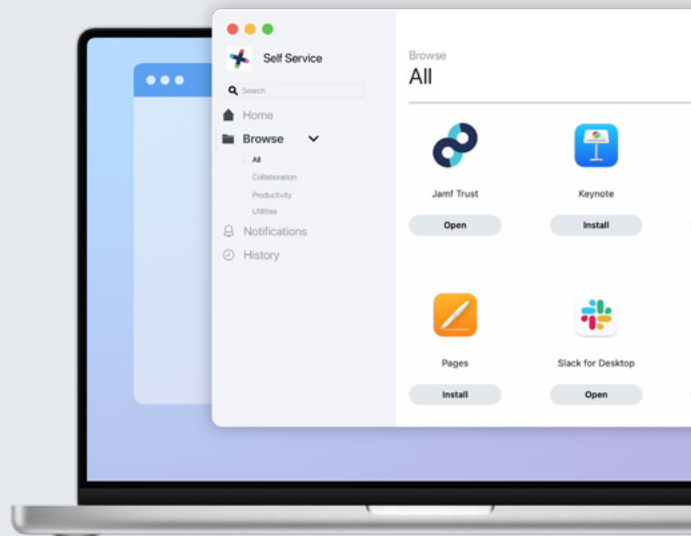


Jamf for Mac – 專業服務導入方案

專家指導，協助您管理、保護並最佳化 Mac 環境



發揮 Apple 裝置管理的最大潛力

管理 macOS 環境需要精準、安全，並能無縫整合企業工具。透過 Jamf for Mac，您的組織能有效導入 Jamf Pro、Jamf Connect 和 Jamf Protect，確保 Apple 裝置被妥善管理、受到保護、符合規範並維持最佳效能。

我們的專業服務導入方案能協助您設定並整合這些強大解決方案，為您的業務需求量身打造可信、可管控且安全的 Apple 體驗。

為什麼選擇 Jamf for Mac？

Jamf for Mac 是一套完整的設定與實作服務，能讓 IT 團隊具備所需工具與專業知識，有效管理、保護並最佳化 Apple 裝置。我們的 Jamf 認證專家會與您的團隊並肩合作，導入裝置管理、身分驗證與安全監控，協助您最大化 Apple 技術投資效益。

- **無縫部署與整合** — 由 Jamf 專家引導的結構化導入流程。
- **安全與合規** — 根據最佳實踐設定 Jamf Protect，有效防禦威脅。
- **零接觸註冊** — 搭配 Jamf Pro 與 Apple Business Manager，自動完成裝置設定。
- **單一登入 (SSO) 與身分管理** — 使用 Jamf Connect 實現安全驗證。
- **持續支援與最佳化** — 確保你的環境維持安全、具擴充性與高效能。



使用者的生產力，最大化

初步了解階段

階段一：導入前規劃

- 與 Jamf 認證專家進行啟動通話，檢視您的環境並釐清目標。
- 確認先決條件，包括網路存取、Apple Business Manager 設定與身分供應商配置。
- 概覽 Jamf 在管理、保護與監控 Apple 裝置中的角色。

建置階段

階段二：Jamf Pro 設定

- 使用者與管理者設定 — 管理員角色、存取權限與通知設定。
- 自動裝置註冊 — 整合 Apple Business Manager，實現零接觸部署。

- 裝置清單與資產管理 — 設定裝置追蹤、動態群組與報告工具。
- 修補管理與軟體部署 — 自動推送 macOS 與第三方應用程式更新，確保安全合規。

階段三：Jamf Connect 的身分與驗證設定

- SSO 與身分提供者整合 — 可與 Azure AD、Okta 或 Google Workspace 設定。
- 密碼同步與驗證政策 — 確保使用者登入安全且順暢。
- 零信任設定 — 強化安全控制，同時維持流暢的使用者體驗。

階段四：Jamf Protect 的安全與威脅防護

- 威脅情報與監控 — 啟用即時安全洞察與合規控制。
- 事件回應與分析 — 建立偵測與補救流程，應對威脅事件。
- 安全政策執行 — 讓 Mac 裝置符合 CIS 基準與法規要求。

部署

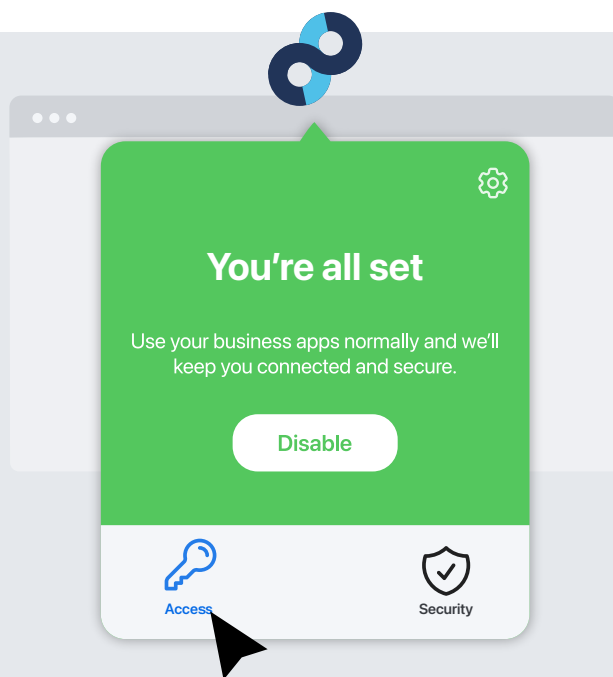
階段五：測試、最佳化與知識轉移

- 為 IT 管理員提供實作訓練，學習管理政策、設定與監控作業。
- 效能驗證與疑難排解，確保整體體驗順暢無礙。

Jamf 專業服務的價值

透過與 **Jamf 專業服務團隊** 合作，可確保您的 Apple 生態系統**順利部署**，並長期維持高效運作。我們的專家團隊協助您避免常見錯誤，最佳化設定，並**確保環境具備未來延展性**。

- 透過自動化流程與自助功能，減輕 IT 工作負擔。
- 透過流暢的存取與身分驗證體驗，提升終端使用者生產力。
- 藉由即時威脅偵測與修復能力，提升整體安全防禦。
- 藉由符合產業安全最佳實務，強化法規遵循。



www.jamf.com/zh-tw/

© 2025 Jamf, LLC. 著作權所有，並保留一切權利