

JAMF SAFE INTERNET

# 走到哪，學到哪，安全 的私人連線一路伴隨



由 Jamf 的「內容過濾」和網路威脅防護引擎提供支援，Jamf Safe Internet 旨在協助校園保護學生、職員與網路免受不良內容影響

現今學生的上網時間幾乎是以往的兩倍，消除網路攻擊，與避免學生造訪不安全內容的數位安全需求也因此水漲船高。Jamf Safe Internet 是一個專為教育打造的「內容過濾」和資安解決方案，它採用 Jamf 開發的資安工具，並結合一流的網路威脅防禦機制和龐大的內容過濾資料庫，以阻止惡意軟體或網路釣魚等不安全的內容和惡意攻擊，並可與我們的旗艦版教育行動裝置管理解決方案 Jamf School 順暢整合。

## 永不間斷的網路安全

在教育領域裡，為維持學習的永續性，保障教職人員與學生的個資，並消除資安攻擊引發的其他潛在風險，則勢必具備保護網路遠離資安攻擊的能力。

透過機器學習工具，Jamf Safe Internet 可識別和修復網路釣魚、惡意軟體、挖礦劫持和其他形式的網路攻擊，確保機構與機構內部網路的安全。



## 實施瀏覽限制

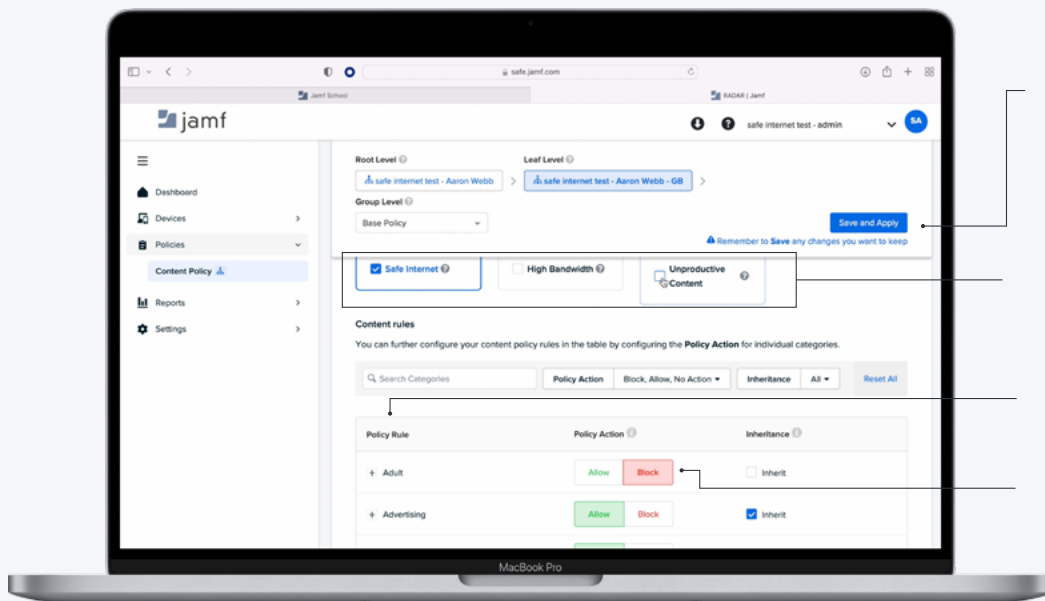
以 Jamf Safe Internet 啟用 YouTube 的「嚴格篩選模式」與 Google 的「安全搜尋」。藉由此功能隱藏 YouTube 搜尋、留言區、嵌入式 YouTube 影片以及 Google 搜尋結果中的露骨內容。

## 內容過濾資料庫

Jamf Safe Internet 可與 MDM 系統深度整合，並針對教育需求改良，為使用者與教育界提供簡單卻強大的全方位內容過濾機制。Jamf Safe Internet 運用輕量級高性能網域名稱系統 (DNS) 技術，允許管理者建立和自訂符合其學校需求的內容篩選結果，全程不侵犯使用者的隱私。

## 自訂控制內容

你可訂定符合自身需求的資安與過濾範圍，或者也可以直接選用 Safe Internet 的預設配置。



只需點選「Save and Apply」  
(儲存並套用) 便可輕鬆更新設定

預先定義規則，讓你可以直接啟用內容過濾機制

可防止多種類型的不良內容

一鍵即可封鎖特定內容

## 裝置端內容過濾 (ODCF)

避免終端使用者以 IP 位址造訪網站的方式來繞過域名型規範。ODCF 首先在限制性沙盒中檢查流量，並在流量離開沙盒時將敏感資料去除，確保提供使用者強大且兼顧隱私的體驗 (僅適用於 Apple 裝置)。

## 提升教育體驗

專為教職人員設計的工作流程與控制介面，並以你原先熟悉的平台與 Jamf School 深度整合，使部署流程與進行中的同步動作變得更加直覺好用。Jamf Safe Internet 也可與 **Jamf Pro** 密切整合。另外，裝置從開箱那一刻起，便可與 **Chromebook** 和 **Windows** 裝置相容。

了解 [Jamf Safe Internet](#) 如何與你的 MDM 平台搭配運作，確保教育科技持續將數位安全與資安放在首要位置



[www.jamf.com/zh-tw/](http://www.jamf.com/zh-tw/)

© 2002–2024 Jamf, LLC. 著作權所有，並保留一切權利

如欲進一步了解 Jamf Safe Internet 是如何確保學生與使用者的安全，歡迎前往 [jamf.com/zh-tw/](http://jamf.com/zh-tw/)