通過零接觸MDM在Android上部署具有保護傘保護的安全客戶端

目錄

簡介

本文檔介紹如何使用零接觸部署在Android裝置上使用Umbrella模組部署Cisco Secure Client。

背景資訊

您可以通過MDM解決方案（如Workspace One、Cisco Meraki或Microsoft Intune）使用零接觸部署在Android裝置上使用Umbrella模組部署Cisco Secure Client。此過程為應用和瀏覽器流量啟用無縫DNS層保護，確保啟用永遠線上VPN，並消除使用者對VPN和SEULA接受的干預。

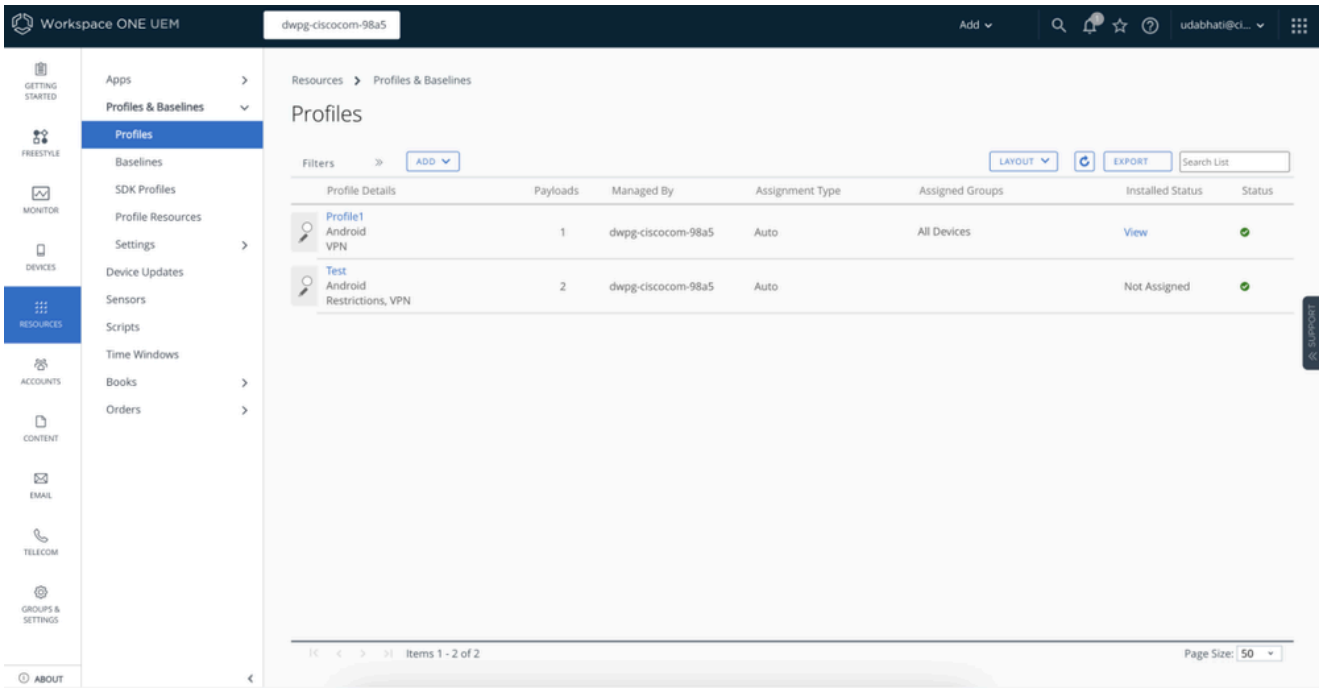
必要條件

- 通過建立工作配置檔案，完成Android企業移動管理(EMM)註冊和裝置註冊。
- MDM應用（中心）必須在工作配置檔案下可見。
- 僅在發佈和將Always On VPN配置檔案安裝到Intelligent Hub之後分配和安裝Cisco Secure Client。

部署步驟

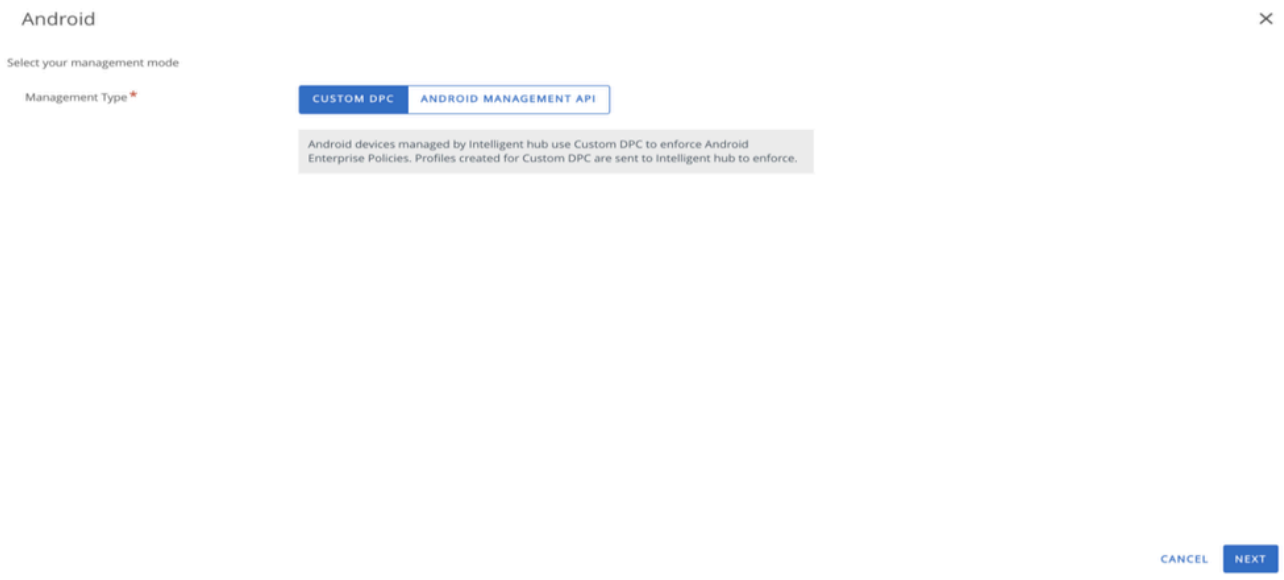
A.建立Always On VPN配置檔案

1. 導航至配置檔案：
    - 轉至資源>概要檔案和基線>概要檔案。
    - 按一下「新增」(Add)建立新配置檔案。

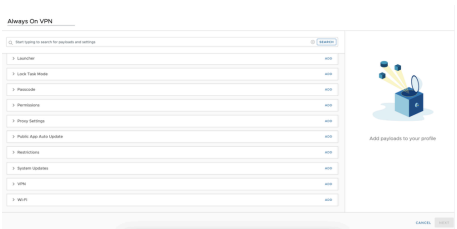


2. 配置檔案設定：

- 選擇Android作為平台。
- 選擇requiredManagement Type。



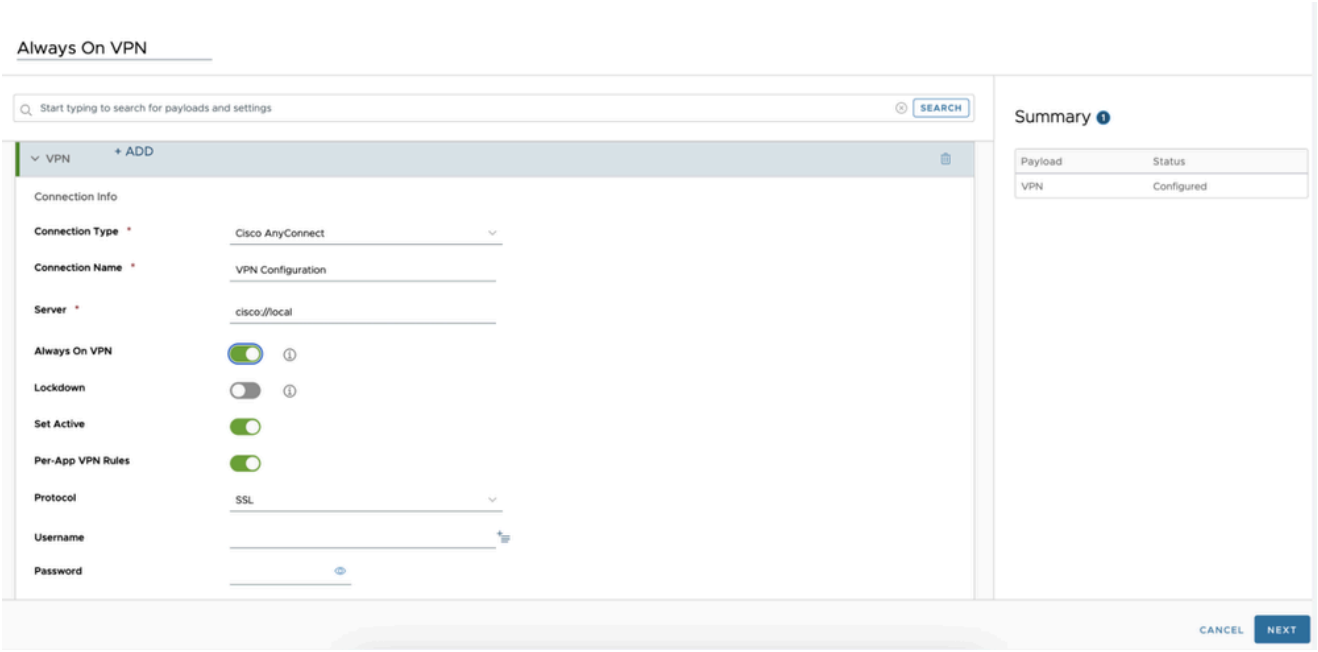
3. 配置VPN設定：



- 在profile部分中，轉至VPN Settings，然後按一下Add。
- 填寫必填欄位：
  - 連線型別:Cisco AnyConnect

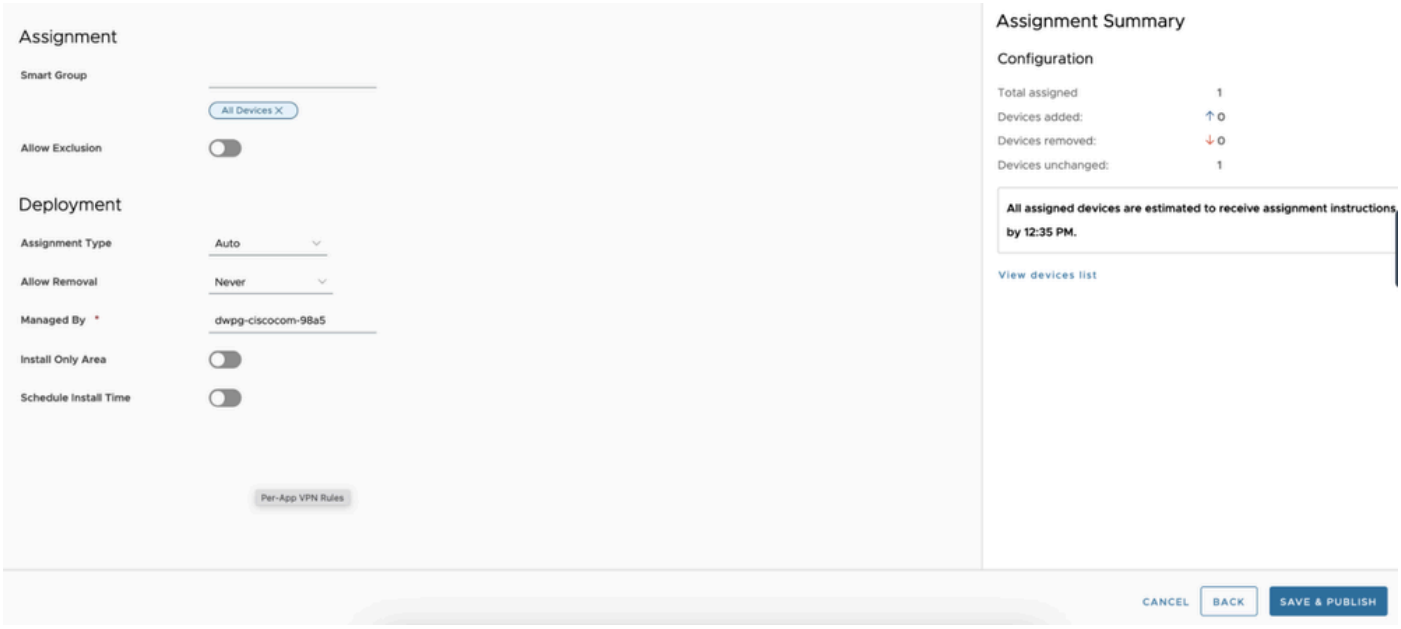
- 伺服器：cisco://local
- 啟用Always On VPN並根據需要配置其他屬性。
- EnablePer-App VPN規則。
- EnableSet Active。

- 按一下「下一步」。



4. 分配配置檔案：

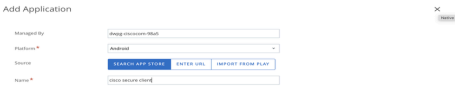
- 將智慧組留空。
- 將配置檔案分配到必要的裝置。
- 選擇部署值。
- 按一下「儲存並發佈」(Save & Publish)。



B.分配思科安全客戶端應用

1. 新增應用：

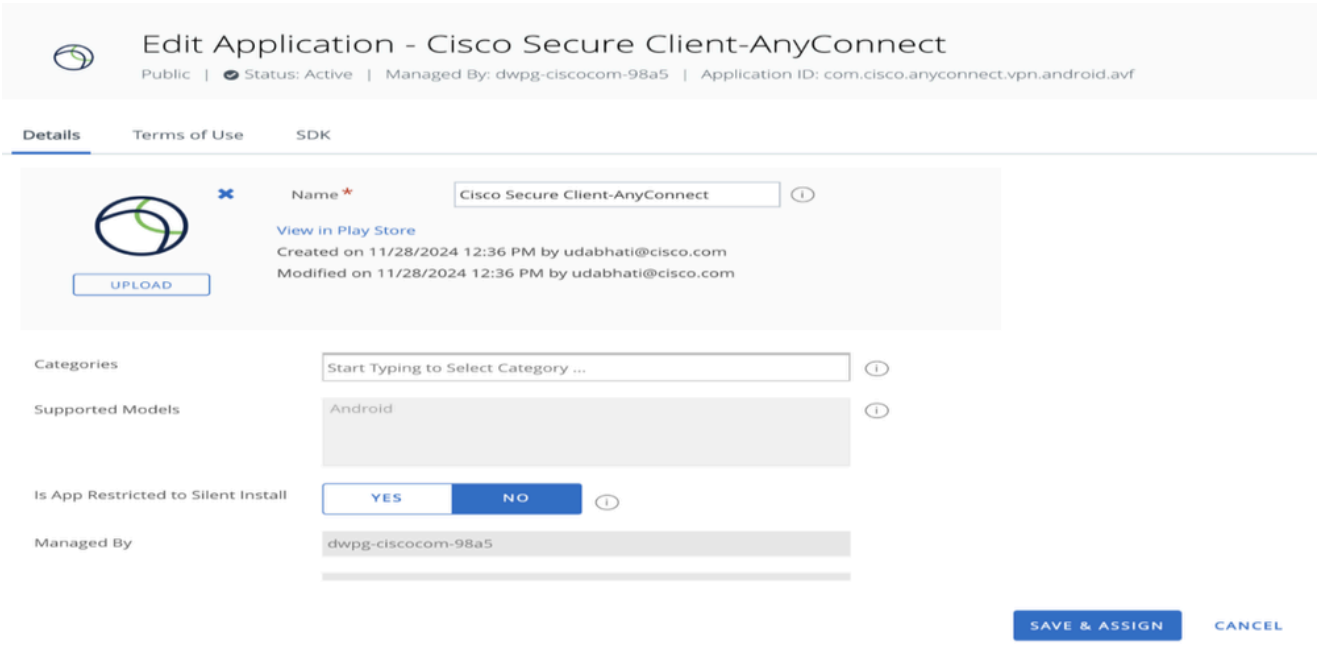
- 轉至Resources > Native > Public。



- 從Play Store新增Cisco安全客戶端（如果尚不可用）。

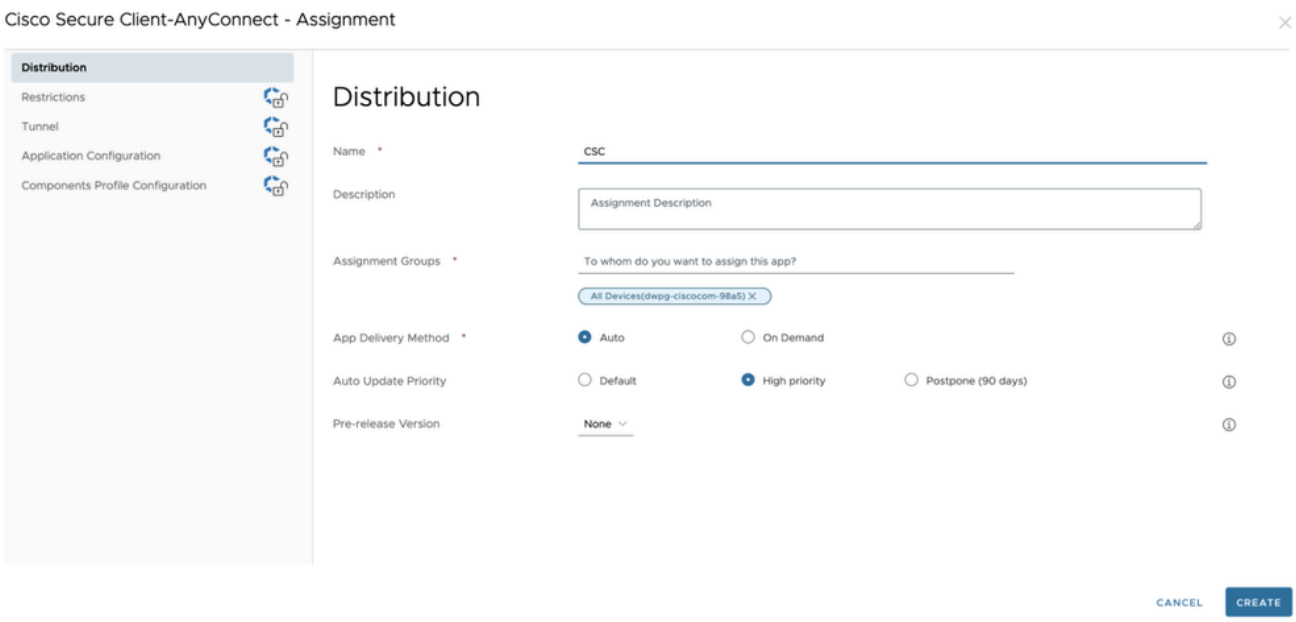
2. 應用程式分配：

- 選擇應用程式並填寫所需的值。
- 在assignment部分，建立新分配。



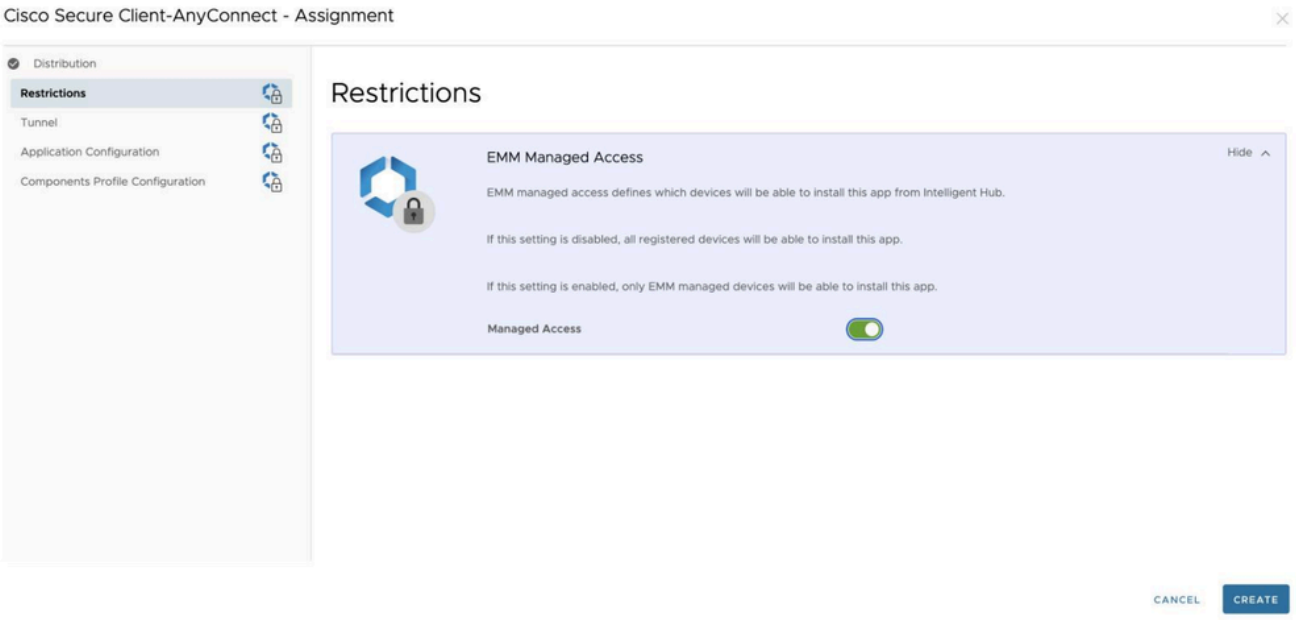
3. 配置分發：

- 在Distribution部分輸入詳細資訊。



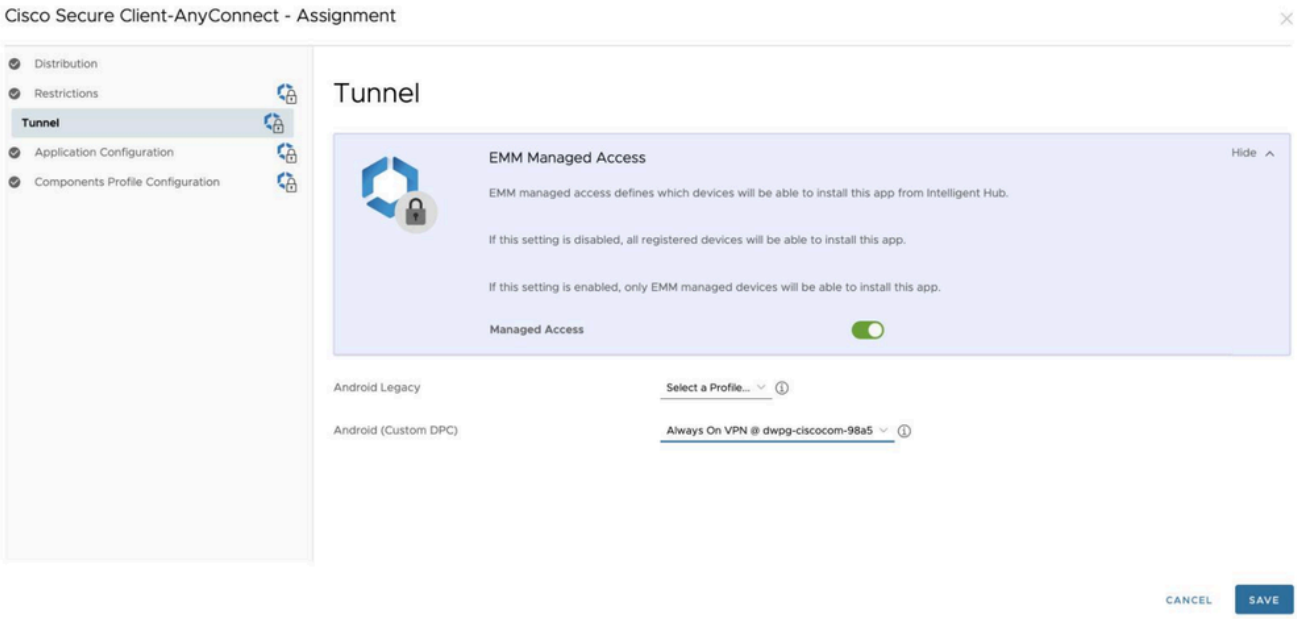
4. 啟用託管訪問：

- 在Restrictionstab中，enableManaged Access。



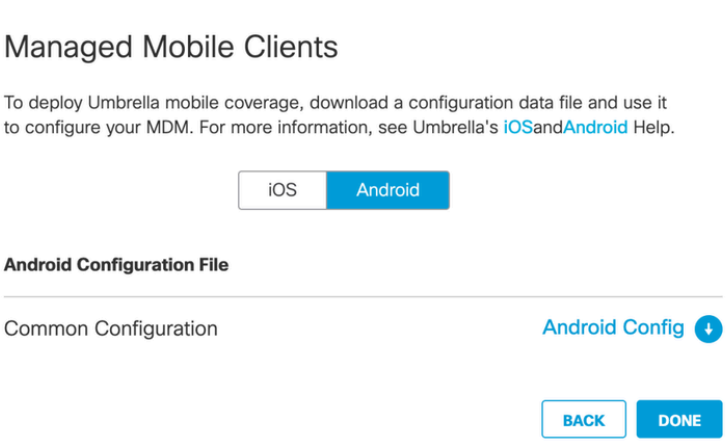
5. 選擇配置檔案：

- 在Tunneloption中，在Android（自定義DPC）下選擇以前建立的配置檔案(「Always On VPN」)。

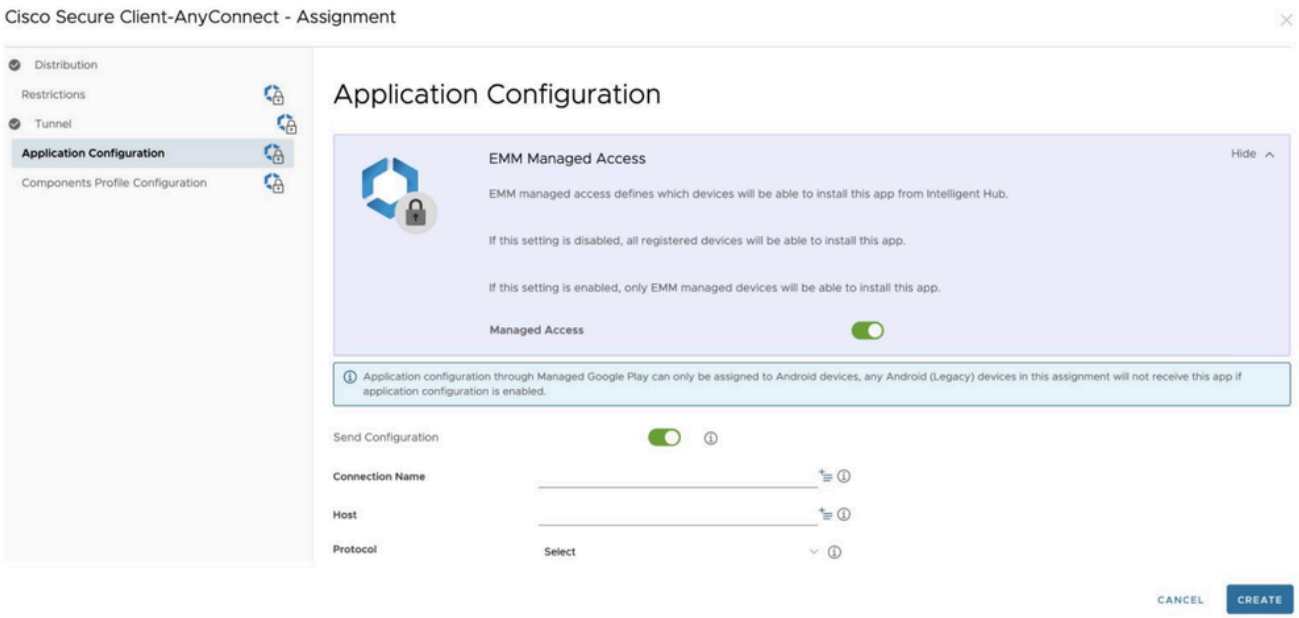


6. 應用程式配置：

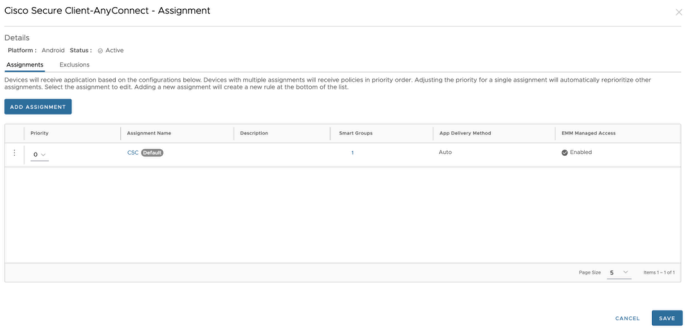
- 從從Umbrella控制面板下載的Android配置檔案輸入應用程式配置詳細資訊，如Org ID和



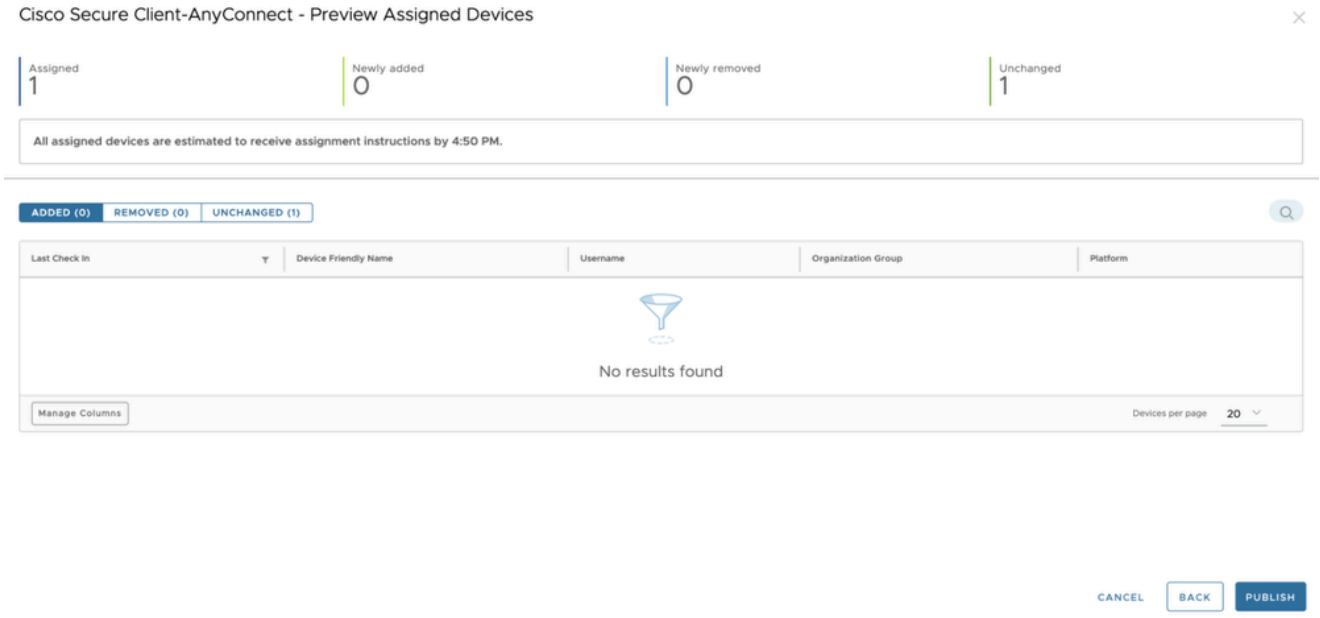
  RegTokend。
- 啟用接受SEULA以使使用者繞過手動接受SEULA。
- 啟用始終在VPN模式以進行Umbrella保護，僅用於思科安全客戶端的無縫VPN管理。
- 阻止使用者建立新的VPN連線（將Host欄位留空）。



7. 儲存並發佈：



- 儲存更改並發佈思科安全客戶端應用。



8. 推送Umbrella證書：

- 有關說明，請參閱：[將Umbrella證書推送到裝置]

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）。