概覽

在 iOS 上管理裝置與企業資料

概覽

目錄

全球各地企業正使用 iPhone 與 iPad，來強化員工能力。

行動策略的成功關鍵，就在如何落實 IT 控制，又能保留使用者發揮的空間。允許使用者加入自屬的 app 與內容，讓 iOS 裝置更為個人化，使用者對裝置會有更強的擁有權和責任感，進而更常使用裝置，帶動生產力的提升。Apple 的管理框架可達成此一目標，它以智慧的方式，來個別管理企業資料和 app，流暢區隔工作資料與個人資料。此外，使用者也能清楚了解裝置如何受到管理，並安心信任個人的隱私權受到良好保護。

本文件將提供指引，說明企業能如何掌握關鍵 IT 控制，又能讓使用者藉由最佳工具，在工作上大放異彩。它可和《iOS 部署參考》交互參照，這份 Apple 線上技術文件提供了詳盡說明，可供了解如何在企業中部署與管理 iOS 裝置。

如需參閱《iOS 部署參考》，請前往 help.apple.com/deployment/ios。

基本管理概念

iOS 中的各項內建技術，可供簡化帳號設定、配置政策、發布 app 和遠端套用裝置限制，大幅精簡 iPhone 與 iPad 部署。

Apple 的簡易框架

Apple 在 iOS、macOS 與 tvOS 中採用的統一管理框架，可供 IT 配置及更新設定、部署應用程式、監控合規狀況、查詢裝置，還能遠端清除或鎖定裝置。這套框架可同時支援企業持有、使用者持有兩種裝置使用類型，也能支援個人持有的裝置。Apple 的 iOS 統一管理框架，是行動裝置管理作業的基礎。此框架內建於 iOS，讓企業組織透過低度的干涉，就能進行必要的控管，而非一逕鎖用或停用功能。因此在 Apple 的 iOS 統一管理框架中，借助協力廠商的行動裝置管理 (MDM) 解決方案，就能對公司內部的裝置、app 與資料進行精細的控制。最重要的是，你能進行一切所需的控制，卻不影響使用者體驗或員工隱私權。

市面上各種裝置管理方法，有時會為 MDM 功能冠上不同名稱，如企業行動管理 (EMM)，或行動應用管理 (MAM)。然而這些解決方案都有著一致目標，也就是透過無線傳輸方式，來管理公司的裝置和企業資料。由於 Apple 管理框架已在 iOS 中充分內建，無須再使用 MDM 解決方案供應商所提供的代理程式。

區隔工作與個人資料

無論公司支援的裝置為使用者持有或公司持有，你都能順利達成 IT 管理目標，同時讓員工徹底發揮生產力。工作資料與個人資料可以分開管理，使用者也能保有一致的體驗。如此一來，企業 app 與最熱門的生產力 app，都能在使用者的裝置上並行不悖，員工在工作上則享有更多自由。iOS 可畢其功於一役，無須再借助協力廠商解決方案，像是容器等方法，往往會為使用者的體驗及心情帶來負面影響。

了解各種管理模式

其他平台出現的問題，往往會採用容器來解決，iOS 卻不會遇到這些問題。有些容器會採取雙重角色的策略，在同一裝置上分別建立兩個獨立的執行環境。其他容器類型，則主要透過程式碼整合或 app 封裝解決方案，將應用程式本身容器化。這些方法都有礙使用者發揮生產力，因為他們必須反覆登入登出多個工作空間，或增加對專屬程式碼的依賴，後者更經常導致 app 不相容於作業系統更新項目。

有些企業在停用容器之後，發現 iOS 的原生管理控制項目能為使用者提供最佳體驗，並提升其生產力。你可以藉由政策控管的方式，在背景中流暢管理資料流，讓使用者不論將裝置用於公務或私事，都能行雲流水，使用無礙。

管理企業資料

有了 iOS，你無須鎖定裝置。iOS 中的各項關鍵技術，可控制 app 之間的企業資料流，防止企業資料外流至使用者的個人 app 或雲端服務。

受控內容

受控內容涵蓋 App Store 與自訂內部 app、帳號、書籍和網域的安裝、配置、管理及移除。

- **受控 app。**使用 MDM 安裝的 app 稱為受控 app。它們可能是 App Store 上的免額外付費或付費 app，或是自訂的內部 app，而且都能使用 MDM 以無線傳輸方式安裝。受控 app 通常包含機敏資訊，也能提供比使用者下載的 app 更多的控制。MDM 伺服器可隨需移除受控 app 及其相關資料，或指定是否要在移除 MDM 描述檔時，一併移除 app。此外，MDM 伺服器還可防止受控 app 的資料被備份至 iTunes 與 iCloud。
- **受控帳號。**MDM 可自動為你的使用者設定郵件和其他帳號，協助他們快速上手。視 MDM 解決方案供應商，還有方案本身和內部系統的整合狀況，系統可為帳號預先填寫使用者名稱、郵件位址，以及供認證和簽署用的憑證識別身分等承載資料。MDM 可以配置下列類型的帳號：IMAP/POP、CalDAV、訂閱的行事曆、CardDAV、Exchange ActiveSync 和 LDAP。
- **受控書籍。**使用 MDM 時，書籍、ePub 書籍和 PDF 文件皆可自動推播至使用者裝置，讓員工隨手取得一切所需。受控書籍只能與其他受控 app 共享，或透過受控帳號郵寄分享。不再需要書籍時，可以從遠端將其移除。
- **受控網域。**來自 Safari 的下載項目若源自受控網域，就會被視為受控文件。特定 URL 與子網域都可以納入管理。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。

受控的發布方式

採用受控的發布方式時，你可利用 MDM 解決方案或 Apple Configurator 2，為透過「Apple 商務管理」購買的 app 和書籍進行控管。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。無論裝置使用者是否已擁有 Apple ID，只要 MDM 伺服器連結到「Apple 商務管理」，就能直接將 app 指派到裝置上。App 在裝置上可供安裝時，使用者會收到提示。如果裝置受到監管，app 會以背景運作方式推播到該裝置，使用者不會收到任何提示。

若要使用 MDM 解決方案，來完整保有 app 的控制權，請將 app 直接指派到裝置。

受控 app 配置

藉著受控 app 配置，MDM 可使用原生 iOS 管理框架，在部署過程中或完成部署之後配置 app。當開發人員的 app 是以受控 app 的形式安裝時，此一框架可協助他們識別應導入哪些配置設定。以這種方式配置的 app，使用者不必自行設定，就能開始使用。IT 也能確保 app 內的企業資料安全無虞，無須借助專屬 SDK 或 app 封裝技術。

App 開發人員可以透過受控 app 配置來啟用多種功能，例如 app 配置、防止 app 備份、停用螢幕畫面擷取，以及遠端清除 app 等。

AppConfig Community 社群致力於為行動作業系統內的原生功能提供工具與最佳實務。社群中的頂尖 MDM 解決方案供應商，已合作建立一套標準架構，讓所有 app 開發者用於支援受控 app 配置。這個社群採用更一致、開放且簡單的做法，來配置行動 app 並維護其安全性，藉此提高企業的行動化比例。

進一步了解 AppConfig Community，請參閱 www.appconfig.org。

受控的資料流

MDM 解決方案提供多項特定功能，讓企業資料受到精細的控管，不致外洩至員工的個人 app 和雲端服務。

為了保護企業資料，唯有由 MDM 安裝並控管的 app 可以打開此工作文件。

- **受控的打開方式。**「打開方式」管理功能可利用一組取用限制，防止受控來源的附件或文件在未受控目的地中開啟，反之亦然。

  舉例來說，如果公司有受控的郵件帳號，你可防止該帳號中的機密電子郵件附件，在任何使用者的個人 app 中開啟。只有由 MDM 所安裝並控管的 app，可以打開這份工作文件。使用者未受控的個人 app 不會出現在可打開附件的 app 列表中。除了受控 app、帳號、書籍和網域之外，受控的打開方式中的限制也適用於多項延伸功能。

- **受控延伸功能。**App 延伸功能，可讓協力廠商開發者為其他 app 開拓功能，甚至包括 iOS 內建的主要系統 (如「通知中心」)，進而在 app 之間創造全新的商務工作流程。受控的打開方式，可防止未受控的延伸功能與受控 app 產生互動。以下範例，說明了各種延伸功能的類型：
  - **「文件提供者」延伸功能**：讓生產力 app 從各式雲端服務開啟文件，免除不必要的拷貝。
  - **「動作」延伸功能**：讓使用者在其他 app 所屬環境中操控或檢視內容。例如使用者可利用動作，直接在 Safari 中翻譯其他語言文字。
  - **「自訂鍵盤」延伸功能**：提供 iOS 內建鍵盤之外的其他鍵盤。受控的打開方式可防止未經授權的鍵盤在企業 app 中顯示。
  - **「今天」延伸功能**：也稱為「小工具」，用來提供可在「通知中心」的「今天顯示方式」中瀏覽的資訊。這是使用者即時取得最新資訊的絕佳方式，他們還能透過更簡約的互動，打開完整的 app 以取得更多資訊。
  - **「分享」延伸功能**：方便使用者將內容分享給其他實體對象，像是社群分享網站或上傳服務。例如，在內含「分享」按鈕的 app 中，使用者可以選擇代表社群分享網站的「分享」延伸功能，來張貼留言或其他內容。

靈活彈性的管理選項

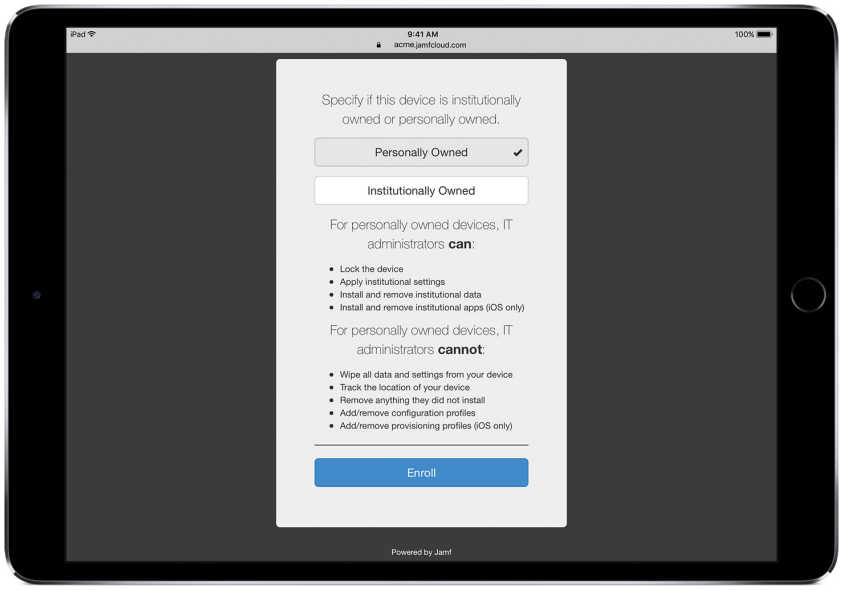
Apple 的 iOS 統一管理框架靈活且富彈性，讓你在企業中管理使用者持有及公司持有的裝置時，同時兼顧兩者的需求。搭配使用協力廠商 MDM 解決方案與 iOS，你將能透過一系列選項，隨需進行裝置管理，從高度開放到力求精細，皆能執行。

持有權模式

你可根據公司內部的單一或多種裝置持有權模式，以不同方式來管理裝置和 app。企業最常採用的兩種 iOS 裝置持有權模式，是使用者持有和企業持有。

使用者持有的裝置

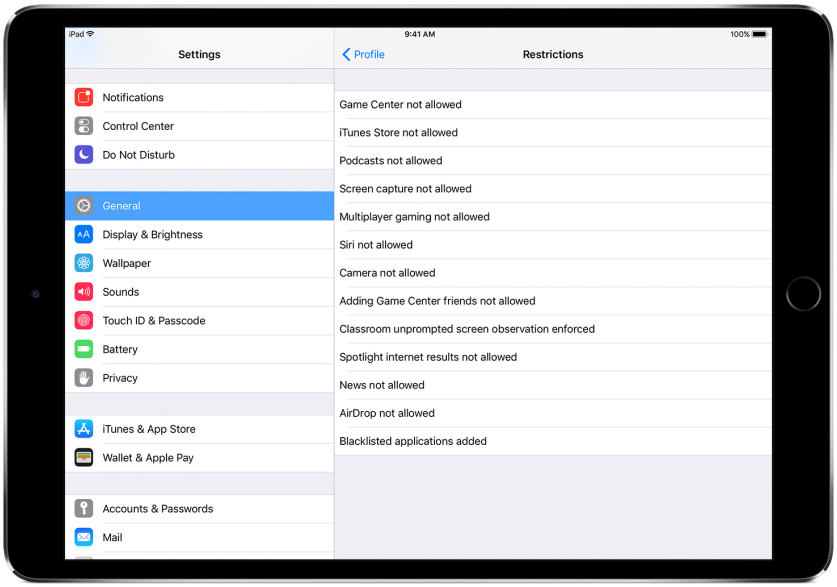
在使用者持有的部署模式中，iOS 可讓使用者進行個人化設定，也能透明檢視該裝置所受的配置，還能確保使用者的個人資料不受公司存取。



一般而言，協力廠商 MDM 解決方案都有簡單易用的介面，讓員工在註冊裝置時能安心選擇加入。*

*螢幕影像由 Jamf 提供。

- **選擇加入和選擇退出註冊。**如果裝置是由使用者自行購買並設定，也就是一般稱為 BYOD 的方式，你還是可以為他們提供 Wi-Fi、郵件和行事曆等企業服務的存取功能，使用者只要選擇註冊至你公司的 MDM 解決方案即可。當使用者第一次在 iOS 裝置上註冊至 MDM，他們會獲得相關資訊，例如 MDM 能從其裝置上存取的項目，以及即將配置的各項功能。如此一來，使用者便能清楚知道那些項目受到控管，你也能建立和使用者之間的信任。請務必讓使用者了解，如果他們對這樣的管理方式感覺有任何不妥之處，可以隨時從裝置上移除管理描述檔，自行選擇退出註冊。一旦他們選擇退出，所有由 MDM 安裝的企業帳號和 app 也會一併移除。
- **更公開透明的做法。**使用者註冊到 MDM 之後，可以透過「設定」輕鬆查看哪些 app、書籍和帳號受到控管，以及裝置套用了哪些限制。iOS 會將所有 MDM 安裝的企業設定、帳號和內容標示為「受控」狀態。



使用者可以在「設定」中，透過設定描述檔的使用者介面，清楚看到裝置上已配置的項目。

- **使用者隱私。**雖然你可以透過 MDM 伺服器管理 iOS 裝置，但無法檢視所有設定和帳號資訊。你可以管理透過 MDM 佈建的企業帳號、設定及資訊，但無法存取使用者個人帳號。事實上，目前的安全防護功能具有雙重任務，除了保護公司控管的 app 中所有資料，也保護使用者個人內容不致流入公司的資料串流。

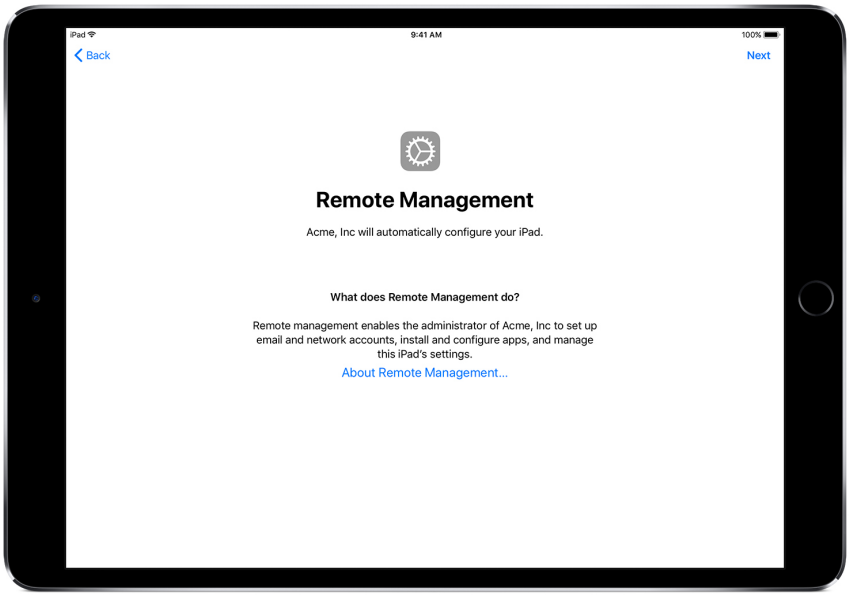
以下範例，是協力廠商 MDM 伺服器在個人 iOS 裝置上可以查看及無法查看的項目：

MDM 可以查看：	MDM 無法查看個人資料，例如：
裝置名稱	個人或工作郵件、行事曆、聯絡資訊
電話號碼	SMS 或 iMessage
序號	Safari 瀏覽記錄
機型名稱和型號	FaceTime 或電話通話記錄
容量和可用空間	個人的提醒事項和備忘錄
iOS 版本號碼	App 的使用頻率
已安裝的 app	裝置位置

- **裝置個人化設定。**企業發現，允許使用者以自己的 Apple ID 對裝置進行個人化設定，可提高他們對裝置的擁有權與責任感，進而提升生產力，因為他們可以自行選擇最有利於工作進行的 app 及內容來完成工作。

企業持有的裝置

在企業持有的部署模式中，你可以採用兩種做法：一是為每位使用者提供裝置，也稱為個人使用的部署；另一種是讓使用者輪流使用裝置，也稱為非個人化部署。多種 iOS 功能，如自動化註冊、可鎖定的 MDM 設定、裝置監管，以及總是開啟 VPN，可確保裝置皆根據公司特定需求進行配置，讓公司擁有充分的裝置掌控權，同時確保企業資料受到嚴密保護。



使用「Apple 商務管理」，你的 MDM 解決方案會在「設定輔助程式」執行期間自動配置 iOS 裝置。

- **自動化註冊。**公司持有的 iPhone、iPad 裝置與 Mac 系統進行初次設定時，你可使用「Apple 商務管理」自動進行 MDM 註冊。此一註冊程序，可設為強制執行且無法移除。你也可以在註冊過程中，將裝置設為受監管的模式，並允許使用者略過某些設定步驟。
- **受監管的裝置。**啟用監管功能，就能對公司持有的 iOS 裝置進行額外控管。這些功能，包括可透過全域代理伺服器來過濾網頁，確保使用者的網頁流量符合公司規範，以及防止使用者將裝置重置為原廠預設值等。所有 iOS 裝置，在預設狀態下皆為未受監管。監管模式可透過「Apple 商務管理」自動啟用，或透過 Apple Configurator 2 手動啟用。

即使你尚未規劃使用任何受監管裝置專用功能，依然建議你在設定裝置時，先行啟用監管模式，以利日後能充分運用。否則屆時需要，就得清除已部署的裝置才能啟用。監管並非等同於鎖定裝置，而是擴大管理功能，讓公司持有的裝置受到更完善的管理。長期而言，監管甚至能為你的企業提供更多選擇。

如需完整的監管設定列表，請參閱《iOS 部署參考》。

限制

iOS 支援下列幾種限制類別，你可以視公司需求，透過無線傳輸方式配置這些限制，不必擔心影響使用者：

- AirPrint
- App 安裝
- App 的使用情況
- 課堂 app
- 裝置
- iCloud
- 描述檔管理程式使用者和使用者群組限制
- Safari
- 安全性和隱私權設定
- Siri

下列類別也提供可透過 MDM 解決方案予以配置的選項：

- 自動化 MDM 註冊設定
- 設定輔助程式畫面

額外的管理功能

查詢裝置

除了配置裝置外，MDM 伺服器還可查詢裝置以取得各種資訊，如裝置詳細資料、網路、應用程式、合規情況，以及安全性資料，這些資訊有助於確保裝置持續遵守必要政策。MDM 伺服器會自行判斷取得這些資訊的頻率。

以下範例，是可供在 iOS 裝置上查詢的資訊：

- 裝置詳細資料 (名稱)
- 機型、iOS 版本、序號
- 網路資訊
- 漫遊狀態、MAC 位址
- 安裝的應用程式
- App 名稱、版本、大小
- 合規情況與安全性資料
- 安裝的設定、政策、憑證
- 加密狀態

控管作業

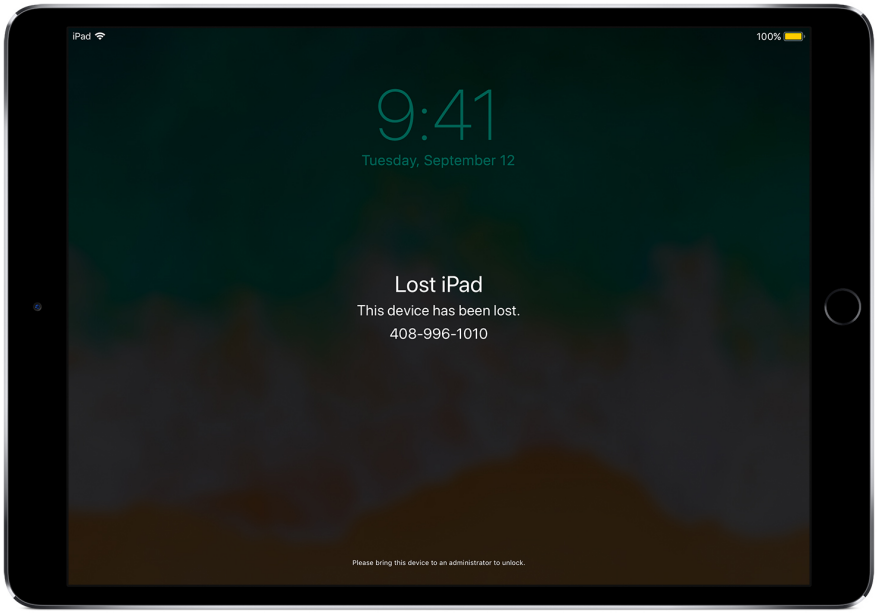
裝置受到控管時，MDM 伺服器可以執行各種管理作業，包括無須使用者操作即可自動變更配置設定、在以密碼鎖定的裝置上執行 iOS 更新、遠端鎖定或清除裝置，或是清除密碼鎖定，讓使用者在忘記密碼時進行重置。MDM 伺服器也可要求 iOS 裝置開始 AirPlay 鏡像輸出至特定的目的地，或結束目前的 AirPlay 工作階段。

遺失模式

如果使用 iOS 9.3 或後續版本，你的 MDM 解決方案即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顯示訊息與電話號碼。

受監管裝置進入「遺失模式」之後，MDM 可遠端查詢受監管裝置前一次上線的位置，協助找出遺失或遭竊的裝置。使用「遺失模式」不需啟用「尋找我的 iPhone」。

如果 MDM 遠端停用「遺失模式」，裝置就會解鎖，同時 MDM 會記錄裝置位置。為了讓使用者清楚了解裝置情況，他們會在「遺失模式」關閉時收到通知。



當 MDM 將遺失的裝置設為「遺失模式」時，它會鎖定裝置、允許訊息顯示在螢幕上，並判斷裝置位置。

啟用鎖定

在 iOS 7.1 或後續版本中，只要使用者在受監管裝置上開啟「尋找我的 iPhone」功能，你就能使用 MDM 來開啟「啟用鎖定」功能。這可讓你的公司享有「啟用鎖定」防竊功能所帶來的好處，另一方面，遇到像是離職員工未以其 Apple ID 先行移除「啟用鎖定」的情況，你也能略過這個功能。

MDM 解決方案可以根據下列情況取得略過代碼，並允許使用者在裝置上開啟「啟用鎖定」功能：

- 如果 MDM 解決方案允許使用「啟用鎖定」，只要使用者開啟「尋找我的 iPhone」功能，「啟用鎖定」就會隨之開啟。
- 如果 MDM 解決方案允許使用「啟用鎖定」，但「尋找我的 iPhone」功能為關閉狀態，則「啟用鎖定」會在下次使用者開啟「尋找我的 iPhone」時開啟。

總結

Apple 的 iOS 統一管理框架是你兩全其美的選擇，不僅可供 IT 配置、管理與保護裝置，並控制裝置上所傳輸的企業資料，同時也協助使用者透過自己喜愛的裝置，成就出色的工作表現。