



# Mac 部署概覽

# 簡介

Apple 相信，工欲善其事，必先利其器。提供員工最佳工具與技術，他們就能在工作上大放異彩。我們所有產品的設計，讓員工無論在公司裡外，都能大幅提升創造力與生產力，工作方式煥然一新。這正是現今世界中員工所渴望的工作方式 – 存取資訊更便捷、合作與分享順暢無礙，而且在任何地方都能隨心所欲地保持聯繫與完成工作。

在當今的企業環境中設定及部署 Mac 電腦，可說前所未有地容易。使用 Apple 的關鍵服務，搭配第三方行動裝置管理 (MDM) 解決方案，你的企業組織就能輕鬆大規模部署及支援 Mac。如果組織已於內部部署各項 iOS 和 iPadOS 裝置，則實作 macOS 所需的多數基礎設施可能早已建置完成。

近期 Mac 在安全、管理和部署等方面的功能提升，有助組織跳脫單體映像檔建立與傳統目錄綁定的做法，轉變為流暢無縫的佈建模式與部署流程，不僅改以每位使用者為中心，而且幾乎可以完全仰仗 macOS 內建的工具。

這份文件提供詳細指引，為你說明大規模部署 Mac 所需的知識與技巧，從了解現有基礎設施，到裝置管理與精簡的佈建程序，一應俱全。對於本文件介紹的主題如需更詳盡的說明，請參閱線上

「Deployment Reference for Mac」(Mac 部署參考)：  
[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

# 開始使用

部署流程的首要步驟，是制訂部署策略與配發計畫，以及評估員工目前的任何 macOS 使用情況。請確保必要的團隊能及早參與，並對於你的專案擁有一致的願景與目標。有些團隊會先從小規模的概念驗證著手，藉此了解所在環境面臨的獨特挑戰。與現有使用者互動交流，是較大規模的試行計畫中相當關鍵的一環，你可以從中了解裝置在整個組織內部的使用情況，並得知團隊是否需要留意任何問題。

在這個階段收集的資訊，有助於判斷哪些員工角色與職務內容可以藉由 Mac 發揮最大成效。IT 可據此評估 macOS 的適用範圍，決定讓全組織一體適用，或僅供特定職務來選用。

往往也是在這個流程階段，可完整檢視在全面配發 Mac 之前，有哪些內部 app 與工具需要與它相容。大多數使用者常用的核心生產力、合作和通訊 app，會是主要的考量項目。企業內部網路、目錄，以及開支管理軟體等關鍵性的內部服務，對大幅提升組織生產力而言，也至關重要。

請針對其他的內部工具，紀錄並傳達各種解決方法或替代方案，同時鼓勵各應用程式的擁有者，根據需求來進行現代化。使用者若選用 Mac，請以公開透明的方式，告知他們所能使用的各種商務 app，並依使用者需求，排定任何現代化作業的優先順序。如有需要，請與應用程式擁有者合作，針對如何更新 app、如何運用 macOS SDK 與 Swift，以及如何連結能協助開發的各界企業夥伴，來制訂計畫。

一般配發給員工的 Mac 電腦，裝置會由公司持有，有些企業則可能採行自攜裝置 (BYOD) 方案，讓員工使用自己的 Mac 來工作。無論持有權模式為何，員工自選 Apple 產品為工作配備，都能讓整個組織充分獲益：員工生產力、創造力、參與度，以及工作滿意度皆可提升。將剩餘價值和支援列入之後，成本也更為降低。組織也可善用各種租賃與分期付款選項，來降低前期成本。還可以讓員工在升級時，以薪資扣抵的個人支付方式，或在租期或裝置生命週期結束時向雇主買斷裝置，來抵銷成本支出。

本文件所述的企業政策，以及部署、管理與支援流程，可能視團隊於試行階段所得的部分資訊不同，而有所差異。同一公司不同群組或團隊之間的要求，往往差異極大，因此每位使用者對政策、設定與 app 的需求也不盡相同。

# 部署步驟

部署 macOS 有四大主要步驟：準備環境、設定 MDM、部署裝置給員工，然後完成持續性的管理工作。

## 1. 準備

任何部署作業的第一步，都是先考量現有的企業環境。這個階段，除了更深入了解你的企業網路與主要基礎設施，還需要為系統進行設定，以利成功部署。

### 評估基礎設施

儘管 Mac 能和大多數標準的企業 IT 環境流暢整合，你還是必須評估現有的基礎設施，以確保你的組織能充分善用 macOS 提供的各項功能。如果組織在這方面需要協助，可以洽詢 Apple 專業服務，或是通路合作夥伴或經銷商的技術團隊。

### Wi-Fi 與網路連線

穩定且可靠的無線網路連線，是設定與配置 macOS 裝置的關鍵。請確認公司的 Wi-Fi 網路經過適當設計，包括存取點的擺放位置與功率都已審慎考量，以確保能符合漫遊與流量的需求。

如果裝置無法存取 Apple 伺服器、「Apple 推播通知服務」(APNs)、iCloud 或 iTunes Store，你也可能需要調整各網頁代理伺服器或防火牆傳輸埠的配置。如同 iPad 與 iPhone，Mac 部署流程中的部分環節 (特別是使用較新的 Mac 硬體時) 會需要存取這些服務以執行作業，例如在安裝期間更新韌體。

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。

公司也須評估 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，只有在需要時，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。

請確認你的網路基礎設施已正確設定，可與 Bonjour 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 功能也會使用 Bonjour 來尋找其他裝置，以進行合作與共享。

進一步了解 Wi-Fi 網路設計：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

進一步了解如何配置網路以供 MDM 使用：

[support.apple.com/zh-tw/HT210060](https://support.apple.com/zh-tw/HT210060)

進一步了解 Bonjour：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

### 管理身分識別

macOS 可存取目錄服務，以管理身分識別與其他的使用者資料，包括 Active Directory、Open Directory 與 LDAP。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。來自內部與外部憑證管理中心 (CA) 各種類型的憑證，也可以由 MDM 解決方案進行管理，讓身分識別自動受到信任。

進一步了解全新的 Kerberos 單一登入延伸功能：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

進一步了解目錄整合：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

### 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。

進一步了解如何配置 Microsoft Exchange：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

進一步了解標準服務：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

### 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 macOS、iOS 或 iPadOS 皆適用。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/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

## 建立管理解決方案

MDM 能讓組織安全地將 Mac 註冊到商務環境中、以無線方式配置與更新設定、部署 app、監控政策的合規情況、查詢裝置，以及遠端清除或鎖定受控裝置。IT 人員可輕鬆製作描述檔，來管理使用者帳號、配置系統設定、強制執行限制，並設定密碼政策，所有一切，沿用 iPhone 與 iPad 的同一套行動裝置管理解決方案即可執行。

所有 Apple 平台皆在背景中使用 Apple 的通用管理框架，這組框架讓顧客能搭配使用多種第三方 MDM 解決方案。還有 Jamf、VMware 與 MobileIron 等第三方廠商所提供的多樣化裝置管理解決方案。儘管 macOS 的眾多裝置管理框架均與 iOS 和 iPadOS 相同，第三方 MDM 解決方案在管理功能、作業系統支援、價格結構和代管模式上仍有些許差異。它們也可能針對整合、培訓和支援提供不同層級的服務。在選擇解決方案之前，請先評估哪些功能最貼近組織的需求。

一旦選定了要使用的 MDM，你需要前往 Apple Push Certificates Portal，並登入以新增 MDM 推播憑證。

進一步了解如何部署 MDM：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

前往 Apple Push Certificates Portal：

[identity.apple.com/pushcert/](https://identity.apple.com/pushcert/)

## 註冊加入 Apple 商務管理

「Apple 商務管理」是一個網頁式入口網站，可供 IT 管理者集中一處完成 iPhone、iPad、iPod touch、Apple TV 和 Mac 的部署作業。它能與你的行動裝置管理 (MDM) 解決方案流暢搭配運作，以自動進行裝置部署、購買 app 並發布內容，以及為員工建立「管理式 Apple ID」。

「裝置註冊計劃」(DEP) 和「大量採購計劃」(VPP) 現已完全整合至「Apple 商務管理」，組織可在此取得部署 Apple 裝置時所需的一切。從 2019 年 12 月 1 日起，這些計劃將停止提供。

## 裝置

「Apple 商務管理」能進行「自動化裝置註冊」，透過快速精簡的方式，讓組織部署企業持有的 Apple 裝置並註冊到 MDM，無須實際接觸或準備每部裝置。

- 精簡「設定輔助程式」中的步驟，為使用者簡化設定流程，確保員工一啟用裝置，一切皆已配置就緒。IT 團隊現在可為員工提供同意書文字、企業品牌訊息或新式認證，進一步自訂整個體驗。
- 利用監管功能，對企業持有的裝置進行更高階的控管，這項功能提供了其他部署模式沒有的額外裝置管理控制項目，包括不可移除的 MDM。
- 根據裝置類型來設定預設伺服器，讓預設 MDM 伺服器的管理更為簡易。且現在無論 iPhone、iPad 與 Apple TV 購自何處，均可使用 Apple Configurator 2 進行手動註冊。

## 內容

「Apple 商務管理」可讓組織輕鬆地大量購買內容。無論工作團隊使用的是 iPhone、iPad 或 Mac，你都能透過靈活安全的選項，發布可立即用於工作的精彩內容。

- 大量購買 app、書籍和自訂 app，包括你在內部開發的 app。在不同位置之間輕鬆轉移 app 授權，並與同一位置的購買者共用授權。還可檢視經統整的購買記錄列表，包括 MDM 中目前所使用的授權數量。
- 將 app 直接發布給受控裝置或授權使用者，並輕鬆追蹤哪些內容已指派給哪一位使用者或哪部裝置。使用受控的發布方式，控管整個發布流程，同時保有 app 的完整持有權。裝置或使用者不再需要的 app 可以撤銷，再於組織內部重新指派。
- 提供多種付款選項，包括信用卡與訂單。組織可以直接透過 Apple 或 Apple 授權經銷商，以當地貨幣購買特定金額的「大量採購點數」（如適用），這些點數會以電子方式傳送給帳號持有者，讓他們做為商店點數使用。
- App 可以發布至適用國家或地區中的任何裝置或使用者，讓組織得以進行跨國發布。開發者可透過標準的 App Store 發布流程，讓 app 在多個國家或地區上架。

附註：某些國家或地區未在「Apple 商務管理」中提供購買書籍的功能。若要了解各國家或地區提供的功能與購買方式，請參閱 [support.apple.com/zh-tw/HT207305](https://support.apple.com/zh-tw/HT207305)。

## 成員

「Apple 商務管理」可供組織為員工建立並管理帳號，這些帳號能與現有基礎設施整合，並可供存取 Apple 的 app 與服務，以及「Apple 商務管理」。

- 為員工建立「管理式 Apple ID」，讓他們透過 Apple app 與服務進行合作，並在使用「iCloud 雲碟」的受控 app 中存取公司資料。這些帳號都由各組織所持有並控管。
- 將「Apple 商務管理」連結到 Microsoft Azure Active Directory 來使用聯合認證。每位員工首次在相容的 Apple 裝置上使用現有憑證登入時，「管理式 Apple ID」就會自動建立。
- 藉由 iOS 13、iPadOS 和 macOS Catalina 新加入的「使用者註冊」功能，在員工持有的裝置上同時使用「管理式 Apple ID」與個人 Apple ID。此外，「管理式 Apple ID」可以在任何裝置上，做為主要且唯一的 Apple ID 使用。它在首次登入 Apple 裝置後，也可以透過網頁存取 iCloud。
- 在「Apple 商務管理」中為組織內的 IT 團隊指定其他職務，以便有效管理裝置、app 與帳號。如有需要，可使用「管理者」職務來接受條款與約定，若員工離職，也可以輕鬆移交職務。

附註：「使用者註冊」目前不支援使用「iCloud 雲碟」。「管理式 Apple ID」為裝置唯一的 Apple ID 時，方可搭配「iCloud 雲碟」使用。

進一步了解「Apple 商務管理」：[apple.com/tw/business/it](https://apple.com/tw/business/it)

## 註冊加入 Apple Developer Enterprise Program

Apple Developer Enterprise Program 提供一組完整的工具，協助使用者進行 app 的開發、測試與發布作業。你可透過網頁伺服器代管的方式，或採用 MDM 解決方案，來發布 app。你的開發者識別碼可以對 Mac app 與安裝程式進行簽署並公證，以供「門禁」（可為 macOS 阻擋惡意軟體的功能）判別。

進一步了解 Developer Enterprise Program：

[developer.apple.com/programs/enterprise](https://developer.apple.com/programs/enterprise)

## 2. 設定

部署作業的設定中，包括定義企業政策，並備好行動裝置管理解決方案，以配置 Mac 供員工使用。

### 了解 macOS 安全性

安全性與隱私權，是 Apple 所有軟、硬體與服務設計的基本要素。我們透過強式加密與嚴格政策，來控管所有資料的處理方式，從而保護顧客的隱私。為 Apple 裝置提供安全的運算平台，會需要：

- 能防止未經授權使用裝置的各種對策
- 保護裝置上已儲存的資料，即使裝置遺失或遭竊也能有效進行保護
- 網路通訊協定，以及為傳輸中的資料加密
- 讓 app 得以安全執行，且無損平台的完整性

所有 Apple 裝置皆具備多重安全防護，可以安全無虞地存取網路服務，並保護重要資料。macOS、iOS 與 iPadOS 也可以透過 MDM 來發送並強制執行密碼與密碼政策，從而提供安全防護。若裝置不慎落入他人之手，使用者或管理者可使用遠端指令，清除所有私人資訊。

IT 可使用 MDM 來部署一組政策，確保裝置安全無虞。例如可使用 MDM 強制執行「檔案保險箱」與復原密鑰託管、強制採用特定密碼政策或螢幕保護程式鎖定，以及啟動內建防火牆。

進一步了解 Apple 平台安全性：[support.apple.com/zh-tw/guide/security/welcome/web](https://support.apple.com/zh-tw/guide/security/welcome/web)

### 定義企業政策

發展企業政策的第一步，是建立能適用於公司內大多數 Mac 使用者的一般性政策。MDM 解決方案可供你定義使用者專用的自訂項目，例如帳號或對特定 app 的存取權限。你也可以為組織或其他較小的使用者群體，設定其專用政策，例如部署部門專用的軟體或設定。

請與內部團隊合作來更新現有的企業政策，將 Mac 電腦的使用納入其中。有些核心政策會在各平台上沿用，例如密碼複雜度與定期更換密碼要求、螢幕保護程式逾時，以及可接受的用途。

如果企業政策規定使用另一個平台所用的特定技術，請試著了解根本的問題所在，並設法重新制訂政策以納入 macOS 的內建技術。請考慮透過制訂政策，要求在儲存企業資料時進行加密，並透過「檔案保險箱」來達成，而非要求所有電腦使用特定的第三方解決方案來加密整個磁碟。如果政策規定使用特定軟體來防範惡意軟體，請為團隊介紹「門禁」等內建功能，並更新政策內容來允許使用這些功能。

### 在 MDM 中配置設定

為了進行企業政策管理，並確保員工可存取必要資源，每部 Mac 皆會以安全方式註冊到你的 MDM 解決方案中。接著，MDM 解決方案會使用設定描述檔，來套用政策與設定。設定描述檔是 MDM 解決方案所製作的 XML 檔案，可將設定發布到裝置。這些描述檔可以自動進行設定、帳號、政策、限制與憑證的配置。它們也可以被簽署及加密，協助提升系統的安全性。



裝置註冊到 MDM 之後，管理者即可對裝置執行 MDM 政策、查詢或指令。有網路連線時，裝置就會收到「Apple 推播通知服務」(APNs) 傳送的通知，指示它透過安全的連線，直接與所屬的 MDM 解決方案通訊，以執行管理者的動作。由於通訊僅在 MDM 解決方案與裝置之間進行，因此 APNs 不會傳送機密或專屬資訊。如果從管理項目中移除某部裝置，該設定描述檔所控管的設定與政策也會被移除。如有必要，公司也可以遠端清除裝置。

許多組織會將 MDM 解決方案，加入到現有的目錄服務中。macOS 中的「設定輔助程式」可以在「自動化裝置註冊」期間，提示使用者以他們的目錄服務憑證登入。macOS Catalina 提供全新註冊自訂選項，可讓「設定輔助程式」顯示雲端身分識別提供者的認證。裝置一旦指派給特定的使用者，MDM 即可為個人或團體自訂配置與帳號。舉例來說，MDM 可以在註冊期間，自動佈建個別使用者的 Microsoft Exchange 帳號。你也可以搭配 802.1x、VPN 等技術來使用憑證身分識別。

藉由這些系統提供的控管功能，公司通常能安心賦予使用者對 Mac 的管理者存取權限，使用者將能充分進行個人化設定、app 安裝，以及疑難排解，同時仍透過 MDM 接受企業政策的控管。此模式所採用的權限與控制類型，和使用者的 iPhone 或 iPad 受管理時所擁有的權限與控制類型相同。

進一步了解設定描述檔：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

### 為「自動化裝置註冊」做好準備

將裝置註冊到 MDM 最簡單的方式，就是在執行「設定輔助程式」期間使用「Apple 商務管理」的「自動化裝置註冊」功能。如此一來，不須透過 IT 人員即可完成註冊，還可大幅精簡「設定輔助程式」的某些畫面，讓使用者的註冊流程更為迅捷。

若要配置「自動化裝置註冊」，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。系統會使用雙步驟驗證流程，以安全方式授權 MDM 解決方案。你的 MDM 供應商可就特定實行需求，提供詳細說明文件。

如果員工已在使用裝置，或裝置是由個人持有，使用者可以開啟單一設定描述檔並在「系統偏好設定」中驗證，藉此完成註冊。這稱為「使用者核准的 MDM 註冊」。必須透過裝置註冊計劃或「使用者核准的 MDM 註冊」進行註冊，才能管理涉及安全性的某些設定，如「核心延伸功能政策」和「隱私權偏好設定規則控制」。

進一步了解核心延伸功能載入：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

進一步了解「隱私權偏好設定規則控制」：

[support.apple.com/zh-tw/guide/mdm/welcome/web](https://support.apple.com/zh-tw/guide/mdm/welcome/web)

### 準備好發布 App

Apple 提供豐富的方案，協助你的組織善用 macOS 提供的絕佳 app 與內容。有了這些功能，不論是透過「Apple 商務管理」購買的 app，或公司自行開發的應用程式，都能發布給員工，讓他們擁有一切所需，大幅提升生產力。MDM 也可以發布 app，並安裝無法從 Mac App Store 取得的軟體套件。

MDM 解決方案可使用受控的發布方式，在 app 的適用國家或地區內發布購自「Apple 商務管理」的 app。若要啟用受控的發布方式，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 解決方案之後，即可指派 app 給使用者，不論裝置上的 App Store 是否為停用狀態。你也可以直接將 app 指派給裝置，令該裝置的任何使用者都能存取這些 app，大幅提高部署的簡易度。

進一步了解在「Apple 商務管理」中購買內容：

[support.apple.com/zh-tw/guide/apple-business-manager/welcome/web](https://support.apple.com/zh-tw/guide/apple-business-manager/welcome/web)

進一步了解發布 app：

[support.apple.com/zh-tw/guide/apple-business-manager/welcome/web](https://support.apple.com/zh-tw/guide/apple-business-manager/welcome/web)

### 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。

進一步了解如何安裝額外的內容：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

## 3. 部署

macOS 可供你輕鬆為員工部署裝置、視需要加以個人化，以及自行完成設定並開始啟用，完全無需 IT 經手。

### 運用設定輔助程式

員工一開始就能使用 macOS 的「設定輔助程式」，來進行語言與地區偏好設定，以及連上網路。連線到 Internet 時，系統會展示一系列的「設定輔助程式」視窗，引導使用者逐步完成全新 Mac 設定的基本步驟。已註冊到「Apple 商務管理」的裝置，可以在此流程進行期間自動註冊到 MDM。已註冊的 Mac 系統也可以進行配置，以略過特定螢幕畫面，例如條款與約定、Apple ID 登入、定位服務等等。

「設定輔助程式」執行完畢後，即可透過 MDM 完成初始配置以部署各式設定，包括定義使用者是否對其電腦具有完全的管理權限。如同 iPhone 與 iPad 的做法，這個步驟能讓使用者控制自己的裝置，同時仍遵守受 MDM 控管的企業政策與設定。若要讓使用者在「設定輔助程式」執行完畢後，能立即發揮生產力，建議你只鎖定最重要的應用程式與套件，於背景進行下載和安裝，以避免妨礙員工開始工作。大型應用程式的下載與安裝，可排在背景中進行，或稍後由使用者在 MDM 解決方案的自助工具中完成。

### 配置企業帳號

MDM 可自動設定郵件與其他使用者帳號。視你所用的 MDM 解決方案，還有方案本身和內部系統的整合狀況，系統也可為帳號預先填寫使用者名稱、電子郵件地址，以及可供認證和簽署用的憑證身分識別等承載資料。

## 允許使用者個人化

使用者個人化自己的裝置，可以提高生產力，因為使用者可選擇最有助於完成工作與達成目標的 app 及內容。現在，藉由「管理式 Apple ID」和 macOS Catalina 中的「使用者註冊」功能，組織可以為使用者提供新的選擇，讓他們透過組織持有的 Apple ID，或搭配個人 Apple ID 來存取 Apple 服務。

### Apple ID 與管理式 Apple ID

員工使用 Apple ID 來登入 FaceTime、iMessage、App Store 和 iCloud 等 Apple 服務後，即可存取各式各樣的內容，以大幅精簡商務工作、提升生產力與支援合作。如同任何 Apple ID，「管理式 Apple ID」可用來登入個人裝置，也可用來存取 Apple 服務 (包括 iCloud 與 iWork 和「備忘錄」的合作功能)，以及「Apple 商務管理」。與 Apple ID 不同的是，「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。

透過「使用者註冊」進行註冊的裝置，必須具備「管理式 Apple ID」。「使用者註冊」支援選用個人 Apple ID；其他註冊選項則可支援個人 Apple ID 或「管理式 Apple ID」。只有「使用者註冊」才能支援多個 Apple ID。

若要讓這些服務發揮最大效益，使用者應使用自己的 Apple ID，或專為他們建立的「管理式 Apple ID」。沒有 Apple ID 的使用者，在尚未收到裝置前即可先行建立。「設定輔助程式」也能讓沒有個人 Apple ID 的使用者建立 Apple ID。建立 Apple ID 無須使用信用卡。

進一步了解「管理式 Apple ID」：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

### iCloud

iCloud 能讓使用者自動同步文件與個人內容，例如聯絡人、行事曆、文件與照片，同時還能讓這些內容在多部裝置上保持最新狀態。使用者可利用「尋找」，找出遺失或遭竊的 Mac、iPhone、iPad 或 iPod touch。「iCloud 鑰匙圈」與「iCloud 雲碟」等 iCloud 特定功能，可透過取用限制予以停用，這些限制可在裝置上手動方式輸入，或透過 MDM 來設定。如此一來，組織即可進一步控制帳號所存放的資料。

進一步了解如何管理 iCloud：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

## 4. 管理

使用者順利上手使用裝置後，可透過各式各樣的管理功能，為裝置與內容進行長期管理與維護。

### 管理裝置

MDM 解決方案可透過一組特定作業，來管理受控裝置。這類作業包括向裝置查詢資訊，以及開始啟動作業來管理未遵循政策、遺失或遭竊的裝置。

### 查詢

MDM 解決方案可以向裝置查詢各種資訊，協助確保使用者保有一組適當的應用程式與設定。這類查詢可以和硬體有關，例如序號或裝置機型，也可以和軟體有關，例如 macOS 版本或安裝的應用程式列表。此外，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。

### 管理作業

裝置受到控管時，MDM 解決方案可執行各式管理作業，包括無須使用者操作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。

進一步了解管理作業：

[support.apple.com/guide/deployment-reference-macos](https://support.apple.com/guide/deployment-reference-macos)

### 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，盡速升級。

MDM 可以自動將 macOS 更新項目推播給已註冊的 Mac 裝置。若重要系統尚未準備就緒，也可以為已註冊的 Mac 裝置進行配置，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。

### 管理額外的軟體

除了最初的一組 app 之外，組織通常還需要為使用者發布其他的 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，或是安裝非 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。

### 維持裝置安全性

除了裝置部署之前所制訂的一組初始安全性政策，也建議你的團隊監控機器的政策合規情況，並透過 MDM 解決方案盡可能取得詳細報告。這可能包括監控各裝置的安全狀態，或是收集軟體修補程式的安裝資訊。雖然大多數的組織都習慣使用原生工具來加密及保護每部 Mac，但仍有部分組織可能要求使用其他檔案同步與共享服務或資料遺失預防工具，以防範企業資料外洩並提供任何敏感資料的深入報告。

若 Mac 遺失或遭竊，可啟用 iCloud 的「尋找我的 Mac」功能，來執行遠端清除指令，移除所有資料並停用裝置。IT 團隊也可利用 MDM 來執行遠端清除。

### 重新佈建裝置

遇到員工離職的情況時，組織可以透過「Internet 復原」和本機上的「復原分割區」，輕鬆地將 Mac 重新佈建以供其他員工使用。此功能可清除每部 Mac 的內容，並安裝最新版本作業系統。在「Apple 商務管理」中指派給特定 MDM 的 Mac，會在「設定輔助程式」執行期間使用 MDM 自動重新註冊、為新使用者配置設定、套用企業政策，並部署所有適當的軟體。未註冊的 Mac 電腦可以使用相同流程進行清除並重新佈建，然後以手動方式重新註冊。

## 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，開發穩固的 Mac 支援網頁、開設自助論壇，以及提供現場技術支援櫃台。MDM 解決方案也讓使用者能執行支援作業，例如可從自助式入口網站安裝或更新軟體。

就最佳做法而言，公司不應強制使用者完全以自助方式取得支援。我們建議以合作的方式來解決問題，聚焦於賦予使用者能力，讓他們在聯絡服務台之前，先自行進行疑難排解。鼓勵使用者參與流程，讓他們在求助之前，先行找出問題所在。

共同分擔支援服務的責任，有助於減少員工停機時間，就支援成本和人員而言，也能減少總體足跡。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。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，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，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

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 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/](https://apple.com/tw/support/professional/)

# 總結

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-reference-macos/welcome/web](https://support.apple.com/zh-tw/guide/deployment-reference-macos/welcome/web)

了解 IT 適用的行動裝置管理設定：

[support.apple.com/guide/mdm](https://support.apple.com/guide/mdm)

了解「Apple 商務管理」：

[support.apple.com/zh-tw/guide/apple-business-manager](https://support.apple.com/zh-tw/guide/apple-business-manager)

了解「企業適用的管理式 Apple ID」：

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

[Overview\\_of\\_Managed\\_Apple\\_IDs\\_for\\_Business.pdf](#)

了解 Apple at Work：

[www.apple.com/tw/business/](https://www.apple.com/tw/business/)

了解 IT 功能：

[www.apple.com/tw/business/it/](https://www.apple.com/tw/business/it/)

了解 Apple 平台安全性：

[www.apple.com/security/](https://www.apple.com/security/)

瀏覽適用的 AppleCare 方案：

[www.apple.com/tw/support/professional/](https://www.apple.com/tw/support/professional/)

探索 Apple Training and Certification：

[training.apple.com](https://training.apple.com)

洽詢 Apple 專業服務：

[consultingservices@apple.com](mailto:consultingservices@apple.com)

© 2019 Apple Inc. 保留一切權利。Apple、Apple 標誌、AirPlay、AirPrint、Apple TV、Bonjour、FaceTime、「檔案保險箱」、iMessage、iPad、iPhone、iPod touch、iTunes、Mac 與 macOS 是 Apple Inc. 在美國及其他國家或地區註冊的商標。Swift 是 Apple Inc. 的商標。App Store、AppleCare、Apple Books、iCloud、「iCloud 雲碟」、「iCloud 鑰匙圈」與 iTunes Store 是 Apple Inc. 在美國及其他國家或地區註冊的服務標章。IOS 是 Cisco 在美國及其他國家或地區的商標或註冊商標，依授權規定使用。此處提及的其他產品和公司名稱可能為其所屬公司的商標。產品規格可能依情況有所變動，恕不另行通知。本素材僅供參考資訊用途；Apple 對其使用不承擔任何責任。