Google for Education

Google Workspace for Education 유료 버전을 사용하는 40가지 이상의 방법

goo.gle/use-edu-workspace

자료 활용법

이 자료는 **Google Workspace for Education 유료 버전** 사용자를 위한 일반적인 사용 사례를 제시합니다. 해당 버전을 사용하면 **데이터 보안, 교사의 효율성, 학생 참여도, 학교 전반의 공동작업** 등을 개선할 수 있습니다.

이 자료는 **기능**에 대한 정보, **일반적인 사용 사례**, 간단한 기능 **사용 방법 안내**로 구성되어 있습니다. 전체 자료를 살펴보고 Google Workspace for Education 유료 버전을 통해 어떤 이점을 누릴 수 있는지 알아보세요.

Google Workspace for Education 유료 버전

Google Workspace for Education의 3가지 유료 버전으로 조직의 니즈를 충족하는 데 필요한 옵션, 제어, 유연성을 확보하세요.

Google Workspace for Education Plus

Education Standard 및 Teaching and Learning Upgrade와 더불어 Plus 전용 추가 기능이 제공됩니다.

Education Plus는 **고급 보안 및 통계, 풍부한 교육 및 학습**을 위한 사용하기 쉬운 도구를 제공하는 **통합형** 에듀테크 솔루션을 통해 학생, 교사, 교육 리더, IT 관리자의 역량 강화에 도움을 줍니다.

Google Workspace for Education Standard

고급 보안 및 통계 도구로 학습 환경 전반에 걸쳐 가시성과 제어 기능을 향상하여 위험을 줄이고 위협을 완화하는 데 도움이 됩니다.

Teaching and Learning Upgrade

향상된 교육 및 학습 도구를 사용하면 학습을 더욱 개별화하고, 수업의 효율성을 높이고, 어디서든 교육 및 학습이 가능하게 함으로써 교육 효과를 향상할 수 있습니다.

목차

고급 보안 및 통계 기능

보안 대시보드

- 대량의 스팸
- 외부 파일 공유
- 서드 파티 애플리케이션
- 피싱 시도

보안 상태 페이지

- 보안 권장사항
- 위험 영역에 대한 권장사항

조사 도구

- 공유되고 있는 악성 자료
- 실수로 공유한 파일
- 피싱 및 멀웨어 이메일
- 악의적인 행위자 차단
- 더 심층적인 보안 통계
- 감독되지 않는 회의 방지

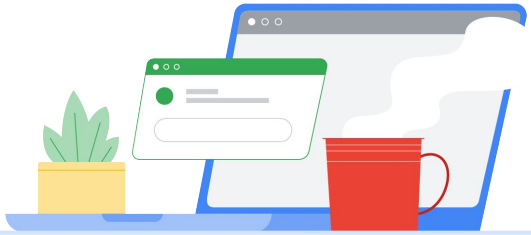
도메인 관리 및 제어

- Gmail 첨부파일의 위협 여부 검사
- 사용 대시보드 및 보고서 생성
- 파일 더 쉽게 찾기
- 내부 문서 정리
- 부서 그룹 자동으로 채우기
- 내부 파일 공유용 대상 생성
- 파일 공유 제한
- Workspace 앱 제한사항
- 스토리지 관리
- 데이터 규정
- 지원금 규정
- 엔드포인트 기기 관리
- Windows 기기 관리
- Windows 10 기기 맞춤 설정
- Windows 10 기기 업데이트 자동화
- 클라이언트 측 암호화 활용

목차

고급 보안 및 통계 기능

선제적 보안 도구를 사용하여 도메인 전반에서 더욱 세부적으로 제어함으로써 위협을 예방하고, 보안 사고를 분석하고, 학생 및 교직원 데이터를 보호할 수 있습니다.

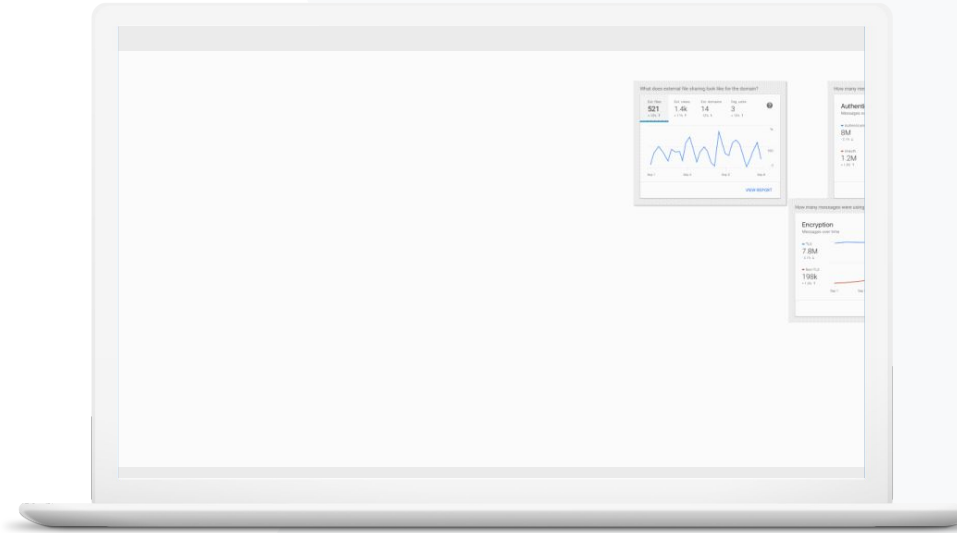


- 보안 대시보드
- 보안 상태 페이지
- 조사 도구
- 도메인 관리 및 제어

보안 대시보드

기본 개념

보안 대시보드를 사용하여 다양한 보안 보고서의 개요를 볼 수 있습니다. 기본적으로 각 보안 보고서 패널에는 최근 7일 동안의 데이터가 표시됩니다. 대시보드를 맞춤설정하여 오늘, 어제, 이번 주, 지난주, 이번 달, 지난달 또는 며칠 전(최대 180일 전)의 데이터를 확인할 수 있습니다.



사용 사례

대량의 스팸	단계별 방법
외부 파일 공유	단계별 방법
서드 파티 애플리케이션	단계별 방법
피싱 시도	단계별 방법

“지나치게 많거나 불필요한 이메일을 제어하여 학교의 보안 위협을 줄이고 싶습니다.”

대량의 스팸

보안 대시보드에서는 다음을 비롯해 Google Workspace for Education 환경 전반의 활동이 시각적으로 표시됩니다.

- 스팸
- 피싱
- 멀웨어
- 의심스러운 첨부파일
- 기타

단계별 방법

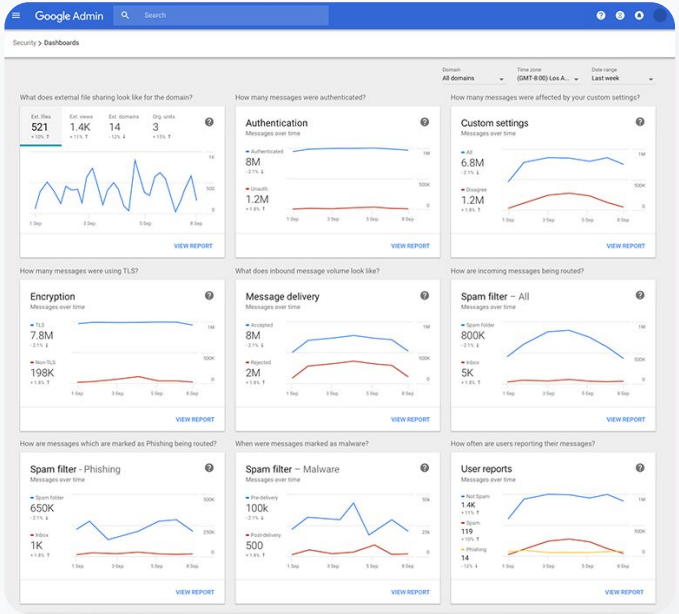
관련 고객센터 문서

- 보안 대시보드 정보

방법: 대시보드 개요

보안 대시보드 확인 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **대시보드**를 클릭합니다.
- 보안 대시보드에서 데이터를 살펴보거나, Sheets 또는 서드 파티 도구로 데이터를 내보내거나, 조사 도구에서 조사를 시작할 수 있습니다.



관련 고객센터 문서

- 보안 대시보드 정보

민감한 정보가 제3자와 공유되는 것을 방지하기 위해 외부 파일 공유 활동을 확인하고 싶습니다.”

외부 파일 공유

보안 대시보드의 **파일 노출 보고서**를 사용하여 다음을 비롯해 도메인에 대한 외부 파일 공유 관련 측정항목을 확인할 수 있습니다.

- 특정 기간 동안 도메인 외부 사용자에게 공유된 이벤트 수
- 특정 기간 동안 수신된 외부 파일 조회수

단계별 방법

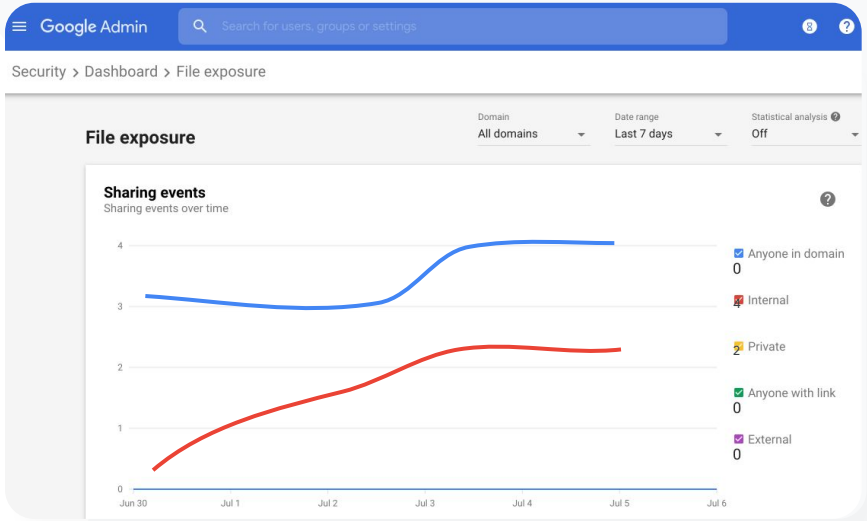
관련 고객센터 문서

- 보안 상태 페이지 시작하기

방법: 외부 파일 공유

파일 노출 보고서를 보는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **대시보드**를 클릭합니다.
- **도메인의 외부 파일 공유 상태는 어떤가요?**라는 제목의 패널에서 오른쪽 하단 모서리의 **보고서 보기**를 클릭합니다.



관련 고객센터 문서

- 보안 대시보드 정보
- 파일 노출 보고서

서드 파티 애플리케이션

내 도메인의 데이터에 액세스할 수 있는 서드 파티 애플리케이션을 확인하고 싶습니다."

보안 대시보드에서 **OAuth 권한 활동 보고서**를 사용하여 도메인에 연결된 서드 파티 애플리케이션 및 애플리케이션에서 액세스할 수 있는 데이터를 모니터링할 수 있습니다.

- OAuth는 사용자의 암호를 노출하지 않으면서 서드 파티 서비스에게 사용자 계정 정보에 액세스할 수 있는 권한을 부여합니다. 액세스 권한을 갖는 서드 파티 앱을 제한하는 것이 좋습니다.
- OAuth 권한 활동 패널을 사용하여 앱, 범위 또는 사용자별로 권한 활동을 모니터링하고 권한 부여 여부를 업데이트할 수 있습니다.

단계별 방법

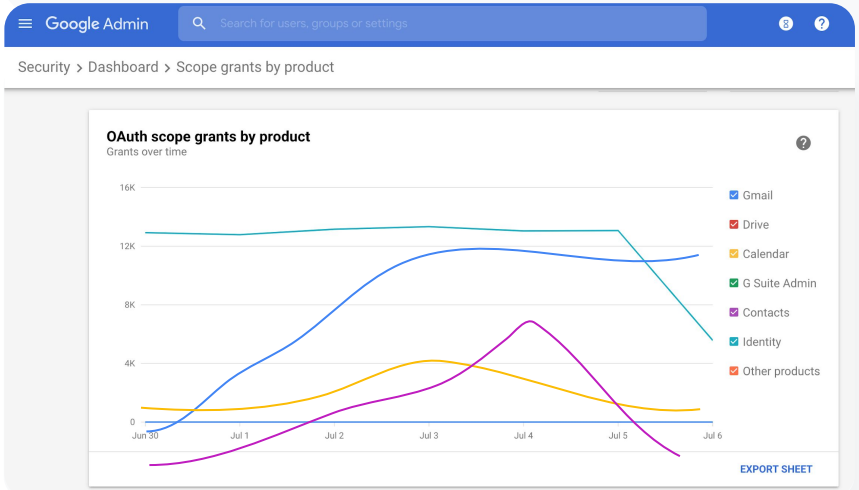
관련 고객센터 문서

- OAuth 권한 활동 보고서

방법: 서드 파티 애플리케이션

OAuth 권한 활동 보고서를 보는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **대시보드**를 클릭합니다.
- 하단에서 **보고서 보기**를 클릭합니다.
- 제품(앱), 범위 또는 사용자별로 OAuth 권한 활동을 확인할 수 있습니다.
- 정보를 필터링하려면 **앱**, **범위**, 또는 **사용자**를 클릭합니다.
- 스프레드시트 보고서를 생성하려면 **시트 내보내기**를 클릭합니다.



관련 고객센터 문서

- OAuth 권한 활동 보고서

“사용자들이 피싱 시도를 신고했습니다. 피싱 이메일이 언제 도착했는지, 사용자가 받은 이메일 내용이 정확히 무엇인지, 어떤 위험에 노출되었는지 추적하고 싶습니다.”

단계별 방법

관련 고객센터 문서

- 사용자가 문제가 있는 이메일을 어떻게 표시하고 있나요?
- 사용자 보고서

피싱 시도

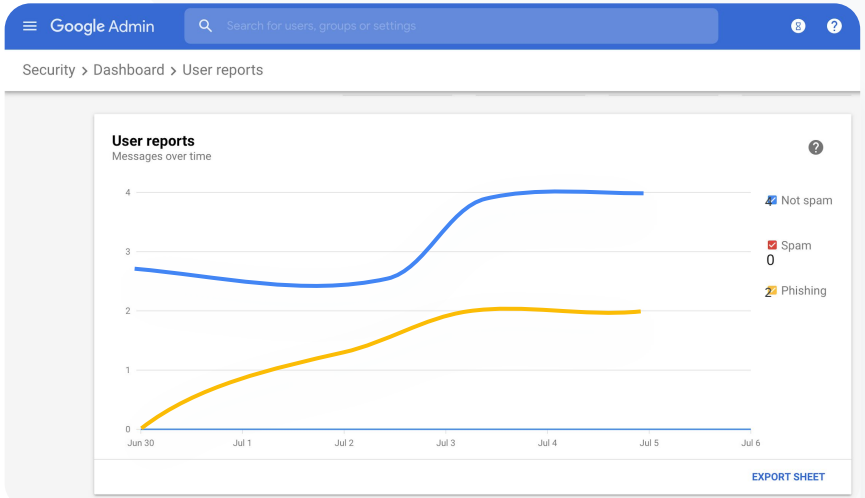
보안 대시보드의 **사용자 보고서 패널**에서는 특정 기간 동안 피싱 또는 스팸으로 신고된 메시지 관련 정보를 제공합니다. 피싱으로 표시된 이메일의 정보(수신자, 열람 여부 등)를 확인할 수 있습니다.

- 사용자 보고서를 사용하여 특정 기간에 사용자가 메시지를 어떻게 표시(예: 스팸, 스팸이 아님, 피싱)하는지 확인할 수 있습니다.
- 메시지의 내부 또는 외부 전송 여부, 기간 등 특정 유형의 메시지에 대한 세부정보만 제공하도록 그래프를 맞춤설정할 수 있습니다.

방법: 피싱 시도

사용자 보고서 패널을 보는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **대시보드**를 클릭합니다.
- **사용자 보고서 패널**의 오른쪽 하단에서 **보고서 보기**를 클릭합니다.



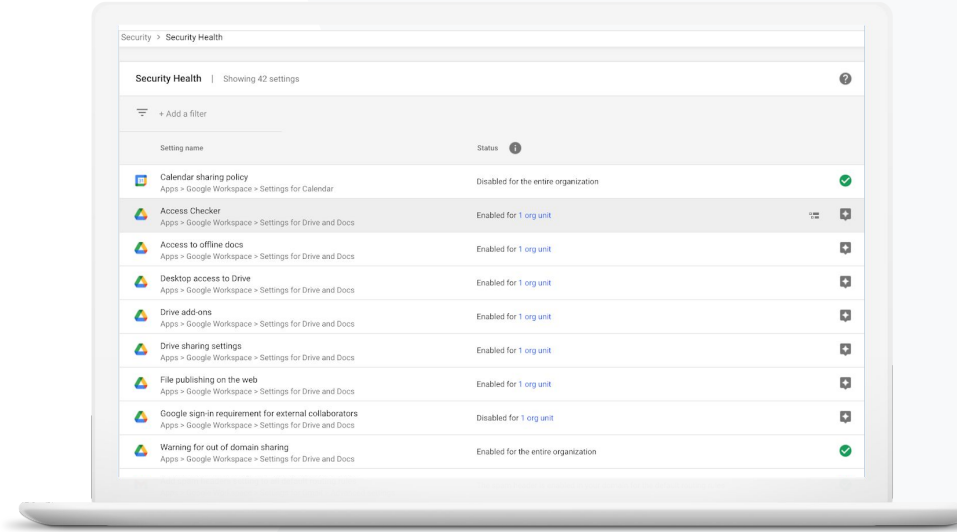
관련 고객센터 문서

- 보안 대시보드 정보
- 파일 노출 보고서

보안 상태

기본 개념

보안 상태 페이지를 사용하면 내 Google Workspace 환경의 보안 상태를 전반적으로 확인하고 현재 사용 중인 구성을 Google 권장사항과 비교하여 보안 문제가 발생하기 전에 선제적으로 조직을 보호할 수 있습니다.



사용 사례

보안 권장사항 — 단계별 방법

위험 영역에 대한 권장사항 — 단계별 방법

“보안 정책을 설정하는 방법에 대한 권장사항이나 추천사항을 따르고 싶습니다.”

보안 권장사항

보안 상태 페이지에서는 보안 정책에 관한 권장사항과 함께 다음 정보를 제공합니다.

- 도메인의 잠재 위험 영역에 관한 권장사항
- 보안 효과를 높이는 최적의 설정에 대한 권장사항
- 설정으로 직접 연결되는 링크
- 추가 정보 및 지원 도움말

단계별 방법

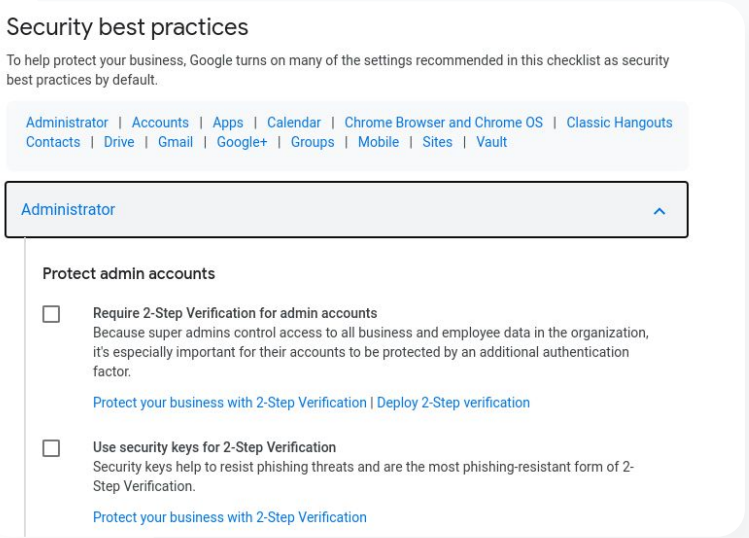
관련 고객센터 문서

- 보안 상태 페이지 시작하기

방법: 보안 권장사항 체크리스트

조직을 보호하기 위해 Google은 기본적으로 체크리스트에서 추천하는 대부분의 설정을 보안 권장사항으로 사용합니다. 아래에 강조표시된 항목을 더 자세히 살펴보세요.

- **관리자:** 관리자 계정 보호
- **계정:** 계정 도용 방지 및 해결 지원
- **앱:** 핵심 서비스에 대한 서드 파티 액세스 검토
- **Calendar:** 외부 캘린더 공유 제한
- **Drive:** 도메인 외부 사용자와의 공유 및 공동작업 제한
- **Gmail:** 인증 및 인프라 설정
- **Vault:** Vault 계정 관리, 감사, 보안 설정



관련 고객센터 문서

- 보안 설정 상태 모니터링하기

“

도메인 보안 설정을 한눈에 쉽게 파악하고 싶습니다. 잠재 위험 영역의 문제를 해결할 수 있는 실행 가능한 권장사항도 필요합니다.”

위험 영역에 대한 권장사항

보안 상태 페이지에서는 보안 구성을 검토하고 권장 변경사항을 표시합니다. 보안 상태 페이지에서 다음 작업을 수행할 수 있습니다.

- 도메인에서 잠재적인 위험 영역을 빠르게 파악
- 보안 효과를 높일 수 있는 최적의 설정에 대한 권장사항 확인
- 권장사항에 대한 추가 정보 및 지원 도움말 확인

단계별 방법

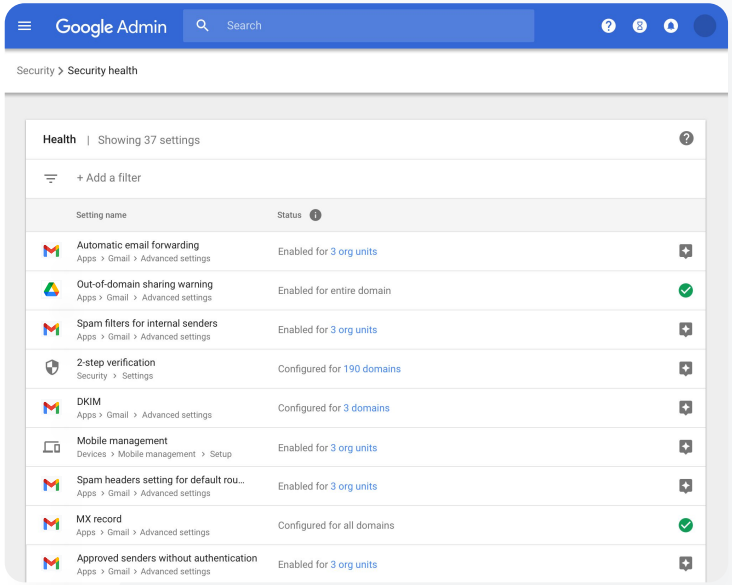
관련 고객센터 문서

- 보안 상태 페이지 시작하기

방법: 보안 권장사항

권장사항을 확인하는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **보안 상태**를 클릭합니다.
- 맨 오른쪽 열에서 상태 설정을 볼 수 있습니다.
  - 녹색 체크표시는 보안 설정을 나타냅니다.
  - 회색 아이콘은 해당 설정을 탐색하기 위한 권장사항을 나타냅니다. 아이콘을 클릭하면 세부정보 및 안내가 표시됩니다.



관련 고객센터 문서

- 보안 상태 페이지 시작하기

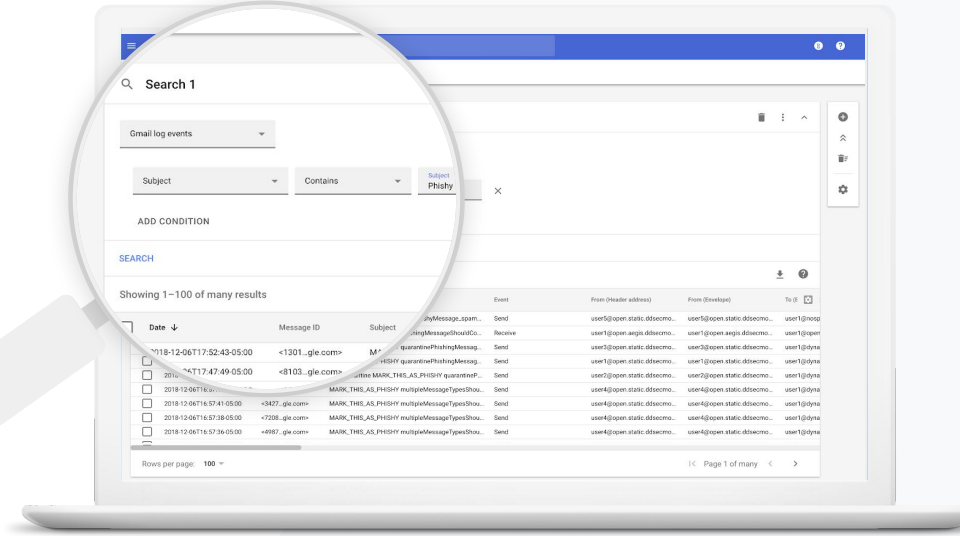
조사 도구

기본 개념

조사 도구를 사용해 도메인의 보안 및 개인 정보 보호 문제를 식별 및 분류하여 조치를 취할 수 있습니다.

사용 사례

공유되고 있는 악성 자료	단계별 방법
실수로 공유한 파일	단계별 방법
이메일 분류	단계별 방법
피싱/멀웨어 이메일	단계별 방법
악의적인 행위자 차단	단계별 방법
더 심층적인 보안 통계	단계별 방법
감독되지 않는 회의 방지	단계별 방법



“악성 자료가 포함된 파일이 공유되고 있습니다. 누가 언제 만들었는지, 누가 누구와 공유하고 누가 수정했는지 확인한 다음 파일을 삭제하고 싶습니다.”

공유되고 있는 악성 자료

조사 도구의 **Drive 로그 이벤트**를 사용하여 도메인 내 원하지 않는 파일을 찾아서 추적하여 격리하거나 삭제할 수 있습니다. Drive 로그 이벤트에 액세스하면 다음 작업을 수행할 수 있습니다.

- 이름, 작업자, 소유자 등을 기준으로 문서를 검색합니다.
- 파일 사용 권한을 변경하거나 파일을 삭제하여 조치를 취합니다.
- 사용자가 Google Workspace에서 만드는 콘텐츠와 Drive에 업로드하는 콘텐츠를 검색합니다.
- 해당 문서와 관련된 모든 로그 정보를 확인합니다.
  - 생성 날짜
  - 소유자, 조회한 사용자, 편집자
  - 공유된 날짜

단계별 방법

관련 고객센터 문서

- Drive 로그 이벤트의 조건
- Drive 로그 이벤트 관련 작업

“

파일 하나가 실수로 액세스 권한을 가지면 안 되는 그룹에 공유됐습니다.

파일에 대한 해당 그룹의 액세스 권한을 삭제하고 싶습니다.”

실수로 공유한 파일

조사 도구의 **Drive 로그 이벤트**를 사용하여 파일 공유 문제를 추적하고 해결할 수 있습니다. Drive 로그 이벤트에 액세스하면 다음 작업을 수행할 수 있습니다.

- 이름, 작업자, 소유자 등을 기준으로 문서를 검색합니다.
- 문서를 본 사용자 및 공유된 날짜를 포함하여 문서와 관련된 모든 로그 정보를 확인합니다.
- 권한을 변경하고 다운로드, 인쇄, 복사 기능을 사용 중지하여 조치를 취합니다.

단계별 방법

관련 고객센터 문서

- 조사 도구에서 검색 실행하기
- 검색결과에 따라 조치 취하기

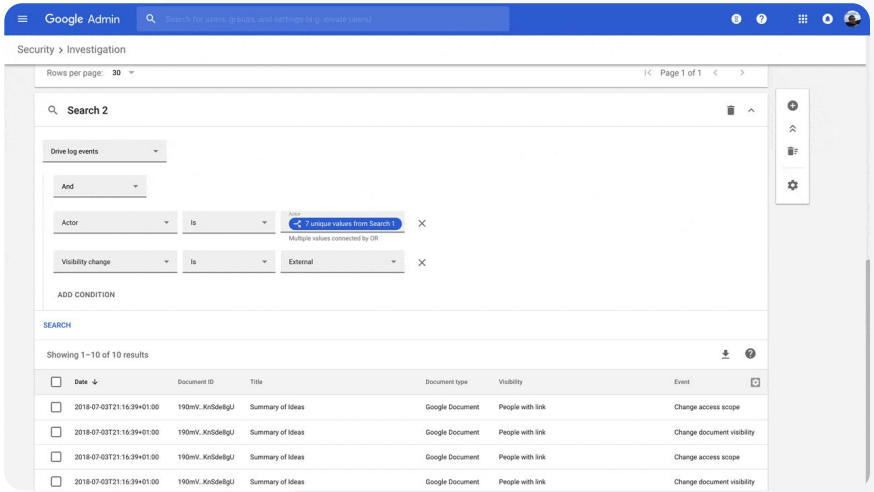
방법: Drive 로그 이벤트

Drive 로그 이벤트를 조사하는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **조사 도구**를 클릭합니다.
- **Drive 로그 이벤트**를 선택합니다.
- **조건 추가** > **검색**을 클릭합니다.

조치 방법

- 검색 결과에서 관련 파일을 선택합니다.
- **작업** > **파일 권한 감사**를 클릭하여 권한 페이지를 엽니다.
- 액세스 권한이 있는 사용자를 보려면 **사용자**를 클릭합니다.
- 선택한 파일의 링크 공유 설정을 확인 또는 수정하려면 **링크**를 클릭합니다.
- 저장하기 전에 변경사항을 검토하려면 **대기 중인 변경사항**을 클릭합니다.



관련 고객센터 문서

- 조사 도구에서 검색 실행하기
- 검색결과에 따라 조치 취하기

“누군가가 보내선 안 되는 이메일을 보냈습니다. 이러한 이메일이 누구에게 전송되었는지, 수신자가 이메일을 열었는지, 수신자가 답장했는지 확인하고 이메일을 삭제하고 싶습니다. 또한 이메일 내용도 확인하고 싶습니다.”

단계별 방법

관련 고객센터 문서

- Gmail 로그 및 Gmail 메시지 조건
- Gmail 메시지 및 Gmail 로그 이벤트 관련 작업
- 이메일의 내용을 확인하기 위한 단계

이메일 분류

조사 도구의 **Gmail 로그를** 사용하여 도메인 내에서 위험하거나 악의적인 이메일을 식별하고 조치를 취할 수 있습니다. Gmail 로그에 액세스하면 다음 작업을 수행할 수 있습니다.

- 제목, 메시지 ID, 첨부파일, 발신자 등을 기준으로 특정 이메일을 검색합니다.
- 작성자, 수신자, 열람 여부, 전달 여부 등 이메일 세부정보를 확인합니다.
- 검색결과에 따라 조치를 취합니다. Gmail 메시지에 삭제, 복원, 스팸 또는 피싱으로 표시, 받은편지함으로 전송, 스팸 격리 저장소로 전송 등을 비롯한 조치를 취할 수 있습니다.

피싱 및 멀웨어 이메일

조사 도구, 특히 **Gmail 로그를** 열면 도메인 내에서 악성 이메일을 찾고 격리하는 데 도움이 될 수 있습니다. Gmail 로그에 액세스하면 다음 작업을 수행할 수 있습니다.

- 첨부파일 등 특정 내용을 찾기 위해 이메일 메시지를 검색합니다.
- 수신자 및 열람 여부 등 특정 이메일에 대한 정보를 확인합니다.
- 메시지 및 대화목록을 확인하여 악성 여부를 파악합니다.
- VirusTotal 보고서를 통해 이메일 첨부파일을 검사하여 자세한 위협 컨텍스트 및 평판 데이터를 얻습니다.
- 메시지를 스팸 또는 피싱으로 표시하거나, 특정 받은편지함 또는 스팸 격리 저장소로 전송하거나, 삭제하여 조치를 취합니다.

“피싱 또는 멀웨어 이메일이 사용자에게 전송되었습니다. 이메일에 있는 링크를 클릭하거나 첨부파일을 다운로드하면 사용자와 도메인이 위험에 노출되기에 사용자가 이러한 작업을 수행했는지 확인하고 싶습니다.”

단계별 방법

관련 고객센터 문서

- Gmail 로그 및 Gmail 메시지 조건
- Gmail 메시지 및 Gmail 로그 이벤트 관련 작업
- 이메일의 내용을 확인하기 위한 단계
- VirusTotal 보고서 보기

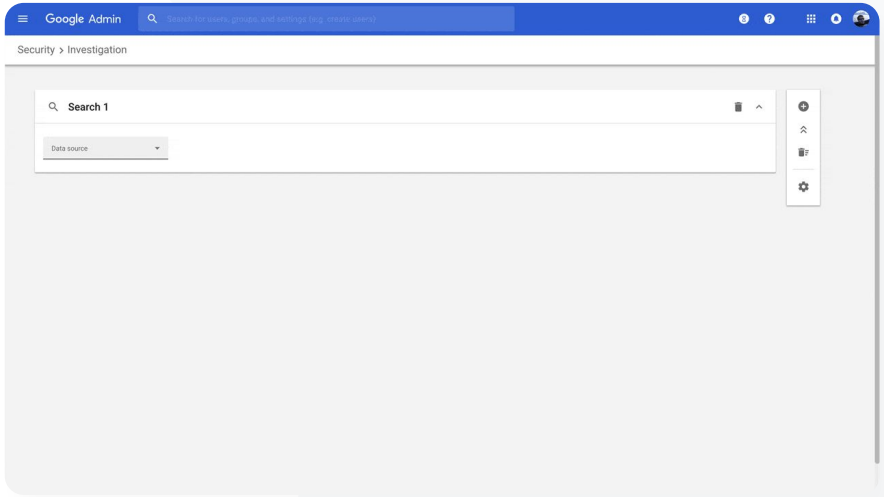
방법: Gmail 로그

Gmail 로그를 조사하는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **조사 도구**를 클릭합니다.
- **Gmail 로그 이벤트** 또는 **Gmail 메시지**를 선택합니다.
- **조건 추가** > **검색**을 클릭합니다.

조치 방법

- 검색 결과에서 관련 파일을 선택합니다.
- **작업**을 클릭합니다.
- **받은편지함에서 메시지 삭제**를 선택합니다.
- 작업 결과를 확인하려면 페이지 하단의 '보기'를 클릭합니다.
- **결과** 열에서 작업 상태를 볼 수 있습니다.



관련 고객센터 문서

- Gmail 로그 및 Gmail 메시지 조건
- Gmail 메시지 및 Gmail 로그 이벤트 관련 작업
- 이메일의 내용을 확인하기 위한 단계

“

악의적인 행위자가 도메인 내의 인지도 높은 사용자를 타겟팅하고 있는데, 도용 시도를 막았다 하면 금세 또 시도하곤 합니다.

어떻게 해야 끝낼 수 있나요?”

악의적인 행위자 차단

조사 도구의 사용자 로그를 사용하여 다음을 수행할 수 있습니다.

- 조직의 사용자 계정을 도용하려는 시도를 파악하고 조사합니다.
- 조직의 사용자가 어떤 2단계 인증 방법을 사용하는지 모니터링합니다.
- 조직의 사용자가 실패한 로그인 시도에 대해 자세히 알아봅니다.
- 조사 도구를 사용해 활동 규칙을 만듭니다. 특정 행위자의 메일 및 기타 악의적인 활동을 자동으로 차단할 수 있습니다.
- 고급 보호 프로그램으로 인지도 높은 사용자를 보호합니다.
- 사용자를 복원하거나 정지합니다.

단계별 방법

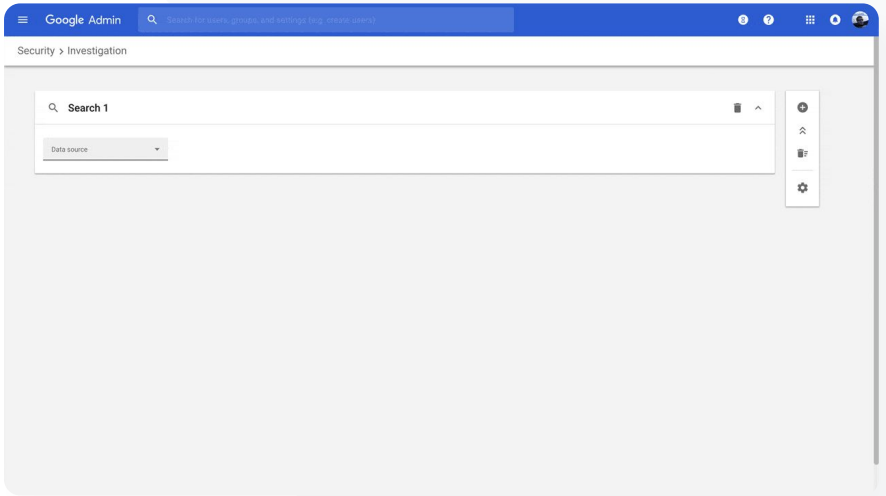
관련 고객센터 문서

- 사용자 로그 이벤트 검색 및 조사하기
- 조사 도구로 활동 규칙 만들기

방법: 악의적인 행위자 차단

사용자 로그 이벤트를 조사하는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **조사 도구**를 클릭합니다.
- **사용자 로그 이벤트**를 선택합니다.
- **조건 추가** > **검색**을 클릭합니다.



사용자를 복원하거나 정지하는 방법

- 검색 결과에서 한 명 또는 여러 명의 사용자를 선택합니다.
- 작업 드롭다운 메뉴를 클릭합니다.
- **사용자 복원** 또는 **사용자 정지**를 클릭합니다.

특정 사용자에 대한 세부정보를 확인하는 방법

- 검색 결과 페이지에서 한 명의 사용자만 선택합니다.
- 작업 드롭다운 메뉴에서 **세부정보 보기**를 클릭합니다.

관련 고객센터 문서

- 사용자 로그 이벤트 검색 및 조사하기

교사 중 한 명이 Gmail에서 첨부된 파일이 의심스러워 보인다고 신고했습니다.

IT팀에서 파일이 보안 위협에 해당하는지 확인할 방법이 있나요?"

단계별 방법

관련 고객센터 문서

- 조사 도구에서 검색 실행하기
- 조사 도구에서 VirusTotal 보고서 보기

더 심층적인 보안 통계 확인

VirusTotal 보고서는 종합적인 개요를 제공하여 보안 조사의 결과를 더 자세하게 설명합니다. 이를 통해 관리자는 크라우드소싱 정보를 기반으로 특정 도메인, 첨부파일, IP 주소 또는 URL의 보안을 확인할 수 있습니다.

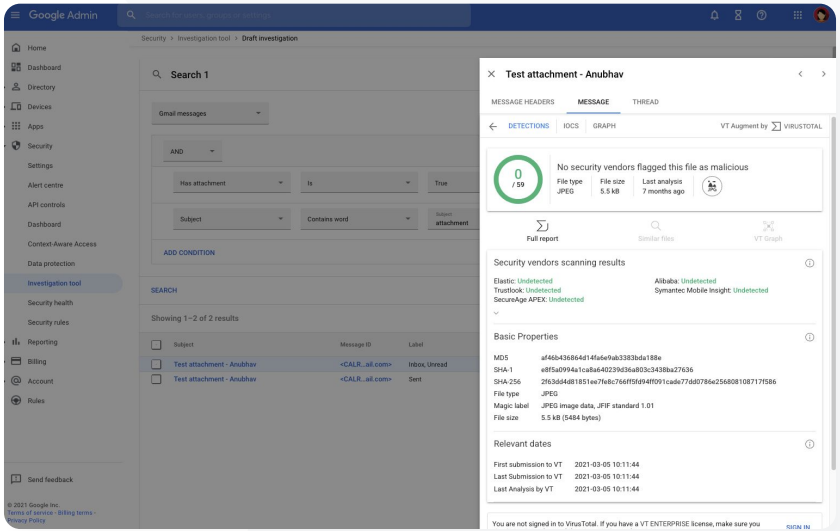
- Gmail 및 Chrome 로그 이벤트에 대한 추가 보안 통계를 확인할 수 있습니다.
- 의심스러운 파일, URL, 도메인, IP 주소를 분석할 수 있습니다.
- 첨부파일이나 웹사이트가 위험하다고 표시된 이유에 대한 크라우드소싱 세부정보에 액세스할 수 있습니다.
- 보안 문제를 해결을 위한 의사 결정을 내리는 데 도움을 받을 수 있습니다.

방법: 더 심층적인 보안 통계 확인

Gmail과 관련된 VirusTotal 보고서를 보는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **보안 센터** > **조사 도구**를 클릭합니다.
- **Gmail 메시지**를 선택합니다.
- **조건 추가** > **첨부파일 있음**을 클릭합니다.
- 검색결과에서 **메시지 ID** 또는 **제목 링크**를 클릭합니다.
- 측면 패널에서 **메시지** 또는 **스레드** 탭을 클릭합니다.
- **VirusTotal 보고서 보기**를 선택합니다.

관리자는 Chrome과 관련된 VirusTotal 보고서도 볼 수 있습니다. 위의 안내를 따른 다음, 조사 도구에서 **Chrome 로그 이벤트**를 선택하세요.



관련 고객센터 문서

- 조사 도구에서 VirusTotal 보고서 보기

감독되지 않는 온라인 회의 방지

수업이 끝난 후에도 학생들이 Google Meet 통화에 계속 남아 있습니다. 학습에 방해가 되지 않도록 모두의 Meet 통화를 종료할 방법이 필요합니다."

Google Workspace 관리자는 조사 도구에서 **모든 참석자를 내보내고 회의 종료** 작업을 사용하여 조직 내의 회의에서 모든 사용자를 삭제할 수 있습니다. 각 Google Meet 통화의 회의 주최자도 이 기능을 사용할 수 있습니다.

- 회의에 참여한 모든 사용자(소그룹 채팅방 사용자 포함)의 회의를 종료합니다.
- 모든 사용자를 대상으로 회의 주최자가 없는 회의의 향후 모든 일정에 참석하는 것을 방지합니다.

단계별 방법

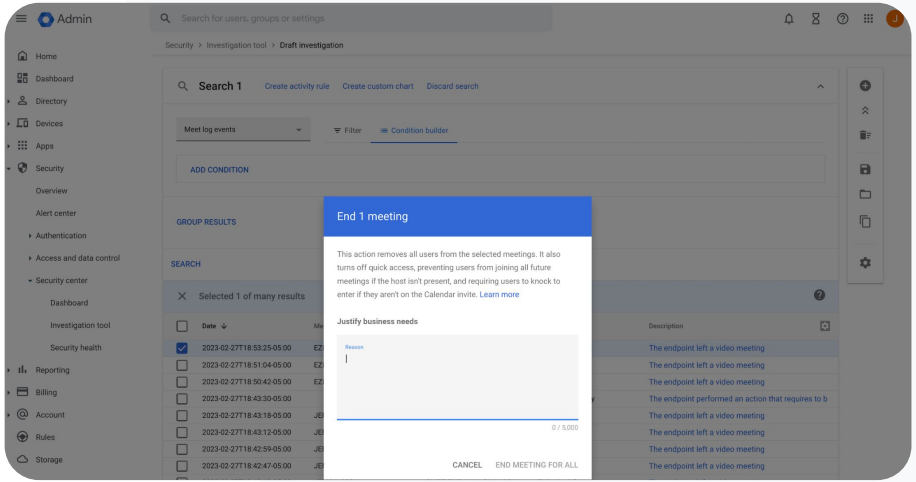
관련 고객센터 문서

- 조사 도구를 사용하여 회의 종료하기

방법: 감독되지 않는 온라인 회의 방지

조사 도구를 사용하여 모든 참석자를 내보내고 회의를 종료하는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **보안 센터** > **조사 도구**를 클릭합니다.
- **Meet 로그 이벤트**를 선택합니다.
- **검색**을 클릭하면 검색결과에 Meet 로그 이벤트 목록이 표시됩니다.
- 모든 사용자를 내보내고 종료하려는 회의의 체크박스를 선택합니다.
- **작업**을 선택합니다.
- **모든 참석자를 내보내고 회의 종료**를 클릭합니다.



관련 고객센터 문서

- 조사 도구를 사용하여 회의 종료하기

도메인 관리 및 제어

관리자는 Google Workspace 고급 도구에 대한 액세스 권한을 통해 조직의 데이터를 관리하고, 제어를 설정하고, 사용을 모니터링하고, 교육 표준을 준수하도록 유지할 수 있습니다.

사용 사례

Gmail 첨부파일의 위협 여부 검사	단계별 방법
사용 대시보드 및 보고서 생성	단계별 방법
파일 더 쉽게 찾기	단계별 방법
내부 문서 정리	단계별 방법
부서 그룹 자동으로 채우기	단계별 방법
내부 파일 공유용 대상 생성	단계별 방법
파일 공유 제한	단계별 방법
Workspace 앱 제한사항	단계별 방법
스토리지 관리	단계별 방법
데이터 규정	단계별 방법
지원금 규정	단계별 방법
엔드포인트 기기 관리	단계별 방법
Windows 기기 관리	단계별 방법
Windows 10 기기 맞춤 설정	단계별 방법
Windows 10 기기 업데이트 자동화	단계별 방법
클라이언트 측 암호화 활용	단계별 방법

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 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

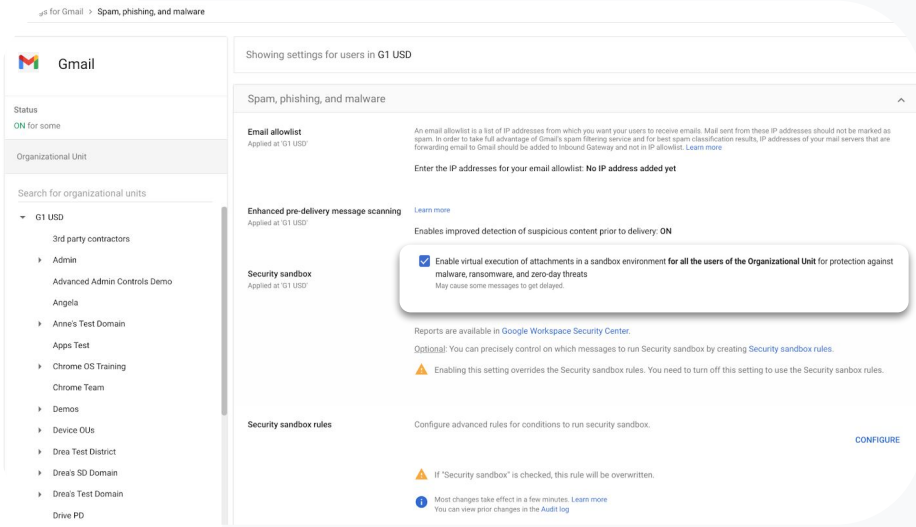
How to: Scan Gmail attachments for threats

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**



Relevant Help Center documentation

- Set up rules to detect harmful attachments

“어떻게 하면 도메인 전반의 클래스룸 사용을 파악할 수 있나요?”

사용 대시보드 및 보고서 생성

관리자는 **BigQuery Export 및 Looker Studio 템플릿**을 통해 클래스룸 활동 로그를 기반으로 Looker Studio와 같은 분석 도구 및 BigQuery에 통합된 서드 파티 시각화 파트너를 사용해 맞춤 대시보드 및 보고서를 만들 수 있습니다.

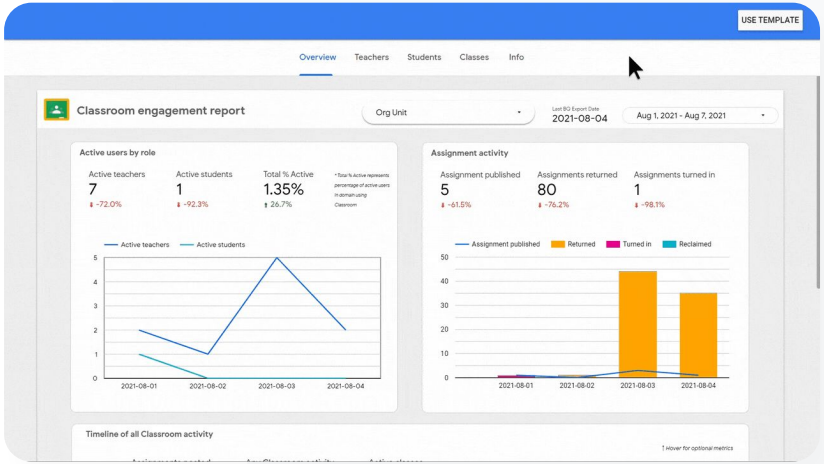
- 관리 콘솔에서 BigQuery 및 Looker Studio로 클래스룸 로그 데이터를 내보낼 수 있습니다.
- 도메인 전반에 대한 사용량 및 채택 보고서를 빠르게 살펴보고 누가 수업에서 학생을 삭제했거나 특정한 날짜의 수업을 보관 처리했는지 등을 파악할 수 있습니다.
- 맞춤설정 가능한 Looker Studio 대시보드 템플릿을 통해 중요한 추세를 이해하고 더 빠르게 조치를 취할 수 있습니다.

단계별 방법

관련 고객센터 문서

- BigQuery Export 및 데이터 스튜디오 템플릿 설정

방법: 사용 대시보드 및 보고서 생성



01 BigQuery 프로젝트 설정 및 내보내기

- console.cloud.google.com에 로그인하고 **새 프로젝트 만들기**로 이동합니다.
- admin.google.com에 로그인하고 **보고서** > **BigQuery Export**로 이동합니다.
- **Cloud BigQuery 프로젝트**를 클릭하고 > 데이터 세트의 이름을 지정한 다음 > **저장**합니다.

02 Looker Studio에 BigQuery Export 추가

- Looker Studio에 로그인하고 **만들기** > **데이터 소스**로 이동합니다.
- **BigQuery 커넥터** > **내 프로젝트**를 선택하고 생성한 프로젝트 > **활동**을 클릭합니다.
- **파티션을 나눈 테이블** 아래의 상자를 선택하고 > **연결**을 클릭합니다.

03 Looker Studio 대시보드 만들기

- 템플릿을 열고 > **템플릿 사용**을 선택합니다.
- **새 데이터 소스**에서 **활동** 데이터 소스를 선택합니다.
- **보고서 복사**를 클릭합니다.

관련 고객센터 문서

- BigQuery Export 및 데이터 스튜디오 템플릿 설정

학부모가 Gmail, Chat 및 Docs를 통해 제출한 현장학습 동의서를 추적해야 합니다.

도메인 전반에서 이러한 파일을 어떻게 찾을 수 있나요?”

단계별 방법

관련 고객센터 문서

- Google Cloud Search 가이드
- 사용자별로 Cloud Search 사용/사용 중지

파일 더 쉽게 찾기

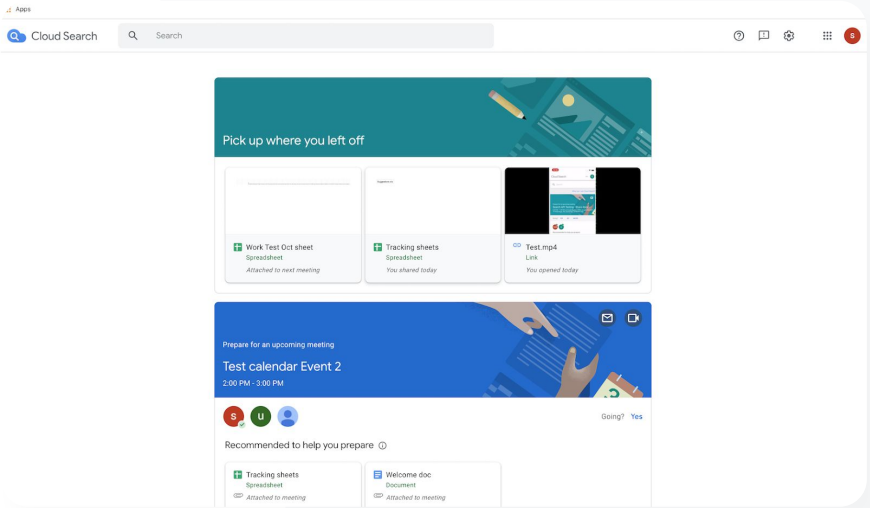
교육자는 Google Cloud Search를 사용하여 Google Workspace 및 서드 파티 앱 전반에서 콘텐츠를 빠르게 찾을 수 있습니다.

- 노트북, 휴대전화 또는 태블릿을 사용해 어디서나 업무 시 필요한 정보를 찾을 수 있습니다.
- Drive, 주소록, Gmail 및 서드 파티 데이터 소스 등 Google Workspace 전반에서 검색할 수 있습니다.

방법: 파일 더 쉽게 찾기

사용자에 대해 Cloud Search 사용 설정

- **관리 콘솔**에 로그인하고 **메뉴** > **앱** > **Google**로 이동합니다.
- **서비스 상태**를 클릭합니다.
- 조직의 모든 사용자에 대해 서비스를 사용 또는 사용 중지하려면 **모든 사용자에 대해 사용 설정** 또는 **모든 사용자에 대해 사용 중지**를 선택합니다.
- **저장**을 클릭합니다.
- 여러 조직 단위 간 또는 조직 단위 내에서 사용자에 대해 서비스를 사용 설정하려면 **액세스 그룹**을 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- Google Cloud Search 가이드
- 사용자별로 Cloud Search 사용/사용 중지

“기관의 파일에 민감도 라벨을 적용해 규정 준수 요구사항에 맞추도록 조정하고, 오용을 방지하고, 파일 구성을 개선하고 싶습니다.”

도메인 전반에서 문서 정리

Drive 라벨은 사용자가 도메인 전반에서 정책을 찾고, 정리하고, 적용하는 데 도움이 됩니다. 관리자는 Drive 라벨을 만들고 관리하여 파일 오용을 방지하고 학생 데이터가 규정 준수 요구사항을 충족하도록 할 수 있습니다.

- 라벨은 IEP, DOD 또는 규정 준수 문서와 같은 민감한 교육 파일을 정리하는 데 도움이 되는 메타데이터입니다.
- 관리자만 라벨을 만들고, 구조를 정의하고, 게시할 수 있습니다. 조직의 사용자는 수정 권한이 있는 파일에 라벨을 적용할 수 있으며 필드 값을 설정할 수 있습니다.
- Drive 라벨은 자동 데이터 손실 방지를 지원하는 데 사용할 수 있습니다.

단계별 방법

관련 고객센터 문서

- Drive 라벨 관리

방법: 도메인 전반에서 문서 정리

작동 방식

Google Drive는 도메인 전반에서 파일을 정리하는 데 도움이 되도록 배지(시각적 표시기)가 있는 라벨과 표준 라벨을 제공합니다.

기관에서 Drive 라벨을 사용 설정하는 방법

- **관리 콘솔**에 로그인합니다.
- **메뉴** > **앱** > **Google Workspace** > **Drive 및 Docs**를 클릭합니다.
- **라벨**을 선택합니다.
- 라벨을 **사용 설정** 또는 **사용 중지**합니다.
- **저장**을 클릭합니다.

관련 고객센터 문서

- Drive 라벨 관리

“기관에 새 교육자가 들어올 때마다 '교육자' 이메일 목록에 포함되도록 그룹 멤버십을 자동화하려면 어떻게 해야 하나요?”

부서 그룹 자동으로 채우기

동적 그룹을 사용하면 관리자는 맞춤 기준으로 학교 차원의 그룹 멤버십을 업데이트할 수 있습니다.

- 멤버십을 자동으로 관리하는 동적 그룹을 만듭니다.
- 생성한 멤버십 쿼리를 기반으로 그룹을 최신 상태로 유지합니다.
- 동적 그룹을 다음 용도로 사용할 수 있습니다.
  - 이메일 및 메일링 리스트
  - 검토 대상 그룹 및 공동작업 받은편지함
  - 보안 그룹

단계별 방법

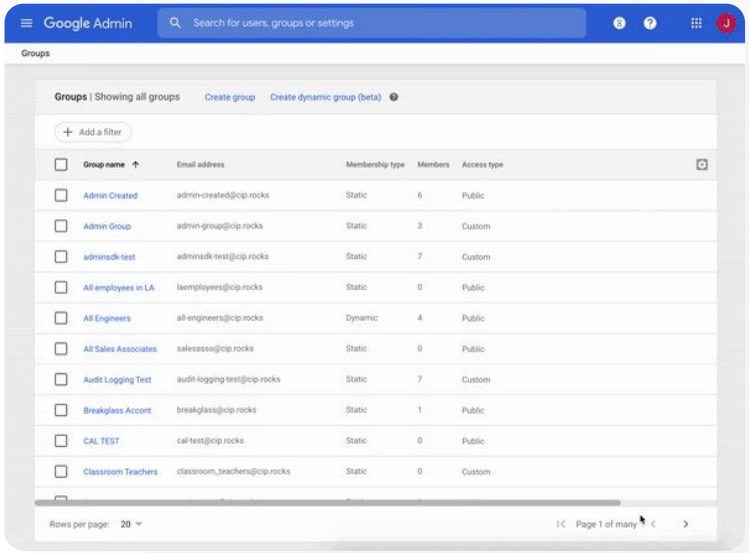
관련 고객센터 문서

- 동적 그룹을 사용하여 멤버십을 자동으로 관리하기

방법: 그룹 자동으로 채우기

동적 그룹 만들기

- **관리 콘솔**에 로그인하고 **메뉴** > **디렉터리** > **그룹스**로 이동합니다.
- **동적 그룹 만들기**를 클릭합니다.
- 다음에서 멤버십 쿼리를 만듭니다.
  - 조건 목록: 멤버십(예: 부서)에 사용할 기준입니다.
  - 값 필드: 사용하려는 값입니다.
- 다음 정보를 입력합니다.
  - 이름: 목록 및 메시지에서 그룹을 식별합니다.
  - 설명: 그룹의 목적입니다.
  - 그룹 이메일: 그룹에서 사용하는 이메일 주소입니다.
- **저장**을 클릭합니다.
- **완료**를 클릭합니다.



관련 고객센터 문서

- 동적 그룹을 사용하여 멤버십을 자동으로 관리하기

내부 파일 공유용 대상 생성

공유 대상 그룹 설정을 사용하면 사용자가 파일을 실수로 과도하게 공유할 가능성이 줄어들어 조직의 데이터 보안을 강화할 수 있습니다.

- 사용자가 적절한 사용자(예: 특정 팀 또는 부서)와만 파일을 공유하도록 합니다.
- 공유 대상 그룹은 관리자가 사용자에게 항목 공유를 권장하는 사용자 그룹입니다.
- 관리자는 사용자의 공유 설정에 공유 대상 그룹을 추가하여 더 구체적인 대상과 공유하도록 권장할 수 있습니다.
- Google Drive, Docs 및 Chat에서 사용할 수 있습니다.

"교직원이 실수로 조직 전체와 문서를 공유하여 민감한 데이터가 위험에 처하는 일이 발생하고 있습니다. 어떻게 하면 교직원이 관련성 있는 더 작은 그룹을 대상으로 공유하도록 제한할 수 있나요?"

단계별 방법

관련 고객센터 문서

- 공유 대상 그룹에 대한 정보
- 공유 대상 그룹 배포 시 권장사항
- 공유 대상 그룹 만들기

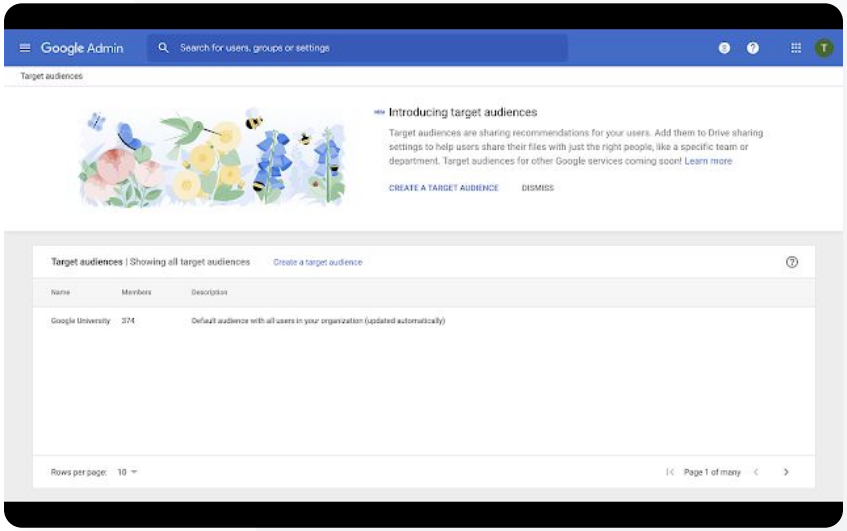
방법: 내부 파일 공유용 대상 생성

작동 방식

공유 대상 그룹을 만든 다음 구성원을 추가하고 Google Drive에 공유 대상 그룹을 적용하여 사용자의 공유 설정에서 사용하도록 할 수 있습니다. 예를 들어, 교직원이 Drive 파일을 공유할 때 '모든 교직원' 공유 대상 그룹이 보이게 할 수 있습니다.

기관에서 Drive 라벨을 사용 설정하는 방법

- **관리 콘솔**에 로그인하고 **메뉴** > **디렉터리** > **공유 대상** 그룹으로 이동합니다.
- **공유 대상 그룹 생성**을 클릭합니다.
- **이름**에 공유 대상 그룹의 이름을 입력합니다.
- **구성원 추가**를 선택하고 > 원하는 구성원을 포함합니다.
- **완료**를 클릭합니다.



관련 고객센터 문서

- 공유 대상 그룹에 대한 정보
- 공유 대상 그룹 배포 시 권장사항
- 공유 대상 그룹 만들기

“중고등학교 학생이 초등학교 학생과 문서를 공유하지 않도록 하려면 어떻게 해야 하나요?”

파일 공유 제한

Drive 신뢰 규칙을 사용하면 관리자가 Google Drive 파일에 대한 액세스 권한을 누구에게 부여할지를 제어할 수 있어 기관 데이터의 개인 정보를 보호하는 데 도움이 됩니다. 정책은 개별 사용자, 그룹, 조직 단위, 도메인에 적용될 수 있습니다.

- 민감한 정보를 보호하고 업계 표준과 규정을 준수합니다.
- 내부 및/또는 외부 도메인 공유를 제한합니다. 관리자는 신뢰 규칙을 만들어 조직 내에서 학생만 Drive 파일을 공유하도록 허용할 수 있습니다.
- '신뢰 규칙' 사용 설정 시 Google Drive 관리자 제어의 기존 '공유 옵션'을 대체하게 됩니다.

단계별 방법

관련 고객센터 문서

- Drive 공유 신뢰 규칙 만들기 및 관리하기

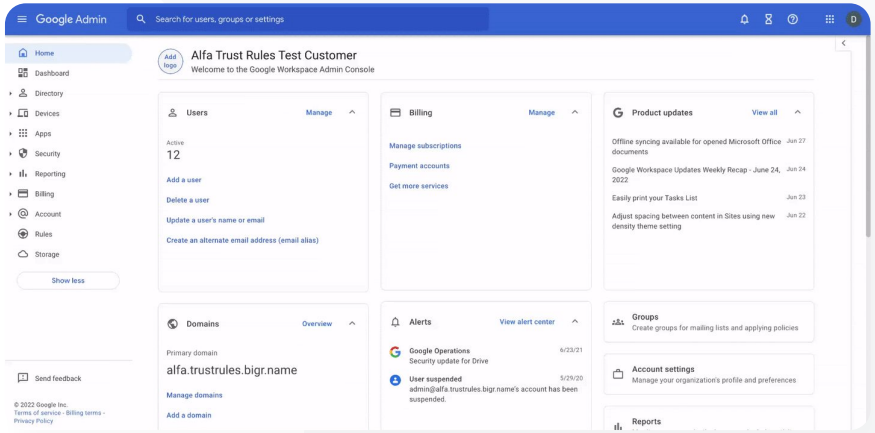
방법: 파일 공유 제한

Drive 신뢰 규칙 사용 설정

- **관리 콘솔**에 로그인하고 **메뉴 > 규칙**으로 이동합니다.
- 페이지 상단의 **안전한 공동작업** 카드에서 **신뢰 규칙 사용 설정**을 클릭합니다.
- 작업 목록이 자동으로 열리고 신뢰 규칙 활성화 진행 상황이 표시됩니다.

관리자는 신뢰 규칙을 만들고, 신뢰 규칙 세부정보를 확인 및 편집하고, 신뢰 규칙을 삭제하고, 신뢰 규칙 로그 이벤트를 볼 수 있습니다.

신뢰 규칙 관리를 위한 단계별 안내를 확인하려면 관리자 고객센터를 방문하세요.



관련 고객센터 문서

- Drive 공유 신뢰 규칙 만들기 및 관리하기

Google Workspace 앱 제한사항

컨텍스트 인식 액세스를 사용하여 사용자 신원, 위치, 기기 보안 상태, IP 주소와 같은 속성을 기반으로 **Google Workspace 및 서드 파티 보안 보장 마크업 언어(SAML)** 앱에 대한 상세 액세스 제어 정책을 만들 수 있습니다. 네트워크 외부에서 앱에 액세스하는 것을 제한할 수도 있습니다.

- 핵심 Google Workspace for Education 서비스에 컨텍스트 인식 액세스 정책을 적용할 수 있습니다.
- 예를 들어 기관에서 발급한 기기에서 이루어지는 Workspace 앱에 대한 액세스를 제한하거나 사용자의 저장 기기가 암호화된 경우에만 Drive에 대한 액세스를 허용하도록 할 수 있습니다.

"사용자가 네트워크에 있을 때 특정 앱에 대한 액세스를 제한하고 싶습니다."

단계별 방법

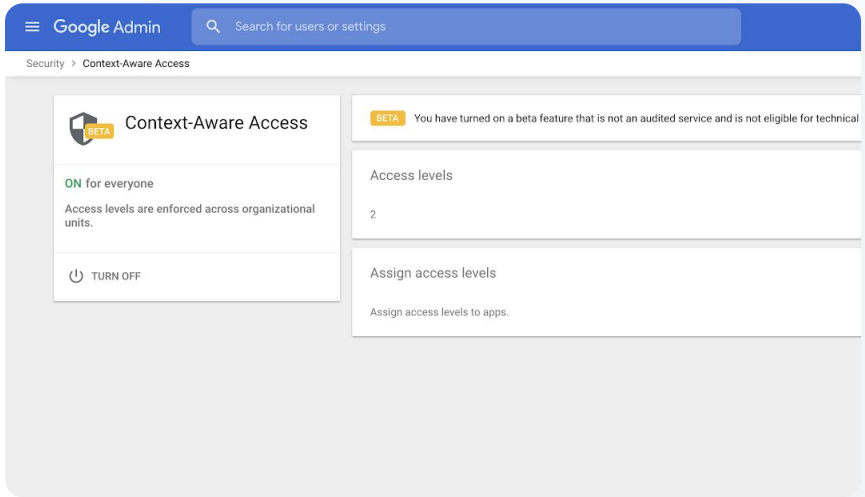
관련 고객센터 문서

- 컨텍스트 인식 액세스 개요
- 앱에 컨텍스트 인식 액세스 수준 할당하기

방법: Google Workspace 앱 사용 제한

컨텍스트 인식 액세스를 사용하는 방법

- **관리 콘솔**에 로그인합니다.
- **보안** > **컨텍스트 인식 액세스** > **할당**을 선택합니다.
- **액세스 수준 지정하기**를 선택하면 앱 목록이 표시됩니다.
- **조직 단위 또는 구성 적용 그룹**을 선택하여 목록을 정렬합니다.
- 조정하려는 앱 옆의 **할당**을 선택합니다.
- 하나 이상의 액세스 수준을 선택합니다.
- 사용자가 둘 이상의 조건을 충족하도록 하려면 여러 수준을 만듭니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- 컨텍스트 인식 액세스 개요
- 앱에 컨텍스트 인식 액세스 수준 할당하기

“도메인 전반에 새 스토리지 관리 계획을 구현하고 싶습니다.”

도메인 전반의 스토리지 관리

Google Workspace for Education이 있는 기관에서는 기본 100TB의 공용 클라우드 스토리지를 이용할 수 있습니다. 이는 약 1억 개 이상의 문서, 800만 개의 프레젠테이션 또는 40만 시간의 동영상을 저장하기에 충분한 용량입니다. **공용 Drive 스토리지를 관리**하여 기관에서 스토리지를 효과적으로 사용하도록 보장합니다.

관리자 도구, 보고 및 로그를 사용하여 다음을 수행합니다.

- 스토리지 사용량 파악
- 스토리지 한도 설정
- 스토리지를 과도하게 사용하는 계정 식별

Teaching and Learning Upgrade 및 Education Plus에서는 기본 제공 스토리지에 더해 추가 스토리지 용량을 제공합니다.

- Teaching and Learning Upgrade의 경우 라이선스당 공용 스토리지에 100GB가 추가됩니다.
- Education Plus의 경우 라이선스당 공용 스토리지에 20GB가 추가됩니다.

단계별 방법

관련 고객센터 문서

- 관리자를 위한 스토리지 가이드
- 스토리지 가용성 및 사용량 이해하기
- 여유 공간 확보 또는 추가 스토리지 구매하기
- 스토리지 한도 설정하기

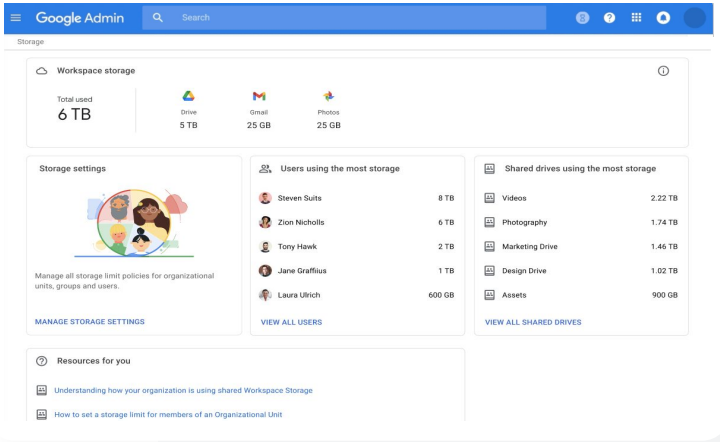
방법: 도메인 전반의 스토리지 관리

사용자별로 스토리지 사용량 파악하기

- **관리 콘솔**에 로그인하고 **메뉴** > **스토리지**로 이동합니다.
- 조직 및 사용자별로 스토리지 사용량을 확인합니다.

스토리지 한도 설정하기

- **관리 콘솔**에서 **메뉴** > **스토리지**로 이동합니다.
- **스토리지 설정**에서 **관리**를 클릭합니다.
- **사용자 스토리지 한도**를 클릭하고 > 한도를 적용할 항목을 선택합니다.
  - 조직 단위: **조직 단위**를 클릭합니다.
  - 그룹: **그룹스**를 클릭하고 > **검색창**을 클릭하고 > **그룹 이름**을 입력한 다음 > **그룹**을 클릭합니다.
- **사용**을 선택하고 **스토리지**를 설정합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- 관리자를 위한 스토리지 가이드
- 스토리지 가용성 및 사용량 이해하기
- 여유 공간 확보 또는 추가 스토리지 구매하기
- 스토리지 한도 설정하기

“규제법에 따라 학생, 교수진, 교직원 데이터가 EU 내에 머물어야만 합니다.”

데이터 규정

관리자는 **데이터 리전 정책**을 사용하여 미국 또는 영국/유럽과 같이 특정 지리적 위치에 데이터를 저장할 수 있습니다.

- Education Plus 및 Education Standard 사용자는 사용자 일부에 대해 특정 데이터 리전을 선택하거나 부서별로 서로 다른 데이터 리전을 선택하고 데이터 리전 이전 진행률을 확인할 수 있습니다.
- 사용자를 조직 단위에 추가하거나(부서별로 설정하려는 경우) 구성 적용 그룹에 추가합니다(여러 부서 간 또는 부서 내 사용자에 대해 설정하려는 경우).
- Education Standard 또는 Education Plus 라이선스가 할당되지 않은 사용자에게는 데이터 리전 정책이 적용되지 않습니다.

단계별 방법

관련 고객센터 문서

- 데이터를 저장할 지리적 위치 선택하기

지원금 규정에 따라 교수진의 연구 자료가 미국 내에 머물어야만 합니다.”

지원금 규정

관리자는 **데이터 리전 정책**을 사용하여 특정 지리적 위치(미국 또는 유럽)에 교수진의 연구 자료를 저장할 수 있습니다.

- 데이터 리전 정책은 Google Workspace for Education 핵심 서비스 대부분의 기본 저장 데이터(백업 포함)에 적용됩니다. 목록은 여기에서 확인할 수 있습니다.
- 데이터가 있는 리전 외부의 사용자는 경우에 따라 지연 시간이 길어질 수 있으므로 데이터 리전 정책을 설정하기 전에 그에 따른 영향을 고려하는 것이 좋습니다.

단계별 방법

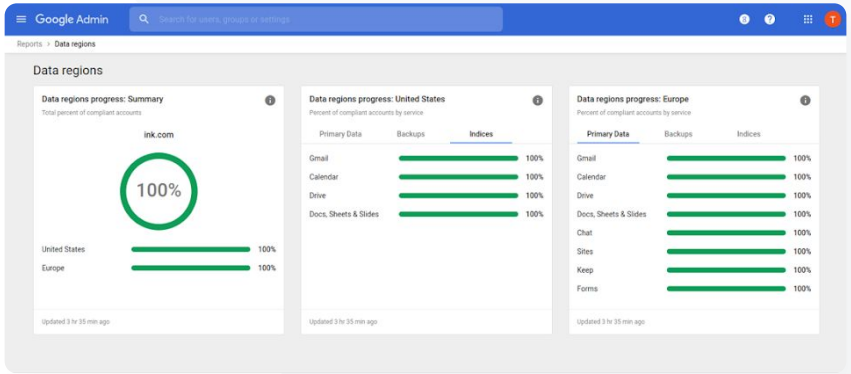
관련 고객센터 문서

- 데이터를 저장할 지리적 위치 선택하기

방법: 데이터 규정

데이터 리전을 정의하는 방법

- **관리 콘솔**에 로그인합니다.
  - 참고: 최고 관리자로 로그인해야 합니다.
- **회사 프로필** > **더보기** > **데이터 리전**을 클릭합니다.
- 리전을 제한할 **조직 단위** 또는 **구성 적용 그룹**을 선택하거나 전체 열을 선택하여 모든 단위와 그룹을 포함합니다.
- **선호하는 리전 없음, 미국, 유럽** 등으로 리전을 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- 데이터를 저장할 지리적 위치 선택하기

“제 담당 교육구 전반에서 정책을 관리하고 Chromebook뿐만 아니라 iOS, Windows 10 등 모든 유형의 기기에 푸시할 방법이 필요합니다. 특히 보안이 침해된 기기가 있다면 더욱 필요하죠.”

엔드포인트 기기 관리

엔터프라이즈 엔드포인트 관리를 사용하면 휴대기기를 통해 조직의 데이터를 더욱 세부적으로 제어할 수 있습니다. 휴대기기 기능을 제한하고, 기기 암호화를 요구하며, Android 기기와 iPhone 및 iPad 앱을 관리하고, 기기에서 데이터를 완전히 삭제할 수도 있습니다.

- 관리 콘솔에서 기기를 승인, 차단, 차단 해제, 삭제할 수 있습니다.
- 사용자가 기기를 분실하거나 학교에서 제적된 경우 특정 관리 모듈 기기에서 사용자의 계정, 프로필을 비롯한 모든 데이터를 삭제할 수 있습니다. 컴퓨터나 웹 브라우저에서는 이 데이터를 계속 사용할 수 있습니다.

단계별 방법

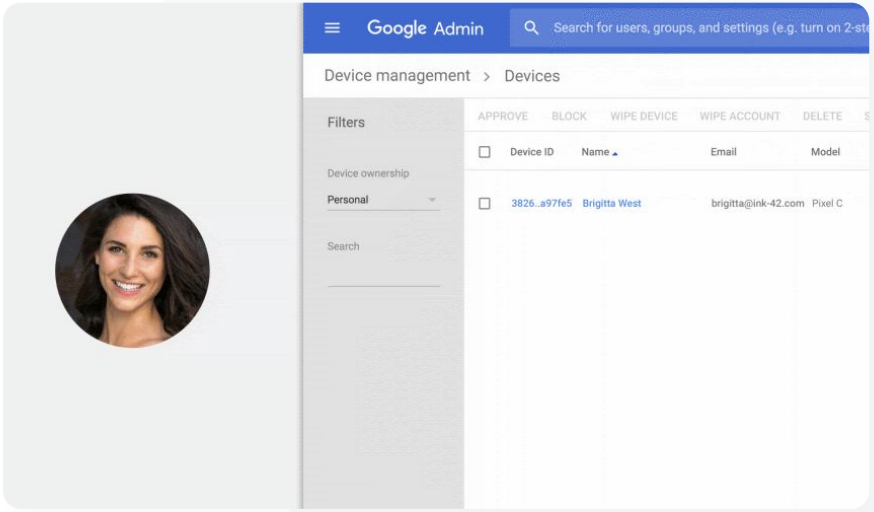
관련 고객센터 문서

- Google 엔드포인트 관리로 기기 관리하기
- 고급 모바일 관리 설정하기

방법: 엔드포인트 기기 관리

고급 모바일 관리를 사용 설정하는 방법

- **관리 콘솔**에 로그인합니다.
- **관리 콘솔** > **기기**로 이동합니다.
- 왼쪽에서 **설정** > **범용 설정**을 클릭합니다.
- **일반** > **모바일 관리**를 클릭합니다.
- 모든 사용자에게 설정을 적용하려면 최상위 조직 단위를 선택하고 그렇지 않으면 하위 조직 단위를 선택합니다.
- **고급**을 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- Google 엔드포인트 관리로 기기 관리하기
- 고급 모바일 관리 설정하기

Microsoft Windows 기기 관리

Android, iOS, Chrome 및 Jamboard 기기와 마찬가지로 관리 콘솔을 통해 기관의 Windows 10 기기를 관리 및 보호할 수 있습니다.

“일부 교육자가 Windows 10 기기를 사용합니다. 기관의 기기를 모두 한곳에서 관리하려면 어떻게 해야 하나요?”

- 사용자가 Windows 10 기기에서 Google Workspace에 더 쉽게 액세스할 수 있도록 싱글 사인온(SSO)을 사용 설정합니다.
- 관리 콘솔에서 기기를 관리하여 Google Workspace에 액세스하는 데 사용되는 기기가 업데이트되고, 안전하고, 규정 준수 표준에 부합하는지 확인합니다.
- 기기를 완전 삭제하고, 기기 구성 업데이트를 푸시하는 것을 비롯해 클라우드에서 Windows 10 기기에 대해 더 많은 작업을 할 수 있습니다.

단계별 방법

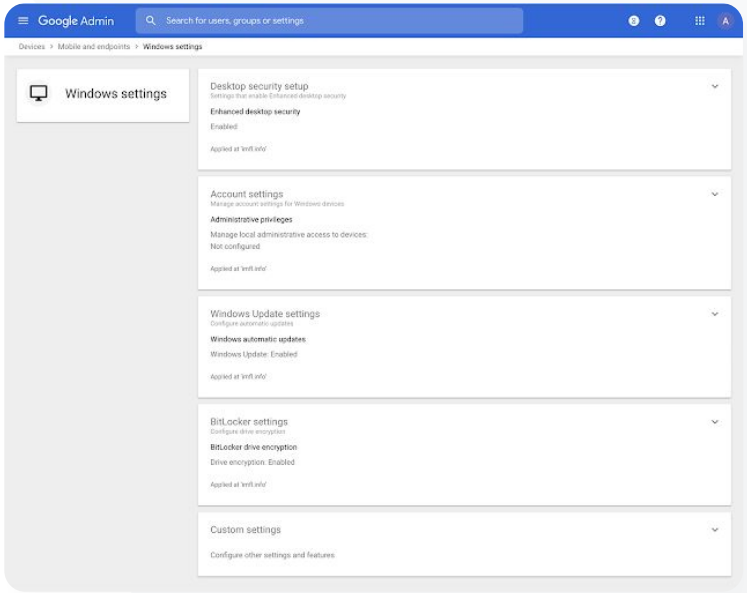
관련 고객센터 문서

- Windows 기기 관리 사용 설정하기
- Windows 기기 관리에 기기 등록하기

방법: Microsoft Windows 기기 관리

Windows 기기 관리 사용 설정하기

- **관리 콘솔**에서 **메뉴** > **기기** > **모바일 및 엔드포인트** > **설정** > **Windows 설정**으로 이동합니다.
- **Windows 관리 설정**을 선택합니다.
- 모든 사용자에게 설정을 적용하려면 최상위 조직 단위를 선택합니다.
- **Windows 기기 관리** 옆의 **사용 설정됨**을 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- Windows 기기 관리 사용 설정하기
- Windows 기기 관리에 기기 등록하기

“Windows 10 기기에 Wi-Fi 프로필을 설정하려면 어떻게 해야 하나요?”

Windows 10 기기 맞춤 설정

관리자는 Google의 Windows 기기 관리를 사용하여 조직의 기기에 맞춤 설정을 추가할 수 있습니다.

- 관리 콘솔에서 기기 맞춤 설정 제어
- 설정 적용 대상:
  - 기기 관리
  - 보안
  - 하드웨어 및 네트워크
  - 소프트웨어
  - 개인 정보 보호

단계별 방법

관련 고객센터 문서

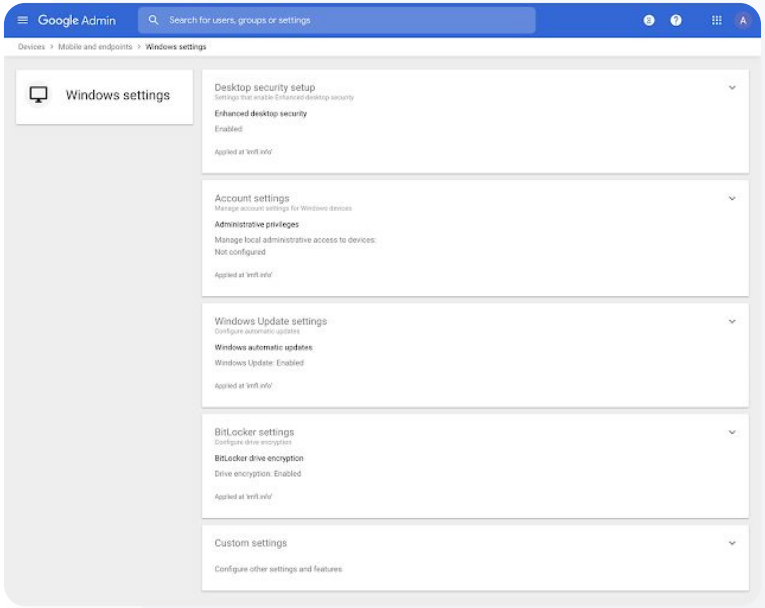
- 일반적인 맞춤 설정
- 맞춤 설정 추가

방법: Windows 10 기기 맞춤 설정

새 맞춤 설정 추가하기

- **관리 콘솔**에서 **메뉴** > **기기** > **모바일 및 엔드포인트** > **설정** > **Windows 설정**으로 이동합니다.
- **맞춤 설정**을 선택합니다.
- **맞춤 설정 추가**를 클릭하고 요청한 필드를 작성합니다.
- **다음**을 클릭합니다.
- 설정을 적용할 **조직 단위**를 선택합니다.
- **적용**을 클릭합니다.

참고: Google은 서드 파티 제품 또는 설정에 대한 기술 지원을 제공하거나 책임을 지지 않습니다.



관련 고객센터 문서

- 일반적인 맞춤 설정
- 맞춤 설정 추가

“조직의 Windows 10 기기가 최신 업데이트를 받도록 하고 싶습니다.”

Windows 10 기기 업데이트 자동화

기관의 Windows 10 기기에서 Windows 자동 업데이트 서비스를 통해 보안 업데이트와 기타 주요 다운로드를 수신할 방법과 시기를 지정할 수 있습니다.

- Windows Update 제어판에서 업데이트를 다운로드하도록 알림을 설정하고, 업데이트 재부팅이 예약되지 않는 시간을 설정하는 것을 비롯한 다양한 작업을 수행할 수 있습니다.
- 전체 기관 또는 특정한 조직 단위에 설정을 적용할 수 있습니다.
- 변경사항이 적용되는 데 최대 24시간이 소요될 수 있지만 일반적으로 더 빠르게 적용됩니다.

단계별 방법

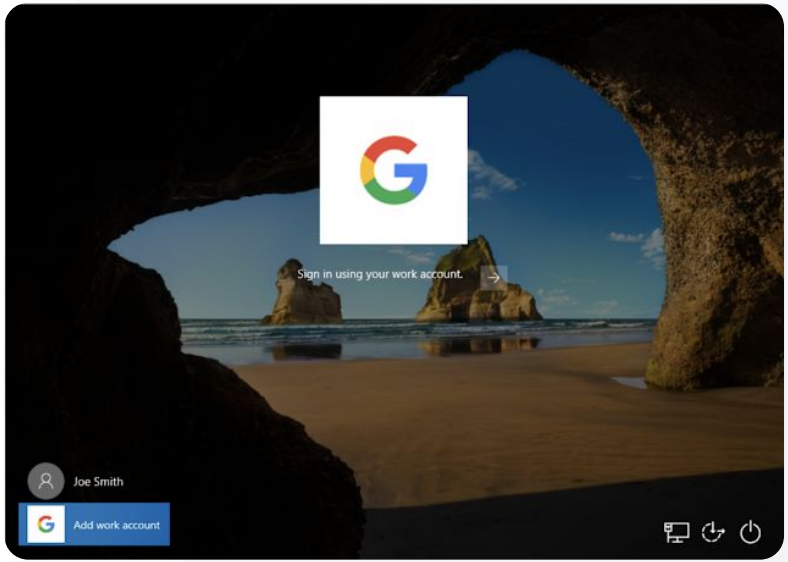
관련 고객센터 문서

- 자동 업데이트 관리

방법: Windows 10 기기 업데이트 자동화

업데이트 구성하기

- **관리 콘솔**에서 **메뉴** > **기기** > **모바일 및 엔드포인트** > **설정** > **Windows 설정**으로 이동합니다.
- **Windows 업데이트 설정** > **사용 설정됨**을 선택합니다.
- **Windows 기기 관리** 옆의 **사용 설정됨**을 선택합니다.
- 여러 옵션 중에서 아래의 옵션을 선택합니다.
  - Microsoft 애플리케이션의 업데이트 수락
  - 자동 업데이트 동작
  - 자동 업데이트 빈도
- **저장**을 클릭합니다.



관련 고객센터 문서

- 자동 업데이트 관리

클라이언트 측 암호화 활용

Google Workspace는 이미 최신 암호화 표준을 사용하여 저장 데이터 및 시설 간의 전송 중인 모든 데이터를 암호화하고 있습니다. **클라이언트 측 암호화**를 사용하면 관리자는 암호화 키와 암호화 키에 액세스하는 데 사용되는 ID 공급업체를 직접 제어할 수 있습니다.

- 자체 암호화 키를 사용하여 기관의 지식 재산과 같은 민감한 정보를 암호화할 수 있습니다.
- 데이터가 Google의 클라우드 기반 저장소로 전송되거나 저장되기 전에 브라우저에서 콘텐츠 암호화가 처리됩니다.
- 클라이언트 측에서 암호화된 콘텐츠를 만들고 내부 또는 외부에 공유할 수 있는 사용자를 선택할 수 있습니다.

> “Google이 가장 높은 데이터 암호화 기준을 가지고 있다는 것을 알고 있지만, 대학교의 지식 재산 및 지원금을 받는 연구에 대한 암호화 키를 직접 제어하고 싶습니다.”

단계별 방법

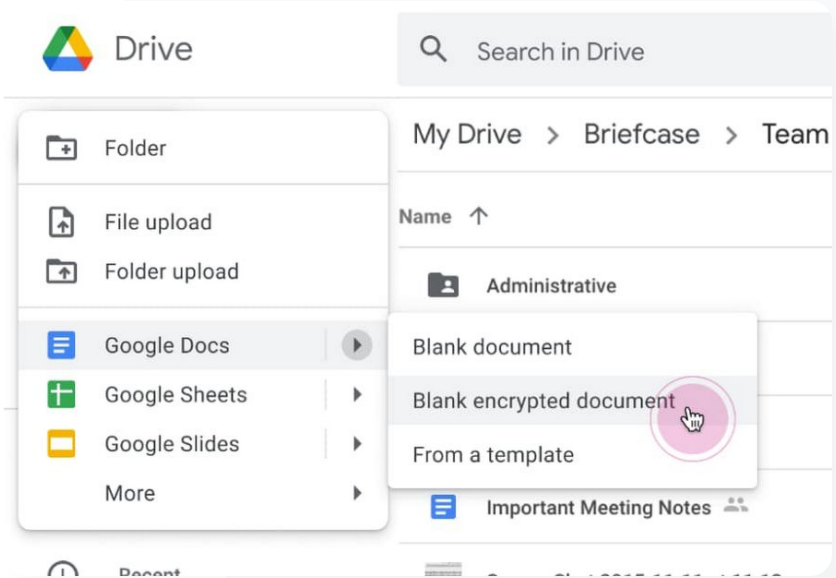
관련 고객센터 문서

- 클라이언트 측 암호화에 관한 정보

방법: 클라이언트 측 암호화 활용

클라이언트 측 암호화 (CSE) 설정하기

- 암호화 키 관리 서비스 설정
  - 키 관리 서비스를 만들어 키 관리 및 제어 기능으로 데이터를 보호합니다.
- Google Workspace를 외부 키 관리 서비스에 연결
  - 관리 콘솔에 키 관리 서비스 URL을 포함하여 클라이언트 측 암호화에 필요한 키 관리 서비스를 추가 및 관리합니다.
- 키 관리 서비스를 조직 단위 또는 그룹에 할당
  - 하나의 키 관리 서비스를 전체 기관의 기본 서비스로 할당합니다.
- Google Workspace를 IdP에 연결
  - 클라이언트 측 암호화에 필요한 ID 공급업체(IdP)에 연결하여 사용자가 콘텐츠를 암호화하거나 암호화된 콘텐츠에 액세스하도록 허용하기 전에 사용자의 ID를 확인합니다.
- 사용자에 대해 CSE 사용 설정
  - 클라이언트 측 암호화를 사용 설정하여 클라이언트 측 암호화가 적용된 콘텐츠를 만들어야 하는 사용자가 있는 조직 단위 또는 그룹을 허용합니다.

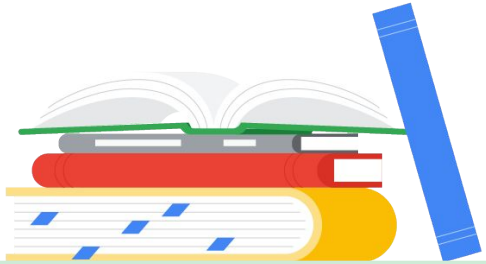


관련 고객센터 문서

- 클라이언트 측 암호화에 관한 정보

교육 및 학습 기능

개선된 수업 환경, 학습 윤리를 도모하는 도구, 향상된 동영상 커뮤니케이션을 갖춘 디지털 학습 환경에서 교사에게 추가 기능을 제공하세요.

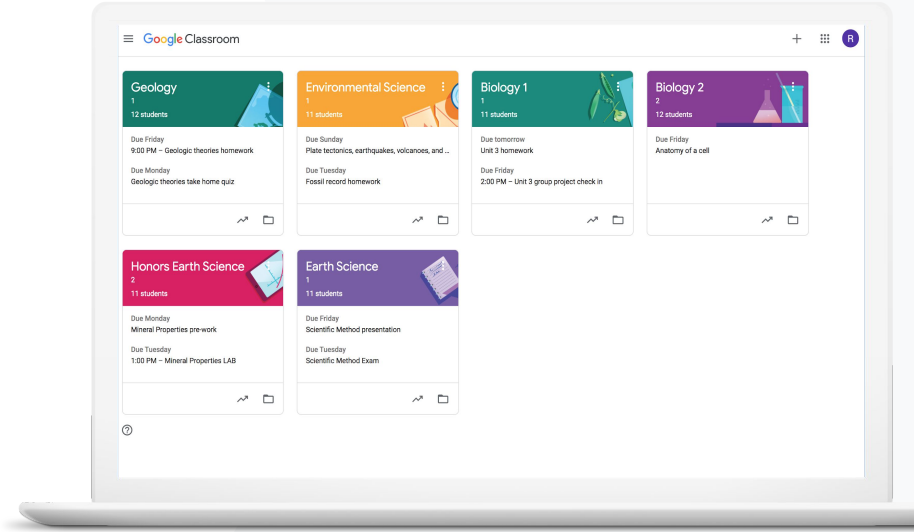


- Google 클래스룸
- 원본성 보고서
- Docs, Sheets, Slides
- Google Meet

Google Classroom

기본 개념

Google 클래스룸은 교육과 학습이 이루어지는 거점입니다. 클래스룸의 유료 기능은 클래스 도구를 한곳으로 모으는 데 도움이 됩니다. 교육자는 클래스룸에서 자주 사용하는 도구에 바로 액세스하고 수업 목록이 외부 시스템과 동기화되도록 유지할 수 있습니다.



사용 사례

클래스룸 부가기능 액세스 관리	단계별 방법
클래스룸에 흥미로운 콘텐츠 통합	단계별 방법
대규모로 클래스 생성	단계별 방법

“교육자가 자주 사용하는 에듀테크 도구에 대한 싱글 사인온(SSO) 액세스를 제공할 방법이 있으면 좋겠습니다.”

단계별 방법

관련 고객센터 문서

- Google Workspace Marketplace 앱 관리하기
- 클래스룸에서 부가기능 사용하기
- 허용 목록에 있는 Marketplace 앱 관리하기
- 사용자에게 Marketplace 앱 배포하기
- 클래스룸 부가기능 [관리자를 위한 시작 가이드]

클래스룸 부가기능 액세스 관리

도메인 허용 목록을 통해 기관에서 액세스할 수 있는 서드 파티 교육 앱을 지정합니다. 교육자가 몇 번의 클릭만으로 쉽게 부가기능을 설치하고 학생 과제에 포함할 수 있도록 합니다.

- 도메인 전반에서 허용 목록을 만들어 교육자가 Google Workspace Marketplace에서 설치 가능한 서드 파티 앱을 지정합니다.
- 보충 학습 앱을 통해 학습 결과를 지원합니다. 교육자는 Google Classroom 내에서 바로 과제를 내고, 검토하고, 채점할 수 있습니다.
- Google Workspace Marketplace에는 Adobe Creative Cloud Express, BookWidgets, CK-12, Formative, Genially, Google 아트 앤 컬처, IXL, Kahoot!, Nearpod, Newsela, Pear Deck, SAFARI Montage, Sora, Wordwall 등이 포함되어 있습니다.

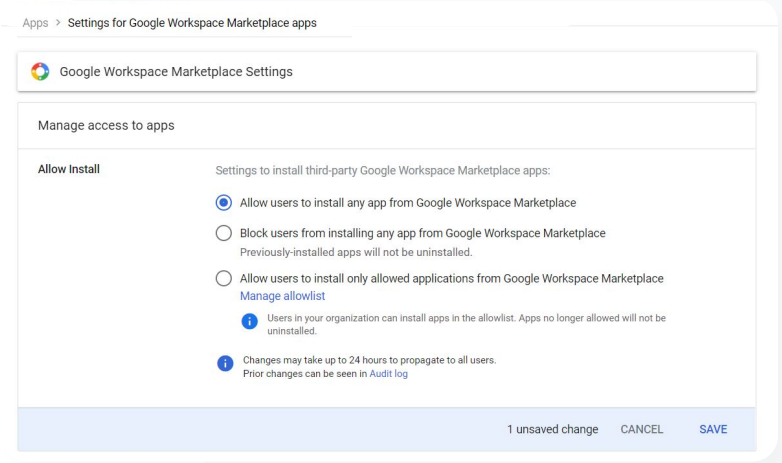
방법: 클래스룸 부가기능 액세스 관리

도메인 허용 목록으로 부가기능 액세스 관리

- 관리 콘솔에서 **메뉴** > **Google Workspace Marketplace 앱** > **앱 목록**을 선택합니다.
- **허용 목록 앱**을 선택합니다.
- 원하는 부가기능의 이름을 입력하거나 검색합니다.
- **선택**을 클릭하고 **사용자가 이 앱을 설치하도록 허용**이 선택되어 있는지 확인합니다.
- **계속** 및 **완료**를 클릭합니다.

원하는 허용 목록에 부가기능 액세스 권한 부여

- 관리 콘솔에서 **메뉴** > **Google Workspace Marketplace 앱** > **앱 목록**을 선택합니다.
- 배포하려는 부가기능을 클릭합니다.
- **사용자 액세스**에서 **조직 단위 및 그룹 보기**를 클릭합니다.
- **모든 사용자 이용 가능** 또는 **특정 그룹**이나 **조직 단위**로 액세스를 조정 중에서 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- Google Workspace Marketplace 앱 관리하기
- 클래스룸에서 부가기능 사용하기
- 허용 목록에 있는 Marketplace 앱 관리하기
- 사용자에게 Marketplace 앱 배포하기
- 클래스룸 부가기능 [관리자를 위한 시작 가이드]

“Google 클래스룸에서 나가지 않은 채 학생에게 Kahoot! 학습 게임을 과제로 내고 채점하고 싶습니다.”

클래스룸에 흥미로운 콘텐츠 통합

교육자는 **클래스룸 부가기능**을 통해 클래스룸 내에서 과제에 부가기능, 질문, 자료 또는 공지사항을 첨부하여 수업에서 흥미로운 활동과 콘텐츠를 공유할 수 있습니다.

- 교육자와 학생이 클래스룸을 나가지 않고도 Kahoot!, Nearpod, Pear Deck과 같이 좋아하는 도구를 사용할 수 있도록 지원할 수 있습니다.
- 부가기능을 사용하면 학생이 여러 개의 비밀번호를 관리하거나 외부 웹사이트로 이동하지 않아도 됩니다.
- 클래스룸 내에서 부가기능을 통해 학생 과제물을 바로 채점하고 검토할 수 있습니다.

단계별 방법

관련 고객센터 문서

- 클래스룸에서 부가기능 사용하기
- 클래스룸 부가기능 [교사를 위한 시작 가이드]

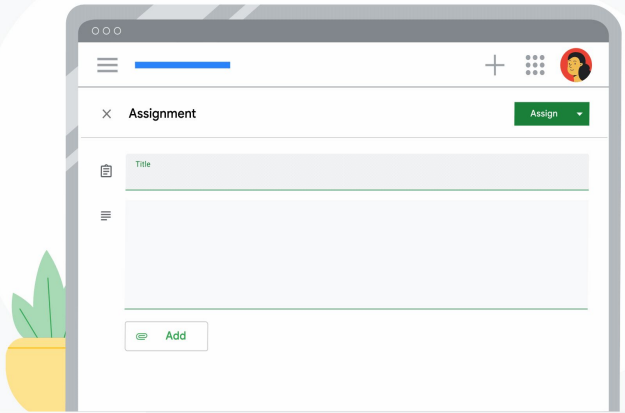
방법: 클래스룸에 흥미로운 콘텐츠 통합

과제, 퀴즈 또는 질문에 부가기능을 첨부하는 방법

- classroom.google.com에서 클래스룸 계정에 로그인합니다.
- 목록에서 관련 있는 수업을 선택한 다음 **수업 과제**를 선택합니다.
- **만들기**를 선택하고 > 만들려는 항목을 선택합니다.
- 제목과 설명을 입력합니다.
- **부가기능**에서 사용하려는 부가기능을 선택합니다.
- **할당**을 선택합니다.

공지사항에 부가기능을 첨부하는 방법

- 수업의 **스트림** 페이지에서 **학생에게 공지사항 게시**를 선택합니다.
- 공지사항을 입력합니다.
- **부가기능**에서 사용하려는 부가기능을 선택합니다.
- **게시**를 선택합니다



관련 고객센터 문서

- 클래스룸에서 부가기능 사용하기
- 클래스룸 부가기능 [교사를 위한 시작 가이드]

“Google 클래스룸에서 수업의 설정을 자동화하고 학생 출석부를 관리할 방법이 필요합니다.”

대규모로 클래스 생성

SIS 출석부 가져오기를 사용하면 자동으로 수업을 생성하고 Clever를 통해 수업 목록을 학교의 학생 정보 시스템(SIS)과 동기화되도록 유지할 수 있습니다.

- Education Plus를 사용하여 미국 및 캐나다의 K-12 교육구에서 이용할 수 있습니다.
- 관리자는 SIS에서 출석부를 Google 클래스룸으로 가져와 수업을 자동으로 설정할 수 있습니다.
- Google 클래스룸에서 원활하게 수업 목록을 자동화하고 관리합니다.

단계별 방법

관련 고객센터 문서

- SIS 출석부 가져오기 시작하기
- Clever를 통해 SIS 출석부 가져오기 설정하기

방법: 대규모로 클래스 생성

SIS 출석부 가져오기를 설정하는 방법

- Clever 내에서 Google 클래스룸 출석부 동기화를 설정합니다.
- Clever의 교육구 관리자 및 Google Workspace 최고 관리자의 경우 Clever의 단계별 안내를 따릅니다.

교육구에 Clever 계정이 없는 경우:

- Clever 계정을 만듭니다.

교육구에 Clever 계정이 있는 경우:

- Clever 대시보드 내에서 출석부 가져오기를 요청합니다.

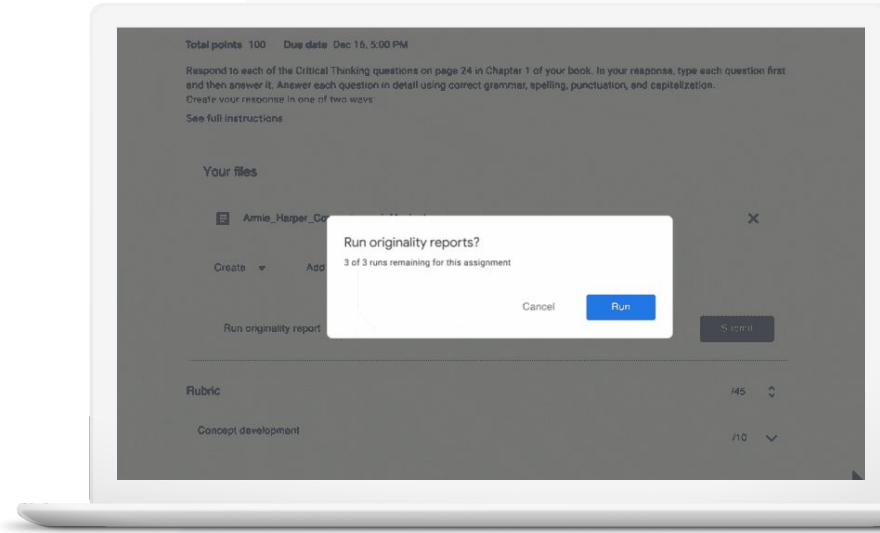
관련 고객센터 문서

- Clever를 통해 SIS 출석부 가져오기 설정하기

원본성 보고서

기본 개념

원본성 보고서를 사용하면 교육자와 학생은 Google 검색을 통해 학생의 과제물을 수십억 개의 웹페이지 및 4,000만 권 이상의 책과 비교하여 표절 여부를 확인할 수 있습니다. 원본성 보고서의 유료 기능은 교육자가 학생 과제물을 학교 소유 저장소에 있는 지난 학생 과제물과 비교할 수 있도록 무제한 액세스를 제공합니다.



사용 사례

표절 검사	단계별 방법
지난 학생 과제물과 비교해 원본성 확인	단계별 방법
표절 감지를 학습 기회로 활용	단계별 방법

“학생 과제물에 표절이나 부적절한 인용이 있는지 확인하고 싶습니다.”

표절 검사

교사는 **원본성 보고서**를 사용하여 학생 과제물의 진위성을 확인할 수 있습니다. 원본성 보고서는 감지된 출처를 링크로 표시하고 올바르게 인용되지 않은 텍스트를 알려줍니다.

- Docs, Slides 및 Microsoft Word 문서에 대해 원본성 보고서를 실행합니다.
- Teaching and Learning Upgrade 또는 Education Plus를 사용하는 교육자는 다음과 같은 기능을 이용할 수 있습니다.
  - 원본성 보고서에 대한 무제한 액세스
  - 학교 소유 저장소에 있는 이전에 제출한 과제물과 비교하여 다른 학생의 과제물과 일치하는 부분이 있는지 확인

데이터의 소유권은 항상 기관에 있지만, 안전한 비공개 보관은 Google이 책임집니다.

단계별 방법

관련 고객센터 문서

- 원본성 보고서 사용 설정하기
- 원본성 보고서 및 개인 정보 보호

방법: 표절 검사

클래스룸에서 원본성 보고서 사용 설정하기

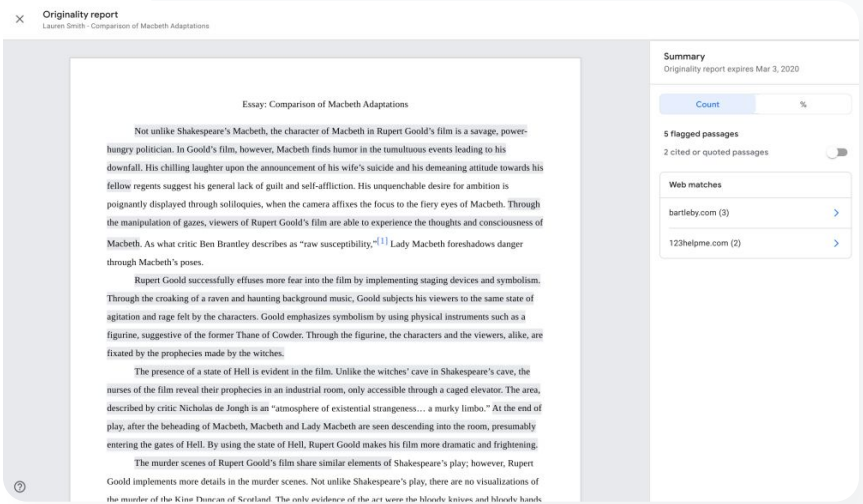
- **classroom.google.com**에서 클래스룸 계정에 로그인합니다.
- 목록에서 관련 있는 수업을 선택한 다음 **수업 과제**를 선택합니다.
- **만들기** > **과제**를 선택합니다.
- **원본성 보고서** 옆의 체크박스를 선택하여 사용 설정합니다.

학생 과제물에 원본성 보고서 실행하기

- 목록에서 해당 학생의 파일을 선택한 다음 클릭하여 평가 도구에서 파일을 엽니다.
- 학생의 과제에서 **원본성 확인**을 클릭합니다.

LMS에서 과제에 원본성 보고서 사용 설정하기

- **학습 관리 시스템**에 로그인합니다.
- 관련 있는 **과정**을 선택합니다.
- 과제를 만들고 > **Google 과제**를 선택합니다.
- **원본성 보고서 사용** 체크박스를 선택합니다.



관련 고객센터 문서

- 클래스룸: 원본성 보고서 사용 설정하기
- Google 과제: 원본성 보고서 사용 설정하기

“교사가 학생의 과제물을 과거에 제출된 학생 과제물과 비교해 표절 여부를 검사할 수 있도록 하려면 어떻게 해야 하나요?”

지난 학생 과제물과 비교해 원본성 확인

원본성 보고서의 **교내 일치 항목**을 사용하면 교육자가 기관의 비공개 저장소에 있는 학생 과제물을 바탕으로 검사하면서 학생 과제물을 이전 학생 과제물과 비교할 수 있습니다.

- Teaching and Learning Upgrade 또는 Education Plus를 통해 현재 및 이전 학생 과제물에 대해 다른 학생의 과제물과 일치하는 부분이 있는지 비교하여 표절 여부를 검사합니다.
- 학생 과제물은 도메인 전반의 학교 소유 비공개 저장소 내에 안전하게 보관 및 백필할 수 있습니다.

단계별 방법

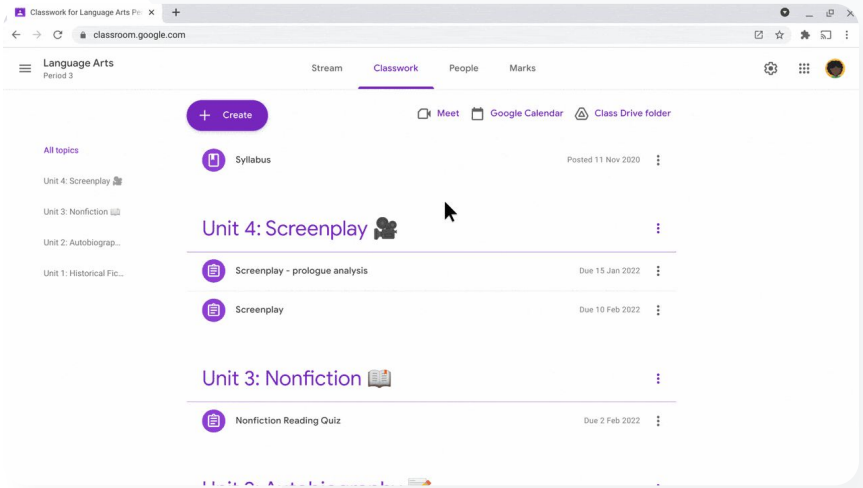
관련 고객센터 문서

- 원본성 보고서 사용 설정하기
- 클래스룸에서 원본성 보고서에 교내 일치 항목 사용 설정하기

방법: 지난 학생 과제물과 비교해 원본성 확인

원본성 보고서에 교내 일치 항목을 사용 설정하는 방법

- 관리 콘솔에서 **메뉴** > **앱** > **추가 Google 서비스** > **클래스룸**을 선택합니다.
- **교사 조직 단위**를 선택합니다.
- **원본성 보고서**를 클릭하고 **원본성 보고서 교내 일치 항목 사용** 체크박스를 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- 클래스룸에서 원본성 보고서에 교내 일치 항목 사용 설정하기

“학생들에게 출처를 올바르게 인용하는 방법에 대한 학습 기회를 제공하고 싶습니다.”

표절 감지를 학습 기회로 활용

학생들은 과제를 제출하기 전에 **원본성 보고서**를 과제당 최대 3번 실행함으로써 올바르게 인용되지 않은 콘텐츠와 의도치 않은 표절을 파악할 수 있습니다. 원본성 보고서는 학생의 과제물을 다양한 출처와 비교하고 올바르게 인용되지 않은 텍스트를 원본이 아닌 콘텐츠로 표시하여 학생들에게 교훈을 얻고, 실수를 바로잡으며, 떳떳하게 과제를 제출할 기회를 제공합니다.

- Teaching and Learning Upgrade 및 Education Plus에서는 교사가 원하는 만큼 원본성 보고서를 사용할 수 있지만 Education Fundamentals에서는 이 기능을 수업당 5번만 사용할 수 있습니다.
- 과제를 제출하면 클래스룸에서 교사만 볼 수 있는 보고서가 자동으로 실행됩니다. 과제물 제출을 취소한 다음 다시 제출할 경우 클래스룸에서 교사를 위해 원본성 보고서를 다시 실행합니다.

단계별 방법

관련 고객센터 문서

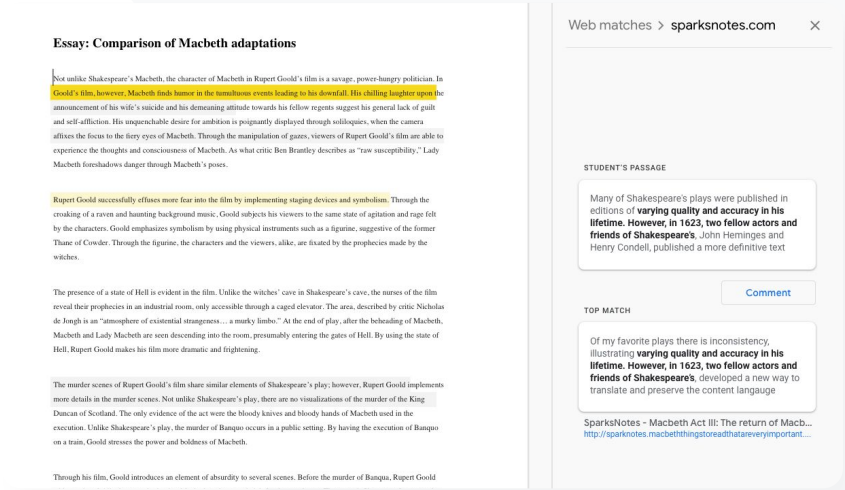
- 과제에 원본성 보고서 실행하기

방법: 표절 감지를 학습 기회로 활용

학생들이 클래스룸에서 원본성 보고서를 실행하는 방법

- classroom.google.com에서 클래스룸 계정에 로그인합니다.
- 목록에서 관련 있는 수업을 선택한 다음 **수업 과제**를 선택합니다.
- 목록에서 관련 있는 과제를 선택한 다음 **과제 보기**를 클릭합니다.
- **내 과제**에서 **파일을 업로드**하거나 **작성**합니다.
- **원본성 보고서** 옆에 있는 **실행**을 클릭합니다.
- 보고서를 열려면 과제 파일 이름 아래에서 **원본성 보고서 보기**를 클릭합니다.
- 과제를 수정하여 원본이 아닌 콘텐츠로 표시된 문구를 다시 작성하거나 올바르게 인용하려면 하단에서 **수정**을 클릭합니다.

학생은 Google 과제를 사용하여 LMS 내에서 원본성 보고서를 실행할 수 있습니다.



관련 고객센터 문서

- 클래스룸에서 원본성 보고서 실행하기
- LMS에서 원본성 보고서 실행하기

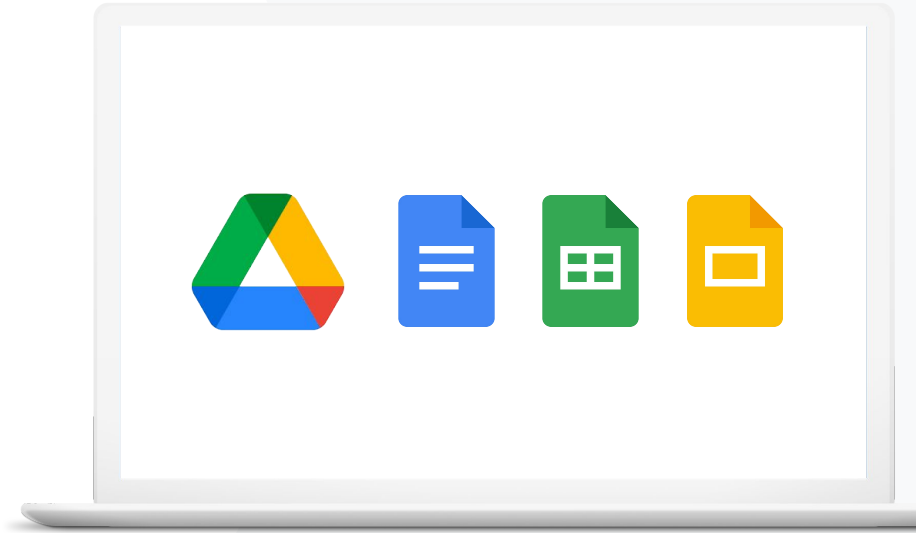
Docs, Sheets, Slides

기본 개념

학교 커뮤니티는 Docs, Sheets, Slides를 활용해 실시간으로 동시에 공동작업, 공동 생성, 검토 및 편집을 할 수 있습니다. Education Plus의 유료 기능을 사용하면 교육자와 관리자가 기관 전반에 내부 문서 승인 프로세스를 도입할 수 있습니다.

사용 사례

내부 문서 승인 단계별 방법



“

과학 부서에서 새 교육과정을 개발하고 있습니다.

어떻게 하면 모든 부서의 리더가 승인한 교육과정 제안서임을 확인할 수 있을까요?”

내부 문서 승인

승인 기능을 사용하면 학교 커뮤니티가 정식 승인 절차를 통해 Google Drive에서 문서를 전송할 수 있습니다.

- 검토자가 Drive, Docs 및 기타 Google Workspace 앱에서 직접 문서를 승인, 거부하거나 의견을 남길 수 있습니다.
- 승인 담당자는 문서의 링크를 따라가 문서를 검토하고 댓글을 남기거나 승인 또는 거부할 수 있습니다.
- 계약 또는 신규 고용에 대한 승인, 게시될 문서의 변경사항 승인 등을 관리할 수 있습니다.

단계별 방법

관련 고객센터 문서

- 승인 관리

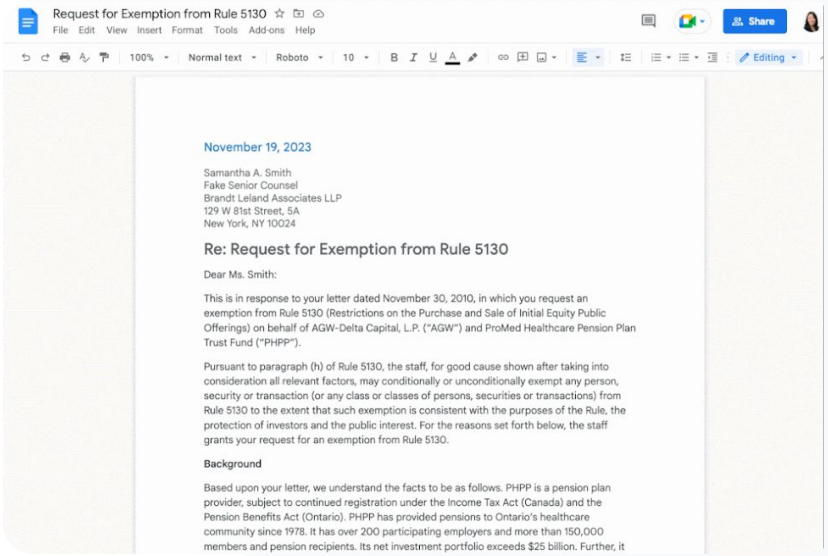
방법: 내부 문서 승인

작동 방식

관리자가 승인 프로세스에서 사용자 및 파일이 어떤 역할을 하는지 제어할 수 있습니다.

승인을 관리하는 방법

- **관리 콘솔**에 로그인하고 **메뉴** > **앱** > **Google Workspace** > **Drive 및 Docs**로 이동합니다.
- **승인**을 클릭합니다.
- 모든 사용자에게 설정을 적용하려면 하위 **조직 단위** 또는 **구성 그룹**을 선택합니다.
- **저장**을 클릭합니다.



관련 고객센터 문서

- 승인 관리

Google Meet

기본 개념

Google Meet의 고급 기능에는 실시간 스트리밍, 소그룹 채팅방, 대규모 회의, 회의 녹화, 실시간 번역 자막 등이 포함됩니다.

사용 사례

회의 녹화	단계별 방법	질문하기	단계별 방법
수업에서 논의한 내용 참조	단계별 방법	의견 수집	단계별 방법
언어 장벽 허물기	단계별 방법	소규모 학생 그룹	단계별 방법
모임 및 학교 행사 방송	단계별 방법	참석 관리	단계별 방법

> 기관에서 전문성 개발에 관한 대규모 온라인 수업을 제공하는데, 출석할 수 없는 교육자를 위해 수업을 녹화해야 합니다.”

회의 녹화

Teaching and Learning Upgrade 및 Education Plus에서는 교육자가 수업, 교수진 회의, 전문성 개발 교육 등을 녹화할 수 있습니다. 회의는 Drive에 자동으로 저장됩니다.

- 녹화 파일은 회의 주최자의 Drive에 저장됩니다. 녹화 전에 Drive에 충분한 공간이 있는지 확인하세요.
- IT 관리자는 교직원 대상으로만 녹화를 사용 설정하는 것이 좋습니다.

단계별 방법

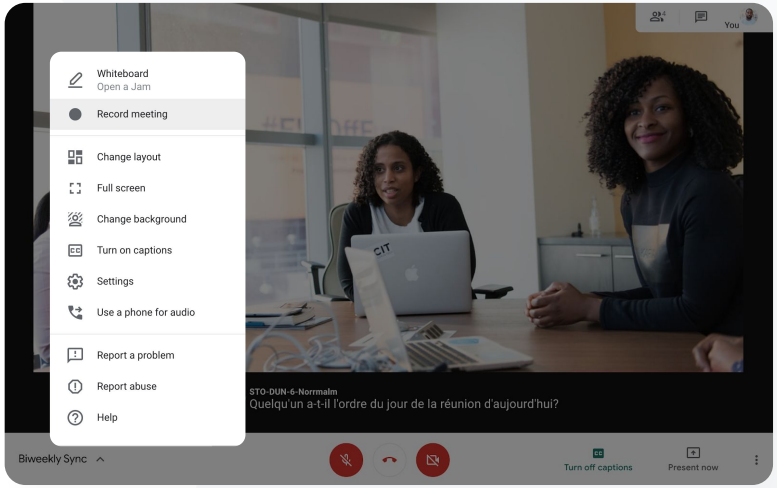
관련 고객센터 문서

- 화상 회의 녹화하기

방법: 회의 녹화

녹화를 시작하는 방법

- Google Meet에서 회의를 시작하거나 회의에 참여합니다.
- **활동** > **녹화**를 클릭합니다.
- **녹화 시작**을 선택합니다.
- 창이 열리면 **시작**을 클릭합니다.
- 화면의 오른쪽 하단에 회의가 녹화되고 있음을 나타내는 빨간색 점이 표시됩니다.
- 회의의 동영상 파일이 자동으로 Drive에 저장됩니다.



관련 고객센터 문서

- 화상 회의 녹화하기

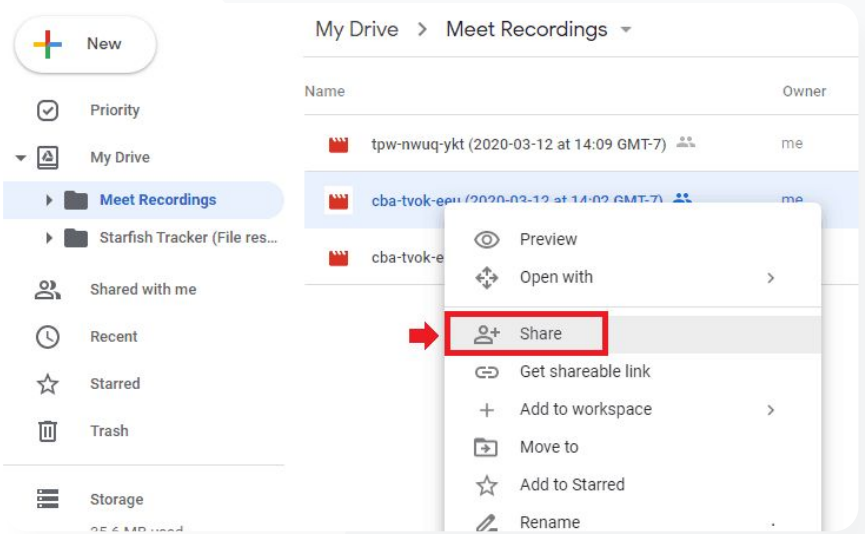
방법: 녹화 파일 시청 및 공유

녹화를 시작하는 방법

- 원하는 파일을 선택합니다.
- **공유** 아이콘을 선택합니다.
- 승인된 시청자를 **추가**합니다.

또는

- **링크** 아이콘을 선택합니다.
- 이메일 또는 채팅 메시지의 링크를 **붙여넣습니다.**



녹화 파일을 다운로드하는 방법

- 원하는 파일을 선택합니다.
- **더보기** 아이콘 > 다운로드를 클릭합니다.
- **더블클릭하면** 다운로드 가능한 파일이 재생됩니다.

Drive에서 녹화 파일을 재생하는 방법

- Drive에서 녹화 파일을 더블클릭하여 재생합니다. 온라인으로 볼 수 있도록 파일이 준비될 때까지 '아직 처리 중'이라는 메시지가 표시됩니다.
- 녹화 내용을 내 Drive에 추가하려면 파일을 선택하고 **내 드라이브에 추가**를 클릭합니다.

관련 고객센터 문서

- 화상 회의 녹화하기

“학생들이 나중에 개념을 검토할 수 있도록 온라인 수업 스크립트를 작성하려면 어떻게 해야 하나요?”

수업에서 논의한 내용 참조

교육자는 회의 스크립트를 통해 수업 및 수업 토론 내용을 자동으로 기록하여 학생들이 개념을 더 쉽게 되새기도록 할 수 있습니다. 스크립트는 회의 출석을 추적하고 회의에서 누가 어떤 말을 했는지 표시합니다.

- 컴퓨터 또는 노트북에서 Google Meet 사용자에게 영어로 제공됩니다.
- 관리자는 학교 커뮤니티에 대해 스크립트 작성 기능을 사용 설정할 수 있습니다.
- 스크립트는 회의 주최자의 Drive에 자동으로 저장됩니다.
- 회의 스크립트 작성 기능이 사용 설정되면 회의의 모든 사용자에게 왼쪽 상단에 스크립트 아이콘이 표시됩니다.
- 스크립트에는 회의에서 발언한 단어만 포함됩니다. 채팅 메시지의 스크립트를 받으려면 회의를 녹화하세요.

단계별 방법

관련 고객센터 문서

- Google Meet에서 스크립트 작성 기능 사용하기
- 스크립트 작성 사용 또는 사용 중지하기

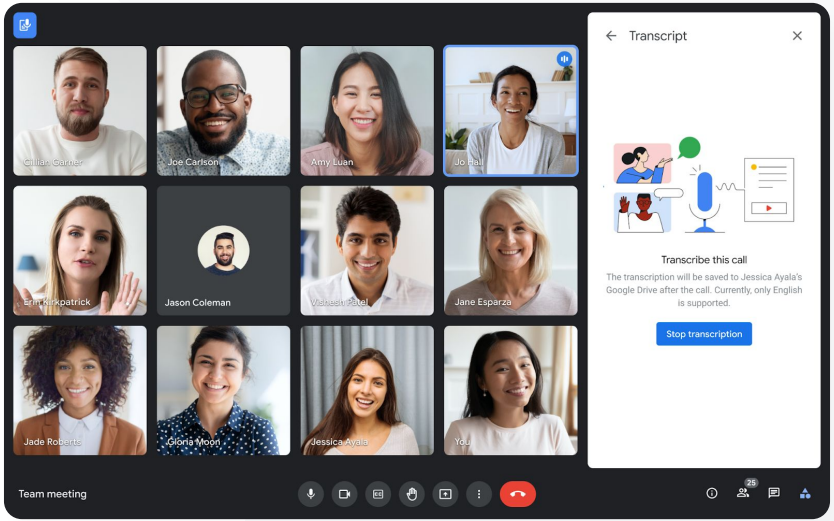
방법: 수업에서 논의한 내용 참조

Google Meet에서 스크립트 작성을 사용 설정하는 방법

- 회의 오른쪽 상단에서 **활동** 아이콘을 선택합니다.
- **스크립트** > **스크립트 시작** > **시작**을 클릭합니다.

Google Meet에서 스크립트 작성을 중지하는 방법

- **활동** 아이콘 > **스크립트** > **스크립트 중지** > **중지**를 선택합니다.



관련 고객센터 문서

- Google Meet에서 스크립트 작성 기능 사용하기
- 스크립트 작성 사용 또는 사용 중지하기

학부모 및 교사 회의를 온라인으로 주최해 오고 있는데, 서로 사용하는 언어가 다를 때가 있습니다.

어떻게 하면 회의의 포용성을 높이고 언어 장벽을 극복할 수 있나요?”

언어 장벽 허물기

번역된 자막을 사용하면 언어 숙련도에 따른 장벽을 허물어 회의의 포용성을 높일 수 있습니다. 회의 참석자가 원하는 언어로 콘텐츠를 사용하면 정보 공유, 학습 및 공동작업에 형평성을 더하는 데 도움이 됩니다.

- 교육자는 다른 언어를 사용하는 학생, 부모님 및 커뮤니티 이해관계자와 상호작용할 수 있습니다.
- 번역된 자막을 사용하여 영어를 프랑스어, 독일어, 포르투갈어 또는 스페인어로, 또는 그 반대로 번역합니다.
- 또는 영어를 일본어, 중국어 또는 스웨덴어로 번역할 수 있습니다.

단계별 방법

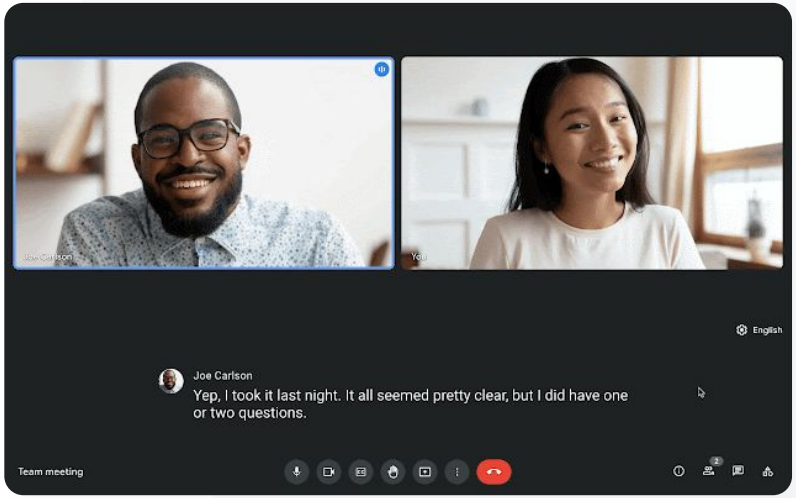
관련 고객센터 문서

- Google Meet에서 번역된 자막 사용하기

방법: 언어 장벽 허물기

번역된 자막을 사용 설정하는 방법

- 회의 중 화면 하단에서 옵션 더보기 > **설정** > **자막**을 클릭합니다.
- **자막**을 사용 설정합니다.
- **회의 언어**를 선택합니다.
- **번역된 자막**을 사용 설정합니다.
- **번역될 언어**를 선택합니다.



관련 고객센터 문서

- Google Meet에서 번역된 자막 사용하기

모임, 학교 행사 및 회의 방송

Teaching and Learning Upgrade의 경우 최대 1만 명의 시청자, Education Plus의 경우 최대 10만 명의 시청자를 대상으로 실시간 스트림을 진행할 수 있습니다. 이메일이나 Calendar 초대에서 주최자가 제공한 실시간 스트림 링크를 선택하면 참여 가능합니다.

- 실시간 스트림을 얼마나 광범위하게 공유할지 결정합니다. 스트림이 다음 중 어떤 것에 해당하도록 할지 선택합니다.
  - 조직의 사용자에게만 공개(조직 전용)
  - 신뢰할 수 있는 다른 Google Workspace 도메인과 공유
  - YouTube에서 시청 가능
- IT 관리자는 교직원 대상으로만 실시간 스트리밍을 사용 설정하는 것이 좋습니다.
- 실시간 스트림을 놓친 사용자는 회의가 완료된 후 다시보기를 이용할 수 있습니다.
- 실시간 스트림에 자막, 설문조사 및 Q&A를 추가해 포용성 및 참여도를 높일 수 있습니다.

> “교직원 회의를 광범위한 관계자와 학부모 그룹에 실시간 스트리밍할 수 있으면 좋겠습니다.”

단계별 방법

관련 고객센터 문서

- Meet에서 실시간 스트리밍 사용 설정/중지하기
- 화상 회의 실시간 스트리밍하기

방법: 모임, 학교 행사 및 회의 방송

실시간 스트림 이벤트를 만드는 방법

- Google Calendar를 엽니다.
- **+ 만들기** > **옵션 더보기**를 선택합니다.
- 날짜, 시간, 설명과 같은 일정 세부정보를 추가합니다.
- 화상 회의에 전체 권한으로 참여할 수 있는 참석자를 추가합니다. 해당 참석자는 회의 화면에 자신의 모습이 표시되고 음성이 들리며 화면을 발표할 수 있습니다.
- **Google Meet 참여 추가** > **Meet**을 클릭합니다.
- Google Meet 참여 옆에서 **아래쪽 화살표**를 선택한 다음 **실시간 스트림 추가**를 선택합니다.
- 사용자를 유료 버전에서 허용하는 최대한도로 초대하려면 실시간 스트림 URL을 **복사하고** 공유합니다.
- **저장**을 선택합니다.
- 스트리밍은 자동으로 시작되지 않습니다. 회의 중에 **더보기** > **스트리밍 시작**을 선택합니다.

관련 고객센터 문서

- Meet에서 실시간 스트리밍 사용 설정/중지하기
- 화상 회의 실시간 스트리밍하기

“질문을 던지고, 학생들의 지식 수준을 파악하고, 참여를 계속해서 유도할 수 있도록 상호작용할 간단한 방법이 필요합니다.”

질문하기

Google Meet의 **Q&A** 기능을 사용하여 학생들의 지속적인 참여를 유도하고 상호작용이 활발한 수업을 진행할 수 있습니다. 교육자는 온라인 수업이 끝날 때 모든 질문과 답변에 대한 자세한 보고서를 받을 수도 있습니다.

- 회의 진행자는 필요한 만큼 질문할 수 있습니다. 질문을 필터링하거나 정렬하고, 답변된 것으로 표시하고, 질문을 숨기거나 우선순위를 지정할 수도 있습니다.
- 질문 기능이 사용 설정된 회의가 끝나면 회의 진행자에게 질문 보고서가 이메일로 자동 전송됩니다.

단계별 방법

관련 고객센터 문서

- Google Meet에서 참석자에게 질문하기

방법: 질문하기

질문하기

- 오른쪽 상단 모서리에 있는 회의에서 **활동 아이콘** > **질문**을 선택합니다(Q&A를 사용 설정하려면 **Q&A 사용 설정** 선택).
- 질문을 하려면, 오른쪽 하단에서 **질문하기**를 클릭합니다.
- **질문을 입력**하고 > **게시**를 선택합니다.

질문 보고서 보기

- 회의가 끝나면 회의 진행자에게 **질문 보고서가 이메일로 전송됩니다.**
- 이메일을 연 다음 > **보고서 첨부파일**을 클릭합니다.

관련 고객센터 문서

- Google Meet에서 참석자에게 질문하기

“수업이나 교직원 회의를 진행할 때 학생과 다른 교육자들의 의견을 수집할 수 있는 간단한 방법이 있으면 좋겠습니다.”

의견 수집

온라인 회의를 예약하거나 시작한 사용자는 회의 참석자를 대상으로 **설문조사**를 실시할 수 있습니다. 이는 빠르고 참여도 높은 방식으로 회의에 참가한 모든 학생 또는 참석자로부터 정보를 얻을 수 있는 방법입니다.

- 회의 진행자는 설문조사를 저장해 두고 회의 진행 중에 표시되도록 할 수 있습니다. 온라인 회의 내의 설문조사 섹션 아래에 저장되어 편리하게 이용할 수 있습니다.
- 회의가 끝나면 설문조사 결과에 대한 이메일 보고서가 회의 진행자에게 자동으로 전송됩니다.

단계별 방법

관련 고객센터 문서

- Google Meet에서 설문조사 진행하기

방법: 의견 수집

설문조사 만들기

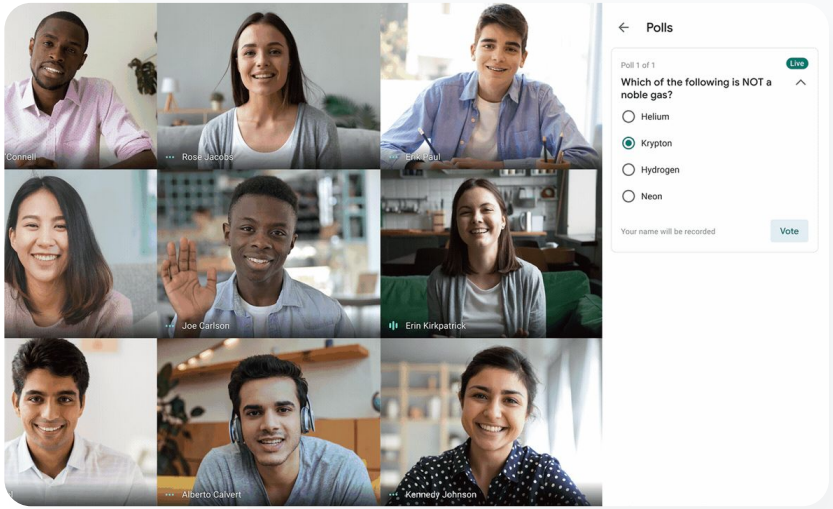
- 회의 오른쪽 상단에서 **활동 아이콘** > **설문조사**를 선택합니다.
- **설문조사 시작**을 선택합니다.
- 질문을 입력합니다.
- **실행** 또는 **저장**을 선택합니다.

설문조사 검토하기

- 회의 오른쪽 상단에서 **활동 아이콘** > **설문조사**를 선택합니다.
- 참석자가 설문조사 결과를 실시간으로 볼 수 있도록 하려면 **모두에게 결과 표시** 옆의 스위치를 클릭하여 **켬**으로 전환합니다.
- 설문조사를 닫고 더 이상 응답을 받지 않으려면 **설문조사 종료**를 클릭합니다.
- 설문조사를 영구적으로 삭제하려면 **삭제 아이콘**을 선택합니다.

설문조사 보고서 보기

- 회의가 끝나면 회의 진행자에게 **보고서가 이메일로 전송됩니다.**
- 이메일을 연 다음 > **보고서 첨부파일**을 선택합니다.



관련 고객센터 문서

- Google Meet에서 설문조사 진행하기

“가끔 학생들이 집에서 학습할 때가 있습니다. 소규모 그룹 활동을 할 때 사전 정의된 그룹을 기반으로 쉽게 소그룹 채팅방을 만들 방법이 필요합니다.”

소규모 학생 그룹

교육자는 소그룹 채팅방을 사용하여 온라인, **하이브리드 또는 오프라인 학습** 중에 학생들을 소그룹으로 나눌 수 있습니다. 소그룹 채팅방은 컴퓨터에서 영상 통화가 진행되는 중에 회의 진행자가 시작해야 합니다.

- 소그룹 채팅방은 이벤트를 생성하면서 미리 만들거나 회의 진행 중에 만들 수 있습니다.
- 온라인 회의당 최대 100개의 소규모 채팅방을 만들 수 있습니다.
- 교사는 여러 소그룹 채팅방 사이를 손쉽게 이동하여 필요할 때 도움을 줄 수 있습니다.
- 관리자는 소그룹 채팅방을 만들 수 있는 권한을 교사 또는 교직원으로 제한할 수 있습니다.

단계별 방법

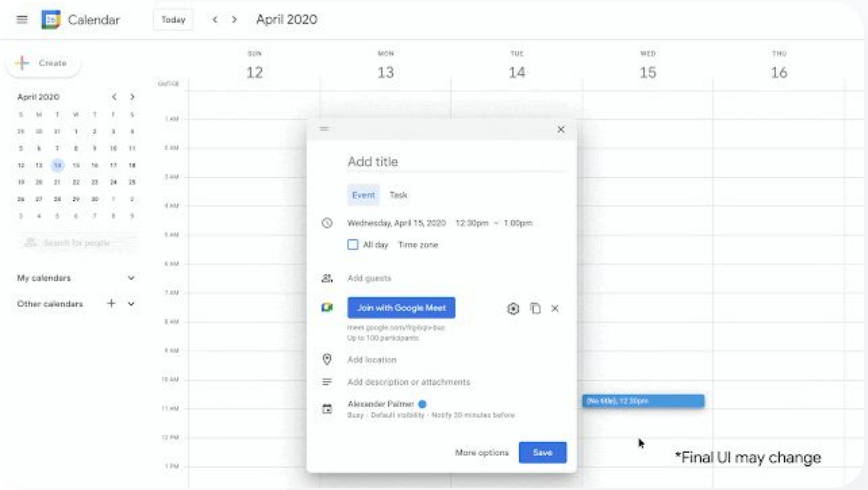
관련 고객센터 문서

- Google Meet에서 소그룹 채팅방 사용하기

방법: 소규모 학생 그룹 만들기

회의 전에 소그룹 채팅방 만들기

- 새 Google Calendar 일정을 만듭니다.
- **Google Meet 화상 회의 추가**를 클릭합니다.
- 참석자를 추가하고 > **회의 설정 변경**을 선택합니다.
- **소그룹 채팅방**을 클릭합니다.
- 소그룹 채팅방 수를 선택하고 다음 중 하나를 선택합니다.
  - 참석자를 다른 채팅방으로 드래그합니다.
  - 채팅방에 직접 이름을 입력합니다.
  - **무작위로 섞기**를 클릭하여 그룹을 혼합합니다.
- **저장**을 클릭합니다.



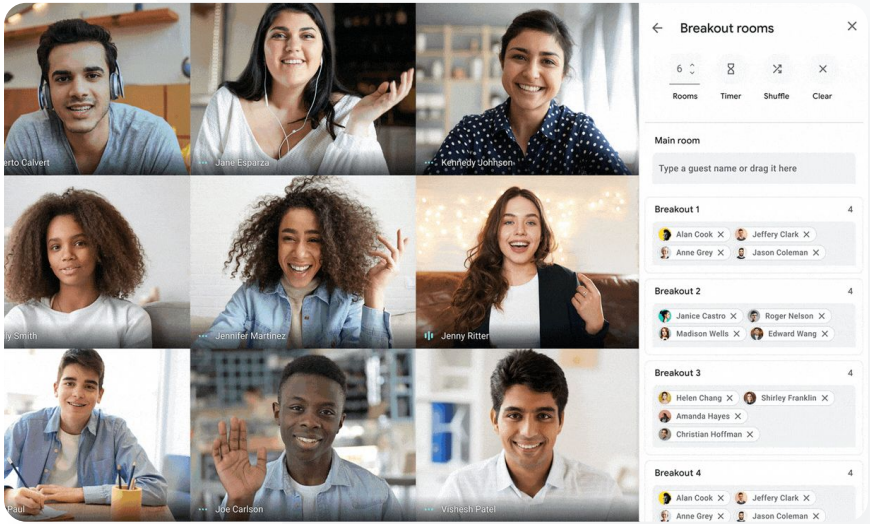
관련 고객센터 문서

- Google Meet에서 소그룹 채팅방 사용하기

방법: 소규모 학생 그룹 만들기

회의 중에 소그룹 채팅방 만들기

- 영상 통화를 시작합니다.
- 오른쪽 하단에서 **활동 아이콘** > **소그룹 채팅방**을 선택합니다.
- 소그룹 채팅방 생성 패널에서 **소그룹 채팅방 수**를 필요한 만큼 선택합니다.
- 학생들이 여러 채팅방으로 배정됩니다. 필요한 경우 회의 진행자가 수동으로 다른 채팅방으로 이동시킬 수 있습니다.
- 오른쪽 하단에서 채팅방 **열기**를 클릭합니다.



여러 소그룹 채팅방에서 질문에 답하기

- 참석자가 도움을 요청하면 회의 진행자의 화면 하단에 알림이 표시됩니다. 참여를 선택하여 해당 참석자의 소그룹 채팅방에 참여합니다.

관련 고객센터 문서

- Google Meet에서 소그룹 채팅방 사용하기

“온라인 수업 참석자를 확인하는 데 어려움을 겪고 있습니다. 도메인 전반에서 수업 참석을 쉽게 보고할 방법이 필요합니다.”

참석 관리

참석 관리를 사용하면 참석자가 5명 이상인 모든 회의에 대해 참석 보고서가 자동으로 제공됩니다. 보고서에는 수업 참석자의 이름, 참석자의 이메일, 온라인 수업에 참여한 시간이 표시됩니다.

- 실시간 스트림 보고서를 사용하여 실시간 스트림 이벤트 중에도 참석을 관리할 수 있습니다.
- 회의 진행자는 회의 내에서 또는 Calendar 일정에서 참석 관리 및 실시간 스트림 보고서를 사용 설정하거나 사용 중지할 수 있습니다.

단계별 방법

관련 고객센터 문서

- Google Meet에서 참석 확인하기

방법: 참석 관리

회의 중에 참석을 관리하는 방법

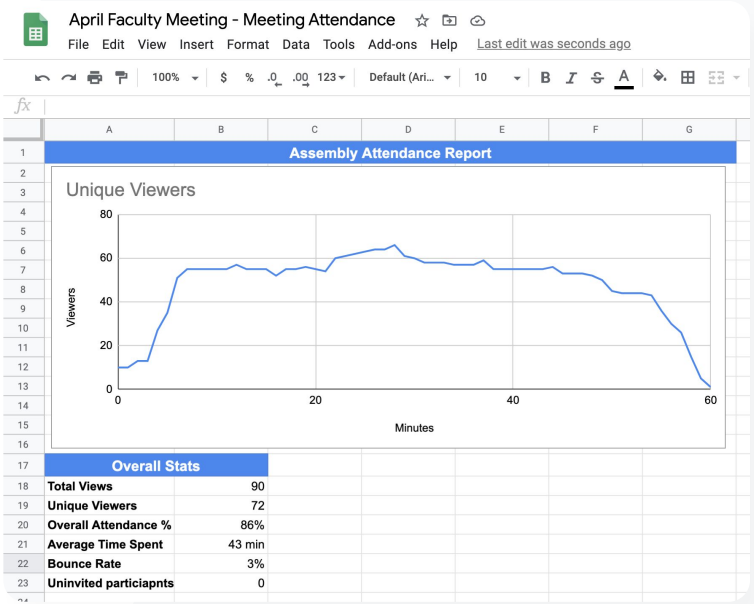
- 영상 통화를 시작합니다.
- 하단에서 **메뉴 아이콘**을 선택합니다.
- **설정 아이콘** > **주최자 제어**를 선택합니다.
- **참석 관리**를 사용 설정 또는 사용 중지합니다.

Calendar에서 참석을 관리하는 방법

- Calendar 일정에서 **Google Meet 화상 회의 추가**를 클릭합니다.
- 오른쪽에서 **회의 설정 변경 아이콘**을 클릭합니다.
- **참석 관리** 옆의 체크박스를 선택하고 > **저장**을 클릭합니다.

참석 보고서 받기

- 회의가 끝나면 회의 진행자에게 **보고서가 이메일로 전송됩니다.**
- 이메일을 연 다음 보고서 **첨부파일**을 선택합니다.



관련 고객센터 문서

- Google Meet에서 참석 확인하기

감사합니다