ゼロタッチMDM経由でAndroid上にUmbrella Protectionを備えたセキュアクライアントを導入

内容

はじめに

このドキュメントでは、ゼロタッチ導入を使用してAndroidデバイスにCisco Secure ClientとUmbrellaモジュールを導入する方法について説明します。

背景説明

Workspace One、Cisco Meraki、Microsoft IntuneなどのMDMソリューションによるゼロタッチ導入を使用して、AndroidデバイスにCisco Secure ClientとUmbrellaモジュールを導入できます。このプロセスにより、アプリケーションとブラウザトラフィックに対するシームレスなDNSレイヤ保護が可能になり、Always On VPNが有効になり、VPNとSEULA受け入れに関するユーザの介入が不要になります。

前提条件

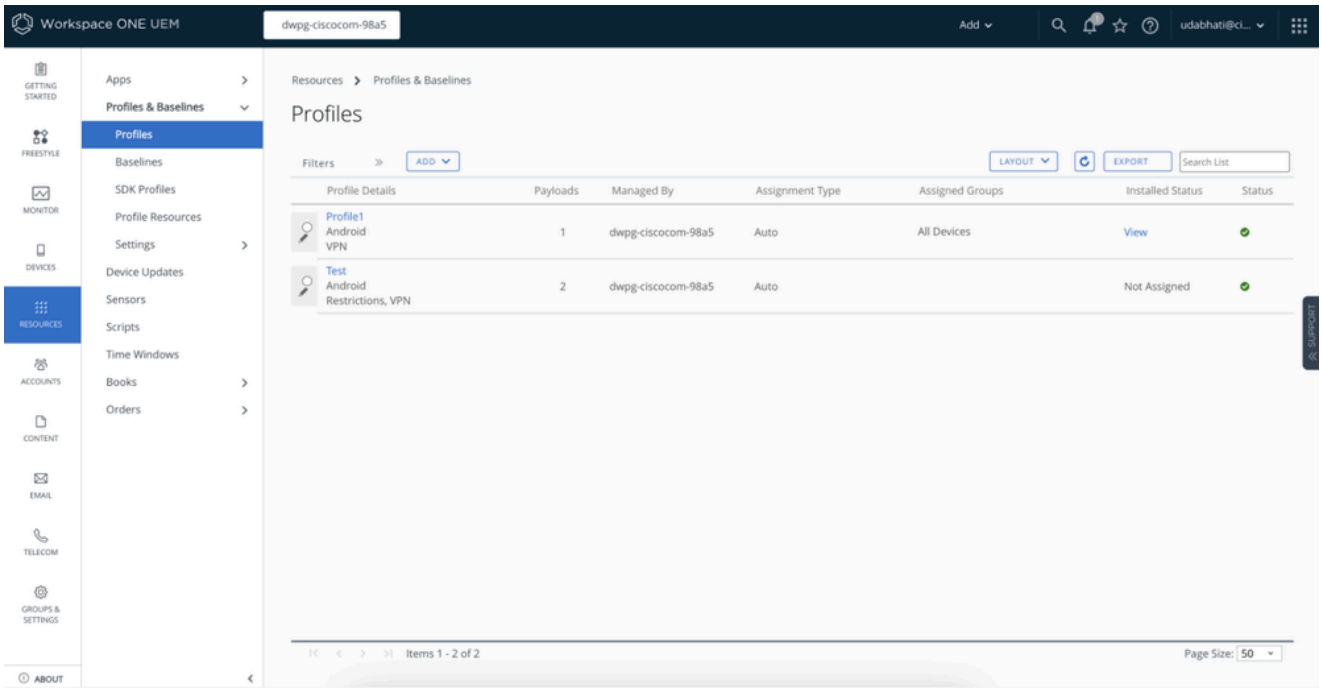
- Android Enterprise Mobility Management(EMM)の登録とデバイス登録を完了し、作業プロファイルを作成します。
- MDMアプリケーション(Hub)は、作業プロファイルの下に表示されている必要があります。
- Cisco Secure Clientの割り当てとインストールは、Always On VPNプロファイルをIntelligent Hubに公開してインストールした後に行ってください。

導入手順

A. Always On VPNプロファイルの作成

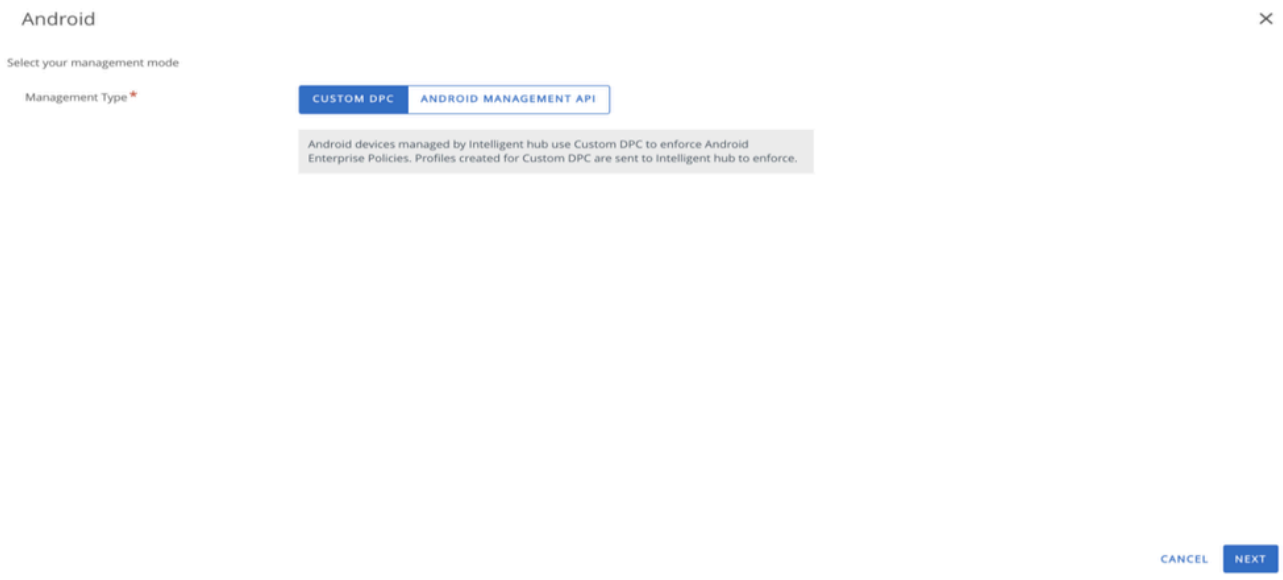
1. プロファイルに移動：

    - Resources > Profiles & Baselines > Profilesの順に選択します。
    - Addaddをクリックして、新しいプロファイルを作成します。

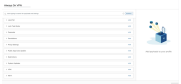


2. プロファイル設定：

- プラットフォームとしてAndroidasを選択します。
- requiredManagement Typeを選択します。

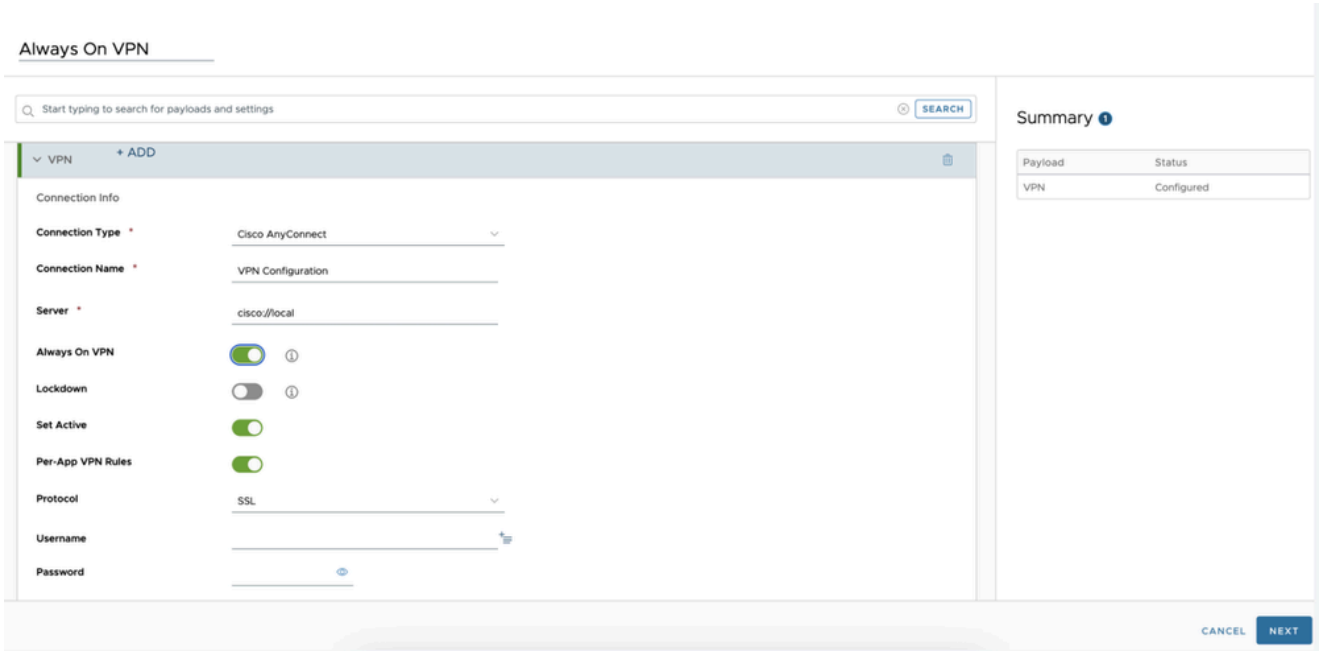


3. VPNの設定：



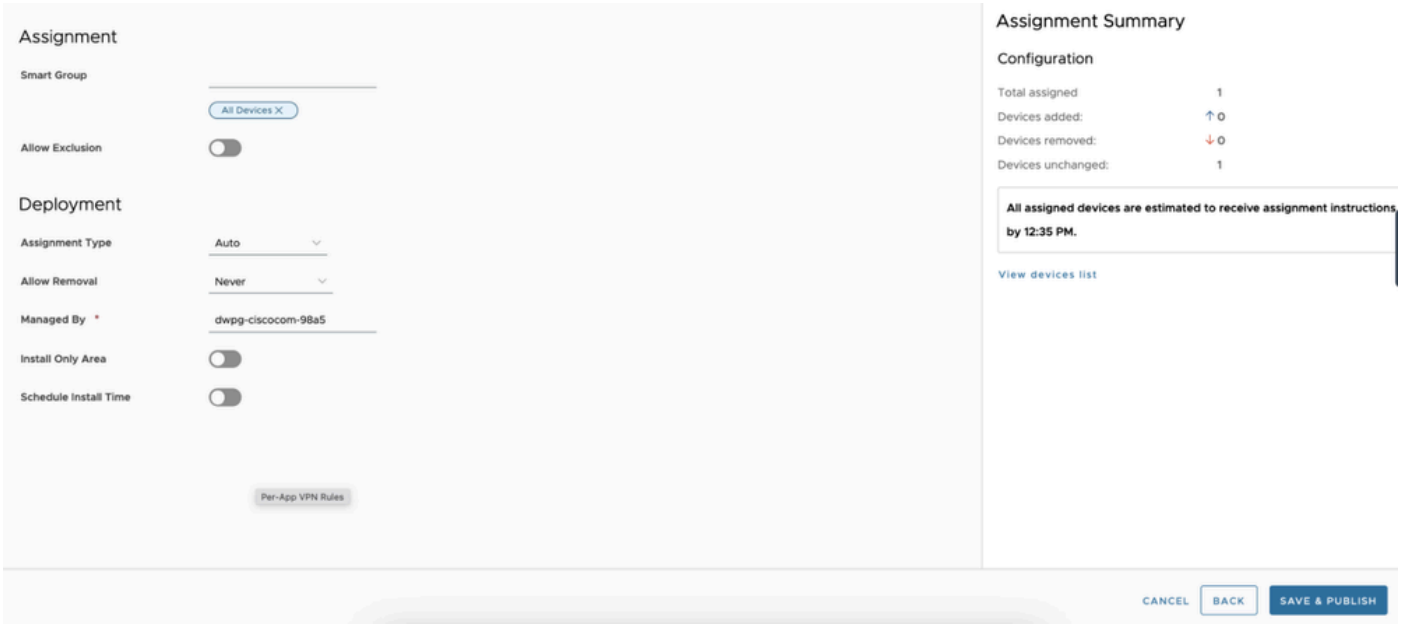
- プロファイルセクションで、VPN設定に移動し、追加をクリックします。
- 次の必須フィールドに入力します。
  - 接続タイプ：Cisco AnyConnect
  - サーバ：cisco://local
  - EnableAlways On VPN：必要に応じて、その他のプロパティを設定します。
  - EnablePer-App VPN Rules』を参照してください。
  - EnableSet Activeを発行します。

- Next をクリックします。



4. プロファイルの割り当て：

- スマートグループは空白のままにします。
- 必要なデバイスにプロファイルを割り当てます。
- 配置値を選択します。
- [保存してパブリッシュ]をクリックします。



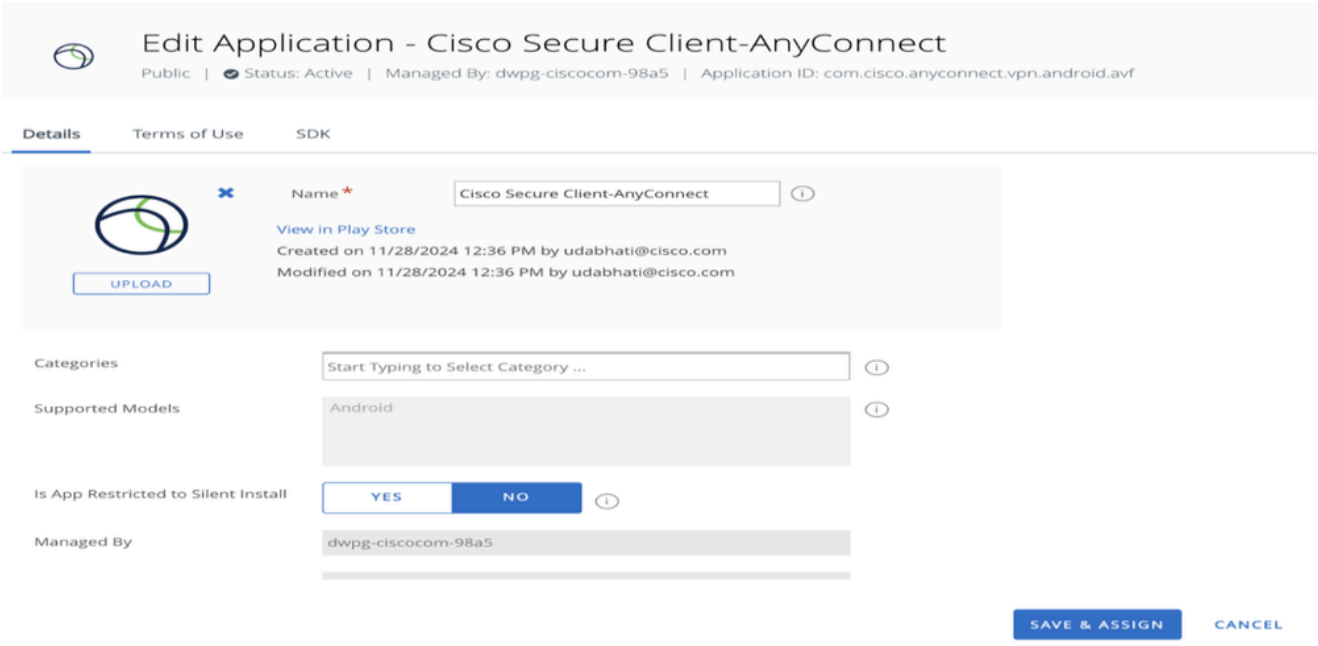
B. Cisco Secure Clientアプリケーションの割り当て

1. アプリを追加します。

- Resources > Native > Publicの順に選択します。
- Play StoreからCisco Secure Clientを追加します（まだ使用できない場合）。

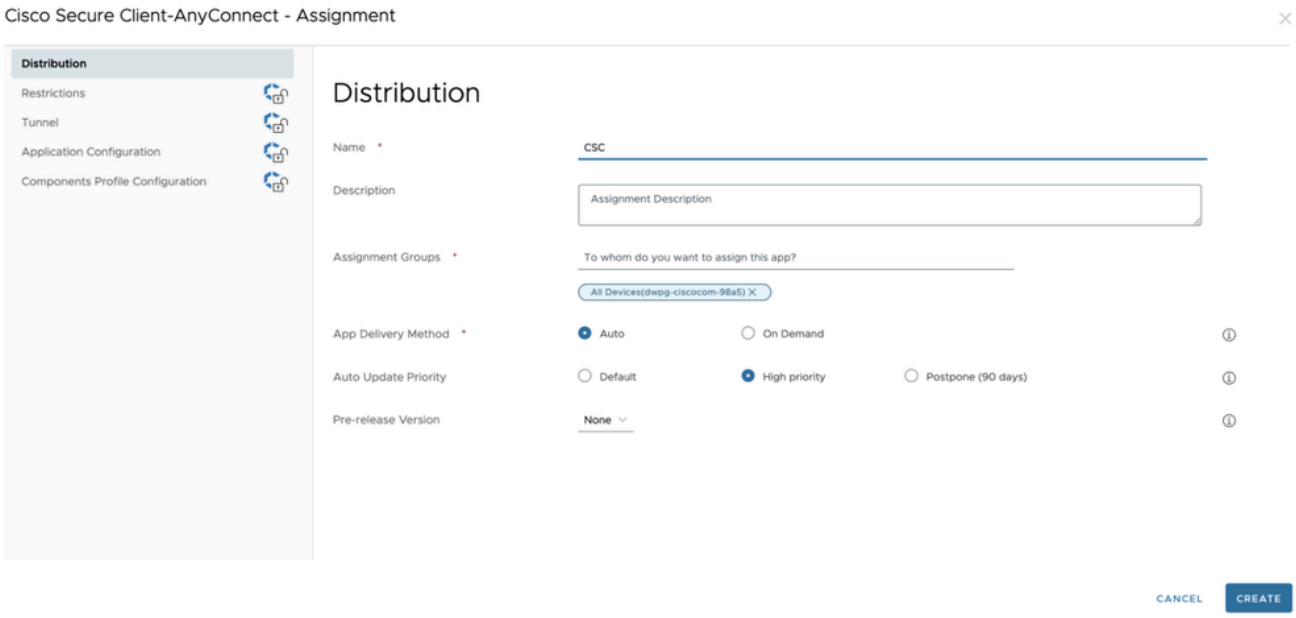
2. アプリの割り当て：

- アプリを選択し、必要な値を入力します。
- [割り当て]セクションで、新しい割り当てを作成します。



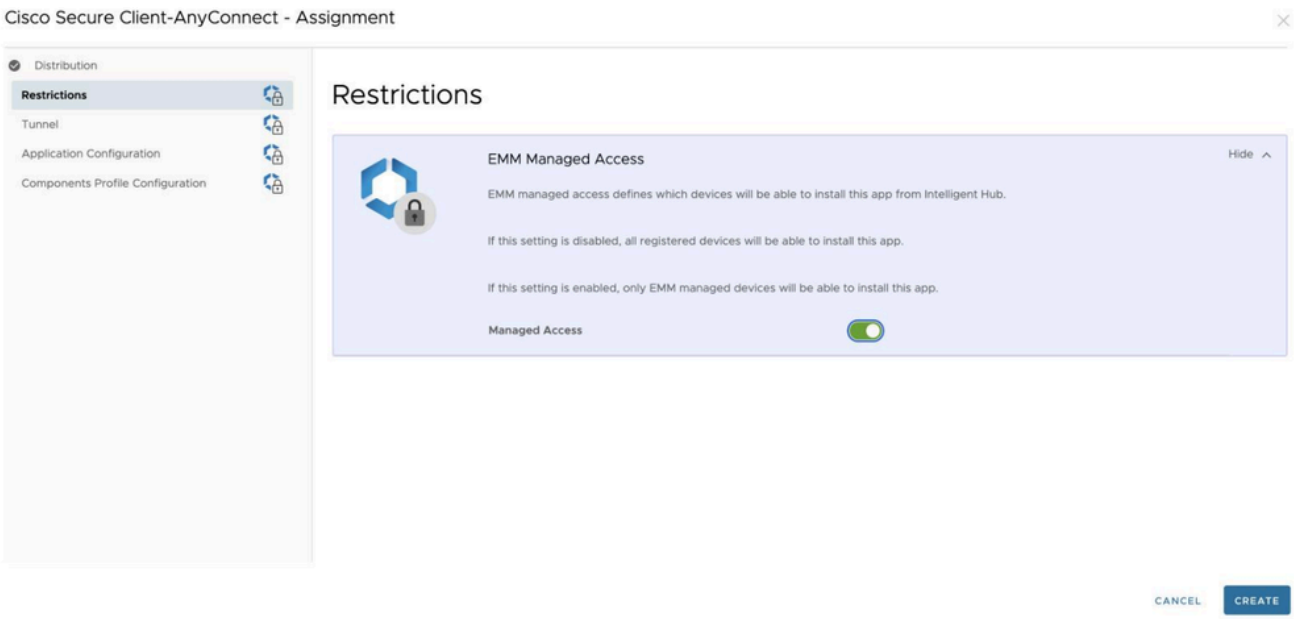
3. 配信の設定：

- [Distribution]セクションに詳細を入力します。



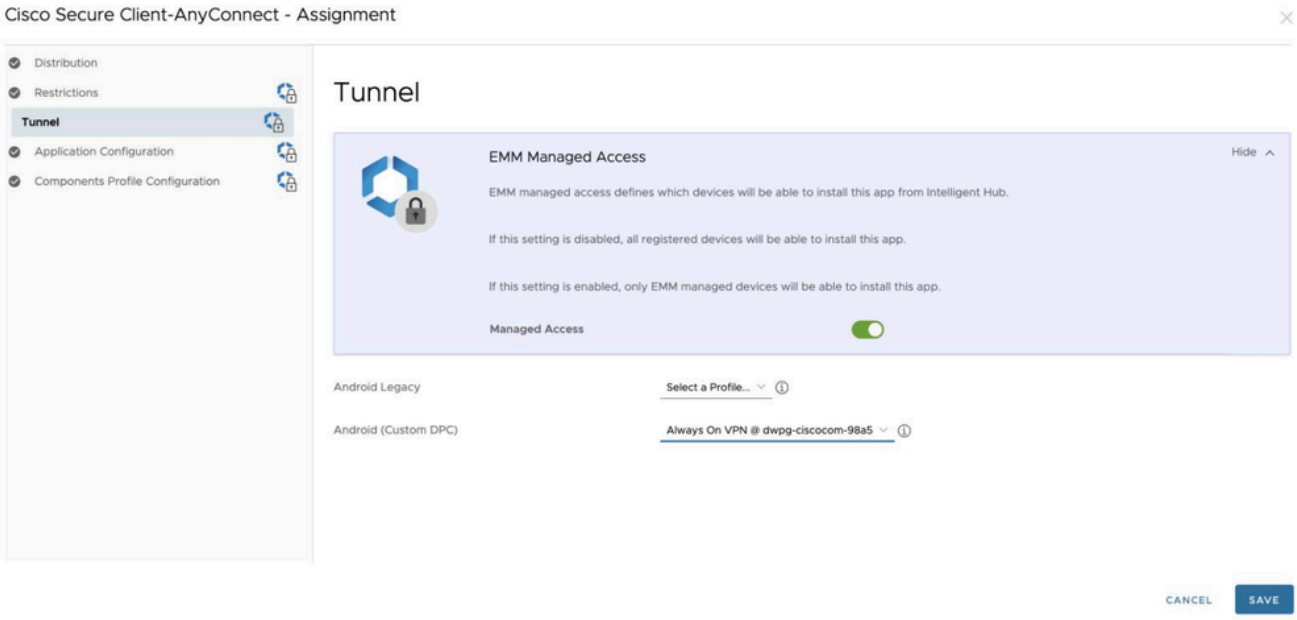
4. 管理アクセスの有効化：

- Restrictionstabで、Managed Accessを有効にします。



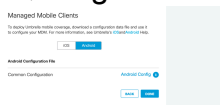
5. プロファイルの選択：

- Tunneloptionで、Android (Custom DPC)の下で以前作成したプロファイル('Always On VPN')を選択します。



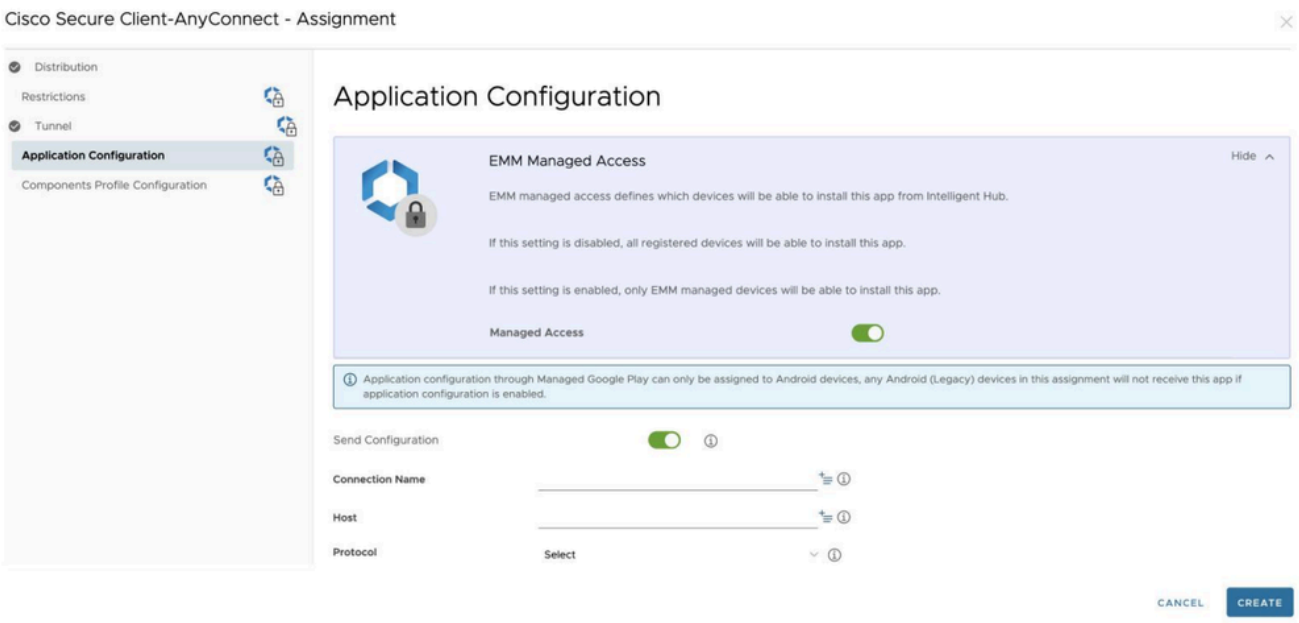
6. アプリケーションの設定：

- Umbrellaダッシュボードからダウンロードしたandroid設定ファイルから、Org IDandReg トークンなどのアプリケーション設定の詳細を入力します。



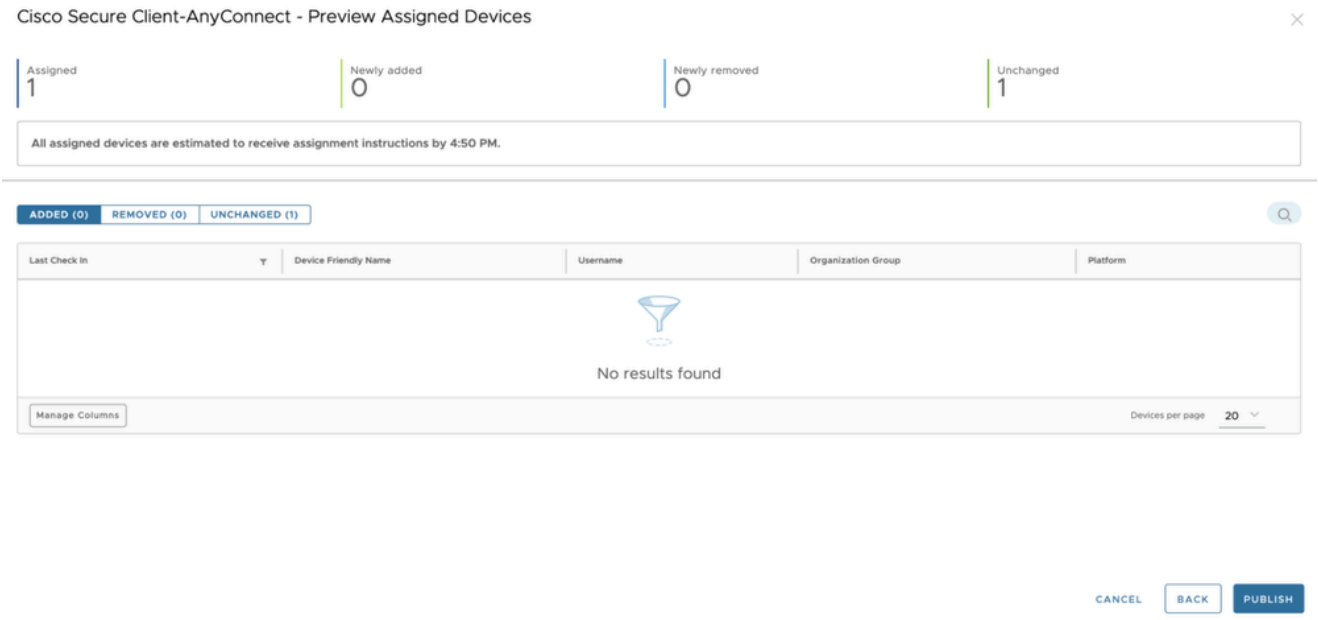
- EnableAccept SEULA：ユーザが手動によるSEULA受け入れをバイパスできるようにします。
- EnableAlways On VPN Mode for Umbrella Protection:Cisco Secure Clientによるシームレスなvpn管理のみを行います。
- ユーザによる新しいVPN接続の作成をブロックします（Hostフィールドは空のままに

します）。



7. 保存してパブリッシュ：

- 変更を保存し、Cisco Secure Clientアプリケーションを公開します。



8. Umbrella証明書のプッシュ：

- 手順については、「デバイスへのUmbrella証明書のプッシュ」を参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。