



iOS 與 iPadOS 部署概覽

目錄

概覽

持有模式

部署步驟

裝置安全性

支援選項

總結和資源

概覽

iPhone 與 iPad，結合 iOS 與 iPadOS，讓員工不限工作地點都能創造最佳成果。它們也讓 IT 部門能大幅省下管理裝置的時間，將專業能力投入企業策略面，放眼在比技術支援和成本控管更長遠的需求。

本文件將提供為企業組織部署 iOS 與 iPadOS 裝置的相關指引，並協助你為所屬環境所適用的部署計畫奠定良好基礎。

這些主題，包括基於 iOS 與 iPadOS 近期更新項目的相關部署最新資訊，皆會於《[Apple 平台部署](#)》指南線上文件中進一步說明。

持有模式

組織經常會使用下列兩種 iOS 與 iPadOS 裝置持有模式：

- 組織持有
- 使用者持有

兩種模式各有其優勢，因此，請務必考量最符合組織需求的選擇。雖然大多數組織會擇一而行，你也能在所屬環境中採用兩種模式並行的做法。

找到你的組織所適用的模式，你的團隊就能開始深入探索 Apple 的部署與管理功能了。

組織持有的裝置

在組織持有的模式中，裝置是由你的組織或是參與相關方案的 Apple 授權經銷商或電信業者所購買。如果裝置以一人一機的方式提供，就是所謂的一對一部署。裝置也可供多名使用者輪流使用，一般稱之為共享部署。「共享 iPad」就是共享部署的範例之一，可讓多名使用者在不共用資訊的情況下共享 iPad 裝置。組織可在整體環境中結合共享和一對一部署模式。

使用組織持有模式時，IT 可透過監管和「自動裝置註冊」保有更高層級的控制權，如此一來，組織就能自裝置開箱的那一刻起，立即配置和管理裝置。

進一步了解受監管裝置的限制：

support.apple.com/guide/deployment/welcome/web

Apple 裝置接受監管時，IT 擁有更大的控制權。

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

使用者持有的裝置

在使用者持有模式中，使用者會自行購買、設定和配置裝置。這些類型的部署一般稱為 BYOD，或稱為自攜裝置部署。使用者通常須要在組織的行動裝置管理 (MDM) 解決方案中註冊其裝置，才能使用組織服務 (例如 Wi-Fi、郵件和行事曆)，或配置裝置以符合特定教育或商務需求。他們會透過名為「使用者註冊」的 Apple 功能來實行這些步驟。

「使用者註冊」可讓企業資源和資料安全地受到管理，同時也尊重使用者的隱私以及他們的個人資料和 app。IT 可強制執行、存取和管理下方表格所列的特定功能。

使用者須透過自己的「管理式 Apple ID」，才能在個人裝置上存取企業資料。「管理式 Apple ID」是「使用者註冊」描述檔的一部分，使用者必須成功通過認證，才能完成註冊。「管理式 Apple ID」可以和使用者已登入的個人 Apple ID 一起使用，兩者之間不會產生任何互動。這會在裝置上建立資料區隔。如果組織具有 iCloud 儲存空間，就會為適用「管理式 Apple ID」的所有受管理資料，建立個別的「iCloud 雲碟」。

進一步了解 MDM 解決方案中的「使用者註冊」：

support.apple.com/guide/deployment/welcome/web

MDM 功能在個人裝置上的限制。

✔ 配置帳號	✗ 存取個人資訊
✔ 配置「個別 App VPN」	✗ 存取個人 app 詳細目錄
✔ 安裝與配置 app	✗ 移除任何個人資料
✔ 要求輸入密碼	✗ 收集裝置上的任何紀錄
✔ 強制執行特定取用限制	✗ 接管個人擁有的 app
✔ 存取工作 app 詳細目錄	✗ 須使用複雜密碼
✔ 僅移除工作資料	✗ 遠端清除整部裝置
	✗ 存取裝置位置

部署步驟

本節將概要說明部署裝置與內容的五個步驟，範圍涵蓋準備環境、設定裝置、展開部署與進行管理。你所使用的步驟，將視裝置為組織持有或使用者持有而定。

若要進一步了解這些步驟，請造訪 [《Apple 平台部署》](#) 指南線上文件。

1. 整合與設定

為你的組織找出適當的部署模式後，請務必為部署做好各項準備工作。

MDM 解決方案：Apple 為 iOS 與 iPadOS 提供的管理框架，讓組織能夠安全地在企業環境中註冊裝置、以無線方式配置及更新設定、監控政策合規情況、部署 app，並可遠端清除或鎖定受管理裝置。這類管理功能會透過第三方 MDM 解決方案啟用。種類繁多的第三方 MDM 解決方案，可支援不同的伺服器平台。每種解決方案都提供不同的管理主機、功能與價位。

Apple 商務管理：這個網頁式入口網站可讓 IT 管理者集中部署 iPhone、iPad、iPod touch、Apple TV 和 Mac。「Apple 商務管理」能與你的 MDM 解決方案順暢搭配運作，可供輕鬆地進行自動裝置部署、購買 app 和發布內容，以及為員工建立「管理式 Apple ID」。

管理式 Apple ID：與個人 Apple ID 一樣，管理式 Apple ID 會用來登入 Apple 裝置與服務，例如 FaceTime、iMessage、App Store、iCloud、iWork 和「備忘錄」，讓使用者可以存取各種內容和功能，藉此提升生產力並支援各方合作。不過，管理式 Apple ID 是由組織所持有，且為 Apple 裝置管理不可或缺的一環。這些帳號讓你的組織可以管理密碼重置和以角色為基礎的管理等功能，並且具有特定的限制設定。

進一步了解「管理式 Apple ID」：

support.apple.com/guide/apple-business-manager

Wi-Fi 與網路連線：Apple 裝置內建安全的無線網路連線功能。請確認公司的 Wi-Fi 網路可以支援多部裝置，且可供你所有的使用者同時連線。請確保你的網路基礎設施已完成設定，可與 Bonjour 正確搭配運作。Bonjour 是 Apple 所開發、以業界標準為基礎的零配置網路協定。Bonjour 可讓裝置自動尋找網路上的服務。iOS 與 iPadOS 裝置會使用 Bonjour 來連接與 AirPrint 相容的印表機，以及與 AirPlay 相容的裝置，例如 Apple TV。而部分 app 會使用 Bonjour 來尋找其他裝置，以進行合作與共享。

進一步了解 Wi-Fi 和網路連線：

support.apple.com/guide/deployment/welcome/web

進一步了解 Bonjour：

developer.apple.com/bonjour

VPN：評估 VPN 基礎設施，確定使用者可以從 iOS 與 iPadOS 裝置，在遠端安全存取公司資源。請考慮使用 iOS 與 iPadOS 的「隨選即用 VPN」或「個別 App VPN」功能，讓 VPN 連線僅在需要時才會啟動。若規劃使用「個別 App VPN」功能，請確定 VPN 閘道支援這些功能，而且已購買充足的授權以供應適當的使用者人數與連線負載。

郵件、內容和行事曆：iPhone、iPad 和 Mac 能與 Microsoft Exchange、Office 365 和其他熱門電子郵件服務（例如 Google Workspace）搭配運用，在加密的 SSL 連線上使用即時存取來推播電子郵件、行事曆、聯絡人和工作。若使用 Microsoft Exchange，請先確核 ActiveSync 服務為最新版本，並配置為支援網路上所有使用者。若使用雲端版的 Office 365，請確定你有足夠的授權，來支援可能會連線使用的 iOS 與 iPadOS 裝置數量。iOS 與 iPadOS 也運用 OAuth 2.0 與多重認證功能，支援 Office 365 新式認證。若未使用 Exchange，iOS 與 iPadOS 也可以和 IMAP、POP、SMTP、CalDAV、CardDAV 和 LDAP 等標準型伺服器搭配使用。

2. 身分識別管理

除了準備你的環境之外，IT 團隊還須選擇他們想要管理身分驗證和授權的方式，為部署做好進一步準備。這有助於確保裝置和資料安全。

認證：認證方法有很多類型。使用單一登入和 Apple 服務，例如**管理式 Apple ID**、iCloud、iMessage 等，可讓使用者安全地通訊、線上建立文件以及備份個人資料，過程間都不會對組織的資料帶來損害。每項服務都會使用本身的安全架構，來確保達到以下目標：安全處理資料（無論是在 Apple 裝置上還是透過無線網路傳輸）、保護使用者的個人資料，以及防止惡意或未經授權存取資訊和服務的威脅。MDM 解決方案可用來限制和管理對 Apple 裝置上特定服務的存取。

進一步了解單一登入：

support.apple.com/guide/deployment/depfdbf18f55/1/web/1.0

進一步了解 Kerberos 單一登入：

support.apple.com/guide/deployment/depe6a1cda64/1/web/1.0

授權：授權與驗證是不同的程序。驗證是證明你的身分，授權則是定義你被允許執行的動作。例如，這可以透過向 IdP 提供使用者名稱和密碼來完成。在本範例中，授權機構是你的身分提供者或 Active Directory，認證聲明是使用者名稱和密碼，而代號是成功登入後收到的資料。其他可以使用的認證聲明，包括憑證、智慧卡、其他多重認證裝置。

身分聯合驗證：身分聯合驗證要求管理者設定網域，使彼此相互信任，並就識別使用者的方法達成一致。一個常見的例子是，使用你的企業帳號登入雲端身分提供者。例如，IT 團隊可以啟用 Microsoft Azure Active Directory (Azure AD) 和「Apple 商務管理」之間的聯合驗證，以簡化組織建立管理式 Apple ID 的程序。然後，使用者將使用他們現有的 Azure AD 憑證來登入 iCloud，或是登入與「Apple 商務管理」相關聯的 Apple 裝置。

3. 部署規劃和佈建

完成準備工作後，即可著手配置裝置並準備發布內容。只要使用 MDM 解決方案，搭配「Apple 商務管理」或 Apple Configurator 2，就能讓所有的持有和部署模式發揮最佳成效。

自動裝置註冊

這個註冊方式可透過快速且簡潔的方式，在無須實際接觸或準備每部裝置的情況下，部署企業持有的 Apple 裝置，並將其註冊到 MDM 中。對終端使用者而言，IT 團隊可將「設定輔助程式」中的步驟化繁為簡，讓設定流程更明快簡潔，以確保員工能在裝置啟用後，立即收到正確的配置。只有直接向 Apple 購買或是向參與相關方案的 Apple 授權經銷商或電信業者購買的裝置，才能透過「自動裝置註冊」進行部署。

裝置註冊

裝置也可透過 Apple Configurator 2 或組織的 MDM 解決方案來手動部署。無論是企業持有或使用者持有的裝置，都可透過「裝置註冊」進行部署。手動管理的裝置在運作上，與其他任何指派裝置一樣，須要接受必要的監管和 MDM 註冊。IT 團隊管理的裝置中，如果包括不是直接購自 Apple 或是參與相關方案的 Apple 授權經銷商或電信業者的裝置，就很適合使用這個部署方法。

進一步了解 Apple Configurator 2：

support.apple.com/zh-tw/apple-configurator

使用者註冊

使用者持有的裝置，可透過「使用者註冊」來配置和部署，這讓 IT 在即使沒有鎖定裝置的情況下，也能保護企業資料。請參閱 <持有模式> 小節，進一步了解「使用者註冊」。

無論裝置為組織或使用者所持有，IT 團隊都能在發布裝置時，透過「設定輔助程式」掌控設定體驗。「設定輔助程式」會由你的 MDM 解決方案加以配置，且可讓使用者立即使用其裝置。

裝置註冊之後，管理者可啟動 MDM 政策、選項或指令；可用於裝置的管理動作，將依據監管與註冊方式而有所不同。之後，iOS 或 iPadOS 裝置就會收到透過「Apple 推播通知」服務 (APNs) 傳送的管理者動作通知，透過安全的連線，直接與所屬的 MDM 伺服器通訊。APNs 可透過網路連線，將指令傳送到位於世界各地的裝置。不過，APNs 並不會傳輸任何機密或專屬資訊。

4. 配置管理

Apple 裝置內建安全的管理框架，可讓 IT 使用各種管理功能來管理裝置。這個管理框架可劃分為四個部分：

設定描述檔

設定描述檔包含承載資料，可將設定和授權資訊載入 Apple 裝置。設定描述檔可以自動進行設定、帳號、取用限制與憑證的配置。依據 MDM 解決方案供應商，還有方案本身與公司內部系統的整合狀況，系統可為帳號預先填寫使用者名稱、郵件地址，並在適用的情況下，填入可供認證和簽署用的憑證身分識別等承載資料。

限制

限制可在無須鎖定裝置的情況下，讓你強制執行安全政策，並協助使用者保持專注。限制的範例包括多種功能，例如「受管理的打開方式」，可以防止在未受管理的目標位置開啟來自受管理來源的附件或文件；還有「單一 App 模式」，可將裝置限制為僅執行單一 app；以及「防止備份」，可防止受管理 app 將資料備份到 iCloud 或裝置。

管理作業

裝置受到控管時，MDM 伺服器可以執行各種管理作業，包括無須使用者操作即可自動變更配置設定、在以密碼鎖定的裝置上執行軟體更新、遠端鎖定或清除裝置，或是清除密碼鎖定，讓使用者在忘記密碼時進行重置。MDM 伺服器也可以要求 iPhone 或 iPad 開始 AirPlay 鏡像輸出至特定的目標位置，或結束目前的 AirPlay 工作階段。你可防止使用者透過無線方式手動更新受監管的裝置，最多可延後 90 天。你也能使用 MDM 解決方案，為受監管的裝置排程軟體更新。

查詢

透過 MDM 伺服器可查詢裝置的各種資訊，包含硬體詳細資訊，如序號、裝置 UDID 或 Wi-Fi MAC 位址；以及軟體詳細資訊，如 iOS 或 iPadOS 版本與裝置所安裝的所有 app 詳細列表。你的 MDM 解決方案可以使用這類資訊，保有最新的詳細目錄資訊、做出明智的管理決策，並自動執行各項管理作業，例如確保使用者擁有一組最適用的 app。

5. 內容發布

在註冊完成後，管理者現也能使用受管理發布。這可讓 MDM 解決方案或 Apple Configurator 2 在有提供該款 app 的任何國家或地區，對購自「Apple 商務管理」商店的所有 app 進行管理。若要啟用受管理發布，你必須先使用一組安全代號，將 MDM 解決方案連結到你的「Apple 商務管理」帳號。連接 MDM 伺服器之後，不論裝置上的 App Store 是否為停用狀態，皆可指派「Apple 商務管理」app。

可發布給使用者的內容，目前僅限受管理的 app。受管理 app 可由 MDM 伺服器進行遠端部署和移除，或在使用者的裝置退出 MDM 後一併移除。移除 app 也會一併移除與其相關聯的資料。

將內容發布給使用者，可透過兩種方式：

將 app 指派給裝置：你可以使用 MDM 解決方案或 Apple Configurator 2，將 app 直接指派給裝置。在初次導入時採用這種方式，可以省略數個步驟，不僅大幅提高部署的簡易度與速度，還能讓你全權掌控受管理裝置與內容。將 app 指派給裝置後，即可將該 app 透過 MDM 推播至裝置，不須發送邀請給使用者。該裝置的所有使用者，都能取用該 app。

將 app 指派給使用者：另外一種方法是使用 MDM 解決方案，透過電子郵件或推播通知訊息，邀請使用者下載 app。使用者若要接受邀請，須以個人 Apple ID 登入他們的裝置。Apple ID 在註冊「Apple 商務管理」服務之後，仍完全保有其私密性，管理者也無法看見。使用者一旦同意接受邀請，就會連接到你的 MDM 伺服器，開始接收所指派的 app。這些 app 會自動出現在使用者的所有裝置上等候下載，不需要額外的操作或成本。

若某個裝置或使用者不再需要某些已指派的 app，你可將 app 撤銷，再重新指派給不同的裝置或使用者，你的組織對於所購買的 app 始終保有完整的持有權與控制權。

裝置安全性

Apple 從設計之初，就為裝置融入先進的安全性。裝置設定完成之後，內建的安全功能，以及透過 MDM 提供的額外控制項目，就成為協助 IT 團隊管理和保護企業資料的一大功臣。而跨越 app 的通用框架，則有助於啟用配置，並持續管理設定。

進一步了解 Apple 平台安全性：

support.apple.com/guide/security/welcome/web

保護工作資料：IT 部門可透過 MDM，來強制執行與監控安全性政策。舉例來說，在 iOS 與 iPadOS 裝置上要求輸入密碼，會自動啟用「資料保護」，為裝置提供檔案加密。而 MDM 可用來配置 Wi-Fi 和 VPN，以及部署憑證，建立更多的安全保障。

MDM 解決方案可提供更精細的裝置管理等級，無需任何容器，使企業資料安全無虞。透過「受管理的打開方式」，IT 可設定限制，以防止附件或文件在未受管理的目標位置開啟。

鎖定、尋找和清除：即使裝置遺失，也不會造成企業資料外流。IT 可遠端鎖定 iOS 與 iPadOS 裝置並刪除其中所有機敏資料，保護公司的資訊安全。IT 可為受監管的 iOS 與 iPadOS 裝置啟用「遺失模式」，查看裝置所在的位置。IT 還擁有管理公司 app 的工具，這可以在不清除個人資料的情況下，立即從裝置中移除公司 app。

App：得力於共通的框架與受控的生態系統，Apple 平台上的 app 皆具備了講求安全性的設計。我們的開發者方案會驗證所有開發者的身分，在 App Store 上發布 app 之前，也會經過系統驗證。Apple 為開發者提供多種功能的框架，包括簽署、app 延伸功能、授權及沙箱機制，來確保更高階的安全防護。

遺失模式：MDM 解決方案可從遠端將受監管裝置設為「遺失模式」。這個動作可以鎖定裝置，並在裝置的鎖定畫面上顯示訊息與電話號碼。受監管裝置進入「遺失模式」之後，MDM 可從遠端查詢受監管裝置最後上線的位置，定位遺失或遭竊的裝置。「遺失模式」不須啟用「尋找」功能。

啟用鎖定：使用者開啟受監管裝置的「尋找」功能時，就能使用 MDM 來開啟「啟用鎖定」功能。這可讓你的組織享有「啟用鎖定」防竊功能所帶來的好處，另一方面，遇到使用者無法以他們的 Apple ID 驗證的情況，你也能略過這項功能。

支援選項

Apple 提供各種服務專案和支援資源。

AppleCare OS Support 方案

AppleCare OS Support 方案可針對 iOS 及 iPadOS 伺服器部署，為 IT 部門提供企業級電話與電子郵件支援。視你所購買的支援層級而定，它能提供 24 小時全年無休的支援，以及一位指定的技術客戶經理。AppleCare OS Support 方案可讓 IT 員工直接聯繫技術人員，以處理整合、移轉和進階伺服器運作的相關問題，大幅提升他們部署與管理裝置以及解決問題的效率。

AppleCare Help Desk Support 方案

AppleCare Help Desk Support 方案可提供與 Apple 資深技術支援專家優先通話的權利，它也包含一套診斷與排解 Apple 硬體疑難的工具，可協助大型組織更具效率地管理資源、加快回應速度並減少培訓成本。AppleCare Help Desk Support 方案提供不限事故次數的支援服務，範圍涵蓋 iOS 和 iPadOS 裝置的硬體與軟體診斷、疑難排解與問題釐清。

分別適用於 iPad、iPhone 與 iPod touch 的 AppleCare+ 服務專案

每部 iOS 與 iPadOS 裝置均隨附一年有限保固，以及自購買日起 90 天免額外付費電話技術支援。凡購買分別適用於 iPhone、iPad 與 iPod touch 的 AppleCare+ 服務專案，即可將服務期限延長為原購買日起兩年。你可以隨時致電聯繫 Apple 的技術支援專家，詢問各種問題。裝置需要維修時，Apple 也有便利的維修服務選項。此外，這些專案也提供多達兩次意外損壞的保固服務，每次服務視情況酌收服務費。

iOS Direct Service Program

iOS Direct Service Program 是 AppleCare+ 服務專案提供的服務，能讓你的服務台人員可自行找出有問題的裝置，而無須致電 Apple 支援或造訪 Apple 直營店。如有需要，你的組織可直接透過此專案來訂購替換用的 iPhone、iPad、iPod touch 或包裝盒內的配件。

進一步了解各項 AppleCare 專案：

apple.com/tw/support/professional

總結和資源

無論你的公司想為部分使用者或整個組織部署 iPhone 或 iPad，都有許多選項可供輕鬆部署與管理裝置。為你的組織選擇適當的部署策略，可以協助員工提高生產力，並以全新方式完成工作。

了解 iOS 與 iPadOS 的部署、管理和安全功能：

support.apple.com/guide/deployment/welcome/web

了解「Apple 商務管理」：

support.apple.com/guide/apple-business-manager

了解企業適用的「管理式 Apple ID」：

[apple.com/tw/business/docs/site/](https://apple.com/tw/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf)

[Overview_of_Managed_Apple_IDs_for_Business.pdf](https://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 專案：

apple.com/tw/support/professional

探索 Apple 培訓與認證相關資訊 (英文版)：

training.apple.com

測試 Beta 版本軟體、加入測試計畫，以及提供意見反映：

beta.apple.com/zh-TW