

Google for Education

# Lebih dari 40 cara menggunakan Google Workspace for Education edisi berbayar

[goo.gle/use-edu-workspace](https://goo.gle/use-edu-workspace)



# Cara menggunakan presentasi ini

Presentasi ini menyajikan pilihan kasus penggunaan populer yang tersedia jika Anda menggunakan salah satu **Google Workspace for Education** edisi berbayar. Google Workspace for Education dapat membantu meningkatkan keamanan data, efisiensi pengajar, interaksi siswa, kolaborasi di tingkat sekolah, dan banyak lagi.

Presentasi ini disusun berdasarkan fitur, diikuti dengan kasus penggunaan umum, dan petunjuk sederhana untuk menggunakan fitur tersebut. Pelajari presentasi ini secara menyeluruh dan lihat seberapa banyak yang dapat Anda lakukan dengan Google Workspace for Education edisi berbayar.

# Google Workspace for Education edisi berbayar

Dapatkan lebih banyak pilihan, kontrol, dan fleksibilitas untuk memenuhi kebutuhan organisasi Anda dengan tiga Google Workspace for Education edisi berbayar.



## Google Workspace for Education Plus

Mencakup Education Standard, Teaching and Learning Upgrade, dan fitur-fitur lain yang hanya tersedia pada edisi Education Plus.



Education Plus memberdayakan siswa, pengajar, pimpinan lembaga pendidikan, dan admin TI dengan solusi teknologi pendidikan **lengkap**, yang menawarkan alat yang mudah digunakan untuk **keamanan dan insight yang canggih, serta pengajaran dan pembelajaran yang diperkaya**.



## Google Workspace for Education Standard

**Alat keamanan dan insight yang canggih** membantu mengurangi risiko dan mengatasi ancaman dengan visibilitas dan kontrol yang ditingkatkan di seluruh lingkungan pembelajaran Anda.



## Teaching and Learning Upgrade

**Alat pengajaran dan pembelajaran yang diperkaya** membantu meningkatkan dampak pengajaran dengan menjadikan pembelajaran lebih terpersonalisasi, menciptakan efisiensi di ruang kelas, serta memungkinkan pengajaran dan pembelajaran dari mana saja.

# Daftar isi



## Kapabilitas Keamanan dan Insight yang Canggih

### Dasbor Keamanan

- Volume spam
- Berbagi file secara eksternal
- Aplikasi pihak ketiga
- Upaya phishing

### Halaman Kondisi

#### Keamanan

- Praktik terbaik keamanan
- Rekomendasi untuk area berisiko

### Alat Investigasi

- Dibagikannya materi yang melanggar
- Dibagikannya file tanpa disengaja
- Email phishing dan malware
- Menghentikan pelaku kejahatan
- Insight keamanan yang lebih mendalam
- Mencegah rapat yang tidak diawasi

### Pengelolaan dan kontrol domain

- Memeriksa ancaman pada lampiran Gmail
- Membuat dasbor dan laporan penggunaan
- Menemukan file dengan lebih mudah
- Dokumen internal yang rapi
- Mengisi grup departemen secara otomatis
- Membuat audiens untuk berbagi file internal
- Membatasi aktivitas berbagi file
- Pembatasan aplikasi Workspace
- Mengelola penyimpanan
- Peraturan data
- Peraturan hibah
- Mengelola perangkat endpoint
- Mengelola perangkat Windows
- Setelan kustom untuk perangkat Windows
- Mengotomatiskan update perangkat Windows
- Memanfaatkan enkripsi sisi klien

# Daftar isi



## Kapabilitas Pengajaran dan Pembelajaran yang Diperkaya

### Google Classroom

- Mengelola akses ke add-on Classroom
- Mengintegrasikan konten yang menarik di Classroom
- Membuat kelas dalam skala besar

### Laporan Keaslian

- Memeriksa plagiarisme dengan laporan keaslian
- Memeriksa keaslian berdasarkan tugas siswa sebelumnya
- Mengubah deteksi plagiarisme menjadi peluang belajar

### Dokumen, Spreadsheet, dan Slide

- Menyetujui dokumen internal

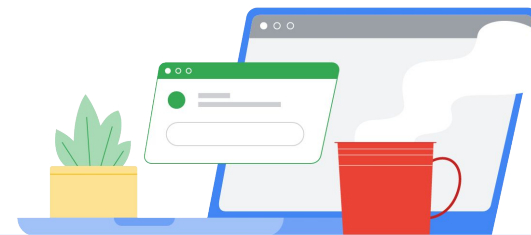
### Google Meet

- Merekam rapat
- Merujuk topik yang telah dibahas di kelas
- Menghilangkan kendala bahasa
- Menyiarkan pertemuan dan acara sekolah
- Mengajukan pertanyaan
- Mengumpulkan output
- Grup kecil siswa
- Melacak kehadiran



# Kapabilitas keamanan dan insight yang canggih

Dapatkan kontrol yang lebih besar di seluruh domain dengan alat keamanan proaktif yang membantu Anda terlindung dari ancaman, menganalisis insiden keamanan, serta melindungi data siswa dan pengajar.



[Dasbor keamanan](#)



[Halaman kondisi keamanan](#)



[Alat investigasi](#)



[Pengelolaan dan kontrol domain](#)



# Dasbor keamanan

[Alat keamanan dan insight](#)

## Apa ini?

Gunakan dasbor keamanan untuk melihat ringkasan berbagai laporan keamanan Anda. Secara default, setiap panel laporan keamanan menampilkan data dari tujuh hari terakhir. Anda dapat menyesuaikan dasbor untuk melihat data dari hari ini, kemarin, minggu ini, minggu lalu, bulan ini, bulan lalu, atau beberapa hari yang lalu (hingga 180 hari).

## Kasus penggunaan

Volume spam



[Petunjuk langkah demi langkah](#)

Berbagi file secara eksternal



[Petunjuk langkah demi langkah](#)

Aplikasi pihak ketiga

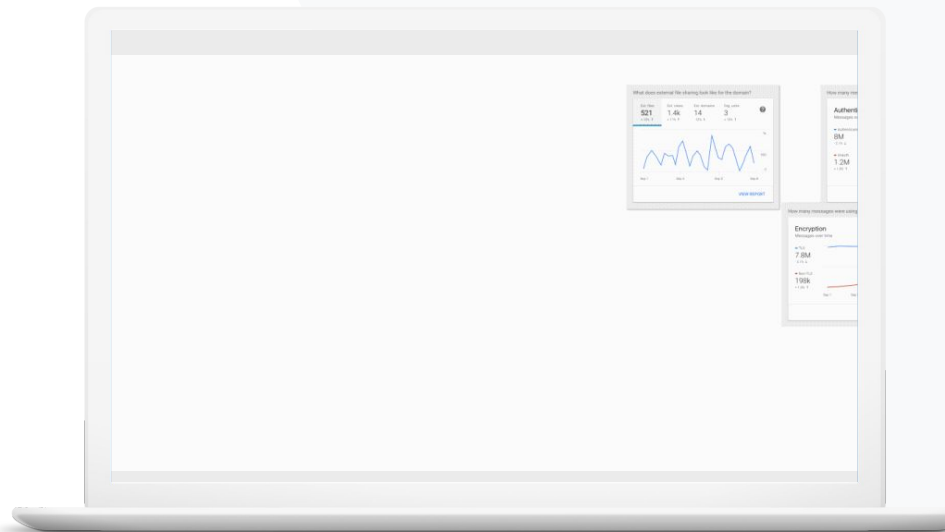


[Petunjuk langkah demi langkah](#)

Upaya phishing




[Petunjuk langkah demi langkah](#)





Saya ingin dapat mengontrol email yang terlalu banyak dan tidak perlu, sekaligus mengurangi ancaman keamanan untuk sekolah saya.”






 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Tentang dasbor keamanan](#)

## Volume spam

Dasbor keamanan memberikan representasi visual aktivitas di seluruh lingkungan Google Workspace for Education Anda, termasuk:

-  Spam
-  Lampiran yang mencurigakan
-  Phishing
-  Dan lainnya
-  Malware

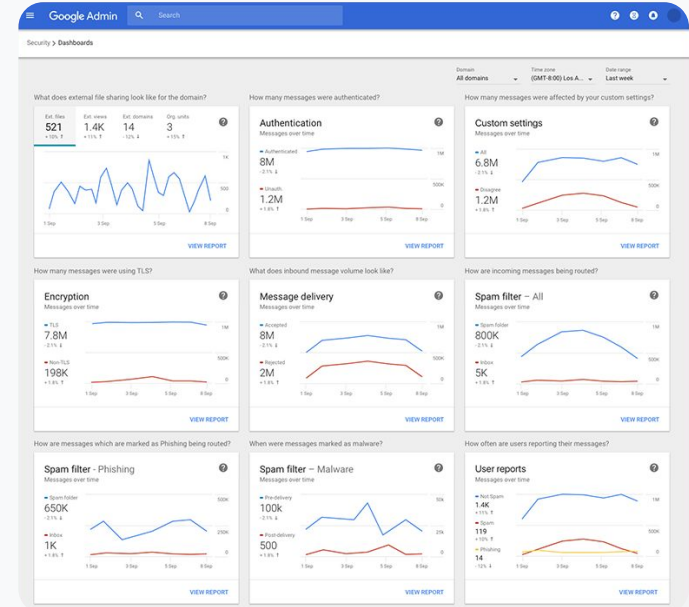



# Petunjuk: Ringkasan dasbor

## Cara melihat dasbor keamanan

- Login ke konsol Admin
- Klik keamanan > dasbor
- Dari dasbor keamanan, Anda dapat menjelajahi data, mengekspor data ke Spreadsheet atau alat pihak ketiga, atau meluncurkan investigasi di alat investigasi

 Dasbor keamanan

 Alat keamanan dan insight


 Dokumentasi Pusat Bantuan yang relevan

- [Tentang dasbor keamanan](#)



Saya ingin melihat aktivitas berbagi file secara eksternal untuk mencegah dibagikannya data sensitif kepada pihak ketiga.”



[Petunjuk langkah demi langkah](#)



Dokumentasi Pusat Bantuan yang relevan

- [Mulai menggunakan halaman kondisi keamanan](#)

## Berbagi file secara eksternal

Gunakan laporan eksposur file dari dasbor keamanan untuk melihat metrik berbagi file eksternal untuk domain Anda, termasuk:



Jumlah peristiwa berbagi kepada pengguna di luar domain Anda selama jangka waktu tertentu.



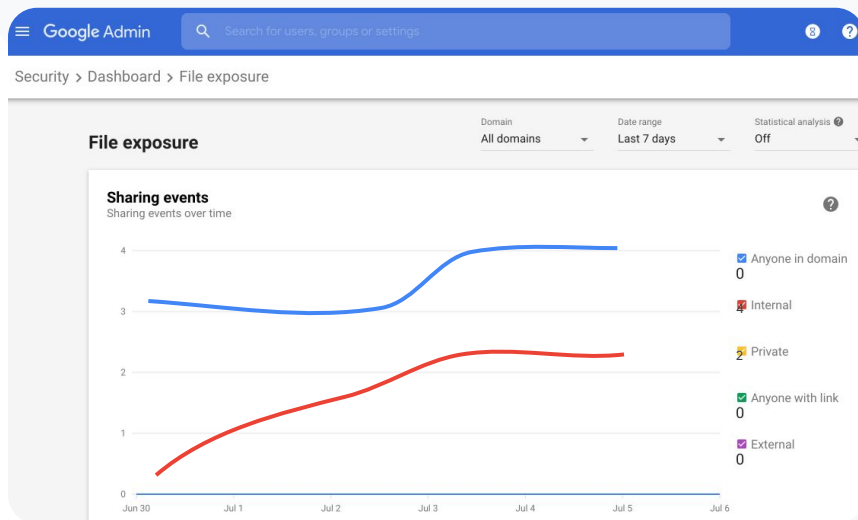
Berapa kali file eksternal dilihat selama jangka waktu tertentu.



# Petunjuk: Berbagi file secara eksternal

## Cara melihat laporan eksposur file

- Login ke konsol Admin
- Klik keamanan > dasbor
- Di panel berjudul, 'Bagaimana kondisi pembagian file eksternal untuk domain ini?', klik lihat laporan di pojok kanan bawah



[Dokumentasi Pusat Bantuan yang relevan](#)

- [Tentang dasbor keamanan](#)
- [Laporan eksposur file](#)



Saya ingin melihat aplikasi pihak ketiga yang memiliki akses ke data domain saya.”



 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Laporan aktivitas pemberian izin OAuth](#)

## Aplikasi pihak ketiga

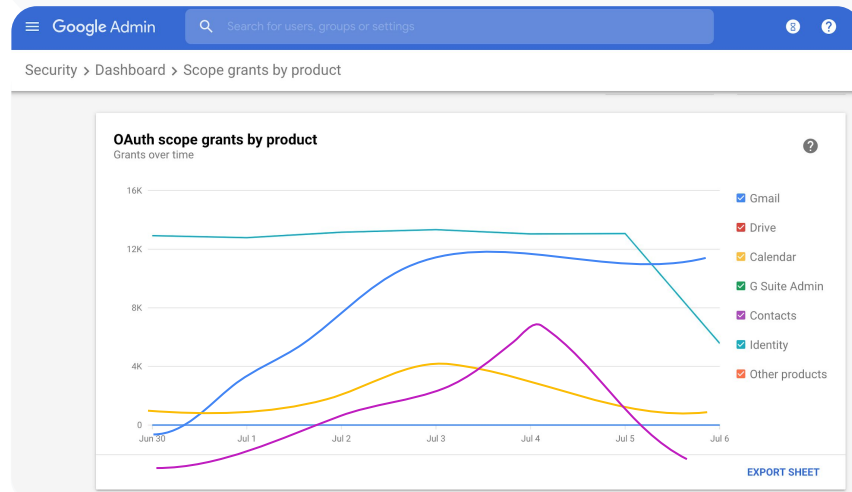
Gunakan Laporan aktivitas pemberian izin OAuth dari dasbor keamanan untuk memantau aplikasi pihak ketiga mana yang terhubung ke domain Anda dan data apa yang dapat mereka akses.

-  OAuth memberikan izin kepada layanan pihak ketiga untuk mengakses informasi akun pengguna tanpa mengungkapkan sandi pengguna yang bersangkutan. Anda mungkin ingin membatasi aplikasi pihak ketiga mana yang memiliki akses.
-  Gunakan panel aktivitas pemberian izin OAuth untuk memantau aktivitas pemberian izin berdasarkan aplikasi, cakupan, atau pengguna dan untuk memperbarui izin yang diberikan.

# Petunjuk: Aplikasi pihak ketiga

## Cara melihat Laporan aktivitas pemberian izin OAuth:

- Login ke konsol Admin
- Klik keamanan > dasbor
- Di bagian bawah, klik lihat laporan
- Anda dapat melihat aktivitas pemberian izin OAuth berdasarkan produk (aplikasi), cakupan, atau pengguna
- Untuk memfilter informasi, klik aplikasi, cakupan, atau pengguna
- Untuk membuat laporan spreadsheet, klik ekspor spreadsheet

[Dasbor keamanan](#)[Alat keamanan dan insight](#)[Dokumentasi Pusat Bantuan yang relevan](#)

- [Laporan aktivitas pemberian izin OAuth](#)



Pengguna melaporkan upaya phishing. Saya ingin dapat melacak kapan email phishing masuk, email apa yang diterima pengguna saya, dan risiko apa yang mereka hadapi.”



[Petunjuk langkah demi langkah](#)



Dokumentasi Pusat Bantuan yang relevan

- [Bagaimana cara pengguna menandai email?](#)
- [Laporan pengguna](#)

## Upaya phishing

Panel laporan pengguna di dasbor keamanan dapat Anda gunakan untuk melihat pesan yang ditandai sebagai phishing atau spam selama jangka waktu tertentu. Anda dapat melihat informasi email yang ditandai sebagai phishing, seperti siapa yang menerima dan membukanya.



Laporan pengguna memungkinkan Anda melihat bagaimana pengguna menandai pesan mereka—spam, bukan spam, atau phishing—selama jangka waktu tertentu.

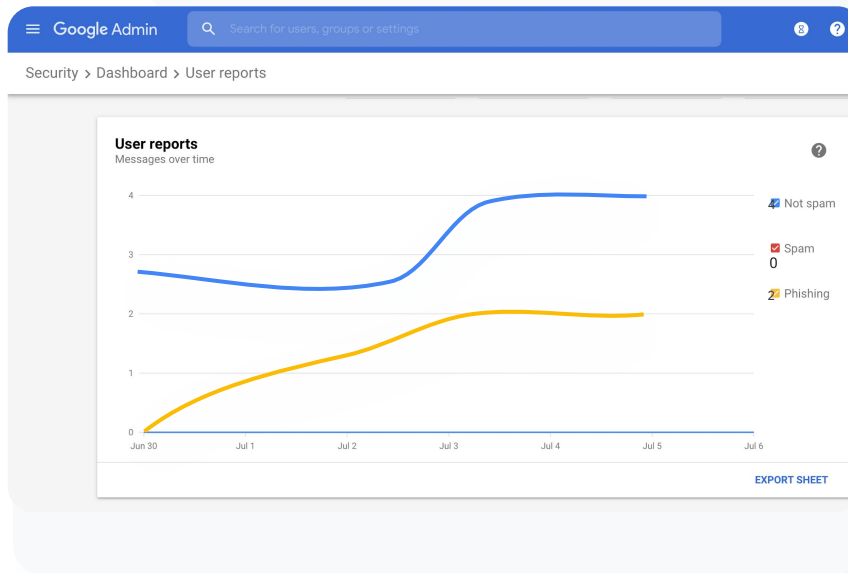


Anda dapat menyesuaikan grafik untuk memberikan detail hanya tentang jenis pesan tertentu, seperti apakah pesan dikirim secara internal atau eksternal, berdasarkan rentang tanggal, dan sebagainya.

# Petunjuk: Upaya phishing

## Cara melihat panel laporan pengguna

- Login ke konsol Admin
- Klik keamanan > dasbor
- Di pojok kanan bawah panel laporan pengguna, klik lihat laporan

[Dasbor keamanan](#)[Alat keamanan dan insight](#)[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Tentang dasbor keamanan](#)
- [Laporan eksposur file](#)

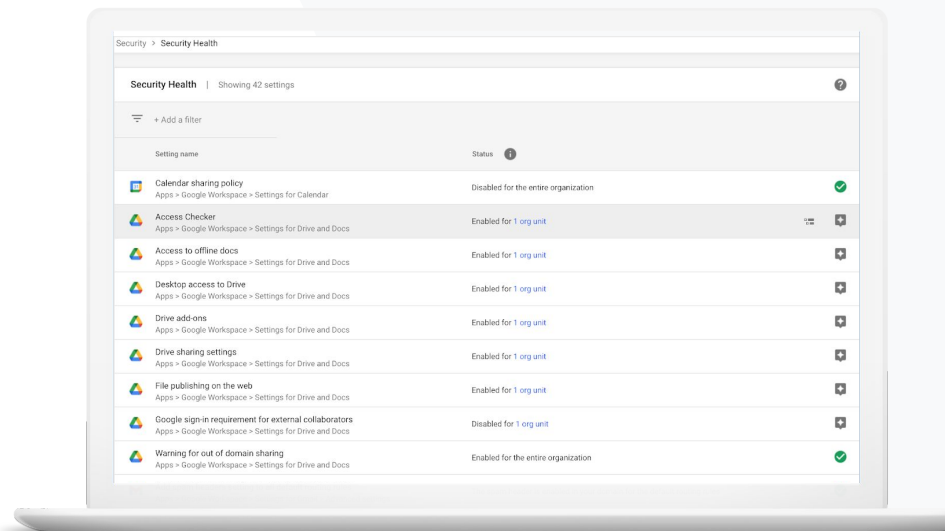
# Kondisi keamanan

[Alat keamanan dan insight](#)

## Apa ini?

Halaman kondisi keamanan menyediakan ringkasan komprehensif tentang kondisi keamanan lingkungan Google Workspace Anda, sehingga Anda dapat membandingkan konfigurasi dengan rekomendasi dari Google untuk melindungi organisasi Anda secara proaktif.

## Kasus penggunaan


[Praktik terbaik keamanan](#)[Petunjuk langkah demi langkah](#)[Rekomendasi untuk area berisiko](#)[Petunjuk langkah demi langkah](#)





Arahkan saya ke praktik terbaik atau rekomendasi terkait cara menyiapkan kebijakan keamanan.”





 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mulai menggunakan halaman kondisi keamanan](#)

## Praktik terbaik keamanan

Buka halaman kondisi keamanan untuk menerima praktik terbaik mengenai kebijakan keamanan beserta:

-  Rekomendasi untuk area risiko potensial di domain Anda
-  Rekomendasi setelan optimal untuk meningkatkan efektivitas keamanan Anda
-  Link langsung ke setelan
-  Informasi tambahan dan artikel dukungan

# Petunjuk: Checklist praktik terbaik keamanan



Kondisi keamanan



Alat keamanan dan insight

Untuk membantu melindungi organisasi Anda, Google secara default mengaktifkan banyak setelan yang direkomendasikan dalam checklist berikut sebagai praktik terbaik keamanan. Sebaiknya pelajari teks yang diperjelas di bawah ini secara lebih mendetail.

- **Administrator:** Melindungi akun admin
- **Akun:** Membantu mencegah dan mengatasi akun yang disusupi
- **Apl:** Meninjau akses pihak ketiga ke layanan inti
- **Kalender:** Membatasi opsi berbagi kalender eksternal
- **Drive:** Membatasi opsi berbagi dan kolaborasi di luar domain
- **Gmail:** Menyiapkan autentikasi dan infrastruktur
- **Vault:** Mengontrol, mengaudit, dan mengamankan akun Vault

## 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](#)

 [Dokumentasi Pusat Bantuan yang relevan](#)

- [Memantau kondisi setelan keamanan Anda](#)



Saya menginginkan ringkasan yang mudah dipahami mengenai setelan keamanan domain saya dengan rekomendasi yang dapat ditindaklanjuti untuk mengatasi area risiko yang potensial.”

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Mulai menggunakan halaman kondisi keamanan](#)

## Rekomendasi untuk area berisiko

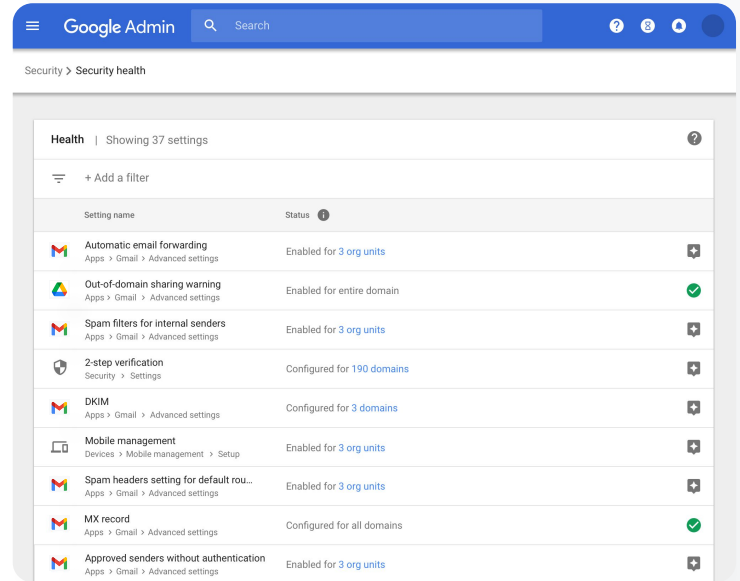
Halaman **kondisi keamanan** meninjau konfigurasi keamanan dan menandai perubahan yang disarankan. Di halaman kondisi keamanan, Anda bisa:

- ✓ Mengidentifikasi dengan cepat area risiko potensial di domain Anda
- ✓ Mendapatkan rekomendasi setelan optimal untuk meningkatkan efektivitas keamanan Anda
- ✓ Membaca informasi tambahan dan artikel dukungan tentang rekomendasi










# Petunjuk: Rekomendasi Keamanan

## Cara melihat rekomendasi

- Login ke konsol Admin
- Klik keamanan > kondisi keamanan
- Lihat setelan status di kolom paling kanan
  - Tanda centang hijau menunjukkan bahwa setelan aman
  - Ikon abu-abu menunjukkan rekomendasi untuk mempelajari setelan tersebut; klik ikon ini untuk membuka detail dan petunjuk

 Kondisi keamanan Alat keamanan dan insight

The screenshot shows the Google Admin console's Security Health page. At the top, there's a search bar and navigation icons. Below the header, the page title is "Security > Security health". The main content area is titled "Health | Showing 37 settings" and includes a filter button. A table lists various security settings with their status and icons. The table has two columns: "Setting name" and "Status".

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

 Dokumentasi Pusat Bantuan yang relevan

- [Mulai menggunakan halaman kondisi keamanan](#)

# Alat investigasi

## Apa ini?

Gunakan alat investigasi untuk mengidentifikasi, menentukan prioritas, dan mengambil tindakan terhadap masalah keamanan dan privasi di domain Anda.

## Kasus penggunaan

Dibagikannya materi yang melanggar



[Petunjuk langkah demi langkah](#)

Dibagikannya file tanpa sengaja



[Petunjuk langkah demi langkah](#)

Penentuan prioritas email



[Petunjuk langkah demi langkah](#)

Email phishing/malware



[Petunjuk langkah demi langkah](#)

Menghentikan pelaku kejahatan



[Petunjuk langkah demi langkah](#)

Insight keamanan yang lebih mendalam

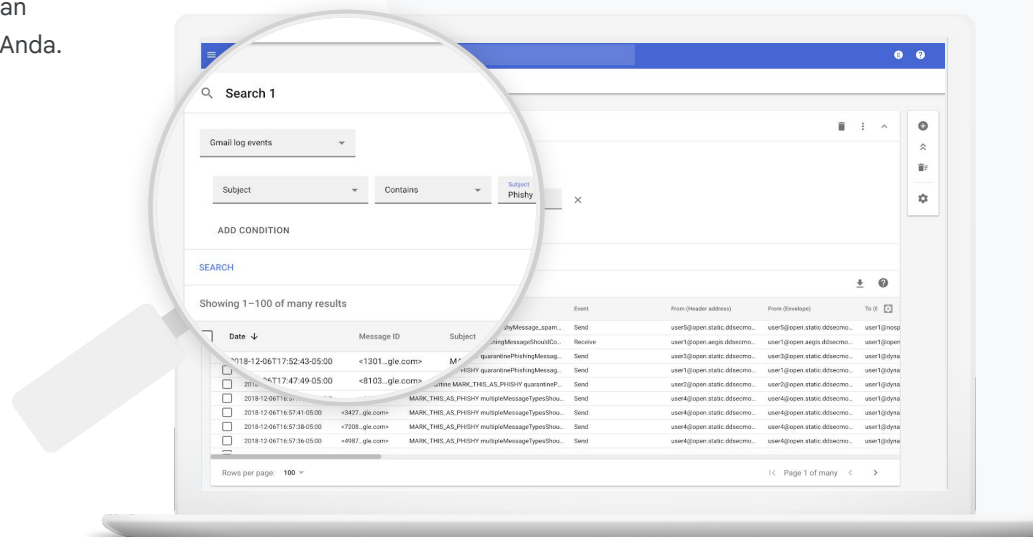


[Petunjuk langkah demi langkah](#)

Mencegah rapat yang tidak diawasi



[Petunjuk langkah demi langkah](#)





Saya tahu ada file berisi materi melanggar yang sedang dibagikan. Saya ingin tahu siapa yang membuat file tersebut, kapan dibuatnya, siapa yang membagikannya kepada siapa, siapa yang mengeditnya, dan saya ingin menghapusnya.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Kondisi untuk peristiwa log Drive](#)
- [Tindakan untuk peristiwa log Drive](#)

## Dibagikannya materi yang melanggar

Peristiwa log Drive dalam alat investigasi dapat membantu Anda menemukan, melacak, dan mengisolasi atau menghapus file yang tidak diinginkan dalam domain Anda. Dengan mengakses [data peristiwa log Drive](#), Anda dapat:

- ✓ Mencari dokumen menurut nama, pelaku, pemilik, dan sebagainya
- ✓ Mengambil tindakan dengan mengubah izin file atau menghapus file tersebut
- ✓ Mencari konten yang dibuat pengguna di Google Workspace dan yang mereka upload ke Drive
- ✓ Melihat semua informasi log yang terkait dengan dokumen tersebut
  - Tanggal pembuatan
  - Siapa pemiliknya, siapa yang melihatnya, dan siapa yang mengeditnya
  - Kapan dokumen tersebut dibagikan



Ada file yang secara tidak sengaja dibagikan kepada grup yang seharusnya TIDAK memiliki akses ke file itu.

Saya ingin menghapus akses mereka ke file tersebut.

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Menjalankan penelusuran di alat investigasi](#)
- [Mengambil tindakan berdasarkan hasil penelusuran](#)

## File yang tidak sengaja dibagikan

Peristiwa log Drive dalam alat investigasi dapat membantu Anda melacak dan menyelesaikan masalah berbagi file. Dengan mengakses [data peristiwa log Drive](#), Anda dapat:

- ✓ Mencari dokumen menurut nama, pelaku, pemilik, dan sebagainya
- ✓ Melihat semua informasi log yang terkait dengan dokumen, termasuk siapa yang melihatnya dan kapan dokumen itu dibagikan
- ✓ Mengambil tindakan dengan mengubah izin dan menonaktifkan fitur download, cetak, dan salin

# Petunjuk: Peristiwa log Drive

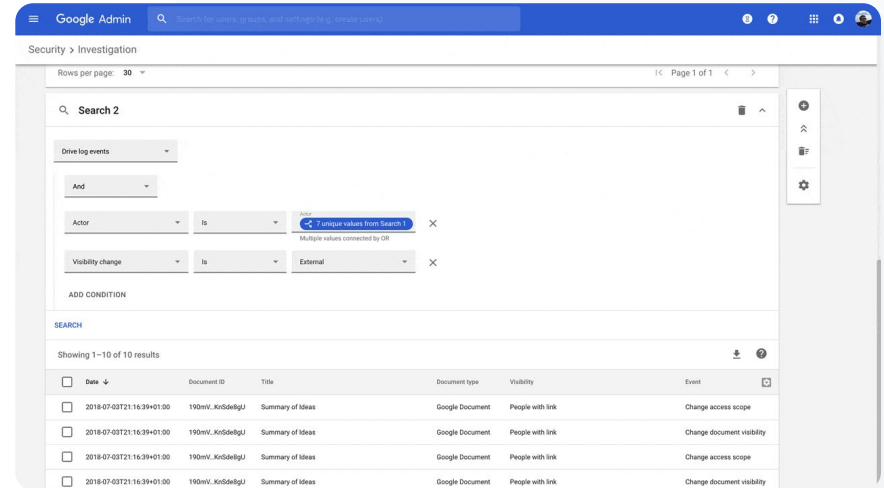
[Alat investigasi](#)
[Alat keamanan dan insight](#)

## Cara menginvestigasi peristiwa log Drive

- Login ke konsol Admin
- Klik keamanan > alat investigasi
- Pilih peristiwa log Drive
- Klik tambahkan kondisi > telusuri

## Cara mengambil tindakan

- Pilih file yang relevan di hasil penelusuran
- Klik tindakan > audit izin file untuk membuka halaman Izin
- Klik Orang untuk melihat siapa saja yang memiliki akses
- Klik Link untuk melihat atau mengubah setelan berbagi link pada file yang dipilih
- Klik perubahan dalam proses untuk meninjau perubahan sebelum menyimpan



[Dokumentasi Pusat Bantuan yang relevan](#)

- [Menjalankan penelusuran di alat investigasi](#)
- [Mengambil tindakan berdasarkan hasil penelusuran](#)





Seseorang mengirim email yang seharusnya TIDAK dikirim. Kami ingin tahu siapa saja penerimanya, apakah mereka membukanya, apakah mereka merespons, dan kami ingin menghapus email tersebut. Saya juga ingin tahu isi emailnya.”

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Kondisi untuk log Gmail dan pesan Gmail](#)
- [Tindakan untuk pesan Gmail dan peristiwa log Gmail](#)
- [Langkah-langkah yang dapat membantu Anda melihat isi email](#)

## Penentuan prioritas email

Log Gmail dalam alat investigasi dapat membantu Anda mengidentifikasi dan menindaklanjuti email berbahaya atau melanggar dalam domain Anda. Dengan mengakses log Gmail, Anda dapat:

- ✓ Mencari email tertentu menurut subjek, ID pesan, lampiran, pengirim, dan sejenisnya
- ✓ Melihat detail email, termasuk penulis, penerima, siapa yang membukanya, dan kepada siapa email diteruskan.
- ✓ Melakukan tindakan berdasarkan hasil penelusuran. Tindakan pada pesan Gmail meliputi hapus, pulihkan, tandai sebagai spam atau phishing, kirim ke kotak masuk, dan kirim ke karantina.



Email phishing atau malware dikirim kepada pengguna. Kami ingin mengetahui apakah pengguna mengklik link yang ada dalam email tersebut atau mendownload lampiran yang disertakan, karena hal itu berpotensi membahayakan pengguna dan domain kami.”

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Kondisi untuk log Gmail dan pesan Gmail](#)
- [Tindakan untuk pesan Gmail dan peristiwa log Gmail](#)
- [Langkah-langkah yang dapat membantu Anda melihat isi email](#)
- [Melihat laporan VirusTotal](#)

## Email phishing dan malware

Membuka alat investigasi, khususnya log Gmail, dapat membantu Anda menemukan dan mengisolasi email berbahaya dalam domain Anda. Dengan mengakses log Gmail, Anda dapat:

- ✓ Mencari konten tertentu dalam pesan email, termasuk lampiran
- ✓ Melihat informasi tentang email tertentu, termasuk penerima dan yang membukanya
- ✓ Melihat pesan dan rangkaian pesan untuk menentukan apakah pesan tersebut berbahaya
- ✓ Memindai lampiran email untuk mendapatkan data reputasi dan konteks ancaman yang lebih lengkap dengan laporan VirusTotal
- ✓ Mengambil tindakan dengan menandai pesan sebagai spam atau phishing, mengirimnya ke kotak masuk atau karantina tertentu, atau menghapusnya

# Petunjuk: Log Gmail

Alat investigasi

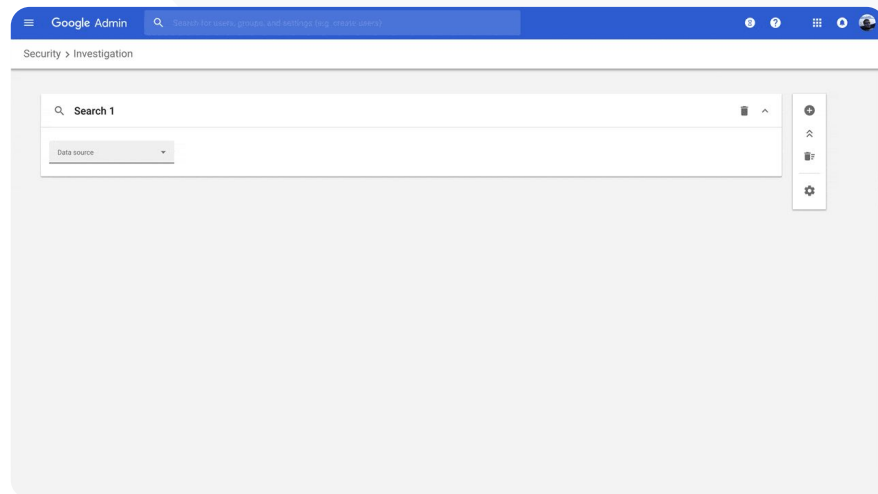
Alat keamanan dan insight

## Cara memeriksa log Gmail

- Login ke konsol Admin
- Klik keamanan > alat investigasi
- Pilih peristiwa log Gmail ATAU pesan Gmail
- Klik tambahkan kondisi > telusuri

## Cara mengambil tindakan

- Pilih file yang relevan di hasil penelusuran
- Klik tindakan
- Pilih hapus pesan dari kotak masuk
- Untuk mengonfirmasi tindakan, klik lihat di bagian bawah halaman
- Di kolom hasil, Anda dapat melihat status tindakan



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Kondisi untuk log Gmail dan pesan Gmail](#)
- [Tindakan untuk pesan Gmail dan peristiwa log Gmail](#)
- [Langkah-langkah yang dapat membantu Anda melihat isi email](#)



Seseorang yang tidak bertanggung jawab terus-menerus menarget pengguna penting dalam domain saya, sementara upaya saya untuk menghentikannya tidak sepenuhnya berhasil.

Bagaimana cara mengatasi masalah ini?”

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Menelusuri dan menyelidiki peristiwa log pengguna](#)
- [Membuat aturan aktivitas dengan alat investigasi](#)

## Menghentikan pelaku kejahatan

Log pengguna dalam alat investigasi dapat membantu Anda:

- ✓ Mengidentifikasi dan menyelidiki upaya pembajakan akun pengguna di organisasi Anda
- ✓ Memantau metode verifikasi 2 langkah mana yang digunakan pengguna di organisasi Anda
- ✓ Mempelajari lebih lanjut upaya login yang gagal oleh pengguna di organisasi Anda
- ✓ [Membuat aturan aktivitas dengan alat investigasi](#): Otomatis memblokir pesan dan aktivitas berbahaya lainnya dari pihak tertentu
- ✓ Meningkatkan perlindungan bagi pengguna penting dengan [Program Perlindungan Lanjutan](#)
- ✓ Memulihkan atau menangguhkan pengguna

# Petunjuk: Menghentikan pelaku kejahatan

## Cara memeriksa peristiwa log pengguna

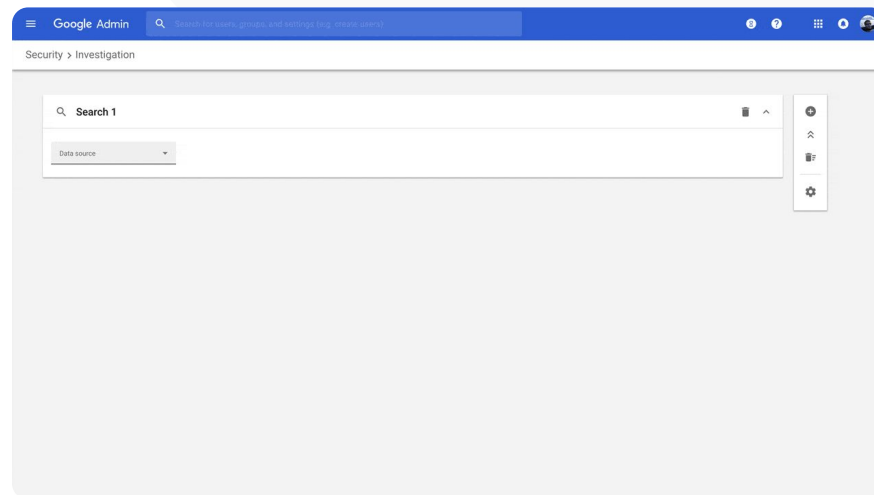
- Login ke konsol Admin
- Klik keamanan > alat investigasi
- Pilih peristiwa log pengguna
- Klik tambahkan kondisi > telusuri

## Cara memulihkan atau menangguhkan pengguna

- Dari hasil penelusuran, pilih satu atau beberapa pengguna
- Klik menu drop-down tindakan
- Klik pulihkan pengguna atau tangguhkan pengguna

## Cara melihat detail tentang pengguna tertentu

- Dari halaman hasil penelusuran, pilih hanya satu pengguna
- Dari menu drop-down TINDAKAN, klik lihat detail

[Alat investigasi](#)[Alat keamanan dan insight](#)[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Menelusuri dan menyelidiki peristiwa log pengguna](#)



Salah seorang pengajar kami melaporkan bahwa file yang dilampirkan di Gmail tampak mencurigakan.

Adakah cara bagi departemen TI untuk mengetahui apakah file tersebut merupakan ancaman keamanan?”



[Petunjuk langkah demi langkah](#)



[Dokumentasi Pusat Bantuan yang relevan](#)

- [Menjalankan penelusuran di alat investigasi](#)
- [Melihat laporan VirusTotal dari alat investigasi](#)

## Mendapatkan insight keamanan yang lebih mendalam

Laporan VirusTotal memperluas hasil investigasi keamanan dengan memberikan ringkasan yang komprehensif, sehingga admin dapat memeriksa keamanan domain, lampiran file, alamat IP, atau URL tertentu berdasarkan insight yang diperoleh melalui crowdsourcing.



Dapatkan insight keamanan tambahan terkait peristiwa log Gmail dan Chrome



Analisis file, URL, domain, dan alamat IP yang mencurigakan



Akses informasi yang diperoleh melalui crowdsourcing tentang mengapa lampiran atau situs tertentu dianggap berisiko



Dapatkan bantuan dalam mengambil keputusan saat menangani masalah keamanan

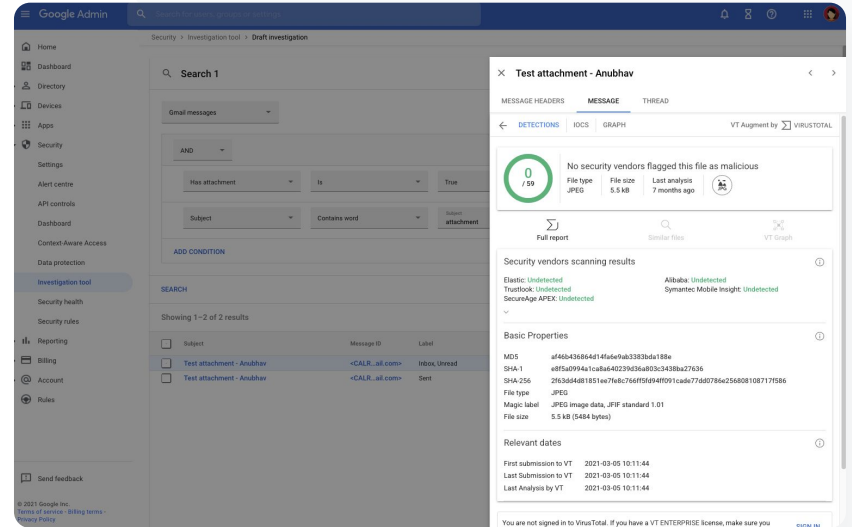
# Petunjuk: Mendapatkan insight keamanan yang lebih mendalam

[Alat investigasi](#)
[Alat keamanan dan insight](#)

## Cara melihat laporan VirusTotal yang terkait dengan Gmail

- Login ke konsol Admin
- Klik keamanan > pusat keamanan > alat investigasi
- Pilih pesan Gmail
- Klik tambahkan kondisi > memiliki lampiran
- Dari hasil penelusuran, klik ID Pesan atau link Subjek
- Dari panel samping, klik tab Pesan atau Rangkaian pesan
- Pilih Lihat Laporan VirusTotal

Admin juga dapat melihat laporan VirusTotal yang terkait dengan Chrome. Cukup ikuti petunjuk di atas dan pilih peristiwa log Chrome di alat investigasi.



[Dokumentasi Pusat Bantuan yang relevan](#)

- [Melihat laporan VirusTotal dari alat investigasi](#)



Para siswa masih menggunakan panggilan Google Meet setelah kelas mereka berakhir. Saya memerlukan cara untuk mengakhiri panggilan Meet bagi semuanya guna menghindari gangguan pembelajaran.”



[Petunjuk langkah demi langkah](#)



Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan alat investigasi untuk mengakhiri rapat](#)

## Mencegah rapat virtual yang tidak diawasi

Administrator Google Workspace dapat menggunakan tindakan **Akhiri rapat untuk semuanya** di alat investigasi untuk menghapus semua pengguna dari rapat apa pun dalam organisasi Anda. Untuk panggilan Google Meet individu, penyelenggara rapat juga memiliki kemampuan ini.



Rapat akan berakhir bagi semua pengguna yang sedang mengikutinya, termasuk yang berada di ruang kerja kelompok.



Mencegah siapa pun menghadiri rapat tersebut pada masa mendatang tanpa kehadiran penyelenggara.



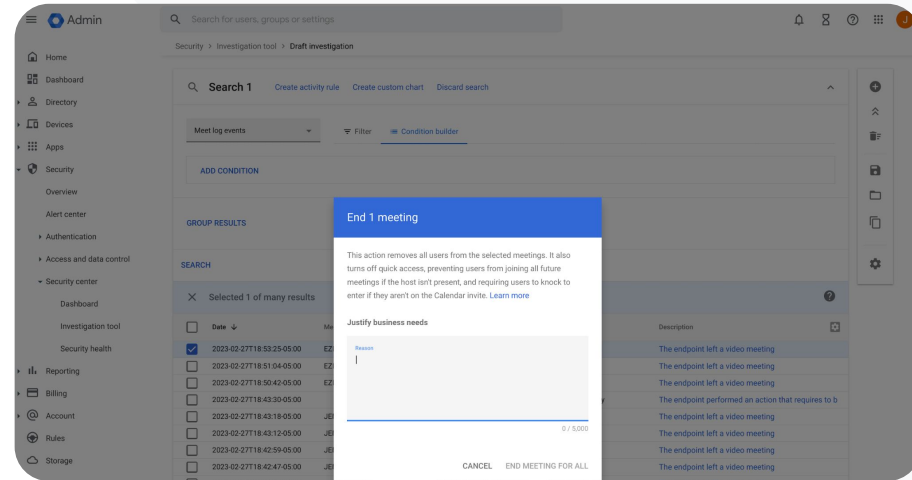
# Petunjuk: Mencegah rapat virtual yang tidak diawasi

Cara menggunakan alat investigasi untuk mengakhiri rapat bagi semua pengguna

- Login ke konsol Admin
- Klik keamanan > pusat keamanan > alat investigasi
- Pilih peristiwa log Meet
- Klik Telusuri > Di hasil penelusuran, Anda akan melihat daftar peristiwa log Meet
- Centang kotak untuk rapat yang ingin Anda akhiri bagi semua pengguna
- Pilih Tindakan
- Klik Akhiri rapat untuk semuanya

🔍 Alat investigasi

👁️ Alat keamanan dan insight




🔗 Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan alat investigasi untuk mengakhiri rapat](#)



## Pengelolaan dan kontrol domain

 [Alat keamanan dan insight](#)


Admin memiliki akses ke berbagai alat lanjutan Google Workspace untuk mengelola data organisasi, menetapkan kontrol, memantau penggunaan, dan terus mematuhi standar pendidikan.


### Kasus penggunaan

[Memeriksa ancaman pada lampiran Gmail](#)  [Petunjuk langkah demi langkah](#)


[Membuat dasbor dan laporan penggunaan](#)  [Petunjuk langkah demi langkah](#)

[Menemukan file dengan lebih mudah](#)  [Petunjuk langkah demi langkah](#)

[Menata dokumen internal](#)  [Petunjuk langkah demi langkah](#)

[Mengisi grup departemen secara otomatis](#)  [Petunjuk langkah demi langkah](#)

[Membuat audiens untuk berbagi file internal](#)  [Petunjuk langkah demi langkah](#)

[Membatasi aktivitas berbagi file](#)  [Petunjuk langkah demi langkah](#)

[Pembatasan aplikasi Workspace](#)  [Petunjuk langkah demi langkah](#)

[Mengelola penyimpanan](#)  [Petunjuk langkah demi langkah](#)

[Peraturan data](#)  [Petunjuk langkah demi langkah](#)

[Peraturan hibah](#)  [Petunjuk langkah demi langkah](#)

[Mengelola perangkat endpoint](#)  [Petunjuk langkah demi langkah](#)

[Mengelola perangkat Windows](#)  [Petunjuk langkah demi langkah](#)

[Setelan kustom untuk perangkat Windows](#)  [Petunjuk langkah demi langkah](#)

[Mengotomatiskan update perangkat Windows](#)  [Petunjuk langkah demi langkah](#)

[Memanfaatkan enkripsi sisi klien](#)  [Petunjuk langkah demi langkah](#)



How can I better protect my domain against zero-day malware and ransomware threats?"




 [Step-by-step how to](#)

 Relevant Help Center documentation

- [Set up rules to detect harmful attachments](#)

## Scan Gmail attachments for threats

Email attachments can include malicious software. To identify these threats, Gmail can scan or run attachments in Security Sandbox. Attachments identified as threats are sent to the Spam folder.

-  Detect malware by virtually “executing” it in a private, secure sandbox environment and analyzing the side effects to determine malicious behavior
-  Scan Microsoft Word, PowerPoint, PDF, zip files, and more
-  Enable scanning for the entire domain, or create scanning rules based on specific conditions like sender, domain, and more

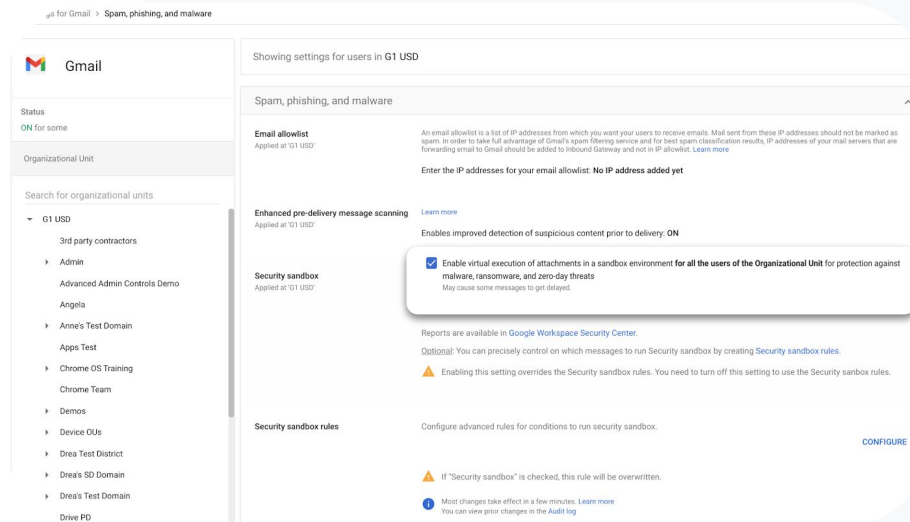
# How to: Scan Gmail attachments for threats

## How it works

Email attachments are detonated within a sandbox in a matter of minutes prior to the delivery of the email, providing an extra layer of security.

## How to scan all attachments in Security Sandbox

- Sign in to your Admin console
- Click Menu > Apps > Google Workspace > Gmail > Spam, Phishing, and Malware
- Select an organizational unit or apply settings across your domain
- Scroll to Security sandbox under Spam, Phishing, and Malware
- Check the Enable virtual execution of attachments in a sandbox environment box
- Click Save



us for Gmail > Spam, phishing, and malware

Gmail

Status  
ON for some

Organizational Unit

Search for organizational units

- ▼ G1 USD
  - 3rd party contractors
  - Admin
  - Advanced Admin Controls Demo
  - Angela
  - Anne's Test Domain
  - Apps Test
  - Chrome OS Training
  - Chrome Team
  - Demos
  - Device OUs
  - Drea Test District
  - Drea's SD Domain
  - Drea's Test Domain
  - Drive PD

Showing settings for users in G1 USD

Spam, phishing, and malware

**Email allowlist**  
Applied at 101 USD

An email allowlist is a list of IP addresses from which you want your users to receive emails. Mail sent from these IP addresses should not be marked as spam. In order to take full advantage of Gmail's spam filtering service and for best spam classification results, IP addresses of your mail servers that are forwarding email to Gmail should be added to Inbound Gateway and not in IP allowlist. [Learn more](#)

Enter the IP addresses for your email allowlist. **No IP address added yet**

**Enhanced pre-delivery message scanning** [Learn more](#)  
Applied at 101 USD

Enables improved detection of suspicious content prior to delivery: ON

**Enable virtual execution of attachments in a sandbox environment for all the users of the Organizational Unit for protection against malware, ransomware, and zero-day threats**  
May cause some messages to get delayed.

Reports are available in [Google Workspace Security Center](#).

Optional: You can precisely control on which messages to run Security sandbox by creating [Security sandbox rules](#).

⚠ Enabling this setting overrides the Security sandbox rules. You need to turn off this setting to use the Security sandbox rules.

**Security sandbox rules**

Configure advanced rules for conditions to run security sandbox. [CONFIGURE](#)

⚠ If "Security sandbox" is checked, this rule will be overridden.

🕒 Most changes take effect in a few minutes. [Learn more](#)  
You can view prior changes in the [Audit log](#)

[🔗 Relevant Help Center documentation](#)

- [Set up rules to detect harmful attachments](#)



Bagaimana cara memahami penggunaan Classroom di seluruh domain saya?”




 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Menyiapkan templat BigQuery Export & Data Studio](#)

## Membuat dasbor dan laporan penggunaan

Dengan templat BigQuery Export dan Looker Studio, admin dapat menggunakan log aktivitas Classroom untuk membuat dasbor dan pelaporan kustom dengan alat analisis seperti Looker Studio dan partner visualisasi pihak ketiga yang terintegrasi ke dalam BigQuery.

-  Ekspor data log Classroom dari konsol Admin ke BigQuery dan Looker Studio.
-  Lihat laporan penggunaan dan pengadopsian dengan cepat di seluruh domain. Ketahui siapa yang menghapus siswa dari kelas, siapa yang mengarsipkan kelas pada tanggal tertentu, dan banyak lagi.
-  Pahami tren keseluruhan dan ambil tindakan lebih cepat dengan templat dasbor Looker Studio yang dapat disesuaikan.

# Petunjuk: Membuat dasbor dan laporan penggunaan

## 01 Menyiapkan dan mengekspor proyek BigQuery

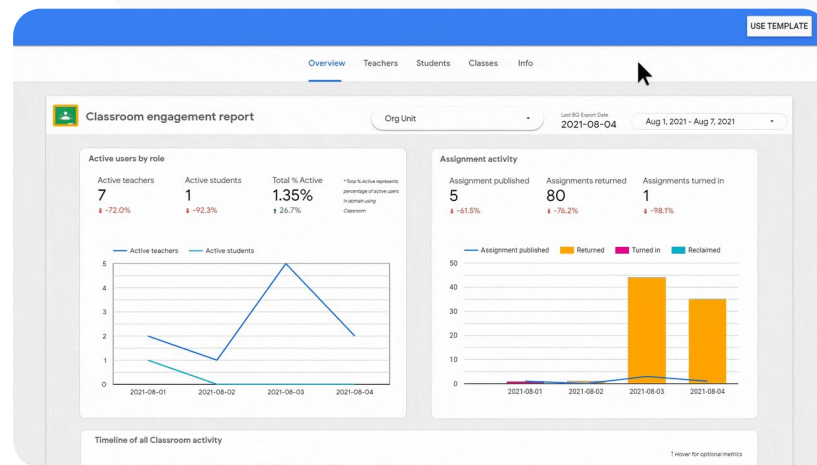
- Login ke [console.cloud.google.com](https://console.cloud.google.com) > Buat proyek baru
- Login ke [admin.google.com](https://admin.google.com) > Laporan > BigQuery Export
- Klik proyek Cloud BigQuery > Namai set data Anda > Simpan

## 02 Menambahkan BigQuery Export di Looker Studio

- Login ke [Looker Studio](https://lookerstudio.google.com) > Buat > Sumber data
- Pilih konektor BigQuery > Proyek saya > klik proyek yang Anda buat > Aktivitas
- Centang kotak pada Tabel Berpartisi > klik Hubungkan

## 03 Membuat Dasbor Looker Studio

- Buka [templat](#) > pilih Gunakan Templat
- Pada Sumber Data Baru, pilih sumber data aktivitas
- Klik Salin Laporan



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Menyiapkan templat BigQuery Export & Data Studio](#)



Saya perlu melacak slip izin karyawan yang dikirimkan orang tua melalui Gmail, Chat, dan Dokumen.

Bagaimana cara menemukan file tersebut di seluruh domain saya?

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Panduan Google Cloud Search](#)
- [Mengaktifkan atau menonaktifkan Google Cloud Search untuk pengguna](#)

## Menemukan file dengan lebih mudah

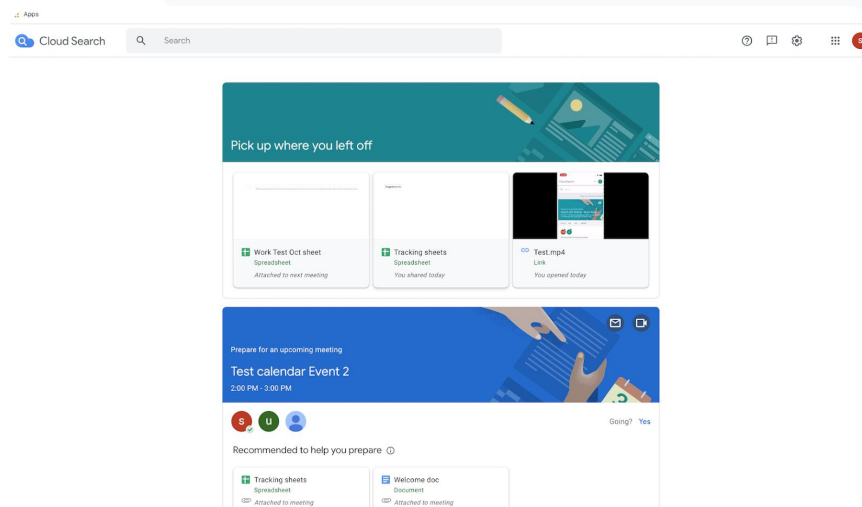
Dengan Google Cloud Search, pendidik di lembaga Anda dapat dengan cepat menemukan konten di seluruh Google Workspace dan aplikasi pihak ketiga.

- ✓ Temukan informasi yang Anda perlukan - dari mana saja, menggunakan laptop, ponsel, atau tablet
- ✓ Telusuri berbagai aplikasi Google Workspace seperti Drive, Kontak, Gmail, dan sumber data pihak ketiga

# Petunjuk: Menemukan file dengan lebih mudah

## Mengaktifkan Google Cloud Search bagi pengguna

- Login ke konsol Admin > buka Menu > Aplikasi > Google
- Klik Status layanan
- Untuk mengaktifkan atau menonaktifkan layanan bagi semua orang di organisasi Anda, klik **Aktif untuk semua orang** atau **Nonaktif untuk semua orang**
- Klik Simpan
- Untuk mengaktifkan layanan bagi sekelompok pengguna lintas atau di dalam unit organisasi, pilih grup akses.
- Klik Simpan



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Panduan Google Cloud Search](#)
- [Mengaktifkan atau menonaktifkan Google Cloud Search untuk pengguna](#)





Saya ingin menerapkan label sensitivitas ke file lembaga untuk memenuhi persyaratan kepatuhan, mencegah penyalahgunaan, dan meningkatkan keteraturan file.

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengelola Label Drive](#)

## Mengatur dokumen di seluruh domain

Label Drive membantu pengguna menemukan, mengatur, dan menerapkan kebijakan di seluruh domain. Admin dapat membuat dan mengelola label Drive untuk mencegah penyalahgunaan file dan memastikan data siswa memenuhi persyaratan kepatuhan.

- ✓ Label adalah metadata yang dapat membantu mengatur file pendidikan yang sensitif seperti IEP, DOD, atau dokumen kepatuhan.
- ✓ Hanya admin yang dapat membuat, menentukan struktur, dan menerbitkan label. Pengguna di organisasi Anda dapat menerapkan label ke file yang mereka edit dan dapat menetapkan nilai kolomnya.
- ✓ Label Drive dapat digunakan untuk mendukung [Pencegahan Kebocoran Data](#) otomatis.

# Petunjuk: Mengatur dokumen di seluruh domain

## Cara kerjanya

Google Drive menawarkan label dengan badge (indikator visual) dan label standar untuk membantu mengatur file di seluruh domain Anda.

## Cara mengaktifkan label Drive untuk lembaga

- Login ke konsol Admin
- Klik Menu > Aplikasi > Google Workspace > Drive dan Dokumen
- Pilih Label
- Aktifkan atau nonaktifkan label
- Klik Simpan

 Pengelolaan dan kontrol domain Alat keamanan dan insight Dokumentasi Pusat Bantuan yang relevan

- [Mengelola Label Drive](#)



Bagaimana cara mengotomatiskan keanggotaan grup sehingga setiap kali ada pendidik baru yang bergabung ke lembaga kami, ia akan dimasukkan ke milis ‘pendidik?’”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengelola keanggotaan secara otomatis dengan grup dinamis](#)

## Mengisi grup departemen secara otomatis

Grup dinamis memungkinkan administrator memperbarui keanggotaan grup di tingkat sekolah dengan kriteria kustom.


- ✓ Buat grup dinamis yang otomatis mengelola keanggotaan
- ✓ Jaga grup tetap terbaru, berdasarkan kueri keanggotaan yang Anda buat
- ✓ Gunakan grup dinamis sebagai:
  - Daftar distribusi dan email
  - Grup termoderasi dan kotak masuk kolaboratif
  - Grup keamanan

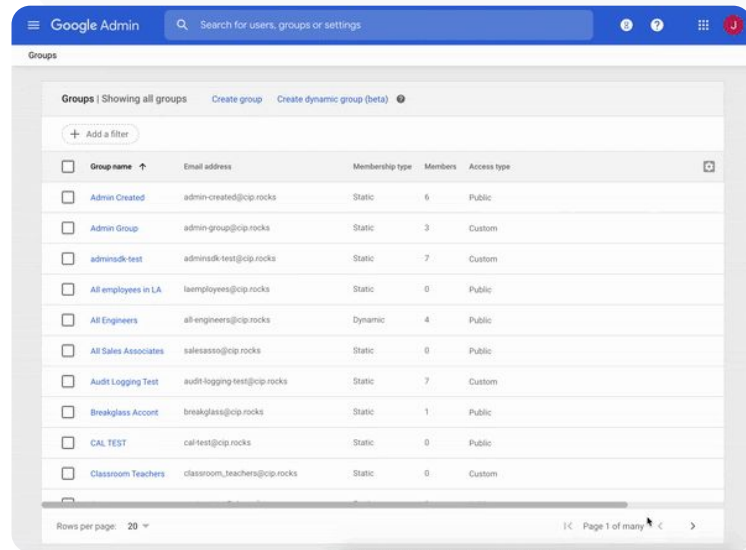
# Petunjuk: Mengisi grup secara otomatis


## Membuat grup dinamis

- Login ke konsol Admin > buka Menu > Direktori > Grup
- Klik Buat grup dinamis
- Buat kueri keanggotaan di:
  - **Daftar kondisi:** kriteria yang akan digunakan untuk keanggotaan, misalnya Departemen
  - **Kolom nilai:** nilai yang ingin digunakan.
- Masukkan informasi berikut:
  - **Nama:** mengidentifikasi grup dalam daftar dan pesan
  - **Deskripsi:** kegunaan grup
  - **Email grup:** alamat email yang digunakan untuk grup
- Klik Simpan
- Klik Selesai

 Pengelolaan dan kontrol domain

 Alat keamanan dan insight



 Dokumentasi Pusat Bantuan yang relevan

- [Mengelola keanggotaan secara otomatis dengan grup dinamis](#)



Staf kami tidak sengaja membagikan dokumen ke seluruh organisasi sehingga membahayakan data sensitif. Bagaimana cara membatasi opsi berbagi ke grup yang lebih kecil dan lebih relevan?”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Tentang target audiens](#)
- [Praktik terbaik untuk men-deploy target audiens](#)
- [Membuat target audiens](#)

## Membuat audiens untuk berbagi file internal

Setelan **target audiens** membantu meningkatkan keamanan data organisasi dengan mengurangi potensi dibagikannya file secara tidak sengaja oleh pengguna.

- ✓ Pastikan file dibagikan hanya dengan orang yang tepat, misalnya tim atau departemen tertentu
- ✓ Target audiens adalah kelompok orang yang dapat direkomendasikan kepada pengguna oleh Admin untuk diajak berbagi file
- ✓ Admin dapat menambahkan target audiens ke setelan berbagi pengguna untuk mendorong aktivitas berbagi file dengan audiens yang lebih spesifik
- ✓ Tersedia di Google Drive, Dokumen, dan Chat

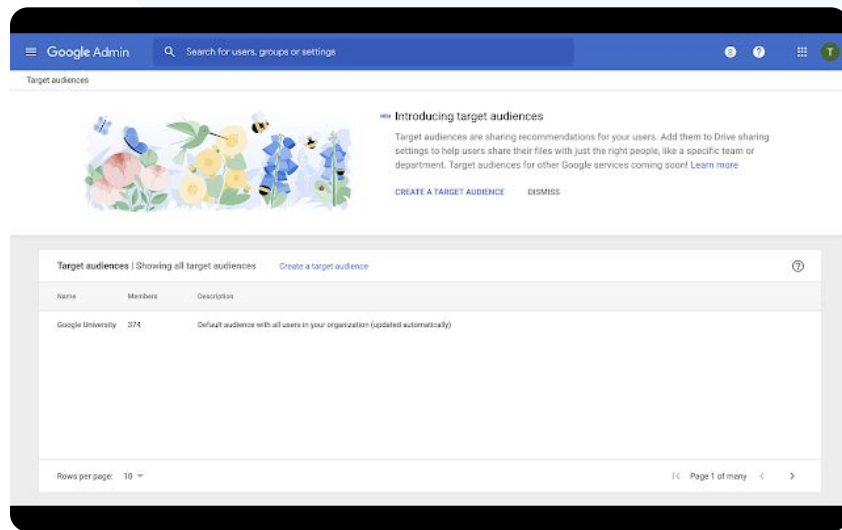
# Petunjuk: Membuat audiens untuk berbagi file internal

## Cara kerjanya

Setelah membuat target audiens, Anda dapat menambahkan anggota dan menerapkan Target audiens ke Google Drive agar tersedia di setelan berbagi pengguna. Misalnya, Anda dapat memungkinkan anggota staf melihat target audiens 'Semua Staf' ketika membagikan file Drive.

## Cara mengaktifkan label Drive untuk lembaga

- Login ke konsol Admin > buka Menu > Direktori > Target audiens
- Klik Buat target audiens
- Di bagian Nama, masukkan nama untuk target audiens tersebut
- Pilih Tambahkan anggota > masukkan anggota yang Anda inginkan
- Klik Selesai



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Tentang target audiens](#)
- [Praktik terbaik untuk men-deploy target audiens](#)
- [Membuat target audiens](#)



Bagaimana caranya agar siswa sekolah menengah tidak membagikan dokumen kepada siswa sekolah dasar?”

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Membuat dan mengelola aturan kepercayaan untuk berbagi Drive](#)

## Membatasi aktivitas berbagi file

Aturan kepercayaan Drive memungkinkan admin menetapkan aturan untuk mengontrol siapa yang dapat memperoleh akses ke file Google Drive, sehingga membantu memastikan privasi data lembaga. Kebijakan ini dapat diterapkan ke pengguna perorangan, grup, unit organisasi, dan domain.

- ✓ Amankan informasi sensitif dan jaga kepatuhan terhadap peraturan dan standar industri.
- ✓ Batasi aktivitas berbagi domain internal dan/atau eksternal. Admin dapat membuat aturan kepercayaan yang hanya mengizinkan siswa saja untuk berbagi file Drive di dalam organisasi Anda
- ✓ Setelah diaktifkan, 'Aturan kepercayaan' akan menggantikan 'Opsi berbagi' yang ada di kontrol admin Google Drive.

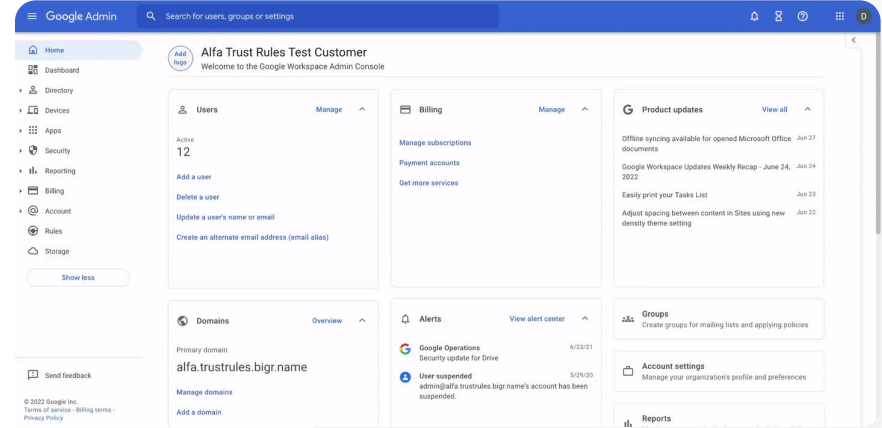
# Petunjuk: Membatasi aktivitas berbagi file

## Mengaktifkan aturan kepercayaan Drive

- Login ke konsol Admin > buka Menu > Aturan
- Pada kartu Berkolaborasi dengan aman di bagian atas halaman, klik Aktifkan aturan kepercayaan
- [Daftar tugas](#) Anda akan otomatis terbuka dan menampilkan progres aktivasi aturan kepercayaan

Admin dapat membuat aturan kepercayaan, melihat dan mengedit detail aturan kepercayaan, menghapus aturan kepercayaan, dan melihat peristiwa log aturan kepercayaan.

Kunjungi [Pusat Bantuan Admin](#) untuk mempelajari petunjuk langkah demi langkah dalam mengelola aturan kepercayaan



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Membuat dan mengelola aturan kepercayaan untuk berbagi Drive](#)





Saya ingin membatasi akses ke aplikasi tertentu saat pengguna berada di jaringan kami.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Ringkasan Akses Kontekstual](#)
- [Menetapkan tingkat Akses Kontekstual ke aplikasi](#)

## Pembatasan aplikasi Google Workspace

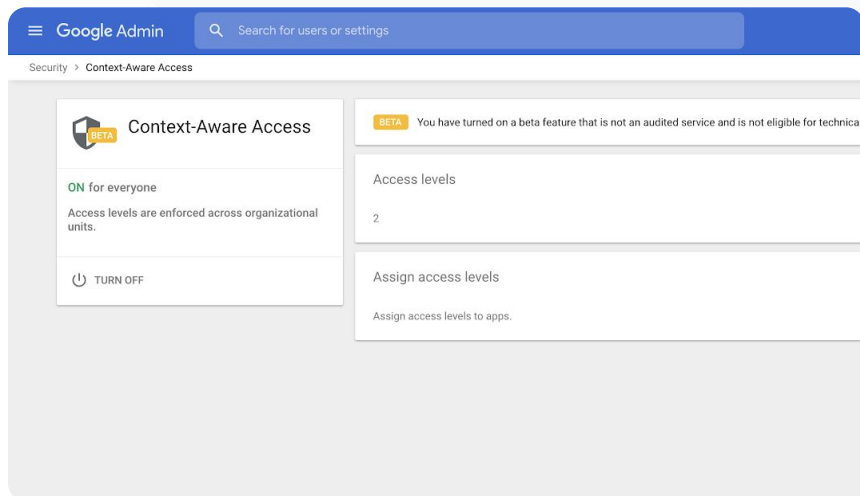
Dengan **Akses Kontekstual**, Anda dapat membuat kebijakan kontrol akses yang terperinci untuk aplikasi Google Workspace dan SAML (Security Assertion Markup Language) pihak ketiga berdasarkan berbagai atribut, seperti identitas, lokasi, status keamanan perangkat, dan alamat IP pengguna. Anda bahkan dapat membatasi akses ke aplikasi dari luar jaringan.

- ✓ Anda dapat menerapkan kebijakan Akses Kontekstual ke layanan Google Workspace for Education inti
- ✓ Misalnya, batasi akses ke aplikasi Workspace dari perangkat yang disediakan lembaga atau akses Drive hanya jika perangkat penyimpanan pengguna dienkripsi.

# Petunjuk: Membatasi penggunaan aplikasi Google Workspace

## Cara menggunakan Akses Kontekstual

- Login ke konsol Admin
- Pilih keamanan > Akses Kontekstual > tetapkan
- Pilih tetapkan tingkat akses untuk melihat daftar aplikasi Anda
- Pilih unit organisasi atau grup konfigurasi untuk mengurutkan daftar
- Pilih **Tetapkan** di samping aplikasi yang ingin Anda sesuaikan
- Pilih satu atau beberapa tingkat akses
- Buat beberapa tingkat jika Anda ingin pengguna memenuhi lebih dari satu kondisi
- Klik **Simpan**

[Pengelolaan dan kontrol domain](#)[Alat keamanan dan insight](#)[Dokumentasi Pusat Bantuan yang relevan](#)

- [Ringkasan Akses Kontekstual](#)
- [Menetapkan tingkat Akses Kontekstual ke aplikasi](#)



Saya ingin menerapkan rencana pengelolaan penyimpanan baru di seluruh domain.”

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Panduan penyimpanan bagi Admin](#)
- [Memahami ketersediaan dan penggunaan penyimpanan](#)
- [Mengosongkan ruang penyimpanan atau mendapatkan penyimpanan ekstra](#)
- [Menetapkan batas penyimpanan](#)

## Mengelola penyimpanan di seluruh domain

Lembaga yang menggunakan Google Workspace for Education mendapatkan penyimpanan gabungan dasar sebesar 100 TB—cukup untuk lebih dari 100 juta dokumen, 8 juta presentasi, atau 400.000 jam video. **Kelola penyimpanan Drive gabungan** untuk memastikan lembaga Anda menggunakan penyimpanan secara efektif.

- ✓ Gunakan berbagai alat administrator, pelaporan, dan log untuk memahami
  - Kapasitas penyimpanan yang Anda gunakan
  - Menetapkan batas penyimpanan
  - Mengidentifikasi akun yang menggunakan penyimpanan secara tidak proporsional
- ✓ Teaching and Learning Upgrade dan Education Plus menawarkan kapasitas penyimpanan tambahan selain penyimpanan dasar yang disediakan
  - Menambahkan 100 GB ke penyimpanan bersama untuk setiap lisensi Teaching and Learning Upgrade
  - Menambahkan 20 GB ke penyimpanan bersama untuk setiap lisensi Education Plus

# Petunjuk: Mengelola penyimpanan di seluruh domain

Mengidentifikasi penggunaan penyimpanan berdasarkan pengguna

- Login ke konsol Admin > buka Menu > Penyimpanan
- Lihat penggunaan penyimpanan berdasarkan organisasi dan pengguna

Menetapkan batas penyimpanan

- Di konsol Admin > Menu > Penyimpanan
- Di Setelan penyimpanan, klik Kelola
- Klik Batas penyimpanan pengguna > pilih entitas yang akan dikenai batasan:
  - **Unit organisasi:** Klik unit organisasi
  - **Grup:** Klik Grup > klik kolom penelusuran > masukkan nama grup > klik grup
- Pilih Aktif dan tetapkan kapasitas penyimpanan
- Klik Simpan

Pengelolaan dan kontrol domain

Alat keamanan dan insight

**Workspace storage**

Total used: 6 TB

- Drive: 5 TB
- Gmail: 25 GB
- Photos: 25 GB

**Storage settings**

Manage all storage limit policies for organizational units, groups and users.

[MANAGE STORAGE SETTINGS](#)

**Users using the most storage**

Steven Suits	8 TB
Zion Nicholls	6 TB
Tony Hawk	2 TB
Jane Graffius	1 TB
Laura Ulrich	600 GB

[VIEW ALL USERS](#)

**Shared drives using the most storage**

Videos	2.22 TB
Photography	1.74 TB
Marketing Drive	1.46 TB
Design Drive	1.02 TB
Assets	900 GB

[VIEW ALL SHARED DRIVES](#)

**Resources for you**

- Understanding how your organization is using shared Workspace Storage
- How to set a storage limit for members of an Organizational Unit

[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Panduan penyimpanan bagi Admin](#)
- [Memahami ketersediaan dan penggunaan penyimpanan](#)
- [Mengosongkan ruang penyimpanan atau mendapatkan penyimpanan ekstra](#)
- [Menetapkan batas penyimpanan](#)



Data siswa, pengajar, dan staf kami harus tetap berada di Uni Eropa sesuai dengan hukum yang berlaku.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Memilih lokasi geografis untuk data Anda](#)

## Peraturan data

Sebagai admin, Anda dapat memilih untuk menyimpan data di lokasi geografis tertentu, baik di Amerika Serikat maupun Inggris Raya/Eropa, menggunakan kebijakan region data.

- ✓ Pengguna Education Plus dan Education Standard dapat memilih satu region data untuk sebagian pengguna, atau region data berbeda untuk departemen tertentu, dan melihat progres pemindahan region data.
- ✓ Tempatkan pengguna di unit organisasi untuk ditetapkan berdasarkan departemen, atau tempatkan dalam grup konfigurasi untuk ditetapkan bagi pengguna di dalam atau lintas departemen.
- ✓ Pengguna yang tidak diberi lisensi Education Standard atau Education Plus tidak tercakup dalam kebijakan region data.



Hasil riset pengajar kami harus tetap berada di Amerika Serikat sesuai dengan ketentuan dalam peraturan hibah.”



 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Memilih lokasi geografis untuk data Anda](#)

## Peraturan hibah

Sebagai administrator, Anda dapat memilih untuk menyimpan hasil riset pengajar di lokasi geografis tertentu (Amerika Serikat atau Eropa) menggunakan kebijakan region data.

-  Kebijakan region data mencakup data dalam penyimpanan utama (termasuk cadangan) untuk sebagian besar Layanan Inti Google Workspace for Education, yang tercantum [di sini](#)
-  Pertimbangkan konsekuensinya sebelum menetapkan kebijakan region data karena, dalam beberapa kasus, pengguna di luar region tempat data mereka berada mungkin mengalami latensi yang lebih tinggi

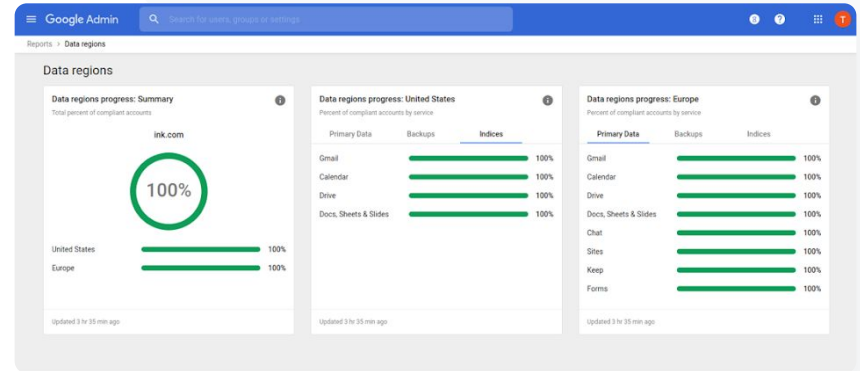
# Petunjuk: Peraturan data

## Cara menetapkan region data

- Login ke konsol Admin
  - **Catatan:** Harus login sebagai admin super
- Klik profil perusahaan > tampilkan lainnya > region data
- Pilih unit organisasi atau grup konfigurasi yang ingin Anda batasi ke sebuah region, atau pilih seluruh kolom untuk menyertakan semua unit dan grup
- Pilih region Anda, termasuk tidak ada preferensi, Amerika Serikat, Eropa
- Klik Simpan

Pengelolaan dan kontrol domain

Alat keamanan dan insight



[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Memilih lokasi geografis untuk data Anda](#)



Saya perlu cara untuk mengelola dan mengirim kebijakan ke semua jenis perangkat – iOS, Windows 10, dll. – di seluruh distrik saya, bukan hanya Chromebook, terutama jika ada yang disusupi.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengelola perangkat dengan pengelolaan Endpoint Google](#)
- [Menyiapkan pengelolaan seluler lanjutan](#)

## Mengelola perangkat endpoint

Pengelolaan endpoint perusahaan memberi Anda kontrol lebih besar atas data organisasi melalui perangkat seluler. Batasi fitur perangkat seluler, wajibkan enkripsi perangkat, kelola aplikasi di perangkat Android atau iPhone dan iPad, bahkan hapus total data dari perangkat.

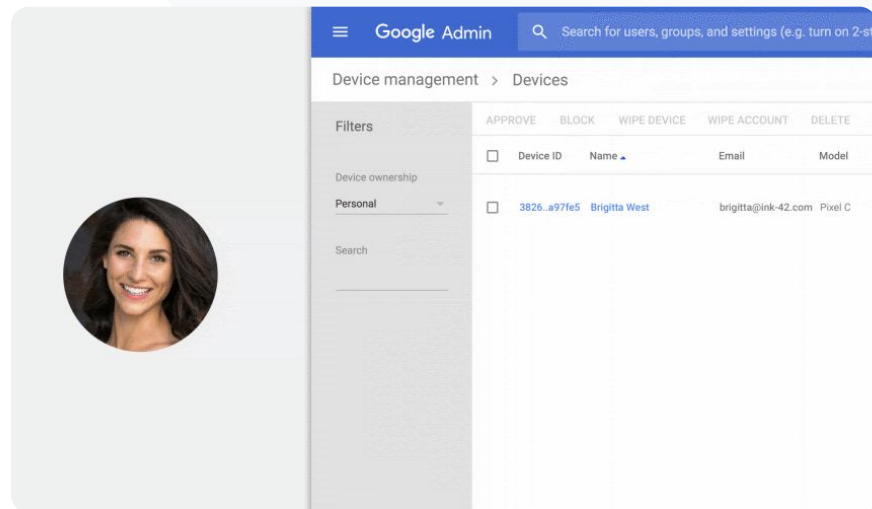
- ✓ Anda dapat menyetujui, memblokir, berhenti memblokir, atau menghapus perangkat dari konsol Admin.
- ✓ Jika seseorang kehilangan perangkat atau dikeluarkan dari sekolah, Anda dapat menghapus total akun pengguna, profilnya, atau bahkan semua data dari perangkat modul terkelola tertentu. Data ini akan tetap tersedia di komputer atau browser web.



# Petunjuk: Mengelola perangkat endpoint

## Petunjuk terkait pengelolaan seluler lanjutan

- Login ke konsol Admin
- Dari konsol Admin > perangkat
- Di bagian kiri, klik **setelan > setelan universal**
- Klik **umum > pengelolaan seluler**
- Untuk menerapkan setelan ke semua orang, biarkan unit organisasi teratas dipilih. Jika tidak, pilih unit organisasi turunan.
- Pilih **lanjutan**.
- Klik **Simpan**



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Mengelola perangkat dengan pengelolaan Endpoint Google](#)
- [Menyiapkan pengelolaan seluler lanjutan](#)



Sebagian pendidik kami menggunakan perangkat Windows 10. Bagaimana cara mengelola semua perangkat lembaga kami di satu tempat?”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan pengelolaan perangkat Windows](#)
- [Mendaftarkan perangkat di pengelolaan perangkat Windows](#)

## Mengelola perangkat Microsoft Windows

Kelola dan amankan perangkat Windows 10 lembaga Anda melalui konsol Admin, sebagaimana yang Anda lakukan untuk perangkat Android, iOS, Chrome, dan Jamboard.

- ✓ Aktifkan Single Sign-On sehingga pengguna dapat dengan mudah mengakses Google Workspace di perangkat Windows 10 miliknya
- ✓ Pastikan perangkat yang digunakan untuk mengakses Google Workspace diupdate, aman, dan memenuhi standar kepatuhan dengan mengelola perangkat di konsol Admin
- ✓ Hapus total perangkat, kirim update konfigurasi perangkat, dan sebagainya ke perangkat Windows 10 dari cloud

# Petunjuk: Mengelola perangkat Microsoft Windows

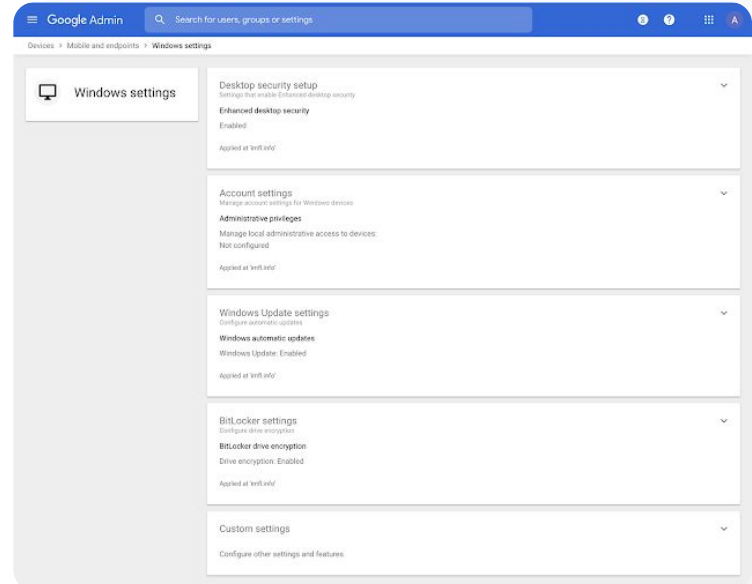
## Mengaktifkan pengelolaan perangkat Windows


- Di konsol Admin, buka Menu > Perangkat > Seluler dan endpoint > Setelan > Setelan Windows
- Pilih Penyiapan pengelolaan Windows
- Untuk menerapkan setelan ke semua orang, biarkan unit organisasi teratas dipilih
- Di samping Pengaktifan perangkat Windows, pilih Diaktifkan
- Klik Simpan



Pengelolaan dan kontrol domain

Alat keamanan dan insight



 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan pengelolaan perangkat Windows](#)
- [Mendaftarkan perangkat di pengelolaan perangkat Windows](#)



Bagaimana cara menyiapkan profil Wi-Fi di perangkat Windows 10?"

🔗 [Petunjuk langkah demi langkah](#)

🔗 Dokumentasi Pusat Bantuan yang relevan

- [Setelan kustom umum](#)
- [Menambahkan setelan kustom](#)

## Setelan kustom untuk perangkat Windows 10

Dengan fitur pengelolaan perangkat Windows dari Google, Admin dapat menambahkan setelan kustom ke perangkat lembaganya.

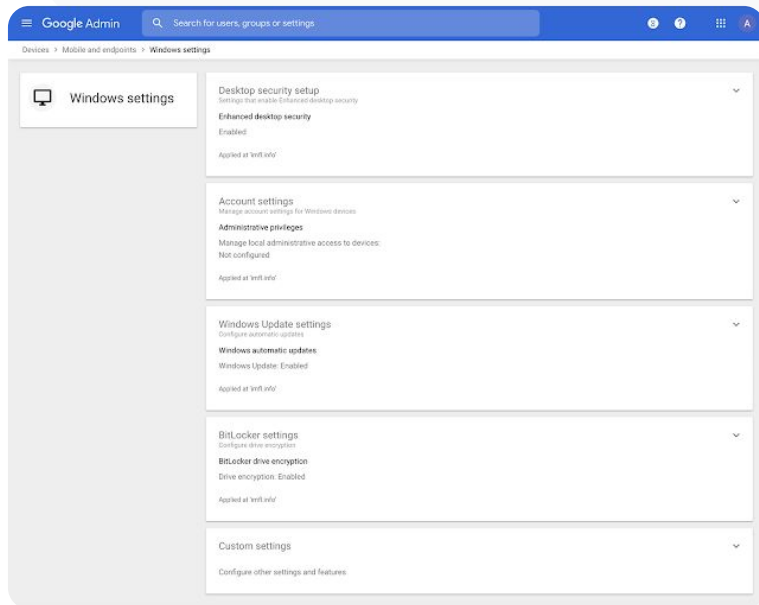
- ✓ Kontrol setelan perangkat kustom dari konsol Admin
- ✓ Terapkan setelan pada:
  - Pengelolaan perangkat
  - Keamanan
  - Hardware dan jaringan
  - Software
  - Privasi

# Petunjuk: Setelan kustom untuk perangkat Windows 10

## Menambahkan setelan kustom baru

- Di konsol Admin, buka Menu > Perangkat > Seluler dan endpoint > Setelan > Setelan Windows
- Pilih Setelan kustom
- Klik Tambahkan setelan kustom > dan isi kolom yang diminta
- Klik Berikutnya
- Pilih unit organisasi tempat Anda ingin menerapkan setelan
- Klik Terapkan

Perlu diperhatikan bahwa Google tidak memberikan dukungan teknis atau bertanggung jawab atas produk atau setelan pihak ketiga.




[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Setelan kustom umum](#)
- [Menambahkan setelan kustom](#)



Kami ingin memastikan perangkat Windows 10 di lembaga kami mendapatkan update terbaru.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengelola update otomatis](#)

## Mengotomatiskan update untuk perangkat Windows 10

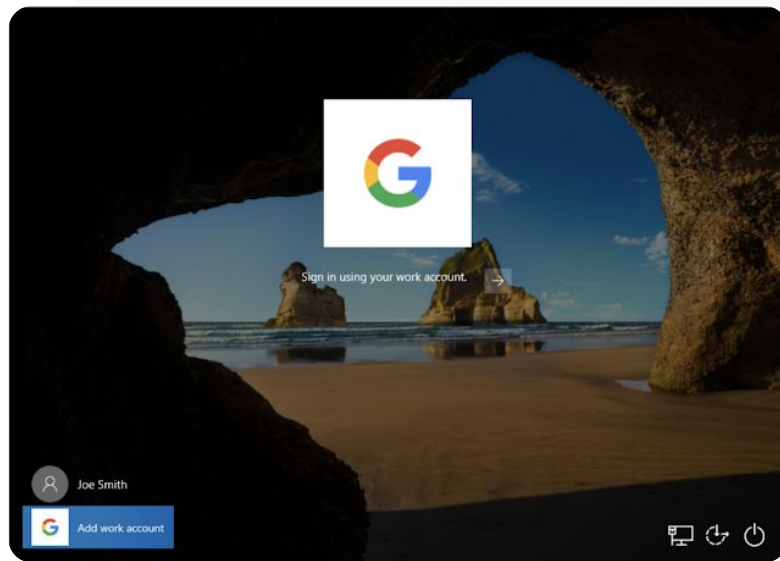
Tentukan bagaimana dan kapan perangkat Windows 10 lembaga Anda menerima update keamanan dan download penting lainnya melalui layanan update otomatis Windows.

- ✓ Atur notifikasi untuk mendownload update dari panel kontrol Windows Update, setel jam kapan reboot update tidak dijadwalkan, dan sebagainya
- ✓ Terapkan setelan ke seluruh lembaga atau unit organisasi tertentu
- ✓ Perubahan dapat membutuhkan waktu hingga 24 jam, tetapi biasanya berlangsung lebih cepat

# Petunjuk: Mengotomatiskan update untuk perangkat Windows 10

## Mengonfigurasi update

- Di konsol Admin, buka Menu > Perangkat > Seluler dan endpoint > Setelan > Setelan Windows
- Pilih Setelan Windows Update > Diaktifkan
- Di samping Pengaktifan perangkat Windows, pilih Diaktifkan
- Konfigurasi opsi berikut, [antara lain](#):
  - Menerima update untuk aplikasi Microsoft
  - Perilaku update otomatis
  - Mengotomatiskan frekuensi update
- Klik **Simpan**

[Pengelolaan dan kontrol domain](#)[Alat keamanan dan insight](#)[Dokumentasi Pusat Bantuan yang relevan](#)

- [Mengelola update otomatis](#)



Kami tahu Google memiliki standar tertinggi terkait enkripsi data, tetapi kami ingin mengontrol kunci enkripsi untuk kekayaan intelektual dan riset hibah universitas.”



[Petunjuk langkah demi langkah](#)



Dokumentasi Pusat Bantuan yang relevan

- [Tentang enkripsi sisi klien](#)

## Memanfaatkan enkripsi sisi klien

Google Workspace telah menggunakan standar kriptografi terbaru untuk mengenkripsi semua data dalam penyimpanan maupun data dalam pengiriman di antara fasilitasnya. Dengan **enkripsi sisi klien**, Admin memiliki kontrol langsung atas kunci enkripsi dan Penyedia Identitas yang digunakan untuk mengakses kunci tersebut.



Gunakan kunci enkripsi Anda sendiri untuk mengenkripsi data sensitif, seperti kekayaan intelektual lembaga Anda



Enkripsi konten ditangani di browser Anda sebelum data dikirim atau disimpan di penyimpanan berbasis cloud Google.



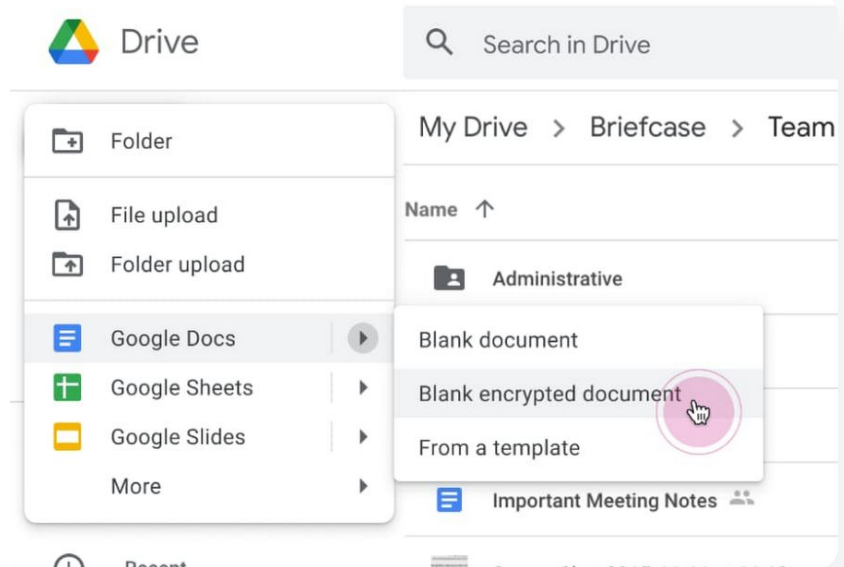
Pilih pengguna yang dapat membuat konten terenkripsi sisi klien dan membagikannya secara internal atau eksternal



# Petunjuk: Memanfaatkan enkripsi sisi klien

## Menyiapkan enkripsi sisi klien (CSE)

- Menyiapkan layanan kunci enkripsi
  - Lindungi data Anda dengan kapabilitas pengelolaan dan kontrol kunci enkripsi dengan [membuat layanan kunci enkripsi](#)
- Menghubungkan Google Workspace ke layanan kunci enkripsi eksternal
  - [Tambahkan dan kelola layanan kunci enkripsi](#) untuk enkripsi sisi klien dengan menyertakan URL layanan kunci enkripsi di konsol Admin
- Menetapkan layanan kunci enkripsi ke unit organisasi atau grup
  - [Tetapkan satu layanan kunci enkripsi](#) sebagai default untuk seluruh lembaga
- Menghubungkan Google Workspace ke IdP
  - [Hubungkan Penyedia Identitas](#) (IdP) untuk enkripsi sisi klien guna memverifikasi identitas pengguna sebelum mengizinkan mereka mengenkripsi konten atau mengakses konten terenkripsi
- Mengaktifkan CSE untuk pengguna
  - [Aktifkan enkripsi sisi klien](#) untuk mendukung unit organisasi atau grup yang penggunanya perlu membuat konten terenkripsi sisi klien



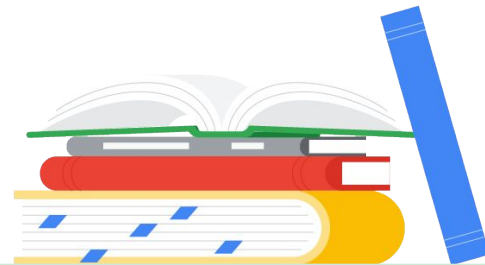
[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Tentang enkripsi sisi klien](#)



# Kapabilitas pengajaran dan pembelajaran

Bekali pendidik Anda dengan kapabilitas tambahan di lingkungan pembelajaran digital Anda dengan pengalaman kelas yang diperkaya, alat untuk mendorong integritas akademik, dan komunikasi video yang ditingkatkan.



[Google Classroom](#)



[Laporan keaslian](#)



[Dokumen, Spreadsheet, dan Slide](#)



[Google Meet](#)



## Apa ini?

Google Classroom adalah tempat terpusat Anda untuk pengajaran dan pembelajaran. Fitur-fitur berbayar Classroom membantu menghimpun aneka alat kelas di satu tempat. Pendidik dapat mengakses alat favoritnya langsung di Classroom, dan menjaga sinkronisasi daftar kelas dengan sistem eksternal.

## Kasus penggunaan

[Mengelola akses ke add-on Classroom](#)



[Petunjuk langkah demi langkah](#)

[Mengintegrasikan konten yang menarik di Classroom](#)

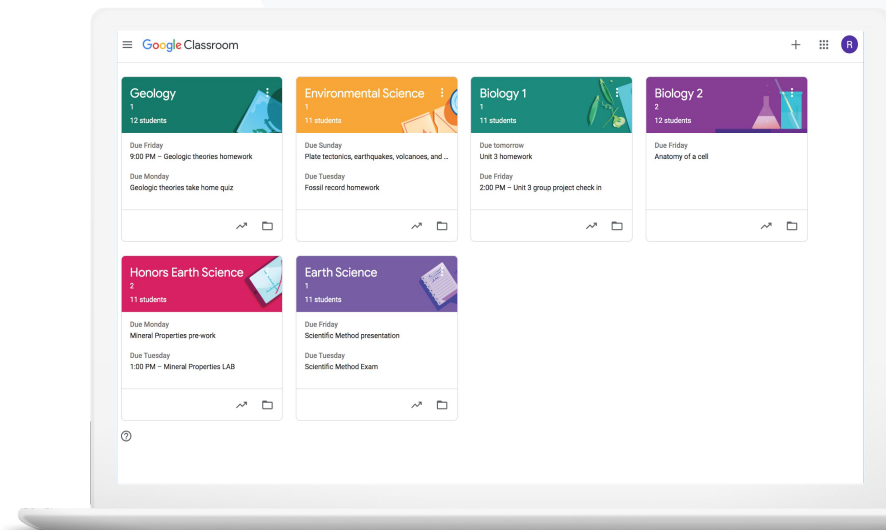


[Petunjuk langkah demi langkah](#)

[Membuat kelas dalam skala besar](#)



[Petunjuk langkah demi langkah](#)





Kami berharap ada cara untuk menyediakan akses single sign-on ke alat-alat Teknologi Pendidikan favorit pendidik kami. ”

[🔗 Petunjuk langkah demi langkah](#)

[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Mengelola aplikasi Google Workspace Marketplace](#)
- [Menggunakan add-on di Classroom](#)
- [Mengelola aplikasi Marketplace dalam daftar yang diizinkan](#)
- [Mendistribusikan aplikasi Marketplace kepada pengguna](#)
- [Add-on Classroom \[Panduan Memulai untuk Pengajar\]](#)

## Mengelola akses ke add-on Classroom

Tentukan aplikasi pendidikan pihak ketiga yang dapat diakses lembaga Anda dengan daftar domain yang diizinkan. Dukung pendidik agar dapat dengan mudah menginstal add-on dan menyertakannya ke dalam tugas siswa, hanya dengan beberapa klik.

- ✓ Buat daftar yang diizinkan di seluruh domain Anda untuk menentukan aplikasi pihak ketiga yang dapat diinstal pendidik dari Google Workspace Marketplace.
- ✓ Dukung hasil pembelajaran dengan aplikasi pendidikan pelengkap. Pendidik dapat menetapkan, meninjau, dan memberikan nilai langsung dari dalam Google Classroom.
- ✓ Google Workspace Marketplace mencakup Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google Seni & Budaya, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora, Wordwall, dan banyak lagi.

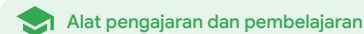
# Petunjuk: Mengelola akses ke add-on Classroom

## Mengelola akses add-on dengan daftar domain yang diizinkan

- Di konsol Admin, pilih Menu > Aplikasi Google Workspace Marketplace > Daftar aplikasi
- Pilih Izinkan aplikasi
- Masukkan nama add-on yang diinginkan atau telusuri untuk menemukannya
- Klik Pilih dan pastikan Izinkan pengguna menginstal aplikasi ini dipilih
- Klik Lanjutkan dan Selesai

## Memberikan akses add-on ke daftar diizinkan yang diinginkan

- Di konsol Admin, pilih Menu > Aplikasi Google Workspace Marketplace > Daftar aplikasi
- Pilih add-on yang ingin didistribusikan
- Di bagian Akses Pengguna, klik Lihat grup dan unit organisasi
- Pilih antara tersedia bagi semua orang atau persempit akses ke grup atau unit organisasi tertentu
- Klik Simpan



Apps > Settings for Google Workspace Marketplace apps

### Google Workspace Marketplace Settings

#### Manage access to apps

##### Allow install

Settings to install third-party Google Workspace Marketplace apps:

- Allow users to install any app from Google Workspace Marketplace
- Block users from installing any app from Google Workspace Marketplace  
Previously-installed apps will not be uninstalled.
- Allow users to install only allowed applications from Google Workspace Marketplace  
[Manage allowlist](#)
  - 1 Users in your organization can install apps in the allowlist. Apps no longer allowed will not be uninstalled.
  - 1 Changes may take up to 24 hours to propagate to all users. Prior changes can be seen in [Audit log](#)

1 unsaved change CANCEL SAVE

## Dokumentasi Pusat Bantuan yang relevan

- [Mengelola aplikasi Google Workspace Marketplace](#)
- [Mengggunakan add-on di Classroom](#)
- [Mengelola aplikasi Marketplace dalam daftar yang diizinkan](#)
- [Mendistribusikan aplikasi Marketplace kepada pengguna](#)
- [Add-on Classroom \[Panduan Memulai untuk Pengajar\]](#)



Saya ingin menugaskan dan memberi nilai game pembelajaran Kahoot! untuk siswa saya tanpa keluar dari Google Classroom.”



[Petuniuk langkah demi langkah](#)



[Dokumentasi Pusat Bantuan yang relevan](#)

- [Menggunakan add-on di Classroom](#)
- [Add-on Classroom \[Panduan Memulai untuk Pengajar\]](#)

## Mengintegrasikan konten yang menarik di Classroom

Dengan add-on Classroom pendidik dapat membagikan aktivitas dan konten yang menarik kepada siswa dengan menambahkan add-on ke tugas, pertanyaan, materi, atau pengumuman dalam Classroom.



Buat agar pendidik dan siswa dapat menggunakan alat favorit mereka, seperti Kahoot!, Nearpod, dan Pear Deck, tanpa harus keluar dari Classroom



Dengan add-on, siswa tidak perlu mengelola beberapa sandi atau membuka situs eksternal



Beri nilai dan tinjau tugas siswa melalui add-on, langsung dalam Classroom



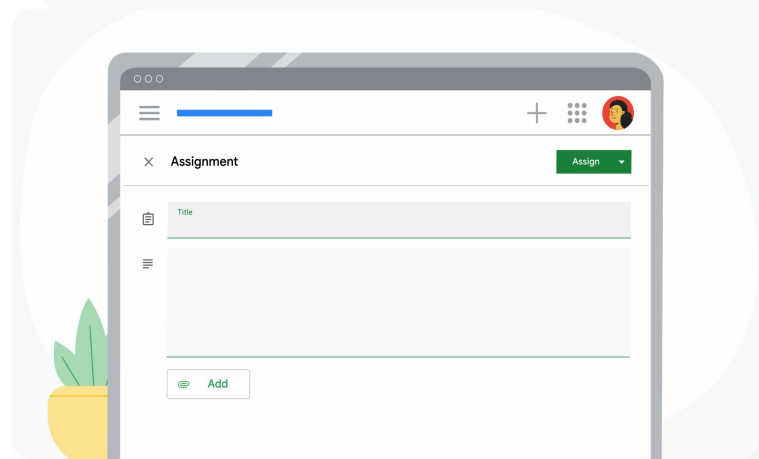
## Petunjuk: Mengintegrasikan konten yang menarik di Classroom

### Cara menambahkan add-on ke tugas, kuis, atau pertanyaan

- Login ke akun Classroom Anda di [classroom.google.com](https://classroom.google.com)
- Pilih kelas yang relevan dari daftar, lalu pilih Tugas kelas
- Pilih **Buat** > tentukan apa yang ingin Anda buat
- Masukkan judul dan petunjuk
- Di bagian **Add-on**, pilih add-on yang ingin Anda gunakan
- Pilih **Tugaskan**

### Cara menambahkan add-on ke pengumuman

- Dari dalam halaman Forum kelas, pilih **Umumkan sesuatu ke kelas Anda**
- Masukkan pengumuman
- Di bagian **Add-on**, pilih add-on yang ingin Anda gunakan
- Pilih **Posting**



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan add-on di Classroom](#)
- [Add-on Classroom \[Panduan Memulai untuk Pengajar\]](#)



Saya memerlukan cara untuk mengotomatiskan persiapan kelas dan mengelola daftar nama siswa di Google Classroom.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Memulai impor daftar nama siswa SIS](#)
- [Menyiapkan impor Daftar Nama Siswa SIS melalui Clever](#)

## Membuat kelas dalam skala besar

Impor Daftar Nama Siswa SIS memungkinkan pembuatan kelas secara otomatis dan menjaga daftar kelas tetap sinkron dengan sistem informasi siswa (SIS) sekolah Anda menggunakan Clever.

- ✓ Tersedia untuk distrik sekolah dasar dan menengah di Amerika Serikat dan Kanada yang menggunakan Education Plus
- ✓ Admin dapat mengimpor daftar nama siswa kelas dari SIS ke Google Classroom untuk menyiapkan kelas secara otomatis
- ✓ Otomatiskan dan kelola daftar kelas di Google Classroom dengan lancar





# Petunjuk: Membuat kelas dalam skala besar

## Cara menyiapkan impor Daftar Nama Siswa SIS

- Siapkan sinkronisasi daftar nama siswa Google Classroom di Clever
- Administrator Distrik Anda di Clever dan Admin Super Google Workspace dapat [mengikuti petunjuk langkah demi langkah dari Clever](#)

## Jika distrik Anda tidak memiliki akun Clever:

- Buat [akun Clever](#)

## Jika distrik Anda memiliki akun Clever:

- Minta impor daftar nama siswa dari [dasbor Clever](#)

[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Menyiapkan impor Daftar Nama Siswa SIS melalui Clever](#)



# Laporan keaslian

## Apa ini?

Laporan keaslian memungkinkan pendidik dan siswa memeriksa keaslian tugas menggunakan Google Penelusuran untuk membandingkan tugas siswa dengan miliaran halaman web dan lebih dari 40 juta buku. Fitur berbayar laporan keaslian memberikan akses tanpa batas yang memungkinkan pendidik memindai kiriman siswa berdasarkan repositori tugas siswa sebelumnya yang dimiliki sekolah.

## Kasus penggunaan

[Memeriksa plagiarisme](#)



[Petunjuk langkah demi langkah](#)

[Memeriksa keaslian berdasarkan tugas siswa sebelumnya](#)

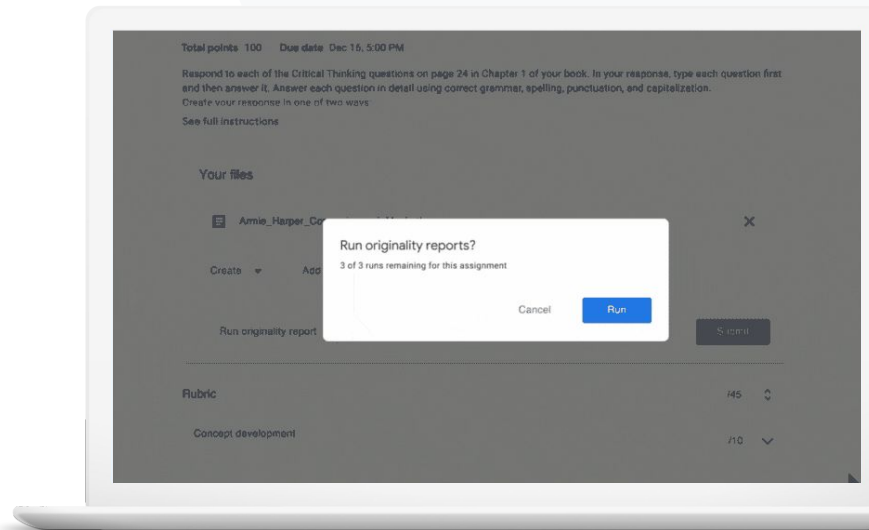


[Petunjuk langkah demi langkah](#)

[Mengubah deteksi plagiarisme menjadi peluang belajar](#)




[Petunjuk langkah demi langkah](#)





Saya ingin memeriksa tugas siswa untuk mengetahui apakah ada plagiarisme atau kutipan yang salah.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan laporan keaslian](#)
- [Laporan keaslian dan privasi](#)

## Memeriksa plagiarisme

Pengajar dapat memeriksa keaslian tugas siswanya menggunakan **laporan keaslian**. Laporan ini ditautkan ke sumber-sumber yang terdeteksi dan menandai teks yang dikutip dengan tidak semestinya.

- ✓ Jalankan laporan keaslian pada dokumen Slide, Dokumen, dan Microsoft Word
- ✓ Pendidik yang menggunakan Teaching and Learning Upgrade atau Education Plus dapat:
  - Mengakses laporan keaslian tanpa batas
  - Membandingkan kecocokan antar-siswa dengan repositori kiriman tugas sebelumnya yang dimiliki sekolah

Data Anda tetap menjadi milik Anda—tanggung jawab kami adalah menjaga privasi dan keamanannya.

# Petunjuk: Memeriksa plagiarisme

## Mengaktifkan laporan keaslian untuk tugas di Classroom

- Login ke akun Classroom Anda di [classroom.google.com](https://classroom.google.com)
- Pilih kelas yang relevan dari daftar, lalu pilih tugas kelas
- Pilih buat > tugas
- Centang kotak di samping laporan keaslian untuk mengaktifkannya

## Menjalankan laporan keaslian pada tugas Anda

- Pilih file siswa yang relevan dari daftar, lalu klik untuk membuka file tersebut pada alat penilaian
- Pada tugas siswa, klik Periksa keaslian

## Mengaktifkan laporan keaslian untuk tugas di LMS

- Login ke Sistem Pengelolaan Pembelajaran
- Pilih kursus yang relevan
- Buat tugas > pilih Google Tugas
- Centang kotak aktifkan laporan keaslian

Originality report  
Lauren 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,"<sup>[1]</sup> Lady Macbeth foreshadows danger through Macbeth's poses.

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

The presence of a state of Hell is evident in the film. Unlike the witches' cave in Shakespeare's cave, 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)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Classroom: Mengaktifkan laporan keaslian](#)
- [Google Tugas: Mengaktifkan laporan keaslian](#)



Bagaimana caranya agar pengajar dapat membandingkan tugas siswa dengan kiriman siswa dari tahun-tahun sebelumnya untuk mengetahui ada tidaknya plagiarisme?”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan laporan keaslian](#)
- [Mengaktifkan kecocokan di sekolah untuk laporan keaslian di Classroom](#)

## Memeriksa keaslian berdasarkan tugas siswa sebelumnya

Kecocokan di sekolah pada laporan keaslian memungkinkan pendidik membandingkan tugas siswa dengan kiriman siswa sebelumnya dengan memindai tugas siswa berdasarkan repositori tugas siswa yang dimiliki lembaga.



Bandingkan kecocokan antar-siswa berdasarkan tugas siswa saat ini dan sebelumnya untuk mendeteksi plagiarisme, dengan Teaching and Learning Upgrade atau Education Plus

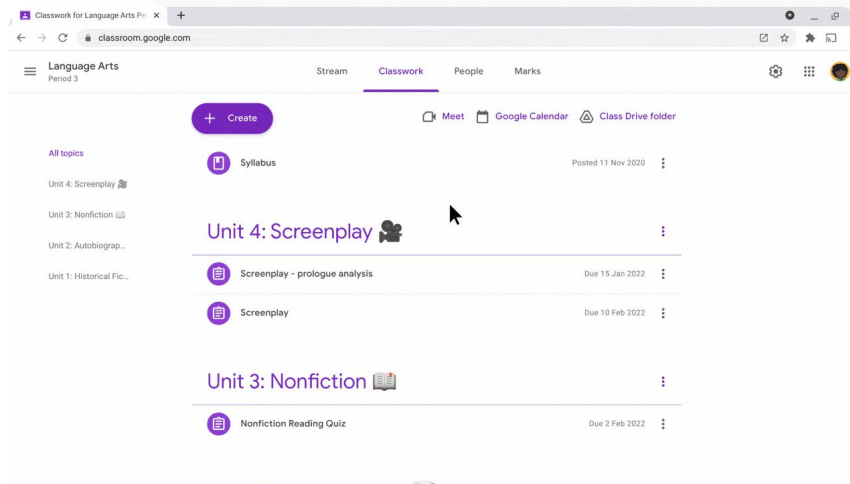


Tugas siswa dapat disimpan dan diisi ulang dengan aman dalam repositori tingkat domain dan pribadi yang dimiliki sekolah

## Petunjuk: Memeriksa keaslian berdasarkan tugas siswa sebelumnya

Cara mengaktifkan kecocokan di sekolah untuk laporan keaslian

- Di konsol Admin, pilih Menu > Aplikasi > Layanan Google tambahan > Classroom
- Pilih unit organisasi pengajar
- Klik Laporan keaslian > centang kotak Aktifkan kecocokan di sekolah untuk laporan keaslian
- Klik Simpan




 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan kecocokan di sekolah untuk laporan keaslian di Classroom](#)



Saya ingin memberi para siswa peluang belajar terkait cara mengutip sumber dengan benar.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Menjalankan laporan keaslian pada tugas](#)

## Mengubah deteksi plagiarisme menjadi peluang belajar

Siswa dapat mengidentifikasi teks yang dikutip dengan tidak semestinya dan plagiarisme yang tidak disengaja sebelum mereka menyerahkan tugas dengan menjalankan laporan keaslian hingga tiga kali per tugas. Laporan keaslian membandingkan tugas siswa dengan berbagai sumber dan menandai teks yang dikutip dengan tidak semestinya, sehingga memberi mereka kesempatan untuk belajar, memperbaiki kesalahan, dan menyerahkan tugas sekolah mereka dengan percaya diri.



Di Teaching and Learning Upgrade dan Education Plus, pendidik dapat menggunakan laporan keaslian sesering yang diinginkan, sedangkan di Education Fundamentals mereka hanya dapat mengaktifkan fitur ini lima kali per kelas.



Setelah tugas diserahkan, Classroom akan otomatis menjalankan laporan yang hanya dapat dilihat oleh pengajar. Jika Anda membatalkan pengiriman dan mengirim ulang tugas, Classroom akan menjalankan laporan keaslian lagi untuk pengajar.

# Petunjuk: Mengubah deteksi plagiarisme menjadi peluang belajar

## Cara siswa menjalankan laporan keaslian di Classroom

- Login ke akun Classroom Anda di [classroom.google.com](https://classroom.google.com)
- Pilih kelas yang relevan dari daftar, lalu pilih tugas kelas
- Pilih tugas yang relevan dari daftar, lalu klik lihat tugas
- Pada tugas Anda, pilih upload atau buat file Anda
- Di samping laporan keaslian, klik jalankan
- Untuk membuka laporan, klik lihat laporan keaslian di bawah nama tugas file
- Untuk merevisi tugas guna menulis ulang atau mengutip bagian yang ditandai dengan benar, klik edit di bagian bawah

Siswa dapat menjalankan [laporan keaslian dari dalam LMS](#), menggunakan Google Tugas.

Laporan keaslian

Alat pengajaran dan pembelajaran

### 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," 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 creaking of a raven and humming 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 Cawdor. Through the figurine, the characters and the viewers, alike, are fooled 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 cave, the scenes of the film reveal their prophecies in an industrial room, only accessible through a cage-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 x

#### 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.macbeththegreatestofalltimeeverimportant...>

Dokumentasi Pusat Bantuan yang relevan

- [Menjalankan laporan keaslian di Classroom](#)
- [Menjalankan laporan keaslian di LMS](#)





# Dokumen, Spreadsheet, dan Slide

## Apa ini?

Dokumen, Spreadsheet, dan Slide memungkinkan komunitas sekolah berkolaborasi, berkreasi bersama, meninjau, dan mengedit secara bersamaan dan real time. Dengan fitur-fitur berbayar di Education Plus, pendidik dan admin dapat menerapkan proses persetujuan untuk dokumen internal di seluruh lembaga Anda.

## Kasus penggunaan

[Menyetujui dokumen internal](#)



[Petunjuk langkah demi langkah](#)





Departemen sains sedang mengembangkan kurikulum baru.

Bagaimana mereka dapat memastikan bahwa usulan kurikulum mereka disetujui oleh semua pemimpin departemen?"

[Petunjuk langkah demi langkah](#)

[Dokumentasi Pusat Bantuan yang relevan](#)

- [Mengelola persetujuan](#)

## Menyetujui dokumen internal

Dengan **Persetujuan**, komunitas sekolah Anda dapat mengirimkan dokumen di Google Drive melalui proses persetujuan formal.

- ✓ Peninjau dapat menyetujui, menolak, atau memberikan masukan atas dokumen tersebut secara langsung di Drive, Dokumen, dan aplikasi Google Workspace lainnya
- ✓ Pemberi persetujuan dapat membuka link ke dokumen tempat mereka dapat meninjau, memberikan komentar, dan menolak atau menyetujui dokumen tersebut
- ✓ Kelola persetujuan atas kontrak atau karyawan baru, setuju perubahan dokumen sebelum dipublikasikan, dan banyak lagi

# Petunjuk: Menyetujui dokumen internal

 Dokumen, Spreadsheet, dan Slide


Alat pengajaran dan pembelajaran

## Cara kerjanya

Administrator dapat mengontrol bagaimana pengguna dan file ambil bagian dalam proses persetujuan.

## Cara mengelola persetujuan

- Login ke konsol Admin > buka Menu > Aplikasi > Google Workspace > Drive dan Dokumen
- Klik Persetujuan
- Untuk menerapkan setelan ke semua orang, pilih unit organisasi turunan atau grup konfigurasi
- Klik Simpan


[Dokumentasi Pusat Bantuan yang relevan](#)

- [Mengelola persetujuan](#)



## Apa ini?

Fitur lanjutan Google Meet mencakup live streaming, ruang kerja kelompok, rapat dengan kapasitas lebih besar, rekaman rapat, teks terjemahan langsung, dan banyak lagi.

## Kasus penggunaan

[Merekam rapat](#)



[Petunjuk langkah demi langkah](#)

[Merujuk topik yang telah dibahas di kelas](#)



[Petunjuk langkah demi langkah](#)

[Menghilangkan kendala bahasa](#)



[Petunjuk langkah demi langkah](#)

[Menyiarkan pertemuan dan acara sekolah](#)



[Petunjuk langkah demi langkah](#)

[Mengajukan pertanyaan](#)



[Petunjuk langkah demi langkah](#)

[Mengumpulkan masukan](#)



[Petunjuk langkah demi langkah](#)

[Grup kecil siswa](#)



[Petunjuk langkah demi langkah](#)

[Melacak kehadiran](#)



[Petunjuk langkah demi langkah](#)



Lembaga kami menawarkan kelas pengembangan profesi online berskala besar dan kami perlu merekamnya untuk pendidik yang tidak dapat hadir.”



[Petunjuk langkah demi langkah](#)



Dokumentasi Pusat Bantuan yang relevan

- [Merekam rapat video](#)

## Merekam rapat

Dengan Teaching and Learning Upgrade dan Education Plus, pendidik dapat merekam pelajaran, rapat pengajar, pelatihan pengembangan profesi, dan banyak lagi. Rapat akan otomatis disimpan ke Drive.



Rekaman disimpan ke Drive penyelenggara rapat. Sebelum merekam, pastikan ada cukup ruang penyimpanan di Drive

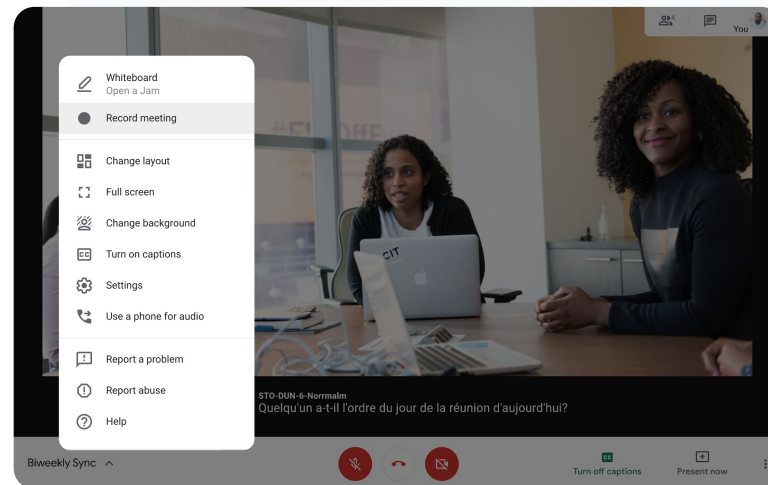


Sebaiknya admin TI mengaktifkan perekaman hanya untuk pengajar dan staf saja

# Petunjuk: Merekam rapat

## Cara mulai merekam

- Mulai atau gabung ke rapat di Google Meet
- Klik **Aktivitas > Perekaman**
- Pilih **Mulai merekam**
- Di jendela yang terbuka, klik **Mulai**
- Titik merah akan muncul di pojok kanan bawah layar untuk menunjukkan bahwa rapat sedang direkam
- File video rapat akan otomatis disimpan ke Drive Anda



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Merekam rapat video](#)

## Petunjuk: Melihat dan membagikan rekaman

### Cara mulai merekam

- Pilih filenya
- Klik ikon bagikan
- Tambahkan audiens yang disetujui

ATAU

- Pilih ikon link
- Tempel link di email atau pesan Chat

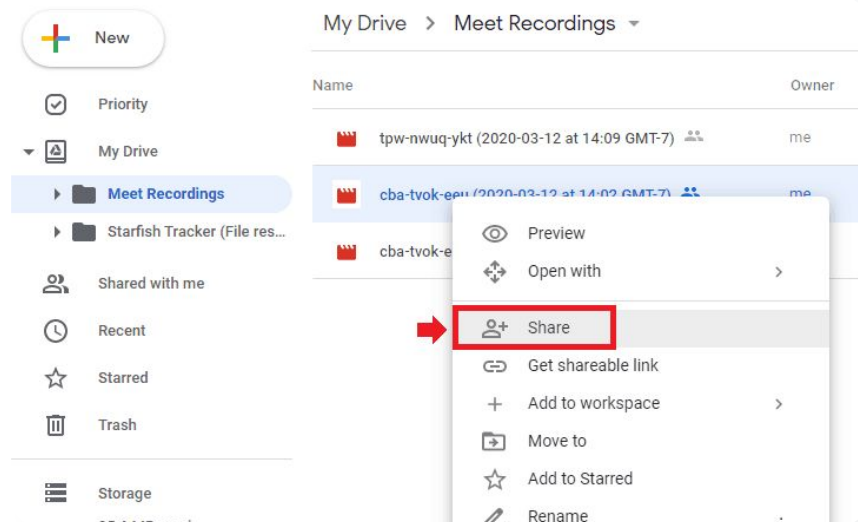
### Cara mendownload rekaman

- Pilih filenya
- Klik ikon lainnya > download
- Klik dua kali file yang telah didownload untuk memutarinya

### Cara memutar rekaman dari Drive

- Di Drive, klik dua kali file rekaman untuk memutarinya; pesan "masih memproses" akan muncul hingga file siap untuk dilihat secara online
- Untuk menambahkan rekaman ke Drive, pilih filenya dan klik tambahkan ke Drive saya

 Google Meet


 Alat pengajaran dan pembelajaran


 Dokumentasi Pusat Bantuan yang relevan

- [Merekam rapat video](#)



Bagaimana cara mentranskripsi kelas virtual agar siswa dapat mempelajari kembali konsep yang telah diajarkan?”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan transkrip dengan Google Meet](#)
- [Mengaktifkan atau menonaktifkan transkripsi](#)

## Merujuk topik yang telah dibahas di kelas

Dengan transkrip rapat, pendidik dapat otomatis menangkap pelajaran dan diskusi kelas, sehingga siswa dapat mempelajari kembali konsep yang telah disampaikan dengan lebih mudah. Transkrip melacak kehadiran rapat dan menunjukkan siapa yang mengatakan apa dalam sebuah rapat.

- ✓ Tersedia dalam bahasa Inggris bagi pengguna Google Meet yang menggunakan komputer atau laptop.
- ✓ Admin dapat mengaktifkan transkripsi untuk komunitas sekolahnya.
- ✓ Transkrip otomatis disimpan ke Drive penyelenggara rapat.
- ✓ Saat transkrip rapat aktif, ikon Transkrip ditampilkan di kiri atas layar dan terlihat oleh semua peserta rapat.
- ✓ Transkrip berisi kata-kata yang diucapkan dalam rapat. Untuk mendapatkan transkrip pesan chat, [rekam rapat Anda](#).



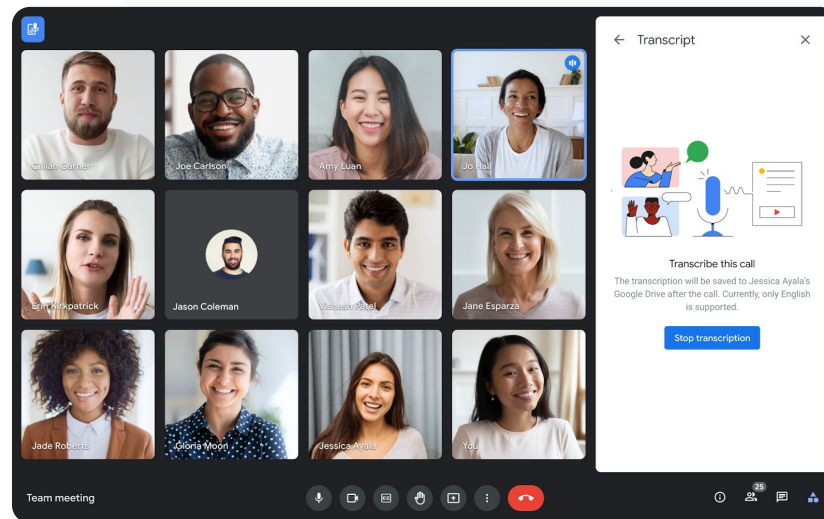
## Petunjuk: Merujuk topik yang telah dibahas di kelas

### Cara mengaktifkan transkrip di Google Meet

- Di pojok kanan bawah rapat, pilih ikon Aktivitas
- Klik Transkrip > Mulai Transkripsi > Mulai

### Cara menghentikan transkrip di Google Meet

- Pilih ikon Aktivitas > Transkrip > Hentikan Transkripsi > Hentikan



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan transkrip dengan Google Meet](#)
- [Mengaktifkan atau menonaktifkan transkripsi](#)



Kami mengadakan konferensi orang tua/pengajar secara virtual, tetapi terkadang kami tidak menggunakan bahasa yang sama.

Bagaimana cara mengatasi kendala bahasa agar rapat bisa diikuti semua orang?”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan teks terjemahan di Google Meet](#)

## Menghilangkan kendala bahasa

Teks terjemahan membuat rapat dapat diikuti oleh semua peserta dengan meniadakan kendala kemahiran bahasa. Ketika peserta rapat memahami konten dalam bahasa pilihan masing-masing, semua orang dapat berbagi informasi, belajar, dan berkolaborasi.

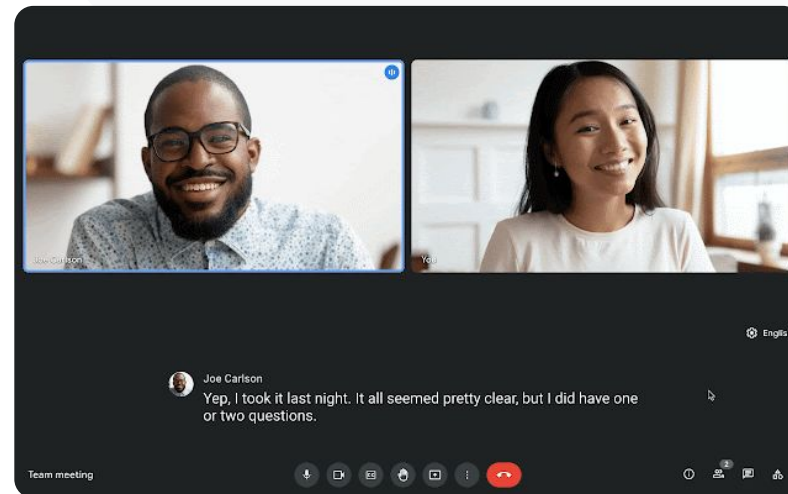
- ✓ Pendidik dapat berinteraksi dengan siswa, orang tua, dan pemangku kepentingan komunitas yang menggunakan bahasa lain
- ✓ Gunakan teks terjemahan untuk menerjemahkan bahasa Inggris ke atau dari bahasa Prancis, Jerman, Portugis, atau Spanyol
- ✓ Atau, terjemahkan bahasa Inggris ke dalam bahasa Jepang, Mandarin, atau Swedia



## Petunjuk: Menghilangkan kendala bahasa

### Cara mengaktifkan teks terjemahan

- Di bagian bawah layar rapat, klik Opsi lainnya > Setelan > Teks
- Aktifkan Teks
- Pilih Bahasa dalam rapat
- Aktifkan Teks terjemahan
- Pilih bahasa target




[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan teks terjemahan di Google Meet](#)



Kami ingin mengadakan live stream rapat staf dan pengajar ke semua pemangku kepentingan dan orang tua.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan atau menonaktifkan live streaming untuk Meet](#)
- [Melakukan live stream rapat video](#)

## Menyiarkan pertemuan, acara sekolah, dan rapat

Lakukan live stream ke hingga 10.000 audiens dengan Teaching and Learning Upgrade dan hingga 100.000 audiens dengan Education Plus. Peserta dapat bergabung dengan memilih link live stream yang disediakan oleh penyelenggara di email atau undangan Kalender.



Tentukan seberapa luas live stream Anda akan dibagikan. Pilih apakah live streaming akan:

- Terlihat hanya oleh pengguna di organisasi Anda (dalam domain)
- Dibagikan kepada domain Google Workspace tepercaya lainnya
- Tersedia untuk ditonton di YouTube



Sebaiknya admin TI mengaktifkan live streaming hanya untuk pengajar dan staf saja



Jika pengguna melewatkan live stream tersebut, mereka dapat mengakses tayangan ulangnya setelah rapat selesai



Tambahkan teks, polling, dan Tanya Jawab ke live stream untuk meningkatkan inklusivitas dan interaksi

## Petunjuk: Menyiarkan pertemuan, acara sekolah, dan rapat

### Cara membuat acara live stream

- Buka Google Kalender
- Pilih +buat > opsi lainnya
- Tambahkan detail acara, seperti tanggal, waktu, dan deskripsi
- Tambahkan peserta yang dapat berpartisipasi penuh dalam rapat video, yang berarti mereka akan dilihat, didengar, dan dapat mempresentasikan
- Klik **tambahkan konferensi > Meet**
- Di samping Gabung Meet, pilih panah bawah kemudian **tambahkan live stream**
- Untuk mengundang individu sebanyak yang diizinkan oleh edisi berbayar Anda, klik **salin dan bagikan URL live stream**
- Pilih **Simpan**
- Streaming tidak otomatis dimulai; selama rapat, pilih **lainnya > mulai streaming**



 Dokumentasi Pusat Bantuan yang relevan

- [Mengaktifkan atau menonaktifkan live streaming untuk Meet](#)
- [Melakukan live stream rapat video](#)



Saya membutuhkan cara cepat untuk mengajukan pertanyaan, mengukur pengetahuan siswa, dan berinteraksi dengan kelas agar mereka tetap aktif terlibat.”



 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Mengajukan pertanyaan kepada peserta di Google Meet](#)

## Mengajukan pertanyaan

Gunakan fitur **Tanya Jawab** di Google Meet untuk membantu siswa tetap aktif terlibat dan membuat kelas lebih interaktif. Pendidik bahkan akan mendapatkan laporan mendetail dari semua pertanyaan dan jawaban di akhir kelas virtual.

-  Moderator dapat mengajukan pertanyaan sebanyak yang mereka butuhkan. Mereka juga dapat memfilter atau mengurutkan pertanyaan, menandainya sebagai telah dijawab, dan bahkan menyembunyikan atau memprioritaskan pertanyaan.
-  Setelah setiap rapat yang mengaktifkan pertanyaan, laporan pertanyaan akan otomatis dikirim melalui email ke moderator.

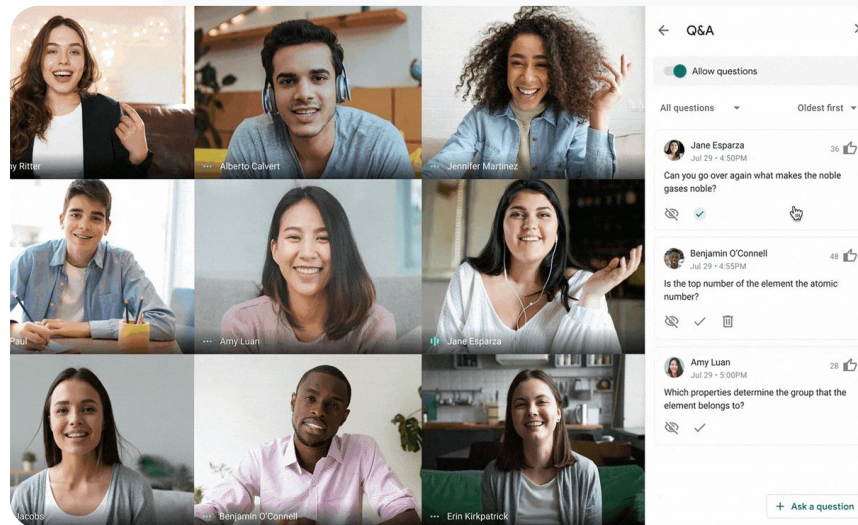
# Petunjuk: Mengajukan pertanyaan

## Mengajukan pertanyaan

- Di pojok kanan atas rapat, pilih ikon Aktivitas > Pertanyaan (untuk mengaktifkan Tanya Jawab, pilih Aktifkan Tanya Jawab)
- Untuk mengajukan pertanyaan, klik Ajukan pertanyaan di pojok kanan bawah
- Masukkan pertanyaan Anda > pilih Posting

## Melihat laporan pertanyaan

- Setelah rapat selesai, moderator akan menerima laporan pertanyaan melalui email
- Buka email > klik lampiran laporan




[Dokumentasi Pusat Bantuan yang relevan](#)

- [Mengajukan pertanyaan kepada peserta di Google Meet](#)



Saya membutuhkan cara mudah untuk mengumpulkan masukan baik dari siswa maupun pendidik lainnya saat saya memimpin kelas atau rapat staf.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Melakukan polling di Google Meet](#)

## Mengumpulkan masukan

Individu yang menjadwalkan atau memulai rapat virtual dapat membuat **polling** untuk peserta rapat. Fitur ini membantu mengumpulkan informasi dari semua siswa atau peserta rapat secara cepat dan menarik.



Moderator dapat menyimpan polling untuk diposting nanti selama rapat. Polling tersebut disimpan dengan baik di bagian Polling dalam rapat virtual.



Setelah rapat selesai, laporan hasil polling akan otomatis dikirim ke moderator melalui email.



# Petunjuk: Mengumpulkan masukan



## Membuat polling

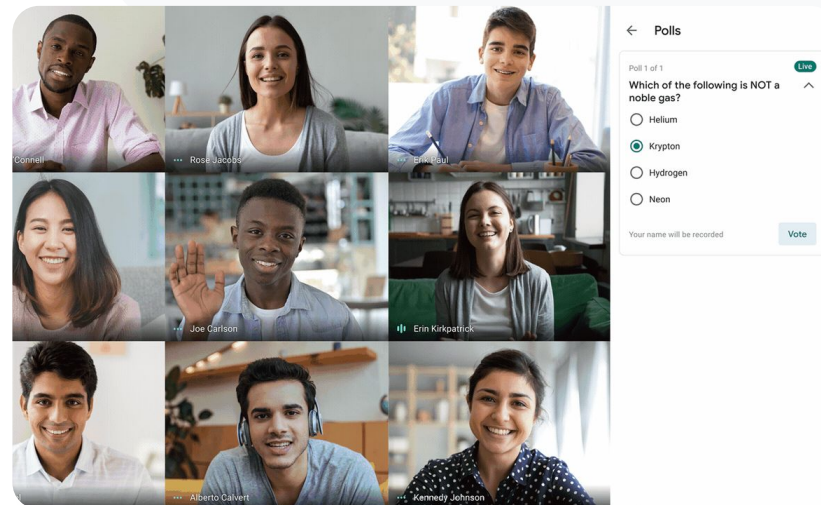
- Di pojok kanan atas rapat, pilih ikon Aktivitas > Polling
- Pilih Mulai polling
- Masukkan pertanyaan
- Pilih luncurkan atau simpan

## Memoderasi polling

- Di pojok kanan atas rapat, pilih ikon Aktivitas > Polling
- Agar peserta dapat melihat hasil polling secara real-time, di samping Tampilkan hasil kepada semua orang, pilih alihkan ke aktif
- Untuk menutup polling dan tidak mengizinkan respons, klik Akhiri polling
- Untuk menghapus polling secara permanen, pilih ikon Hapus

## Melihat laporan polling

- Setelah rapat selesai, moderator akan menerima laporan melalui email
- Buka email > pilih lampiran laporan



[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Melakukan polling di Google Meet](#)



Terkadang, ada siswa kami yang belajar dari rumah. Saat mengerjakan tugas grup kecil, kami memerlukan cara mudah untuk membuat ruang kerja kelompok berdasarkan grup yang telah ditentukan.”

 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Menggunakan ruang kerja kelompok di Google Meet](#)

## Grup kecil siswa

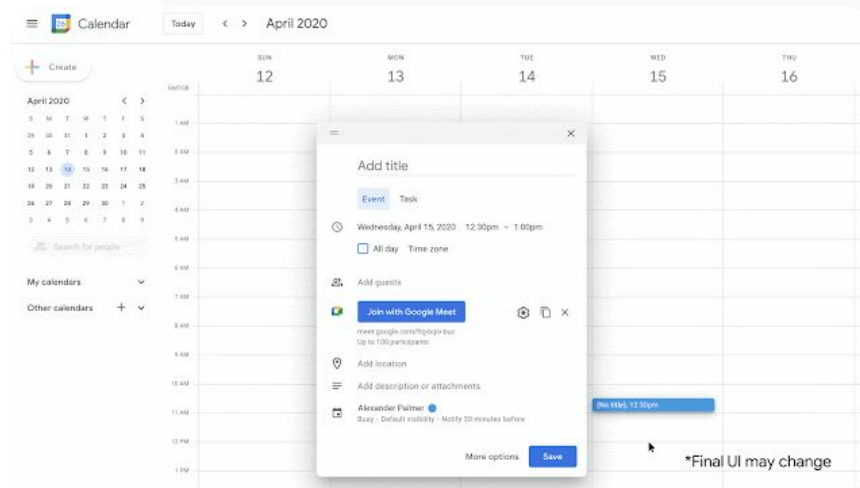
Pendidik dapat menggunakan ruang kerja kelompok untuk membagi siswa menjadi grup-grup yang lebih kecil selama pembelajaran tatap muka atau hybrid virtual. Ruang kerja kelompok harus dimulai oleh moderator selama panggilan video di komputer.

- ✓ Ruang kerja kelompok dapat dibuat sebelumnya saat menyiapkan acara, atau selama pertemuan berlangsung.
- ✓ Buat hingga 100 ruang kerja kelompok per pertemuan virtual
- ✓ Pengajar dapat dengan mudah beralih dari satu ruang kerja kelompok ke ruang yang lain untuk membantu grup jika diperlukan
- ✓ Admin dapat memastikan bahwa hanya pengajar atau staf yang dapat membuat ruang kerja kelompok

# Petunjuk: Membuat grup kecil siswa

## Membuat ruang kerja kelompok sebelum pertemuan

- Buat acara Google Kalender baru
- Klik Tambahkan konferensi video Google Meet
- Tambahkan peserta > pilih Ubah setelan konferensi
- Klik Ruang kerja kelompok
- Pilih jumlah ruang kerja kelompok dan tentukan antara:
  - Menarik peserta ke ruang berbeda
  - Memasukkan nama langsung ke dalam ruang
  - Mengklik Acak untuk mengacak grup
- Klik Simpan



[🔗 Dokumentasi Pusat Bantuan yang relevan](#)

- [Menggunakan ruang kerja kelompok di Google Meet](#)

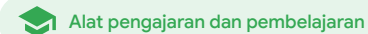
## Petunjuk: Membuat grup kecil siswa

### Membuat ruang kerja kelompok selama pertemuan

- Mulai panggilan video
- Di kanan atas, pilih ikon Aktivitas > Ruang kerja kelompok
- Di panel Ruang kerja kelompok pilih jumlah ruang kerja kelompok yang dibutuhkan
- Selanjutnya, siswa akan didistribusikan ke berbagai ruang, tetapi moderator dapat memindahkan peserta ke ruang lain secara manual, jika diperlukan.
- Di kanan bawah, klik Buka ruang

### Menjawab pertanyaan di ruang kerja kelompok lain

- Notifikasi di bagian bawah layar moderator akan muncul saat peserta meminta bantuan. Pilih Gabung untuk bergabung ke ruang kerja kelompok peserta tersebut




[Dokumentasi Pusat Bantuan yang relevan](#)

- [Menggunakan ruang kerja kelompok di Google Meet](#)



Kami kesulitan melacak siapa saja yang menghadiri kelas online. Saya perlu cara yang mudah untuk melaporkan kehadiran dalam kelas di seluruh domain saya.”



 [Petunjuk langkah demi langkah](#)

 Dokumentasi Pusat Bantuan yang relevan

- [Melacak kehadiran di Google Meet](#)

## Melacak kehadiran

Pelacakan kehadiran menyediakan laporan kehadiran otomatis untuk pertemuan apa pun yang dihadiri lima atau lebih peserta. Laporan menunjukkan siapa yang bergabung dalam panggilan, email peserta, dan berapa lama mereka berada di kelas virtual.

-  Anda dapat melacak kehadiran selama acara live stream dengan laporan live stream
-  Moderator dapat mengaktifkan dan menonaktifkan pelacakan kehadiran dan laporan live stream dari dalam pertemuan atau acara Kalender



# Petunjuk: Melacak kehadiran

## Cara melacak kehadiran dalam rapat

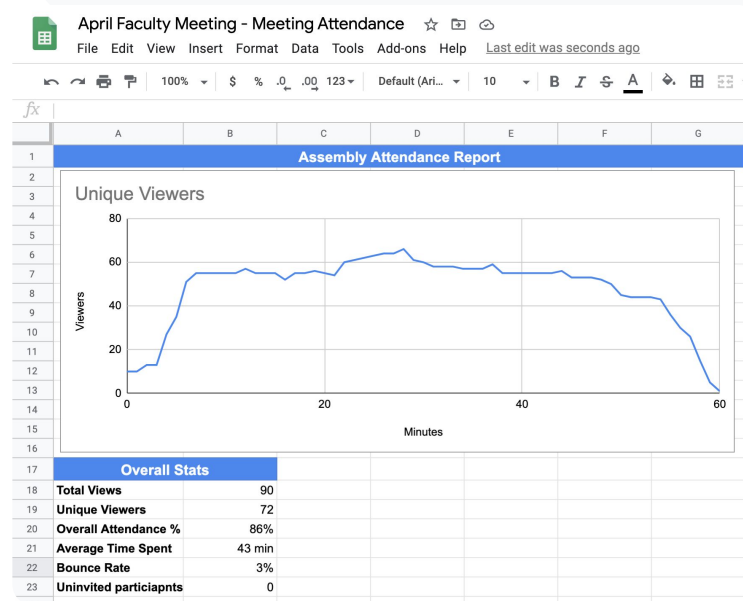
- Mulai panggilan video
- Dari bawah, pilih ikon menu
- Pilih ikon setelan > kontrol penyelenggara
- Aktifkan atau nonaktifkan Pelacakan kehadiran

## Cara melacak kehadiran di Kalender

- Aktifkan konferensi Google Meet dari acara Kalender
- Di sebelah kanan, pilih ikon setelan
- Pilih kotak di samping Pelacakan kehadiran > klik Simpan

## Mendapatkan laporan kehadiran

- Setelah rapat selesai, moderator akan menerima laporan melalui email
- Buka email > pilih lampiran laporan



[🔗](#) Dokumentasi Pusat Bantuan yang relevan

- [Melacak kehadiran di Google Meet](#)

Terima kasih