



1,000 台裝置，1 位 IT 管理員：

如何在教育領域擴展 Apple 裝置管理與資安防護

前言：比例問題

學校投資科技有明確目標：為每位學生落實個人化學習、擴大學習資源可近性，並提升學習成效。這項投資反映在裝置機群不斷成長、1:1 計畫擴展，以及更致力於提供符合學生需求、支援最佳學習模式的數位工具。

但隨著裝置數量增加，當部署規模超越[教育界平均 1000:1 的裝置與 IT 支援比例](#)時，學習環境的營運壓力會加倍累積。當這種情況發生時，教育營運便會失序紊亂，變得難以維持。

結果為何？IT 團隊會持續處於「滅火模式」，技術人員忙於處理各種問題，無法專注運用其專業技能，開發能為所有使用者創造價值的改善方案。

當核心的裝置生命週期管理任務，例如：

- 裝置佈建
- 修補程式管理
- 安全性監測
- 事件應變
- 安全退役

以有限 IT 資源在數千甚至數萬個端點上以手動方式執行時，即使是通常只需幾分鐘就能解決的例行任務，例如：

- 重設密碼
- 安裝 App
- 設定 Wi-Fi 連線

卻需要耗費超乎尋常的漫長等待時間才能解決，這完全是因為請求數量與可處理待辦問題的人員數量之間存在巨大落差。

總結起來就是一個詞：失衡。

失衡會引發各種中斷

而這會在整個機構中引發漣漪效應。

課堂中，連線問題經常阻礙數位資源存取；一旦發生，教育工作者經常成為第一線支援，被迫在課程中從教學轉為故障排除。

對學生而言，失衡會帶來使用阻力。原本旨在提升教學的科技，當裝置反應遲緩、應用程式閃退時，反而讓學習者感到挫折，分散了他們對眼前任務的注意力。

隨著時間推移，失衡的壓力會不斷累積。學生與教師之間的差距日益擴大，進而導致教育工作者與學校本身之間的錯位。從學生因故障的科技而無法學習，到機構本身受到教育目標和預期成效的負面影響，可以追溯出一條共同的脈絡。

這些影響都只是更大問題的症狀，卻揭露了一個更廣泛的策略問題：學校或許能順利分發裝置，但如果缺乏可擴展的管理與支援流程整合進整體 IT 策略中，機構將難以實現科技原本要實現的學習成效。科技不但沒有彌平數位落差，反而因為可靠性、可用性與安全性未能對齊學生、教師和學校的需求，而製造出額外的障礙。

手動流程的成本

手動佈建一台裝置平均需耗費 2-4 小時。以最低工時計算，結果如下：

$$\begin{array}{ccccc} \mathbf{1,000} & \times & \mathbf{2} & = & \mathbf{2,000} \\ \text{台裝置} & & \text{小時} & & \text{佈建工時} \end{array}$$

現在對比實際可用的工時。學校通常每週運作 5 天、每天 8 小時。暑假是年度換裝的主要期間，平均為 10 週。

$$\begin{array}{ccccc} \mathbf{8} & \times & \mathbf{10} & = & \mathbf{400} \\ \text{小時} & & \text{週} & & \text{每位 IT 人員工時} \end{array}$$

以 400 小時完成 2,000 小時的工作量。這還未計入裝置組態錯誤、流程疲勞，或其他會讓佈建時間逼近 4 小時上限的不可避免變因。

手動流程從來不是為現代國民及學前教育裝置部署所需的規模經濟所設計。需求與實際能力的落差不是人力配置問題，而通常是架構問題。

準備階段

就裝置生命週期管理而言，規模是能否有效地將就緒狀態裝置交付使用者、並盡可能降低停機時間的關鍵。它還有另一層相似但略有微妙差異的含義：在這第二種情境下，擴展指的是能夠有效率地執行部署（包含持續的裝置維護），並將對教學營運的影響降至最低。

儘管它們常被視為彼此的同義詞，但本質上，它們是截然不同的概念，只是需要相同的解決方案來應對。

**先從 IT 領域中「擴展」的基本定義開始：
「在更多裝置上重複執行相同步驟」。**

有鑑於此，論及擴展時，無論機構是要部署新裝置、維持其合規性，或兩者兼顧，有三個關鍵要素必須納入考量：



不一致性：大規模標準化的重要性

建立標準的關鍵性就在於它是可擴展性的基石，也決定了擴展工作的成敗。為什麼標準如此重要？因為任何引入的變因，都會以不同且意想不到的方式影響裝置。

若未加以處理或考量，其影響範圍從輕微的不便，到嚴重到需要完全重新部署端點和/或學習所需的軟體、組態及系統設定。

標準化的第一步，是定義出「此裝置已準備好供指派的使用者使用」的裝置狀態。對學生而言，可以將此狀態視為「學習就緒」，它必須包含您學校、年級及其所選修課程的學生所需的一切項目，以便他們能以學習者的身分發揮最佳能力。

考量本白皮書的範圍，決定各校、各學生的「學習就緒」樣貌也許看似大同小異，但最終仍會因許多重要差異而有所不同，例如學生、教育工作者、學校、機構與區域需求。本白皮書的目標不在於提供所有可能存在的潛在標準組合，而是要強調學校主管與教育工作者定義「學習就緒」樣貌的重要性，以及讓 IT 將此標準納入其佈建工作流程，以確保每次部署的裝置都能滿足該使用者的基準需求。

擴增裝置數量 ≠ 擴展部署能力

制訂標準時的重要考量是其彈性能力。若標準過於僵化，一旦發生問題（必然會發生），標準將無法對應需求，導致額外停機，因為 IT 必須手動設定裝置以滿足特定使用情境的獨特需求。然而，如果標準太過寬鬆，就無法達成提供目標使用者所需必要工具的目標，同時也欠缺大規模的基礎管理能力與資安防護。這兩種極端都會導致 IT 必須手動設定裝置來滿足不同使用者需求。

彈性的關鍵在於平衡。涵蓋的軟硬體組態越多樣，標準就越通用，但相對地安全性也會降低。試想一下，部署一台內含教師用成績輸入 App 的 iPad 給學生；或是指派給老師的筆電，卻同時兼作推車上的共享學生裝置。當老師試圖儲存教案時，裝置卻跳出錯誤訊息，因為所有學生資料已將儲存空間完全用盡。

彈性的重點並不是裝置不能雙重用途。而是制定標準時必須把「使用目的」納入考量。這不只能更精準反映學校的獨特需求，也能符合使用者實際可用的軟硬體資源現況。如此一來，靈活性便內建其中，讓裝置可毫不費力地部署或重新佈建，同時讓學習或教學中的使用者，能安全存取順利履行職責所需的工具與資源。

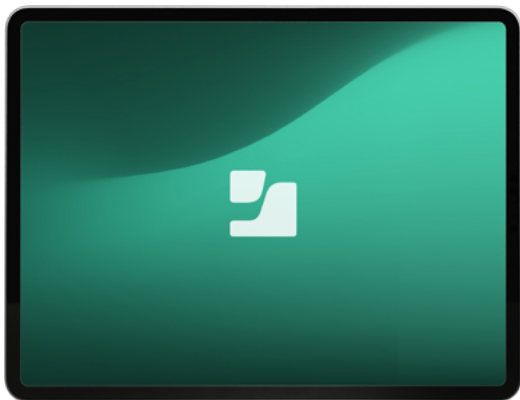
擴展規模在實務上的失效點

總結來說，標準提供每次部署時將裝置設定為學習就緒狀態的基礎框架。彈性衡量標準能否適應使用者需求變化，目標是盡量無縫運作，將對教學或 IT 營運的中斷降至最低。

在此情境下，效率取決於 IT 在整個裝置機群中彈性實現標準所花費的時間。由於各機構的裝置機群各不相同，效率並非以可量化的裝置數量來衡量。而是取決於現有工作流程能否無縫佈建、部署裝置給使用者，並在裝置生命週期中持續維運，無論是全班共用的 iPad 套組，還是跨年級、跨校區、跨區域部署的 1:1 MacBook 計畫。

試圖擴展規模時，仍依賴手動工作流程的學校經常卡在效率問題上。雖然佈建時最常見的問題是裝置組態錯誤或缺少必要軟體，但即便充分掌握使用者需求（標準化）、並考量影響機構計畫的變因（彈性），整個部署流程仍會崩壞，因為手動流程會隨裝置數量增加而呈指數級變得不穩定。

判斷高效率、可擴展工作流程的真正標準，是它能否像處理 1 台、10 台、100 台裝置一樣，穩定且輕鬆地處理 1,000 台（甚至 10,000 台）的部署作業，不中斷使用者、不影響營運、不讓 IT 團隊在過程中過勞。



引用 Apple 的設計理念：

「就是這麼好用。」



關鍵轉折：可重複性是擴展規模而不過勞的關鍵

談到擴展國民及學前教育裝置計畫時，最能引起共鳴的詞就是**可重複性**。在裝置機群中的多台裝置上重複執行相同步驟且不受變因影響的能力，能將營運負擔降至最低。

但究竟是什麼驅動力，能實現從被動到主動、從混亂到敏捷、從手動到協調式管理的轉變？

答案是自動化。具體來說，將多種工具整合為單一無縫架構，可讓裝置管理、身份識別與存取、端點資安工作流程協同運作，達成以下三大目標。這些目標正是實現可重複性擴展且不讓 IT 或技術團隊過勞的核心標誌：



資源

標準化軟硬體佈建，透過一致的使用者體驗支援教育目標。



成效

建立**彈性**工作流程，簡化學習工具存取，將教與學的中斷降到最低。



財務

透過運用科技帶來的**效率**消除手動繁瑣作業，重新配置教育預算，為機構帶來可觀的投資報酬率 (ROI)。

制訂部署策略的核心考量，並非一次將所有作業自動化，而是先評估學校、機構及 / 或區域的獨特需求，優先針對部署與裝置管理最關鍵的環節導入自動化，以率先取得自動化的最大效益。

專業建議：並非所有可自動化的項目都應該自動化，也不是所有自動化都能讓使用者從中受惠。

自動化的明確目標，是透過完善規劃的架構與可重複使用的整體工作流程，將重複性的手動任務轉換為可預測的作業，以滿足擴展需求（透過可重複流程實現自動化的一致性），而非透過強增人力來因應手動作業的需求。

後者只會帶來無止境的障礙。當 IT 試圖讓手動工作流程與教育目標對齊時，技術團隊仍會處於滅火模式，持續處理以下事項：

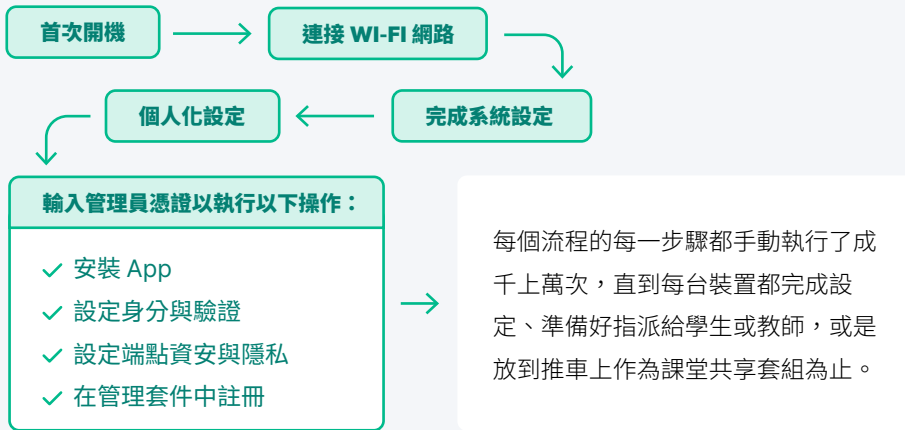
- 維護精準的軟硬體資源資產清單**，包含裝置與授權的指派。
- 主動監控裝置機群**並套用作業系統、軟體與資安更新，以降低有漏洞裝置帶來的風險。
- 為不同年級、不同校區的師生**設定裝置機群**，同時滿足各方的不同需求。
- 跨多個平台與裝置類型**強制執行基準合規規範**，同時提供統一報告與可供稽核的證明。
- 確保端點獲得完善防護**，以抵禦不斷演變的網路威脅，並依相關規範要求維護使用者的隱私。
- 處理服務呼叫與設備維修**，以及達到使用壽命 (EOL) 裝置的停用與報廢處理。

相反地，前者透過結合成統一解決方案的精密技術（我們將在本白皮書各章節中探討），「將理想的工作流程順暢地轉化為營運現實」。最終形成一套統一、完整的裝置生命週期管理策略，可實現以下目標：

- 隨著裝置計畫的增長而有效擴展。
- 為學習就緒裝置提供一致性與合規性。
- 支援學習目標與教育成效。
- 將焦點從手動設定轉為與教學保持一致。
- 採用可重複、自動化的部署模式。
- 透過可重複使用的工作流程赋能各種規模的 IT 團隊。

大規模註冊與佈建

IT 人員耗費大半的暑假時間，拆封新裝置、排成生產線、逐台親手操作設定：



然而，到了新學年的開學第一天。教師無法授課、學生無法學習，原因如下：

- ✘ 裝置無法連上 Wi-Fi
- ✘ 安全設定組態錯誤
- ✘ 使用者無法登入
- ✘ 教師裝置被套用了學生的個人化設定（反之亦然）
- ✘ 未安裝必要 App
- ✘ 並非所有裝置都能與 MDM 正常通訊

上述是一個真實案例，說明了自國民及學前教育採用科技以來，一直困擾全球學校的問題。

問題不在於「IT 不夠努力」，而是手動佈建流程從來就不是為了達到在緊湊時間內成功部署大型裝置機群所需的規模經濟而設計的。從人為限制到流程疲乏，再加上一點墨菲定律，裝置數量越龐大，壓力與不受控的變因就越會讓手動流程的裂痕變得更加明顯。

您不需要像哈利波特一樣會魔法才能做到這一點，因為這並非魔法，而是架構。

看著超過 1,000 台裝置在您的 MDM 中註冊，開箱即自動為目標使用者完成佈建，確實有種神奇的感覺——但可以說最棒的部分是，IT 人員完全不必親手觸碰就能完成所有作業。裝置只需開箱並開機，工作流程就會自動啟動。而且由於裝置可以在其餘工作流程執行時同時使用，讓使用者能夠更快地投入教學與學習。



手動設定一台裝置平均需耗費 2-4 小時，視組態需求而定。從被動（手動）轉為主動（自動化）工作流程後，**Mac 的設定時間可縮短至約 15 分鐘，iPad 更可進一步縮短至 5-7 分鐘。**



策略：更聰明地工作，而非更賣力地工作

擴展始於註冊。畢竟，沒有集中化管理、身分與安全機制的裝置機群，就像沒有堅固地基的房子。

有鑑於此，我們實現可擴展性的秘訣，仰賴三項密切配合的基本技術，以提供完全自動化的註冊與佈建工作流程。該流程可在班級、年級、學校、多個校區乃至整個區域，實現無縫執行。



透過 Apple School Manager (ASM) 實現自動註冊

從 Apple 或授權經銷商直接採購的 Apple 硬體，例如 Mac 電腦、iPad 和 Apple TV 裝置，都會連結到您的 ASM 帳號。此外，您的 Jamf 執行個體也會與 ASM 連結，建立一個傳遞通道，讓現有和未來的設備採購自動出現在 Jamf 中，簡化註冊流程。此外，將學生資訊系統 (SIS) 資料與 ASM 整合後，可輕鬆存取學生與教職員的資訊，節省為每位學生與教職員手動建立裝置資源存取憑證的大量工時。

簡單來說：透過 MDM 註冊裝置或建立受管理 Apple ID，完全不需要手動輸入或繁瑣作業，一切都已自動完成。



透過 Jamf，隨需求成長擴展核心管理功能

Jamf 是一套專屬打造的單一解決方案，可將複雜度降至最低，並在裝置管理時作為唯一的真實資料來源。同樣重要的是，它透過原生整合裝置管理、身分與存取管理、端點資安，大幅降低國民及學前教育裝置機群在整個生命週期的管理負擔。它同時支援國民及學前教育環境常用的工具，包括數位電子看板、學習管理系統 (LMS) 與統一報告功能，從註冊階段就奠定基礎，並作為後續每個階段的核心接觸點。實施基準安全態勢？沒問題。執行主動監控並觸發政策導向修復？也搞定了。維護最新資產清單並執行安全退役工作流程？全部都在 Jamf 內完成。



透過零接觸技術簡化裝置佈建

ASM 與 Jamf 的無縫整合，可為您的整個國民及學前教育基礎架構提供零接觸部署。無論是跨年級、跨多棟建築、在校內或校外擴展，裝置都能維持部署一致性，不論是新設備指派，或是需要重置以解決問題的裝置。裝置會依據使用者需求自動完成佈建，不僅一致性更高、耗時大幅縮短，還能減少中斷狀況與服務台工單請求，讓使用者更快進入生產狀態，同時釋放 IT 團隊的時間，專注於提供更優質的使用體驗。



跨校組態一致性

在本白皮書中，「不一致性」指的是變異性所帶來的問題。具體來說，它是裝置組態錯誤（又稱組態漂移）的首要成因，也是導致部署失敗的重要因素。

一般而言，組態漂移是裝置長期使用後的必然結果。即便是安裝 App、執行作業系統更新這類必要操作，都足以導致現有組態發生變更。話雖如此，也必須認知到，漂移也是執行重複性任務時，因人為疏忽而產生的副產品。一個步驟的遺漏或輕微的組態錯誤，每台裝置需要 30 秒手動修復，每 1,000 台裝置就會累積超過 8 小時因手動修正而損失的教學時間。

而這還只是單一事件中的一項資源耗損。試想，老師、學生、IT、主管和機構若能運用這些時間（或其所代表的同等財務效益），能成就多少事？

這個答案精準地突顯了一致性的重要性，也強調了大規模環境下，以一致性為核心的工作流程的關鍵性。

學校如何透過佈建與部署工作流程實現一致性與效率？在部署工作流程之前，必須先將其設計為能執行特定任務。這些任務定義了裝置的「學習就緒」狀態的具體樣貌。雖然各校的學習就緒狀態會有所差異，但國民及學前教育機構實現一致性的第一步，是盤點並定義學生與教師進行教學與學習所需的所有應用程式、設定與組態，並為您的單位記錄「學習就緒」狀態的具體樣貌。



1,000

台裝置

X

30秒

每台裝置

=

>8

小時損失時間

方法：以韌性為導向進行規劃

「一小時的規劃，能節省十小時的執行。」

—戴爾·卡內基

定義「學習就緒」狀態，是註冊流程與可擴展性的交匯核心。具備這些關鍵資訊後，Jamf 內建的工具能協助 IT 為每種使用者角色建立一致性，確保部署標準化，同時降低大規模組態漂移的風險。

透過 Jamf 藍圖套用樣板化組態

當教學科技團隊定義好學習就緒狀態後，即可將機構專屬需求、必要 App、設定與單一登入 (SSO) 組態儲存為藍圖。在佈建階段，每台裝置會依照指派的藍圖自動完成組態設定，並持續維持學習就緒狀態的一致性。

管理學生、教師、職員等多種使用者角色，只需為每種使用情境建立專屬藍圖即可實現。這能確保指派給特定使用者的裝置，每次都套用對應的藍圖設定，以滿足其專屬需求。

透過現代化管理自動防止組態漂移

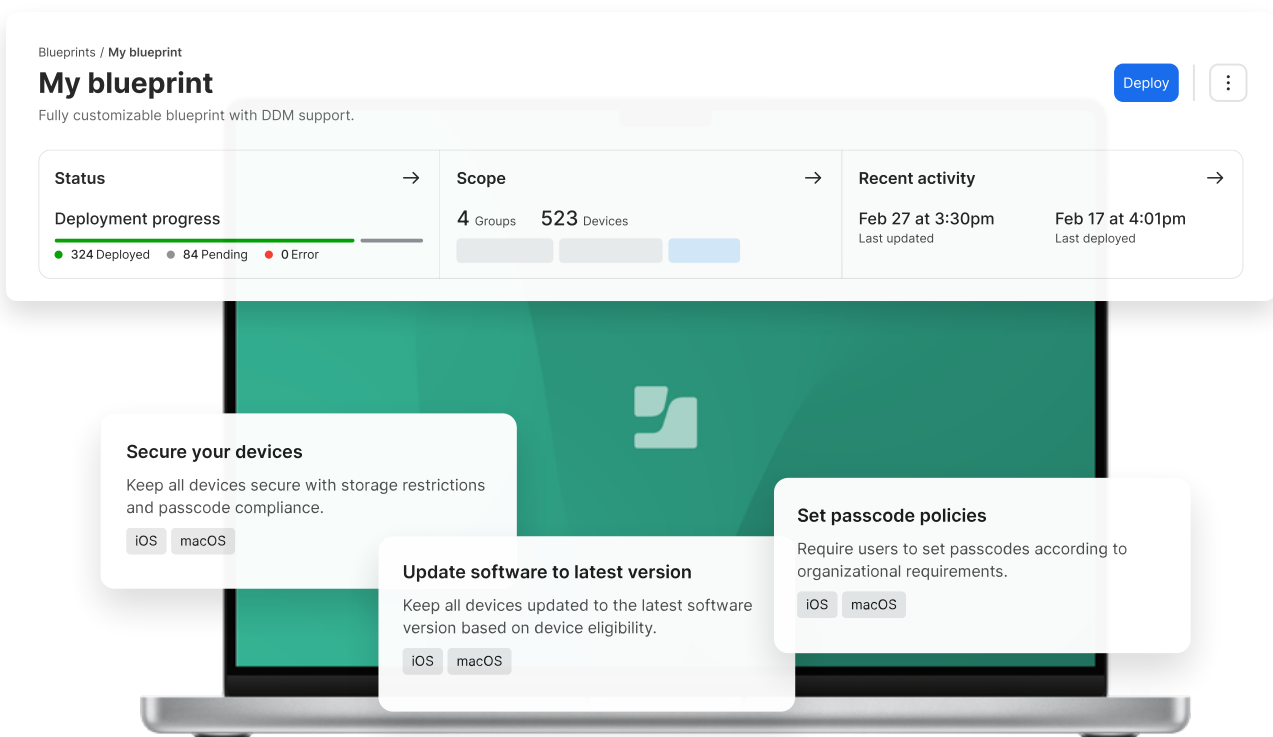
宣告式裝置管理 (DDM) 是由 Apple 設計的現代裝置管理通訊協定。DDM 能在兼顧效能與可擴展性的前提下，確保裝置被正確組態並強制執行這些組態，是驅動藍圖的引擎。非同步通訊會轉為主動式裝置健康狀態回報，並在裝置本機儲存必要的設定副本，確保端點即使處於離線狀態也能維持一致性。

裝置數量增加會產生額外的網路流量，導致通訊效率下降。但 DDM 的設計目的是將 MDM 伺服器與裝置機群之間的輪詢降到最低，避開連線問題，並高效率地處理更新作業，讓學生不論在學校、家中或任何地方都能順利學習。

智慧群組實現彈性管理組合

Jamf 的範圍設定技術，是大規模自動化背後的秘密武器，可依目標使用者角色動態分組裝置，並派送自訂項目、設定、應用程式及藍圖等多項內容。例如，當學生更換年級時，只需將那些裝置從原先的年級移除，並添加到新年級，系統就會自動部署並將這些裝置組態到適合該年級的「學習就緒」狀態。

從資安角度（後續章節將詳細說明），智慧群組可搭配政策偵測不合規的裝置，觸發對應政策自動執行，在背景修復端點裝置，既不中斷使用者，也無需使用者提交服務台工單請求。



App 與更新管理

在本節中，「軟體」一詞指任何可在裝置上執行功能的程式碼基底。例如協助學生創意發揮的 App、教師用於點名的服務，或是資安更新、底層作業系統更新。這樣的區分至關重要，因為從微觀層面來看，應用程式管理不只是保持 App 更新，更凸顯了國民及學前教育依賴於「在正確的時間，於正確的裝置上提供正確的 App」，讓數位學習與教學能不中斷地進行。

從宏觀角度來看，App 生命週期管理是軟體生態的關鍵一環。軟體數量與政策規範等因素會增加變異性，使得在大規模下手動管理軟體變得異常困難，而且隨著裝置數量與變異性蔓延，未修補的漏洞呈指數級增長，風險也隨之顯著提高。

簡單來說，當軟體管理失效時，教學與學習就會中斷。

但在國民及學前教育中，究竟是什麼原因造成這種狀況？



App 部署到錯誤的裝置
(或完全未部署)



因缺少軟體更新
而導致的不相容



因不安全或組態錯誤的
App 所帶來的風險提升



不同年級需使用不同的教學軟體工具



存取權限與組態設定會依使用者角色不同而變動

單獨來看，每一項都只是單台裝置上數分鐘就能解決的小不便。但當這些問題乘以數百、數千甚至數萬台裝置時，負擔會擴大成為 IT 數天甚至數週的工作量，並導致機構無法取得推動預期學習成效所需的必要工具。這類大規模問題永遠不會有「合適的時機」，尤其在即將面臨或正處於決定成敗的測驗期間時最為棘手，此時所有使用者都已承受著必須成功的巨大壓力。

成功的大規模軟體管理是什麼樣子？



- ✔ 學生裝置能在需要時取得所需學習工具。
- ✔ 教師可導入新工具，無須提交服務台工單請求。
- ✔ 修補程式管理自動背景執行，不需要使用者介入。
- ✔ 受管理 App 預設即已配置好資安與隱私保護。
- ✔ 基於政策的管理確保裝置保持合規。
- ✔ IT 只需進行一次變更，架構即可自動完成派送作業。
- ✔ 變更會被記錄下來並且易於檢索，以便向稽核人員證明合規性。

流程：在故障發生前就解決

透過導入預防性流程處理潛在阻礙，避免故障發生，讓 IT 團隊從被動應對轉為主動管理。現在，團隊可以將注意力和技能轉向加強與教學營運的協同，以提供卓越的使用者體驗，而不是忙於解決一個又一個的問題，或更糟的是，成為使用者無法完成任務或目標的「原因」。

自動化修補程式管理以維持安全態勢

遺憾的是，教育機構仍是資料外洩與組態錯誤（包含未安裝更新）的高價值目標，根據 [Verizon 2025 資料外洩調查報告](#)，這類錯誤占雜項錯誤風險的 30%。自動化修補程式可運用架構隨需擴展，彌補裝置機群的資安缺口，同時考量國民及學前教育教學時程（例如將更新延後至合適時段，避免課中執行）。

透過 Jamf Teacher 優化學習環境

教師可透過專用 App 強化數位教學，並安全地將受管理 App 部署至班級。此工具簡單易用，可縮短「我們需要此工具」到「學生取得此工具」的等待時間，無需存取 Jamf 管理主控台，也不具備 IT 專業背景即可使用。

透過 App Installer 消除 App 管理負擔

由 Jamf 精選並持續擴充的應用程式清單，均從開發者端安全取得並經專業封裝。App Installers 不僅可維持基準安全態勢，還能免除 macOS App 的手動分發作業。搭配智慧群組後，系統可依年級、角色、群組成員資格或學校自訂屬性，自動將正確的 App 派送給對應裝置，以滿足學校的獨特需求。

透過 Self Service 減少 IT 服務請求並賦能使用者

想像您能使用一個專屬於學校的 App Store，內含精選軟體、設定與常用組態。這就是 Jamf Self Service。師生與職員可取得 IT 核可的工具，自行下載並安裝，無需提交服務台工單或等待延遲。可將其視為：使用者能在需要時取得所需工具，或是在安全框架內保有使用彈性。

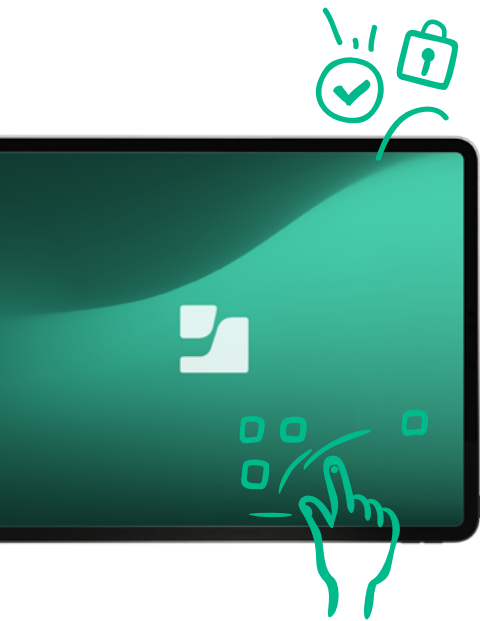
Jamf Student 讓學習者專注、不受干擾

要讓學生上網時還能專心學習本來就很困難。App 相關的問題很容易從中斷演變成干擾。這就是 Jamf Student 的設計目的：即時控制學生裝置上可存取的內容與時機，讓教學時段維持學習專注度。

身分識別與登入阻力

身分識別即等同於驗證。「登入阻力」一詞雖常用於描述兩者，但過度側重後者（驗證），對前者（身分識別）的語境說明不足。在本白皮書中，**登入阻力**指的是密碼重設，以及因登入疲勞（密碼過多）所導致的繁瑣手動作業等驗證相關問題；而身分識別則是以資安為導向的帳號佈建與國民及學前教育資源存取保護概念。

若說大規模管理密碼是造成登入阻力的主因，這並非誇大其詞。在 1:1 計畫中，密碼重設與存取問題僅次於裝置實體損壞，是產生最多 IT 服務台工單、進而導致課堂中斷的主要來源。



相較於數量受限於現有硬體的裝置，身分識別的範圍更為廣泛：每位使用者帳號、非人稱身分（NHI，又稱服務帳號），以及各帳號類型所配置的權限與特權，均納入管理範圍。這些問題不僅會成為 IT 團隊的潛在痛點，若以手動方式管理，持續湧入的服務台工單不僅會拖慢請求支援的使用者，更會隨著裝置、使用者與需獨立登入的 App / 服務數量增加，形成愈發難以控管的工單佇列。

當單一支援問題乘以 1,000 至 10,000 位使用者時，登入阻力不僅會拖慢個別使用者，更會癱瘓學習、教學與日常營運的運作節奏。若未加以處理，初期輕微的作業延遲將會不斷累積，最終導致所有營運作業完全停擺。

架構：建構驗證與授權機制

上述場景充分凸顯了大規模身分識別的關鍵性。對教師而言，可安全存取儲存於雲端的教案等教學資源，無需輸入三組不同密碼。對學習者而言，換課時可在不同 App 間無縫切換，無需重新驗證身分。以下將說明現代化身分整合如何消除手動重複性作業，降低大規模環境中累積的登入阻力，同時強化數位使用者安全、營運資安與教育營運的連續性。

透過單一登入 (SSO) 無縫存取 App

SSO 可讓使用者僅需完成一次性驗證，即可存取所有受保護的 App、平台與服務。透過讓使用者在初次驗證裝置或入口網站後，即可專注於學校相關作業，有效降低忘記憑證、弱密碼或重複密碼等資安風險。

減輕 IT 密碼重設負擔

以「少即是多」的原則，減少憑證數量即可降低密碼重設需求，避免使用者因記憶數十組帳號密碼而造成認知超載。對 IT 團隊而言，這代表兩大優勢：帳號相關問題產生的服務台工單減少，讓團隊有更多時間投入高階技能工作，例如優化使用者體驗，並透過與教育目標高度對齊來創造價值。

透過 Jamf + 您使用的身分識別提供者 (IdP) 擴展身分管理

將機構現有 IdP 與 Jamf 整合，即可從手動帳號維護轉向集中式身分管理，進而擴展身分管理與資安工作流程。設定並強制執行與使用者憑證綁定的一致性存取政策（而非綁定特定裝置），讓權限隨使用者在國民及學前教育環境中移動，無需依 App、裝置或年級手動重新設定。

確保每次帳號佈建與存取保護權限設定正確無誤

為新生、教職員自動化帳號佈建，可讓使用者從第一天起就能取得所需的正確工具。無需提交服務台工單或等待 IT 開通——只需驗證，所需 App、網站與服務的存取權限皆已設定完畢。年級或人員配置變更怎麼辦？透過 Jamf + 您的 IdP + 智慧群組整合，可確保存取權限依年級與角色需求自動更新。

資安防護，不 增加額外負擔

在維護隱私並與法規遵循要求保持同步的同時，還要保護使用者、裝置和資料，這已相當困難，更遑論混合使用案例所帶來的額外挑戰。1:1 計畫、電腦教室、存放於行動推車 (COWS) 中的共用裝置——部分裝置在校內受邊界防護機制保護，其餘則可在家中、學校與課後活動地點等場所間自由移動。這裡的要點是，除了年度換新期，這些裝置大多數時間都在校外。

這種「移動目標」的場景，加上現代威脅環境專門針對全球國民及學前教育的精密攻擊，例如：



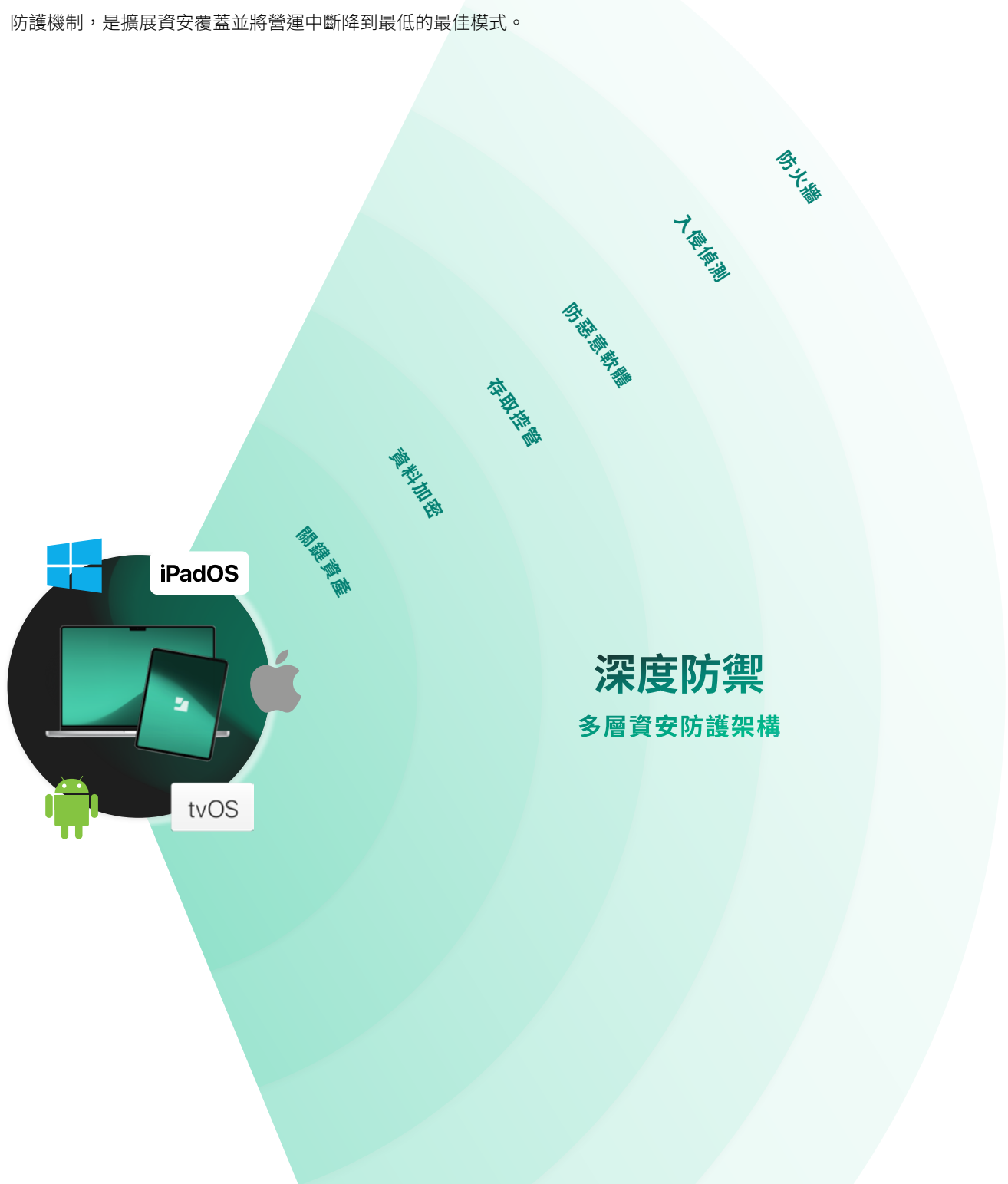
再加上裝置機群持續擴增帶來的規模乘數效應，將為本白皮書中討論的擴展挑戰，再增添一層資安管理的複雜度。

IT 團隊需直接監管每台裝置、每個 App 與網路連線，同時降低來自漏洞、威脅行為者與使用者行為的安全風險。在大規模環境中，這代表 IT 團隊每天需評估數千個資料點。《2025 年 CIS MS-ISAC 國民及學前教育網路安全報告：教育與社區韌性的交匯》指出，在 2023 年 7 月至 2024 年 12 月的 18 個月期間，已確認發生 9,300 起網路安全事件。進一步量化來看，這相當於在 [在這 548 天的期間內](#)，每天發生近 17 起網路攻擊。

換句話說，威脅行為者不會配合學校時段運作，因此國民及學前教育網路安全防護必須自動化、情境化且具備整體性，無論裝置是在教室、家中或假期期間都能持續運作。當威脅防護永不中斷，政策能依裝置地點與時間自動調整時，這不僅是更優質的資安防護，更是唯一能動態、有效且一致地擴展至國民及學前教育基礎架構的營運模式。

模式：深度防禦 (DiD)

深度防禦 (DiD) 是將多種資安控制措施與流程整合於單一框架下的概念，透過有效的分層防護機制，為使用者、裝置與機構提供對抗精密攻擊的多重保護層。若威脅成功逃過任一層防護，其上、下層防護將提供額外的安全防護網，在風險擴大前有效降低其影響。現代教學環境包含多種裝置類型（電腦、平板、多媒體連接設備）與多種平台（macOS、iPadOS、tvOS、Android、Windows），皆被教育使用者用於學習、教學與日常營運作業；因此，降低複雜度、強化動態防護機制，是擴展資安覆蓋並將營運中斷降到最低的最佳模式。



跨平台防範網路型威脅

網路釣魚、竊聽、加密劫持等攻擊對國民及學前教育機構的攻擊量創歷史新高。無論桌上型裝置或行動裝置，只要處於網路連線狀態，Jamf Security 就如同守門員，既能為學習開放大門，也能封閉威脅學校資料安全的攻擊管道。搭配裝置健康資料可視化功能，IT 團隊可詳細瞭解哪些裝置成為攻擊目標及其原因，進而適當緩解各項風險因子。

透過 Jamf Safe Internet (JSI) 保護學生遠離有害內容

國民及學前教育學生年齡與成熟度差異極大，「一刀切」的管理方式不僅不利於學習，還需要持續手動調整，往往為滿足高年級學生需求而犧牲低年級學生的使用體驗。JSI 不僅能封鎖不當內容與學習干擾，還提供細粒度管控功能，例如依年齡分級的過濾機制與政策，可自動在課外時段（如週末）開放網路資源，並且不損及學生的線上安全。

可持續進化的 AI 驅動威脅防護

駭客正運用 AI 提升攻擊的精確程度。這類攻擊難以辨識與防禦，因此 Jamf 採用「網路內控制 + 裝置端防護」的雙重機制，內建機器學習 (ML) 以偵測 AI 驅動威脅（如零時差網路釣魚攻擊）並加以阻擋，即使使用者不慎點擊惡意連結也能有效防護。此外，裝置端防護的優勢在於：無論使用者使用何種第三方 VPN、代理伺服器或 DNS 設定，資安防護機制皆能正常運作，從而消除防護規避與覆蓋缺口。

依情境需求自動套用政策

過去，在校內使用裝置可獲得使用者所需的所有資源和防護，而在校外使用則幾乎得不到任何保護。國民及學前教育使用者越來越常在校外以同等程度依賴科技，其需求與在校內時無異，但情境的改變往往需要隨之調整設定。這正是「排程型政策調整」的優勢所在：可依時間、校曆（如週末或假期）等情境資訊自動切換資安政策。IT 團隊只需定義一次規則，Jamf 即可自動處理後續所有情境切換，無需中斷教學流程或手動調整組態設定。



結語

在本白皮書中，我們探討了國民及學前教育機構平均每位 IT 人員需管理 1,000 台裝置的比例。相較於企業組織中約 70:1 的比例，國民及學前教育機構受限於預算，難以透過增加人力來縮減此差距。

事實上，部分地區的比例已接近（甚至達到）10,000:1。

這只會讓國民及學前教育環境中原本就沉重的學生、教師與行政人員支援負擔，在大規模營運下變得更加難以負荷，其背後的多種變異因素包括：

- ✔ 佈建多樣化且持續擴增的裝置機群
- ✔ 跨機構的適齡考量
- ✔ 身分與驗證阻力（本地端／雲端環境）
- ✔ 多校區、多建築與機構級部署作業
- ✔ 各校之年級需求
- ✔ 校內外資安防護一致性
- ✔ 跨平台支援與合規強制執行

問題所在：手動流程已不堪使用

面對 1,000 台裝置時，無論是一天的時數、一週的天數，還是年度更新期間的週數，都不足以大規模地逐一執行每一項任務。

解決方案：以更完善的架構取代額外人力投入

在此，我們再次回到需反覆強調的核心關鍵詞：大規模環境下的可重複性，永遠優於手動作業。

貫穿裝置生命週期的各個階段，包含：

 **採購**
規劃與註冊

 **維護**
資安與漏洞管理

 **部署**
組態與 APP 管理

 **退役**
資產盤點與安全處置

 **監控**
身分與存取報告

「在裝置機群中的多台裝置上重複執行相同步驟且不受變因影響的能力，能將營運負擔降至最低。」

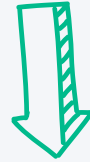
標準化、彈性與效率是自動化的核心主題。本白皮書各章節的核心主軸均圍繞「自動化作業與流程」，這正是「實現可重複性擴展且不讓 IT 過勞」的關鍵。

願景：從被動應對轉向主動管理

透過自動化，手動與重複性作業可轉化為可預測的標準化作業，建立全面且整體的工作流程，並能一再重複使用；無論是新增裝置或現有裝置需重新佈建，每次都能以一致、有效且高效的方式完成大規模作業。

更重要的是，這一切都不會中斷學習環境，也不需要 IT 每次都親自介入執行作業。事實上，此架構在設計時已充分考量不同技術程度的使用者，因此教師在教學過程中若收到更新提示並選擇延後，仍能迅速回到課程教學。此外，亦可提升學生的學習投入度：當需要使用未安裝的 App 時，學生僅需透過 Self Service 安裝已預先核可的軟體，即可繼續學習。

這兩種常見情境均無需提交服務台工單或 IT 團隊介入；更重要的是，使用者的作業不會受到阻礙，也無需等待具備管理員權限的人員處理問題。



IT 與技術團隊重點整理

隨著裝置數量增加，手動作業負荷將迅速變得難以為繼，不僅會影響 IT 團隊的即時支援能力，更會導致教育成效以指數級速度下滑。



透過自動化突破裝置數量瓶頸

以自動化工作流程取代手動佈建作業，可將佈建時間從數小時縮短至數分鐘。



大規模標準化「學習就緒」裝置

使用樣板化組態，確保師生裝置從第一天起就維持一致設定。



透過零接觸部署消除 IT 繁瑣作業

讓裝置能夠開箱即自動註冊和設定，實現開學首日即就緒。



從被動支援轉向主動營運

透過自動化整合裝置、身分與資安管理，專注提升學習成效，而非四處滅火。



在正確時間無阻力的資源派送

依角色與年級動態指派 App 與資源，讓使用者能即時存取，無延遲。



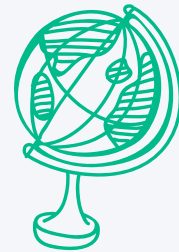
消除登入阻力與密碼疲勞

導入單一登入 (SSO) 與自動化身分識別工作流程，減少密碼重設需求並維持安全存取。



擴展資安防護，不干擾教學作業

套用多層防護，在校內外無縫動態調整執行強度。



瞭解 Jamf 如何減輕國民及學前教育營運負擔，透過賦能使用者自行解決日常問題，無需中斷當前任務，同時協助 IT 團隊從滅火模式轉型為支援學習成效。



www.jamf.com/zh-tw/

©2026 Jamf, LLC. 著作權所有，並保留一切權利。