

# 國民及學前教育機構 之身分識別與存取管 理新手指南

每個學生都是獨一無二的。有的學生可能熱愛數學，有的則鍾於閱讀。有些學生透過互動遊戲學習的效果最好，而不是聽老師口頭講解。也有些學生可能因為身心障礙，在特定學科上倍感吃力。

如果裝置的目的是為了強化學習，就必須因應學生的需求來調整。如果每位學生拿到的「共享 iPad」都跟同學的一模一樣，完全沒有個人特色，那他們真的有發揮這台裝置的最大價值嗎？

但是，學校該如何確保每位學生都能以最適合自己的方式學習呢？在自訂裝置設定之前，您必須先知道使用者是**誰**——換句話說，就是學生的「身分」。

學校的 IT 管理員在幕後已經做了很多工作。如果還要加上「身分識別與存取管理 (IAM)」這項任務，聽起來確實讓人壓力很大。但只要選對工具，IAM 不僅能簡化工作流程並提升資安，還能同時優化學生的課堂體驗。接下來，我們將帶您了解這是如何實現的。



這本電子書將涵蓋：

- ✓ 什麼是「身分識別與存取管理 (IAM)」
- ✓ 國民及學前教育環境面臨的身分識別挑戰
- ✓ 建立您的身分識別基礎
- ✓ IAM 為國民及學前教育帶來的效益
- ✓ 學校的 IAM 準備程度清單

## IAM 能夠塑造不同的課堂體驗。

根據您的身分識別工作流程，每堂課的樣貌可能會大不相同。



不流暢的身分識別流程可能會透過幾種方式干擾學習：



學生必須記住（或忘記）多組  
帳號密碼（例如不同的 App 或  
工具）



因為裝置配置問題，導致學生  
難以跟上教學進度



單一登入 (SSO) 不完全，無法  
連接學生的所有帳號



存取原則不夠完善  
導致的資安事件



其實，管理方式可以更簡單。





## 想像一下這種體驗：



1.

學生從教室推車上拿起一台共享 iPad。

2.

他們點擊自己的照片並輸入密碼。



3.

這台 iPad 會根據該學生的年級、課程等資訊，自動配置好專屬的 App 與設定。



4.

透過「管理式 Apple 帳號」與身分提供者 (IdP)，學生可以登入任何資源，無需記住一堆繁雜的密碼。

5.

當學生使用完畢，他們的個人工作資訊會從該台 iPad 上清除。



這讓裝置能順暢地融入老師的教案中。透過免密碼驗證技術，需要記住（或被盜用）的密碼也變少了。



## 現代 IAM 總覽

我們先別操之過急。在進入這些簡化流程之前，我們必須先了解 IAM 到底代表什麼，以及它如何應用在您的學校。

它建立在兩個核心概念之上：

1.

### 身分驗證



確認學生或老師的真實身分

2.

### 授權



控管他們可以存取的權限。

首先，我們需要記錄所有使用者，並提供一種讓他們證明身分的方式（如帳號密碼）。接著，我們需要將權限與該身分連結，決定他們可以存取哪些 App、資料與資源。

為了實現這一點，我們需要一個「目錄」來命名每位使用者。這可能包含使用者的：

- 姓氏與名字
- 使用者名稱
- Email
- 屬性資訊（如班級、年級或校名）
- 驗證資訊（如雜湊值/Hashes）

有了這些資訊，我們就可以開始建立權限。例如，如果您知道某位使用者是某位老師數學班的五年級學生，您就可以授權讓他們使用該位老師愛用的數學遊戲 App。

## 那麼，IAM 具體可以做到什麼呢？

IAM 不僅僅是一個儲存學生名單的目錄。它包含帳號資訊（使用者對各種應用程式的存取權限），這意味著它可以規定使用者可以存取什麼，以及如何存取。

IAM 是動態的，會根據使用者帳號的情境進行調整。如果學生換了班級需要一套新的 App，IAM 可以自動配置正確的 App，並撤銷不再需要的權限。三年級和十二年級的學生都可以上網，但十二年級學生的內容篩選限制可能會相對寬鬆。如果十一年級學生退選了科學課，IAM 將不再授權他們使用該課程專用的昂貴軟體。

換句話說，IAM 就像您的「學生點名冊」——但它更聰明。它是確保您的使用者帳號與資料安全的關鍵。它能為學生與老師帶來更好的課堂體驗；稍後我們會詳細說明。

### 教育領域 IAM 詞彙表

#### 身分提供者 (IdP) :

您的「數位通訊錄」，負責驗證使用者及其權限（例如：Google Workspace、Microsoft Entra ID 或 Okta）。

#### 單一登入 (SSO) :

只需一組帳號密碼即可登入所有資源，包含 Apple、Google 及學習管理系統 (LMS) 等。

#### 多重身分驗證 (MFA) :

帳號的額外防護層，除了密碼外還需要生物辨識或一次性密碼 (OTP) 才能登入。

#### 身分編排 (Identity Orchestration) :

身分管理的控制中心，負責整合目錄與身分工作流程，並啟用 SSO 等功能。

## 為什麼國民其學前教育學校需要 IAM

學校裡總是有各種變動。學生每年都會升級、換班或更換教室大樓。年紀小的學生會忘記密碼。裝置會易手、遺失，或被學生帶回家。

幾乎沒有部門能完全免於這些混亂，尤其是 IT 部門。您可能會發現自己正在努力發揮那些並非由您挑選的工具價值，或是必須在 Apple、Google、Microsoft 以及學生資訊系統 (SIS) 等混合系統中苦苦掙扎。



如果沒有 IAM，身分驗證會變得異常困難。  
這會影響到每個人：

**IT 團隊**必須處理混亂的登入問題、更多的支援請求單，以及延誤的資源配置。

**老師**損失了寶貴的教學時間，導致挫折感，甚至可能被迫修改課程。

無法登入的**學生**會感受到與同學不同的學習待遇；若被迫共用帳號，則會讓隱私暴露在風險中。



## 在 Apple 環境中使用與不使用 IAM 的差異

有了 IAM，學生與教職員的身分識別將成為您 Apple 環境的根基。連結您的身分提供者 (IdP)、Apple School Manager (ASM) 與行動裝置管理 (MDM)，能協助您提供簡單、安全且個人化的學習體驗。



### 有導入 IAM

- 🔑 一組帳號通行所有資源
- ⚙️ 自動化資源配置與存取控管
- 👤 在共享 iPad 上享有個人化體驗
- 🛡️ 透過 SSO 與 MFA 建立強大資安屏障



### 未導入 IAM

- 🗃️ 每位學生需記住多組登入帳號
- 🗣️ 需手動設定帳號與人工干預
- 🕒 損失教學時間且 IT 報修件數激增
- 🔒 資安防護與存取權限不一致



# 建立您的身分識別基礎

那麼，如果您現在也想在學校推行 IAM ..... 該如何開始呢？

1.

## 建立單一事實來源 (Single Source of Truth)

**整合您的系統**：將您的 SIS 與 IdP 連結，確保資料即時且連續。

**自動化帳號佈建**：根據 SIS 中的資料，自動建立、管理與移除使用者帳號。這有助於避免在開學或學期末出現管理瓶頸，確保學生在開學第一天就能順利存取資源。

**保持同步**：確保班級名冊、裝置分配與 App 存取權限始終保持一致並同步。學生可以根據這些資訊被分配到正確的班級，並存取指定的 App。

### 您的資料一致性如何？

當系統間的資料保持一致時，IAM 運作效果最好。但要達到這個目標並不總是那麼容易。身分資料管理工具會在 IAM 之上增加一個「資料編排層 (Data Orchestration Layer)」，將您的原始資料轉換為乾淨且標準化的記錄。如果處理資料一直讓您感到頭疼，請參考這個方案。





## 2.

### 與 Apple 校務管理整合

**優化您的部署：**Apple 校務管理 (ASM) 能協助您發揮 iPad 部署的最大效益。首先，它支援新裝置的「自動裝置註冊 (ADE)」功能，讓您可以大量採購 App 與電子書。

**自動化身分管理：**ASM 可以與您的 SIS 整合，自動建立「管理式 Apple 帳號」，並因應整個學年中的變動進行調整。有了這些帳號，IT 管理員還可以執行密碼重設等各項管理功能。學生可獲得 200 GB 的 iCloud 儲存空間，也能夠存取其他 Apple App 與服務——例如與同學共同協作 Keynote。

**個人化學習：**管理式 Apple 帳號可啟用「共享 iPad」功能。學生只需點擊自己的個人資料並輸入 PIN 碼，就能擁有一台按其偏好與需求配置好的 iPad。



### 3.

## 串聯 MDM 行動裝置管理



**發揮身分提供者 (IdP) 的價值：**將 MDM 與 IdP 整合，即可針對不同裝置自動派發部署描述檔與存取原則。

**自動化佈建：**根據使用者身分，自動派發對應的 App 與系統設定。

**簡化前置作業：**依照身分預先分配裝置，確保開學第一天所有設備都能立即進入教學狀態。





4.



## 落實身分管理最佳實務

**導入單一登入 (SSO)：**透過 SSO 讓師生登入各類 App 變得更輕鬆。當需要記憶的密碼變少，不僅能緩解「密碼疲勞」並減少重設需求，駭客也更難有機可乘。

**強制執行多重身分驗證 (MFA)：**為教職員與管理員帳號增加額外安全防線。

**自動化帳號生命週期管理：**整合 MDM、IdP 與各項系統後，即可自動執行帳號的啟用與停用。這能即時修補資安漏洞，無需耗時等待人工處理。

**定期進行權限稽核：**理想狀態下，應根據角色屬性落實「最小權限原則」，僅授予必要的存取權限。但人員異動頻繁，務必定期審視存取原則，確保權限配置精確無誤。



5.



## 先試辦，再擴大規模

**從小規模開始：**建議先從單一年級或單一校舍啟動試行。在全面推廣前，這能讓您先解決流程與工具中的各種小問題。

**調整與優化：**收集老師的回饋——課堂干擾是否減少了？學生登入帳號是否變得更順手？透過這些意見，您可以排除疑慮並確保科技是「輔助」而非「阻礙」教學。

**強調跨部門協作：**科技要發揮影響力，就不該只侷限在 IT 部門的「孤島」中。與校方行政人員、課程領導者共同合作，才能確保所有人都能從中受益。而學生也將會是最終的受益者。



# IAM 全面強化了 IT 工作流程、資安防護以及 課堂學習體驗。

一旦打好這個基礎，後續效益將隨之而來。

## 精簡 IT 維運：

將各項系統與核心 IAM 結合後，即可開啟強大的自動化功能，化繁為簡。

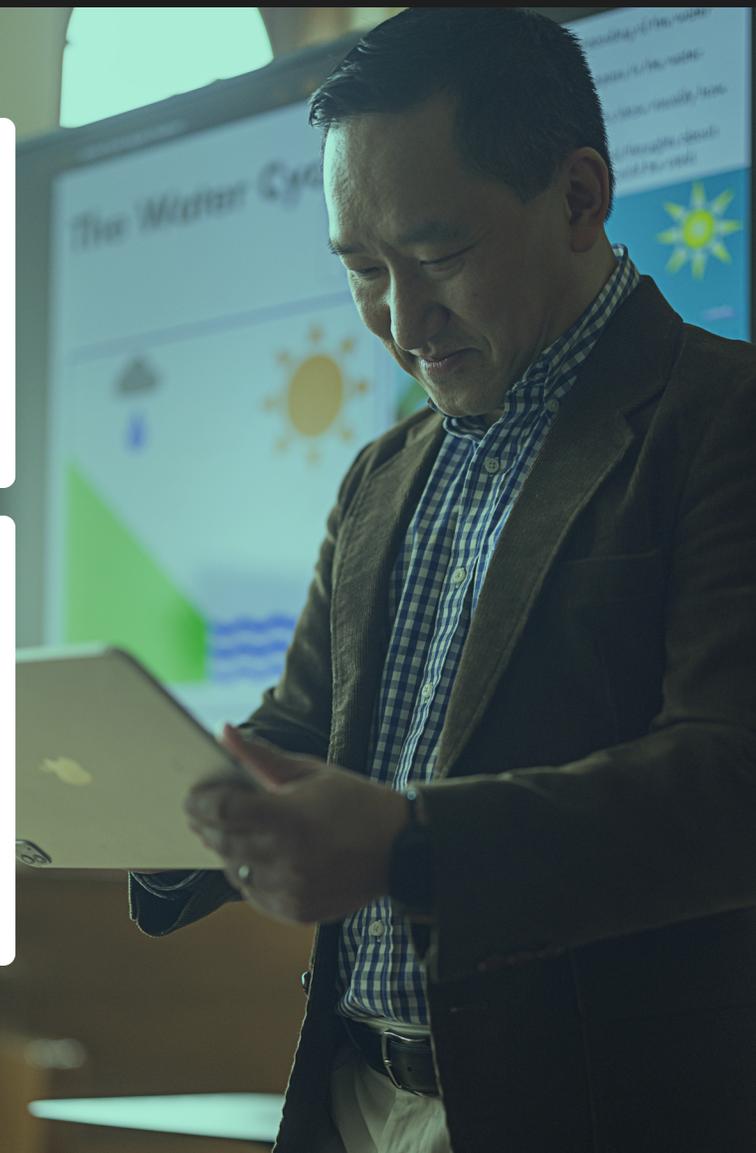
## 自動化身分生命週期：

只要設定正確，您就能自動管理整學年（甚至更久）的身分資料。當 IAM 能因應名單、職務、校區或班級變動而「自動調整」時，IT 人員幾乎無需介入即可完成權限指派。

 提升資安合規性： SSO 與自動化機制能在問題發生前，就先堵住資安漏洞。IAM 能減少密碼疲勞、自動管理權限、防止未經授權的存取並節省 IT 時間——這些特點都能全方位提升安全性與合規表現。

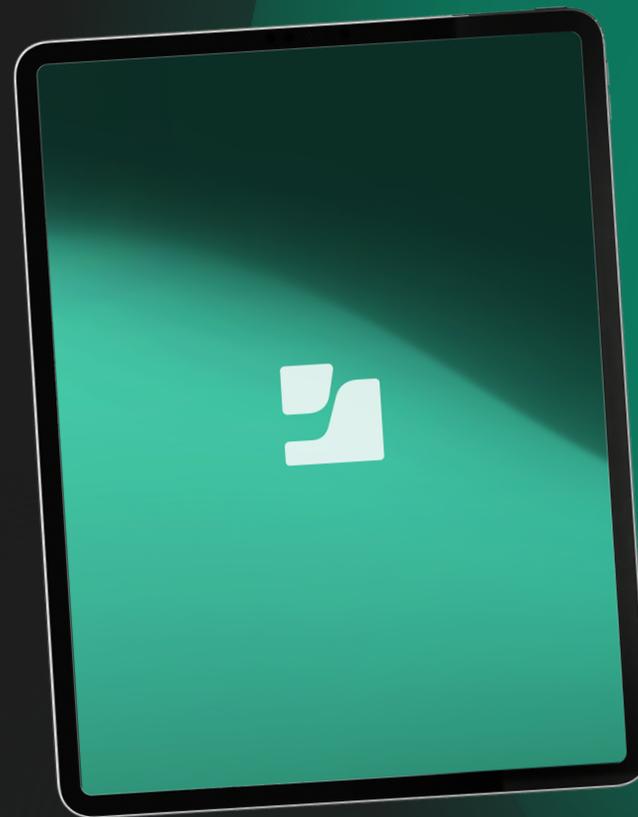
## 優化使用者體驗：

如前所述，學生需要記的密碼越少，學習成效就越好。由於存取權限是根據身分自動指派，學生從第一天起就能使用所有必備的 App。這意味著課堂干擾更少，IT 服務台不再被重設密碼的求救電話淹沒，老師也省去了不少麻煩。



## IAM 是一個循序漸進的過程： 先從簡單的部分做起。

這是一個龐大的學習領域。如果您是從零開始，導入 IAM 聽起來可能令人望而生畏。好在這並不是非黑即白的選擇，您可以視需求彈性導入。先從觸手可及的部分開始。例如，先確保各系統間的資料一致。或是將 Apple 校務管理 (ASM) 與您的 MDM 進行整合。您會發現，小小的改變就能為學校帶來極大效益：行政負擔減輕、登入速度加快，學生的環境也變得更安全。



## 自我檢核清單：我的學校準備好導入 IAM 了嗎？

利用這份清單，快速評估您的學校是否具備導入 IAM 的條件。

### 了解現有的架構

- 我清楚學生與教職員帳號的新增與移除流程。
- 各系統（SIS、Google、Microsoft 等）間的資料保持一致。

### 奠定基礎

- 我們已使用（或計畫導入）雲端身分提供者，例如 Google Workspace、Microsoft Entra ID 或 Okta。
- ASM 已完成設定並與 MDM（如 Jamf School 或 Jamf Pro）串聯。

### 遵循最佳實務

- 核心教學工具皆已採用單一登入（SSO）。
- 教職員與管理員帳號皆受到多重身分驗證（MFA）保護。
- 已實現使用者帳號自動配置，並定期審視存取權限。

如果您已勾選大部分項目，代表您已準備好透過 IAM 來簡化登入流程、強化資安並提升學習體驗。



立即試用 Jamf