宣告式裝置管理（DDM）

DDM 對現代化管理的影響之大，怎麼形容都不為過。

行動裝置管理（MDM）本身就是一項強大的工具。

在 Jamf 的帶領下，Apple 的 MDM 從早期以 binary 強制拉取設定的裝置管理模式，進化成如今彈性強大又好用的解決方案，遠遠超出當初的想像。

MDM 讓 Apple 管理人員第一次真正擁有自動化、可控性與可視性。 它減少重複性工作、降低人為錯誤風險，並支援更完善的資安防護。

但工作型態早已從辦公桌，轉變成全球分散的混合與遠端團隊。需求改變了，組織也必須跟著改變裝置管理方式，走向更彈性、更行動化、更安全的**「現代化管理」**。

什麼是現代管理？

現代管理是一種能因應當前工作環境，同時為未來職場做好準備的策略。

透過雲端管理與保護裝置、使用者、作業系統與應用程式。整合這些元素能強化資安、防護與 IT 的全局掌握能力。 這種整體式作法帶來更高可視性與更快的應變 能力。

閱讀我們關於「現代 管理」的深入白皮書 >

現代化管理究竟比傳統裝置管理好在哪？

傳統裝置管理以公司配發給員工的裝置為核心。只有這些授權裝置才能存取公司的內部網路。在當時，這確實是一個很好的管理方式。

但職場環境已經徹底改變。混合與遠端工作已成常態，即使是傳統辦公室，也需要讓各類型使用者在不危及公司資料的情況下保持高效。

現代化管理將一切移到雲端，並透過更安全、加密的連線運作。與地端部署相比，雲端部署具備多項資安優勢，例如：

- **驗證式註冊：**透過內建的註冊機制，確保 組織中每一台受管裝置的完整性與可信度。
- **身分與存取管理：**IT 依據雲端 身分控管誰能存取哪些資源。
- **權限管理。**使用者只取得必要的權限，有效保護敏感資料。
- **針對應用程式與資料提供精細的存取政策。**僅允許受信任裝置上的授權使用者存取應用程式與資料，大幅提升 安全性。
- **安全的網路流量：**透過加密機制防止未授權存取。
- **條件式存取：**依即時風險狀態自動限制存取，確保網路安全。

現代化管理在工作地點、工作時間，以及裝置是公司配發或自攜裝置（BYOD）上，都提供更高彈性。

直到 Apple 推出宣告式裝置管理（DDM），現代化管理的未來才真正 被實現。

什麼是宣告式裝置管理？

Apple 將 DDM 形容為對既有 MDM 通訊協定的一項「具變革性的更新」，讓裝置能夠主動、且自主地採取行動。

> 「裝置管理的未來，就是宣告式管理。」
>
> — Apple，WWDC 2021

在 Jamf，我們完全認同這樣的說法。這也是為什麼我們從一開始就準備好支援 DDM。

主動且具自主能力的裝置，正是宣告式裝置管理的核心基礎。自主裝置內建可依自身狀態變化做出反應的指示與規則。裝置接著會依預先定義的管理邏輯，自行執行所需的動作。

例如，當裝置不再符合合規要求，或出現被判定為疑似惡意程式的行為時，裝置可以立即採取行動。裝置不需要再等待伺服器輪詢狀態、回報結果，然後再等伺服器下達指令才行動。

這樣的機制帶來三個關鍵效益：

1. 減少伺服器與裝置之間的通訊負載，進而提升整體效能。
2. 加快對疑似惡意程式的隔離與修復速度，大幅提升安全性。
3. 因此能以更少的資源，實現更快速的擴充與規模化管理。

DDM 是怎麼運作的？

DDM 主要由三大支柱組成：**宣告（Declarations）**、**狀態（Status）**與**延展性（Extensibility）**。

宣告（Declarations）

宣告是由伺服器定義、發送到裝置上的設定內容。它們定義要直接在裝置上強制執行的政策，例如帳號、設定與限制。可以套用到所有使用者、小群組，甚至單一使用者或單一裝置。

每一個宣告都包含三個**必要**屬性：

1. **Type**：定義這個設定代表哪一種政策。
2. **Identifier key**：在一組宣告中識別某一個特定宣告。用來與伺服器同步宣告內容。
3. **Value**：用來限制資料範圍或指定可用的值集合。這些值可以是字串、數字、布林值、陣列或字典。

宣告類型

啟用條件（Activations）

啟用條件是一組會自動套用的配置與資產，且必須全部符合條件才能生效。例如，某個動作只會在特定裝置類型或特定作業系統版本上生效。這將判斷責任從伺服器轉移到裝置本身，由裝置依條件自行決定要套用哪些設定。

資產（Assets）

資產指的是配置內容運作時所需要的資料。如果資料量很大，資產宣告會提供一個 URL，讓裝置從 MDM 伺服器或內容傳遞伺服器下載。資產可以是各種資料，例如姓名、電子郵件、密碼或憑證。

配置內容

配置內容類似於 MDM 既有的描述檔承載資料（profile payloads），用來說明要套用到裝置上的政策，例如帳號、設定與限制。

裝置管理（Management）

管理宣告決定每一台裝置的整體管理狀態。它們傳遞伺服器與組織的靜態資訊。

狀態通道（Status Channel）

狀態通道用來追蹤裝置狀態的變化。裝置會回報狀態給伺服器，而伺服器只需訂閱它最關心的更新項目，例如作業系統版本、異常活動或合規狀態變化。

之後裝置只會回報變更內容，而不是每次都送出完整狀態資訊。 因此能更快取得更有價值的關鍵資訊。裝置主動觸發的非同步更新，讓伺服器能更精準監控裝置，同時大幅降低雜訊與網路流量。**進而提升整體效能。**

延展性（Extensibility）

幾乎沒有組織能讓所有 Apple 裝置與作業系統版本完全一致。 畢竟 Apple 裝置的使用年限很長。要發揮裝置投資的最大價值，就必須維持不同軟體版本與硬體能力之間的相容性。

透過 DDM，裝置與伺服器會自動同步變更，雙方都能即時知道有哪些新功能可用。不再需要硬編碼軟體版本或硬體相依性。

例如，當 IT 升級伺服器後，變更的能力會自動同步到裝置，裝置立刻就能使用新功能。反過來也一樣，當裝置更新時，伺服器立刻知道它能做到哪些新功能。

宣告式資料模型天生具備延展性，確保你的架構既適用於現在，也準備好迎接未來。

DDM 帶來嶄新的未來藍圖

DDM 與 MDM 的演進才剛剛開始。想像一下這樣的可能性：

- 用簡單又流暢的方式支援更複雜的管理策略
- 提升公司配發與自攜裝置上的使用者體驗
- 帶來更即時、更穩定的使用體驗
- 加快裝置啟用與使用者上線流程
- 讓 IT 擺脫重複又瑣碎的工作，專注在創新與真正需要的裝置管理能力上

如果 IT 團隊有更多時間真正去思考更大的藍圖，他們能為你的組織做到什麼？

當你投入 DDM 策略，組織的可能性就此展開。你的企業能跟著 DDM 一起成長，跟上 Apple 的速度。

你看見組織未來的哪些可能性？對你自己的目標而言呢？對整個工作世界而言呢？

我們相信，這項技術改變工作型態、支援現代管理不斷演進需求的真正潛力，現在才剛剛露出冰山一角。以下是我們對未來的一點預測。

DDM 將如何形塑 MDM 的未來？

雖然沒有人能預知未來，但可以確定的是，Apple 將透過 DDM 開啟更多創新空間。以下是我們認為會持續成長的幾個重點領域。

更強化的安全性

當你把 DDM 與近期的變化放在一起看，就會發現一個趨勢。

Apple Silicon 幾乎已經封鎖所有由指令碼或本機代理程式（以 root 權限執行）所觸發的無人值守更新。這不但阻斷駭客常用的惡意軟體手法，也減少使用核心延展功能（Kernel extension）等高風險做法，保護作業系統完整性。

未來管理動作將更仰賴正式的管理工具來執行，以降低風險。

更精細化的存取控管

透過 Managed Apple IDs，組織將能結合 iCloud Keychain 的 Passkeys 與 Apple Wallet，進一步強化對服務與設施的存取控管能力。

但這不代表管理會變得更強硬。DDM 讓 Apple 管理人員能以更精細的方式控管「誰、在哪裡、如何」 存取資源。

身分整合能力提升，帶來更好的使用者體驗

Apple 商務管理與 Apple 校務管理讓客製化身分整合變得更容易。任何身分提供者（如 Microsoft、Google、Okta、OpenID／SCIM）都能輕鬆整合並建立 Managed Apple IDs，是管理 Apple 裝置與使用者的最佳方式。使用者只要一把鑰匙就能存取工作所需的一切，不但體驗更好，也更安全。

這樣的觀點與能力演進，代表 MDM 將會：

- **更安全**—透過宣告式管理直接設定開箱即用的合規性，並限制與低階二進位檔的程式互動
- **更加原生化**—讓終端使用者的互動都以宣告為核心來運作
- **更有價值**—在 MDM 原本就很穩固的基礎上，透過 DDM 持續進化與強化

若想進一步了解這項深遠轉變所帶來的影響，歡迎觀看 2023 JNUC 簡報〈**MDM 的下一步是什麼？**〉

未來，就在現在。

這次巨大躍進最棒的一點是，現有的 MDM 廠商其實「早就可以」開始使用宣告式管理功能了。不需要為了新協定或伺服器架構而打亂既有作業，宣告與狀態通道可以與現有的 MDM 指令與設定描述檔並行運作。**DDM 完全不會影響既有 MDM 的行為模式。**

這代表 IT 可以依照最適合自己的節奏導入 DDM，不需要一次全面更新所有既有的 MDM 工作流程。

更棒的是：你現在就可以馬上開始導入！

Jamf 是如何支援 DDM 的？

Jamf 與 Apple 保持緊密合作，因此我們總是能在第一時間就支援 Apple 的創新。

從第一步開始就全面支援

自 2022 年 10 月起，Jamf Pro 就已自動為相容的受管裝置啟用宣告式裝置管理功能。 啟用 DDM 的裝置會自動回報狀態變更給 MDM 伺服器，並在發生特定變化時主動回報，同時更新到裝置清單中。管理員可以自訂這些裝置狀態。

狀態通道支援三個全新欄位

在 Jamf Pro 10.46 中，我們新增了 DDM 狀態通道，回報以下三個新欄位：

- `SupplementalBuildVersion`
- `SupplementalOSVersionExtra`
- `Passcode Compliance`

這些新的狀態欄位會自動啟用，讓裝置可以即時、自主地更新狀態到 Jamf Pro。

iOS 專屬支援

DDM 的能力非常強大，而且發展速度非常快！以下是我們運用 DDM 提升易用性與安全性的幾個實際做法：

- iOS 裝置的更新會使用鎖定畫面的密碼產生授權權杖，並在一定時間後失效，以提升安全性
- 終端使用者啟用這個權杖後，更新過程中不需要再解鎖裝置
- 若裝置在預設時間內未被解鎖，更新將暫停，並在使用者解鎖後提示是否允許更新。

由 DDM 驅動的受管軟體更新

在 Apple 推出 DDM 之前，Jamf 管理員通常只能發送大量動作或政策來更新裝置。透過 DDM 的受管軟體更新帶來更多強大功能：

- 軟體更新計畫設定更簡單
- 終端使用者有更彈性的延後更新選項
- 新的自動化與強制執行能力，讓 IT 管理員有更高的掌控度
- 裝置會主動回報更新進度，讓管理員有更高可視性

展望未來

隨著 DDM 協定持續擴展，Jamf 也會善用這項技術，並全程提供支援。例如，我們持續跟上 Apple 的腳步，支援像 Apple Vision Pro、Apple Watch 等新型工作裝置，讓終端使用者用最適合自己的方式保持高效。

從來沒有像現在這樣令人振奮的 Apple 裝置管理時代。

宣告式裝置管理為邁向現代管理帶來了巨大的推力。甚至可以說是「火箭推進等級」。

我們已經跳脫傳統裝置管理的框架。一夜之間，我們從大量往返通訊，進化到裝置自主運作。我們積極擁抱未來。

管理與 MDM 的未來正在此刻成形，而我們正一起打造它！

現代管理的時代已經來臨。

能把握這波前所未有成長機會的組織，將會為未來做好準備，而導入 Apple 裝置生態正是關鍵一步。

你可以思考的重點

檢視你目前的技術策略。是否夠彈性？是否容易擴展與移轉？是否符合現代管理的裝置管理與資安思維？

如果沒有，導入現代管理你能獲得什麼？快速成長的能力？ 能不能快速調整方向、靈活應變？吸引頂尖人才，同時確保所有人都安全又連線順暢？

如果跟不上，你可能會失去什麼？

現代管理的時代已經來臨。 一切取決於你是否願意把握這個機會，為你的組織開啟下一步轉型。

Jamf 會一路陪你前行。

如果您已準備好 **加入 Apple 和 Jamf** 的行列，一起踏上 **現代管理**的轉型之路，並希望能放大 雲端和 DDM 功能所能帶來的所有優勢，**我們很樂於提供協助！**

jamf