

Google for Education

運用 Google Workspace for Education 付費版本 的 40 多種方法

goo.gle/use-edu-workspace



簡報使用方式

本簡報精選出多種 Google Workspace for Education 付費版最熱門的用途。這些工具能提升資料安全性、教學成效、學生參與度和全校性協同合作，還有許多其他功能。

這份簡報會依序介紹產品功能、常見用途，以及簡易的功能使用操作說明。請查看整份簡報，瞭解 Google Workspace for Education 付費版可提供哪些功能。

Google Workspace for Education 付費版

Google Workspace for Education 的三種付費版本能為貴機構提供更多選擇、
掌控權和使用彈性。



Google Workspace for Education Plus

包含 Education Standard、Teaching and Learning Upgrade 及更多 Education Plus 專屬功能。



Education Plus 是一套**全方位**的教育科技解決方案，提供多項簡單好用的工具，讓學生、老師、教學主管和 管理員能**善用進階安全性功能和洞察資訊，並充實教學與學習體驗。**



Google Workspace for Education Standard

進階安全性與深入分析工具 讓你能進一步瞭解與掌控整個學習環境，進而降低風險及削弱威脅。



Teaching and Learning Upgrade

強化的教學與學習工具 可提供更符合個人需求的學習體驗、提升課堂教學效率，並讓所有人隨時隨地教學與學習，有助教學成效更上一層樓。

目錄



進階安全性與深入分析功能

安全性資訊主頁

- 垃圾郵件量
- 對外共用檔案
- 第三方應用程式
- 網路詐騙

安全性狀態頁面

- 安全性最佳做法
- 針對風險區域的建議做法

調查工具

- 分享不當內容
- 不小心共用檔案
- 網路詐騙和惡意軟體電子郵件
- 阻止不肖人士
- 更深入的安全性分析資訊
- 禁止不受監督的會議

網域管理與控管

- 掃描 Gmail 附件找出潛在威脅
- 建立使用情形資訊主頁及報表
- 尋找檔案更輕鬆
- 整理內部文件
- 自動填入部門群組
- 建立對內共用檔案目標對象
- 限制共用檔案對象
- Workspace 應用程式限制
- 管理儲存空間
- 資料法規
- 授權相關法規
- 管理端點裝置
- 管理 Windows 裝置
- Windows 裝置的自訂設定
- 自動更新 Windows 裝置
- 善用用戶端加密功能

目錄



強化的教學與學習功能

Google Classroom

- 管理 Classroom 外掛程式存取權限
- 在 Classroom 中結合引人入勝的內容
- 大規模建立課程

原創性報告

- 透過原創性報告功能偵測抄襲內容
- 根據學生過往繳交的作業檢查原創性
- 將抄襲偵測功能變成學習機會

文件、試算表和簡報

- 核准內部文件

Google Meet

- 錄製會議過程
- 參考課堂討論內容
- 克服語言隔閡
- 播送大型集會和學校活動
- 提出問題
- 收集意見
- 學生小組
- 追蹤出席狀況



進階安全性與深入分析 功能

透過主動式安全性工具抵禦威脅、分析安全性事件，並保護學生與教職員資料，進一步控管貴機構網域。



[安全性資訊主頁](#)



[安全性狀態頁面](#)



[調查工具](#)



[網域管理與控管](#)



安全性資訊主頁

這是什麼？

使用安全性資訊主頁即可查看各項安全性報告總覽。根據預設，每個安全性報告面板都會顯示最近 7 天的資料。您可以為資訊主頁自訂顯示的資料時間範圍，例如「今天」、「昨天」、「本週」、「上週」、「本月」、「上個月」或「幾天前」（最多 180 天）。

用途

垃圾郵件量



[逐步操作說明](#)

對外共用檔案



[逐步操作說明](#)

第三方應用程式

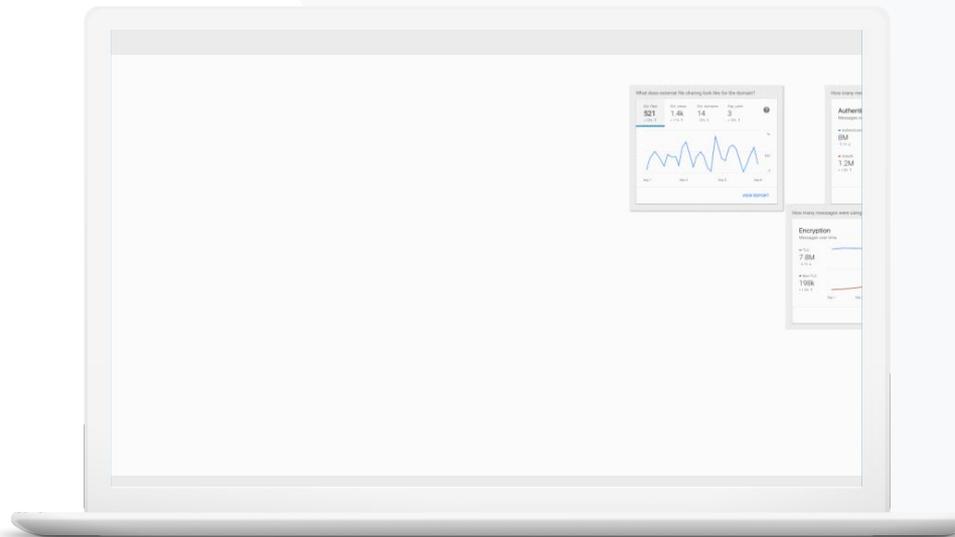


[逐步操作說明](#)

網路詐騙



[逐步操作說明](#)





「我想控管過多且不必要的電子郵件，並減少學校受到的安全性威脅。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [關於安全性資訊主頁](#)

垃圾郵件量

安全性資訊主頁以圖表方式呈現 Google Workspace for Education 環境中各項活動狀態，包括：

- ✓ 垃圾內容
- ✓ 可疑附件
- ✓ 網路詐騙
- ✓ 以及其他活動
- ✓ 惡意軟體

操作說明：資訊主頁總覽

如何查看安全性資訊主頁

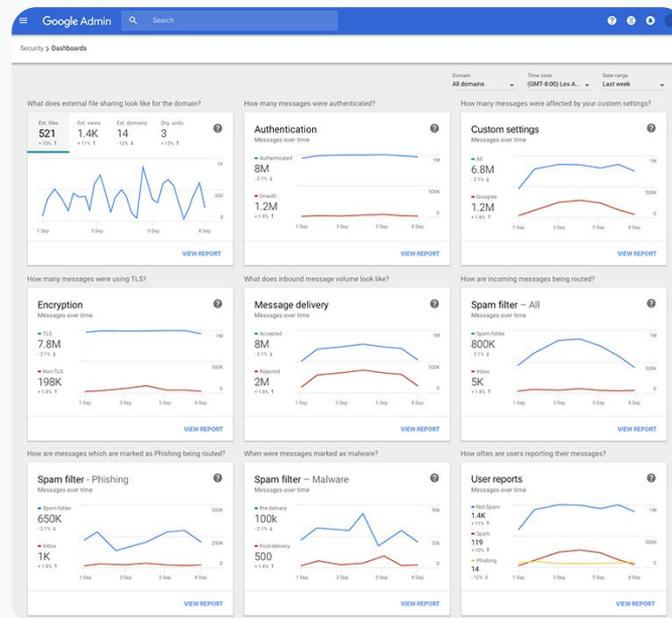
- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 您可透過安全性資訊主頁深入瞭解資料、將資料匯出至試算表或第三方工具，或是在調查工具中展開調查



安全性資訊主頁



安全性與深入分析工具



[說明中心相關文件](#)

- [關於安全性資訊主頁](#)



「我想查看檔案對外共用的活動，防止機密資料外洩至第三方。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [開始使用「安全性狀態」頁面](#)

對外共用檔案

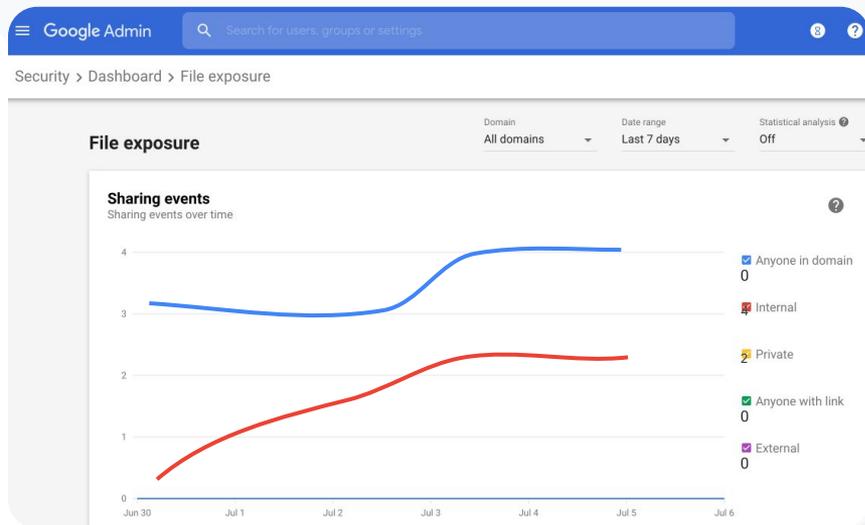
使用安全性資訊主頁中的檔案公開報告，即可查看貴機構網域中的對外共用檔案指標，包括：

-  在特定時間範圍內，與外部使用者共用檔案的事件次數。
-  在特定時間範圍內，對外共用檔案被檢視的次數。

操作說明：對外共用檔案

如何查看檔案公開報告

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 在命名為「這個網域的外部檔案共用狀態為何？」的資訊面板中，點選右下角的「查看報告」



[說明中心相關文件](#)

- [關於安全性資訊主頁](#)
- [檔案公開報告](#)



「我想查看有哪些第三方應用程式能存取我網域中的資料。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [OAuth 授權活動報告](#)

第三方應用程式

使用安全性資訊主頁中的 OAuth 授權活動報告，即可監控連結至貴機構網域的第三方應用程式，以及這些應用程式可存取的資料。



OAuth 可在不揭露使用者密碼的情況下，授權第三方服務存取使用者的帳戶資訊，方便您針對特定第三方應用程式，限制相關存取權。

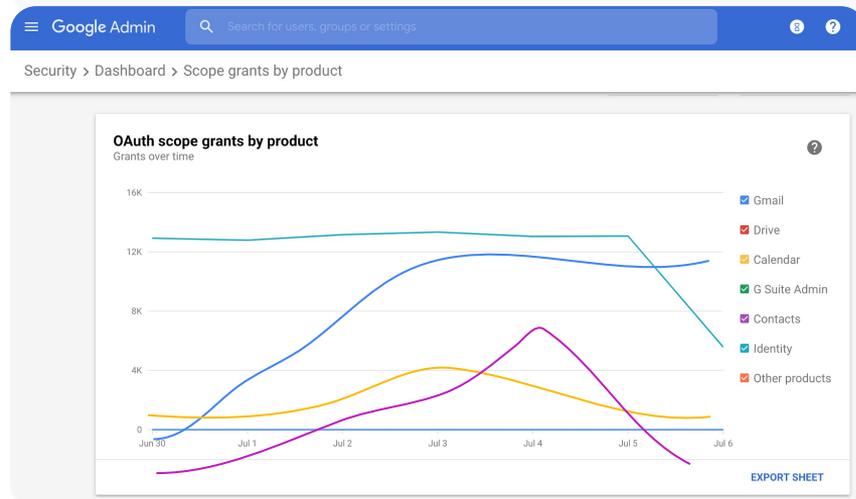


使用 OAuth 授權活動面板並根據應用程式、範圍或使用者來監控授權活動，並更新授予權限。

操作說明：第三方應用程式

如何查看「OAuth 授權活動」報告：

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 按一下底部的「查看報告」
- 您可根據產品（應用程式）、範圍或使用者查看 OAuth 授權活動
- 如要篩選資訊，請點選「應用程式」、「範圍」，或「使用者」
- 如要根據這份報告產生試算表，請點選「匯出試算表」



[🔗 說明中心相關文件](#)

- [OAuth 授權活動報告](#)



「有使用者回報收到網路詐騙電子郵件。
我想追蹤他們收到這封郵件的時間、郵件的性質，以及使用者會面臨的風險。」

[🔗 逐步操作說明](#)

[🔗 說明中心相關文件](#)

- [使用者如何標示電子郵件](#)
- [使用者回報](#)

網路詐騙

使用安全性資訊主頁中的「使用者回報」面板，即可查看在特定時間範圍內被標記為網路詐騙或垃圾郵件的電子郵件。您可查看被標記為網路詐騙的電子郵件資訊，例如收件者與開啟情形。



使用者回報可讓您查看使用者在特定的時間範圍內標示郵件 (垃圾郵件、非垃圾郵件或網路詐騙郵件) 的情況。

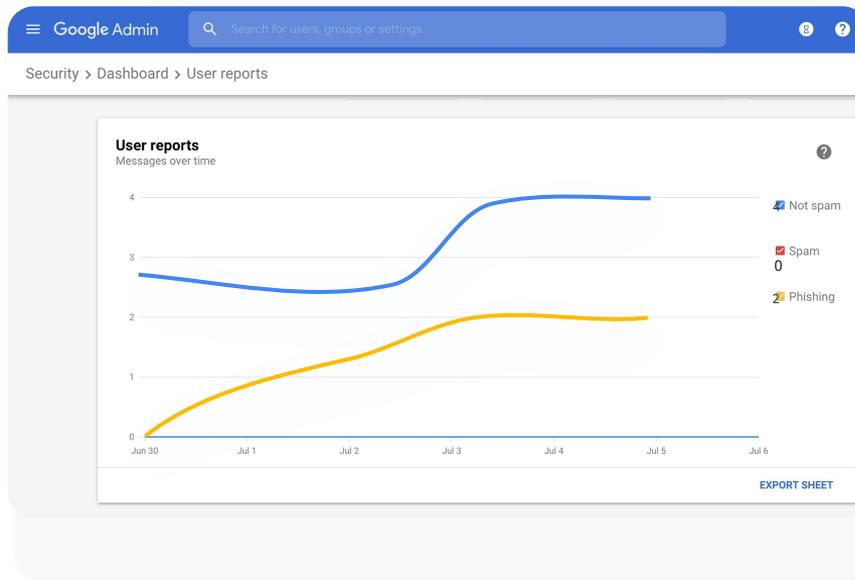


您可以自訂圖表，以便查看特定電子郵件類型的詳細資料，例如由內部或外部網域傳送，或傳送的日期範圍等。

操作說明：網路詐騙

如何查看「使用者回報」面板

- 登入管理控制台
- 依序點選「安全性」>「資訊主頁」
- 在「使用者回報」面板右下角，按一下「查看報告」



[🔗 說明中心相關文件](#)

- [關於安全性資訊主頁](#)
- [檔案公開報告](#)



安全性狀態

這是什麼？

「安全性狀態」頁面提供 Google Workspace 環境中的安全防護設定總覽，可讓您比較現有設定和 Google 的建議設定，以便主動為機構提供保護。

用途

[安全性最佳做法](#)

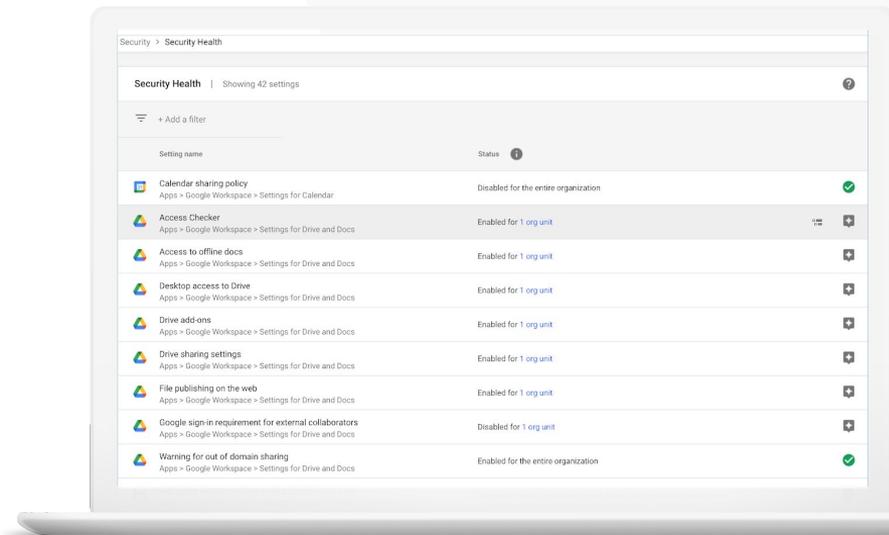


[逐步操作說明](#)

[針對風險區域的建議做法](#)



[逐步操作說明](#)





「請引導我採用最佳做法，或是提供安全性政策的設定建議。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [開始使用「安全性狀態」頁面](#)

安全性最佳做法

開啟「安全性狀態」頁面，即可接收下列安全性政策最佳做法：

-  針對網域中潛在風險區域提供的建議
-  可提高安全性成效的最佳化設定建議
-  直接前往設定的連結
-  額外資訊與支援文章

操作說明：安全性最佳做法檢查清單

為保護貴機構的資料，Google 預設會按照這份檢查清單所列的安全性最佳做法啟用多項建議設定。建議您進一步查看下列項目的詳細說明。

- 管理員：保護管理員帳戶
- 帳戶：防止帳戶被盜及相關因應措施
- 應用程式：檢查第三方應用程式的核心服務存取權
- 日曆：限制日曆外部共用設定
- 雲端硬碟：限制與網域外使用者的共用和協作活動
- Gmail：設定驗證和基礎架構
- 保管箱：控管、稽核保管箱帳戶並確保安全



安全性狀態



安全性與深入分析工具

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](#)

[🔗 說明中心相關文件](#)

- [監控安全性設定狀態](#)



「我想取得網域安全性設定的數據匯報摘要，以及可採取的設定建議，好修正具有潛在風險的區域。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [開始使用「安全性狀態」頁面](#)

針對風險區域的建議做法

「安全性狀態」頁面可用來檢查安全性設定，並標記出建議變更的設定。您可透過「安全性狀態」頁面執行以下操作：

- ✓ 快速辨識網域中具有潛在風險的區域
- ✓ 取得最佳化設定建議，提高機構的安全性成效
- ✓ 在「安全性建議」頁面中查看額外資訊及支援文章

操作說明：安全性建議

如何查看建議

- 登入管理控制台
- 依序點選「安全性」>「安全性狀態」
- 查看最右側欄的狀態設定
 - 顯示綠色勾號即表示設定安全無虞
 - 顯示灰色圖示表示系統建議您進一步檢查設定；只要按一下圖示即可開放詳細資料和操作說明



安全性狀態



安全性與深入分析工具

Google Admin Search

Security > Security health

Health | Showing 37 settings

+ Add a filter

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

[說明中心相關文件](#)

- [開始使用「安全性狀態」頁面](#)

🔍 調查工具

這是什麼？

使用調查工具找出網域內的安全性和隱私權問題，然後加以分類並採取適當措施。

用途

分享不當內容



[逐步操作說明](#)

不小心共用檔案



[逐步操作說明](#)

電子郵件分類



[逐步操作說明](#)

網路詐騙/惡意軟體電子郵件



[逐步操作說明](#)

阻止不肖人士



[逐步操作說明](#)

更深入的安全性分析資訊

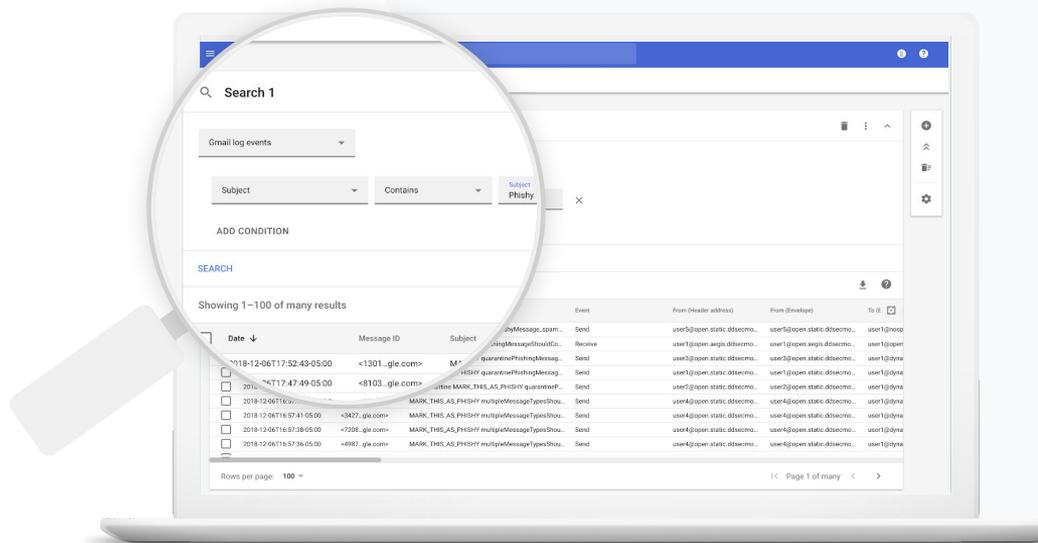


[逐步操作說明](#)

禁止不受監督的會議



[逐步操作說明](#)





「我得知有人分享含有不當內容的檔案。我想知道是誰建立了這個檔案、建立的時間、共用者與共用的對象，以及誰編輯過檔案，而且我想刪除這份檔案。」

[逐步操作說明](#)[說明中心相關文件](#)

- [適用於雲端硬碟記錄事件的條件](#)
- [適用於雲端硬碟記錄事件的動作](#)

分享不當內容

調查工具中的雲端硬碟記錄事件可用來尋找、追蹤、隔離或刪除貴機構網域中的不當檔案。藉由存取[雲端硬碟記錄事件資料](#)，您可以：

- ✓ 根據名稱、執行者和擁有者等條件搜尋文件
- ✓ 變更檔案權限或刪除檔案
- ✓ 搜尋使用者在 Google Workspace 中建立的內容，以及上傳至雲端硬碟的內容
- ✓ 查看該文件的所有記錄資訊
 - 建立日期
 - 文件擁有者、檢視者和編輯者
 - 何時與他人共用



「有人不小心與其他群組共用了某個檔案，而這個群組不該擁有該檔案的存取權。我要移除該群組的檔案存取權。」

[逐步操作說明](#)[說明中心相關文件](#)

- [使用調查工具執行搜尋作業](#)
- [根據搜尋結果執行動作](#)

不小心共用檔案

調查工具中的雲端硬碟記錄事件可協助您追蹤和解決檔案共享問題。藉由存取[雲端硬碟記錄事件資料](#)，您可以：

- ✓ 根據名稱、執行者和擁有者等條件搜尋文件
- ✓ 查看該文件的所有記錄資訊，包括檢視過檔案的對象和檔案共用的時間點
- ✓ 變更權限和停用下載、影印與複製功能

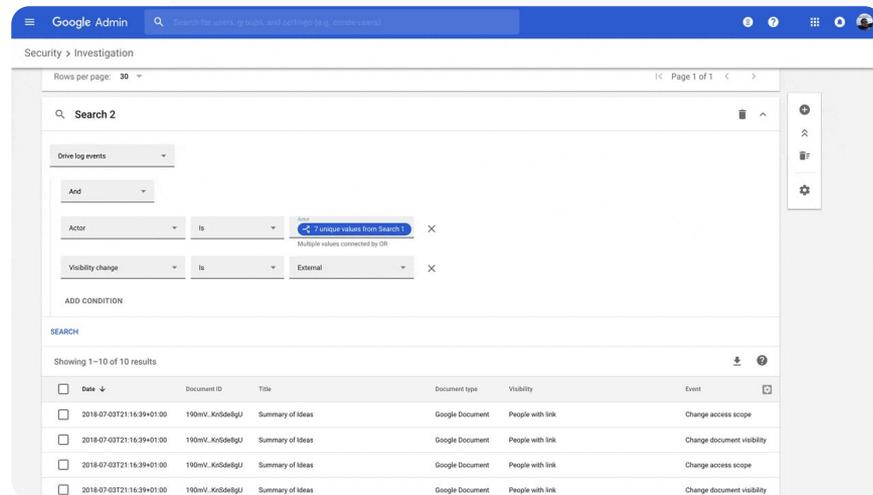
操作說明：雲端硬碟記錄事件

如何調查雲端硬碟記錄事件

- 登入管理控制台
- 依序點選「安全性」>「調查工具」
- 選擇「雲端硬碟記錄事件」
- 依序點選「新增條件」>「搜尋」

如何採取行動

- 在搜尋結果中選取相關檔案
- 依序點選「動作」>「稽核檔案權限」，即可開啟「權限」頁面
- 點選「使用者」來查看誰擁有存取權
- 按一下「連結」查看或修改所選檔案的連結共用設定
- 按一下「待處理的變更」檢查變更內容，然後儲存變更



🔗 說明中心相關文件

- [使用調查工具執行搜尋作業](#)
- [根據搜尋結果執行動作](#)



「有人傳送了不該傳送的電子郵件。我們想知道收件者是誰、對方是否已開啟或回覆郵件，並刪除這封電子郵件。我也想知道電子郵件的內容。」

[逐步操作說明](#)[說明中心相關文件](#)

- [適用於 Gmail 記錄和 Gmail 郵件的條件](#)
- [適用於 Gmail 郵件和 Gmail 記錄事件的動作](#)
- [查看電子郵件內容所需步驟](#)

電子郵件分類

調查工具中的 Gmail 記錄能協助您找出網域中具有危險或不當的電子郵件，並採取行動。藉由存取 Gmail 記錄，貴機構可以：

- ✓ 根據主旨、郵件 ID、附件、寄件者等條件搜尋特定電子郵件
- ✓ 查看電子郵件詳細資料，包括作者、收件者、開啟及轉寄情形
- ✓ 依據搜尋結果執行所需動作。使用者可對 Gmail 郵件採取的動作包括刪除、還原、標記為垃圾郵件或網路釣魚郵件，以及傳送至收件匣或隔離區等



「使用者收到一封疑似是網路詐騙或惡意軟體的電子郵件。我們想知道使用者是否有點擊郵件中的連結或下載附件，因為這麼做可能會讓使用者和我們的網域遭受危害。」

[逐步操作說明](#)[說明中心相關文件](#)

- [適用於 Gmail 記錄和 Gmail 郵件的條件](#)
- [適用於 Gmail 郵件和 Gmail 記錄事件的動作](#)
- [查看電子郵件內容所需步驟](#)
- [查看 VirusTotal 報告](#)

網路詐騙和惡意軟體電子郵件

使用調查工具中的 Gmail 記錄有助於找出並隔離網域中的惡意電子郵件。藉由存取 Gmail 記錄，貴機構可以：

- ✓ 根據特定內容和附件搜尋電子郵件
- ✓ 查看特定電子郵件的資訊，包括收件者和開啟狀態
- ✓ 查看郵件和會話串，判斷郵件是否帶有不當企圖
- ✓ 透過 VirusTotal 掃描電子郵件附件，取得詳盡的威脅情境和信譽資料相關報告
- ✓ 將郵件標記為垃圾郵件或網路釣魚郵件、傳送至特定收件匣或隔離區、刪除郵件，或是進行其他操作

操作說明: Gmail 記錄

調查工具

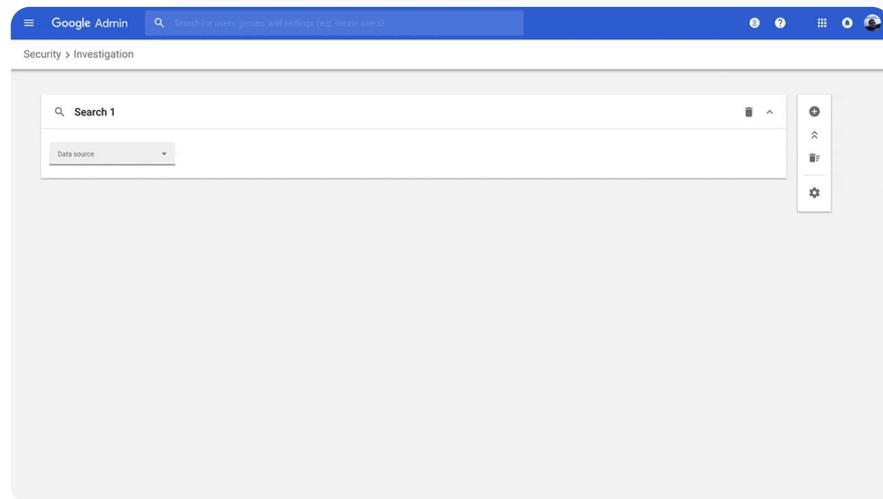
安全性與深入分析工具

如何調查 Gmail 記錄

- 登入管理控制台
- 依序點選「安全性」>「調查工具」
- 選擇「Gmail 記錄事件」或是「Gmail 郵件」
- 依序點選「新增條件」>「搜尋」

如何採取行動

- 在搜尋結果中選取相關檔案
- 按一下「動作」
- 選取「刪除收件匣中的郵件」
- 如要確認此動作，請點選頁面底端的「查看」
- 您可以在「結果」欄中查看動作狀態



[說明中心相關文件](#)

- [適用於 Gmail 記錄和 Gmail 郵件的條件](#)
- [適用於 Gmail 郵件和 Gmail 記錄事件的動作](#)
- [查看電子郵件內容所需步驟](#)



「有惡意行為人不斷嘗試駭入網域中重要的使用者帳戶，我卻怎麼樣都抓不到他們。我該如何遏止這個情況？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [搜尋及調查使用者記錄事件](#)
- [使用調查工具建立活動規則](#)

阻止不肖人士

調查工具中的使用者記錄可協助您：

- 辨識嘗試入侵貴機構使用者帳戶的行為，並進行調查
- 監控貴機構使用者正在使用的兩步驟驗證方式
- 進一步瞭解貴機構使用者登入失敗的情況
- [使用調查工具建立活動規則](#)：自動封鎖來自特定執行者的郵件或其他惡意活動
- [透過進階保護計畫](#)，進一步保護重要的使用者帳戶
- 還原使用者或將使用者停權

操作說明：阻止不肖人士

[調查工具](#)[安全性與深入分析工具](#)

如何調查使用者記錄事件

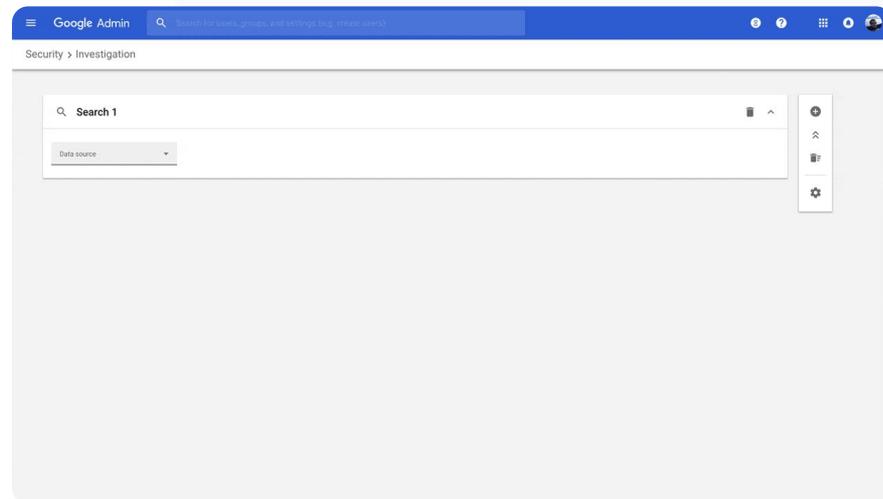
- 登入管理控制台
- 依序點選「安全性」>「調查工具」
- 依序點選「使用者記錄事件」
- 依序點選「新增條件」>「搜尋」

如何還原使用者或將使用者停權

- 在搜尋結果中選取一或多位使用者
- 點選「動作」下拉式選單
- 按一下「還原使用者」或「將使用者停權」

如何查看特定使用者的詳細資料

- 在搜尋結果頁面上選取一位使用者
- 在「動作」下拉式選單中點選「查看詳細資料」

[說明中心相關文件](#)

- [搜尋及調查使用者記錄事件](#)



「我們的教師在 Gmail 中將附加檔案標記為可疑。IT 人員有沒有辦法判斷該檔案是否具安全威脅？」

[逐步操作說明](#)

[說明中心相關文件](#)

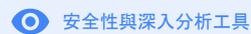
- [使用調查工具執行搜尋作業](#)
- [透過調查工具查看 VirusTotal 報告](#)

取得更詳盡的安全性深入分析資料

VirusTotal 報告會顯示完整資訊總覽，進一步提供安全調查結果，可讓管理員查看群眾外包深入分析資料，確認特定網域、檔案附件、IP 位址或網址的安全性。

- ✓ 取得更多 Gmail 和 Chrome 記錄事件的安全性深入分析資訊
- ✓ 分析可疑檔案、網址、網域和 IP 位址
- ✓ 存取群眾外包詳細資訊，瞭解為何附件或網站被判定為具有風險
- ✓ 取得相關協助，以便在處理安全性疑慮時做出決策

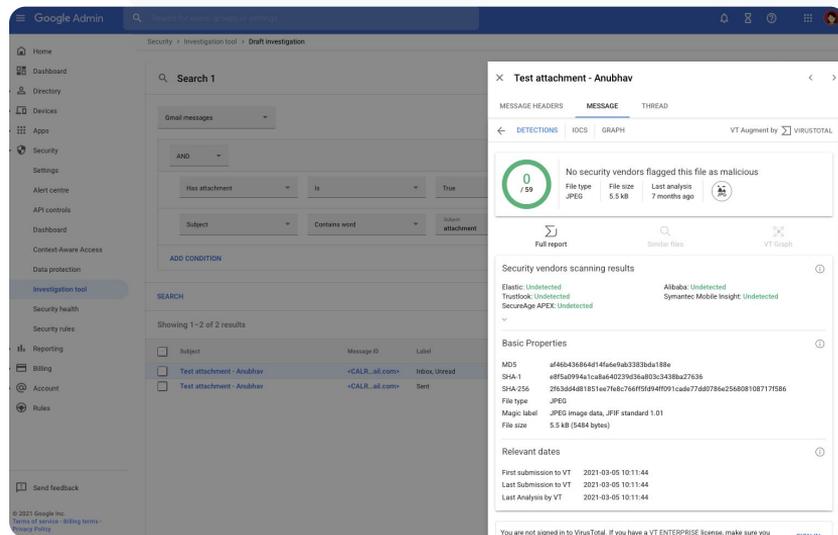
操作說明：取得更詳盡的安全性 深入分析資料



如何查看與 Gmail 相關的 VirusTotal 報告

- 登入管理控制台
- 依序點選「安全性」>「安全中心」>「調查工具」
- 選擇「Gmail 郵件」
- 按一下「新增條件」>「有附件」
- 在搜尋結果中點選「郵件ID」或「主旨」連結
- 在側邊面板中，按一下「郵件」或「會話串」分頁標籤
- 選取「查看 VirusTotal 報告」

管理員也可查看與 Chrome 相關的 VirusTotal 報告。按照上述操作說明，並在調查工具中選取「Chrome 記錄事件」即可。



[說明中心相關文件](#)

- [透過調查工具查看 VirusTotal 報告](#)



「學生在下課後仍繼續進行 Google Meet 即時通話。我需要能為所有人結束 Meet 通話的方法，以避免學習受到干擾。」

[逐步操作說明](#)[說明中心相關文件](#)

- [使用調查工具結束會議](#)

禁止不受監督的虛擬會議

Google Workspace 管理員可使用「安全調查工具」中的「結束整場會議」動作，從機構內的任何會議中移除所有使用者。會議主辦人也能針對個別 Google Meet 通話使用上述動作。



系統會為目前參加會議的所有使用者結束會議，就連在分組討論室中的使用者也不例外。



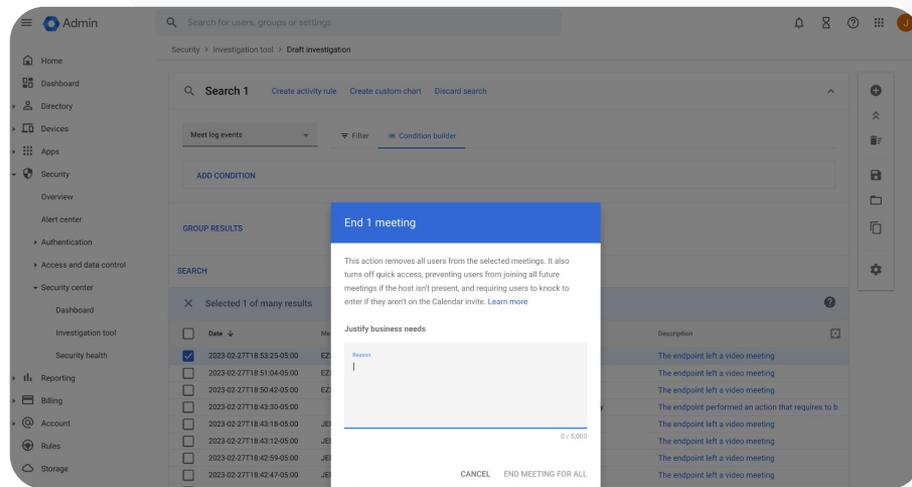
這麼做能防止任何人在主辦人不在場的情況下，加入該會議的後續活動。

操作說明：禁止不受監督的虛擬會議

[🔍 調查工具](#)[👁️ 安全性與深入分析工具](#)

如何使用安全調查工具為所有使用者結束會議

- 登入管理控制台
- 依序點選「安全性」>「安全中心」>「調查工具」
- 選擇「Meet 記錄事件」
- 按一下「搜尋」> 系統會列出 Meet 記錄事件的搜尋結果
- 找出要為所有使用者結束的會議，並勾選對應的方塊
- 選取「動作」
- 按一下「結束整場會議」

[🔗 說明中心相關文件](#)

- [使用調查工具結束會議](#)



網域管理與控管

[安全性與深入分析工具](#)

管理員可使用 Google Workspace 進階工具控管機構資料、設定控制項、監控使用情形，並協助機構遵循教育標準。

用途

[掃描 Gmail 附件找出潛在威脅](#)[逐步操作說明](#)[建立使用情形資訊主頁及報表](#)[逐步操作說明](#)[尋找檔案更輕鬆](#)[逐步操作說明](#)[整理內部文件](#)[逐步操作說明](#)[自動填入部門群組](#)[逐步操作說明](#)[建立對內共用檔案目標對象](#)[逐步操作說明](#)[限制共用檔案對象](#)[逐步操作說明](#)[Workspace 應用程式限制](#)[逐步操作說明](#)[管理儲存空間](#)[逐步操作說明](#)[資料法規](#)[逐步操作說明](#)[授權相關法規](#)[逐步操作說明](#)[管理端點裝置](#)[逐步操作說明](#)[管理 Windows 裝置](#)[逐步操作說明](#)[Windows 裝置的自訂設定](#)[逐步操作說明](#)[自動更新 Windows 裝置](#)[逐步操作說明](#)[善用用戶端加密功能](#)[逐步操作說明](#)



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

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

 Relevant Help Center documentation

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

Scan Gmail attachments for threats

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

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

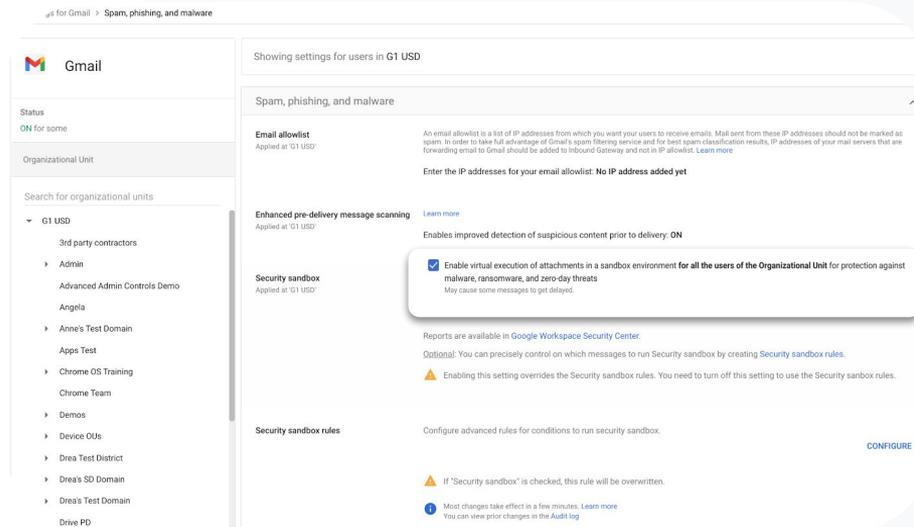
How to: Scan Gmail attachments for threats

How it works

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

How to scan all attachments in Security Sandbox

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



us for Gmail > Spam, phishing, and malware

Gmail

Status
ON for some

Organizational Unit

Search for organizational units

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

Showing settings for users in G1 USD

Spam, phishing, and malware

Email allowlist
Applied at 101 USD

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

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

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

Enables improved detection of suspicious content prior to delivery: ON

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

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

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

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

Security sandbox rules

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

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

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

[🔗 Relevant Help Center documentation](#)

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



「我該如何瞭解整個網域的 Classroom 使用情況？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [設定 BigQuery 匯出和數據分析範本](#)

建立使用情形資訊主頁及報表

有了 BigQuery 匯出作業和 Looker Studio 範本，管理員可使用 Looker Studio，以及與 BigQuery 整合的第三方視覺化合作夥伴等各種分析工具，以 Classrooms 活動記錄建立自訂資訊主頁和報表。

- ✓ 將 Classroom 記錄資料從管理控制台匯出至 BigQuery 和 Looker Studio。
- ✓ 迅速查看整個網域的使用情形和採用率報告。清楚掌握哪位使用者將學生從課程中移除，或是在特定日期封存了特定課程等。
- ✓ 透過可自訂 Looker Studio 資訊主頁範本瞭解各種趨勢，並快速採取行動。

操作說明：建立使用情形資訊主頁及報表

01 設定並匯出 BigQuery 專案

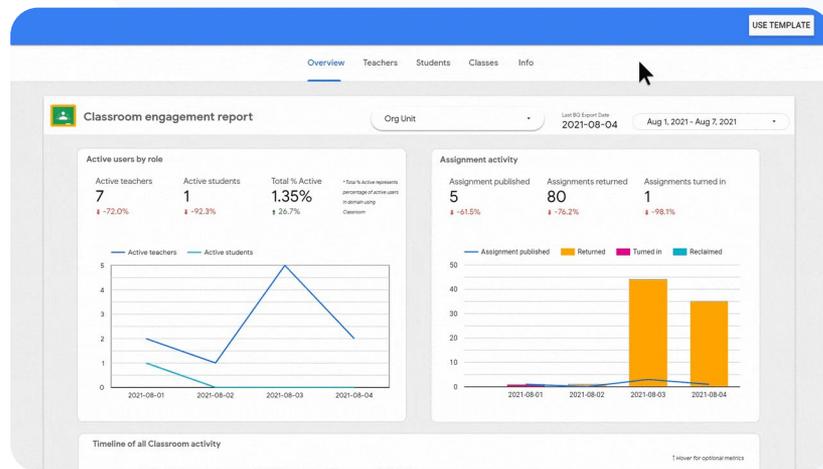
- 登入 console.cloud.google.com > 建立新專案
- 登入 admin.google.com > 依序點選「報告」>「BigQuery Export」
- 點選 Cloud BigQuery 專案 > 為資料集命名 >「儲存」

02 在 Looker Studio 中新增 BigQuery 匯出作業

- 登入 [Looker Studio](https://lookerstudio.google.com) > 點選「建立」>「資料來源」
- 選取 BigQuery 連接器 >「我的專案」> 按一下您建立的專案 >「活動」
- 勾選「分區資料表」下方的方塊 > 點選「連結」

03 建立 Looker Studio 資訊主頁

- 開啟 [範本](#) > 選取「使用範本」
- 在「新資料來源」下方，選取「活動」資料來源
- 按一下「複製報告」



[🔗 說明中心相關文件](#)

- [設定 BigQuery 匯出和數據分析範本](#)



「我需要追蹤家長透過 Gmail、Chat 和文件提交的校外教學同意回條。我該如何在網域中找出這些檔案？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [Google Cloud Search 指南](#)
- [為使用者開啟或關閉 Cloud Search](#)

尋找檔案更輕鬆

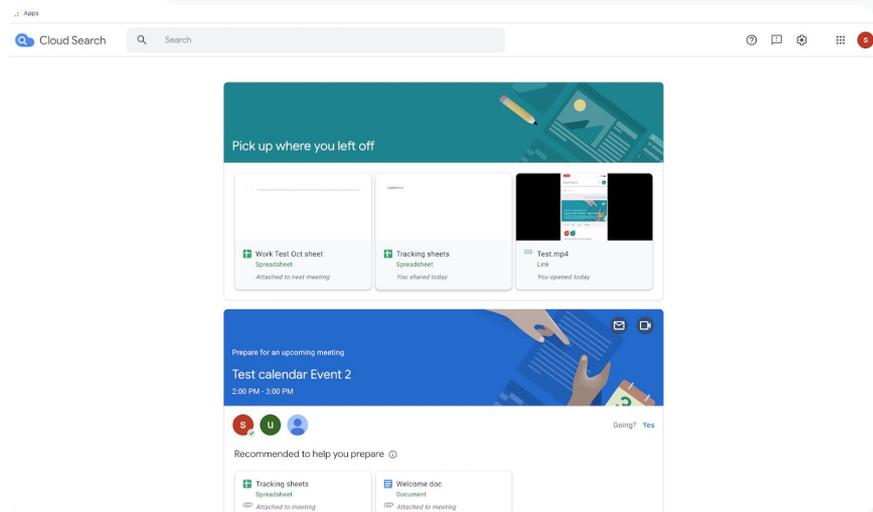
Google Cloud Search 可讓貴機構的教師在 Google Workspace 和第三方應用程式中快速找出內容。

- ✓ 無論您身在何處，使用的是筆電、手機還是平板電腦，都能找到所需資訊
- ✓ 在雲端硬碟、聯絡人、Gmail 等 Google Workspace 應用程式，以及第三方資料來源中進行搜尋

操作說明：尋找檔案更輕鬆

為使用者啟用 Cloud Search

- 登入管理控制台 > 依序前往「選單」>「應用程式」>「Google」
- 按一下「服務狀態」
- 如要為貴機構中的所有使用者開啟或關閉服務，請按一下「為所有人啟用」或「為所有人關閉」
- 按一下「儲存」
- 如要為一群屬於相同或不同機構單位的使用者開啟服務，請選取存取權群組
- 按一下「儲存」



說明中心相關文件

- [Google Cloud Search 指南](#)
- [為使用者開啟或關閉 Cloud Search](#)



「我想為機構的檔案套用敏感程度標籤，藉此配合法規遵循需求、避免濫用並讓檔案更井然有序。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [管理雲端硬碟標籤](#)

整理網域中的文件

雲端硬碟標籤可協助使用者在整個網域中尋找、整理檔案及套用政策。管理員可建立和管理雲端硬碟標籤，以避免檔案濫用，並確保學生資料符合法規遵循要求。

- ✔ 雲端硬碟標籤是中繼資料，可協助您整理個別教育計畫、DOD 或法規遵循文件等教育相關機密檔案。
- ✔ 只有管理員可建立、定義結構並且發布標籤。貴機構的使用者可以將標籤套用至編輯的檔案，也能設定相關的欄位值。
- ✔ 雲端硬碟標籤可用於支援自動化[資料遺失防護](#)功能。

操作說明：整理網域中的文件

運作方式

Google 雲端硬碟提供標記標籤(視覺指標) 和標準標籤, 有助於整理網域中的檔案。

如何為機構啟用雲端硬碟標籤

- 登入管理控制台
- 依序點選「選單」>「應用程式」>「Google Workspace」>「雲端硬碟與文件」
- 選取「標籤」
- 啟用或停用標籤
- 按一下「儲存」

 [說明中心相關文件](#)

- [管理雲端硬碟標籤](#)



「我該如何自動決定群組成員，讓每一位新加入機構的教師都能納入『教師』電子郵件名單中？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [透過動態群組自動管理成員](#)

自動填入部門群組

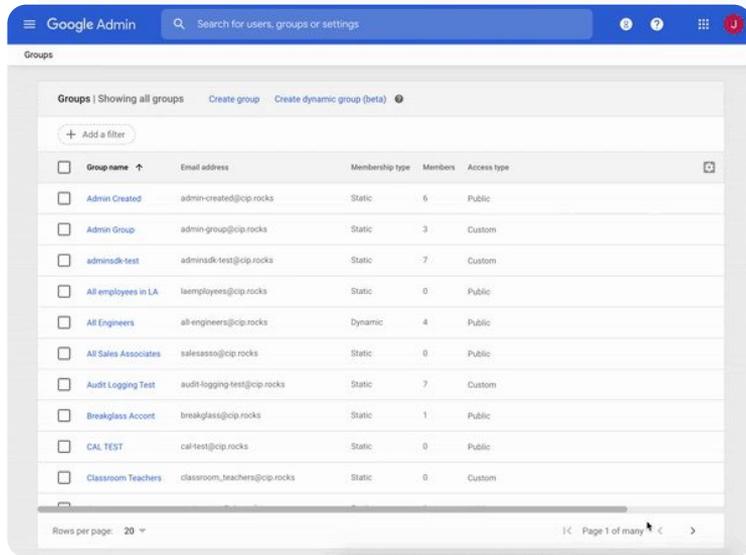
動態群組可讓管理員透過自訂條件更新全校群組成員。

- ✓ 建立可自動管理成員的動態群組
- ✓ 讓系統根據您建立的成員查詢條件隨時更新群組狀態
- ✓ 動態群組的用途如下
 - 電子郵件和通訊群組清單
 - 開啟審核功能的群組和協作收件匣
 - 安全性群組

操作說明：自動填入群組

建立動態群組

- 登入管理控制台 > 依序前往「選單」>「目錄」>「群組」
- 按一下「建立動態群組」
- 建立含有以下條件和值的成員查詢：
 - **條件清單**：定義成員的條件，例如「部門」
 - **「值」欄位**：輸入要使用的值
- 輸入下列資訊：
 - **名稱**：可用於辨識清單和訊息中的群組
 - **說明**：群組的用途
 - **群組電子郵件**：群組使用的電子郵件地址
- 按一下「儲存」
- 按一下「完成」



說明中心相關文件

- [透過動態群組自動管理成員](#)



「職員不小心與整個機構共用文件，讓機密資料暴露在風險中。我該如何將共用對象設為僅限規模較小且更相關的群組？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [關於目標對象](#)
- [部署目標對象的最佳做法](#)
- [建立目標對象](#)

建立對內共用檔案目標對象

目標對象設定可降低使用者不小心過度共用檔案的機率，進而提升貴機構資料的安全性。

- ✓ 確保使用者與正確的對象 (例如特定團隊或部門) 共用檔案
- ✓ 目標對象是一種使用者群組，管理員可以將這類群組當做使用者的建議共用對象
- ✓ 管理員能夠將目標對象新增至使用者的共用設定，鼓勵使用者與特定目標對象共用項目
- ✓ 適用於 Google 雲端硬碟、Google 文件及 Chat

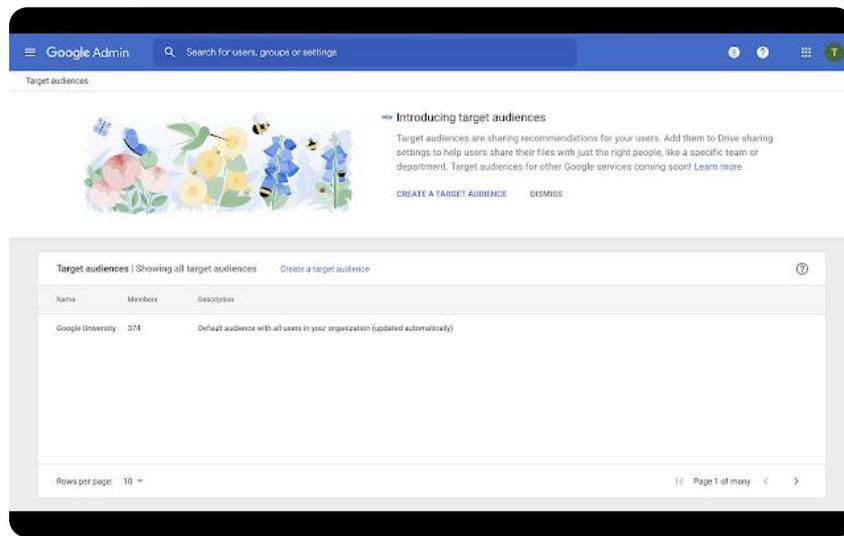
操作說明：建立對內共用檔案目標對象

運作方式

建立目標對象後，您可以新增成員，並將目標對象新增至 Google 雲端硬碟，讓目標對象顯示在使用者的共用設定中。舉例來說，您可以讓職員在共用雲端硬碟檔案時選取「所有職員」目標對象。

如何為機構啟用雲端硬碟標籤

- 登入管理控制台 > 依序前往「選單」>「目錄」>「目標對象」
- 按一下「建立目標對象」
- 在「名稱」下方，輸入目標對象名稱
- 選取「新增成員」> 加入想要的成員
- 按一下「完成」



說明中心相關文件

- [關於目標對象](#)
- [部署目標對象的最佳做法](#)
- [建立目標對象](#)



「我該如何避免中學生和小學生共用文件？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [建立及管理雲端硬碟共用信任規則](#)

限制共用檔案對象

雲端硬碟信任規則可讓管理員設定規則，控管哪些使用者可存取 Google 雲端硬碟檔案，藉此保護機構資料隱私權。這類政策可套用至個別使用者、群組、機構單位及網域。

- ✓ 保護機密資訊，並遵循業界標準和法規
- ✓ 限制內部和/或外部網域共用情況。管理員可建立信任規則，只允許學生在機構內共用雲端硬碟檔案
- ✓ 「信任規則」啟用之後，便會取代 Google 雲端硬碟管理員控制項中現有的「共用選項」

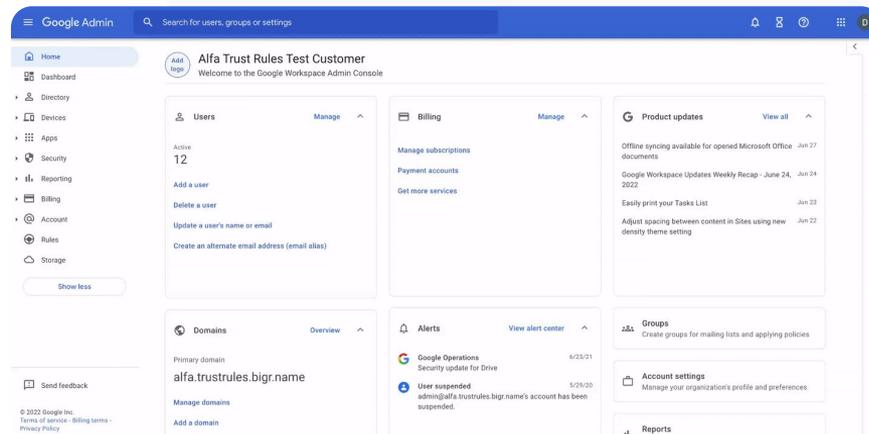
操作說明：限制共用檔案對象

啟用雲端硬碟信任規則

- 登入管理控制台 > 依序前往「選單」>「規則」
- 在頁面頂端的「安全協同合作」資訊卡中，按一下啟用信任規則」
- [工作清單](#)隨即會自動開啟，並顯示信任規則啟用進度

管理員可建立信任規則、查看和編輯信任規則詳細資料、刪除信任規則及查看信任規則記錄事件。

如需管理信任規則的逐步操作說明，請造訪[管理員說明中心](#)



🔗 說明中心相關文件

- [建立及管理雲端硬碟共用信任規則](#)



「我想限制使用者在網路上對特定應用程式的存取權。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [情境感知存取權總覽](#)
- [為應用程式指派情境感知存取權層級](#)

Google Workspace 應用程式限制

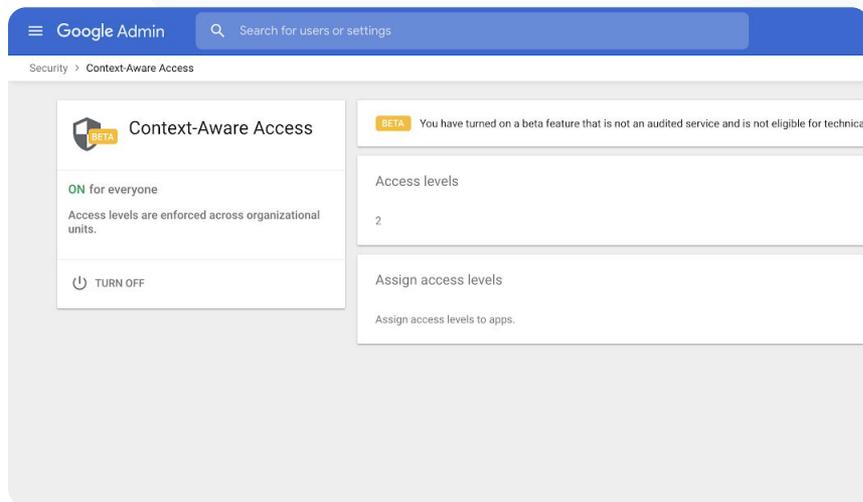
透過情境感知存取權功能，您可以根據使用者身分、位置、裝置安全性狀態和 IP 位址等屬性，為 Google Workspace 和第三方 SAML (安全宣告標記語言) 應用程式建立精細的存取權控管政策。您還可以禁止透過外部網路存取應用程式。

- ✓ 您可以將情境感知存取權政策套用至 Google Workspace for Education 的核心服務
- ✓ 舉例來說，您可以規定使用者僅能透過機構提供的裝置存取 Workspace 應用程式，或是只在使用者的儲存裝置經過加密後才授予雲端硬碟存取權

操作說明：限制 Google Workspace 應用程式存取權

如何使用情境感知存取權功能

- 登入管理控制台
- 依序選取「安全性」>「情境感知存取權」>「指派」
- 選取「指派存取層級」即可查看應用程式清單
- 選取機構單位或配置群組來排序清單
- 在要調整的應用程式旁，選取「指派」
- 選取一或多個存取層級
- 如要讓使用者符合多個條件，請建立多個層級
- 按一下「儲存」



[說明中心相關文件](#)

- [情境感知存取權總覽](#)
- [為應用程式指派情境感知存取權層級](#)



「我想在網域中導入新的
儲存空間管理計畫。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [管理員專用儲存空間指南](#)
- [瞭解可用的儲存空間和用量](#)
- [釋出或取得更多儲存空間](#)
- [設定儲存空間上限](#)

管理網域中的儲存空間

使用 Google Workspace for Education 的機構可享有 100 TB 的基本集區儲存空間；這個儲存空間足以存放約 1 億份文件、8 百萬份簡報，或 40 萬小時的影片。管理集區雲端硬碟儲存空間，確保貴機構有效使用儲存空間。



透過管理員工具、報表和記錄瞭解：

- 貴機構的儲存空間用量
- 設定儲存空間上限
- 找出使用過多儲存空間的帳戶



除了基本儲存空間之外，Teaching and Learning Upgrade 和 Education Plus 還提供額外的儲存空間

- Teaching and Learning Upgrade：每購買一份授權，共用集區就會額外增加 100 GB 的儲存空間
- Education Plus：每購買一份授權，共用集區就會額外增加 20 GB 的儲存空間

操作說明：管理網域中的儲存空間

網域管理與控管

安全性與深入分析工具

找出使用者儲存空間使用量

- 登入管理控制台 > 依序前往「選單」>「儲存空間」
- 依機構和使用者查看儲存空間使用量

設定儲存空間上限

- 在管理控制台中，依序點選「選單」>「儲存空間」
- 在「儲存空間設定」部分，按一下「管理」
- 按一下「使用者儲存空間上限」> 選取要套用上限的實體：
 - **機構單位**：按一下機構單位
 - **群組**：依序按一下「群組」> 搜尋欄位 > 輸入群組名稱 > 按一下群組
- 選取「開啟」並設定儲存空間容量
- 按一下「儲存」

Storage

Workspace storage

Total used
6 TB

Drive 5 TB

Gmail 25 GB

Photos 25 GB

Storage settings

Users using the most storage

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

Shared drives using the most storage

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

Resources for you

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

說明中心相關文件

- [管理員專用儲存空間指南](#)
- [瞭解可用的儲存空間和用量](#)
- [釋出或取得更多儲存空間](#)
- [設定儲存空間上限](#)



「為遵守相關法規，我校內學生和教職員的資料必須存放在歐盟地區。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [選擇資料存放的地理位置](#)

資料法規

資料地區政策可讓管理員選擇將資料存放在美國或英國/歐洲等特定地理位置。

- ✓ 使用 Education Plus 與 Education Standard 的機構可以為部分使用者選擇單一資料地區，也可以為特定部門或團隊選擇不同資料地區，並查看資料地區遷移進度。
- ✓ 將使用者加入依部門設定的機構單位，或是加入可包含不同部門使用者的配置群組。
- ✓ 資料地區政策不適用於不具備 Education Standard 或 Education Plus 授權的使用者。



「根據授權法規，我機構內的研究資料必須存放在美國境內。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [選擇資料存放的地理位置](#)

授權相關法規

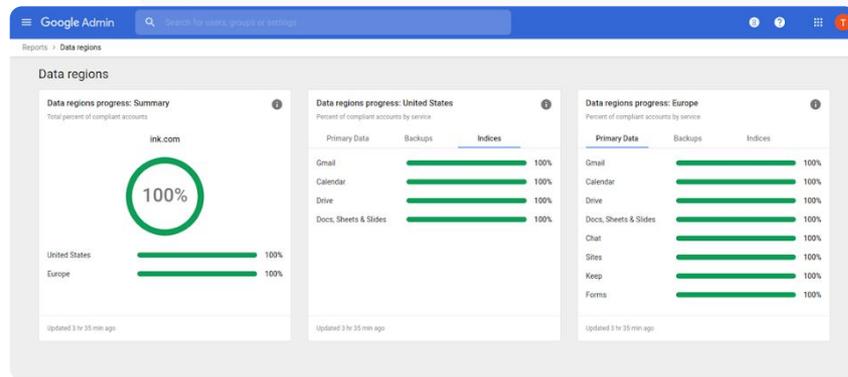
資料地區政策可讓管理員選擇將教職員的研究資料存放在特定地理位置 (美國或歐洲)。

- 資料地區政策適用於多數 Google Workspace for Education 核心服務的主要靜態資料 (包括備份資料)。如要查看資料清單，請點選[這裡](#)
- 如果使用者不在資料存放的地區，有時會經歷較長的延遲時間，因此在設定資料地區政策前請先評估損益

操作說明：資料法規

如何指定資料地區

- 登入管理控制台
 - **注意：**必須以超級管理員的身分登入，才能進行設定。
- 依序點選「公司資料」>「顯示更多」>「資料地區」
- 選取要限制地區的機構單位或配置群組 或是選取整欄以涵蓋所有單位和群組
- 選取地區，選項包括「無偏好設定」、「美國」或「歐洲」
- 按一下「儲存」



[說明中心相關文件](#)

- [選擇資料存放的地理位置](#)



「我需要管理學區內所有類型的裝置，包括 Chromebook、iOS 和 Windows 10 等裝置，並統一套用相同的政策，尤其是裝置遭駭時，就更需要這樣的功能。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [使用 Google 端點管理服務管理裝置](#)
- [設定進階行動管理服務](#)

管理端點裝置

您可以使用企業端點管理服務，透過行動裝置進一步控管機構資料。您可以對行動裝置功能設定限制、要求加密保護裝置、管理 Android 裝置、iPhone 和 iPad 上的應用程式，以及抹除裝置資料。



您可以透過管理控制台核准、封鎖、解除封鎖或刪除裝置。

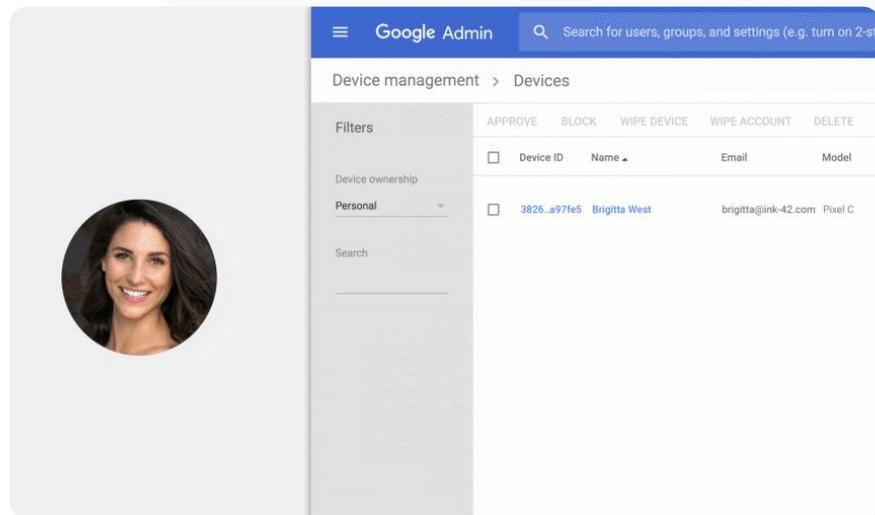


若是有成員遺失裝置或遭到學校退學，您可以從特定的管理模組裝置上抹除使用者的帳戶、個人設定檔，甚至是所有資料。該資料仍會出現在電腦或網路瀏覽器上。

操作說明：管理端點裝置

如何啟用進階行動管理服務

- 登入管理控制台
- 依序前往「管理控制台」>「裝置」
- 點選左側的「設定」>「通用設定」
- 依序點選「一般」>「行動管理服務」
- 如要為所有使用者套用設定，請選取頂層機構單位；否則請選取子機構單位。
- 選取「進階」
- 按一下「儲存」



[🔗 說明中心相關文件](#)

- [使用 Google 端點管理服務管理裝置](#)
- [設定進階行動管理服務](#)



「我機構內有些教師使用 Windows 10 裝置，我該如何在同一處管理所有機構裝置？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [啟用 Windows 裝置管理服務](#)
- [為裝置註冊 Windows 裝置管理服務](#)

管理 Microsoft Windows 裝置

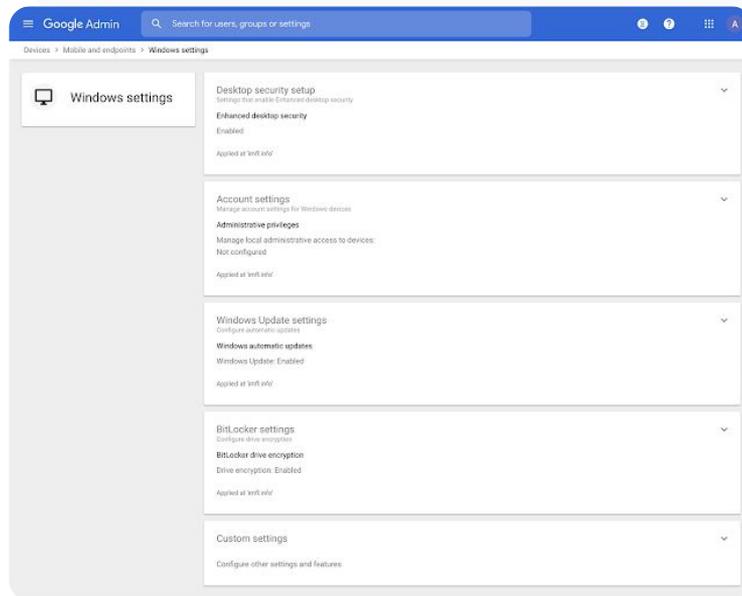
您可以透過管理控制台管理及保護機構的 Windows 10 裝置，做法和 Android、iOS、Chrome 及 Jamboard 裝置一樣。

- ✓ 啟用單一登入功能，讓使用者輕鬆在 Windows 10 裝置上存取 Google Workspace
- ✓ 在管理控制台中管理裝置，確保用來存取 Google Workspace 的裝置都已更新、安全無虞且符合相關規範
- ✓ 透過雲端為 Windows 10 裝置抹除資料、推送裝置設定更新等

操作說明：管理 Microsoft Windows 裝置

啟用 Windows 裝置管理服務

- 在管理控制台中，依序前往「選單」>「裝置」>「行動裝置與端點」>「設定」>「Windows 設定」
- 選取「Windows 管理設定」
- 如要為所有使用者套用設定，請選取頂層機構單位
- 在「Windows 裝置管理」旁邊，選取「已啟用」
- 按一下「儲存」



[說明中心相關文件](#)

- [啟用 Windows 裝置管理服務](#)
- [為裝置註冊 Windows 裝置管理服務](#)



「如何在 Windows 10 裝置上 設定 Wi-Fi 設定檔？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [常見自訂設定](#)
- [新增自訂設定](#)

Windows 10 裝置的自訂設定

管理員可使用 Google 的 Windows 裝置管理服務，將自訂設定新增至所有裝置。

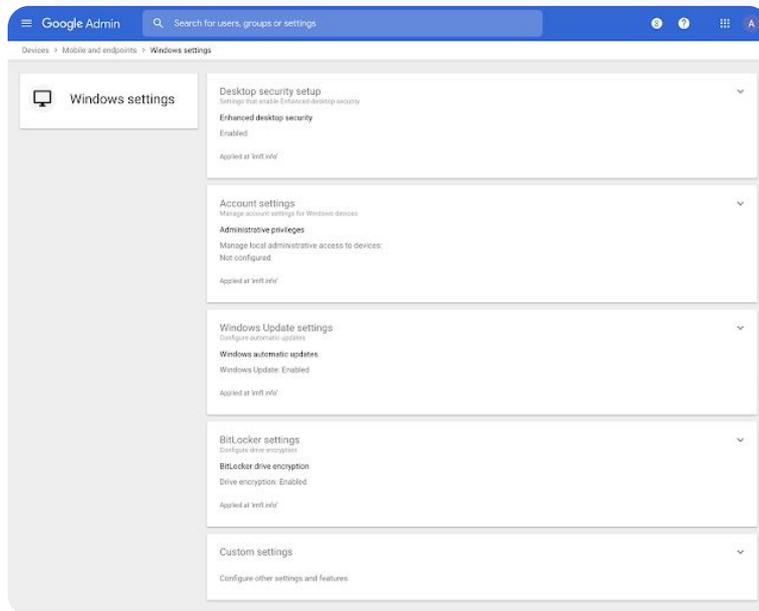
- ✓ 透過管理控制台控管自訂裝置設定
- ✓ 對下列部分套用設定：
 - 裝置管理
 - 安全性
 - 硬體和網路
 - 軟體
 - 隱私權

操作說明: Windows 10 裝置的 自訂設定

新增自訂設定

- 在管理控制台中, 依序前往「選單」>「裝置」>「行動裝置與端點」>「設定」>「Windows 設定」
- 選取「自訂設定」
- 按一下「新增自訂設定」> 填妥所有必填欄位
- 點選「下一步」
- 選擇要套用設定的機構單位
- 按一下「套用」

請注意, Google 不提供第三方產品或設定的相關技術支援服務。



[說明中心相關文件](#)

- [常見自訂設定](#)
- [新增自訂設定](#)



「我想確保機群中的
Windows 10 裝置都能
接收最新更新項目。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [管理自動更新設定](#)

自動更新 Windows 10 裝置

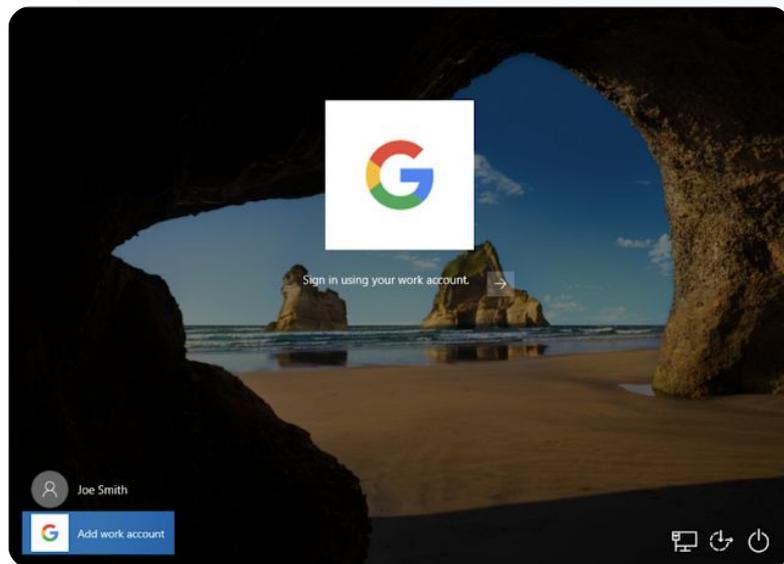
您可以為機構的 Windows 10 裝置指定更新方式和時間，讓裝置透過 Windows 自動更新服務接收安全性更新和其他重要下載內容。

- ✓ 您能透過 Windows Update 控制台設定下載更新的通知、設定系統不要在某時段安排更新後的重新啟動作業等等
- ✓ 將設定套用至整個機構或特定機構單位
- ✓ 變更最多可能需要 24 小時才會生效，但通常不會這麼久

操作說明：自動更新 Windows 10 裝置

設定更新作業

- 在管理控制台中，依序前往「選單」>「裝置」>「行動裝置與端點」>「設定」>「Windows 設定」
- 依序選取「Windows Update 設定」>「啟用」
- 在「Windows 裝置管理」旁邊，選取「已啟用」
- 設定下列選項，此外還有[更多選項](#)：
 - 接受 Microsoft 應用程式的更新
 - 自動更新行為
 - 自動更新頻率
- 按一下「儲存」



[說明中心相關文件](#)

- [管理自動更新設定](#)



「我知道 Google 在資料加密方面堅持最嚴格的標準，但我想控管我們大學的智慧財產和補助研究計畫加密金鑰。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [關於用戶端加密](#)

善用用戶端加密功能

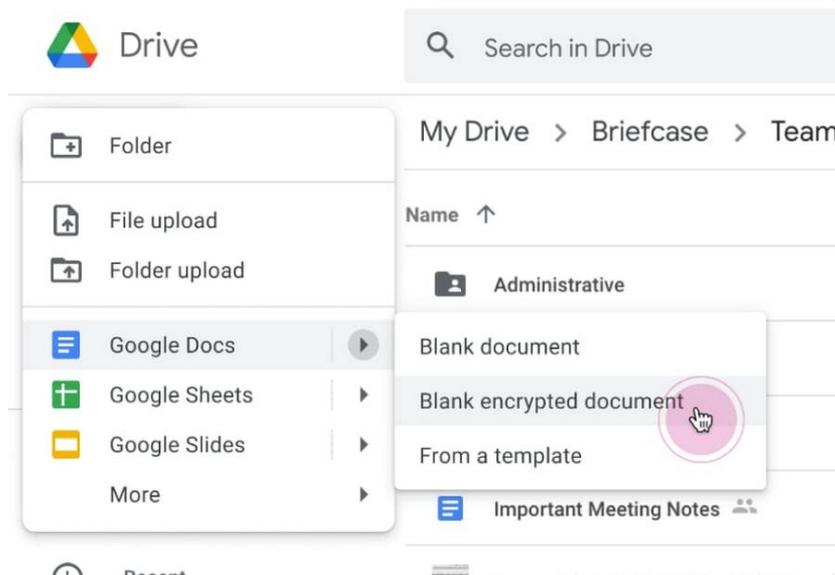
Google Workspace 已經採用最新的密碼學標準，為所有靜態資料及在各處傳輸的資料進行加密。透過用戶端加密功能，管理員可以直接控管加密金鑰，以及用於存取這些金鑰的識別資訊提供者。

- ✓ 使用自己的加密金鑰來加密機密資料，例如貴機構的智慧財產
- ✓ 系統會先在您的瀏覽器中進行內容加密，再將資料傳輸至他處或儲存在 Google 的雲端儲存空間
- ✓ 您可以選擇哪些使用者可建立用戶端加密內容，以及是否能對內或對外共用內容

操作說明：善用用戶端加密功能

設定用戶端加密功能 (CSE)

- 設定加密金鑰服務
 - [建立金鑰服務](#)，透過金鑰管理和控制功能保護您的資料
- 將 Google Workspace 連線至外部金鑰服務
 - 在管理控制台中加入金鑰服務網址，[新增及管理金鑰服務以進行用戶端加密](#)
- 為機構單位或群組指派金鑰服務
 - 為整個機構[指派一個預設金鑰服務](#)
- 將 Google Workspace 連線至 IdP
 - [連線至識別資訊提供者](#) (IdP) 以進行用戶端加密，藉此在驗證使用者身分後，才允許他們為內容加密或存取加密內容
- 為使用者啟用 CSE
 - 如果使用者需要建立用戶端加密內容，您可以為其所屬機構單位或群組[開啟用戶端加密功能](#)



[🔗 說明中心相關文件](#)

- [關於用戶端加密](#)



教學與學習功能

透過豐富的課程體驗、可促進學術誠信的各项工具，以及更強大的視訊溝通服務，讓貴機構的教師在數位學習環境中享有更多功能。



[Google Classroom](#)



[原創性報告](#)



[文件、試算表和簡報](#)



[Google Meet](#)



這是什麼？

Google Classroom 是集教學與學習於一處的集中式平台，Classroom 付費版功能可協助教師整合各種課程工具。教師能直接在 Classroom 中使用喜愛的工具，並讓課堂學生名單與外部系統保持同步。

用途

[管理 Classroom 外掛程式存取權限](#)



[逐步操作說明](#)

[在 Classroom 中結合引人入勝的內容](#)

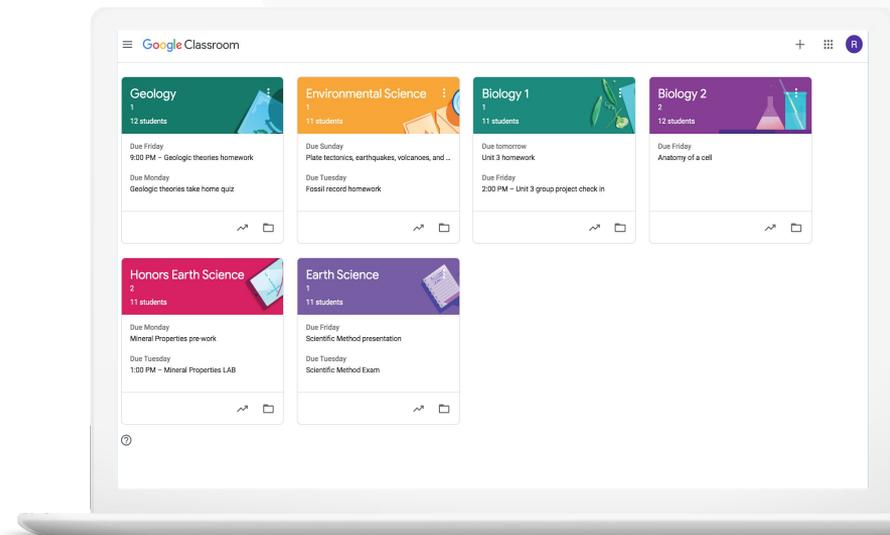


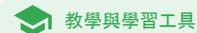
[逐步操作說明](#)

[大規模建立課程](#)



[逐步操作說明](#)





「我希望能透過單一登入，讓教師存取最喜愛的教育科技工具。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [管理 Google Workspace Marketplace 中的應用程式](#)
- [在 Classroom 中使用外掛程式](#)
- [管理許可清單中的 Marketplace 應用程式](#)
- [向使用者發布 Marketplace 中的應用程式](#)
- [Classroom 外掛程式 \[管理員專用入門指南\]](#)

管理 Classroom 外掛程式存取權限

透過網域許可清單，決定貴機構可存取哪些第三方教育應用程式讓教師只要點擊幾下，即可輕鬆安裝外掛程式並加入學生作業中。



在網域中建立許可清單，決定教師可透過 Google Workspace Marketplace 安裝哪些第三方應用程式。



教師可透過補充教育應用程式提升學習成果，並且在 Google Classroom 中出作業、批改內容和打分數。



Google Workspace Marketplace 包含 Adobe Creative Cloud Express、BookWidgets、CK-12、Formative、Genially、Google 藝術與文化、IXL、Kahoot!、Nearpod、Newsela、Pear Deck、SAFARI Montage、Sora 和 Wordwall 等。

操作說明：管理 Classroom 外掛程式存取權限

透過網域許可清單控管外掛程式存取權

- 在管理控制台中，依序選取「選單」>「Google Workspace Marketplace 中的應用程式」>「應用程式清單」
- 選取「將應用程式加入許可清單」
- 輸入想要的外掛程式名稱，或是搜尋應用程式
- 按一下「選取」，並確認已選取「允許使用者安裝這個應用程式」
- 依序點選「繼續」和「完成」

授予想要的外掛程式許可清單存取權

- 在管理控制台中，依序選取「選單」>「Google Workspace Marketplace 中的應用程式」>「應用程式清單」
- 選取要發布的外掛程式
- 在「使用者存取權」下方，按一下查看機構單位及群組」
- 選擇要開放所有人使用 或是讓特定群組或機構單位存取
- 按一下「儲存」

Apps > Settings for Google Workspace Marketplace apps

Google Workspace Marketplace Settings

Manage access to apps

Allow install

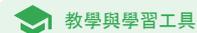
Settings to install third-party Google Workspace Marketplace apps:

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

1 unsaved change CANCEL SAVE

說明中心相關文件

- [管理 Google Workspace Marketplace 中的應用程式](#)
- [在 Classroom 中使用外掛程式](#)
- [管理許可清單中的 Marketplace 應用程式](#)
- [向使用者發布 Marketplace 中的應用程式](#)
- [Classroom 外掛程式「管理員專用入門指南」](#)



「我想直接在 Google Classroom 中指派 Kahoot! 學習遊戲，並且評分。」

[🔗 逐步操作說明](#)

[🔗 說明中心相關文件](#)

- [在 Classroom 中使用外掛程式](#)
- [Classroom 外掛程式 \[教師專用入門指南\]](#)

在 Classroom 中結合引人入勝的內容

教師可以透過 Classroom 外掛程式，在作業、問題、教材或公告中附加外掛程式，與學生分享深具吸引力的活動和內容。



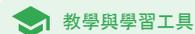
讓教師和學生無須離開 Classroom 也可使用喜愛的工具，例如 Kahoot!、Nearpod 和 Pear Deck



有了外掛程式，學生無須管理多組密碼或前往外部網站



直接在 Classroom 中透過外掛程式查看和批改學生作業



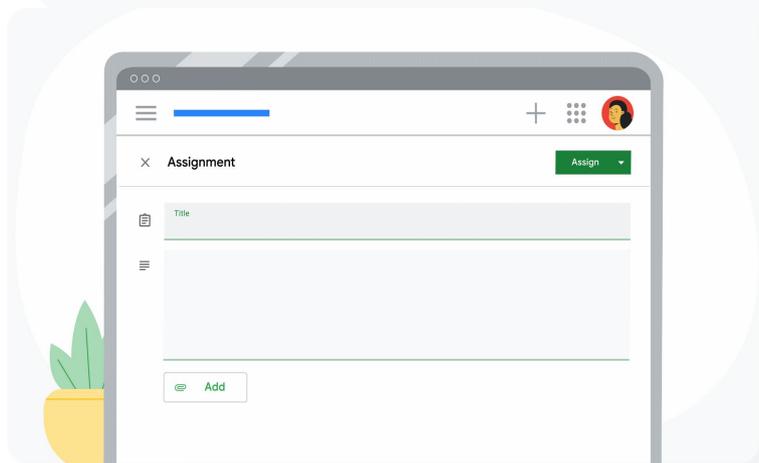
操作說明：在 Classroom 中結合引人入勝的內容

如何在作業、測驗或問題中附加外掛程式

- 透過 classroom.google.com 登入 Classroom 帳戶
- 從清單中選取相關課程，並選擇「課堂作業」
- 選取「建立」> 選取要建立的項目
- 輸入標題和說明
- 在「外掛程式」下方，選擇要使用的外掛程式
- 選取「指派」

如何在公告中附加外掛程式

- 在課堂「訊息串」頁面中，選取「要在課程中宣布的事項」
- 輸入公告內容
- 在「外掛程式」下方，選擇要使用的外掛程式
- 選取「發布」



[🔗 說明中心相關文件](#)

- [在 Classroom 中使用外掛程式](#)
- [Classroom 外掛程式 \[教師專用入門指南\]](#)



「我需要在 Google Classroom 中自動設定課程，以及管理學生名單的方法。」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [認識學生資訊系統學生名單匯入功能](#)
- [透過 Clever 設定要匯入的學生資訊系統學生名單](#)

大規模建立課程

學生資訊系統的學生名單匯入功能可自動建立課程，並透過 Clever，讓課堂學生名單與貴校學生資訊系統保持同步。

- ✓ 適用於美國和加拿大幼兒園到高中學區，且須使用 Education Plus
- ✓ 管理員可以將學生名單從學生資訊系統匯出至 Google Classroom，以便自動設定課程
- ✓ 您可以輕鬆在 Google Classroom 中自動建立和管理課程名單

操作說明：大規模建立課程

如何設定學生資訊系統學生名單匯入作業

- 在 Clever 中設定 Google Classroom 學生名單同步處理作業
- Clever 學區管理員和 Google Workspace 超級管理員可以[按照 Clever 的逐步說明操作](#)

如果您的學區沒有 Clever 帳戶：

- 建立 [Clever 帳戶](#)

如果您的學區有 Clever 帳戶：

- 前往 [Clever 資訊主頁要求匯入學生名單](#)

 [說明中心相關文件](#)

- [透過 Clever 設定要匯入的學生資訊系統學生名單](#)



原創性報告

這是什麼？

原創性報告可讓教師和學生使用 Google 搜尋，將學生作業與數十億個網頁及 4 千多萬本書籍進行比對，檢查作業是否涉嫌抄襲。付費版功能可讓教師產生數量不限的原創性報告，掃描學校專有的非公開作業存放區記錄，找出是否有人涉嫌抄襲之前學生繳交的作業。

用途

[偵測抄襲內容](#)



[逐步操作說明](#)

[根據學生過往繳交的作業檢查原創性](#)

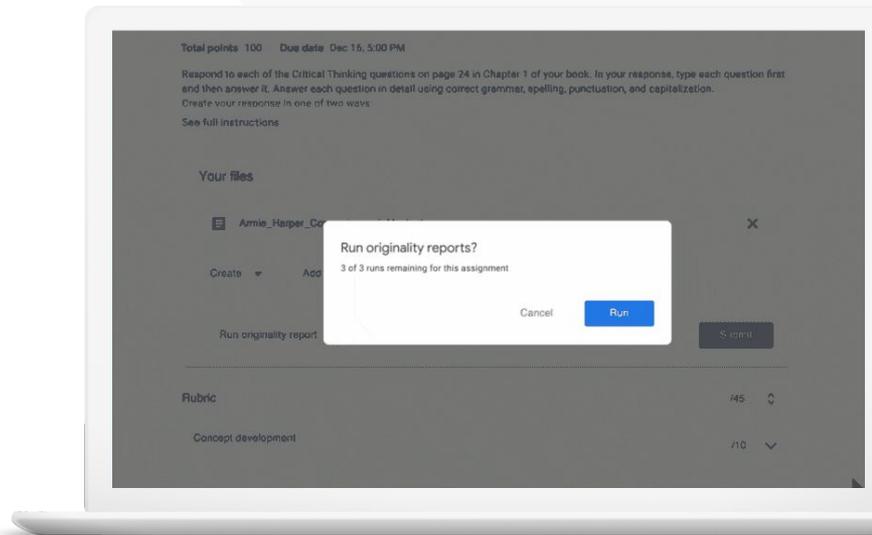


[逐步操作說明](#)

[將抄襲偵測功能變成學習機會](#)



[逐步操作說明](#)





「我想檢查學生的作業是否涉嫌抄襲，或含有不正確的引用出處。」

[🔗 逐步操作說明](#)

[🔗 說明中心相關文件](#)

- [開啟原創性報告功能](#)
- [原創性報告和隱私權](#)

偵測抄襲內容

原創性報告可以讓老師檢查學生的作業是否涉嫌抄襲，然後連結至偵測到的來源，並標記未註明引用出處的文字。



執行原創性報告，與 Google 文件、Google 簡報投和 Microsoft Word 檔案相互比對。



使用 Teaching and Learning Upgrade 或 Education Plus 的教師可獲得以下好處：

- 無限次產生原創性報告
- 透過學校專有的非公開作業存放區，比對學生作業是否抄襲過往的學生作業

機構的資料歸機構所有，我們的責任是確保這些資料的私密性與安全性。

操作說明：偵測抄襲內容

 原創性報告

 教學與學習工具

在 Classroom 中為作業啟用原創性報告

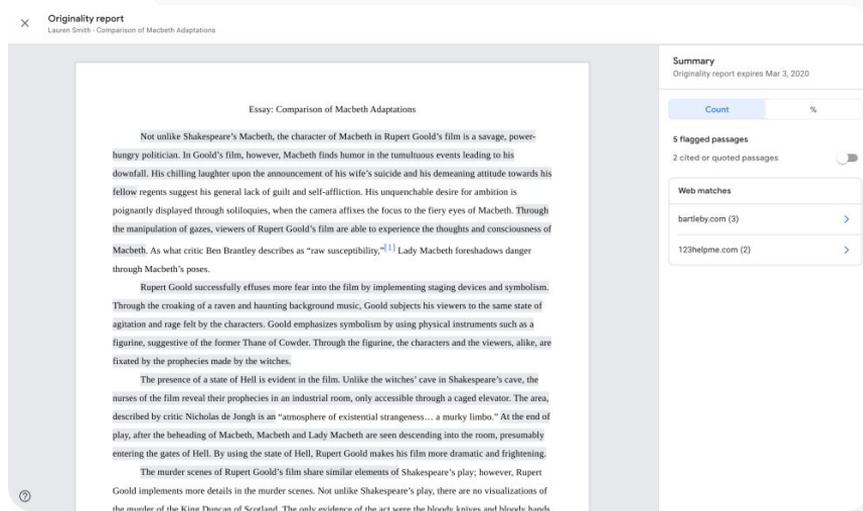
- 透過 classroom.google.com 登入 Classroom 帳戶
- 從清單中選取相關課程，並選擇「課堂作業」
- 依序選取「建立」>「作業」
- 勾選「原創性報告」旁的方塊來啟用報告

針對學生作業產生原創性報告

- 從清單中選取學生的檔案，按一下即可在評分工具中開啟檔案
- 在學生的作業下方點選「檢查原創性」

在學習管理系統 (LMS) 中為作業啟用原創性報告

- 登入您的學習管理系統
- 選取相關課程
- 建立作業 > 選取「Google 作業」
- 勾選「啟用原創性報告」旁的方塊



Originality report
Lauren Smith - Comparison of Macbeth Adaptations

Essay: Comparison of Macbeth Adaptations

Not unlike Shakespeare's Macbeth, the character of Macbeth in Rupert Goold's film is a savage, power-hungry politician. In Goold's film, however, Macbeth finds humor in the tumultuous events leading to his downfall. His chilling laughter upon the announcement of his wife's suicide and his demeaning attitude towards his fellow regents suggest his general lack of guilt and self-affliction. His unquenchable desire for ambition is poignantly displayed through soliloquies, when the camera affixes the focus to the fiery eyes of Macbeth. Through the manipulation of gazes, viewers of Rupert Goold's film are able to experience the thoughts and consciousness of Macbeth. As what critic Ben Brantley describes as "raw susceptibility,"^[1] Lady Macbeth foreshadows danger through Macbeth's poses.

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

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

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

Summary
Originality report expires Mar 3, 2020

Count %

5 flagged passages
2 cited or quoted passages

Web matches

bartleby.com (3)

123helpme.com (2)

 說明中心相關文件

- [Classroom: 開啟原創性報告功能](#)
- [Google 作業: 開啟原創性報告功能](#)



「我該如何讓教師比對學生寫的作業，是否抄襲過去幾年的學生作業？」

[逐步操作說明](#)

[說明中心相關文件](#)

- [開啟原創性報告功能](#)
- [在 Classroom 中開啟原創性報告的校內比對功能](#)

根據學生過往繳交的作業檢查原創性

原創性報告的校內對比功能可讓教師將學生作業和機構非公開存放區的學生作業進行掃描比對，找出是否涉嫌抄襲之前學生繳交的作業。



透過 Teaching and Learning Upgrade 或 Education Plus，教師可檢查學生新交的作業是否抄襲以前的作業

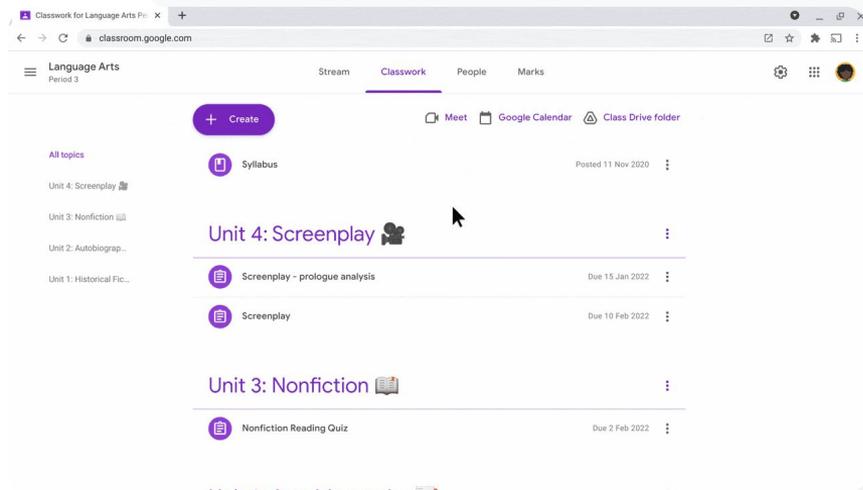


系統會以安全的方式儲存學生作業，並回放至學校專有的非公開全網域存放區中

操作說明：根據學生過往繳交的作業檢查原創性

如何開啟原創性報告的校內比對功能

- 在管理控制台中，依序選取「選單」>「應用程式」>「額外的 Google 服務」>「Classroom」
- 選取老師的機構單位
- 按一下「原創性報告」> 勾選「啟用原創性報告校內比對功能」方塊
- 按一下「儲存」



🔗 說明中心相關文件

- [在 Classroom 中開啟原創性報告的校內比對功能](#)



「我想提供學生一個學習機會，讓他們瞭解如何正確引用資料來源。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [針對作業產生原創性報告](#)

將抄襲偵測功能變成學習機會

學生在繳交每份作業前，最多可產生 3 次原創性報告，以便找出未註明引用出處和無意間抄襲的內容。原創性報告功能會針對各個來源比對學生作業，並標記未引用出處的文字，藉此讓學生有機會學習、修正錯誤，並在繳交作業時更有自信。



使用 Teaching and Learning Upgrade 和 Education Plus 的教師皆可產生無限次原創性報告，Education Fundamentals 的使用者則只能針對每堂課啟用 5 次報告。



學生繳交作業後，Classroom 會自動產生一份只有老師才能查看的報告。如果學生將作業取消繳交後再重新繳交，Classroom 會為老師建立另一份原創性報告。

操作說明：將抄襲防護措施變成學習機會

 原創性報告

 教學與學習工具

學生如何在 Classroom 中產生原創性報告

- 透過 classroom.google.com 登入 Classroom 帳戶
- 從清單中選取相關課程，並選擇「課堂作業」
- 選取清單中的相關作業，並點選「查看作業」
- 在「你的作業」下方，選取「上傳」或「建立檔案」
- 按一下「原創性報告」旁邊的「執行」
- 如要開啟報告，請點選檔案作業名稱下方的「查看原創性報告」
- 如要修改作業或是為標記的段落提供正確引用出處，請按一下底部的「編輯」

學生可以使用 Google 作業，在 [學習管理系統\(LMS\)](#) 中產生原創性報告。

Essay: Comparison of Macbeth adaptations

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

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

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

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

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

Web matches > sparksnotes.com ×

STUDENT'S PASSAGE

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

Comment

TOP MATCH

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

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

 說明中心相關文件

- [在 Classroom 中產生原創性報告](#)
- [在學習管理系統\(LMS\) 中產生原創性報告](#)



文件、試算表和簡報

這是什麼？

透過 Google 文件、試算表和簡報，學校社群成員可以即時地協作、共同製作內容、審核與編輯檔案，而且大家都能同步進行上述操作。有了 Education Plus 的付費版功能，教師和管理員即能針對機構所有內部文件實行核准程序。

用途

[核准內部文件](#)[逐步操作說明](#)



「物理與化學科正在開發新的課程。他們該如何確保課程提案已經過所有學科主管核准？」

[↪ 逐步操作說明](#)

[↪ 說明中心相關文件](#)

- [管理核准功能](#)

核准內部文件

學校社群可透過核准功能，將 Google 雲端硬碟中的文件透過正式程序送交核准。

- ✓ 審查者可以直接在 Google 雲端硬碟、Google 文件和其他 Google Workspace 應用程式內核准或拒絕文件，也可以在文件中加入意見回饋
- ✓ 核准者點選文件連結後，即可開始查看內容、在文件中加註，以及拒絕或核准文件
- ✓ 您可以管理合約或聘僱決定核准程序，或是在文件發布前進行修訂核准等

操作說明：核准內部文件

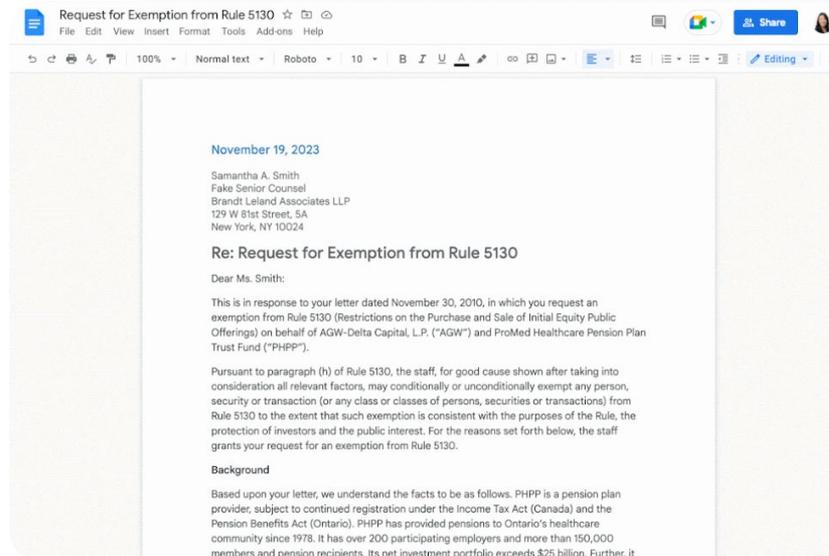
[文件、試算表和簡報](#)
[教學與學習工具](#)

運作方式

管理員可以控制使用者和檔案在核准程序中的牽涉程度。

如何管理核准功能

- 登入管理控制台 > 依序前往「選單」>「應用程式」>「Google Workspace」>「雲端硬碟與文件」
- 按一下「核准」
- 如要為所有使用者套用設定，請選取子機構單位，或是配置群組
- 按一下「儲存」


[說明中心相關文件](#)

- [管理核准功能](#)



這是什麼？

Google Meet 的進階功能包括直播、分組討論室、大型會議、會議內容錄製、即時翻譯字幕等。

用途

[錄製會議過程](#)



[逐步操作說明](#)

[參考課堂討論內容](#)



[逐步操作說明](#)

[克服語言隔閡](#)



[逐步操作說明](#)

[播送大型集會和學校活動](#)



[逐步操作說明](#)

[提出問題](#)



[逐步操作說明](#)

[收集意見](#)



[逐步操作說明](#)

[學生小組](#)



[逐步操作說明](#)

[追蹤出席狀況](#)



[逐步操作說明](#)



「我們機構提供大型線上專業培訓課程，且必須為無法出席的教師錄製課程內容。」

[逐步操作說明](#)

[說明中心相關文件](#)

- [錄製視訊會議內容](#)

錄製會議過程

有了 Teaching and Learning Upgrade 和 Education Plus，教師可以錄製課程、校務會議、專業培訓等活動內容。系統會自動將會議內容儲存至雲端硬碟。



錄製內容會儲存在會議發起人的雲端硬碟中。開始錄製之前，請確保雲端硬碟有足夠的空間

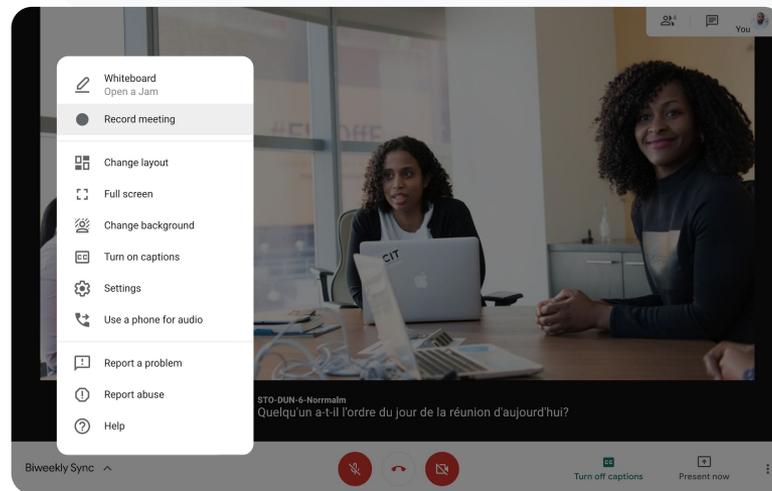


建議 IT 管理員僅針對教職員啟用錄製功能

操作說明：錄製會議過程

如何開始錄製會議

- 在 Google Meet 中發起或加入會議
- 依序點選「活動」圖示>「錄製」
- 選取「開始錄製」
- 在開啟的視窗中按一下「開始」
- 螢幕右下角會顯示紅點，表示系統正在錄製會議
- 該會議的影片檔案會自動儲存到您的雲端硬碟中



[說明中心相關文件](#)

- [錄製視訊會議內容](#)

操作說明：觀看及分享錄製內容

如何開始錄製會議

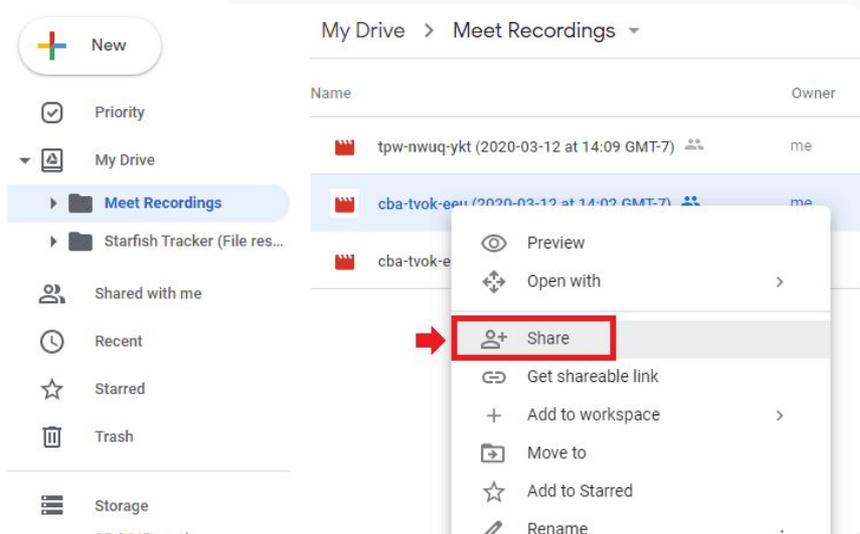
- 選取所需檔案
 - 按一下「分享」圖示
 - 新增核准的檢視者
- 或
- 選取「連結」圖示
 - 在電子郵件或即時通訊訊息中貼上連結

如何下載錄製內容

- 選取所需檔案
- 依序點選「更多」圖示>「下載」
- 在可下載的檔案上按兩下即可播放

如何播放雲端硬碟中的錄製內容

- 在雲端硬碟中按兩下錄製內容即可播放；在檔案可供線上觀看前，系統會顯示「仍在處理中」
- 如要將錄製內容新增至「我的雲端硬碟」，請選取檔案並按一下「新增至我的雲端硬碟」



[說明中心相關文件](#)

- [錄製視訊會議內容](#)



「我該如何轉錄線上課程，讓學生在課後複習相關概念？」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [搭配使用轉錄稿與 Google Meet](#)
- [開啟或關閉會議語音轉錄功能](#)

參考課堂討論內容

有了會議轉錄稿，教師可以自動擷取課程與課堂討論內容，讓學生輕鬆複習課堂上傳授的概念。轉錄功能會追蹤會議出席狀況，並顯示會議期間發言對象及內容。

- ✔ 為使用電腦或筆記型電腦的 Google Meet 使用者提供英文版。
- ✔ 管理員可以為學校社群啟用語音轉錄功能。
- ✔ 系統會自動將轉錄稿儲存至會議主辦人的雲端硬碟中。
- ✔ 開啟會議轉錄稿後，會議的所有參與者都可在畫面左上方看到「轉錄稿」圖示。
- ✔ 轉錄稿包含會議期間的發言內容。如需即時通訊訊息轉錄稿，請[錄製會議](#)。

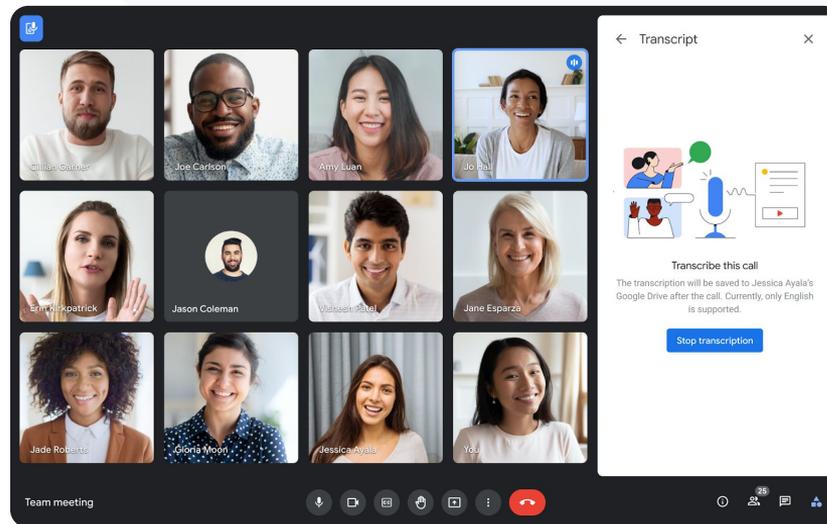
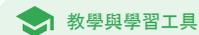
操作說明：參考課堂討論內容

如何在 Google Meet 中開啟轉錄稿功能

- 在會議中，選取右下角的「活動」圖示
- 依序選取「轉錄稿」圖示>「開始語音轉錄」>「開始」

如何在 Google Meet 中停止語音轉錄

- 依序選取「活動」圖示 > 「轉錄稿」圖示 > 「停止語音轉錄」> 「停止」



說明中心相關文件

- [搭配使用轉錄稿與 Google Meet](#)
- [開啟或關閉會議語音轉錄功能](#)



「我們會舉辦虛擬親師座談會，但有時候我們使用的語言不同。我該如何讓會議更多元包容，並克服語言隔閡？」

[↪ 逐步操作說明](#)

[↪ 說明中心相關文件](#)

- [在 Google Meet 中使用翻譯字幕功能](#)

克服語言隔閡

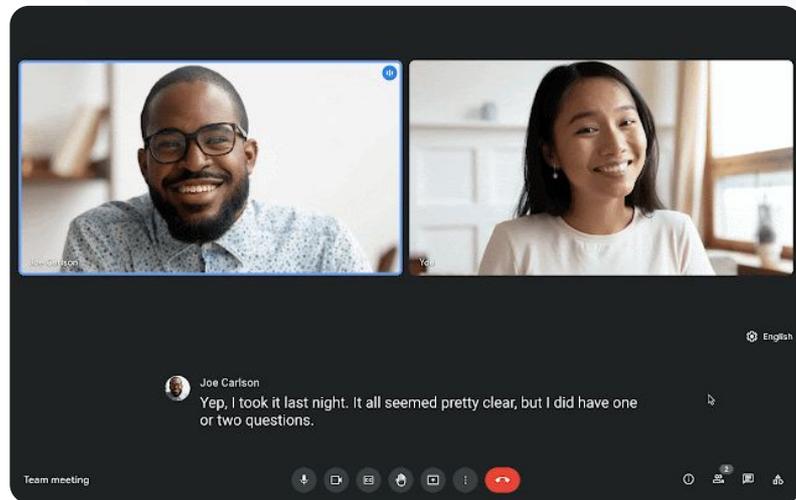
翻譯字幕能夠消除因語言程度不同而造成的隔閡，讓會議更加多元包容。讓會議參與者以偏好的語言觀看內容，有助於促進平等的資訊共享、學習與協同合作機會。

- ✓ 教師可以和使用不同語言的學生、家長及社群相關人士交流互動
- ✓ 您可以使用翻譯字幕功能，將英文與法文、德文、葡萄牙文或西班牙文互譯
- ✓ 也能將英文翻譯成日文、中文或瑞典文

操作說明: 克服語言隔閡

如何開啟翻譯字幕功能

- 在會議中，點選畫面底部的「更多控制項」圖示>「設定」圖示>「字幕」圖示
- 開啟「字幕」
- 選取「會議語言」
- 開啟「翻譯字幕」
- 選取字幕語言



[說明中心相關文件](#)

- [在 Google Meet 中使用翻譯字幕功能](#)



「我們需要直播教職員會議，以便供眾多相關人員和家長觀看。」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [開啟或關閉 Meet 直播功能](#)
- [直播視訊會議](#)

播送大型集會、學校活動和會議

使用 Teaching and Learning Upgrade 進行直播，最多可讓 1 萬名觀眾同步觀看；Education Plus 最多則可讓 10 萬名觀眾觀看。參與者可以點選發起人在電子郵件中提供的直播連結，或是透過日曆邀請加入會議。



決定直播分享範圍，並選擇能夠觀看直播的對象：

- 只供貴機構網域內的使用者觀看
- 與其他信任的 Google Workspace 網域分享
- 是否可透過 YouTube 觀看



建議 IT 管理員僅針對教職員啟用直播功能



如果使用者錯過直播，可以在會議結束後觀看重播



在直播中加入字幕、意見調查和問與答，有助於增進多元包容性和參與度

操作說明：播送大型集會、學校活動和會議

如何建立直播活動

- 開啟 Google 日曆
- 選取「+ 建立」>「活動」>「更多選項」
- 新增活動詳細資料，例如日期、時間和說明
- 新增在視訊會議中具備完整存取權限的邀請對象，這表示受邀者能看到彼此的影像，聽到彼此的發言，也能分享自己的螢幕畫面
- 點選「新增 Google 視訊會議」
- 選取「使用 Google Meet 加入會議」旁的向下箭頭來新增直播
- 如要在網域內邀請貴機構使用的付費版本允許的上限人數，請點選複製直播網址，並分享連結
- 選取「儲存」
- 系統不會自動開始直播；請在會議開始後，選取「更多」>「開始串流播放」



說明中心相關文件

- [開啟或關閉 Meet 直播功能](#)
- [直播視訊會議](#)



「我需要快速張貼問題、評估學生知識，並在課程中和學生互動以維持他們的參與度。」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [在 Google Meet 中向參與者提問](#)

提出問題

使用 Google Meet 的問與答功能維持學生參與度，並增加課程中的互動。教師還可以在虛擬課程結束時，取得所有問與答的詳細報告。



主持人可視需求盡情提問，不受次數限制。還可以過濾問題、將問題加以分類、標示為已回答，甚至是隱藏或優先顯示問題。



在啟用問與答功能的會議結束後，系統會透過電子郵件自動傳送問題報告給主持人。

操作說明：提出問題



提出問題

- 在會議中，依序選取右上角的「活動」圖示「問題」(如要開啟問與答功能，請選取「開啟問與答」)
- 如要提問，請點選右下角的「提出問題」
- 輸入問題 > 點選「張貼」

查看問題報告

- 會議結束後，主持人會收到含有問題報告的電子郵件
- 開啟電子郵件 > 按一下報告中的附件



說明中心相關文件

- [在 Google Meet 中向參與者提問](#)



「我需要在主導課程或教職員會議時，快速收集學生和其他教師的想法。」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [在 Google Meet 中進行意見調查](#)

收集意見

預先排定或發起虛擬會議的使用者可以為與會者建立意見調查。這項功能可以協助主持人快速收集所有與會學生或參與者的資訊。



主持人可以預先儲存意見調查，等到會議開始進行後再張貼。意見調查會儲存在虛擬會議中的「意見調查」專區，方便主持人管理。



會議結束後，系統會透過電子郵件自動將意見調查結果傳送給主持人。

操作說明：收集意見



建立意見調查

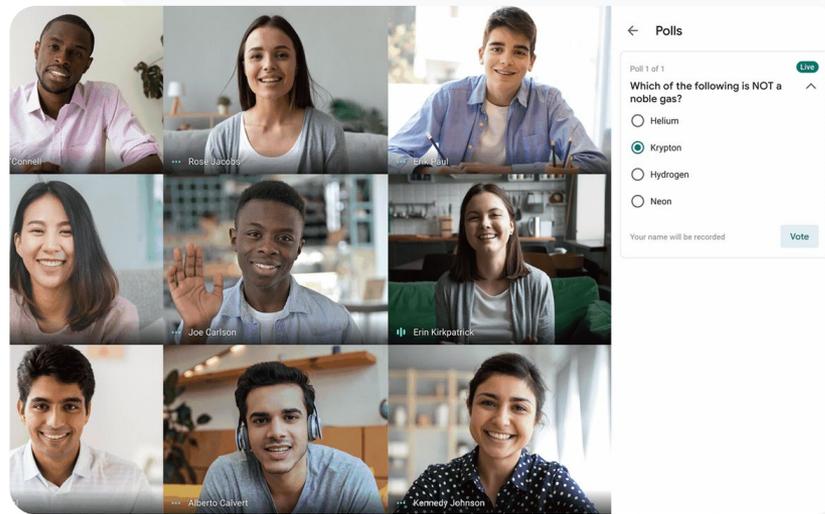
- 在會議中，依序選取右上角的「活動」圖示 >「意見調查」
- 選取「發起意見調查」
- 輸入問題
- 選取「發布」或「儲存」

進行意見調查

- 在會議中，依序選取右上角的「活動」圖示 >「意見調查」
- 如要讓參與者即時查看意見調查結果，請在「對所有人顯示結果」旁選取「切換為開啟」
- 如要關閉意見調查並禁止回覆，請按一下「結束意見調查」
- 如要永久刪除某個意見調查，請選取「刪除」圖示

查看意見調查報告

- 會議結束後，主持人會收到含有報告的電子郵件
- 開啟電子郵件 > 選取報告中的附件



[🔗 說明中心相關文件](#)

- [在 Google Meet 中進行意見調查](#)



「學生有時候會在家遠端學習，而在進入小組作業的環節時，我需要一個輕鬆便捷的方式，根據預先定義的群組建立分組討論室。」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [使用 Google Meet 的分組討論室功能](#)

學生小組

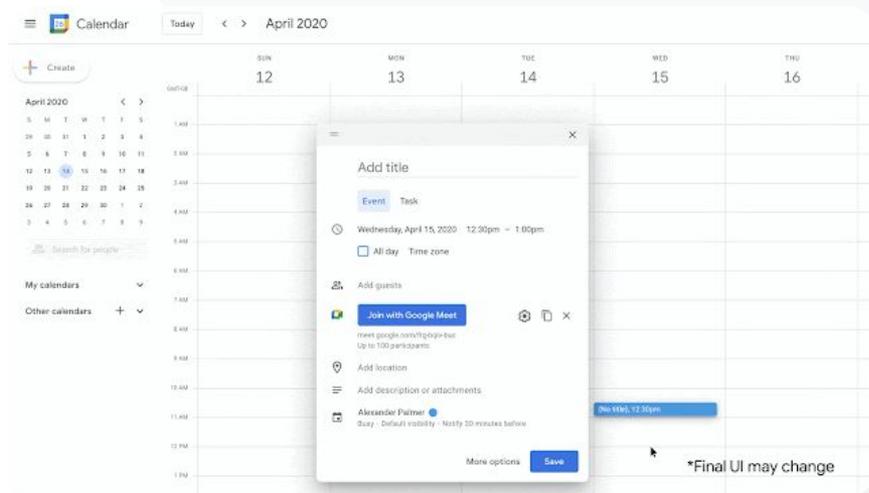
教師可以使用分組討論室功能，將虛擬、混合或面對面教學課程中的學生分成多個小組。主持人必須使用電腦，才能在視訊通話期間建立分組討論室。

-  分組討論室能夠在建立活動時預先建立，或是在會議進行期間建立
-  每場虛擬會議最多可以建立 100 間分組討論室
-  老師可以輕鬆在分組討論室間移動，為有需要的小組提供協助
-  管理員可以確保只有教職員能建立分組討論室

操作說明: 建立學生小組

在會議開始前建立分組討論室

- 建立新的 Google 日曆活動
- 按一下「新增 Google Meet 視訊會議」
- 新增參與者 > 選取「變更會議設定」
- 按一下「分組討論室」
- 選擇分組討論室的數量，並執行下列任一項操作：
 - 將參與者拖曳至不同分組討論室中
 - 直接在分組討論室中輸入參與者的名稱
 - 按一下「隨機分組」圖示即可打散分組
- 按一下「儲存」



[說明中心相關文件](#)

- [使用 Google Meet 的分組討論室功能](#)

操作說明：建立學生小組

在會議期間建立分組討論室

- 發起視訊通話
- 選取右上方的「活動」圖示>「分組討論室」
- 在分組討論室面板中，選擇需要的分組討論室數量
- 系統會自動將學生分配到各個討論室，但主持人能視情況手動將學生移到不同的討論室
- 按一下右下方的「開啟分組討論室」

在不同的分組討論室中回答問題

- 參與者尋求協助時，主持人的螢幕下方會顯示通知。如要加入參與者的分組討論室，請選取「加入」



[🔗 說明中心相關文件](#)

- [使用 Google Meet 的分組討論室功能](#)



「我們難以追蹤有誰參與了線上課程。我需要便捷的回報機制，進而掌握整個網域內的課程出席狀況。」

 [逐步操作說明](#)

 [說明中心相關文件](#)

- [追蹤 Google Meet 會議的出席情況](#)

追蹤出席狀況

出席狀況追蹤功能可針對有 5 位以上參與者的會議，自動產生出席狀況報告。報告會顯示加入通話的參與者、他們的電子郵件，以及待在虛擬課程中的時間。



您可以使用直播報告來追蹤直播活動期間的出席狀況



主持人可以在會議或日曆活動中，選擇是否要開啟出席狀況追蹤功能和直播報告

操作說明：追蹤出席狀況

如何在會議中追蹤出席狀況

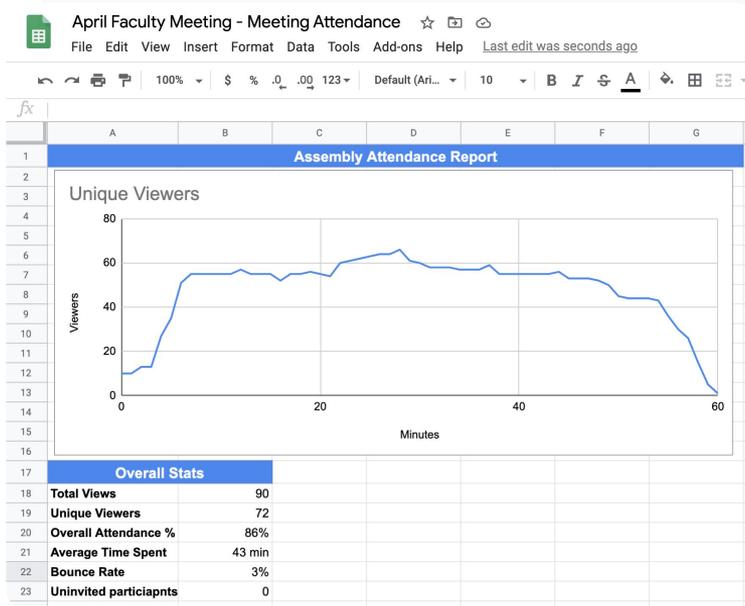
- 發起視訊通話
- 選取底部的「選單」圖示
- 依序選取「設定」圖示>「主辦人控制項」
- 開啟或關閉出席狀況追蹤

如何在 Google 日曆中追蹤出席狀況

- 在日曆活動中啟用 Google Meet 會議通訊
- 選取畫面右側的「設定」圖示
- 勾選「出席狀況追蹤」旁的方塊> 按一下「儲存」

取得出席狀況報告

- 會議結束後，主持人會收到含有報告的電子郵件
- 開啟電子郵件 > 選取報告附件



[說明中心相關文件](#)

- [追蹤 Google Meet 會議的出席情況](#)

謝謝您