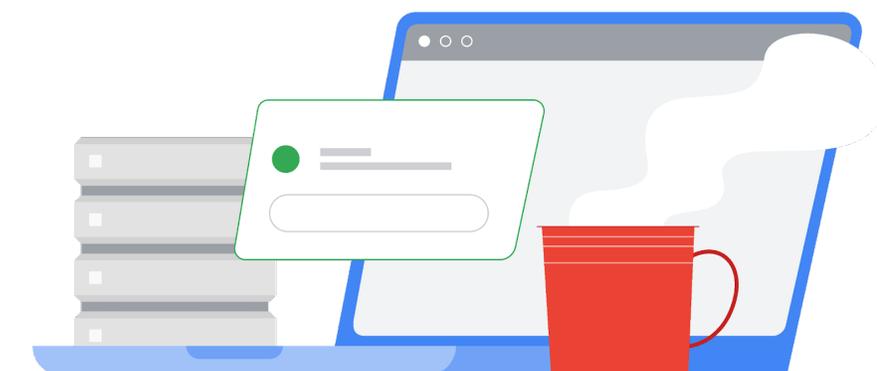


Google for Education

ChromeOS

機群監控最佳做法指南

2023 年 2 月

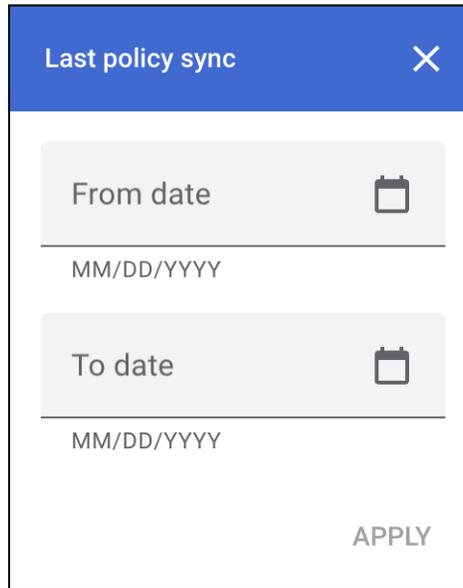


目錄

尋找最近未曾同步政策的裝置	2
偵測使用者是否反覆重新註冊裝置	4
如果您使用的是 Workspace for Education Plus 或 Standard	4
調查裝置	4
針對重新註冊建立活動規則	5
如果您使用的是 Workspace for Education Fundamentals	5
篩選稽核記錄	5
禁止使用者註冊未經授權的裝置	6
監控透過已取消註冊裝置登入的使用者	6
偵測已加入受管理網路但未受管理的裝置	6
建議設定	7

尋找最近未曾同步政策的裝置

在管理控制台中，依序前往「裝置」>「Chrome」>「裝置」，即可查看[所有裝置的報告](#)，裝置會依照上次同步的時間排序。如要顯示曾在特定時間範圍內進行同步的裝置，您可以在清單中新增篩選條件。舉例來說，管理員可以針對「上次同步處理政策時間」設定篩選條件，將「開始日期」與「結束日期」分別設為 2022/01/01 與 2023/01/13，如此一來便只會顯示自 2023 年 1 月 13 日或今年年初起皆未曾同步政策的裝置。



Last policy sync

From date 

MM/DD/YYYY

To date 

MM/DD/YYYY

APPLY

您可以編輯這份裝置清單的資料欄，納入「最近的使用者」，以便顯示上次使用裝置的使用者（「使用者」欄位則是指註冊裝置的使用者，但有可能不是裝置的主要使用者）。如要編輯顯示的資料欄，請按一下齒輪圖示，接著按一下底部的「新增資料欄」，並選取「最近的使用者」。您也可以按一下「X」移除資料欄。完成後請點選「儲存」。

Manage columns	
Device list	
Serial number	
Status	
Asset ID	
Organizational unit (not currently visible)	
Online status (not currently visible)	
Enrollment time	
Last policy sync	
Location	
Most recent user	
 Last user activity	
<i>Add new column</i>	
CANCEL SAVE	

管理員也會自動收到[公司閒置裝置報告](#)，其中會指出在過去 30 天內都未曾同步的公司裝置。

偵測使用者是否反覆重新註冊裝置

如果使用者反覆取消及重新註冊裝置，稽核記錄可擷取這項資訊並通知管理員。使用 Google Workspace for Education Plus 或 Standard 後，如果發生了這類的裝置重新註冊事件，即可觸發自動快訊或動作。

如果您使用的是 Workspace for Education Plus 或 Standard

調查裝置

如要進一步瞭解如何使用調查工具，請參閱「[調查工具](#)」。

- 依序前往「報表」→「調查」→「管理員記錄事件」
- 按一下「條件建構工具」
- 新增「事件」「為」「變更裝置狀態」的條件
- 新增「新值」「包含」「有效」的條件
- 按一下「結果分組依據」，並選取「Group By Resource ID(s)」(依資源 ID 分組)

The screenshot displays the 'Condition builder' interface in the Google Workspace Admin console. At the top, there's a search bar with 'Search 1' and options like 'Create activity rule', 'Create custom chart', and 'Discard search'. Below the search bar, there's a dropdown for 'Admin log events' and a 'Filter' button. The main area is titled 'Condition builder' and shows a logical operator 'AND' at the top. Two conditions are listed: 'Event' is 'Change Device State' and 'New value' 'Contains' 'ACTIVE'. Below the conditions is an 'ADD CONDITION' button. At the bottom, there's a 'Group results by' dropdown set to 'Resource ID(s)' and a 'SEARCH' button.

- 按一下「搜尋」

如果特定裝置頻繁發生重新註冊的情況，可能表示使用者是刻意取消註冊裝置再加以重新註冊。

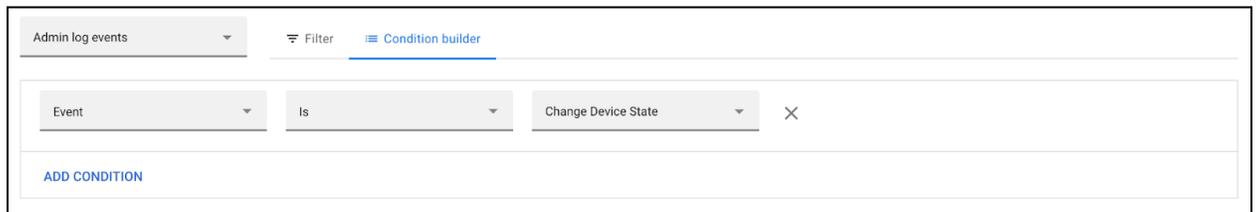
針對重新註冊建立活動規則

選用:按一下頂端的「建立活動規則」, 將此搜尋儲存為規則, 以傳送自動通知。因為系統可能會有誤判的情況, 因此目前不建議自動將重新註冊裝置的使用者停權。如要進一步瞭解如何建立活動規則, 請參閱「[建立及管理活動規則](#)」。

如果您使用的是 Workspace for Education Fundamentals

篩選稽核記錄

- 依序前往「報表」→「調查」→「[管理員記錄事件](#)」
- 按一下「條件建構工具」
- 新增「事件」「為」「變更裝置狀態」的條件



The screenshot shows the 'Condition builder' interface. At the top, there is a dropdown menu for 'Admin log events' and a 'Filter' button. Below this, there is a 'Condition builder' section with a dropdown for 'Event', a dropdown for 'Is', and a dropdown for 'Change Device State'. There is also a close button (X) next to the 'Change Device State' dropdown. Below the condition builder is an 'ADD CONDITION' button.

- 按一下「搜尋」。

根據預設, 畫面上應會顯示「資源 ID」及「說明」欄。

按一下「全部匯出」, 將結果匯出到 Google 試算表。輸入匯出的檔案名稱, 然後按一下「匯出」。

匯出完成後, 向下捲動至「Export action results」(匯出動作執行結果), 然後按一下匯出檔案名稱, 即可開啟 Google 試算表。

新增一個資料欄並在說明中加入測試文字「有效到有效」, 藉此找出重新註冊的裝置。請參閱下方範例公式, 其中 C 代表「說明」欄位。將試算表的儲存格 E1 設為此公式:

```
=Arrayformula(if(row(C:C)=1, "已重新註冊", REGEXMATCH(C:C, "有效到有效")))
```

將欄標題「資源 ID」及「已重新註冊」分別當做列及欄, 並將任一其他欄位 (例如欄標題「執行者」) 的計數當做值, 以此[插入資料透視表](#)。

禁止使用者註冊未經授權的裝置

有些機構允許使用者註冊或重新註冊裝置。這項權限可讓使用者在學校或公司重新註冊裝置, 並在離開網路時取消註冊。管理員如不希望使用者能輕易自行重新註冊裝置, 可考慮對使用者停用此權限; 如果想讓使用者執行這項操作, 則可啟用此權限。

如要切換這項設定，請在管理控制台中依序前往「裝置」>「Chrome」>「設定」>「[使用者與瀏覽器](#)」。在左欄選取相關的機構單位 (例如「學生」)。在「註冊控制項」下的「註冊權限」中，選取「不允許這個機構中的使用者註冊新裝置或重新註冊現有裝置」，以禁止使用者註冊裝置；您也可以選取「僅允許這個機構中的使用者重新註冊現有的裝置 (不得註冊新裝置或已取消佈建的裝置)」，允許使用者重新註冊現有的裝置。

監控透過已取消註冊裝置登入的使用者

您可以變更裝置政策的視覺設定，以便老師或員工能夠更輕鬆地找出未受管理的裝置。這項變更只會套用到目前受管理的裝置。未受管理的裝置則不會顯示這項變更。

管理員可將裝置設定為[一律在登入畫面中顯示系統資訊](#)。未受管理的裝置不會顯示「管理者」或系統資訊。此外，[登入桌布](#)也可變更為受保護的圖片。

管理員可在控制台內監控[裝置清單](#)，檢視近期使用者所進行的政策同步。將預期的使用者清單與最近同步政策的使用者進行交叉比對，即可傳回尚未同步裝置的潛在使用者清單。您可進一步監控這些剩餘的裝置，在必要時實際調查其註冊狀態。

偵測已加入受管理網路但未受管理的裝置

如果有 Chromebook 以未受管理的狀態加入您的 Wi-Fi 網路，您可以快速找出有哪些 Chromebook 應該受到管理。管理員可以使用 [DeviceHostnameTemplate](#) 政策來指定主機名稱格式，其中可包含序號和/或資產標記 ID。此主機名稱會顯示在網路 DHCP 資料表中。如果加入受管理網路的裝置使用的是已知 MAC 位址，卻沒有正確的主機名稱，該裝置極有可能是取消註冊的裝置。

例如：在管理控制台中，依序前往「裝置」>「Chrome」>「設定」>「裝置」，然後向下捲動至「其他設定」下的「裝置網路主機名稱範本」。將「ManagedChromebook- $\{SERIAL_NUM\}$ 」的網路主機名稱範本政策套用至受管理的 Chromebook。如此一來，這些 Chromebook 便會以設定好且易於辨識的主機名稱顯示在學校網路的 DHCP 集區中。該 SSID/網路上的所有其他租約則會以通用或未定義的主機名稱顯示。您可以將這些通用或未定義主機名稱的 MAC 位址匯出，並與匯出的 Workspace 用戶群已知 MAC 位址進行比較，這樣做應該可協助您找出取消註冊的裝置。

如要匯出裝置及其 Wi-Fi MAC 位址的清單，請在管理控制台中依序前往「裝置」>「Chrome」>「裝置」，選取所需的機構單位，然後按一下清單上方的「匯出」。按一下右上角的沙漏圖示，匯出流程即會顯示在工作清單中。完成後，您就可以下載 CSV 查看結果。「macAddress」欄會包含 WiFi MAC 位址 (不含冒號字元)。

接下來，管理員便可對找到的裝置執行多項操作，例如：追蹤裝置/使用者；完全封鎖 MAC 位址，不讓其加入網路；或將這些裝置區隔至存取權受限的 VLAN。網路管理員可以利用內容篩選器或網頁認證入口系統，將找出的這些裝置重新導向至指引頁面，告訴使用者如何與 IT 人員聯繫以尋求協助，或如何重新註冊裝置 (如果管理員允許重新註冊)。

建議設定

- [強制重新註冊](#)：設定為「抹除裝置資料後，強制自動重新註冊裝置」。請參閱[強制重新註冊支援文章](#)
- [恢復原廠設定](#)：除所選使用者外，將所有人設定為「禁止觸發 Powerwash」。請參閱[恢復原廠設定支援文章](#)
- [驗證模式](#)：設定為「『已驗證存取權』需要以已驗證模式啟動」。請參閱[驗證模式支援文章](#)
- [已驗證存取權](#)：設定為「啟用內容保護」。請參閱[已驗證存取權支援文章](#)
- [重新註冊裝置的權限](#)：選取允許使用者重新註冊裝置的特定機構單位。[註冊權限支援文章](#)
- [禁止存取](#)下列內部網址：

```
chrome://policy
chrome://net-export
chrome://prefs-internals
chrome://version
chrome://kill
chrome://hang
```