



Mac 部署概覽

簡介

Mac 結合 macOS 的強大威力，可讓員工在任何地點充分發揮工作效率。此外，IT 部門也能藉此省下管理裝置的時間，進而得以著手調整業務策略，不用再費心修正技術和削減成本，將目光放在更遠大的層面。

本文件將提供在組織部署 macOS 裝置的相關指引，並協助你為自身環境所適用的部署方案打下良好根基。

當中的幾個主題，包括使用最新 macOS 更新進行部署的最新資訊，皆會於線上的《[Apple 平台部署指南](#)》中進一步說明。

持有模式

組織經常會使用下列兩種 macOS 裝置持有模式：

- 組織持有
- 使用者持有

每個模式都有各自的優勢，因此，請務必選擇最適合你的組織的選項。雖然大多數組織都有其偏好的模式，你仍可能在你的組織環境中遇到多重模式。

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。

組織持有的裝置

在組織持有的模式中，裝置是由你的組織所購買，或是由參與計劃的 Apple 授權經銷商或電信業者所購買。如果裝置會提供給每一名使用者，就是所謂的「一對一部署」。另外，裝置也可供多名使用者輪流使用，通常又稱為「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」保有更高的控制權，如此一來，組織就能自裝置開箱的那一刻起，立即設定和管理裝置。

進一步了解受監管裝置的相關限制：

support.apple.com/zh-tw/guide/mdm

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 | ✓ 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 |
| ✓ 要求使用複雜密碼 | ✓ 鎖定單一 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。儘管 BYOD 部署在 macOS 裝置上比較少見，你的組織仍可使用此一模式。使用者通常需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)，或設定裝置以符合特定教育或業務需求。這項作業就是所謂的「使用者註冊」。

「使用者註冊」可讓企業資源和資料安全地進行管理，同時也尊重使用者的隱私與個人資料和 app。IT 可強制執行、存取和管理下方表格列出的特定功能。

使用者需要運用其「管理式 Apple ID」，以便在自身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，就會為使用「管理式 Apple ID」管理的所有資料，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」功能：

support.apple.com/zh-tw/guide/mdm

MDM 功能在個人裝置上有所限制。

- | | |
|------------------|-----------------|
| ✓ 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 | ✗ 收集裝置上的任何記錄 |
| ✓ 強制執行特定取用限制 | ✗ 控制個人 app 操作 |
| ✓ 存取工作 app 詳細目錄 | ✗ 要求使用複雜密碼 |
| ✓ 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四個步驟：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，請造訪線上的《[Apple 部署指南](#)》。

1. 整合與設定

為你的組織找出適當的部署模式後，請務必著手下部署基礎。

MDM 解決方案：Apple 為 macOS 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，能輕鬆地自動部署裝置、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：這個 Apple ID 可讓使用者登入眾多 Apple 服務，例如 FaceTime、iMessage、App Store 和 iCloud，藉此存取有助於提高生產力並支援合作的各種內容和服務。如同任何 Apple ID 一樣，「管理式 Apple ID」會用來登入個人裝置，也是 Apple 裝置管理不可或缺的一環。「管理式 Apple ID」可依照個人 Apple ID 的方式，啟用 Apple 服務（包括 iCloud 以及使用 iWork 與「備忘錄」合作）的存取權限。不過，「管理式 Apple ID」是由組織持有並管理，包括密碼重置與依職務進行分工的管理，也都是由組織負責。「管理式 Apple ID」具有某些限制設定。

進一步了解「管理式 Apple ID」：

support.apple.com/zh-tw/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。請確定公司的 Wi-Fi 網路可以支援多個裝置，且可供你所有的使用者同時連線。Apple 與 Cisco 已針對 Mac 電腦與 Cisco 無線網路間的通訊進行最佳化，使其支援頻寬管理 (QoS) 等 macOS 中的進階網路功能。如果有 Cisco 網路設備，請與你的內部團隊合作，確認 Mac 能夠將關鍵流量最佳化。請確認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。macOS 使用 Bonjour 來連接與 AirPrint 相容的印表機以及與 AirPlay 相容的 Apple TV 等裝置。部分 app 和內建 macOS 功能會使用 Bonjour 來尋找其他裝置，以進行合作與共用。

進一步了解 Wi-Fi 與網路連線：

support.apple.com/zh-tw/guide/deployment-reference-ios

進一步了解如何配置網路以供 MDM 使用：

support.apple.com/zh-tw/HT210060

進一步了解 Bonjour：

developer.apple.com/library

VPN：請評估 VPN 基礎設施，確保使用者能安全地遠端存取公司資源。你可考慮使用 macOS 的「隨選即用 VPN」功能，只在有需要時，才啟動 VPN 連線。如果你計畫使用「個別 App VPN」，請查看 VPN 閘道是否支援這些功能，以及所購買的授權數量是否足以涵蓋合理的使用者與連線數量。

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 G Suite) 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、通訊錄和工作。若使用 Microsoft Exchange，請確定 ActiveSync 服務為最新版本，並設定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，可支援預期連線使用的 macOS 裝置數量。

管理身分識別：macOS 可存取包含 Active Directory、Open Directory 和 LDAP 在內的目錄服務，來管理身分識別和其他使用者資料。部分 MDM 廠商提供開箱即用的工具，將其推出的管理解決方案，與 Active Directory 及 LDAP 目錄加以整合。其他工具包括 macOS Catalina 中的 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。你的 MDM 解決方案可管理來自內部和外部憑證授權單位 (CA) 的各類型憑證，如此即可自動信任身分識別。

進一步了解新的「Kerberos 單一登入」延伸功能：

support.apple.com/zh-tw/guide/deployment

進一步了解目錄整合：

support.apple.com/zh-tw/guide/deployment

核心員工服務：請確認 Microsoft Exchange 的服務是在最新狀態，並已經過配置可支援所有網路上的使用者。若未使用 Exchange，macOS 也可與標準型伺服器搭配運作，包括 IMAP、POP、SMTP、CalDAV、CardDAV 和 LDAP。關於電子郵件、聯絡人、行事曆，以及使用者在重要的日常工作流程中使用比例最高的其他企業生產力與合作軟體，請針對基本工作流程進行測試。

進一步了解 Microsoft Exchange：

support.apple.com/zh-tw/guide/deployment

進一步了解標準型服務：

support.apple.com/zh-tw/guide/deployment

內容快取：macOS 內建的快取服務，可為經常需向 Apple 伺服器要求的內容，儲存一份本機拷貝，有助於將下載內容所需的網路頻寬用量降到最低。你可利用快取，來加快透過 Mac App Store 下載與傳送軟體的速度。它還能快取軟體更新項目，以供組織的裝置快速下載，無論裝置使用 macOS、iOS 或 iPadOS，皆可適用。其他內容也可以透過 Cisco 和 Akamai 提供的第三方解決方案來快取。

進一步了解內容快取：

support.apple.com/zh-tw/guide/deployment

2. 部署規劃和佈建

打下良好根基後，即可著手設定裝置並準備發布內容。只要使用 MDM 和「Apple 商務管理」，或透過 MDM 和 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」中的步驟去蕪存菁，藉此簡化設定流程，從而確保員工能在啟用後立即收到正確的設定。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。不過，透過一般通路以外的管道所購買或募集到的部分 Mac 電腦，也可支援「自動裝置註冊」。Apple 導入了新的 iPhone 版 Apple Configurator app，以因應這些情境。IT 團隊可以透過 iPhone 版 Apple Configurator，將任何搭載 macOS Monterey 的受支援 Mac 輕鬆指派到所屬組織的「Apple 商務管理」帳號中，以充分運用「自動裝置註冊」提供的所有出色裝置管理功能。

進一步了解 iPhone 版 Apple Configurator：

support.apple.com/zh-tw/guide/apple-configurator/welcome/ios

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」部署。手動管理裝置的行為與其他任何指派裝置一樣，需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

如果是使用者持有的裝置，可透過「使用者註冊」來設定和部署，如此 IT 即使在沒有鎖定裝置的情況下，也能保護企業資料。如需「使用者註冊」的詳細資訊，請參閱 [<持有模式>](#) 一節。

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」會使用你的 MDM 解決方案加以設定，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，macOS 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。

3. 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，並填入可供認證和簽署用的憑證身分識別等承載資料。

限制

限制可在無需鎖定裝置的情況下，讓你強制執行安全政策，並協助使用者保持專注。限制會包含「清除所有內容和設定」等功能，可將 Mac 迅速重置為目前的作業系統版本，並在過程中以密碼演算技術移除所有使用者資料。

管理作業

裝置接受管理時，MDM 伺服器可執行各式管理作業，包括無須與使用者互動即可自動變更配置設定、執行 macOS 更新、遠端鎖定或清除裝置，或是管理密碼。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 macOS 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項資訊，來維護最新存貨資訊、做出明智的管理決策，並自動管理各項作業，例如確保使用者具有一組適當的 app。MDM 還可以查詢重要安全功能的狀態，像是「檔案保險箱」或內建防火牆。

受管理軟體更新

在有可用的升級項目時，IT 可讓使用者選擇升級至最新的作業系統。藉由測試發行前版本 macOS，可確保 IT 提早發現應用程式相容性問題，並讓開發者在正式發布前謀求解決。IT 可透過 Apple Beta 版軟體計畫或 AppleSeed for IT，參與各版本的測試。若要讓使用者及其資料獲得保護，請採取完整措施，讓 Mac 電腦保持在最新狀態。請經常更新，並在確定你的工作流程與新版 macOS 相容時，盡速完成升級。

MDM 可以將 macOS 更新項目，自動推播給已註冊的 Mac 裝置。若重要系統尚未準備就緒，也可以配置已註冊的 Mac 裝置延後更新，將更新項目與更新通知延後到最多 90 天以後。在移除此政策或在 MDM 傳送安裝指令之前，使用者將無法手動啟動更新。

Apple 不建議也不支援以建立單體系統映像檔的方式來升級 macOS。如同 iPhone 與 iPad，Mac 電腦通常也需要安裝各機型專用的韌體更新，才能運作。同樣地，如要更新 Mac 作業系統，則必須直接透過 Apple 來安裝這些韌體更新。最可靠的策略，是使用 macOS 安裝程式或 MDM 指令來進行更新。

其他受管理的軟體

組織經常需要在最初提供給使用者的一組 app 之外，另行發布其他 app。可以由 MDM 來自動處理關鍵應用程式和更新，也可讓員工透過 MDM 解決方案提供的自助式入口網站，來申請應用程式。這些入口網站可以提供各項服務，包括安裝經「Apple 商務管理」向 App Store 購買的軟體，以及安裝非 App Store 的 app、工序指令及其他工具程式。

雖然大部分軟體都能自動安裝，有些特定的安裝，可能需由使用者進行操作。為了提升安全性，所有需要核心延伸功能的 app，現在都必須經過使用者的同意才能載入。這項功能稱為「使用者核准載入核心延伸功能」，可透過 MDM 進行管理。

4. 內容發布

在註冊完成後，管理者也可使用受管理發布。這可讓 MDM 或 Apple Configurator 2 在有提供 app 的任何國家或地區，管理購自「Apple 商務管理」商店的所有 app。若要啟用受管理發布，你必須先以一組安全的代碼，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。

受管理 app 可由 MDM 伺服器進行遠端部署和移除，或在使用者從 MDM 移除自己的裝置時一併移除。移除 app 也會一併移除與其關聯的資料。

將內容發布給使用者的方式共有兩種：

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，同時你也能全權掌控受管理裝置與內容。將 app 指派給裝置後，即可將其透過 MDM 推播至裝置，不需要發送邀請給使用者。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，而你的組織對於所購買的 app 一直保有完整的持有權與控制權。

準備額外的內容：MDM 解決方案可協助你發布額外的套件，這些套件包含非來自 Mac App Store 的內容。這是適用於許多企業軟體套件（如內部自訂的應用程式，或 Chrome 或 Firefox 等 app）的常用方法。你可使用此方法來推送必要的軟體，並在完成登記後自動安裝。字體、工序指令或其他項目，也可透過套件來安裝與執行。請確保這些套件皆以你在 Developer Enterprise Program 所使用的開發者 ID 正確簽署。

裝置安全性

Apple 的安全性，是從裝置的設計開始做起。裝置設定完成後，即可透過你的 MDM 解決方案，使用內建的安全功能和其他適用的額外控制項目，來管理和保護企業資料。內建的安全功能，以及透過 MDM 提供的額外控制項目，為協助 IT 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/zh-tw/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 macOS 裝置上透過 MDM 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，以提升安全性。

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。內建的安全功能可讓 IT 進行資料加密，並保護裝置免受惡意軟體侵擾，同時強制執行安全性設定，無需採用第三方工具。

鎖定、尋找和清除：即使裝置遺失，企業資料仍可充分受到保障。IT 可遠端鎖定 iOS、iPadOS 與 macOS 裝置並刪除其中所有機敏資料，保護公司的資訊安全。針對受監管的 macOS 裝置，IT 可啟用「尋找」來查看裝置的所在位置。IT 還擁有多種工具，可進行企業 app 控管，能在不清除個人資料的情況下，立即自裝置移除 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，來提供更高階的安全防護。

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。使用「遺失模式」不須啟用「尋找」。

啟用鎖定：在 macOS Catalina 或以上版本中，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

許多組織發現，Mac 使用者只需最低限度的 IT 支援。為鼓勵自助式支援，並提升支援品質，多數的 IT 團隊會開發自助式支援工具。例如，建立穩固的 Mac 支援網頁、開設自助論壇，以及提供現場技術支援櫃台。MDM 解決方案也可讓使用者執行支援工作，例如從自助式入口網站安裝或更新軟體。

基於最佳做法，公司不應讓使用者全憑一己之力來尋求支援，而是改採合作方式來解決問題。請協助使用者先自行調查和疑難排解問題，再與服務台聯繫，藉此鼓勵他們在過程中做出貢獻。

共同承擔資源責任有助於縮短員工的停機時間，並減少支援成本和人力的整體負擔。組織若有更多需求，AppleCare 還為員工與 IT 提供各式方案和服務，與內部支援結構搭配運作。

AppleCare OS Support

AppleCare OS Support 專業級支援針對 iOS、iPadOS、macOS 及 macOS 伺服器部署，為 IT 部門提供企業級電話與電子郵件支援。依據所購買的支援層級而定，它能提供 24 小時全年無休的支援，並指派一位專屬的技術客務經理。AppleCare OS Support 專業級支援可讓 IT 員工直接聯繫技術人員，來處理整合、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

AppleCare Help Desk Support 可提供與 Apple 資深技術支援人員優先通話的權利，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 提供不限事故次數的支援服務，範圍涵蓋 iOS 和 iPadOS 裝置的軟硬體診斷、疑難排解與問題釐清。

適用於 Mac 的 AppleCare 與 AppleCare+ 服務專案

每部 Mac 電腦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。若購買適用於 Mac 的 AppleCare+ 服務專案或 AppleCare Protection Plan 全方位服務專案，即可將服務涵蓋範圍延長為原購買日期起三年。員工可以致電 Apple 支援，洽詢 Apple 軟硬體的相關問題。裝置需要維修時，Apple 也有便利的維修服務選項。此外，適用於 Mac 的 AppleCare+ 服務專案可提供特定事故的意外損壞保固，每次服務視情況酌收服務費。

進一步了解 AppleCare 支援選項：

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 Mac 電腦，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 macOS 的部署、管理與安全功能：

support.apple.com/zh-tw/guide/deployment/welcome/web

Apple Configurator 使用手冊：

support.apple.com/zh-tw/guide/apple-configurator/welcome/ios

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/](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 方案：

apple.com/tw/support/professional

探索 Apple 的培訓與認證：

training.apple.com

測試 Beta 版本軟體、加入測試計畫，以及提供意見反映：

appleseed.apple.com/sp/welcome