufzeichnungen von Videokonferenzen mit dem Teaching and Learning Upgrade sowie Education Plus automatisch im Drive-Ordner des Organizers der Videokonferenz gespeichert. Um die aufgezeichnete Videokonferenz noch einmal abzuspielen, können Sie den Organizer nach dem Aufzeichnungslink fragen oder über den Kalendertermin darauf zugreifen.

- ✓ Aufzeichnungen werden im Drive-Ordner des Organizers der Videokonferenz gespeichert.
- ✓ Teilnehmer aus derselben Organisationseinheit wie der Organizer erhalten automatisch Zugriff auf die Aufzeichnung.
- ✓ Wenn sich der Organizer der Videokonferenz ändert, wird der Aufzeichnungslink an den ursprünglichen Terminersteller gesendet.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Videokonferenzen aufzeichnen](#)

Anleitung: Aufzeichnungen ansehen und freigeben

Aufzeichnung freigeben

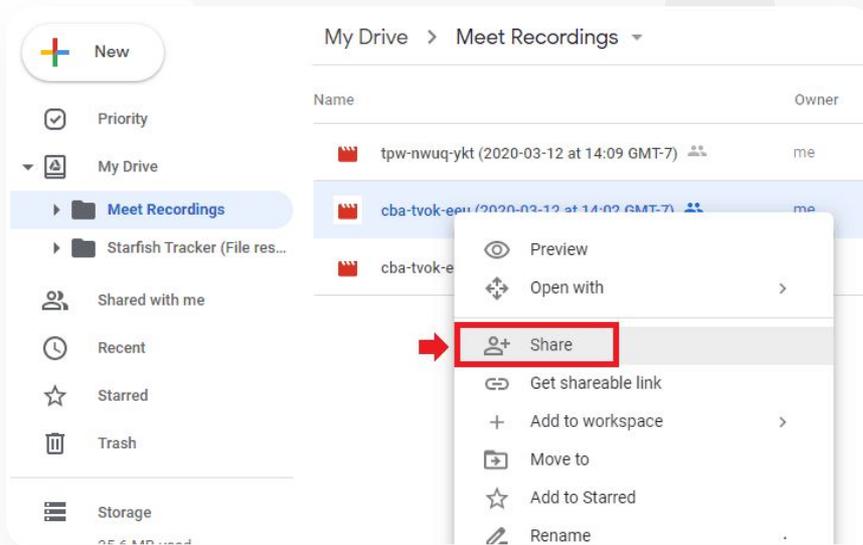
- Wählen Sie die Datei aus.
 - Klicken Sie auf **Freigeben**.
 - Fügen Sie die genehmigten Betrachter hinzu.
- ODER**
- Wählen Sie das **Linksymbol** aus.
 - Fügen Sie den Link in eine E-Mail oder Chat-Nachricht ein.

Eine Aufzeichnung herunterladen

- Wählen Sie die Datei aus.
- Klicken Sie auf das **Dreistrich-Menü** und wählen Sie **Herunterladen** aus.
- Um die heruntergeladene Datei abzuspielen, **doppelklicken Sie darauf**.

Eine Aufzeichnung aus Google Drive abspielen

- Doppelklicken Sie auf die Aufzeichnungsdatei in Drive, um sie abzuspielen; es wird die Meldung „Verarbeitung läuft noch“ angezeigt, bis die Datei online zum Ansehen verfügbar ist.
- Um eine Aufzeichnung zu Drive hinzuzufügen, klicken Sie auf **Zu ‚Meine Ablage‘** hinzufügen.



[Weiterführende Informationen in der Google Workspace-Admin-Hilfe Videokonferenzen aufzeichnen](#)



Wir möchten in der Lage sein, unsere Mitarbeiter- und Fakultätsbesprechungen den Eltern und zusätzlichen Interessenvertretern im Livestream zu zeigen.“

[Detaillierte Anleitung](#)

Livestreaming von Videokonferenzen

Mit dem Teaching and Learning Upgrade lassen sich Livestreams mit bis zu 10.000 Zuschauern in der Domain realisieren, während bei Education Plus Livestreams mit bis zu 100.000 Zuschauern in der Domain möglich sind. Personen können teilnehmen, indem sie auf den Livestream-Link klicken, der ihnen per E-Mail oder Kalendereinladung vom Organisator bereitgestellt wurde. Arbeiten Sie mit Ihrem IT-Administrator zusammen, um sicherzustellen, dass Sie über Livestream-Berechtigungen verfügen.

- ✓ Es wird empfohlen, das Livestreaming ausschließlich für Mitglieder Ihrer Fakultät und Mitarbeiter zu aktivieren.
- ✓ Bei sehr großer Teilnehmerzahl bietet sich ein Livestream statt einer interaktiven Videokonferenz an.
- ✓ Sollte ein Nutzer den Livestream verpassen, kann er ihn noch einmal ansehen, nachdem die Videokonferenz beendet wurde.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Meet für den Fernunterricht nutzen](#)

Livestreaming von Schulveranstaltungen

Sie können Veranstaltungen per **Livestream** direkt an alle in Ihrer Bildungseinrichtung übertragen. Das geht ganz einfach über den Link des Livestreams, den Sie vom Organisator der Veranstaltung per E-Mail oder als Kalendertermin erhalten. Arbeiten Sie mit Ihrem IT-Administrator zusammen, um sicherzustellen, dass Sie über Livestream-Berechtigungen verfügen. Sie können den Livestream auch [noch einmal abspielen](#), nachdem die Übertragung beendet wurde.

- ✓ Mithilfe der Google Meet-Livestream-Funktionen können alle Mitglieder Ihrer gesamten Bildungseinrichtung an Abschlussfeiern, Sportveranstaltungen oder Schulkonferenzen teilhaben.
- ✓ Livestreams mit dem Teaching and Learning Upgrade sind mit bis zu 10.000 Zuschauern in der Domain möglich – bei Education Plus sogar mit bis zu 100.000 Zuschauern.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Meet für den Fernunterricht nutzen](#)



Wir möchten Personen, die nicht persönlich teilnehmen können, Livestreams unserer besonderen Ereignisse wie Sportveranstaltungen oder Abschlussfeiern bieten.“

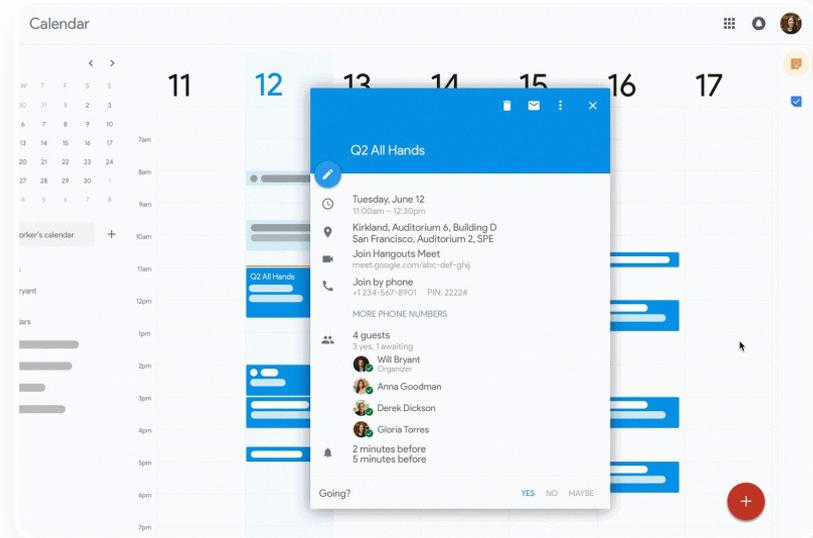
[Detaillierte Anleitung](#)

Anleitung: Livestream

Einen Livestream genehmigen

- Öffnen Sie **Google Kalender**.
- Klicken Sie auf **Erstellen > Weitere Optionen**.
- Geben Sie Termindetails wie Datum und Uhrzeit ein.
- Fügen Sie bis zu 250 Gäste hinzu, die vollständig an der Videokonferenz teilnehmen können – sie werden gesehen, gehört und können Inhalte präsentieren; außerdem lassen sich auch Personen aus anderen Organisationen hinzufügen.
- Klicken Sie auf **Videokonferenz hinzufügen > Meet**.
- Wählen Sie den **Abwärtspfeil** neben „An Videokonferenz teilnehmen“ aus und klicken Sie anschließend auf **Livestream hinzufügen**.
- Um so viele domaininterne Personen einzuladen, wie Ihre kostenpflichtige Version es erlaubt, klicken Sie auf **Kopieren**. Sie können den Livestreamlink dann per E-Mail oder Chatnachricht teilen.
- Klicken Sie auf **Speichern**.
- Das Livestreaming startet nicht automatisch. Wählen Sie dafür während der Videokonferenz **Mehr > Streaming starten**.

Hinweis: Nur Gäste aus Ihrer Organisation können sich den Livestream ansehen.



[↗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe
[Meet für den Fernunterricht nutzen](#)



Ich suche eine einfache Möglichkeit, Fragen zu stellen, das Wissen der Lernenden einzuschätzen und mit der Klasse zu interagieren, damit sie weiterhin motiviert bleibt.“

[Detaillierte Anleitung](#)

Fragen stellen

Die Google Meet-Funktion **Fragen und Antworten** sorgt dafür, dass Lernende motiviert bleiben und die Klasse interaktiver mitarbeiten kann. Lehrkräfte erhalten am Ende der virtuellen Klasse einen detaillierten Bericht mit allen Fragen und Antworten.

- ✓ Moderatoren können so viele Fragen stellen, wie sie möchten. Sie können Fragen filtern und sortieren, sie als beantwortet markieren, priorisieren oder sogar ausblenden.
- ✓ Nach jedem Meeting, in dem Fragen aktiviert wurden, wird per E-Mail automatisch ein Bericht an den Moderator gesendet.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Teilnehmern in Google Meet Fragen stellen](#)

Anleitung: Fragen und Antworten

Frage stellen

- Klicken Sie während einer Videokonferenz in der oberen rechten Ecke auf das **Aktivitätssymbol** > **Fragen**. (Wählen Sie zum Aktivieren **Fragen und Antworten aktivieren** aus.)
- Wenn Sie eine Frage stellen möchten, klicken Sie in der rechten unteren Ecke auf **Eine Frage stellen**.
- Geben Sie Ihre Fragen ein > wählen Sie **Posten** aus.

Bericht mit Fragen ansehen

- Nach der Videokonferenz erhält der Moderator per E-Mail einen Bericht mit den Fragen.
- Öffnen Sie die E-Mail > Klicken Sie auf den **Anhang**.



[↗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Teilnehmern in Google Meet Fragen stellen](#)



Ich möchte auf einfache Weise Feedback von Lernenden und Lehrkräften sammeln, während ich einen Kurs oder eine Mitarbeiterbesprechung moderiere.“

[Detaillierte Anleitung](#)

Feedback sammeln

Die Person, die eine virtuelle Videokonferenz geplant oder gestartet hat, kann für die Teilnehmer eine **Umfrage** erstellen. Dank dieser Funktion lassen sich Informationen aller Schüler oder Studenten bzw. Konferenzteilnehmer auf schnelle und interaktive Weise zusammenfassen.

- ✓ Moderatoren können eine Umfrage speichern, um sie zu einem späteren Zeitpunkt während einer Videokonferenz zu posten.
Die Umfragen werden leicht auffindbar im Umfragebereich einer virtuellen Videokonferenz gespeichert.
- ✓ Nach dem Meeting wird ein Bericht zu den Umfrageergebnissen per E-Mail an den Moderator gesendet.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Umfragen in Google Meet](#)

Anleitung: Umfragen durchführen

Umfrage erstellen

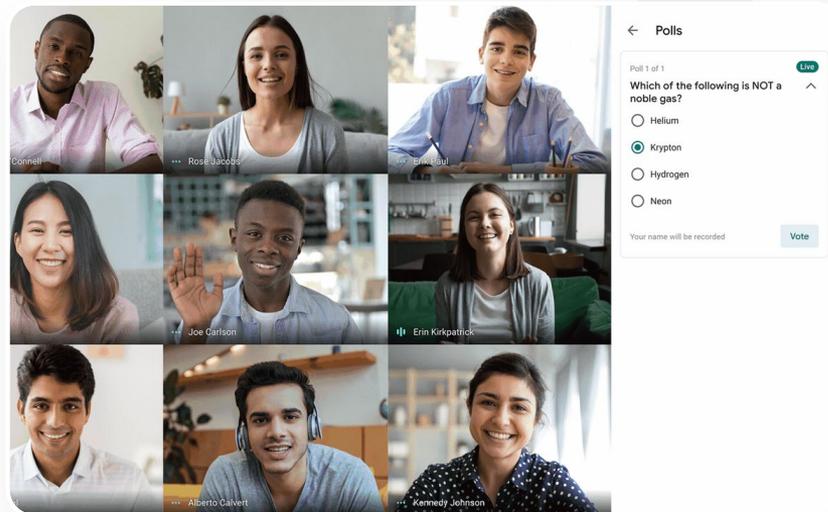
- Wählen Sie in der rechten oberen Ecke einer Videokonferenz das **Aktivitätssymbol** aus > **Umfrage**.
- Wählen Sie **Umfrage starten** aus.
- Geben Sie eine Frage ein.
- Wählen Sie **Starten** oder **Speichern** aus.

Umfrage moderieren

- Wählen Sie in der rechten oberen Ecke einer Videokonferenz das **Aktivitätssymbol** aus > **Umfrage**.
- Um die Umfrageergebnisse in Echtzeit für alle Teilnehmer sichtbar zu machen, schieben Sie den Regler neben **Ergebnisse für alle anzeigen** auf **Ein**.
- Um eine Umfrage zu schließen und keine Antworten mehr zuzulassen, klicken Sie auf **Umfrage beenden**.
- Wenn Sie eine Umfrage endgültig löschen möchten, wählen Sie das Symbol **Löschen** aus.

Bericht zu einer Umfrage ansehen

- Nach der Videokonferenz erhält der Moderator per **E-Mail** einen Bericht.
- Öffnen Sie die E-Mail und klicken Sie auf den **Anhang**.



[🔗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Umfragen in Google Meet](#)



Wir machen ausschließlich Fernunterricht, der aber wie im Klassenzimmer ablaufen soll – mit der Möglichkeit, die Teilnehmer in Kleingruppen aufzuteilen, in die einzelnen Gruppen reinzuhören, sich an Diskussionen zu beteiligen und anschließend ganz einfach wieder zusammenzukommen.“

[Detaillierte Anleitung](#)

Kleine Schüler-/Studentengruppen

Lehrkräfte können **Breakouts** nutzen, um Schüler bzw. Studenten in virtuellen Unterrichtsstunden in kleinere Gruppen einzuteilen. Breakouts müssen von einem Moderator während eines Videoanrufs auf einem Computer gestartet werden. Sie können momentan nicht live gestreamt oder aufgezeichnet werden.

- ✓ Sie können bis zu 100 Breakouts pro Videokonferenz erstellen.
- ✓ Lehrkräfte können ganz einfach von einem Breakout zum anderen springen, um dort zu helfen, wo es nötig ist.
- ✓ Administratoren können sicherstellen, dass ausschließlich Mitglieder der Fakultät bzw. Mitarbeiter Breakouts erstellen können.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Breakouts in Google Meet verwenden](#)

Anleitung: Breakouts erstellen

Breakouts erstellen

- Starten Sie einen Videoanruf.
- Klicken Sie rechts oben auf das **Aktivitätssymbol > Breakouts**.
- Wählen Sie im Steuerfeld des Breakouts die benötigte **Anzahl** aus.
- Die Teilnehmer werden anschließend auf die verschiedenen Räume verteilt, können von den Moderatoren jedoch manuell in einen anderen Raum verschoben werden.
- Klicken Sie rechts unten auf **Breakouts öffnen**.

Fragen in unterschiedlichen Breakouts beantworten

- Eine Benachrichtigung unten auf dem Moderatorenbildschirm erscheint, wenn ein Teilnehmer um Hilfe bittet. Um an dem entsprechenden Breakout teilzunehmen, wählen Sie **Teilnehmen** aus.



[↗](#) Weiterführende Informationen in der
Google Workspace-Admin-Hilfe

[Breakouts in Google Meet verwenden](#)



Wir wissen nicht genau, wer an unseren Onlinekursen teilnimmt. Ich suche nach einem einfachen Weg, um über meine gesamte Domain hinweg festzustellen, wer zu welchem Zeitpunkt an welchen Kursen teilnimmt.“

[Detaillierte Anleitung](#)

Teilnahme erfassen

Teilnahmeberichte liefern einen automatischen Bericht darüber, wer an Videokonferenzen mit fünf oder mehr Personen teilgenommen hat. Sie sehen die Teilnehmer und deren E-Mail-Adresse sowie die Zeitspanne, während der sie am Onlineunterricht teilgenommen haben.

- ✓ Sie können Teilnahmeberichte auch zu laufenden Livestream-Veranstaltungen erhalten.
- ✓ Moderatoren können die Teilnahme- und Livestream-Berichte in der Videokonferenz oder aus dem Google Kalender heraus aktivieren bzw. deaktivieren.

 Weiterführende Informationen in der Google Workspace-Admin-Hilfe

[Teilnahmeberichte in Google Meet](#)

Anleitung: Teilnahmeberichte

In einer Videokonferenz

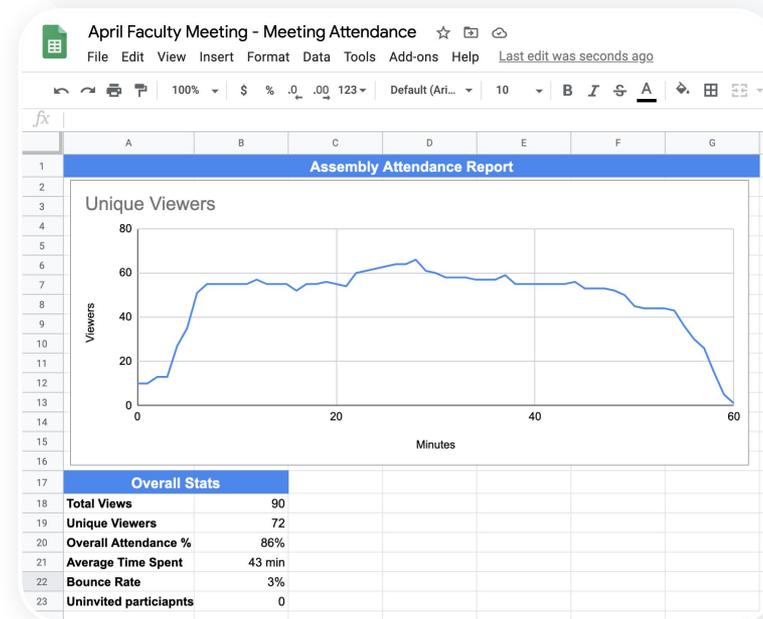
- Starten Sie einen Videoanruf.
- Klicken Sie unten auf das Dreipunkt-Menü.
- Klicken Sie auf **Einstellungen** > **Steuerelemente für den Organisator**.
- Aktivieren oder deaktivieren Sie **Teilnahmeberichte**.

In Google Kalender

- Aktivieren Sie **Google Meet-Videokonferenzen** direkt bei einem Kalendertermin.
- Wählen Sie rechts **Einstellungen** aus.
- Klicken Sie auf das Kästchen neben **Teilnahmeberichte** > **Speichern**.

Teilnahmebericht erhalten

- Nach der Videokonferenz erhält der Moderator per **E-Mail** einen Bericht.
- Öffnen Sie die E-Mail > klicken Sie auf den **Anhang**.



[🔗 Weiterführende Informationen in der Google Workspace-Admin-Hilfe Teilnahmeberichte in Google Meet](#)

Vielen Dank