jamf

白皮書

iOS 安全性檢查清單

落實 iOS 網際網路安全性（CIS）基準

確保 iOS 安全的建議

網際網路安全性（CIS）的 iOS 基準測試被廣泛視為是企業組織保護 iPad 和 iPhone 裝置安全所需的全面性清單。本白皮書將解釋如何落實獨立組織的建議。

要瞭解 Jamf Pro 如何幫助保護和管理您的 iOS 裝置，請參閱 **www.jamf.com**。

什麼是網際網路安全性中心(CIS)？

網際網路安全性中心 (CIS) 是一家 501c3 非營利組織，致力於提高公共和私營部門實體的網路安全準備和應變能力。

CIS 基準是如何建立的

CIS 基準是由該領域的專家共同創立的審查流程。共同參與者提供了來自不同背景的觀點，包括諮詢、軟體開發、審計和合規、安全性研究、運營、政府和法規。

每個CIS基準都必須經過兩個階段的共識審查。第一個 階段始於初始基準測試開發期間。在此階段，主題專家 (SME) 將聚在一起討論、創建和測試基準的工作草案。討論會持續進行到就基準建議達成共識為止。第二個階段則是在基準發佈後開始。在此階段，網路社群提供的所有回饋均由團隊共同審核，以便納入基準測試中。如果您有興趣參與共識過程，請參閱 https://www.cisecurity.org/communities/。

CIS 和 iOS 管理基礎知識

什麼是 MDM？

行動裝置管理 （MDM） 是 Apple 針對 iOS、macOS 和 Apple tvOS 的內建管理框架。設備Jamf Pro 是 Apple MDM 的標準解決方案。

什麼是設定描述檔？

設定描述檔界定了 iOS 裝置上的設定，並透過 MDM 分發到裝置上。

什麼是「監管」？

一旦裝置通過 Apple 的部署計劃或 Apple Configurator 進行管理，監督即可提供更深層的iOS管理。

裝置擁有權

根據企業組織的技術模式，資安需求也有所不同：透過自備裝置(BYOD) 方式由個人擁有，或由企業機構擁有並再分發給使用者。

安全分級

等級 1 (L1) 或等級 2 (L2) 定義必須能套用於個人或企業機構擁有的裝置的安全要求和設定。L2 提供了裝置更大的控制性，並遠超出原本的基本安全需求。

什麼是APNs?

Apple 推送通知服務 （APNs） 為 iOS 管理之必須。請查看以下文章以瞭解有關APNs的更多資訊： https://www.jamf.com/blog/what-is-apple-push-notification-service-apns/requirements。

保護企業機構擁有的裝置

最近一項調查發現，比起個人擁有的裝置，74% 的企業員工更喜歡公司發放的裝置。 Jamf Pro 幫助組織安全地落實其機構擁有的 iOS 裝置計畫，並簡化企業機構擁有的 iPad 和 iPhone 裝置的分發和管理。

網際網路安全性中心（CIS）建議

設定

- 為註冊描述檔設置同意訊息和說明。
- 確保描述檔可以被刪除。

功能性：

- L2：停用螢幕截圖和螢幕錄製。
  - 在裝置鎖定時停用使用語音撥號。
  - 在裝置鎖定時停用 Siri。
  - 停用 iCloud 備份。
  - 停用 iCloud 文件和資料。
  - 停用 iCloud 鑰匙圈。
  - 停用託管 App 將資料儲存在 iCloud 中。
  - 啟用強制加密備份。
  - 停用允許所有內容和設備。
- L2：停用允許使用者接受不受信任的 TLS 憑證。
  - 停用允許安裝設定描述檔。
  - 停用允許新增 VPN 配置。
  - 停用允許修改行動數據 App 設定。
- L2：停用允許與非 Configurator 主機配對。
  - 在非託管目的地中停用來自託管源的文件。
  - 在託管目的地中停用來自非託管源的文件。
  - 啟用「將AirDrop視為非託管目的地」。
  - 禁用允許切換。
  - 強制啟用 Apple Watch 手腕檢測。
  - 停用允許設置附近的新裝置。
  - 停用於鎖定螢幕中顯示控制中心。
  - 停用於鎖定螢幕中顯示通知中心。

Apps：

- 強制啟用詐騙警告。
- 接受 Cookie 設置允許使用「訪問過的網站」或「僅限當前網站」。

網域：

- 配置託管的Safari Web網域。

密碼：

- 停用允許簡單值。
- 密碼長度至少須「6」字元
- 自動鎖定時間最長為「2 分鐘」
- 設備鎖定的最大寬限期設定為「立即鎖定」
- 密碼輸入錯誤次錯不得大於「6」次。

VPN

- 確保 VPN 處於「已設定」 狀態。
- 最好使用按 App 劃分的 VPN

電子郵件：

- 使用電子郵件配置檔設置使用者的電子郵件帳戶。
- 停用允許使用者從此帳戶移動郵件。

通知：

- 配置所有受管理的 App 的通知設定。

鎖定螢幕訊息：

- 設定「如果丟失，請交至...」訊息。

Jamf Pro 中的功能

Jamf Pro 允許您透過設定描述檔設置、啟用和／或禁用上述所有 L1 和 L2 系統偏好。在註冊期間，其中一些設定會要求監督 iOS 設備。有關 iOS 監督的更多資訊，請查看以下內容：https://support.apple.com/en-us/HT202837。

Jamf Pro 讓企業組織能夠設定個人化的鎖定螢幕訊息，以確保裝置安全歸還，不會遭受解鎖及篡改。

*來源：https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/

確保 BYOD 和個人擁有裝置的安全

Jamf Pro 可幫助企業組織為員工減輕多台裝置的負擔，讓他們能夠在工作和家中安全地使用同一台裝置。

網際網路安全中心建議

設定，

- 為註冊描述檔設置同意訊息和說明。
- 確保描述檔可以被刪除。

功能性：

- 在設備鎖定時停用語音撥號。
- 在設備鎖定時禁用 Siri。
- 停用受管理的 App 將資料儲存在 iCloud 中。
- 啟用強制加密備份。

- L2：停用允許使用者接受不受信任的 TLS 憑證
  - 在非託管目的地中停用來自託管源的文件。
  - 在託管目的地中停用來自非託管源的文件。
  - 啟用「將AirDrop視為非託管目的地」
- L2：停用允許切換。
  - 停用在鎖定螢幕中顯示控制中心。
  - 停用在鎖定螢幕中顯示通知中心。

Apps

- 在 Safari 瀏覽器中強制啟用詐騙警告。
- 接受 Cookie 設置允許使用「訪問過的網站」或「僅限當前網站」。

網域：

- 配置託管的Safari Web網域。

密碼：

- 停用允許簡單值。
- 密碼長度至少須「6」字元
- 自動鎖定時間最長為「2 分鐘」
- 設備鎖定的最大寬限期設定為「立即鎖定」
- 密碼輸入錯誤次錯不得大於「6」次。

VPN

- 確保 VPN 處於「已設定」 狀態。
- 最好使用按 App 劃分的 VPN

電子郵件：

- 使用電子郵件配置檔設置使用者的電子郵件帳戶。
- 停用允許使用者從此帳戶移動郵件。

通知：

- 確保 VPN 處於「已設定」 狀態。
- 最好使用按 App 劃分的 VPN

Jamf Pro 中的功能

Jamf Pro 的 BYOD 解決方案可讓您為註冊描述檔建立自訂同意訊息和說明，並為前員工提供一個更簡單的流程，以便在他們離開企業組織或專案時刪除 BYOD 描述檔。

如果您的企業組織需要落實 CIS 建議中所有的 L1 和/或 L2 安全設置，請利用 Jamf Pro 的功能將 iOS 裝置註冊為不受監管的企業裝置。我們也建議在 iOS 註冊「個人擁有裝置」時停用使用者主動註冊設置透過在 Jamf Pro 中建立和分發設定描述檔，可以為單一或一組 iOS 裝置配置、停用和／或啟用所有 L1 和 L2 安全性設定。

其他注意事項

Jamf Pro 可協助企業組織超越裝置管理和設定描述檔的侷限，確保裝置軟體一直保持在最新狀態，不讓惡意攻擊有乘之機。

CIS建議：

- 確保 iOS 裝置沒有越獄。
- 保持軟體最新狀態。
- 啟用應用程式更新自動下載。
- 僅限於終端用戶裝置上能夠開啟「尋找我的 iPad」和／或「尋找我的 iPhone」功能。
- 確保具高價值的攻擊目標（如企業CEO, 人資部門）使用最新的 iOS 裝置架構。

Jamf Pro 中的功能

Jamf Pro 為 iPad 和 iPhone 作業系統提供零時差支援，以確保一直都能支援最新的軟體。此外，Jamf Pro 的Self Service 可以讓企業
自訂 App 目錄，其中包含使用者可能需要的所有資源、應用程式和配置。、使用者可以按需求存取，而無需向 IT 部門請求協助。如果設備遺失或遭竊，Jamf Pro 可以安全地鎖定、抹除和重置裝置，確保公司和個人資料永遠不會外洩。

更好的裝置安全性就從這裡開始

Jamf Pro 讓您可以輕鬆實踐企業組織網路安全中心的 Apple iOS 基準。

現在就 申請免費試用，將本指南付諸實踐。