

Google for Education

Poznaj ponad 30 sposobów wykorzystania płatnych wersji Google Workspace for Education

goo.gle/use-edu-workspace



Jak korzystać z tej prezentacji

W tej prezentacji zebrano najbardziej popularne przykłady zastosowania płatnych wersji Google Workspace for Education. Opisane tu narzędzia pomagają m.in. zwiększyć bezpieczeństwo danych, efektywność pracy nauczycieli, zaangażowanie uczniów oraz współpracę w skali całej szkoły.

Informacje w prezentacji zostały uporządkowane według funkcji, przy których podano typowe przykłady ich zastosowania oraz proste instrukcje używania. Przejrzyj całą prezentację i zobacz, jak wiele możesz zrobić, korzystając z Google Workspace for Education.

Płatne wersje Google Workspace for Education

Większy wybór oraz lepsza kontrola i elastyczność w realizowaniu potrzeb organizacji w 3 płatnych wersjach Google Workspace for Education.



Google Workspace for Education Standard

Zaawansowane narzędzia ochronne i analityczne, które pomagają ograniczyć ryzyko i eliminować zagrożenia dzięki lepszej widoczności i kontroli nad środowiskiem edukacyjnym.



Teaching and Learning Upgrade

Ulepszone narzędzia edukacyjne, które ułatwiają komunikację i pracę podczas zajęć oraz promują uczciwość akademicką.



Google Workspace for Education Plus

Kompleksowe rozwiązanie obejmujące wszystkie funkcje z wersji Education Standard i opcji Teaching and Learning Upgrade. Jest najbardziej efektywnym i spójnym środowiskiem edukacyjnym dla szkolnej społeczności.

Spis treści



Narzędzia ochronne i analityczne

Narzędzia dostępne w wersjach Education Standard i Education Plus

Narzędzie do analizy zagrożeń

- Udostępnienie nieodpowiednich materiałów
- Przypadkowe udostępnienie plików
- Segregowanie e-maili
- E-maile phishingowe i zawierające złośliwe oprogramowanie
- Powstrzymanie hakerów

Panel bezpieczeństwa

- Duże ilości spamu
- Udostępnianie plików poza domenę
- Aplikacje innych firm
- Próba wyłudzenia informacji

Poziom bezpieczeństwa

- Zalecenia dotyczące obszarów ryzyka
- Zawsze na czasie ze sprawdzonymi metodami
- Bezpieczeństwo – sprawdzone metody
- Podnoszenie poziomu bezpieczeństwa w rozwijających się szkołach

Zaawansowane opcje administrowania i kontroli

- Regulacje prawne dotyczące danych
- Przepisy dotyczące grantów
- Ograniczenia aplikacji
- Zarządzanie urządzeniami mobilnymi
- Migracja danych

Spis treści



Narzędzia dla nauczycieli i uczniów

Narzędzia dostępne w opcji Teaching and Learning Upgrade i wersji Education Plus

Raporty antyplagiatowe

- Skanowanie pod kątem oryginalności
- Sprawdzanie oryginalności prac jako możliwość nauczenia się czegoś nowego

Google Meet

- Bezpieczne spotkania wideo
- Zwiększenie bezpieczeństwa rozmów wideo
- Nagrywanie lekcji
- Nagrywanie spotkań nauczycieli
- Opuszczone lekcje
- Transmitowanie spotkań na żywo
- Transmitowanie na żywo wydarzeń szkolnych
- Zadawanie pytań
- Gromadzenie odpowiedzi uczestników
- Małe grupy uczniów
- Śledzenie obecności



Narzędzia ochronne i analityczne

Dzięki narzędziom aktywnej ochrony bezpieczeństwa zyskasz większą kontrolę nad swoją domeną. Obronisz ją przed zagrożeniami, przeanalizujesz incydenty związane z bezpieczeństwem oraz skutecznie ochronisz dane uczniów i nauczycieli.



[Narzędzie do analizy zagrożeń](#)



[Panel bezpieczeństwa](#)



[Strona Poziom bezpieczeństwa](#)



[Zaawansowane opcje administrowania i kontroli](#)

Narzędzie do analizy zagrożeń

Co to jest?

Narzędzie do analizy zagrożeń umożliwia identyfikowanie i segregowanie problemów związanych z bezpieczeństwem oraz prywatnością w domenie, a także ich rozwiązywanie.

Przypadki użycia

Udostępnienie nieodpowiednich materiałów



[Szczegółowe instrukcje](#)

Przypadkowe udostępnienie plików



[Szczegółowe instrukcje](#)

Segregowanie e-maili



[Szczegółowe instrukcje](#)

E-maile phishingowe i zawierające złośliwe oprogramowanie

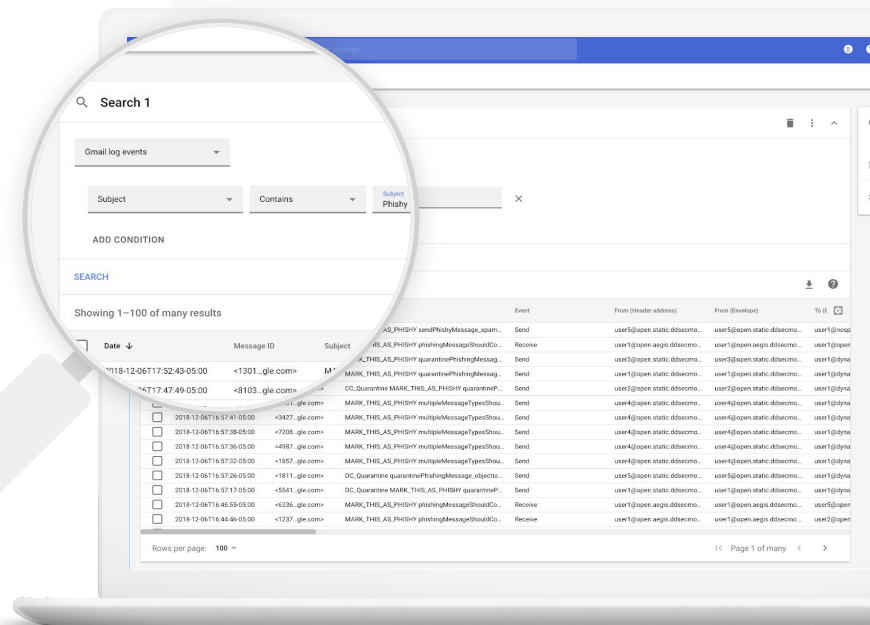


[Szczegółowe instrukcje](#)

Powstrzymanie hakerów




[Szczegółowe instrukcje](#)



Udostępnienie nieodpowiednich materiałów

Dzienniki Dysku dostępne w narzędziu do analizy zagrożeń pomogą Ci w wyszukaniu, prześledzeniu i odizolowaniu lub usunięciu niepożądanych plików w Twojej domenie. Korzystając ze [swoich dzienników Dysku](#), możesz:

- ✓ wyszukiwać dokumenty po nazwie, użytkownika, właściciela itp.;
- ✓ podjąć działania, polegające np. na zmianie uprawnień do pliku lub jego usunięciu;
- ✓ wyświetlać wszystkie informacje na temat dokumentu zawarte w dziennikach, takie jak:
 - data utworzenia;
 - kto jest jego właścicielem, kto go wyświetlał, kto go edytował;
 - kiedy został udostępniony.

 [Dokumentacja w Centrum pomocy](#)

[Warunki dla zdarzeń z dziennika Dysku](#) [Działania na zdarzeniach z dziennika Dysku](#)



Wiem, że został udostępniony plik z treściami naruszającymi nasze zasady. Chcę się dowiedzieć, kto go utworzył, kiedy to nastąpiło, kto i komu go udostępnił, kto go edytował, a następnie chcę usunąć ten plik”.


[Szczegółowe instrukcje](#)

Pliki udostępnione przez przypadek

Dzienniki Dysku dostępne w narzędziu do analizy zagrożeń pomogą Ci w prześledzeniu i rozwiązaniu problemów związanych z udostępnionymi plikami.

Korzystając ze [swoich dzienników Dysku](#), możesz:

- ✓ wyszukiwać dokumenty po nazwie, użytkownika, właściciela itp.;
- ✓ wyświetlać wszystkie informacje na temat dokumentu zawarte w dziennikach, m.in. kto go wyświetlał i kiedy dokument został udostępniony;
- ✓ podjąć działania polegające np. na zmianie uprawnień do plików i wyłączeniu funkcji pobierania, drukowania lub kopiowania.

 [Dokumentacja w Centrum pomocy](#)

[Warunki dla zdarzeń z dziennika Dysku](#) [Działania na zdarzeniach z dziennika Dysku](#)



Pewien plik został udostępniony grupie użytkowników, która NIE powinna mieć do niego dostępu. Chcę usunąć ich dostęp do tego pliku”.

[Szczegółowe instrukcje](#)

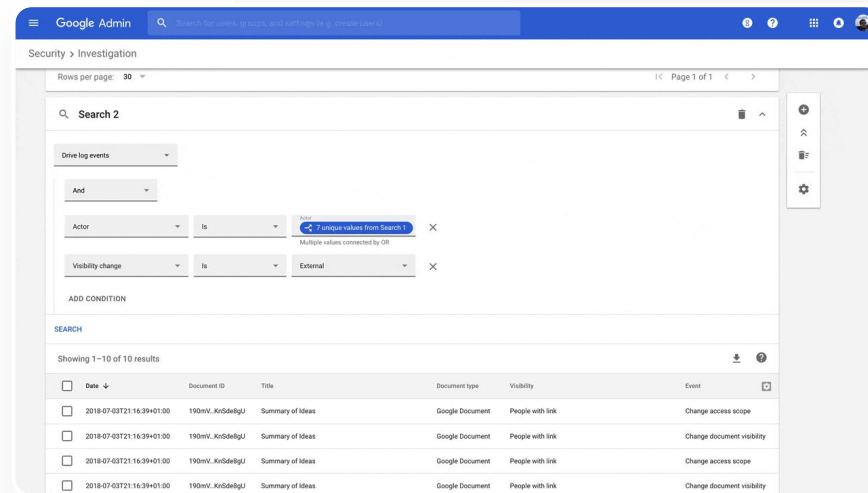
Instrukcje: zdarzenia z dziennika Dysku

Jak ustalić przyczyny

- Zaloguj się w konsoli administracyjnej.
- Kliknij Bezpieczeństwo > Narzędzie do analizy zagrożeń.
- Wybierz Zdarzenia z dziennika Dysku.
- Kliknij Dodaj warunek > Szukaj.

Jak podjąć działanie

- Wybierz odpowiednie pliki w wynikach wyszukiwania.
- Kliknij Czynności > Sprawdź uprawnienia dotyczące plików, aby otworzyć stronę Uprawnienia.
- Kliknij Osoby, aby zobaczyć, kto ma dostęp.
- Kliknij Linki, aby wyświetlić lub zmienić ustawienia udostępniania wybranych plików za pomocą linków.
- Kliknij oczekujące zmiany, aby przejrzeć zmiany przed ich zapisaniem.



[🔗 Dokumentacja w Centrum pomocy](#)


[Warunki dla zdarzeń z dziennika Dysku](#)

[Działania na zdarzeniach z dziennika Dysku](#)

Segregowanie e-maili

Dzienniki Gmaila dostępne w narzędziu do analizy zagrożeń pomogą Ci w rozpoznaniu i rozwiązaniu problemów związanych z niebezpiecznymi i naruszającymi nasze zasady e-mailami w Twojej domenie. Sprawdzając dzienniki Gmaila, możesz:

- ✓ wyszukiwać określone e-maile m.in. po temacie, ID wiadomości, załączniku i nadawcy;
- ✓ wyświetlać szczegółowe informacje o e-mailach, takie jak autor, odbiorca, otwarcie e-maila i jego przekazanie dalej;
- ✓ podejmować działania na podstawie wyników wyszukiwania – działania na wiadomościach w Gmailu obejmują ich usuwanie, przywracanie, oznaczanie jako spamu lub próby wyłudzenia informacji, wysłanie do skrzynki odbiorczej oraz wysłanie do kwarantanny.

 [Dokumentacja w Centrum pomocy](#)

[Warunki dotyczące dzienników i wiadomości Gmaila](#)

[Działania na wiadomościach z Gmaila i zdarzeniach z dziennika Gmaila](#)

[Instrukcje dotyczące wyświetlania zawartości e-maila](#)




Ktoś wysłał e-maila, który NIE powinien zostać wysłany. Chcemy wiedzieć, do kogo e-mail został wysłany, czy adresaci go otworzyli i czy na niego odpowiedzieli. Chcemy też go usunąć. Zależy nam również na poznaniu treści tego e-maila”.

[Szczegółowe instrukcje](#)

E-maile phishingowe i zawierające złośliwe oprogramowanie

Wykorzystując narzędzie do analizy zagrożeń, a konkretnie **dzienniki Gmaila**, znajdziesz i odizolujesz złośliwe e-maile, które trafiły do Twojej domeny. Sprawdzając dzienniki Gmaila, możesz:

- ✓ wyszukać wiadomości e-mail o konkretnej zawartości, w tym z określonymi załącznikami;
- ✓ zobaczyć informacje o konkretnych e-mailach, w tym o ich odbiorcach i otwarciu;
- ✓ wyświetlić wiadomości i całe wątki, aby ustalić, czy są złośliwe;
- ✓ podjąć działania, takie jak oznaczanie wiadomości jako spamu lub prób wyłudzenia informacji, wysyłanie ich do określonej skrzynki odbiorczej lub do kwarantanny, a także ich usuwanie.

 [Dokumentacja w Centrum pomocy](#)

[Warunki dotyczące dzienników i wiadomości Gmaila](#)

[Działania na wiadomościach z Gmaila i zdarzeniach z dziennika Gmaila](#)

[Instrukcje dotyczące wyświetlania zawartości e-maila](#)



Do użytkowników został wysłany e-mail wyłudzający informacje lub zawierający złośliwe oprogramowanie. Chcemy się dowiedzieć, czy użytkownicy klikali link w e-mailu lub pobierali załącznik, ponieważ tego typu działania mogą narazić naszych użytkowników i domenę na szwank”.

[Szczegółowe instrukcje](#)

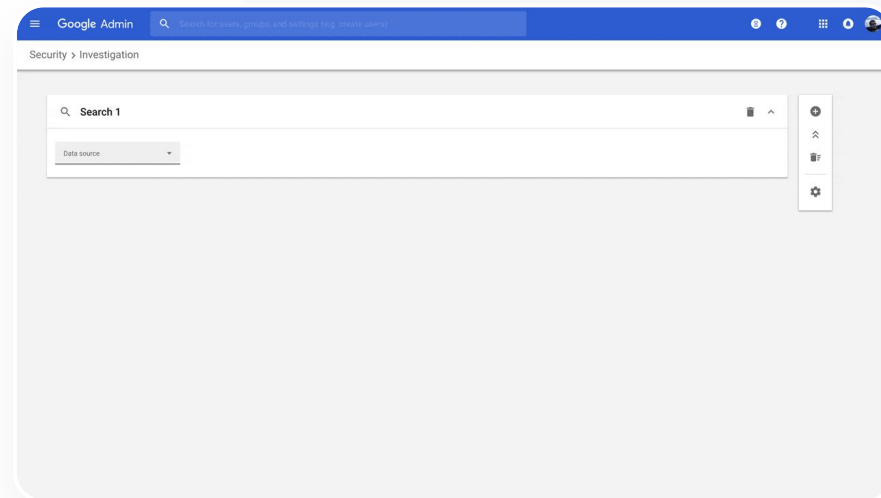
Instrukcje: dzienniki Gmaila

Jak ustalić przyczyny

- Zaloguj się w konsoli administracyjnej.
- Kliknij **Bezpieczeństwo** > **Narzędzie do analizy zagrożeń**.
- Wybierz **Zdarzenia z dziennika Gmaila** LUB **Wiadomości z Gmaila**.
- Kliknij **Dodaj warunek** > **Szukaj**.

Jak podjąć działanie

- Wybierz odpowiednie wiadomości w wynikach wyszukiwania.
- Kliknij **Czynności**.
- Wybierz **Usuń wiadomość z oryginalnej skrzynki odbiorczej**.
- Kliknij **Usuń ze skrzynki odbiorczej**.
- Aby potwierdzić tę operację, kliknij **Wyświetl** na dole strony.
- W kolumnie **Wynik** sprawdzisz stan operacji.



[🔗 Dokumentacja w Centrum pomocy](#)

[Warunki dotyczące dzienników i wiadomości Gmaila](#)


[Działania na wiadomościach z Gmaila i zdarzeniach z dziennika Gmaila](#)

[Instrukcje dotyczące wyświetlania zawartości e-maila](#)

Powstrzymanie hakerów

Dziennik użytkownika w narzędziu do analizy zagrożeń może Ci pomóc:

- ✓ identyfikować i badać próby przejęcia kont użytkowników w organizacji;
- ✓ w sprawdzaniu, z których metod weryfikacji dwuetapowej korzystają użytkownicy w Twojej organizacji;
- ✓ w uzyskiwaniu szczegółowych informacji o nieudanych próbach logowania się użytkowników w Twojej organizacji;
- ✓ [w tworzeniu reguł związanych z aktywnością w narzędziu do analizy zagrożeń](#): automatyczne blokowanie wiadomości i innych złośliwych działań podejmowanych przez określone osoby;
- ✓ w dalszej ochronie użytkowników z najwyższego szczebla organizacji przy pomocy [programu ochrony zaawansowanej](#);
- ✓ w przywracaniu i zawieszaniu kont użytkowników.

 [Dokumentacja w Centrum pomocy](#)

[Wyszukiwanie i badanie zdarzeń w dzienniku użytkownika](#)

[Tworzenie reguł związanych z aktywnością w narzędziu do analizy zagrożeń](#)



Ktoś wciąż atakuje konta osób z najwyższego szczebla organizacji w mojej domenie, a ja próbuję mu przeszkodzić. Jak sobie z tym poradzić?”

[Szczegółowe instrukcje](#)

Instrukcje: zdarzenia w dzienniku użytkownika

Jak ustalić przyczyny

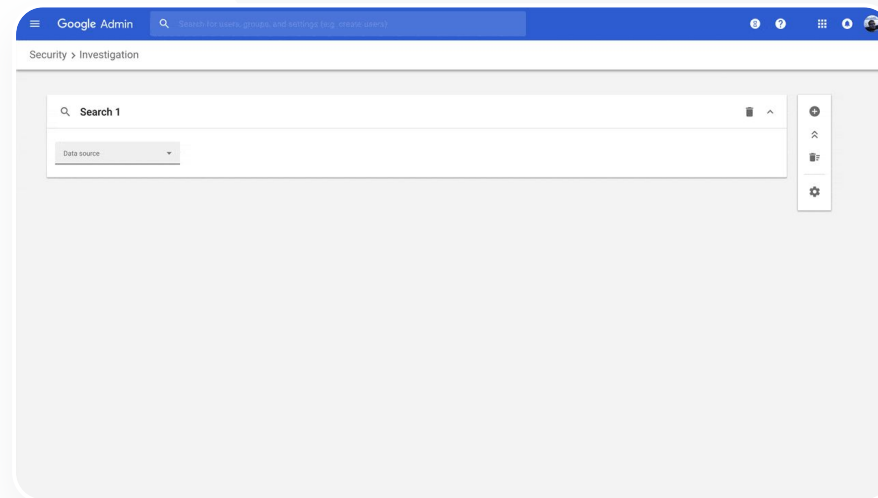
- Zaloguj się w konsoli administracyjnej.
- Kliknij Bezpieczeństwo > Narzędzie do analizy zagrożeń.
- Wybierz zdarzenia w dzienniku użytkownika.
- Kliknij Dodaj warunek > Szukaj.

Jak przywrócić lub zawiesić użytkowników

- Na stronie wyników wyszukiwania wybierz co najmniej jedno konto użytkownika.
- Kliknij menu Działania.
- Kliknij Przywróć konto użytkownika lub Zawieś konto użytkownika.

Jak wyświetlić szczegółowe dane konkretnego użytkownika

- Na stronie wyników wyszukiwania wybierz tylko jednego użytkownika.
- W menu DZIAŁANIA kliknij Wyświetl szczegóły.



[Dokumentacja w Centrum pomocy](#)

[Wyszukiwanie i badanie zdarzeń w dzienniku użytkownika](#)

Panel bezpieczeństwa

Co to jest?

Panelu Bezpieczeństwo można używać do przeglądania różnorodnych raportów na temat zabezpieczeń. Domyślnie każdy panel raportu zabezpieczeń przedstawia dane z ostatnich 7 dni. Możesz dostosować panel, wybierając zakres czasowy danych do wyświetlenia: Dzisiaj, Wczoraj, Bieżący tydzień, Poprzedni tydzień, Bieżący miesiąc, Poprzedni miesiąc lub Ile dni temu (maksymalnie 180 dni).

Przypadki użycia

Duże ilości spamu



[Szczegółowe instrukcje](#)

Udostępnianie plików
poza domenę



[Szczegółowe instrukcje](#)

Aplikacje innych firm

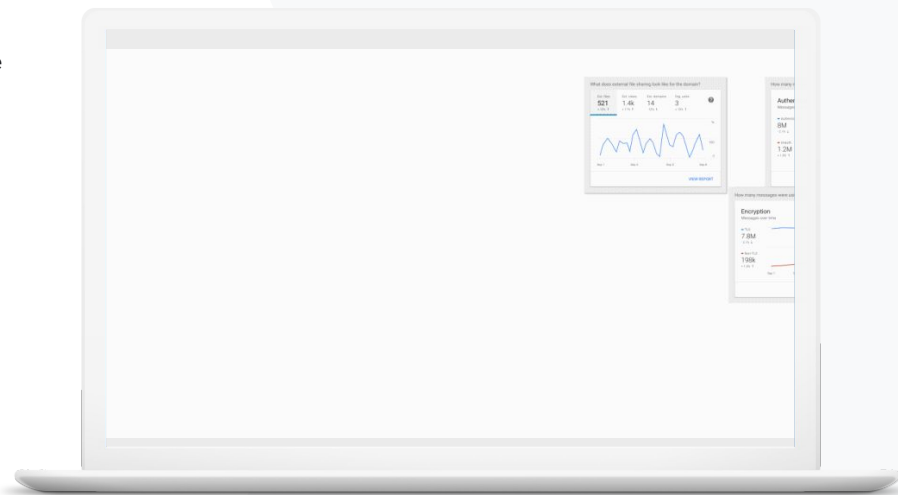


[Szczegółowe instrukcje](#)

Próba wyłudzenia informacji



[Szczegółowe instrukcje](#)





Duże ilości spamu

W panelu bezpieczeństwa znajdziesz obraz aktywności w środowisku Google Workspace for Education, obejmujący:

- ✓ spam,
- ✓ wyłudzenie informacji,
- ✓ złośliwe oprogramowanie,
- ✓ podejrzane załączniki,
- ✓ inne elementy.

[🔗 Dokumentacja w Centrum pomocy](#)

[Informacje o panelu bezpieczeństwa](#)



Chcę mieć możliwość panowania nad nadmiarowymi i niepotrzebnymi e-mailami oraz ograniczania zagrożeń dla bezpieczeństwa mojej szkoły”.

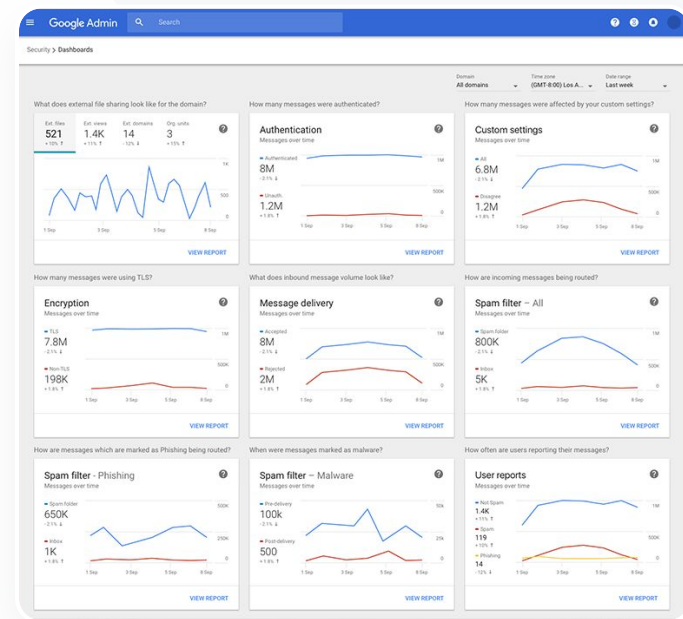
[Szczegółowe instrukcje](#)



Instrukcje: przegląd danych

Jak wyświetlić pulpit

- Zaloguj się w **konsoli administracyjnej**.
- Kliknij **Zabezpieczenia > Panel**.
- W panelu bezpieczeństwa możesz analizować dane i eksportować je do Arkuszy lub narzędzi innych firm, a także badać potencjalne problemy przy pomocy narzędzia do analizy zagrożeń.



[Dokumentacja w Centrum pomocy](#)


[Informacje o panelu bezpieczeństwa](#)



Udostępnianie plików poza domenę

Użyj raportu na temat udostępniania plików, który znajdziesz w panelu bezpieczeństwa, aby zobaczyć dane dotyczące udostępniania plików poza Twoją domenę, w tym:

- ✓ liczbę zdarzeń udostępniania plików użytkownikom spoza domeny w wybranym przedziale czasu;
- ✓ liczbę wyświetleń pliku zewnętrznego w określonym przedziale czasu.

 [Dokumentacja w Centrum pomocy](#)

[Pierwsze kroki na stronie Poziom bezpieczeństwa](#)



Chcę mieć wgląd w aktywność związaną z udostępnianiem plików na zewnątrz, aby zapobiec udostępnianiu danych wrażliwych poza organizację”.

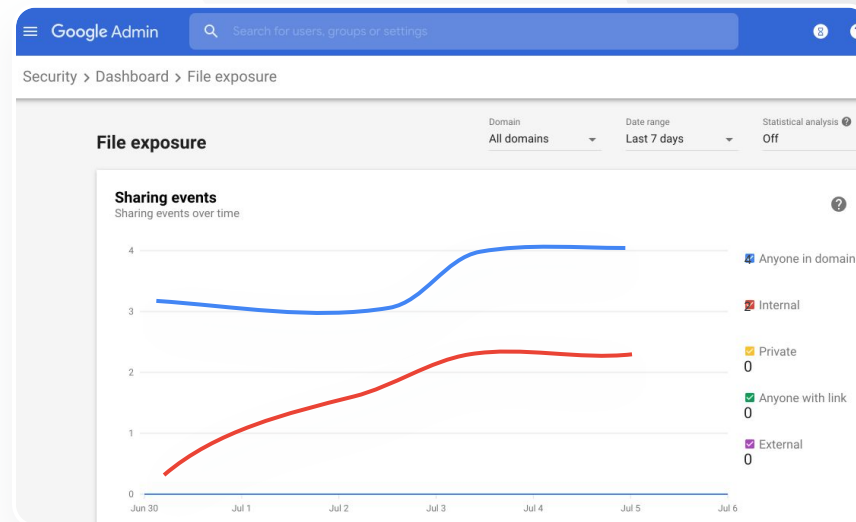
[Szczegółowe instrukcje](#)



Instrukcje: raport na temat udostępniania plików

Jak wyświetlić raport

- Zaloguj się w konsoli administracyjnej.
- Kliknij Zabezpieczenia > Panel.
- W panelu zatytułowanym „Jak jest skonfigurowane udostępnianie plików poza domenę?” kliknij Wyświetl raport w prawym dolnym rogu.



[🔗 Dokumentacja w Centrum pomocy](#)


[Używanie panelu bezpieczeństwa Raport na temat udostępniania plików](#)



Aplikacje innych firm

Użyj raportu Aktywność uwierzytelniania przez OAuth dostępnego w panelu bezpieczeństwa do monitorowania, które aplikacje innych firm są połączone z Twoją domeną, i do jakich danych mają dostęp.

- ✔ Protokół OAuth udziela usługom innych firm pozwolenia na dostęp do informacji o koncie użytkownika bez ujawniania jego hasła. Możesz się zdecydować na ograniczenie listy aplikacji innych firm, które mają takie pozwolenie.
- ✔ Użyj panelu „Aktywność uwierzytelniania przez OAuth” do monitorowania aktywności uwierzytelniania według aplikacji, zakresu lub użytkownika, oraz do aktualizowania udzielonych pozwoleń.

 [Dokumentacja w Centrum pomocy](#)

[Raport Aktywność uwierzytelniania przez OAuth](#)



Chcę zobaczyć, które aplikacje innych firm mają dostęp do danych w mojej domenie”.

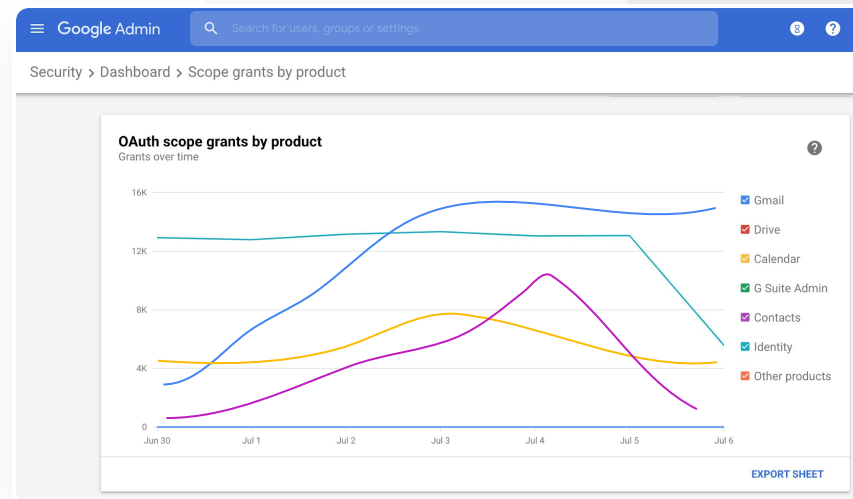
[Szczegółowe instrukcje](#)



Instrukcje: raport Aktywność uwierzytelniania przez OAuth

Jak wyświetlić raport

- Zaloguj się w konsoli administracyjnej.
- Kliknij Zabezpieczenia > Panel.
- Na dole kliknij Wyświetl raport.
- Aktywność uwierzytelniania przez OAuth możesz wyświetlać według usługi (aplikacji), zakresu lub użytkownika.
- Aby odfiltrować dane, kliknij Aplikacja, Zakres lub Użytkownik.
- Aby wygenerować raport w arkuszu kalkulacyjnym, kliknij Eksportuj arkusz.



[Dokumentacja w Centrum pomocy](#)


[Raport Aktywność uwierzytelniania przez OAuth](#)



Próba wyłudzenia informacji

Zgłoszenia użytkowników w panelu Bezpieczeństwo pozwalają Ci wyświetlić wiadomości, które zostały oznaczone jako spam lub próby wyłudzenia informacji w określonym przedziale czasu. Możesz wyświetlać informacje o e-mailach oznaczonych jako potencjalne przypadki wyłudzenia informacji, np. o ich odbiorcach i otwieraniu.

- ✓ Raport Zgłoszenia użytkowników pozwala sprawdzić, jak użytkownicy oznaczają wiadomości – jako spam, nie spam lub wyłudzenie informacji – w wybranym przedziale czasu.
- ✓ Wykres możesz zmodyfikować, aby zobaczyć szczegółowe informacje tylko o konkretnych typach wiadomości, np. wysłanych wewnątrz lub na zewnątrz domeny, albo o wiadomościach z określonego zakresu dat.

 [Dokumentacja w Centrum pomocy](#)

[W jaki sposób użytkownicy oznaczają e-maile?](#) [Raport Zgłoszenia użytkowników](#)



Użytkownicy zgłaszają próbę wyłudzenia informacji. Chcę móc prześledzić, kiedy otrzymaliśmy e-maila wyłudzającego informacje, jaka była dokładnie jego treść i na jakie ryzyko został narażony użytkownik, który go otrzymał”.

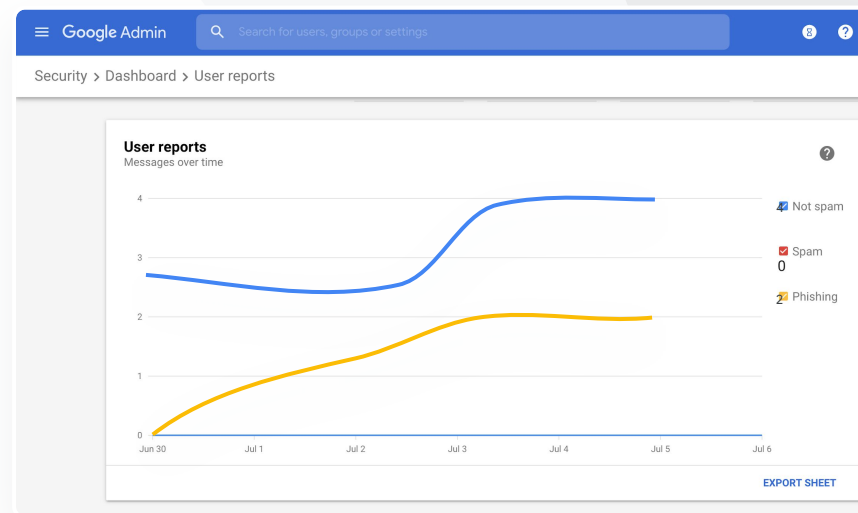
[Szczegółowe instrukcje](#)



Instrukcje: panel Zgłoszenia użytkowników

Jak wyświetlić raport

- Zaloguj się w konsoli administracyjnej.
- Kliknij Zabezpieczenia > Panel.
- W prawym dolnym rogu panelu Zgłoszenia użytkowników kliknij Wyświetl raport.



[🔗 Dokumentacja w Centrum pomocy](#)

[Używanie panelu bezpieczeństwa Raport na temat udostępniania plików](#)

Poziom bezpieczeństwa

Co to jest?

Strona Poziom bezpieczeństwa zawiera pełne omówienie stanu zabezpieczeń środowiska Google Workspace i pozwala Ci porównać Twoje konfiguracje z zaleceniami Google, aby aktywnie chronić organizację.

Przypadki użycia

Zalecenia dotyczące obszarów ryzyka



[Szczegółowe instrukcje](#)

Zawsze na czasie ze sprawdzonymi metodami



[Szczegółowe instrukcje](#)

Bezpieczeństwo – sprawdzone metody

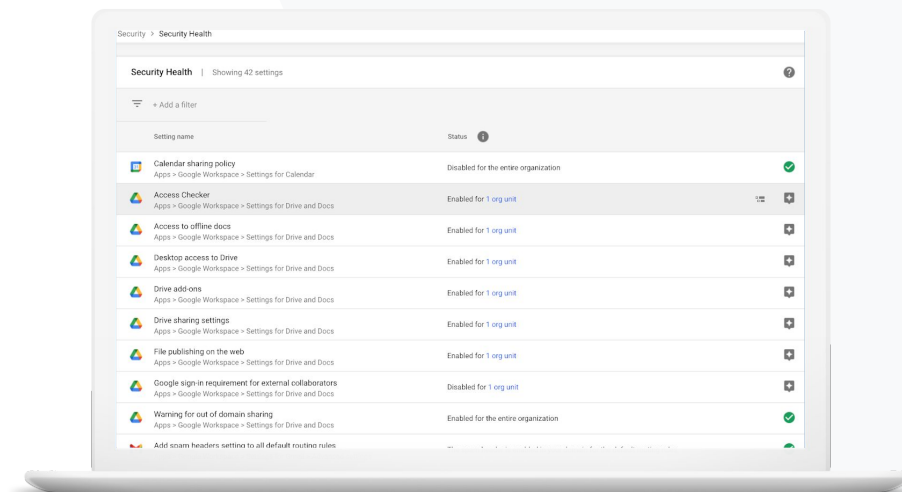


[Szczegółowe instrukcje](#)

Podnoszenie poziomu bezpieczeństwa w rozwijających się szkołach




[Szczegółowe instrukcje](#)



Zalecenia dotyczące obszarów ryzyka

Strona Poziom bezpieczeństwa zawiera informacje o konfiguracji zabezpieczeń oraz wskazuje zalecane zmiany. Na stronie Poziom bezpieczeństwa możesz:

- ✓ szybko rozpoznać obszary wymagające poprawy w Twojej domenie,
- ✓ uzyskać zalecenia dotyczące optymalnych ustawień zwiększających wydajność zabezpieczeń,
- ✓ zapoznać się z dodatkowymi informacjami oraz artykułami pomocy na temat zaleceń.

 [Dokumentacja w Centrum pomocy](#)

[Pierwsze kroki na stronie Poziom bezpieczeństwa](#)




Potrzebuję zwięzłego podsumowania ustawień bezpieczeństwa mojej domeny, z zaleceniami dotyczącymi potencjalnych obszarów zagrożeń, które będą dla mnie wykonalne”.

[Szczegółowe instrukcje](#)

Zawsze na czasie ze sprawdzonymi metodami

Strona Poziom bezpieczeństwa zawiera informacje o konfiguracji zabezpieczeń oraz wskazuje zalecane zmiany. Na stronie Poziom bezpieczeństwa możesz uzyskać:

- ✓ zalecenia dotyczące potencjalnych obszarów ryzyka w Twojej domenie,
- ✓ zalecenia dotyczące optymalnych ustawień zwiększających wydajność zabezpieczeń,
- ✓ dodatkowe informacje i artykuły pomocy.

 [Dokumentacja w Centrum pomocy](#)

[Pierwsze kroki na stronie Poziom bezpieczeństwa](#)



Zarządzam naszą domeną,
ale są pewne rzeczy,
których nie wiem. Pomóż mi
sprawdzić, czy wszystko
jest chronione przy pomocy
odpowiednich ustawień”.


[Szczegółowe instrukcje](#)



Bezpieczeństwo – sprawdzone metody

Otwórz stronę Poziom bezpieczeństwa, aby zapoznać się ze sprawdzonymi metodami dotyczącymi zasad bezpieczeństwa i skorzystaj z:

- ✓ zaleceń dotyczących potencjalnych obszarów ryzyka w Twojej domenie,
- ✓ zaleceń dotyczących optymalnych ustawień zwiększających wydajność zabezpieczeń,
- ✓ bezpośrednich linków do ustawień,
- ✓ dodatkowych informacji i artykułów pomocy.

 [Dokumentacja w Centrum pomocy](#)

[Pierwsze kroki na stronie Poziom bezpieczeństwa](#)



Wskaż mi sprawdzone metody i zalecenia dotyczące konfigurowania zasad bezpieczeństwa”.

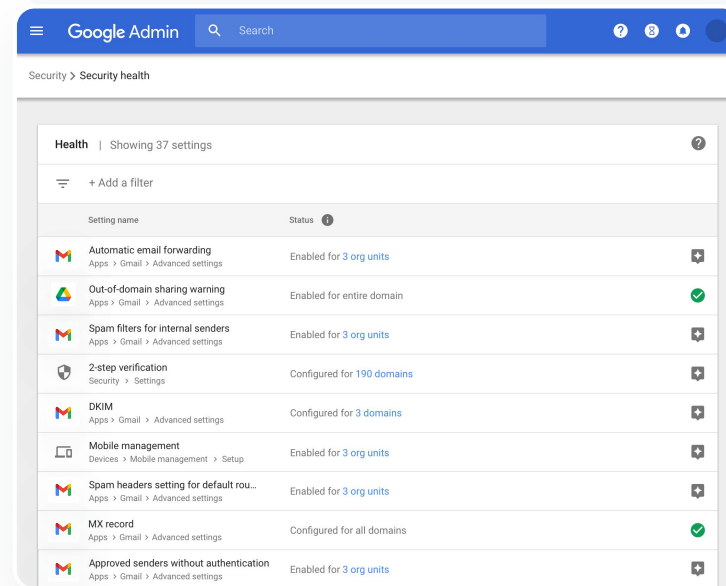
[Szczegółowe instrukcje](#)



Instrukcje: zalecenia dotyczące bezpieczeństwa

Jak wyświetlić zalecenia

- Zaloguj się w konsoli administracyjnej.
- Kliknij **Bezpieczeństwo > Poziom bezpieczeństwa**.
- Wyświetl ustawienia stanu w kolumnie po prawej stronie.
 - Zielony znacznik wyboru oznacza bezpieczne ustawienia.
 - Szara ikona oznacza, że zaleca się sprawdzić to ustawienie. Kliknij ikonę, aby zobaczyć szczegółowe informacje i instrukcje.



[🔗 Dokumentacja w Centrum pomocy](#)


[Pierwsze kroki na stronie Poziom bezpieczeństwa](#)



Podnoszenie poziomu bezpieczeństwa w rozwijających się szkołach

Administratorzy działu IT powinni stosować poniższe [sprawdzone metody zwiększania bezpieczeństwa](#) i poprawiania ochrony prywatności w przypadku danych firmowych. Do wdrażania sprawdzonych metod opisanych na tej liście kontrolnej służą różne ustawienia dostępne w konsoli administracyjnej Google.

- ✓ Zalecenia dotyczące zapobiegania przejmowaniu kont i wykonywania działań naprawczych względem przejętych kont.
- ✓ Instrukcje ograniczania możliwości udostępniania plików i współpracy poza domeną.
- ✓ Funkcje służące do weryfikowania dostępu aplikacji innych firm do usług podstawowych.

 [Dokumentacja w Centrum pomocy](#)

[Lista kontrolna zabezpieczeń dla średnich i dużych firm](#)

“

Chcę mieć pewność, że wraz ze wzrostem liczby uczniów i nauczycieli w mojej szkole, placówka jest chroniona w maksymalnym możliwym stopniu”.

[Szczegółowe instrukcje](#)



Instrukcje: lista kontrolna zabezpieczeń

Aby odpowiednio chronić Twoją organizację, Google ma włączone domyślnie różne ustawienia zalecane na tej liście kontrolnej jako sprawdzone metody w zakresie bezpieczeństwa. Polecamy przyjrzeć się szczególnie tym, które są wyróżnione poniżej.

- **Administrator:** ochrona kont administratorów.
- **Konta:** zapobieganie przejmowaniu kont i wykonywanie działań naprawczych względem przejętych kont.
- **Aplikacje:** weryfikowanie dostępu aplikacji innych firm do usług podstawowych.
- **Kalendarz:** ograniczanie udostępniania kalendarzy poza domenę.
- **Dysk:** ograniczanie możliwości udostępniania i współpracy poza domeną.
- **Gmail:** konfigurowanie uwierzytelniania i infrastruktury.
- **Vault:** kontrolowanie i zabezpieczanie kont 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](#)

 [Dokumentacja w Centrum pomocy](#)

[Monitorowanie stanu ustawień zabezpieczeń](#)

Zaawansowane opcje administrowania i kontroli

Co to jest?

Monitorowanie i kontrolowanie, którzy użytkownicy i urządzenia mają dostęp do Twojej domeny i danych.

Przypadki użycia

[Regulacje prawne dotyczące danych](#)



[Szczegółowe instrukcje](#)

[Przepisy dotyczące grantów](#)



[Szczegółowe instrukcje](#)

[Ograniczenia aplikacji](#)



[Szczegółowe instrukcje](#)

[Zarządzanie urządzeniami mobilnymi](#)

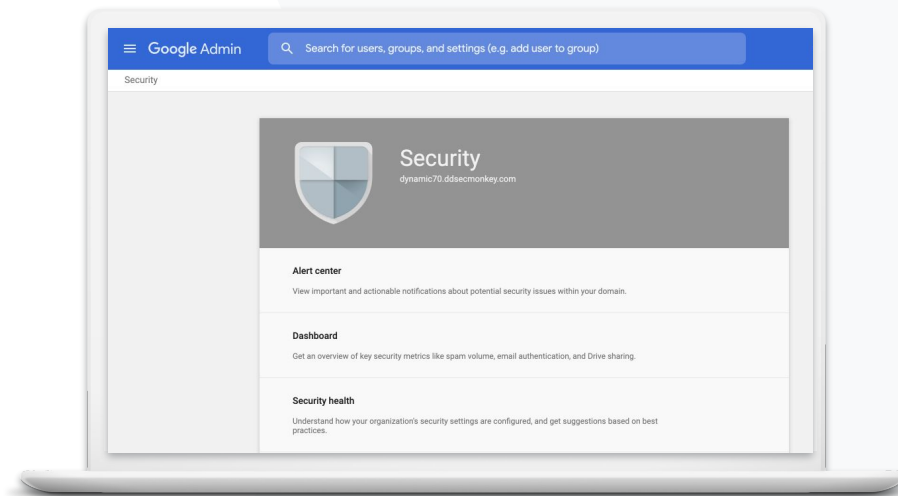


[Szczegółowe instrukcje](#)

[Migracja danych](#)



[Szczegółowe instrukcje](#)






Regulacje prawne dotyczące danych

Jako administrator możesz podjąć decyzję o przechowywaniu danych w konkretnej lokalizacji, zarówno w USA, jak i Wielkiej Brytanii / Europie, kierując się **zasadami** dotyczącymi regionów danych.

- ✓ Możesz wybrać ten sam region danych dla wszystkich użytkowników albo różne regiony dla poszczególnych działów i zespołów.
- ✓ Dodaj użytkowników do jednostki organizacyjnej (aby ustawić strukturę według działów) albo umieść ich w grupach konfiguracji (aby ustawić strukturę według użytkowników z różnych działów lub w ramach działu).
- ✓ Użytkownicy bez przydzielonej licencji na wersję Education Standard lub Education Plus nie podlegają zasadom dotyczącym regionów danych.

 [Dokumentacja w Centrum pomocy](#)

[Wybieranie lokalizacji geograficznej na potrzeby przechowywania danych](#)



Dane uczniów, nauczycieli i innego personelu muszą pozostawać w USA z powodu przepisów”.


[Szczegółowe instrukcje](#)



Przepisy dotyczące grantów

Jako administrator możesz zdecydować o przechowywaniu badań wydziału w określonej lokalizacji geograficznej (w USA lub Europie), stosując zasady dotyczące regionów danych.

- ✓ Zasady dotyczące regionów danych obejmują podstawowe dane w spoczynku (w tym kopie zapasowe) dla większości podstawowych usług Google Workspace wymienionych [tutaj](#).
- ✓ Rozważ wady i zalety tego rozwiązania, zanim skonfigurujesz zasady dotyczące regionów danych. Użytkownicy spoza regionu, w którym znajdują się ich dane, mogą w niektórych sytuacjach doświadczać większych opóźnień w działaniu usługi.

 [Dokumentacja w Centrum pomocy](#)

[Wybieranie lokalizacji geograficznej na potrzeby przechowywania danych](#)



Dane dotyczące badań wydziału muszą pozostać w USA z powodu przepisów dotyczących grantów”.

[Szczegółowe instrukcje](#)




Instrukcje: regiony danych*

Jak określać regiony danych

- Zaloguj się w konsoli administracyjnej.
 - Uwaga: musisz zalogować się na konto superadministradora.
- Kliknij Profil firmy > Pokaż więcej > Regiony danych.
- Wybierz jednostkę organizacyjną lub grupę konfiguracji, którą chcesz wyodrębnić jako region, lub wybierz całą kolumnę, aby uwzględnić wszystkie jednostki i grupy.
- Wybierz region. Dostępne opcje: **Brak preferencji, Stany Zjednoczone, Europa.**
- Kliknij **Zapisz**.

* Przechowywać dane w określonych regionach przy pomocy funkcji regionów danych mogą wyłącznie te instytucje, które korzystają z wersji Education Standard lub Education Plus.

 [Dokumentacja w Centrum pomocy](#)


[Wybieranie lokalizacji geograficznej na potrzeby przechowywania danych](#)



Ograniczenia aplikacji

Za pomocą dostępu zależnego od kontekstu* można utworzyć szczegółowe zasady kontroli dostępu do aplikacji oparte na takich atrybutach, jak tożsamość użytkownika, lokalizacja, stan zabezpieczeń urządzenia oraz adres IP. Możesz nawet ograniczyć dostęp do aplikacji spoza danej sieci.

- ✓ Zasady dostępu zależnego od kontekstu możesz stosować do podstawowych usług Google Workspace for Education.
- ✓ Jeśli na przykład użytkownik zaloguje się w usłudze podstawowej Google Workspace w szkole, a potem pójdzie do kawiarni, zasady dostępu zależnego od kontekstu zostaną ponownie sprawdzone z powodu zmiany lokalizacji.

 [Dokumentacja w Centrum pomocy](#)

[Omówienie dostępu zależnego od kontekstu](#)

[Przypisywanie poziomów dostępu zależnego od kontekstu do aplikacji](#)



Chcę ograniczyć dostęp do pewnych aplikacji, kiedy użytkownicy korzystają z internetu”.

[Szczegółowe instrukcje](#)

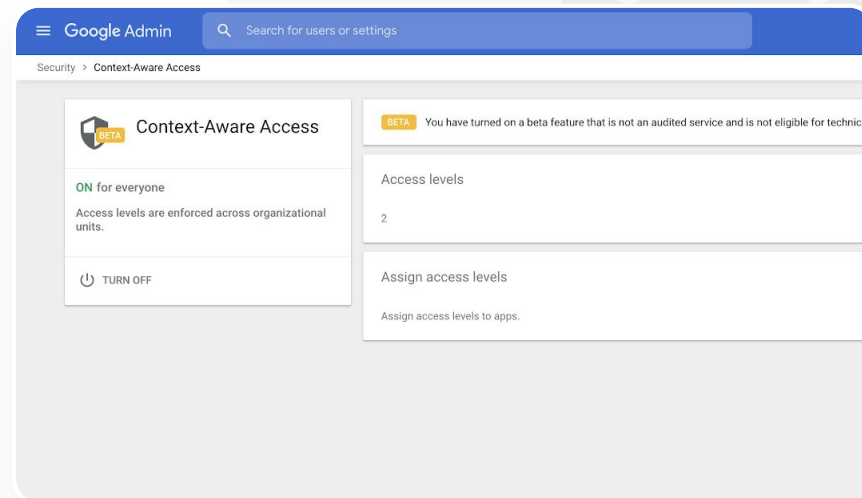
* Zasady dostępu zależnego od kontekstu mogą być stosowane wyłącznie w instytucjach, które korzystają z wersji Education Standard lub Education Plus.



Instrukcje: dostęp zależny od kontekstu

Jak korzystać z dostępu zależnego od kontekstu

- Zaloguj się w konsoli administracyjnej.
- Wybierz Bezpieczeństwo > Dostęp zależny od kontekstu > Przypisz.
- Wybierz Przypisywanie poziomów dostępu, aby zobaczyć swoją listę aplikacji.
- Wybierz jednostkę organizacyjną lub grupę konfiguracji, aby posortować listę.
- Wybierz Przypisz obok aplikacji, którą chcesz dostosować.
- Wybierz co najmniej jeden poziom dostępu.
- Jeśli chcesz, aby użytkownicy spełniali więcej niż jeden warunek, utwórz więcej poziomów.
- Kliknij Zapisz.



[🔗 Dokumentacja w Centrum pomocy](#)

[Omówienie dostępu zależnego od kontekstu](#)


[Przypisywanie poziomów dostępu zależnego od kontekstu do aplikacji](#)



Zarządzanie urządzeniami mobilnymi

Korzystanie z zaawansowanych funkcji zarządzania urządzeniami mobilnymi może dać Ci większą kontrolę nad danymi organizacji na urządzeniach mobilnych. Możesz ograniczać funkcje urządzeń mobilnych, wymagać szyfrowania urządzenia, zarządzać aplikacjami na urządzeniach z Androidem, iPhonech i iPadach, a nawet usuwać dane z urządzeń.

- ✔ Zatwierdzaj, blokuj, znoś blokady lub usuwaj urządzenia, korzystając z konsoli administracyjnej.
- ✔ Jeśli ktoś straci swoje urządzenie lub zostanie wypisany ze szkoły, możesz wyczyścić jego konto użytkownika, profil, a nawet wszystkie dane z konkretnego zarządzanego urządzenia. Dane te będą nadal dostępne na komputerze lub w przeglądarce internetowej.

 [Dokumentacja w Centrum pomocy](#)

[Konfigurowanie zaawansowanego zarządzania urządzeniami mobilnymi](#)

[Zatwierdzanie, blokowanie, odblokowywanie i usuwanie urządzenia](#)

[Usuwanie danych z urządzenia](#)



Muszę znaleźć sposób na zarządzanie i wprowadzenie zasad na wszystkich typach urządzeń – z systemem iOS, Windows 10 itp. – w całym moim rejonie, nie tylko na Chromebookach, na wypadek, gdyby któryś z nich został przejęty”.

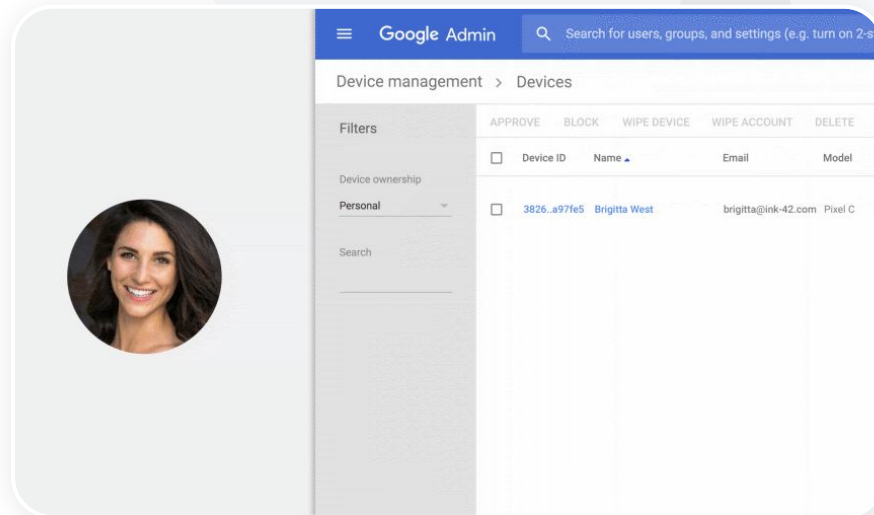
[Szczegółowe instrukcje](#)



Instrukcje: włączanie zaawansowanego zarządzania urządzeniami mobilnymi

Jak włączyć

- Logowanie się w konsoli administracyjnej.
- W konsoli administracyjnej wybierz Urządzenia.
- Po lewej stronie kliknij Ustawienia > Ustawienia uniwersalne.
- Kliknij Ogólne > Zarządzanie urządzeniami mobilnymi.
- Aby zastosować to ustawienie do wszystkich użytkowników, pozostaw wybraną jednostkę organizacyjną najwyższego poziomu. W przeciwnym razie wybierz podrzędną jednostkę organizacyjną.
- Wybierz Zaawansowane.
- Kliknij Zapisz.



[🔗 Dokumentacja w Centrum pomocy](#)
[Konfigurowanie zaawansowanego zarządzania urządzeniami mobilnymi](#)
[Zatwierdzanie, blokowanie, odblokowywanie i usuwanie urządzenia](#)
[Usuwanie danych z urządzenia](#)

Zaawansowane opcje
administrowania i kontroli

Narzędzia ochronne i analityczne

Migracja danych

Skorzystaj z przewodników na temat migracji, które pomogą Ci w przeniesieniu wszystkich danych organizacji – tj. e-maili, kalendarzy, kontaktów, folderów, plików i uprawnień – do Google Workspace.

Dane mniej niż 1000 użytkowników


- ✓ Zapoznaj się z tabelą narzędzi do migracji, aby się zorientować, które rozwiązanie będzie najlepsze dla Twojej instytucji.

[Więcej informacji](#)

Dane więcej niż 1000 użytkowników

- ✓ Użyj narzędzia Google Workspace, jeśli chcesz skutecznie przenieść duże ilości danych.

[Więcej informacji](#)

 [Dokumentacja w Centrum pomocy](#)

[Migracja danych organizacji do Google Workspace](#)

[Tabela narzędzi do migracji Google Workspace](#)

[Informacje o Google Workspace Migrate](#)

[Instalowanie i konfigurowanie narzędzia Google Workspace Migrate](#)



Przechodzimy na Google Workspace i musimy przenieść wszystkie nasze dane do nowego środowiska Google”.

[Szczegółowe instrukcje](#)



Instrukcje: Google Workspace Migrate

Zanim zaczniesz

Zarejestruj się w programie w wersji [beta](#) i potwierdź, że Twoje urządzenia spełniają [wymagania systemowe](#).

Kolejne kroki

1. Skonfiguruj konsolę Google Cloud.

[Włączanie interfejsów API](#)

[Tworzenie identyfikatora klienta usługi internetowej OAuth](#)

[Tworzenie konta usługi Google Workspace](#)

2. Skonfiguruj konsolę administracyjną.

[Konfigurowanie ról administratora](#)

[Autoryzowanie identyfikatora klienta](#)

3. Pobierz i zainstaluj.

[Pobieranie instalatorów](#)

[Instalowanie baz danych](#)

[Instalowanie i konfigurowanie platformy](#)

[Instalowanie serwerów węzłów](#)

[\(Opcjonalnie\) Konfigurowanie serwera węzła, aby używał TLS](#)

4. Skonfiguruj usługę do przeniesienia.

[Konfigurowanie klucza szyfrowania](#)

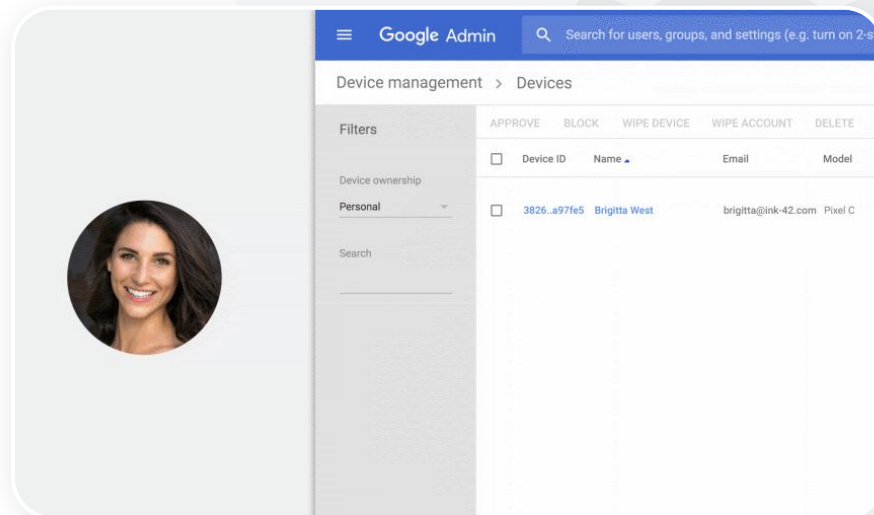
[Konfigurowanie ustawień bazy danych](#)

[Konfigurowanie adresu wywołania zwrotnego](#)

[Dodawanie serwerów węzłów](#)

[Utwórz projekt](#)

Potrzebujesz pomocy? Skontaktuj się [z partnerem Google Cloud](#).



Dokumentacja w Centrum pomocy

[Informacje o Google Workspace Migrate](#)

[Instalowanie i konfigurowanie narzędzia Google Workspace Migrate](#)

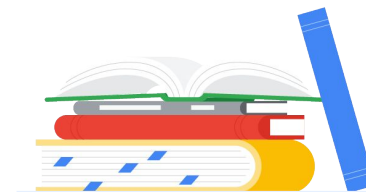
[Migracja danych organizacji do Google Workspace](#)

[Tabela narzędzi do migracji Google Workspace](#)



Narzędzia dla nauczycieli i uczniów

Zapewnij swoim nauczycielom dodatkowe możliwości w cyfrowym środowisku edukacyjnym, w tym zaawansowane narzędzia komunikacji wideo, rozszerzone możliwości prowadzenia zajęć oraz narzędzia promujące uczciwość akademicką.



[Raporty antyplagiatowe](#)



[Google Meet](#)

📄 Raporty antyplagiatowe

Co to jest?

Nauczyciele i uczniowie mogą sprawdzać autentyczność prac. Raporty antyplagiatowe porównują prace uczniów z miliardami stron internetowych i milionami książek przy użyciu wyszukiwarki Google, podają linki do wykrytych stron internetowych i wskazują nieoznaczone cytaty.

Przypadki użycia

[Skanowanie pod kątem oryginalności](#)

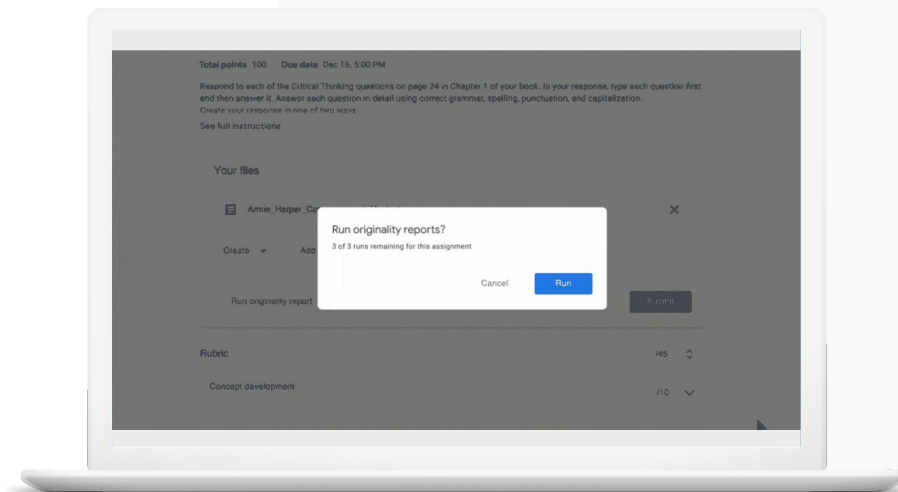


[Szczegółowe instrukcje](#)

[Sprawdzanie oryginalności prac jako możliwość nauczenia się czegoś nowego](#)



[Szczegółowe instrukcje](#)



Skanowanie pod kątem oryginalności

Nauczyciele mogą sprawdzać autentyczność prac swoich uczniów przy pomocy **raportów antyplagiatowych**. Raporty antyplagiatowe porównują prace uczniów z miliardami stron internetowych i milionami książek przy użyciu wyszukiwarki Google.

- ✓ Nauczyciele korzystający z opcji Teaching and Learning Upgrade lub wersji Education Plus mają nieograniczony dostęp do raportów antyplagiatowych.
- ✓ Raporty antyplagiatowe są obecnie dostępne tylko w przypadku:
 - kont Google ustawionych na język angielski,
 - prac wykonanych w Dokumentach,
 - kont Google for Education.

 [Dokumentacja w Centrum pomocy](#)

[Włączanie raportów antyplagiatowych](#)



Chcę sprawdzić, czy moi uczniowie nie popełniają plagiatów i czy poprawnie cytują źródła”.

[Szczegółowe instrukcje](#)

Instrukcje: końcowe sprawdzenie przez nauczyciela

Jak włączyć raporty antyplagiatowe w projekcie

- Zaloguj się na swoje konto Classroom na stronie classroom.google.com.
- Wybierz z listy odpowiednie zajęcia, a następnie kliknij **Zadania**.
- Wybierz **Utwórz > Projekt**.
- Zaznacz pole obok opcji **Wykonaj raport antyplagiatowy** (sprawdź oryginalność), aby ją włączyć.

Jak przygotować raport antyplagiatowy dotyczący pracy danego ucznia

- Wybierz z listy odpowiedni plik z pracą ucznia i kliknij, aby go otworzyć w narzędziu do oceniania.
- Pod nazwą projektu ucznia kliknij **Sprawdź oryginalność**.

The screenshot displays the 'Originality report' interface. The main content area shows an essay titled 'Essay: Comparison of Macbeth Adaptations' by Lewis Smith. The text discusses the character of Macbeth in Rupert Goold's film, comparing it to Shakespeare's play. Several paragraphs are highlighted in light blue, indicating detected matches. The right sidebar contains a 'Summary' section with the text 'Originality report expires Mar 3, 2020'. Below this is a 'Count' section with a percentage indicator. A '5 flagged passages' section shows '2 cited or quoted passages' with a toggle switch. A 'Web matches' section lists 'bartleby.com (3)' and '123helpme.com (2)' with right-pointing arrows.


[🔗 Dokumentacja w Centrum pomocy](#)

[Włączanie raportów antyplagiatowych](#)

Sprawdzanie oryginalności prac jako możliwość nauczenia się czegoś nowego

Uczniowie mogą wykrywać w swoich tekstach nieoznaczone cytaty i uniknąć niezamierzonego plagiatu, zanim oddadzą swoje prace, uruchamiając **raporty antyplagiatowe**. Mogą to zrobić maksymalnie 3 razy w jednym projekcie. Raporty antyplagiatowe porównują prace uczniów, które wykonali przy pomocy Dokumentów, z różnymi źródłami i wyróżniają nieoznaczone cytaty. Dzięki temu uczniowie mogą dowiedzieć się, na czym polega plagiat, poprawić błędy i odesłać pracę bez obaw.

- ✓ Zarówno opcja Teaching and Learning Upgrade, jak i wersja Education Plus umożliwiają nauczycielom wykonanie raportów antyplagiatowych dowolną ilość razy. Natomiast w wersji Education Fundamentals mogą użyć tej funkcji 5 razy na jednych zajęciach.
- ✓ Po oddaniu pracy przez ucznia usługa Classroom automatycznie generuje raport widoczny tylko dla nauczyciela. Jeśli uczeń wycofa swoją pracę, a następnie prześle ją ponownie, Classroom wygeneruje dla nauczyciela kolejny raport antyplagiatowy.

 [Dokumentacja w Centrum pomocy](#)

[Generowanie raportu antyplagiatowego dotyczącego zadania](#)



Chcę dać uczniom możliwość sprawdzania oryginalności ich prac i zmienić postrzeganie tej funkcji z »wykrywacza plagiatów« na okazję do nauki”.

[Szczegółowe instrukcje](#)

Instrukcje: sprawdzanie pracy przez ucznia

Instrukcje uruchamiania raportu antyplagiatowego przez ucznia

- Zaloguj się na swoje konto Classroom na stronie classroom.google.com.
- Wybierz z listy odpowiednie zajęcia, a następnie kliknij Zadania.
- Wybierz odpowiedni projekt z listy i kliknij Wyświetl projekt.
- W sekcji Twoje zadania wybierz Prześlij lub Utwórz plik.
- Obok opcji Raporty antyplagiatowe kliknij Uruchom.
- Aby otworzyć raport, kliknij Wyświetl raport antyplagiatowy pod nazwą pliku projektu.
- Aby poprawić lub odpowiednio zacytować oznaczone fragmenty, u dołu kliknij Edytuj.

Essay: Comparison of Macbeth adaptations

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

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

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

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

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

Web matches > sparksnotes.com ✕

STUDENT'S PASSAGE

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

[Comment](#)

TOP MATCH

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

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

[🔗 Dokumentacja w Centrum pomocy](#)

[Generowanie raportu antyplagiatowego dotyczącego zadania](#)




Co to jest?

Zaawansowane funkcje Google Meet obejmują m.in. transmisje na żywo, pokoje podgrup, zapisywanie nagranych spotkań na Dysku, raporty o obecności oraz spotkania dla maksymalnie 250 uczestników.

Przypadki użycia

[Bezpieczne spotkania wideo](#)  [Szczegółowe instrukcje](#)

[Zwiększenie bezpieczeństwa rozmów wideo](#)  [Szczegółowe instrukcje](#)

[Nagrywanie lekcji](#)  [Szczegółowe instrukcje](#)

[Nagrywanie spotkań nauczycieli](#)  [Szczegółowe instrukcje](#)

[Opuszczone lekcje](#)  [Szczegółowe instrukcje](#)

[Transmitowanie spotkań na żywo](#)  [Szczegółowe instrukcje](#)

[Transmitowanie na żywo wydarzeń szkolnych](#)  [Szczegółowe instrukcje](#)

[Zadawanie pytań](#)  [Szczegółowe instrukcje](#)

[Gromadzenie odpowiedzi uczestników](#)  [Szczegółowe instrukcje](#)

[Małe grupy uczniów](#)  [Szczegółowe instrukcje](#)

[Śledzenie obecności](#)  [Szczegółowe instrukcje](#)

Bezpieczne spotkania wideo

Dzięki Google Meet szkoły i uczelnie mogą korzystać z infrastruktury opartej na zasadzie Secure by design oraz z wbudowanych zabezpieczeń i globalnej sieci. To te same rozwiązania, których Google używa, aby dbać o bezpieczeństwo Twoich danych i chronić Twoją prywatność. Poniżej wymieniamy środki bezpieczeństwa stosowane w Google Meet. Możesz im zaufać.



Na ile tak naprawdę bezpieczna jest usługa Google Meet?”


- ✓ **Prywatność i zgodność z przepisami:** dostosowanie do rygorystycznych standardów bezpieczeństwa w edukacji w celu bezpiecznego przechowywania danych szkoły i uczniów.
- ✓ **Szyfrowanie:** wszystkie dane przesyłane od klienta do Google są szyfrowane.
- ✓ **Środki przeciwdziałania nadużyciom:** przekazanie moderatorom kontroli nad obecnością i dopuszczanie na spotkania wyłącznie osób uprawnionych.
- ✓ **Bezpieczne wdrażanie, dostęp i opcje kontroli:** prywatność i bezpieczeństwo spotkań są zachowane dzięki zastosowaniu różnych środków zapobiegawczych.
- ✓ **Reagowanie na incydenty:** jest to element ogólnego programu Google dotyczącego bezpieczeństwa i prywatności, który ma kluczowe znaczenie dla zapewnienia zgodności z ogólnosięciowymi przepisami związanymi z ochroną prywatności.
- ✓ **Niezawodność:** wielopoziomowa chmurowa infrastruktura przygotowana z myślą o zapewnieniu skalowalności usług, umożliwiająca obsługę zwiększonej liczby użytkowników.
- ✓ **Kontrola nad tym, kto dołącza do spotkań:** udoskonalona funkcja pukania w przypadku zbiorczych próśb o dołączenie oraz blokowanie możliwości pukania, jeśli spełnione są pewne kryteria.
- ✓ **Blokowanie użytkowników:** moderatorzy mogą kontrolować, kto mówi na czacie, kto prowadzi prezentację, a nawet kto ma głos w trakcie wirtualnego spotkania.

[Szczegółowe instrukcje](#)

Zwiększenie bezpieczeństwa rozmów wideo

Opcja Teaching and Learning Upgrade oraz wersja Education Plus obejmują dodatkowe środki przeciwdziałania nadużyciom, np. wymaganie zatwierdzeń w przypadku uczestników zewnętrznych, ulepszone opcje moderowania spotkań oraz **spotkania z nazwą** służące do ochrony przed ponownym wykorzystaniem spotkań zakończonych. Po opuszczeniu spotkania przez ostatniego uczestnika nie można do danego spotkania dołączyć jeszcze raz. Żaden uczeń nie dołączy do spotkania z nazwą, dopóki prowadzący nie rozpocznie go ponownie.

- ✓ Gdy ostatni uczestnik opuści **spotkanie z nazwą** uczestnicy nie będą mogli do niego ponownie dołączyć, a 10-cyfrowy kod spotkania przestanie działać.
- ✓ Żaden uczeń nie dołączy do spotkania z nazwą, dopóki prowadzący nie rozpocznie go ponownie.
- ✓ Nauczyciel może zakończyć spotkanie u wszystkich uczestników, zapobiegając sytuacji, że będą w nim obecni po opuszczeniu spotkania przez nauczyciela.

 [Dokumentacja w Centrum pomocy](#)

[Bezpieczeństwo i prywatność w Meet dla szkół i uczelni](#)

[Rozpoczynanie spotkania wideo w Google Meet](#)



Co mogę zrobić, aby rozmowy wideo były jeszcze bardziej bezpieczne dla mojej szkoły?”

[Szczegółowe instrukcje](#)

Instrukcje: spotkania z nazwą

Jak utworzyć spotkanie z nazwą

- Użyj krótkiego linku, np. [g.co/meet/\[WPISZ NAZWĘ\]](https://g.co/meet/[WPISZ NAZWĘ]).
- Otwórz stronę meet.google.com lub aplikację mobilną Google Meet i wpisz nazwę w polu „Rozpocznij spotkanie lub dołącz”.

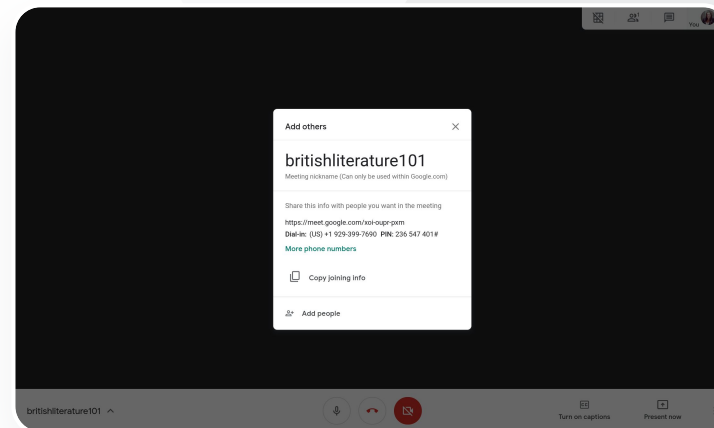
Jak to działa

Gdy nauczyciel rozpoczyna spotkanie z nazwą, tworzony jest 10-znakowy kod spotkania, który tymczasowo łączy się z nazwą spotkania.

Gdy ostatnia osoba opuszcza spotkanie lub nauczyciel je kończy, tymczasowy kod spotkania traci ważność i wygasa jego powiązanie z nazwą i kodem spotkania.

Jeśli uczniowie nie mają uprawnień do tworzenia spotkań, nie mogą korzystać z danej nazwy ani kodu spotkania.

Nauczyciele mogą ponownie użyć nazwy spotkania, co spowoduje utworzenie nowego tymczasowego kodu spotkania. Wtedy uczniowie będą mogli do niego ponownie dołączyć.



[🔗 Dokumentacja w Centrum pomocy](#)
[Bezpieczeństwo i prywatność w Meet dla szkół i uczelni](#)
[Rozpoczynanie spotkania wideo w Google Meet](#)



Nasza uczelnia prowadzi wykłady online dla dużej liczby uczestników. Chcemy je nagrywać dla studentów, którzy uczą się zdalnie lub nie mogli być na wykładach na żywo”.


[Szczegółowe instrukcje](#)

Nagrywanie lekcji

Użytkownicy opcji Teaching and Learning Upgrade oraz wersji Education Plus mogą nagrywać swoje spotkania, które są następnie automatycznie i bezterminowo zapisywane na Dysku.

Dzięki temu można łatwo archiwizować i udostępniać lekcje, warsztaty i sesje współpracy.

- ✓ Jeśli nauczyciele korzystają z Classroom, dzięki integracji z Meet mogą wygenerować dla każdego zajęcia unikalny link Meet, który będzie widoczny w strumieniu zajęć i na stronach Zadania.
- ✓ Link prowadzi do konkretnych zajęć, co ułatwia nauczycielom i uczniom dołączanie do spotkania.
- ✓ Użyj integracji Meet z Classroom do bezproblemowego nagrywania lekcji.


 [Dokumentacja w Centrum pomocy](#)

[Konfigurowanie Google Meet na potrzeby nauki zdalnej](#)

Nagrywanie spotkań nauczycieli

W opcji Teaching and Learning Upgrade oraz wersji Education Plus **nagrania** spotkań wideo są automatycznie zapisywane na Dysku na tak długo, jak użytkownik potrzebuje danego nagrania. Ułatwia to archiwizację i udostępnianie spotkań, kursów rozwoju zawodowego czy zebrań zarządu.

- ✓ Zaleca się, aby administrator IT włączył funkcję nagrywania tylko u kadry nauczycielskiej i innych pracowników.
- ✓ Możesz dodać osobne jednostki organizacyjne dla nauczycieli i dla uczniów, a następnie zastosować do nich odrębne reguły dostępu.
- ✓ Jeśli korzystasz z usługi Classroom, a wśród jej użytkowników są zweryfikowani nauczyciele, możesz włączyć dostęp dla grupy swoich nauczycieli.

 [Dokumentacja w Centrum pomocy](#)

[Konfigurowanie Google Meet na potrzeby nauki zdalnej](#)



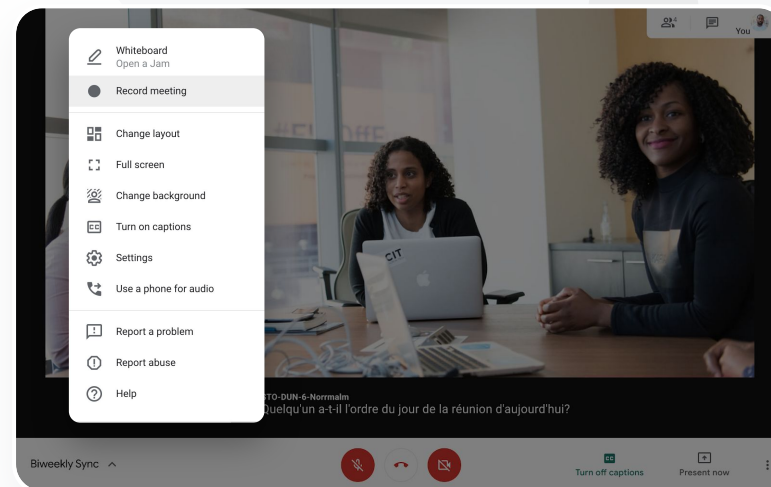
Systematycznie prowadzimy zebrania kadry online i zgodnie z naszą polityką wszystkie je nagrywamy. Poza tym chcielibyśmy nagrywać kursy rozwoju zawodowego oraz zebrania zarządu”.

[Szczegółowe instrukcje](#)

Instrukcje: nagrywanie

Jak nagrać spotkanie

- Otwórz spotkanie w swoim kalendarzu i wybierz **Dołącz w Google Meet**.
- Na stronie potwierdzenia spotkania **otwórz menu opcji**, klikając 3 pionowe kropki w prawym dolnym rogu.
- Kliknij **Nagrywanie spotkania**. W prawym dolnym rogu ekranu pojawi się czerwona kropka, która oznacza nagrywanie spotkania.
- Plik wideo z nagraniem spotkania zostanie automatycznie zapisany na Twoim Dysku.




[🔗 Dokumentacja w Centrum pomocy](#)
[Konfigurowanie Google Meet na potrzeby nauki zdalnej](#)

Opuszczone lekcje

W wersjach Teaching and Learning Upgrade oraz Education Plus dostęp do miejsca na Dysku mają wszyscy użytkownicy w domenie szkoły, a nagrania spotkań wideo są automatycznie zapisywane na Dysku organizatora spotkania. Aby odtworzyć nagrane spotkanie, poproś organizatora o link do nagrania lub otwórz je z poziomu wydarzenia w Kalendarzu.

- ✓ Nagrania są zapisywane na Dysku Google organizatora spotkania.
- ✓ Uczestnicy spotkania z tej samej jednostki organizacyjnej co organizator spotkania otrzymują dostęp do nagrania w sposób automatyczny.
- ✓ Jeśli zmieni się organizator spotkania, link do nagrania zostanie wysłany do użytkownika, który utworzył wydarzenie.

 [Dokumentacja w Centrum pomocy](#)

[Nagrywanie spotkania wideo](#)



Chcę zobaczyć nagraną lekcję,
na której mnie nie było”.

[Szczegółowe instrukcje](#)

Instrukcje: wyświetlanie i udostępnianie nagrań

Jak udostępnić nagranie

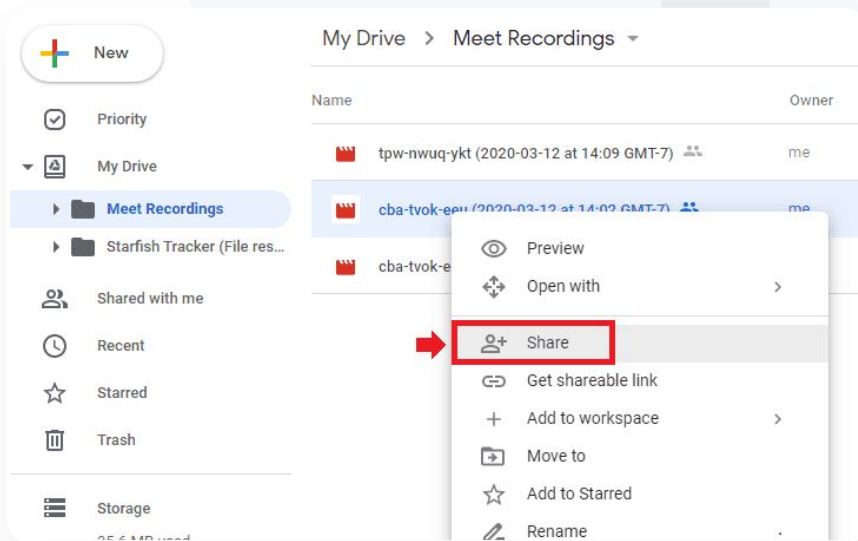
- Wybierz plik.
 - Kliknij ikonę udostępniania.
 - Dodaj zatwierdzonych widzów.
- LUB
- Wybierz ikonę Link.
 - Wklej link w e-mailu lub wiadomości na czacie.

Jak pobrać nagranie

- Wybierz plik.
- Kliknij ikonę Więcej > Pobierz.
- Aby odtworzyć pobrany plik, kliknij go dwukrotnie.

Jak odtworzyć nagranie z Dysku

- Aby odtworzyć nagranie z Dysku, kliknij plik dwukrotnie. Dopóki nie będzie gotowy do odtwarzania online, będzie wyświetlony komunikat „Trwa przetwarzanie”.
- Aby dodać nagranie do swojego Dysku, zaznacz plik i kliknij **Dodaj do Mojego dysku**.



[🔗 Dokumentacja w Centrum pomocy](#)

[Nagrywanie spotkania wideo](#)

Transmitowanie spotkań na żywo

Transmituj na żywo nawet dla 10 tys. odbiorców w domenie w wersji Teaching and Learning Upgrade oraz nawet dla 100 tys. odbiorców w domenie w wersji Education Plus. Uczestnicy mogą dołączać, klikając link do transmisji na żywo przesłany przez organizatora w e-mailu lub zaproszeniu z Kalendarza. Zapytaj swojego administratora IT, czy na pewno masz uprawnienia do prowadzenia transmisji na żywo.

- ✓ Zaleca się, aby administrator IT włączył funkcję transmisji na żywo tylko u kadry nauczycielskiej i innych pracowników.
- ✓ W przypadku dużych wydarzeń korzystaj z transmisji na żywo, zamiast prosić użytkowników o dołączanie do interaktywnego spotkania wideo. W ten sposób zapewnisz im lepszą jakość usługi.
- ✓ Jeśli użytkownik z jakichś powodów nie obejrzy transmisji na żywo, może ją odtworzyć po zakończeniu spotkania.

[🔗 Dokumentacja w Centrum pomocy](#)

[Konfigurowanie Google Meet na potrzeby nauki zdalnej](#)



Chcemy transmitować na żywo zebrania kadry nauczycielskiej i innych pracowników dla rodziców i innych zainteresowanych osób”.

[Szczegółowe instrukcje](#)

Transmitowanie na żywo wydarzeń szkolnych

Zachęcamy do **transmitowania wydarzeń na żywo** do odbiorców w Twojej szkolnej społeczności. Wystarczy kliknąć link do transmisji na żywo, który organizator przysłał Ci e-mailem lub który masz w zaproszeniu z Kalendarza. Zapytaj swojego administratora IT, czy na pewno masz **uprawnienia do prowadzenia transmisji na żywo**. Jeśli nie masz takich uprawnień, możesz [odtworzyć](#) nagranie po zakończeniu spotkania.

- ✓ Funkcji transmisji na żywo w Google Meet możesz używać, aby np. połączyć całą społeczność szkolną podczas ceremonii zakończenia roku, szkolnych imprez sportowych lub zebrań komitetu rodzicielskiego.
- ✓ Transmituj na żywo nawet dla 10 tys. odbiorców w domenie w wersji Teaching and Learning Upgrade oraz nawet dla 100 tys. odbiorców w domenie w wersji Education Plus.

[🔗 Dokumentacja w Centrum pomocy](#)

[Konfigurowanie Google Meet na potrzeby nauki zdalnej](#)



Lubimy transmitować na żywo nasze wydarzenia sportowe i inne ważne uroczystości, np. rozpoczęcie lub zakończenie roku, dla tych osób, które nie mogą wziąć w nich udziału osobiście”.

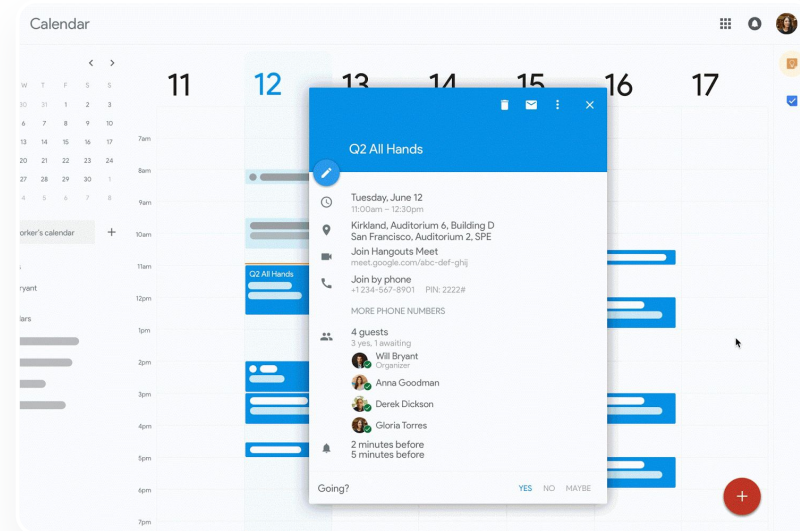
[Szczegółowe instrukcje](#)

Instrukcje: transmisja na żywo

Jak udzielić uprawnień do transmisji na żywo

- Otwórz Kalendarz Google.
- Kliknij + Utwórz > Więcej opcji.
- Dodaj informacje o wydarzeniu, takie jak data, godzina i opis.
- Możesz dodać do 250 gości, którzy będą w pełni uczestniczyć w spotkaniu wideo. Oznacza to, że będzie ich widać i słysać oraz będą mogli prezentować swój ekran. Możesz dodawać osoby z innych organizacji.
- Kliknij Dodaj rozmowę wideo > Meet.
- Obok opcji Dołącz do Meet kliknij strzałkę w dół, a następnie Dodaj transmisję na żywo.
- Aby zaprosić maksymalną liczbę osób z domeny, na którą pozwala Twoja płatna wersja, kliknij kopiuj, a następnie udostępnij adres URL do transmisji na żywo w e-mailu lub wiadomości na czacie.
- Kliknij Zapisz.
- Transmisja na żywo nie rozpocznie się automatycznie. W trakcie spotkania musisz kliknąć Więcej > Rozpocznij transmisję.

Uwaga: transmisję na żywo mogą oglądać tylko goście z Twojej organizacji.




[🔗 Dokumentacja w Centrum pomocy](#)
[Konfigurowanie Google Meet na potrzeby nauki zdalnej](#)

Zadawanie pytań

Użyj funkcji **Pytania i odpowiedzi** w Google Meet, która pomoże Ci utrzymać odpowiedni poziom zaangażowania uczniów i stworzy okazję do interakcji. Pod koniec wirtualnej lekcji nauczyciel otrzyma szczegółowy wykaz pytań i odpowiedzi.

- ✓ Moderatorzy mogą zadawać tyle pytań, ile potrzebują. Mogą również filtrować i sortować pytania, oznaczać je jako te, na które udzielono już odpowiedzi, a także je ukrywać i nadawać im priorytety.
- ✓ Po każdym spotkaniu, w którym używano funkcji **Pytania i odpowiedzi**, raport z pytaniami jest automatycznie wysyłany do moderatora spotkania.

 [Dokumentacja w Centrum pomocy](#)

[Zadawanie pytań uczestnikom spotkania w Google Meet](#)



„Potrzebuję szybkiego sposobu na zadawanie pytań, ocenianie wiedzy uczniów i interakcje z klasą, aby utrzymać zaangażowanie uczniów na odpowiednim poziomie”.

[Szczegółowe instrukcje](#)

Instrukcje: Pytania i odpowiedzi

Zadawanie pytania

- Podczas spotkania w prawym górnym rogu kliknij ikonę Czynności > Pytania (aby włączyć Pytania i odpowiedzi, kliknij **Włącz Pytania i odpowiedzi**).
- Aby zadać pytanie, kliknij **Zadaj pytanie** w prawym dolnym rogu.
- **Wpisz pytania** > kliknij **Opublikuj**.

Wyświetlanie raportu z pytaniami

- Po spotkaniu moderator otrzyma e-maila z raportem o pytaniach.
- Otwórz e-maila > kliknij załącznik z raportem.



[🔗 Dokumentacja w Centrum pomocy](#)
[Zadawanie pytań uczestnikom spotkania w Google Meet](#)

Gromadzenie odpowiedzi uczestników

Osoba, która zaplanowała lub rozpoczęła wirtualne spotkanie, może utworzyć **ankietę** dla jego uczestników. Ta funkcja umożliwi zebranie informacji od wszystkich uczestników spotkania w szybki i angażujący ich uwagę sposób.

- ✓ Moderator może zapisać ankietę z zamiarem opublikowania jej później podczas spotkania.
Ankiety są wygodnie przechowywane w sekcji Ankiety wirtualnego spotkania.
- ✓ Raport z wynikami ankiety jest automatycznie wysyłany e-mailem do moderatora po zakończeniu spotkania.

[🔗 Dokumentacja w Centrum pomocy](#)

[Przeprowadzanie ankiet w Google Meet](#)



Kiedy prowadzę lekcję lub zebranie dla pracowników, potrzebuję łatwego sposobu gromadzenia informacji od uczniów lub nauczycieli”.

[Szczegółowe instrukcje](#)

Instrukcje: przeprowadzanie ankiet

Tworzenie ankiety

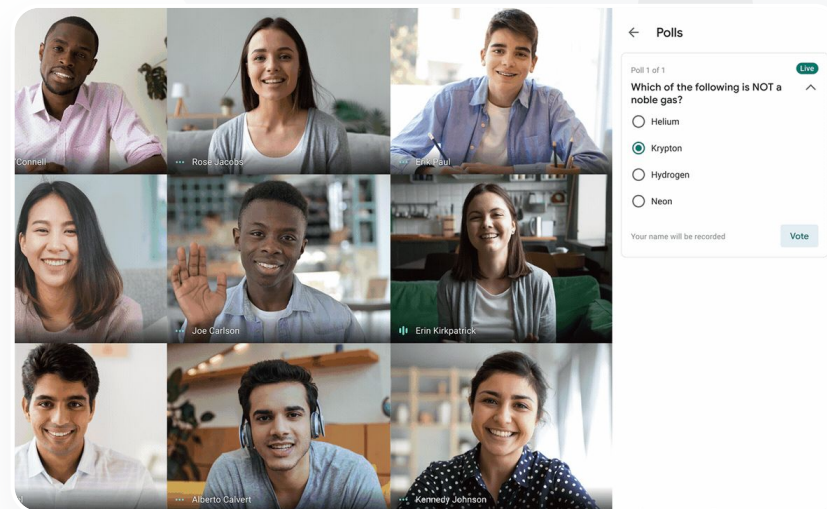
- W prawym górnym rogu spotkania kliknij ikonę Aktywności > Ankieta.
- Wybierz **Rozpocznij** ankietę.
- Wpisz pytanie
- Wybierz **Rozpocznij** lub **Zapisz**.

Moderowanie ankiety

- Podczas spotkania w prawym górnym rogu kliknij ikonę Czynności > Ankieta.
- Aby umożliwić uczestnikom wyświetlanie wyników ankiety w czasie rzeczywistym, obok opcji **Pokaż wszystkim** wyniki ustaw przełącznik w pozycji **włączonej**.
- Aby zamknąć ankietę i nie pozwalać na wysyłanie odpowiedzi, kliknij **Zakończ ankietę**.
- Aby trwale usunąć ankietę, kliknij ikonę **Usuń**.

Wyświetlanie raportu o ankietach

- Po spotkaniu moderator otrzyma e-maila z raportem o pytaniach.
- Otwórz e-maila > Wybierz załącznik z raportem.



[🔗 Dokumentacja w Centrum pomocy](#)

[Przeprowadzanie ankiet w Google Meet](#)



Prowadzimy naukę w 100% zdalnie i potrzebujemy rozwiązania, które będzie umożliwiało dzielenie dzieci na grupy, przysłuchiwanie się ich pracy w podgrupach, włączanie się w dyskusje i łatwe przechodzenie do współpracy na forum całej klasy”.

[Szczegółowe instrukcje](#)

Małe grupy uczniów

Nauczyciele mogą używać **pokoi podgrup** do dzielenia uczniów na mniejsze grupy podczas wirtualnych lekcji. Rozmowy w podgrupach muszą być uruchamiane przez moderatorów w trakcie rozmowy wideo na komputerze. W tej chwili rozmów w podgrupach nie można transmitować na żywo ani nagrywać.

- ✓ Tworzenie do 100 pokoi podgrup na jedno wirtualne spotkanie.
- ✓ Nauczyciel może łatwo przejść z jednego pokoju podgrupy do innego, aby w razie potrzeby pomagać uczniom w podgrupach.
- ✓ Administratorzy mogą tak skonfigurować usługę, aby możliwość tworzenia pokoi podgrup miała wyłącznie kadra nauczycielska i pozostały personel.

[🔗 Dokumentacja w Centrum pomocy](#)

[Używanie pokoi podgrup w Google Meet](#)

Instrukcje: tworzenie pokoi podgrup

Jak utworzyć pokoje podgrup

- Rozpocznij rozmowę wideo.
- W prawym górnym rogu kliknij ikonę Czynności > Pokoje podgrup.
- W panelu Pokoje podgrup wybierz potrzebną Ci liczbę pokoi podgrup.
- Następuje automatyczne przydzielenie uczniów do pokoi podgrup, jednak w razie potrzeby moderatorzy mogą ręcznie przenosić ich do innych pokoi.
- W prawym dolnym rogu kliknij Otwórz pokoje.

Odpowiadanie na pytania w różnych pokojach podgrup

- Kiedy uczestnicy proszą o pomoc, u dołu ekranu moderatora pojawia się powiadomienie. Wybierz Dołącz, aby dołączyć do pokoju podgrup danego uczestnika.



[🔗 Dokumentacja w Centrum pomocy](#)

[Używanie pokoi podgrup w Google Meet](#)




Mamy problem z ustaleniem, kto bierze udział w zajęciach zdalnych. Potrzebuję łatwej metody zgłaszania obecności na zajęciach w całej domenie”.

[Szczegółowe instrukcje](#)

Śledzenie obecności

Śledzenie obecności to funkcja automatycznego rejestrowania obecności na dowolnym spotkaniu z co najmniej 5 uczestnikami. Z raportu można odczytać, kto dołączył do rozmowy, jakie są adresy e-mail uczestników oraz ile czasu spędzili oni na wirtualnych zajęciach.

- ✓ Możesz sprawdzać obecność w czasie wydarzeń z transmisją na żywo przy pomocy raportów.
- ✓ Moderatorzy mogą włączać i wyłączać funkcje śledzenia obecności i tworzenia raportów z transmisji na żywo bezpośrednio na spotkaniu lub z poziomu wydarzenia w Kalendarzu.

 [Dokumentacja w Centrum pomocy](#)

[Sprawdzanie obecności w Google Meet](#)

Instrukcje: raporty o obecności

Śledzenie obecności w trakcie spotkania

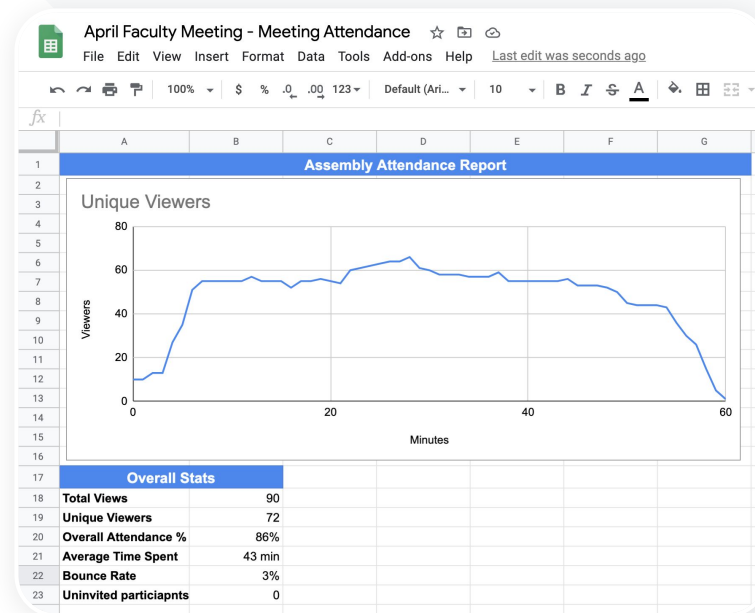
- Rozpocznij rozmowę wideo.
- Na dole kliknij ikonę Menu.
- Wybierz ikonę Ustawienia > Ustawienia gospodarza.
- Włącz lub wyłącz Śledzenie obecności.

Śledzenie obecności w Kalendarzu

- Włącz rozmowę wideo w Google Meet z poziomu wydarzenia w Kalendarzu.
- Po prawej stronie wybierz ikonę ustawień.
- Zaznacz pole wyboru obok opcji Śledzenie obecności > kliknij Zapisz.

Pobieranie raportu o obecności

- Po spotkaniu moderator otrzyma e-maila z raportem.
- Otwórz e-maila > wybierz załącznik z raportem.



[🔗 Dokumentacja w Centrum pomocy](#)

[Sprawdzanie obecności w Google Meet](#)

Dziękujemy