使用Intune部署安全聯結器

目錄

簡介

本文檔介紹如何使用Intune部署安全聯結器。

概觀

本分步指南介紹如何通過Intune對您的iOS/iPadOS裝置進行MDM管理，並通過Apple Configurator推送配置檔案

您還可以在此處參考我們的Intune註冊文檔和PDF指南

附註：此方法向您展示如何通過Intune和Apple Configurator管理您的裝置

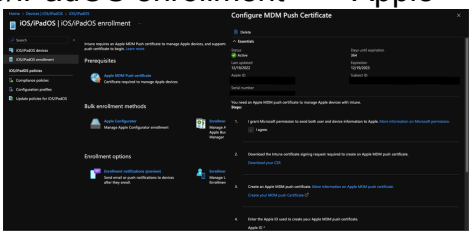
重要附註：

如果您正在通過Company Portal App對受管裝置進行MDM管理，則可以從第14步開始。

本文自2023年12月4日起原樣提供，Umbrella支援不保證這些說明在此日期之後仍然有效，並且可能會根據Microsoft Intune和Apple iOS的更新進行更改。

程式

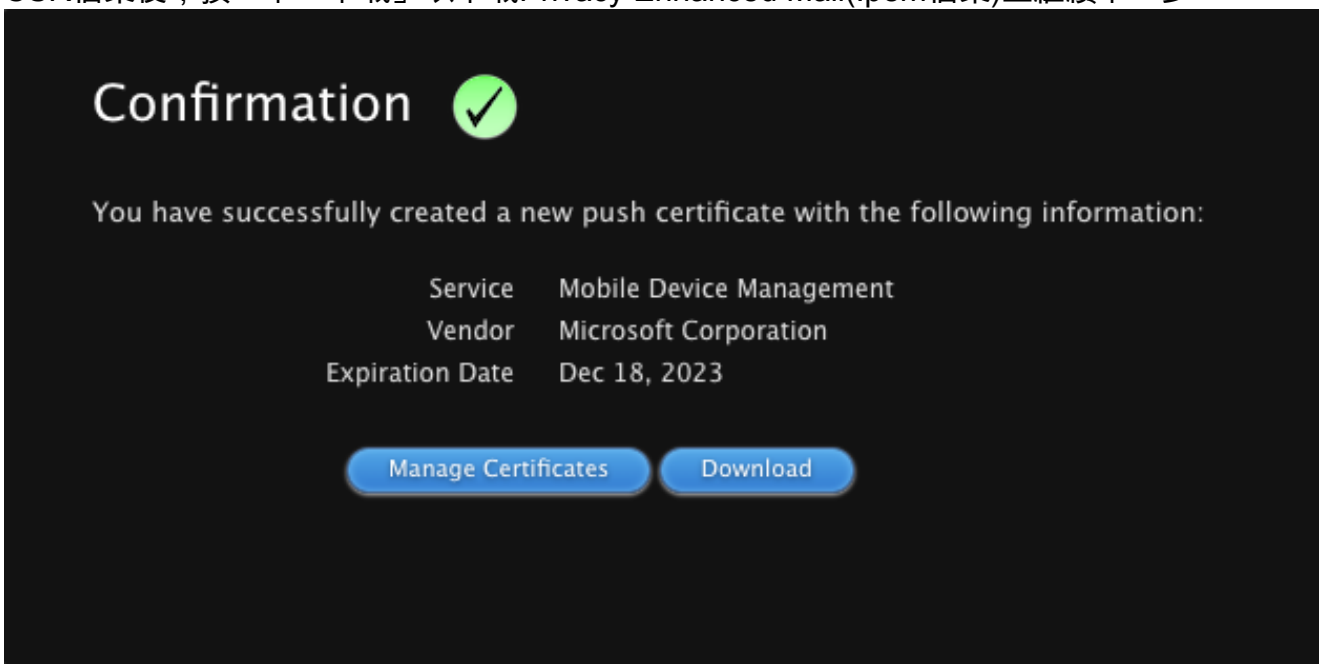
1. 登入到Azure門戶並搜尋「Intune」。 或者，轉到 https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/並登入
2. 進入Intune首頁後，請轉到Devices —> iOS/iPadOS —> iOS/iPadOS enrollment —> Apple MDM Push certificate，然後按一下「Download your CSR」



11752925317012

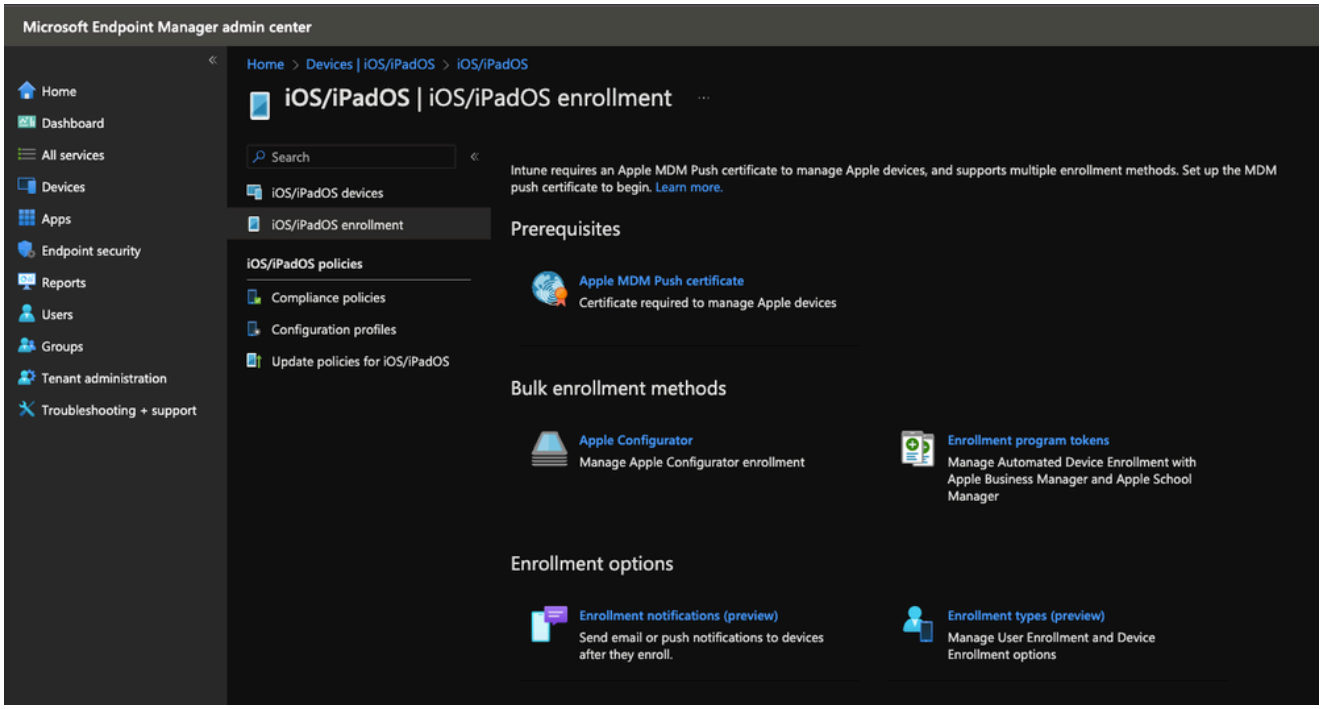
3. 然後，點選「建立您的MDM推送證書」，它將您重定向到https://identity.apple.com/pushcert/

4. 在Apple推送證書門戶上，轉到「建立證書」並上傳剛下載的IntuneCSR.csr檔案。成功上傳CSR檔案後，按一下「下載」以下載Privacy Enhanced Mail(.pem檔案)並繼續下一步



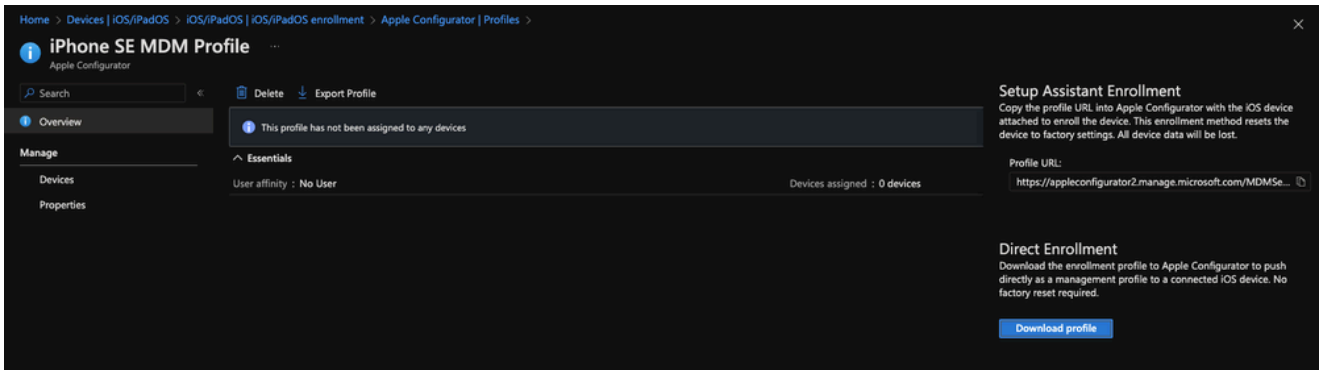
11752968667924

5. 輸入您用於登入Apple Push Certificates門戶的Apple ID帳戶的電子郵件地址，並上傳「Apple MDM推送證書」下的.pem檔案，然後按「上傳」。 如果上傳成功，您將看到「批次註冊方法」解鎖的其他選項。



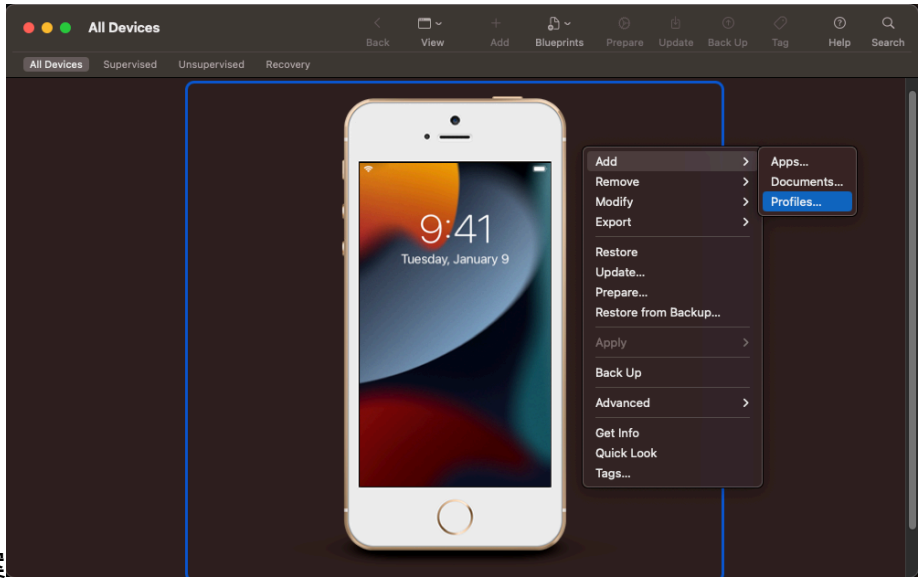
11752971407380

6. 轉到Apple Configurator —> Profiles —> Create並建立新的配置檔案。為其指定一個有意義的名稱，對於User affinity，請選擇「Enroll without user affinity」。 建立配置檔案後，按一下新建立的配置檔案，選擇右側的「Export Profile」（匯出配置檔案）和「Download Profile」（下載配置檔案）



11753020728596

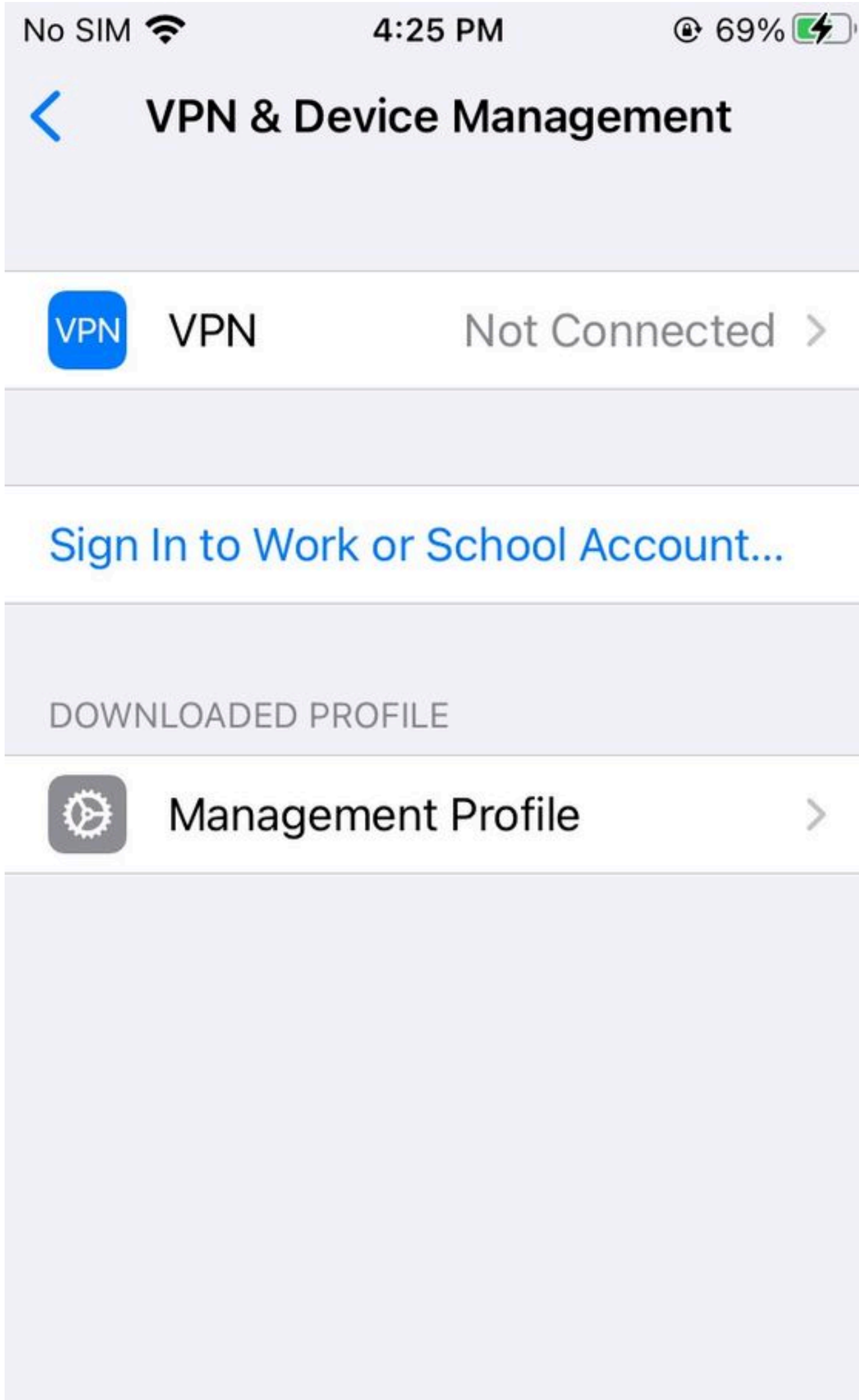
7. 從App Store下載並啟動macOS上的「Apple Configurator」，然後通過Lightning Cable連線手機。在Apple Configurator中按一下右鍵您的裝置，選擇Add —> Profiles，然後選擇您剛剛下載的profile.mobileconfig檔案

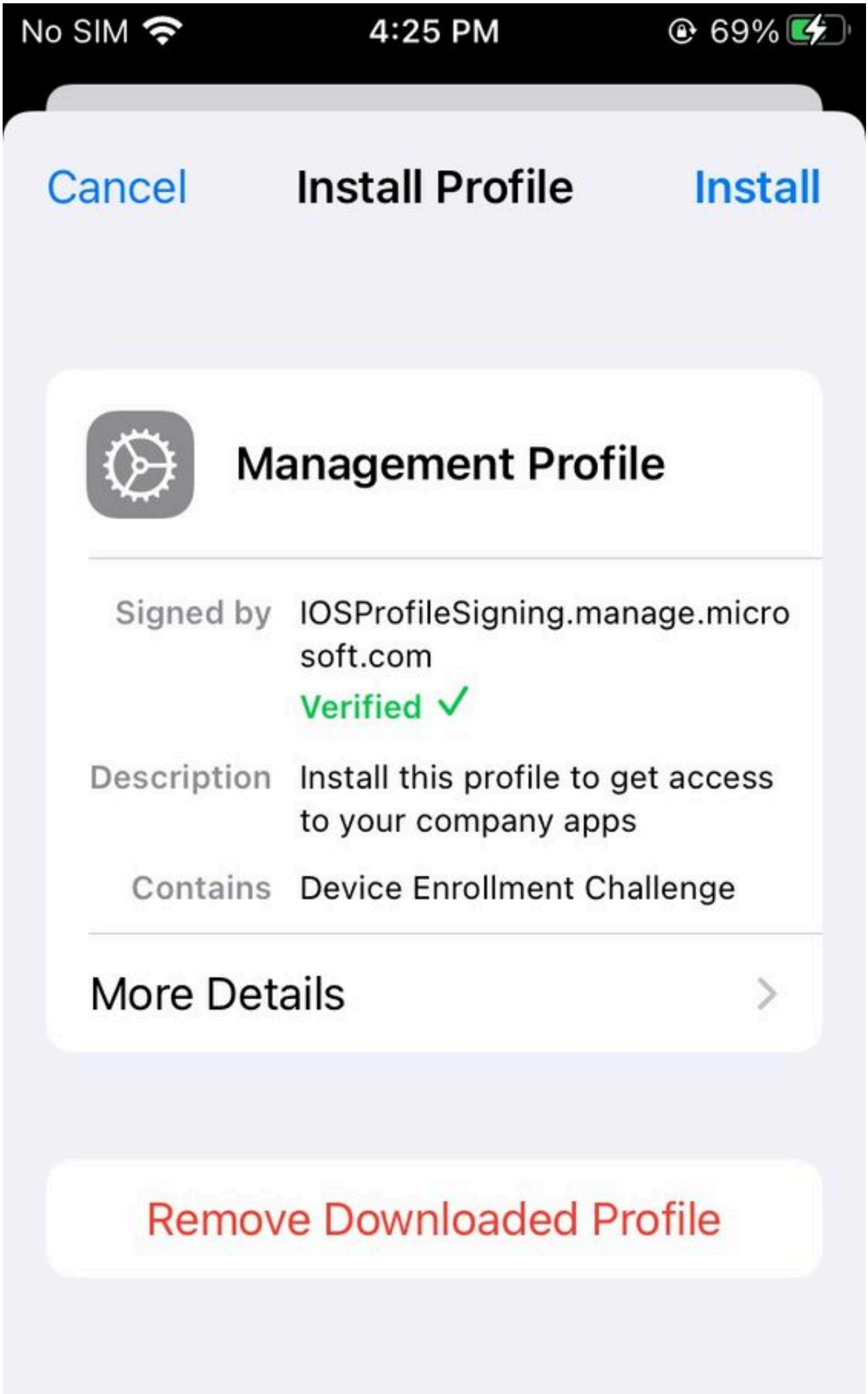


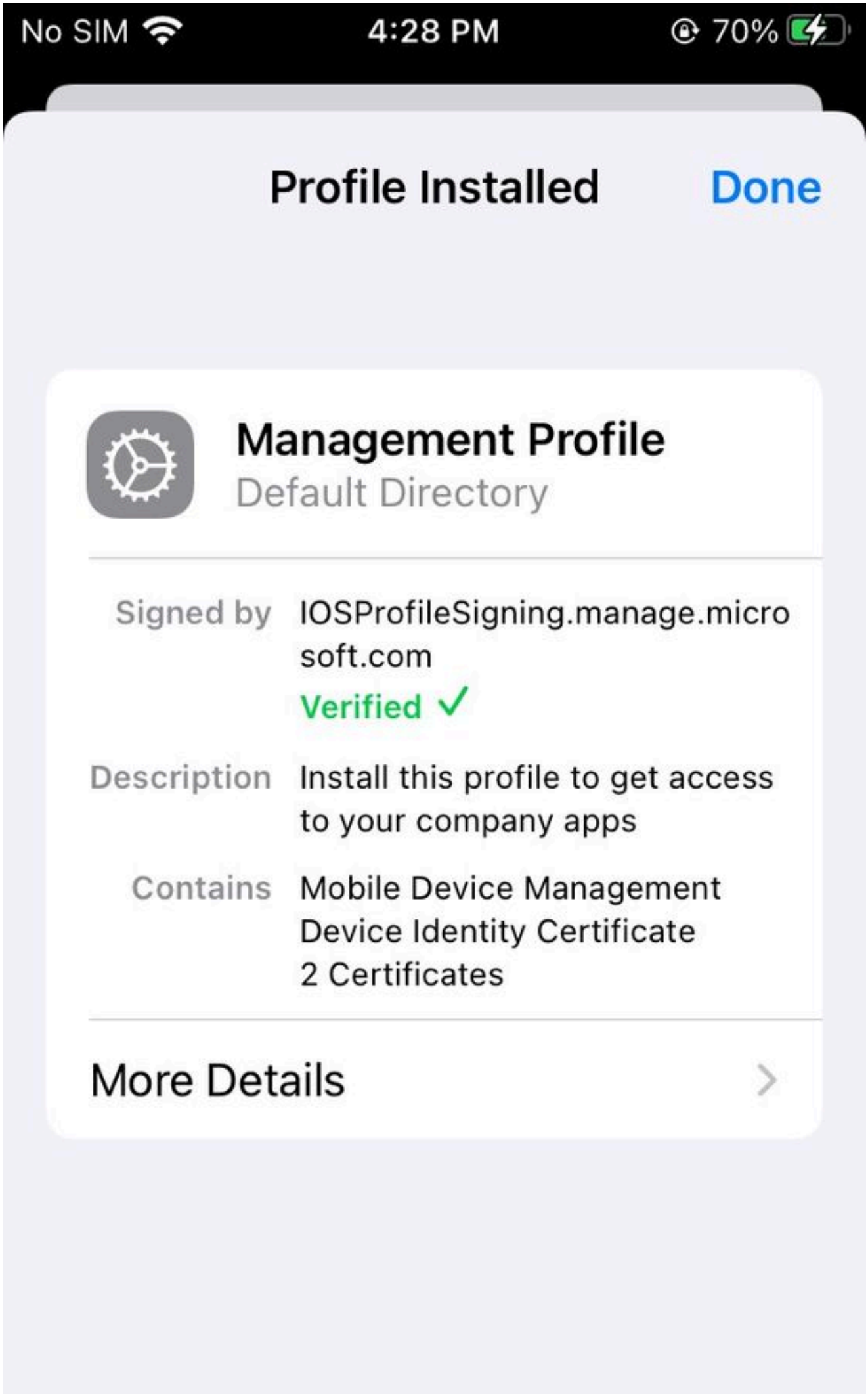
11753024446100

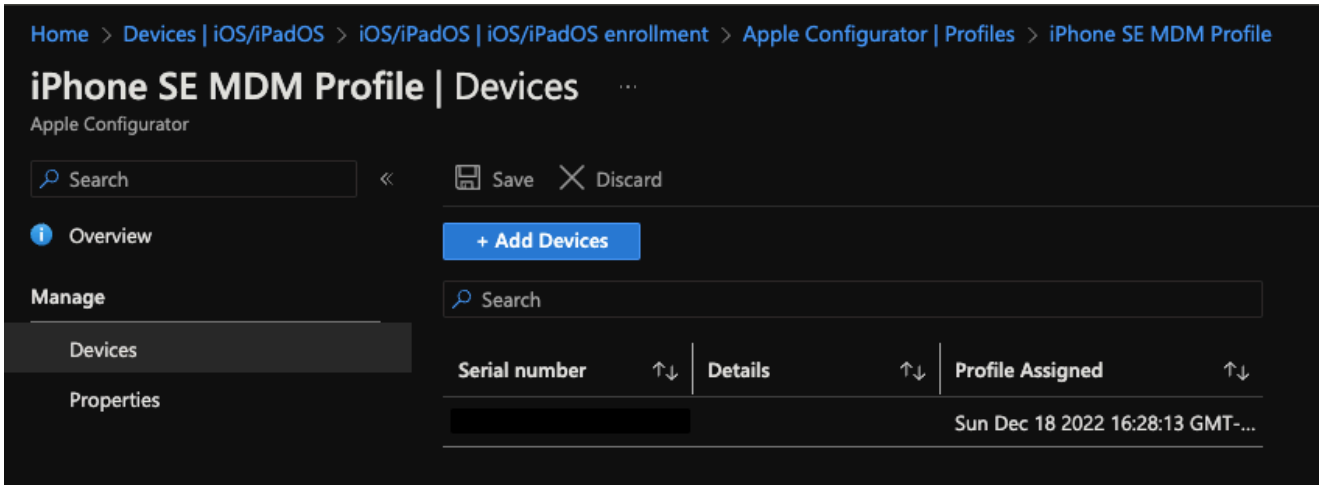
Windows備用：iPhone配置實用程式

8. 同步完成後，在您的iOS/iPadOS裝置上，轉到Settings應用，然後轉到General —> VPN & Device Management —> 管理配置檔案


No SIM
4:25 PM
69%
VPN & Device Management
VPN
VPN
Not Connected
Sign In to Work or School Account...
DOWNLOADED PROFILE
Management Profile

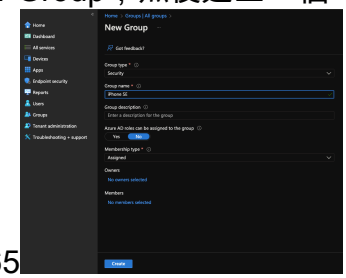

No SIM
4:25 PM
69%
Cancel
Install Profile
Install
Management Profile
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Device Enrollment Challenge
More Details
Remove Downloaded Profile


No SIM
4:28 PM
70%
Profile Installed
Done
Management Profile
Default Directory
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Mobile Device Management
Device Identity Certificate
2 Certificates
More Details



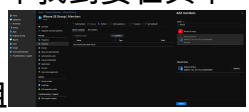
11753595983892

12. 現在，您的裝置已註冊MDM，請轉到Groups —> All Groups —> New Group，然後建立一個新組並分配您的裝置。確保您的組型別是「安全」而不是Microsoft 365



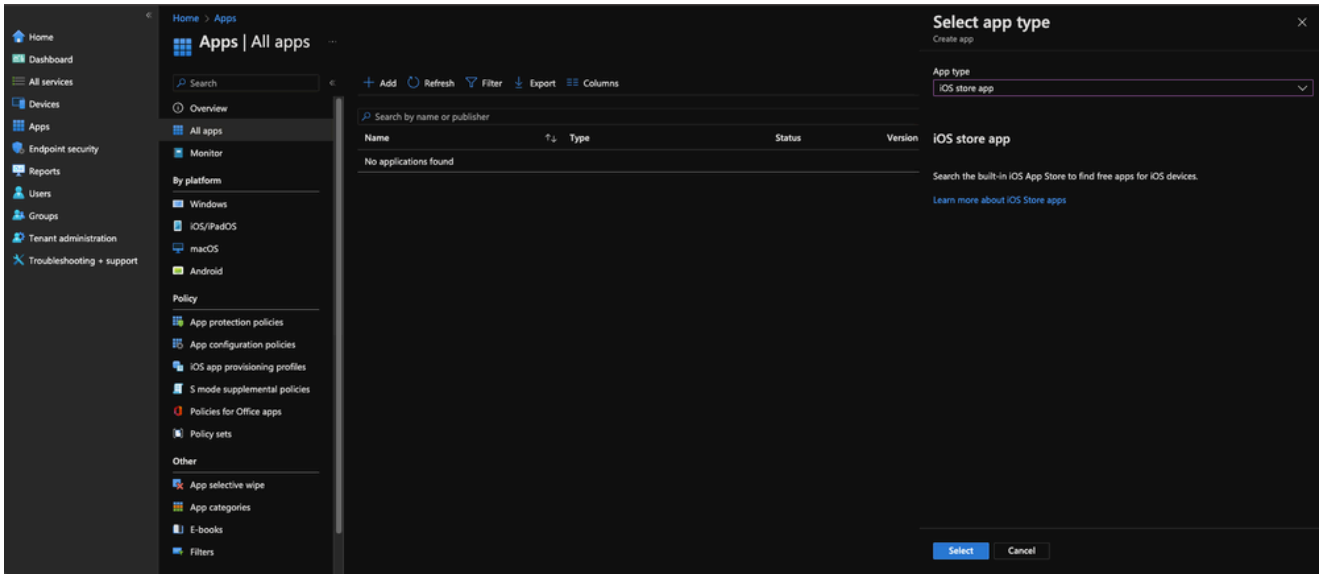
11753690347284

13. 按一下進入您剛剛建立的組，然後轉到Members —> Add Members。在清單中找到要在其中安裝Cisco Security Connector應用的MDM裝置，然後將其新增到剛建立的組



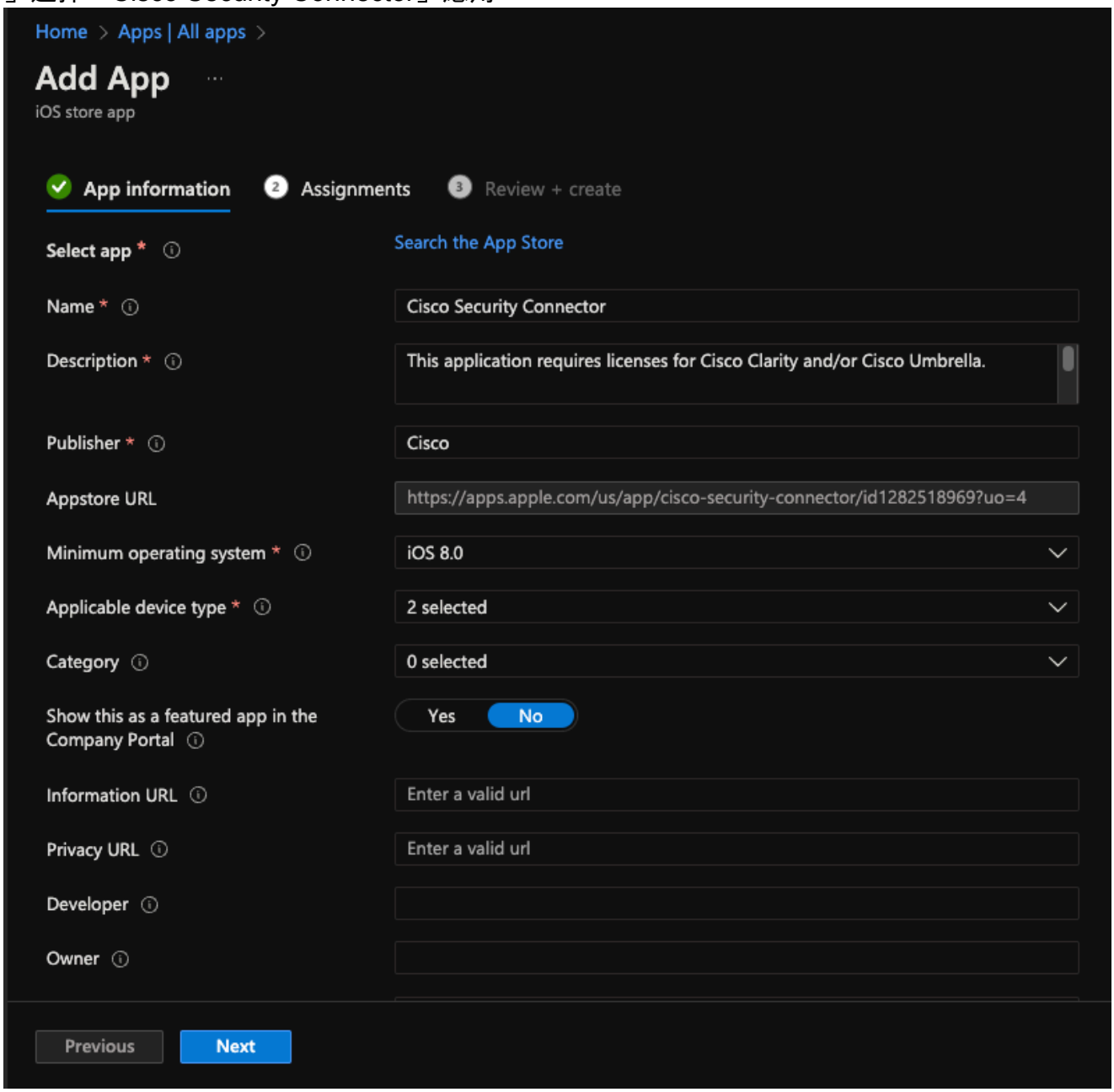
11753692550036

14. 轉到Apps —> All apps —> Add。然後，對於「應用型別」，選擇「iOS應用商店應用」，並按一下「選擇」進行確認



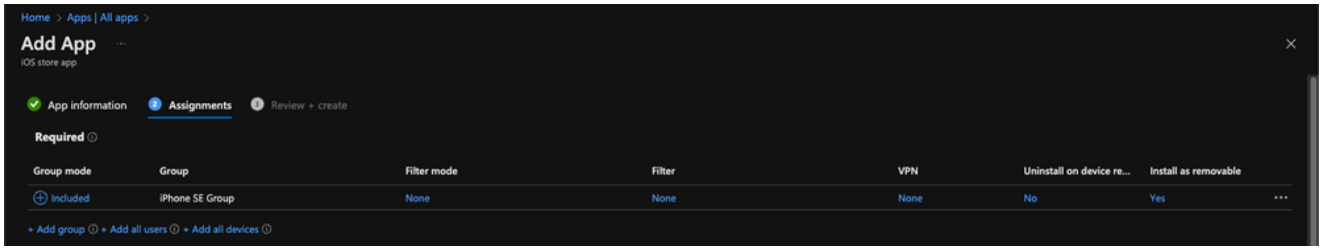
11753797372436

15. 選擇「搜尋App Store」並在搜尋欄中輸入「Cisco Security Connector」，然後按一下「選擇」選擇「Cisco Security Connector」應用



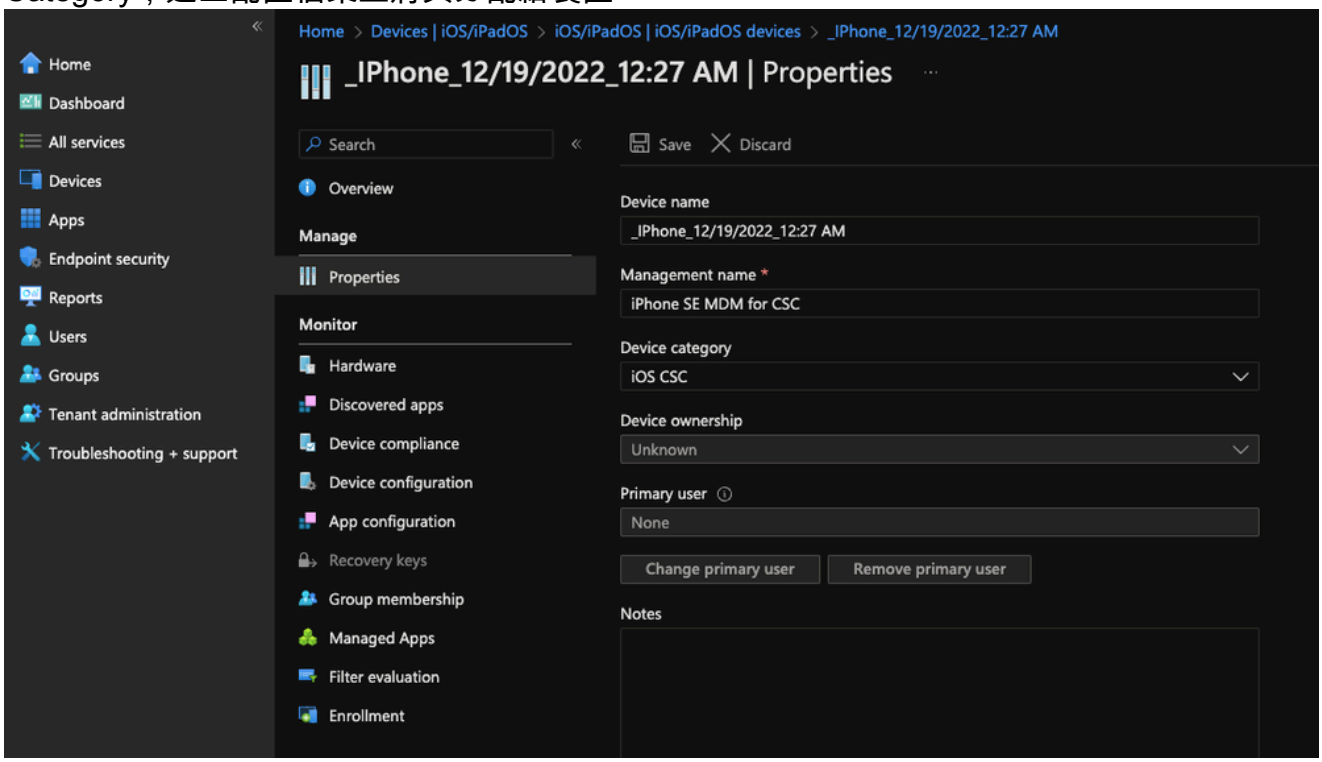
11753844054420

16. 在Assignments下，新增您在前面的步驟中建立的組，該組包含您的MDM裝置，然後繼續 審閱和建立



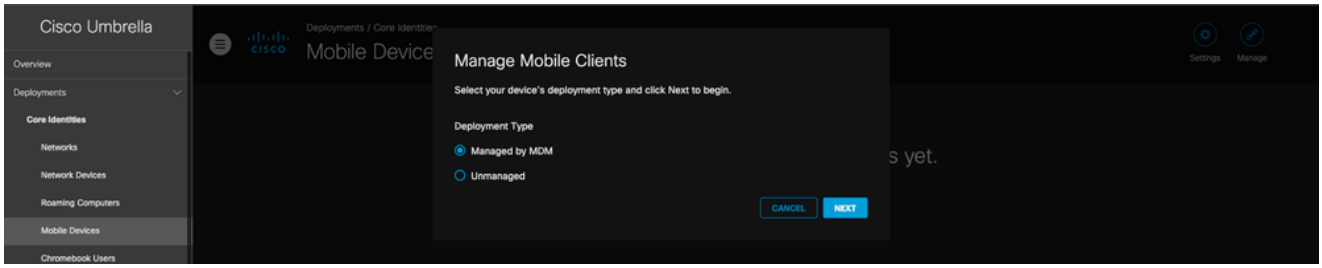
11753839516692

17. [可選步驟]轉到Devices —> iOS/iPadOS—> iOS/iPadOS裝置 —> Properties—> Device Category，建立配置檔案並將其分配給裝置



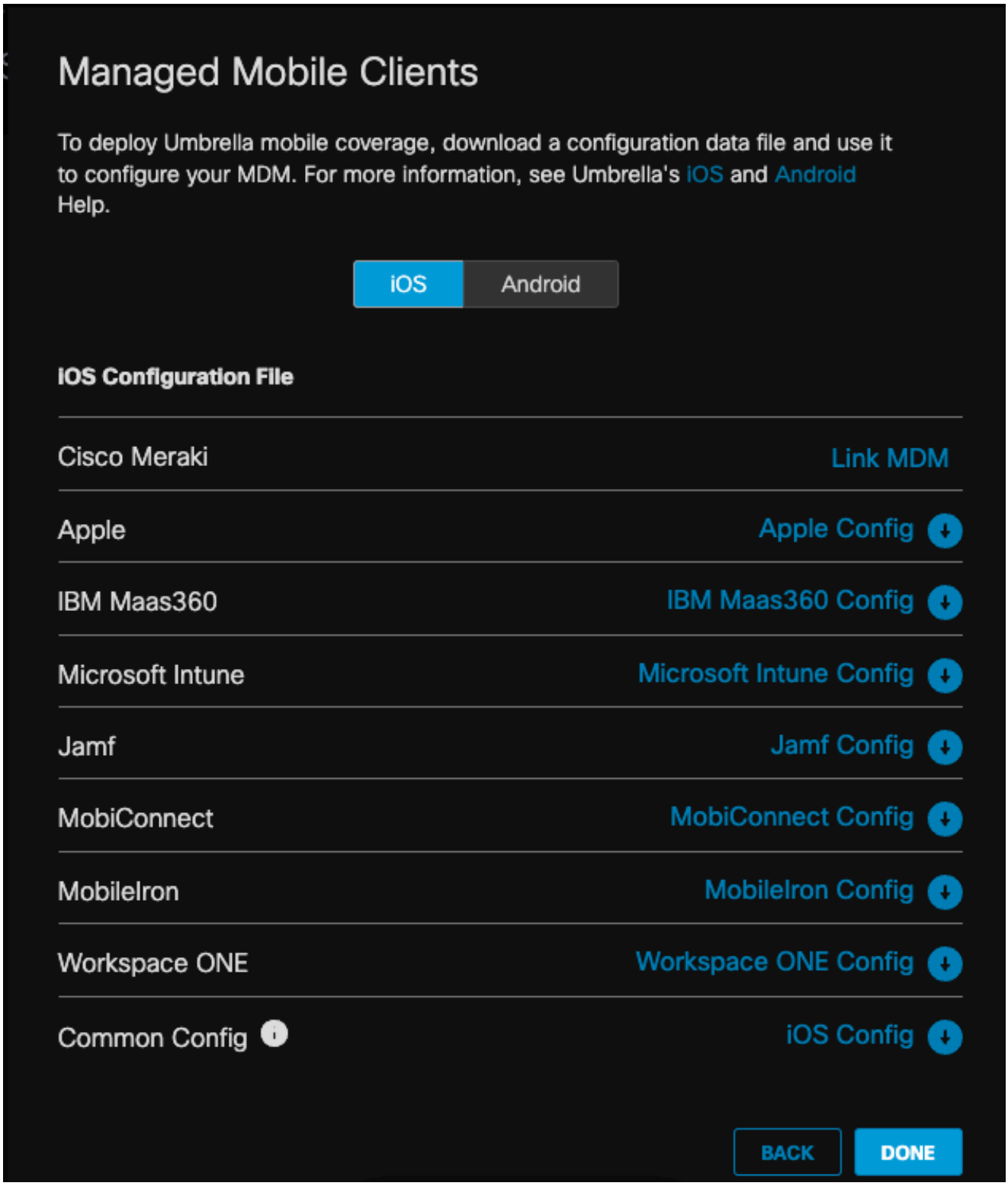
11753916236820

18. 在Deployments —> Core Identities —> Mobile Devices —>右上角登入您的Cisco Umbrella控制面板：管理 — > 由MDM管理



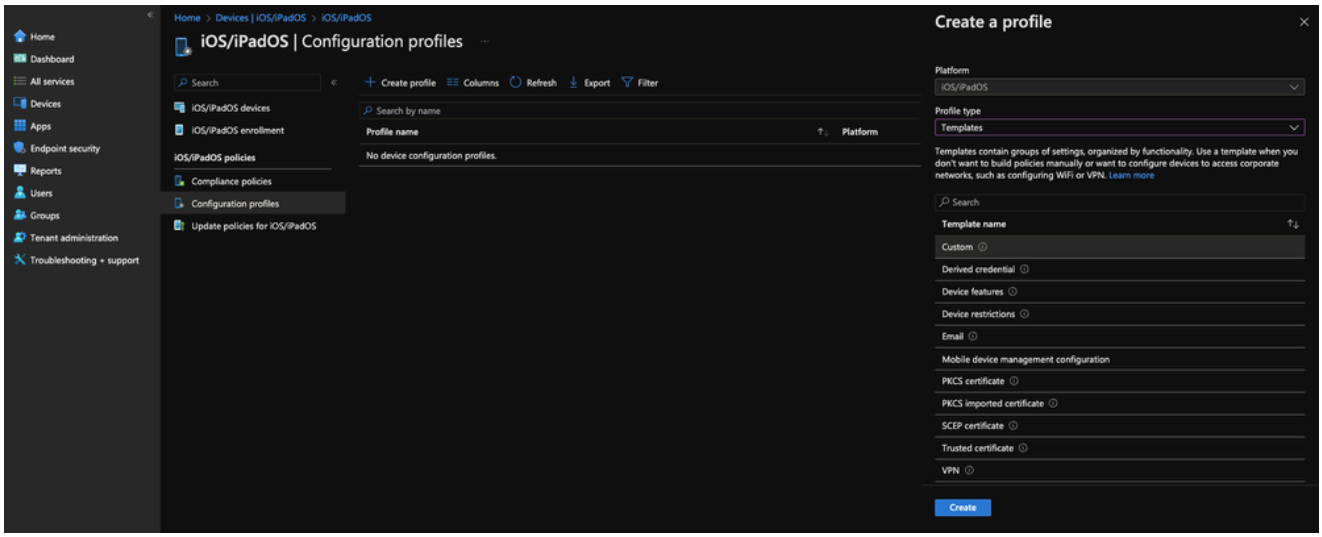
11753923081492

19. 然後轉到iOS —> Microsoft Intune Config download。輸入您希望在使用者在Cisco Security Connector應用中選擇「Report a problem」（報告問題）時電子郵件轉到到的電子郵件地址



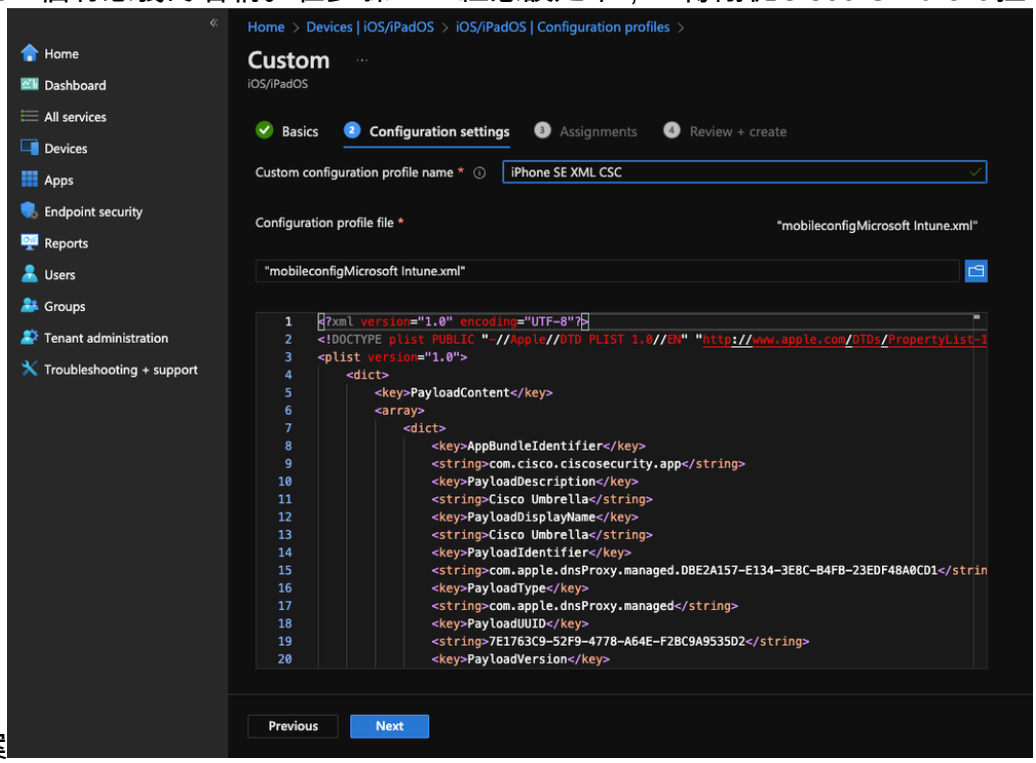
11753924523540

20. 返回您的Intune門戶，位於Devices —> iOS/iPadOS —> Configuration Profiles —> Create Profile —> Templates —> Custom下



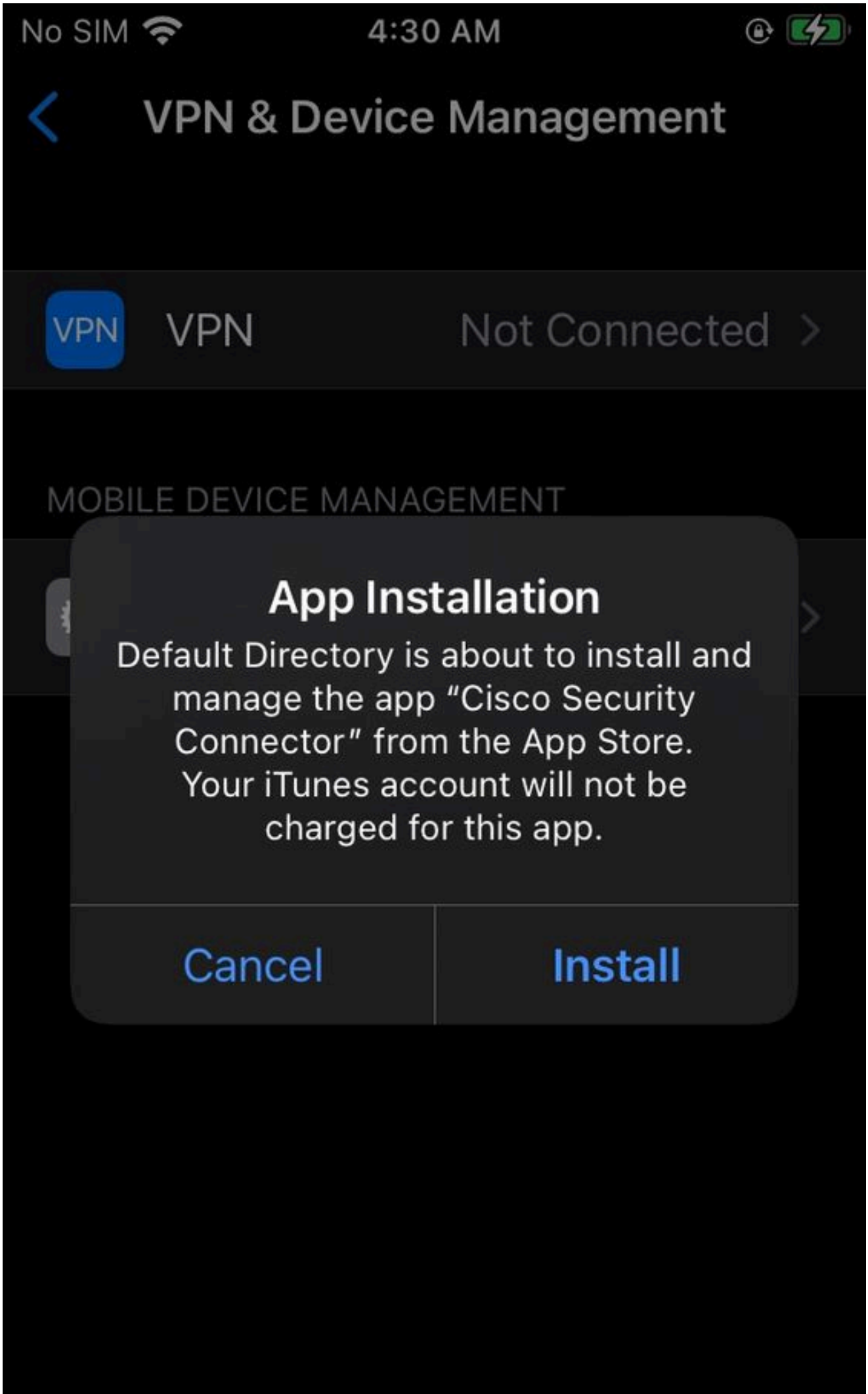
11753988354964

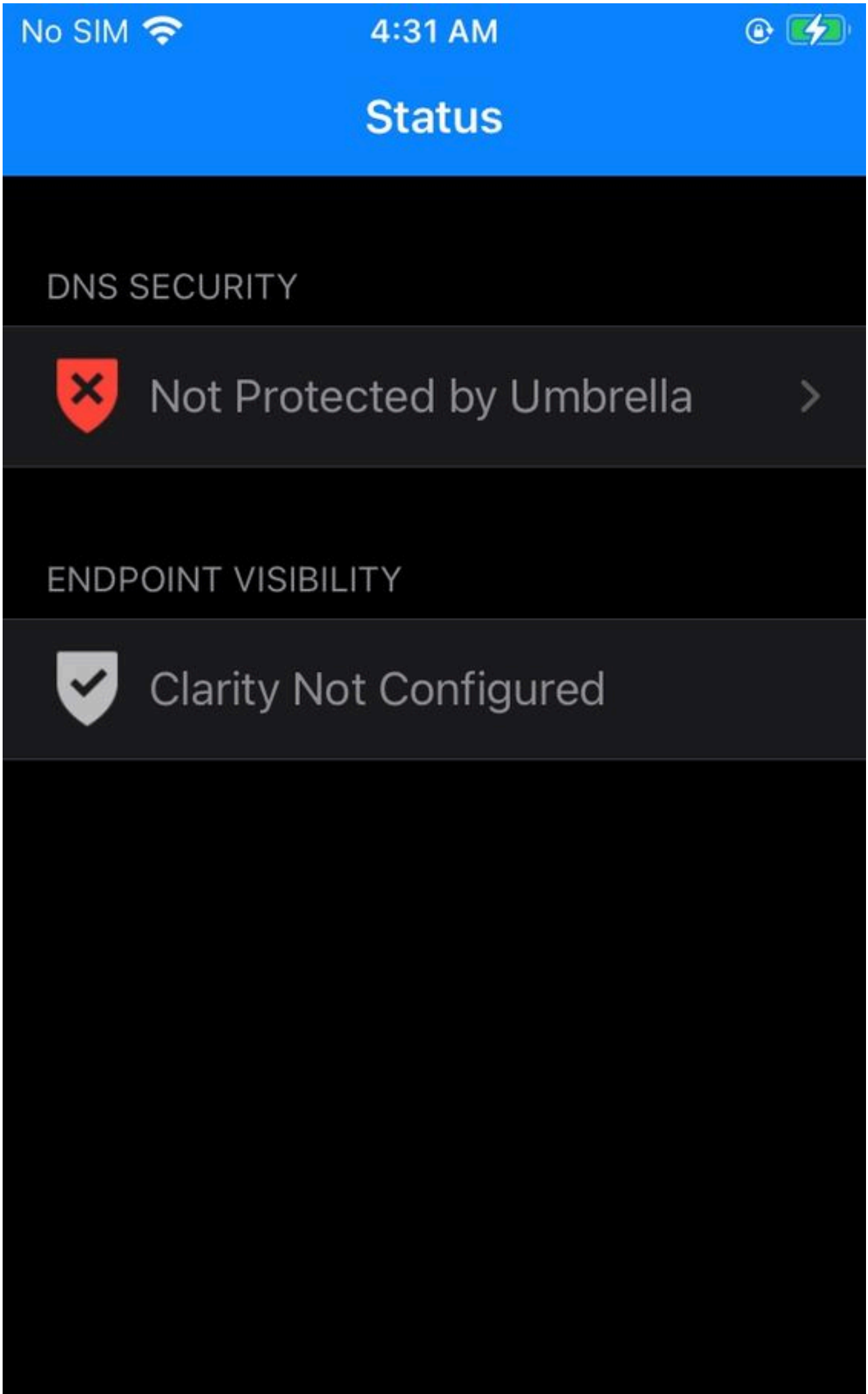
21. 為配置配置檔案指定一個有意義的名稱。在步驟2 — 組態設定中，上傳剛從Cisco Umbrella控制板下載的XML檔案

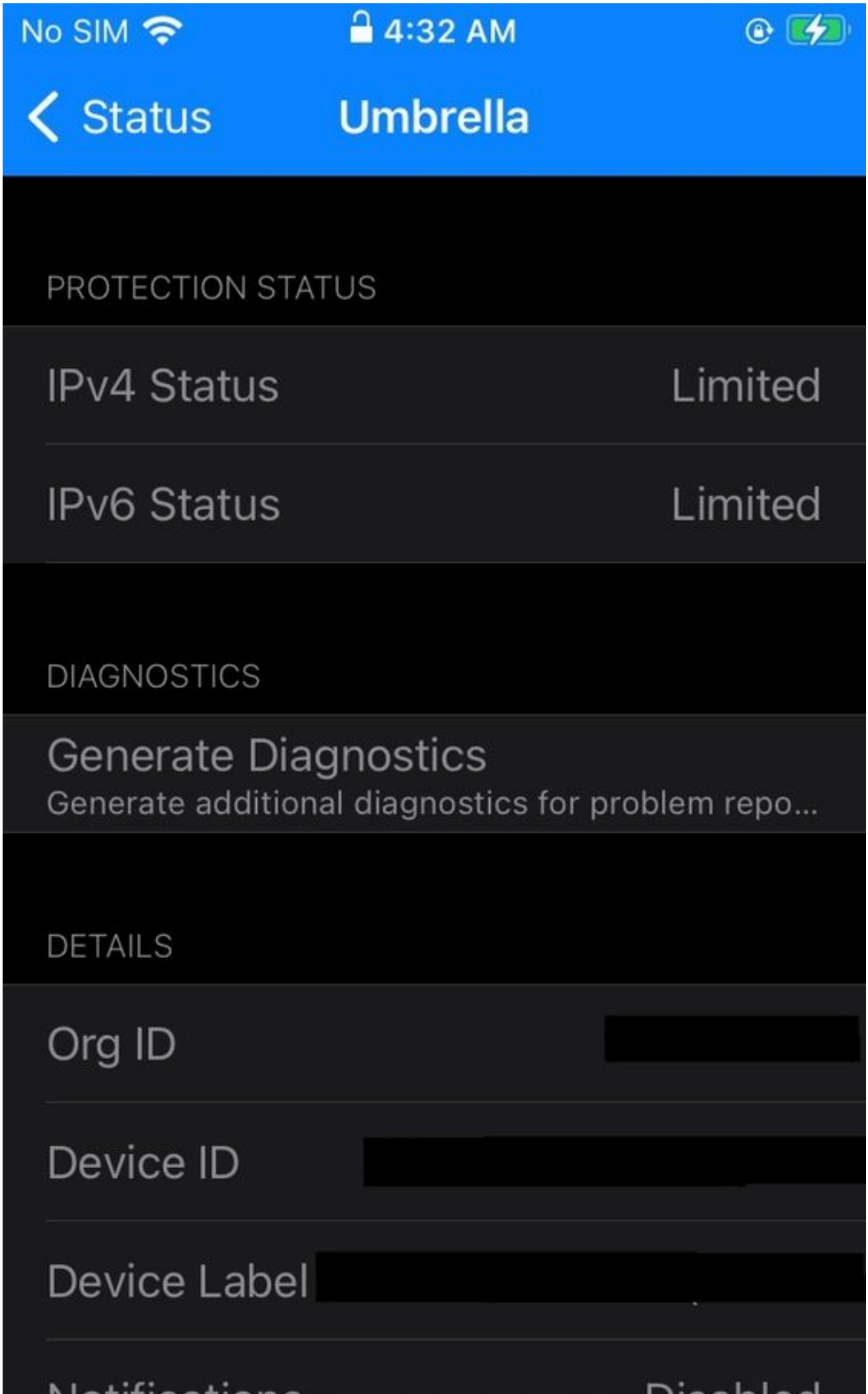


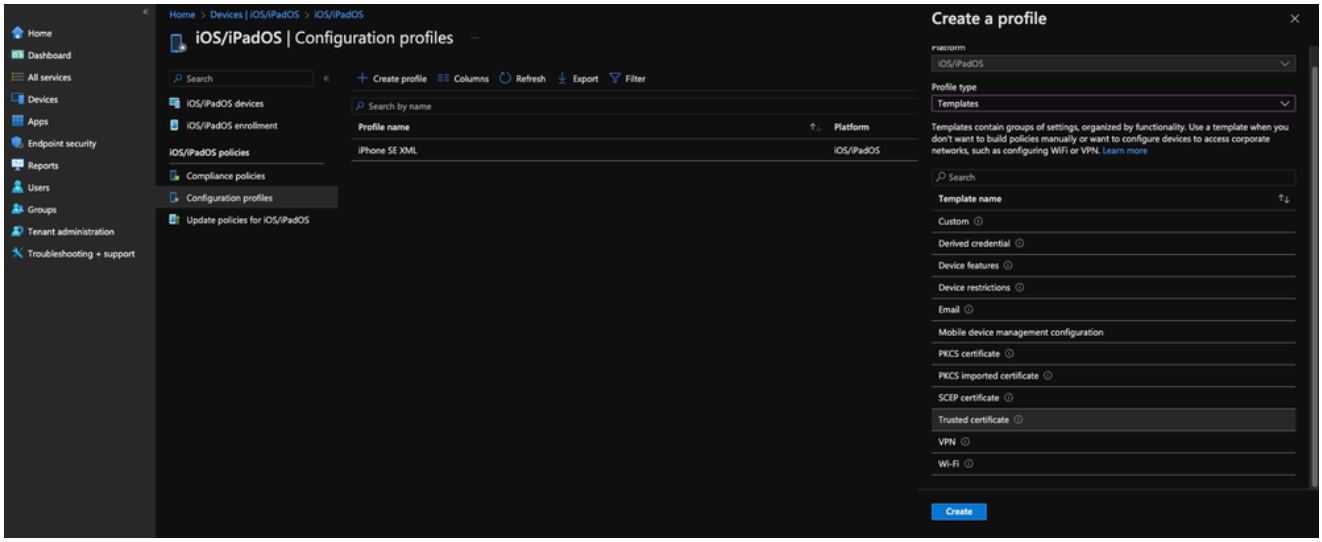
11754000962196

22. 在Assignments下，分配先前建立的包含MDM裝置的組，然後選擇「Review and Create」
23. 返回iOS/iPadOS裝置，選擇您的MDM裝置，並在頂部按一下「同步」，然後您將在MDM iOS/iPadOS裝置上彈出一個彈出視窗，以安裝Cisco Security Connector應用


No SIM
4:30 AM
VPN & Device Management
VPN
VPN
Not Connected
MOBILE DEVICE MANAGEMENT
App Installation
Default Directory is about to install and manage the app “Cisco Security Connector” from the App Store. Your iTunes account will not be charged for this app.
Cancel
Install

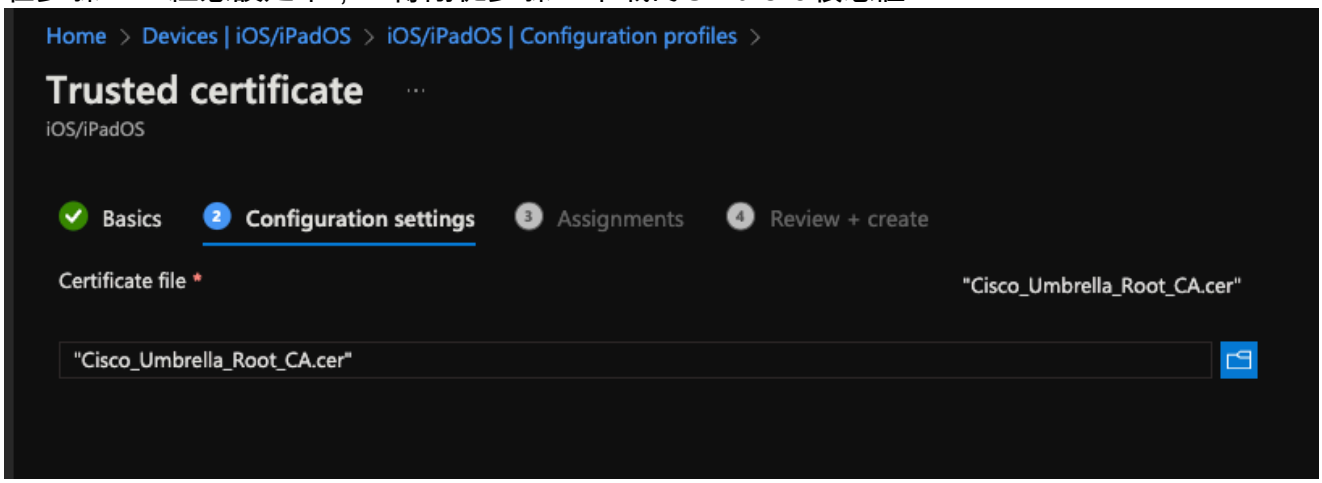

No SIM
4:31 AM
Status
DNS SECURITY
Not Protected by Umbrella
ENDPOINT VISIBILITY
Clarity Not Configured


No SIM
4:32 AM
Status
Umbrella
PROTECTION STATUS
IPv4 Status
Limited
IPv6 Status
Limited
DIAGNOSTICS
Generate Diagnostics
Generate additional diagnostics for problem repo...
DETAILS
Org ID
Device ID
Device Label



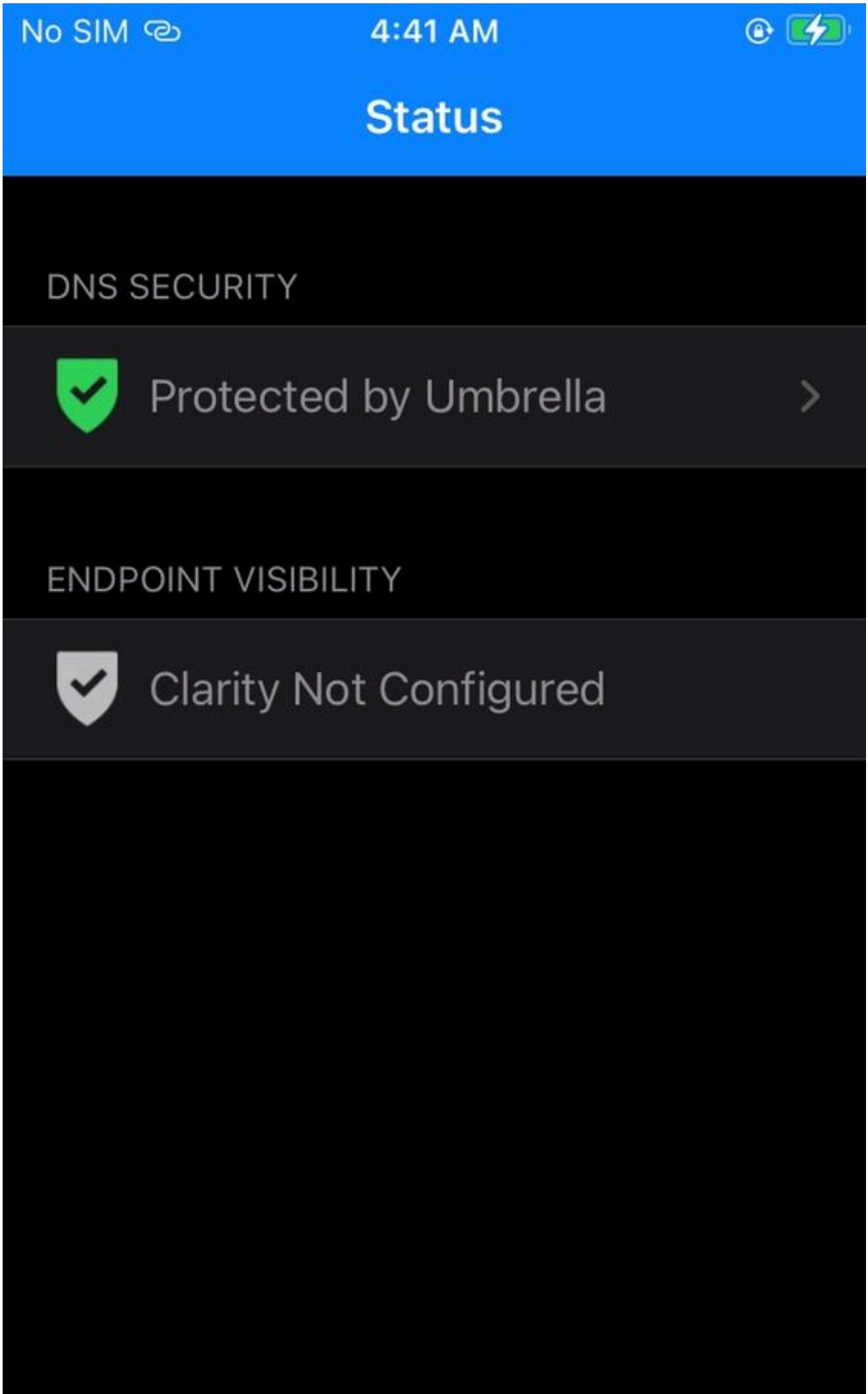
11754159037460

29. 在步驟2 — 組態設定中，上傳剛從步驟27下載的Umbrella根憑證



11754204605460

30. 對於第3步 — 分配，選擇包含您的MDM iOS/iPadOS裝置的組，然後按一下「下一步」和「建立」
31. 返回到iOS/iPadOS裝置並選擇您的MDM裝置，然後再次點選頂部同步（如步驟24）
32. 再次關閉並重新啟動思科安全聯結器應用。您現在看到的狀態是「Protected by Umbrella」


No SIM
4:41 AM
Status
DNS SECURITY
Protected by Umbrella
ENDPOINT VISIBILITY
Clarity Not Configured

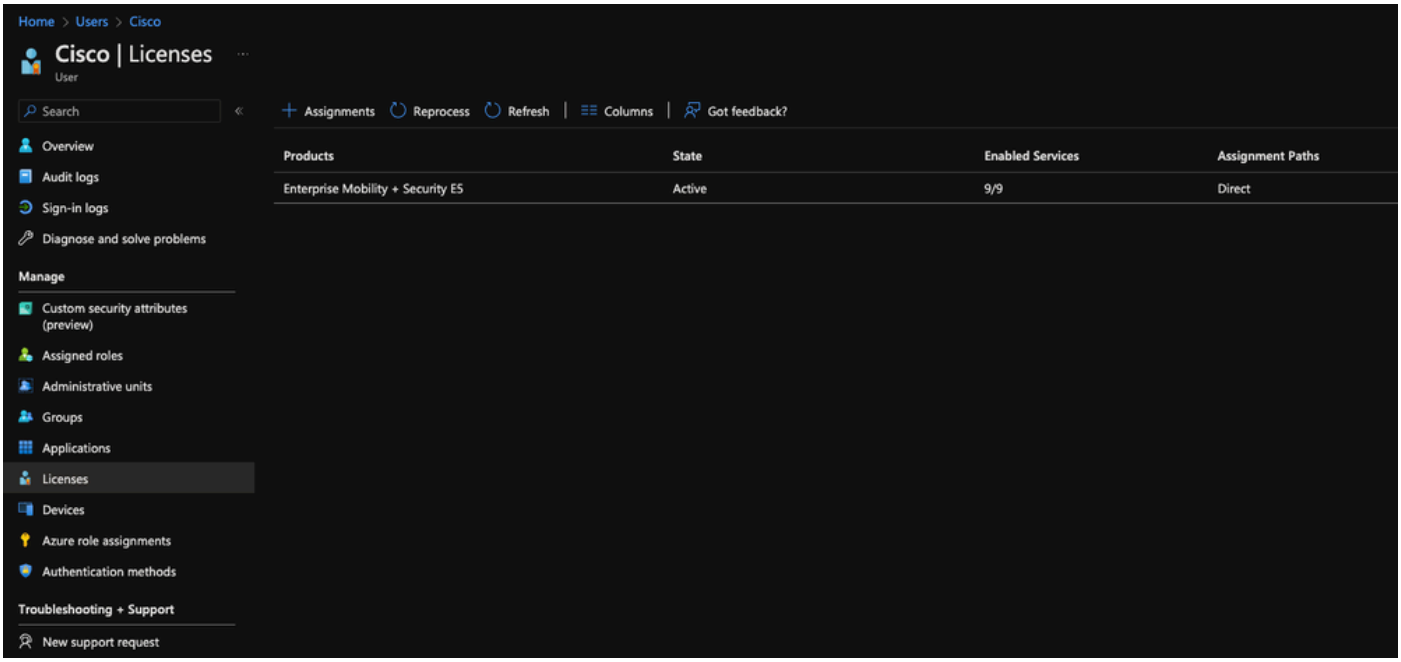

No SIM
4:48 AM
Cisco Umbrella
Welcome to Umbrella!
Your internet is faster, more reliable and better protected because you're using Cisco Umbrella.

裝置，並嘗試重新新增該裝置，則它不會填充在「成員」下面，以便您在步驟14中嘗試查詢「組」的裝置時。
- 您不能具有任何限制Umbrella應用的「受限應用」設定，和/或任何「顯示或隱藏」設定來隱藏在裝置配置配置檔案中應用的Umbrella應用。(在Intune管理中心>裝置> iOS/iPadOS >配置下)

疑難排解

- 如何收集思科安全聯結器診斷日誌
- CSC日誌「報告問題」功能「無管理員電子郵件」錯誤
- CSC:行動網路上的「未保護」狀態

如果您收到Error:「無法識別使用者名稱。此使用者無權使用Microsoft Intune」，請轉到Azure門戶的「使用者」下，選擇用於配置Intune的使用者名稱或帳戶，轉到「許可證」並確保已將有效的Intune許可證分配給該使用者



11754557401748

記錄檔

預設情況下，日誌密碼為bypass_email_filters。也可在UmbrellaProblemReport.txt中找到

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。