管理裝置與企業資料

目錄

概覽

資料是公司最重要的資產之一。不論使用者是在個人擁有或公司提供的裝置上存取企業資料，都要落實個人資料與企業資料的明確區隔，才能保護資料不受攻擊，並避免不慎誤用的情況。Apple 協助 IT 人員輕鬆支援各種層級的裝置管理，也讓使用者在工作上持續發揮最佳生產力。

IT 團隊可以使用「Apple 商務管理」來保護企業持有的裝置，自動為裝置進行註冊，輕鬆快速就能將裝置提供給使用者，無須實際碰觸或親手整備每部裝置。監管功能，則讓 IT 得以存取其他部署模式未能提供的專屬控制項目，包括額外的安全配置、不可移除的 MDM，以及軟體更新管理。

經由「使用者註冊」納入管理的個人裝置，會分別以「管理式 Apple ID」和個人 Apple ID 來區分裝置上的企業和個人資料。這樣就能確保企業資料安全無虞，與任何個人資料明確區隔。當員工離職，或無需再使用某個 app 時，就能將企業資料予以移除。

管理 Apple 裝置

Apple 提供許多裝置管理工具，讓 IT 能順利執行必要的控管，又不會干擾裝置正常運作。成就此一優勢的關鍵，來自 Apple 管理框架與行動裝置管理 (MDM) 解決方案之間的緊密整合。

Apple 針對裝置管理採取的做法

Apple 在 iOS、iPadOS、tvOS 和 macOS 中內建了管理框架，可供 IT 團隊配置並更新設定、部署 app、監控合規情況、查詢裝置，還可遠端清除或鎖定裝置。這套框架同時能支援企業持有和員工持有的裝置，它是裝置部署和管理的基礎。由於這套框架內建於 Apple 作業系統中，所以組織只需做低度的觸及，就能進行所需的管理，而非一逕採取將功能鎖住或停用的做法。這讓 IT 團隊順利進行必要控管的同時，也不致影響使用者體驗和隱私權。

MDM 是什麼？

Apple 結合 MDM 解決方案，讓 IT 能輕鬆部署裝置、發布 app、配置設定，並確保裝置安全無虞。

MDM 支援在每部裝置上的 app、帳號與資料配置，包括強制執行密碼和政策等整合式功能。所有控制項目皆對員工保持透明，並確保員工個人資訊的私密性。如果裝置不慎遺失，IT 團隊也能以安全的方式遠端清除其中的資料。

無論企業採用雲端或內部運作伺服器，都能依據各種功能與價格考量，參考各家廠商不同選項，來購置最適合的 MDM 解決方案，達到靈活整合的目的。

市面上其他的裝置管理方法，可能會為 MDM 功能冠上別的名稱，例如企業行動管理 (EMM) 或統一端點管理 (UEM)。這些解決方案都有一致的目標，也就是透過無線傳輸方式，來管理組織的裝置和企業資料。

MDM 對使用者的影響

Apple 讓 IT 團隊在部署和管理裝置的同時，也能完整保護員工隱私，且不致干擾他們的日常工作。這意味著不論是組織還是員工持有的裝置，功能和裝置都不會因此遭到鎖住或整個停用，資料的使用與收集範圍也有明確限制。

達成這個優勢的關鍵，在於 Apple 將 app 和資料依企業使用和個人使用兩種屬性來建立區隔，並能和大多數的第三方 MDM 解決方案緊密整合，因此 IT 能與 Apple 裝置互動，卻只能看到特定的資訊與設定。不論採用何種部署模式，MDM 框架絕不會存取個人資訊，包括電子郵件、訊息和瀏覽記錄。

MDM 功能在個人裝置上有所限制。

- ✓ 配置帳號
- ✓ 配置「個別 App VPN」
- ✓ 安裝與配置 app
- ✓ 要求輸入密碼
- ✓ 強制執行特定取用限制
- ✓ 存取工作 app 詳細目錄
- ✓ 僅移除工作資料
- ✗ 存取個人資訊
- ✗ 存取個人 app 詳細目錄
- ✗ 移除任何個人資料
- ✗ 收集裝置上的任何記錄
- ✗ 控制個人 app 操作
- ✗ 要求使用複雜密碼
- ✗ 遠端清除裝置上的全部資料
- ✗ 存取裝置位置

裝置持有權方法

裝置可為組織持有，或員工持有。企業持有的裝置通常採用一人一機模式，每位使用者被指派一部專屬裝置，由 IT 進行控管。企業持有的裝置也可能由多名員工共同使用。共用方式包括員工輪班值勤交接，或者多名零售員工使用同一部手持銷售點 (POS) 裝置。企業持有的裝置可以透過監管功能來進行管理，在不鎖定裝置的情況下，運用額外控制項目來管理裝置的配置和取用限制。

使用者持有的裝置也稱為「自攜裝置」(BYOD)，可透過「使用者註冊」的方式來納入管理。這種管理方式能讓員工將個人裝置運用於工作場合。

兩種情境同時指出，Apple 支援各種層級的管理方式，同時注重隱私、安全和資料區隔。

Apple 裝置在受監管的情況下，IT 能實施更多控管措施。

- 配置帳號
- 配置全域代理伺服器
- 安裝、配置與移除 app
- 要求使用複雜密碼
- 強制執行所有取用限制
- 存取所有 app 詳細目錄
- 遠端刪除裝置上的全部資料
- 管理軟體更新
- 移除系統 app
- 修改背景圖片
- 鎖定單一 app
- 略過「啟用鎖定」
- 強制開啟 Wi-Fi
- 讓裝置進入「遺失模式」

企業持有的裝置

IT 可以將企業持有的裝置，配置成僅具備員工職務所需的資料、app 和設定。這些裝置可以透過 MDM 解決方案自動進行部署。若是向 Apple 或 Apple 授權經銷商直接購買的裝置，就能在「Apple 商務管理」中自動註冊，並以無需人工干預的零接觸方式進行部署，IT 團隊無須經手處理每部裝置。

採用企業持有的裝置，組織不僅能進行更高階的控管，也能讓使用者保有隱私，且不干擾裝置的正常使用。註冊企業持有的裝置，意味著 IT 團隊除了配置和安裝帳號與取用限制之外，還能控制 Wi-Fi、VPN、郵件和行事曆的設定。他們可以實施特定的取用限制，防止使用者在裝置上加設帳號。

使用者雖然可以在企業持有的裝置上使用「管理式 Apple ID」、個人 Apple ID 或不使用任何 ID，不過最適合使用的，還是「管理式 Apple ID」。「管理式 Apple ID」是公司專用的帳號，有別於個人建立的 Apple ID。IT 管理者所管理的服務須透過「管理式 Apple ID」進行存取，不適用個人 Apple ID。除此之外，IT 還能藉由監管功能來存取其他部署模式未能提供的專屬控制項目，包括額外的安全配置、不可移除的 MDM，以及軟體更新管理。

不論企業持有的裝置是採用一人一機模式，還是多人合用於共同任務，裝置上的所有資料都能輕鬆確保安全，並獲得充分防護。

使用者持有的裝置

員工使用個人裝置進行工作，可以透過「使用者註冊」來管理企業資料。這是專為 BYOD 方案設計的功能，「使用者註冊」能讓員工保有隱私權，同時保護企業資料的安全，與個人資料建立區隔，並獲得充分防護，所以裝置有個人化的空間，不必像以往一樣處處受限。現在，IT 僅會強制執行特定的設定，就企業規範合規度進行監控，且只能移除企業的資料與 app。IT 團隊不能遠端清除裝置、存取裝置位置，或者存取裝置上的個人資訊或 app。使用者可隨時自行移除 MDM 描述檔，這麼做即可移除所有企業 app 和資料，對照企業持有的裝置，他們更能自主地進行更新和執行其他配置。

使用者必須選擇將裝置註冊到組織的 MDM 解決方案，才能享有「使用者註冊」的功能。一旦完成註冊，他們就能存取企業資源、配置各項設定、安裝設定描述檔，以及安裝企業 app。

「使用者註冊」還能讓個人 Apple ID 和「管理式 Apple ID」在同一部裝置上並用。現有的個人 Apple ID 可供使用者處理個人的所有 iCloud 資料。組織所提供的「管理式 Apple ID」，則能將組織擁有的企業 iCloud 資料完整儲存至由公司控管的「iCloud 雲碟」和「備忘錄」中。

隨著 iOS 15 和 iPadOS 15的推出，使用者現在能直接從「設定」app 註冊他們的裝置。在「設定」中，依序選擇「一般」、「VPN 與裝置管理」，然後點一下「登入公司或學校帳號…」。輸入「管理式 Apple ID」使用者名稱和密碼之後，系統就會啟動身分認證程序。

以這種方式管理資料，使用者對自己的裝置將擁有更多自主權，還能使用「備忘錄」和「iCloud 雲碟」app，將企業資料儲存在單獨設置且加密防護的「Apple 檔案系統」(APFS) 卷宗上，提升企業資料的安全性。如此一來，BYOD 方案更能完善兼顧安全性、隱私權與使用者體驗。如果使用者改用另一部受控裝置或是從公司離職，在裝置取消註冊之後，所有 APFS 卷宗就會立即銷毀。

區隔企業資料的工具

Apple 擁有多種工具，無論你採用何種持有權模式，都能輕鬆區隔裝置上的企業和個人資料。本節內容，將為你介紹如何管理受控的 app、設定、帳號和更多項目中的資料。

受控 App

若要接收組織指派的 app，裝置必須先註冊至 MDM 解決方案中。將 app 指派給裝置後，就會透過 MDM 推播到該裝置。在企業持有的裝置上，會透過監管功能以無提示的方式安裝 app，無需使用者另行操作，也不必使用 Apple ID。

當 IT 或使用者從 MDM 中將裝置取消註冊時，儲存在受控 app 中的資料 (無論裝置是公司或使用者持有) 都會予以刪除。IT 團隊可以防止受控 app 將資料備份到 Finder、iTunes 或 iCloud。若某個 app 經由 MDM 解決方案予以移除後，又由使用者重新安裝，那麼啟用禁止備份的限制可以防止復原受控的 app 資料。

受控設定

使用者註冊到 MDM 之後，可以在「設定」中輕鬆檢視哪些 app 和帳號受到控管，同時查看裝置套用了哪些取用限制。這會將 MDM 安裝的所有企業設定、帳號和內容標示為「受控」狀態。受控設定也包括 Wi-Fi 和 VPN 配置，以及密碼要求。所有設定都可以隨時更新或移除。

取用限制

IT 團隊保護企業資料安全所採取的一項做法，是透過限制來停用分享選項，或無法下載特定的 app。有了 Apple 和個人 MDM 解決方案，IT 就能使用監管功能，對企業持有的裝置進行更高階的控管。他們可運用額外的裝置管理控制功能，包括不可移除的 MDM 等其他部署模式未能提供的專屬項目。除此之外，團隊還能實行各種取用限制，例如停用 iPhone 相機、停用 iCloud、停用 Siri 等。

受控帳號

IT 團隊可以管理裝置上的企業電子郵件、行事曆和聯絡人，協助使用者更快上手，投入工作。為帳號進行控管，能防止使用者加設個人電子郵件、行事曆和聯絡人，避免使用者將裝置個人化，卻能讓 IT 更有效地保護好裝置上的資料。

受控延伸功能

App 延伸功能，可讓第三方開發者為其他 app 開發功能，甚至包括作業系統內建的主要系統，進而在 app 之間創造全新的商務工作流程。為延伸功能進行控管，可防止未受控的延伸功能與受控 app 互動。延伸功能的範例中，「文件提供者」延伸功能可讓生產力 app 從各式雲端服務打開文件；「共享」延伸功能，方便使用者與其他對象共享內容；還有「動作」延伸功能，讓使用者能借用其他 app 的情境，來模擬操作或檢視內容。

iOS 和 iPadOS 適用的受控打開方式

「受控的打開方式」運用三項獨立的功能來保護企業資料：

- **在受控目的地中允許來自未受控來源的文件。**強制執行這項取用限制，有助於防止在組織的受控目的地中打開來自個人來源與帳號的文件。例如，該取用限制可防止使用者在組織的 PDF app 中打開來自隨機網站中的 PDF 文件。
- **在未受控目的地中允許來自受控來源的文件。**強制執行這項取用限制，有助於防止在使用者的個人目的地中打開來自組織的受控來源與帳號的文件。這項取用限制可防止在使用者的任何個人 app 中打開組織受控郵件帳號裡的機密郵件附檔。
- **受控的剪貼板。**在 iOS 15 和 iPadOS 15 或以上版本中，這項取用限制有助於控管在受控和未受控的目的地之間貼上內容。在強制執行上述的取用限制後，貼上內容與否，視第三方或 Apple app (如「行事曆」、「檔案」、「郵件」和「備忘錄」) 之間的「受控的打開方式」界限而定。有了這項取用限制，當內容跨越受控界限時，app 就不能從剪貼板中請求項目。

以最基本的情況而言，這三項功能可為受控裝置區分出兩種環境：一種用於受控的企業 app 和資料，另一種用於未受控的個人 app 和資料。

使用「受控的打開方式」來區隔資料，能讓使用者體驗更順暢。Apple 採取對使用者友善的做法，不鎖住整部裝置，而是讓 IT 團隊能在必要的透明環境中，管理資料來源和目的地，無須依照傳統做法一切從嚴管理。

iOS 和 iPadOS 適用的受控網域

IT 可以管理 iPhone 和 iPad 上的特定 URL 和子網域。舉例來說，若使用者從受控網域下載 PDF，網域會要求該 PDF 必須符合所有受控文件設定。網域之下的路徑會預設為受控。

遺失或遭竊的裝置

裝置不免遇到遺失或遭竊情事。有了 Apple 和 MDM 解決方案，遺失的裝置不會讓有心人有可乘之機，任意存取企業資料。MDM 解決方案可以設定資料保護功能，輸入密碼才能自動打開。此外，受控設定能確保使用者為所有受控裝置設置不易破解的強固密碼。

IT 團隊可以輕鬆遠端鎖定遺失的 macOS 裝置，或為遺失的 iOS 或 iPadOS 裝置打開「遺失模式」。在這兩種情況下，裝置都會被鎖定，直到輸入正確的密碼為止。如果找不到裝置，MDM 解決方案可以遠端鎖定並清除裝置，確保其他人無法存取敏感的企業資料。

身分識別管理

不論組織以何種規模部署 Apple 裝置，身分識別就是使用者向裝置、網站，app 和服務進行認證的核心要素。身分識別已緊密整合到所有作業系統中，使用者可以享有順暢無間、難以察覺任何運作的高直覺體驗。這讓使用者能隨時隨地進行工作，同時讓 IT 團隊能清晰掌握一切，並進行必要控管。有了嚴格的身分識別管理措施，IT 團隊就能事先防止資料洩露，萬一不慎洩露，也能採取明確的後續行動。Apple 開發了許多工具和技術來實現身分識別管理體驗，以下請參考幾個代表性的例子。

裝置認證

Apple 裝置中的身分識別管理，須先經過裝置認證的程序，選擇鎖定螢幕或登入視窗，一旦生效，就能在裝置中全程使用。無論員工使用的是共享的 iPad 還是共享的 Mac，都可以選取個人帳號、輸入個人憑證，然後享有個人化的體驗。透過裝置認證，IT 團隊也能清楚檢視資料中的指令鏈，例如哪位員工存取了哪些檔案項目，以及所進行分享的對象。共享 iPad 上的裝置認證由「管理式 Apple ID」啟用，而在共享的 Mac 上，可以採用本機帳號，或網路帳號來完成認證。

單一登入延伸功能

「單一登入」(SSO) 延伸功能是透過 MDM 解決方案進行配置，可讓原生 app 和 WebKit 提供更順暢的單一登入體驗。這意味著，使用者可以使用現有憑證安全地存取 app，不必建立個別登入資料和密碼。有了 macOS Big Sur 和 iPadOS 14，IT 團隊就能在 macOS 和啟用「共享的 iPad」的 iPadOS 上配置 SSO 延伸功能。而 macOS 還多了其他工具，例如 Kerberos「單一登入」延伸功能，可供與 Active Directory 政策與功能整合，無須使用傳統綁定方式和行動帳號。此外，MDM 解決方案還能管理來自內部和外部憑證授權單位 (CA) 的憑證，以運用用戶端憑證以透明方式進行身分認證，取用安全、受管理信任的服務。

管理式 Apple ID

IT 團隊使用「管理式 Apple ID」在「Apple 商務管理」中為組織管理裝置和 app 購買項目。藉由「管理式 Apple ID」，IT 團隊還能利用一個簡單又安全的身分識別管理架構，那就是聯合認證。結合「管理式 Apple ID」應用的聯合認證，可將已註冊到「Apple 商務管理」中的組織連結至現有的身分識別系統。這會自動將使用者設定為擁有 Apple 服務存取權，因此不需要新的登入憑證。這意味著，當使用者首次使用聯合認證登入其 Apple 裝置時，就會自動建立存取 Apple 服務所需的「管理式 Apple ID」。聯合認證為 IT 團隊和使用者在帳號作業上化繁為簡，確保組織內部所使用的所有 app 和服務，都能一致地強制執行身分識別管理政策。

總結

員工在哪裡，資料就在哪裡，所以確保資料受到保護非常重要。有了 Apple 的管理框架，結合各位所採用的 MDM 解決方案，Apple 就能為使用者賦予能力，讓他們隨時隨地發揮絕佳工作表現。

持續管理旗下裝置和搭建資料區隔框架的同時，以下要點不妨謹記於心：

- 企業持有的裝置可以為企業資料提供最有力的控管和保護。

- 使用者持有的裝置經由「使用者註冊」納入控管後，可以為企業資料提供保護而無須存取個人資料，讓使用者充分保有隱私。
- 使用者隱私和安全性，與保護企業資料同樣重要。
- 裝置和資料的控管，需要大家同心協力，卓越的 IT 團隊會採用對使用者友善的做法來進行。

其他資源

了解 Apple 平台部署：
support.apple.com/zh-tw/guide/deployment/welcome/web

了解「Apple 商務管理」：
support.apple.com/zh-tw/guide/apple-business-manager

了解企業適用的「管理式 Apple ID」：
apple.com/tw/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

了解 Apple at Work：
apple.com/tw/business

了解 IT 功能：
apple.com/tw/business/it

了解 Apple 平台安全性：
apple.com/security

瀏覽適用的 AppleCare 方案：
apple.com/tw/support/professional/

探索 Apple Training：
training.apple.com