AI 助手資安技術白皮書

發布日期：2026 年 4 月 | 文件分級：公開文件

執行摘要

AI 助手是一個整合於 Jamf Pro、Jamf Account 與 Jamf Protect 中的對話式介面，透過 AWS Bedrock 調用 Anthropic 旗下 Claude 模型提供服務。該工具提供用於資產查詢、配置分析、合規檢查與知識檢索的正式生產環境工具。

本文說明 AI 助手在所有 Jamf Cloud 營運區域（美國、歐盟、亞太）運作對應的資安架構、資料處理實務與隱私管控機制。

AI 助手建立在以下四項資安原則之上，每一項都在架構層級強制執行，而非僅止於政策或提示詞層面：預設停用、最小權限存取控制、API 層級的唯讀強制執行，以及透明且可歸因的回應。AWS Bedrock Guardrails 在所有環境中提供額外的內容監控與提示詞注入偵測。

架構概述

基礎架構

AI 助手部署於所有 Jamf Cloud 營運區域。客戶資料在其 Jamf 環境所屬的區域中處理，不會跨區域邊界傳輸。

營運區域	AWS Bedrock 對應區域	狀態
美國	us-east-1	正式營運
歐盟	eu-central-1	正式營運
亞太地區	ap-northeast-1	正式營運

模型

AI 助手透過 AWS Bedrock 調用 Anthropic 開發的 Claude 模型。Bedrock 作為 Jamf 基礎架構與 Anthropic 模型之間的推論中繼層。當前適用模型版本可參閱 Jamf Learning Hub。

與 Anthropic 次處理者關係說明： Anthropic 不會接收或存取客戶資料。模型推論在 AWS Bedrock 基礎架構內進行，該基礎架構運行於 Jamf 的 AWS 環境中。客戶查詢、工具結果與對話上下文皆在 Bedrock 內處理，不會傳輸至 Anthropic。有關 AWS Bedrock 如何處理資料隱私與資安的詳細資訊，請參閱 AWS Bedrock 資料保護文件。

AWS Bedrock 資安特性：

- 客戶資料不會用於訓練或微調 Anthropic 的模型
- 資料在區域內處理，不會離開客戶環境對應 AWS 區域
- 符合 SOC 2 Type II 標準
- AWS 企業級資安控管適用於所有推論請求

模型更新：Jamf 透過 AWS Bedrock 管理模型版本。目前的模型版本維護於 Jamf Learning Hub 中；具備變更管理需求的組織應監控 Learning Hub 以掌握模型版本變更。

工具架構

AI 助手採用工具呼叫架構：使用者送出查詢後，模型會決定要呼叫哪些工具，以使用者現有權限針對特定 Jamf API 執行這些工具，並將結果彙整為回應。

所有工具皆為唯讀。AI 助手工具涵蓋五大類別：知識檢索（Jamf 文件與知識庫）、配置存取（政策、描述檔、腳本、藍圖等）、資產查詢（Mac 與行動裝置資料）、合規檢查（對照 CIS、NIST 與 DoD STIG 等基準）以及資安情資（行動應用程式風險評估）。Jamf Protect 工具（警示分析、惡意軟體查詢）目前提供有限測試版。目前的工具目錄（包含可用性與產品需求）請參閱 Jamf Learning Hub。

第三方資料流程：三項工具會查詢 Jamf 基礎架構之外的外部服務。這些整合已記錄於文件中以確保透明度。

- **Apple OS Lookup** 查詢 Apple 的 Global Device Management Framework（GDMF）API（gdmf.apple.com），此為 Apple 的公開端點。該工具不會傳輸任何客戶資料，僅檢索公開的 Apple 作業系統發布資訊。
- **App Lookup** 查詢 iTunes Search API（itunes.apple.com），作為應用程式版本與修補程式資訊的備用資料來源。該工具不會傳輸任何客戶資料，僅檢索公開的應用程式中繼資料。
- **Mobile App Risk** 查詢 NowSecure 的 MARI（行動應用程式風險情資）資料庫以檢索資安評估。唯一傳輸的資料是應用程式的商店識別碼（例如 iOS bundle ID）與平台（iOS 或 Android）。不會傳輸任何裝置資料、使用者身分或組織資訊。

資安設計原則

預設停用。AI 助手對所有組織預設為停用，需要管理員在 Jamf Account 中手動啟用。各工具群組需分別獨立啟用，開啟 AI 助手核心功能不會自動啟用 Jamf Pro 工具或後續新增產品整合功能。在使用者的組織主動選擇啟用之前，使用者無法使用任何 AI 功能，且管理員可隨時停用任何工具群組。

最小權限存取控制。所有工具查詢皆以已驗證使用者的權限執行，繼承既有的 Jamf Pro RBAC 控管機制，無需任何修改。AI 助手不會提升權限，也不會存取使用者原本無法直接存取的資料。無權限檢視政策的使用者，無法透過 AI 助手檢索該政策。

API 層級的唯讀強制執行。 AI 助手使用已驗證使用者的工作階段權杖呼叫 Jamf Pro API——沒有獨立且具備提升權限的服務帳戶。AI 助手工具發出的所有 API 呼叫皆為 GET 請求。系統中沒有任何工具會對 Jamf Pro 發出 POST、PUT、PATCH 或 DELETE 請求。這是在實作層級強制執行的架構限制，而非提示詞層級的指令，也不是可透過技巧性提示詞覆寫的政策。無論查詢如何建構，AI 助手皆無法修改裝置配置、部署政策、移除應用程式或變更註冊狀態。

透明且可歸因的回應。 每一則回應都會標示其來源，讓管理員能對照官方文件驗證答案。回傳給模型的工具結果為結構化資料，而非自由格式文字，使每一則回應皆可追溯其來源。

Bedrock Guardrails。AWS Bedrock Guardrails 部署於所有 AI 助手環境中。Guardrail 配置包含針對多種有害類別（暴力、色情內容、仇恨言論、侮辱、不當行為）的內容監控，以及高敏感度的提示詞注入偵測。所有 Guardrail 事件皆會被追蹤與記錄，提供完整的被標記輸入與輸出稽核紀錄。

資料處理

資料流程

使用者送出查詢後，執行順序如下：

1. **查詢處理**：使用者的自然語言查詢由 AI 助手後端接收
2. **工具執行**：相關工具使用已驗證使用者的權限查詢 Jamf API
3. **上下文彙整**：彙整使用者的查詢、相關工具結果與當前對話串用於推論
4. **模型推論**：推論請求由 AWS Bedrock 處理並產生回應
5. **回應傳送**：產生的回應透過 Jamf 介面回傳給使用者

推論期間處理的資料類型

資料類型	推論層是否處理	備註
使用者查詢	是	使用者送出的自然語言問題
工具結果	是	與查詢相關的資產資料與配置詳細資訊
對話歷史紀錄	是	當前對話的完整對話串歷史紀錄，由永續儲存載入；資料留存 30 天
使用者憑證或權杖	否	永遠不會納入模型上下文
完整資料庫內容	否	僅納入與查詢相關的結果

資料駐留

AI 助手遵循 Jamf 的區域資料邊界。推論請求會路由至客戶 Jamf 環境所屬區域中的 AWS Bedrock 部署：

- **美國客戶**：資料在 AWS us-east-1 中處理
- **歐盟客戶**：資料在 AWS eu-central-1 中處理
- **亞太客戶**：資料在 AWS ap-northeast-1 中處理

裝置資產、配置資料與其他客戶特定資料不會跨區域傳輸。

知識檢索備註：知識檢索僅查詢 Jamf 的文件語料庫，不會存取裝置資產、配置詳細資訊或其他客戶特定資料。所有 AI 助手查詢，包含知識檢索，皆在客戶指定的區域中處理。

工作階段隔離

每一則 AI 助手對話的範圍皆限定於已驗證使用者及其所屬組織。對話上下文不會在使用者之間或客戶組織之間共享。某一組織的查詢無法顯示另一組織的資產資料或配置詳細資訊。

對話留存 30 天，然後自動且永久刪除。留存期限是透過 DynamoDB TTL 在儲存層強制執行，而非可能被延遲或跳過的排程清理任務。每一則對話僅供建立該對話的使用者與組織存取。對話資料僅儲存於 Jamf 基礎架構；除推論請求本身外，查詢內容與回應不會由 AWS Bedrock、Anthropic 記錄或留存。

資料留存與稽核紀錄

對話內容留存 30 天。30 天後，對話資料將被刪除且無法復原。

稽核紀錄維護於 Jamf Account 的「Activity History → AI Assistant」（活動歷史紀錄 → AI 助手）中。稽核紀錄完整記錄所有 AI 助手配置管理變更，包含：

- AI 助手開啟或關閉操作
- 工具群組的新增、移除或更新動作
- 執行每一項變更的管理員身分（姓名與電子郵件）
- 每一項變更的日期與時間

稽核紀錄條目可供 Jamf Account 中的 Organization Administrator 與 Administrator 角色存取。稽核紀錄提供了完整的配置變更紀錄。

資料類型	留存期限	備註
對話內容	30 天	自動刪除；無法復原
稽核紀錄（配置變更）	Jamf Account 標準留存期限	可在 Jamf Account Activity History 中存取
模型推論上下文	不會留存超過工作階段	工作階段結束時捨棄
模型訓練	不適用	Anthropic 不會使用 AWS Bedrock 客戶資料進行訓練

存取控制

身分驗證

AI 助手繼承已驗證使用者的 Jamf 工作階段。不需要額外的登入、API 金鑰或憑證。未通過其 Jamf 環境身分驗證的使用者無法存取 AI 助手。

啟用 AI 助手 需要在 Jamf Account 中具備 Administrator 或 Organization Administrator 角色。一般使用者與唯讀角色無法啟用、停用或修改 AI 助手工具群組設定。管理員進行的所有變更皆記錄於 Activity History 稽核紀錄中。

授權

所有工具查詢皆以已驗證使用者的權限執行。AI 助手不會提升權限或繞過現有的 Jamf Pro 角色型存取控管：

- 資產查詢僅回傳使用者有權限檢視的裝置
- 配置解讀結果遵循既有的物件層級存取控管
- 合規資料存取遵循標準 Jamf Pro RBAC
- 無權限存取政策的使用者，無法透過 AI 助手檢索該政策的詳細資訊

啟用與停用 AI 助手

AI 助手對所有組織預設為停用。管理員需在 Jamf Account 的「Organization → AI Assistant」（組織 → AI 助手）中手動開啟功能。

停用 AI 助手會立即生效並且可隨時重新開啟。管理員只需取消勾選 Jamf Account 中的「Enable AI Assistant」（啟用 AI 助手）核取方塊。此操作會立即停用組織中所有使用者的全部 AI 助手功能。也可單獨停用各工具群組（Jamf Pro 唯讀工具），無需停用 AI 助手核心功能。

環境層級範圍限定提供額外管控機制，適合希望分階段審慎上線功能的企業。啟用 Jamf Pro 唯讀工具時，管理員可限定僅特定環境和租戶可使用，而非全環境開放。組織可在沙盒或測試環境中先試行 AI 助手，確認無異常後再於正式環境啟用，且過程不會變更正式環境的任何設定。

各產品的工具可用性

目前的工具可用性、產品需求與測試版狀態皆維護於 Jamf Learning Hub。

合規

AI 助手運行於 Jamf 現有的合規計畫框架內。目前的 Jamf 認證清單請參閱 Jamf Trust Center 或聯繫您的客戶團隊。

AWS Bedrock 合規（適用於推論層）：

- SOC 2 Type II
- ISO 27001

FedRAMP 與 StateRAMP：AI 助手不適用於 StateRAMP 或 FedRAMP 授權的環境。有關未來 FedRAMP 與 StateRAMP 可用性的藍圖詳細資訊，請聯繫您的 Jamf 客戶團隊。

滲透測試： AI 助手已作為 Jamf 資安審查計畫的一環完成滲透測試。客戶若有需求，可透過專屬 Jamf 客戶團隊，於簽署保密協議（NDA）後取得測試報告。

資安控管摘要

控管項目	實作方式
傳輸中加密	所有通訊採用 TLS 1.2 以上加密協定
靜態資料加密	AWS KMS 加密
身分驗證	繼承 Jamf Pro 工作階段，無需額外憑證
需要管理員角色	Jamf Account 中的 Administrator 或 Organization Administrator
授權	所有工具查詢強制執行 Jamf Pro RBAC，無法提升權限
資料駐留	分區域獨立處理（美國/歐盟/亞太），無跨區域傳輸
Anthropic 資料存取	Anthropic 不會接收客戶資料，推論過程保持在 AWS Bedrock 內
模型訓練	客戶資料不用於模型訓練（AWS Bedrock）
第三方處理者	NowSecure（應用程式風險情資）：僅應用程式識別碼；Apple GDMF（作業系統版本）：僅公開資料
稽核紀錄	配置變更留存於 Jamf Account Activity History，按執行者、操作內容與時間戳記記錄
對話留存	30 天
唯讀操作	於實作層級強制執行，所有 Jamf Pro API 呼叫皆為 GET 請求，工具程式碼

	中不存在任何寫入方法
工作階段隔離	每則對話僅供已驗證使用者及其所屬組織存取，其他使用者或組織無法存取
預設停用	對所有組織預設為停用，需要管理員手動啟用
功能停用機制	停用立即生效，只需在 Jamf Account 中取消勾選「Enable AI Assistant」（啟用 AI 助手），並且可隨時重新開啟
環境範圍限定	專業工具可限定僅特定環境、租戶使用，實現分階段控管上線
網頁應用程式防火牆（WAF）	在正式環境與測試環境的 API Gateway 層級套用
Bedrock Guardrails	跨有害類別的內容監控與高敏感度提示詞注入偵測；所有事件皆被追蹤與記錄
滲透測試	正式版上線前完成測試；測試結果可於簽署保密協議（NDA）後提供

文件資訊

發布日期	2026 年 4 月
文件分級	公開文件
文件網址	jamf.it/aiassistant

更多參考資源

- Jamf Trust Center——目前的 Jamf 認證、合規文件與資安態勢：https://www.jamf.com/zh-tw/trust-center/
- Jamf Learning Hub——目前的 AI 助手工具目錄、產品需求與模型版本：https://learn.jamf.com/r/zh-TW/jamf-account-documentation/AI_Assistant?content-lang=zh-TW
- 本文件——本文件最新版本下載網址：jamf.it/aiassistant
- 有問題？請聯繫您的 Jamf 客戶團隊。