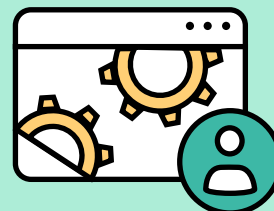




身份識別管理

適合對象：
初學者



每位員工都有自己的數位身分

.....

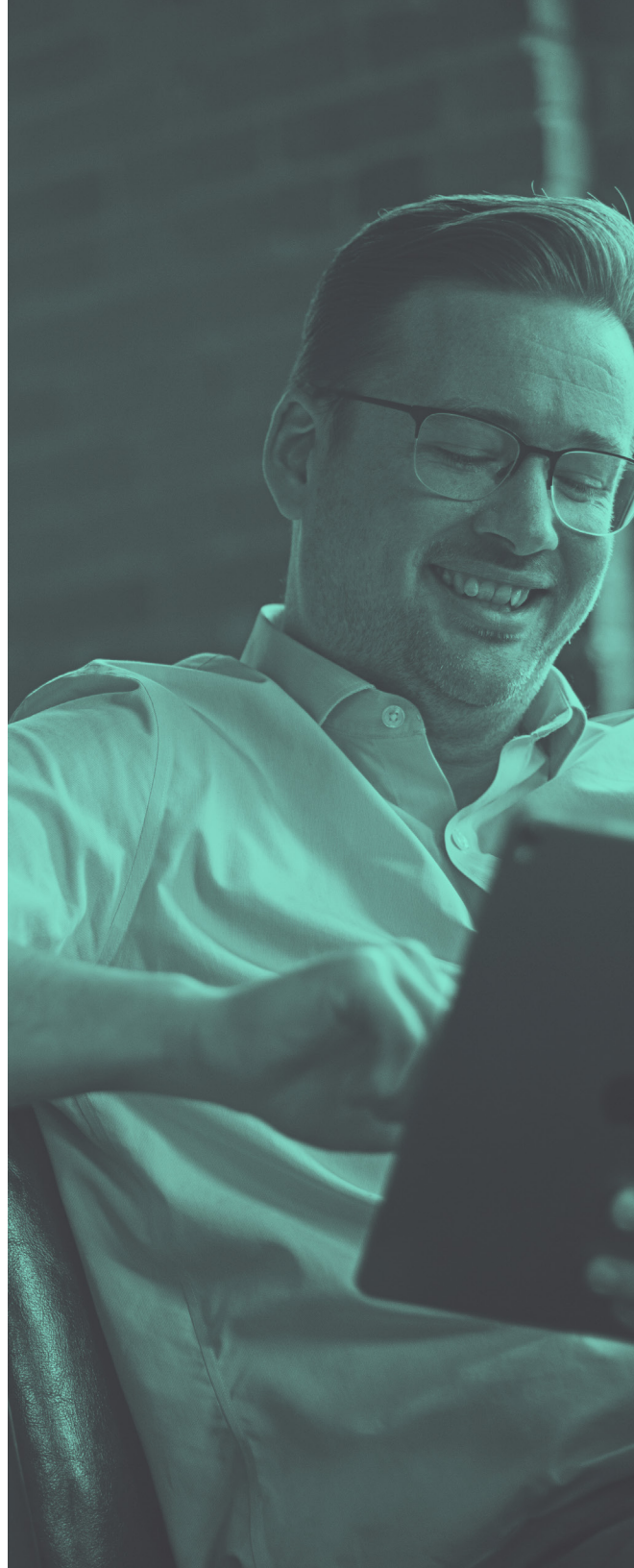
傳統上，員工會到辦公大樓上班，辦公桌上有一台桌上型電腦，而這些裝置從不離開那個位置。若將這種情況放大到整個組織的員工規模，就能看出 IT 需要管理多少裝置與存取權限。現今的工作環境已大不相同。現代員工行動自如，全天在筆電、平板和手機之間無縫切換，並需要隨時隨地存取資訊與資料。

員工的數位足跡不斷擴大，無論是使用裝置的時間，還是他們希望存取的資料量，都呈現大幅增長。公司保護這些資訊的關鍵策略之一，就是嚴格控管誰能存取特定的檔案、軟體和資料。這種方式不僅能確保安全，還能簡化使用者體驗——讓他們在需要的時候獲得剛剛好的資源，不多也不少。

這已成為 IT 的標準做法，但隨著科技演進，員工需求也不斷變化，因此公司必須以現代且可持續的方式來建立工作流程。其中一個核心要素就是身份識別管理，這也是企業的首要任務。

在本電子書中， 您將學習：

- 身份識別管理基本概念
- 現代身份識別管理的工作流程
- 為什麼雲端技術對現代企業如此重要？
- 這些技術如何與 Jamf 整合應用



身份識別管理基本概念

.....

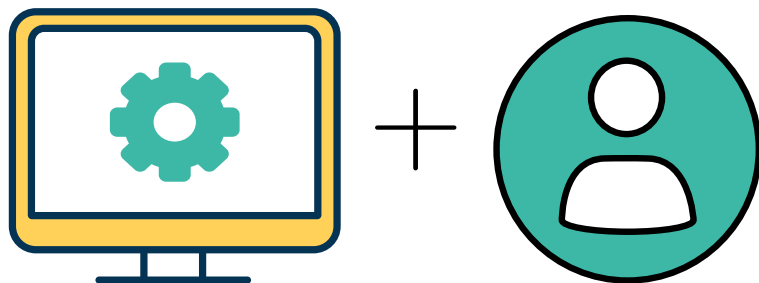
身份識別管理（Identity Management，亦稱為身份識別與存取管理 IAM）是一套用來驗證使用者身份並決定其存取權限的機制。為了實現身份識別管理，使用者必須通過驗證和授權兩個步驟

驗證（Authentication）通常指的是「登入」過程，在這個步驟中，系統會確認你的身份是否屬實。最常見的驗證方式是使用者名稱與密碼。

但在身份識別管理中，通過驗證並不代表你可以直接存取所有資源，它只是確認了你的身份。若要存取系統內的資料、軟體或檔案，還需要授權（Authorization）。

授權 決定了你能存取哪些資源，例如特定的應用程式、資料庫或文件。

身份驗證 = 你是誰
授權 = 你可以做什麼





身份識別管理基本概念

為了讓身份驗證與授權機制能夠有效運作，公司會建立目錄服務（Directory Services），也就是一個包含員工相關資訊的資料庫。例如：姓名、裝置類型、職稱、部門、使用者名稱、密碼，以及可以存取的軟體與檔案。這些目錄服務奠定了身份識別管理的基礎。這種做法在傳統 IT 架構中十分常見，通常被稱為傳統 IT。

15 年前，身份管理的方式相對單純。當時的標準作法是使用輕型目錄存取協定（LDAP）來管理使用者資訊，Kerberos 負責身份驗證，兩者結合就形成了 Active Directory（AD），這基本上就是身份管理的全部內容。然而，在過去 10 年間，身份識別管理技術開始演變，尤其在近 5 年更是發展迅速。

傳統 IT 架構依賴目錄服務作為「資料來源」，但隨著安全性與部署需求的變化，企業需要採取新的身份管理方式，讓 IT 策略與時俱進。透過完整的身份識別管理架構，企業可以統一裝置與應用程式的身份驗證機制，解鎖更多功能、提升效率，最終實現數位轉型。

現代身份 識別管理

從傳統 IT 過渡到現代 IT 不只是技術的改變，更關乎如何善用技術來提升使用者體驗與企業生產力。



身份識別管理架構

目錄服務

目錄服務是用來集中管理員工資訊的系統，例如姓名、部門等資料。這類系統通常與 Jamf Pro 等裝置管理平台整合，以部署符合企業需求的裝置。

傳統方式 本機 Active Directory (AD)

現代方式：雲端目錄 (Cloud Directory)

目錄服務

目錄服務 + 雲端 SSO

雲端 SSO (單一登入)

建立在目錄服務之上，雲端 SSO 讓使用者透過單一帳號驗證即可安全存取企業資源。

傳統方式：每次存取雲端應用或資源時，都需要重新驗證身份。

現代方式：使用者可以更順暢地存取如 Microsoft Outlook、Slack 等雲端應用，減少重複驗證的需求

Jamf Connect

在目錄服務與雲端 SSO 的基礎上，Jamf Connect 進一步整合所有應用與 Mac 裝置的身份管理機制，確保安全性不受影響。使用者只需一組雲端帳號，即可輕鬆且快速存取所需資源，提升工作效率。

現代：

- 簡化開箱即用的配置和身份驗證，為遠端員工提供全面支援。
- 自動同步使用者身份與裝置憑證。
- 確保 IT 擁有完整的身份管理功能。

目錄服務 + 雲端 SSO + Jamf Connect

現代身份 識別管理

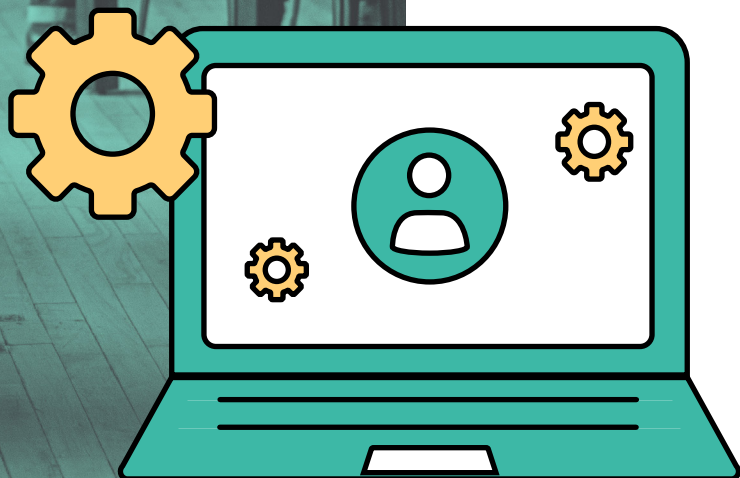
現在的身份管理架構包含三大核心元件：

1. 來自雲端身份識別供應商 (Cloud IdP) (如 Azure 或 Okta) 的目錄服務與雲端單一登入 (SSO)。
2. Jamf 行動裝置管理 (MDM)
3. Jamf Connect，整合雲端身份識別供應商、硬體與軟體

這些元素可共同改善行動工作者的終端使用者體驗，並提升整個部署的整體安全層級。

什麼是身份識別供應商？

身分識別供應商 (IdP) 泛指提供存放和管理數位身分的廠商。企業藉由 IdP 服務，讓員工或使用者可以連線並取得他們需要的資源；IdP 提供一個管理存取、添加或刪除權限的方法，同時確保維持安全性。



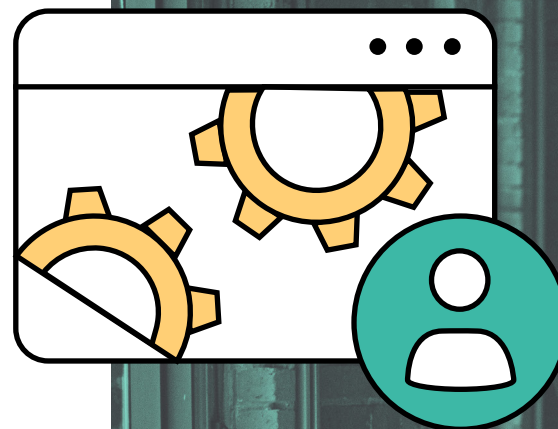
現代身份 識別管理

過去，員工大多待在同一個辦公空間，所使用的技術相對單純，基本的身份管理就已足夠。但現在，員工需要使用更多裝置存取更多資料與軟體，安全風險提升，加上工作模式變得更具流動性，傳統方式已不敷使用。

當工作方式轉變，IT 基礎架構也必須跟著改變。身份管理當然也不例外。使用 Active Directory 和 LDAP 需要將裝置綁定至內部 AD 伺服器。但如前所述，但員工已不再只在辦公室工作，導致多種問題：

- 密碼只能在辦公室內且 AD 可存取時更改。若忘記密碼或要重設，可能導致大量 IT 支援需求。
- AD 是為 Windows 設計的，作為主要身份供應商時，對 Mac 的管理能力較弱。為了支援更多裝置，企業需依賴第三方擴充工具，增加管理複雜度與成本。
- 遠端使用者需透過 VPN 或連接內部網路 (LAN) 才能存取企業資源。這會影響使用體驗，增加挫折感。

以上種種挑戰，使得越來越多企業轉向雲端身份供應商 (Cloud IdP)，這是現代身份管理的關鍵。





為什麼雲端技術 對現代企業如此 重要？

透過雲端身份管理，IT 團隊可以遠端集中管理使用者、群組、密碼，並控管企業應用程式與雲端資源的存取權限。Microsoft、Google、Okta、IBM、OneLogin、Ping 等雲端身份供應商，能讓所有員工（無論在辦公室或遠端工作）安全存取必要的雲端資源，提高生產力。

傳統身份識別管理 (Legacy Identity)

Active Directory

Open Directory

LDAP (輕型目錄
存取協定)

現代身份管理 (Modern Identity)

Azure

Okta

Google

Workspace

無論是因全球疫情影響，還是全球化經濟的需求，現代員工必須隨時隨地存取工作所需的資料與應用程式。辦公室、家裡、機場、飯店、共享辦公空間，甚至是合作夥伴的辦公室——工作的邊界已不復存在。透過與雲端身份供應商合作，企業能夠超越傳統辦公室的限制，確保使用者無論身在何處，都能順暢、安全地存取所需資源。

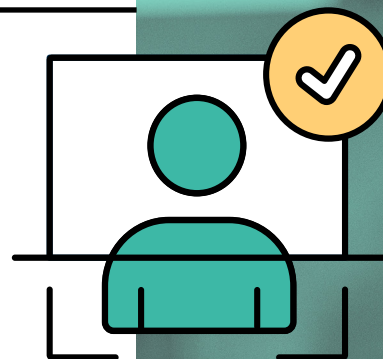
為什麼雲端技術 對現代企業如此 重要？

你的 IdP（身份提供者），例如 Okta、Azure、Google Workspace 等，會作為你的目錄服務，也就是你的「企業通訊錄」。這個目錄包含每位員工的個人資訊、所屬部門、職稱，以及最重要的——他們能夠使用哪些應用程式與資源。當使用者登入雲端 IdP 並通過身份驗證後，就能存取所有對他們開放的雲端資源。身份驗證與授權的實際應用！

雲端 IdP 也能讓你運用單點登入（SSO），同時提升行動裝置的安全性並改善使用者體驗。使用 SSO，使用者只需登入一次，就能安全地存取所有應用程式與服務，而不需要在每個平台上重複輸入帳號密碼。

什麼是單一登錄（SSO）？

SSO 是一種身份驗證機制，讓使用者只需使用一組憑證，就能安全地登入多個應用程式與網站。



為什麼雲端技術 對現代企業如此 重要？



為了再提升安全性，企業可以採用多重要素驗證（MFA）。加入 MFA 之後，使用者需要多做一個簡單的步驟來驗證身份，而不只是輸入容易被攻擊的使用者名稱和密碼，但仍能順利存取所需的資源。

要實現這一點，並將雲端身份供應商與裝置統一整合，Jamf Connect 就能發揮作用。

什麼是多重要素驗證？

多重身份驗證（MFA）是一種身份驗證流程，要求使用者提供兩種或以上的驗證方式，才能存取特定資源。這些驗證方式可以是使用者手機上的 PIN 碼、FaceID、指紋辨識，或其他選項。



JAMF CONNECT

將這一切無縫整合在一起

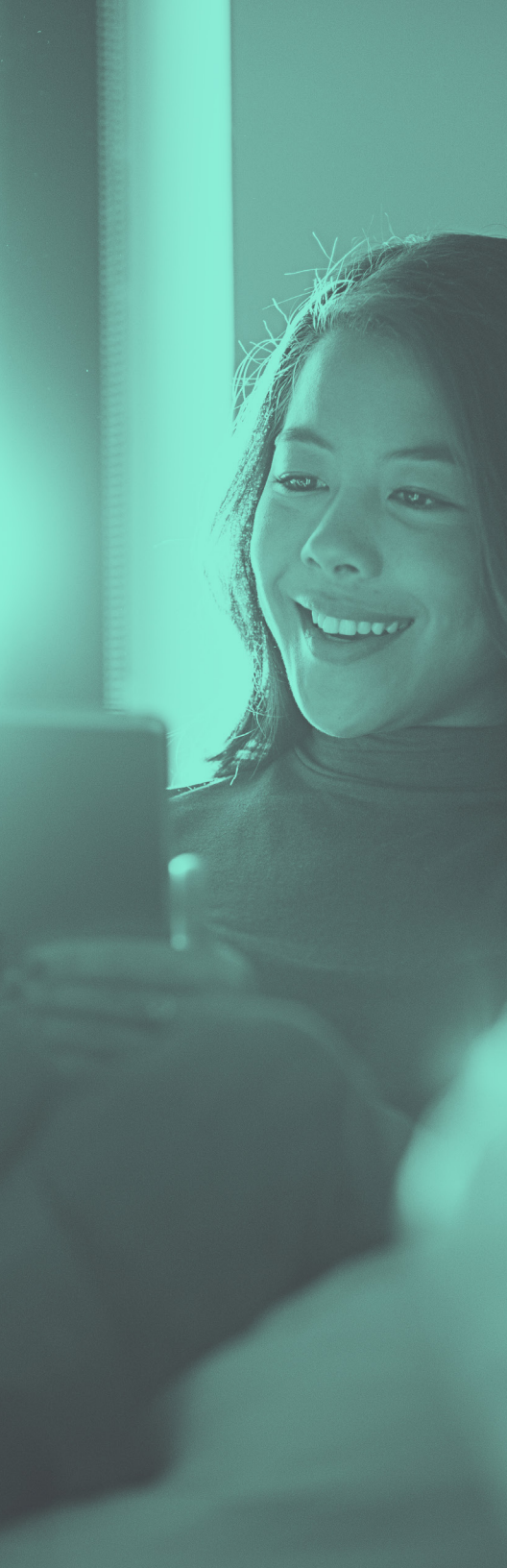
Active Directory 原本是為 Windows 設計的，因此在 Jamf Connect 出現之前，Apple 使用者唯一的選擇就是綁定 AD。

隨著企業逐步轉向雲端，並導入更多 Mac 裝置以滿足日益增加的需求，他們需要建立合適的工作流程，以確保企業資訊安全，同時提供理想的使用者體驗。

透過與 Jamf Connect 整合的雲端身份供應商，IT 人員可以遠端管理使用者密碼及對企業應用程式的存取權限。使用自動 MDM 註冊，整個流程簡單且安全：

1. 使用者會收到邀請，註冊自動 MDM 註冊。
2. 在註冊期過程中，將從 MDM 伺服器下載並安裝 Jamf Connect。
3. 使用者將直接進入 Jamf Connect 登入視窗，輸入其雲端身份憑證，而無需自行建立使用者名稱和密碼。





JAMF CONNECT 將這一切無縫整合在一起

使用者可在所有服務中使用相同的使用者名稱與密碼，既能提升體驗，也能確保帳戶安全。

優勢包括：

- 帳戶建立：根據 Okta、Microsoft Azure、Google Cloud、IBM Cloud、PingFederate 和 OneLogin 的身份資訊建立本機 Mac 帳戶，提升使用者登入體驗，並讓 IT 更有效管理 Mac 裝置。
- 安全註冊：利用現代身份驗證來監控正在訪問的設備、訪問地點和訪問者，確保在部署任何敏感內容之前，設備上有正確的使用者。
- 消除共用管理員帳戶：透過雲端身份供應商的權限管理，建立多個 IT 管理員帳戶，而無需使用共用服務帳戶。
- 強制執行密碼政策：管理員可透過身份供應商實施密碼策略，確保所有使用者的密碼設定符合安全標準。
- 密碼同步：讓 Mac 使用者名稱與密碼與 Azure、Okta 和 PingFederate 的憑證保持同步，實現單一身份登入，提升工作效率。

*目前 Google Cloud 尚不支援密碼同步功能。

身份識別管理已經 到來，並持續發展

隨著遠端辦公模式、行動工作環境及隨時存取工作資源的需求日益增加，這樣的解決方案已成為企業必需品。Jamf 集所有基礎架構於一身，為使用者與 IT 人員提供順暢的體驗。

[申請免費試用](#) 或聯繫您信賴的
Apple 硬體經銷商開始使用。