Déployer un client sécurisé avec protection Umbrella sur Android via Zero-Touch MDM

Table des matières

Introduction

Ce document décrit comment déployer Cisco Secure Client avec le module Umbrella sur des appareils Android en utilisant le déploiement automatique.

Informations générales

Vous pouvez déployer Cisco Secure Client avec le module Umbrella sur des appareils Android en utilisant un déploiement sans intervention via des solutions MDM telles que Workspace One, Cisco Meraki ou Microsoft Intune. Ce processus permet une protection transparente de la couche DNS pour les applications et le trafic du navigateur, garantit l'activation du VPN Always On et élimine l'intervention de l'utilisateur pour l'acceptation du VPN et du SEULA.

Conditions préalables

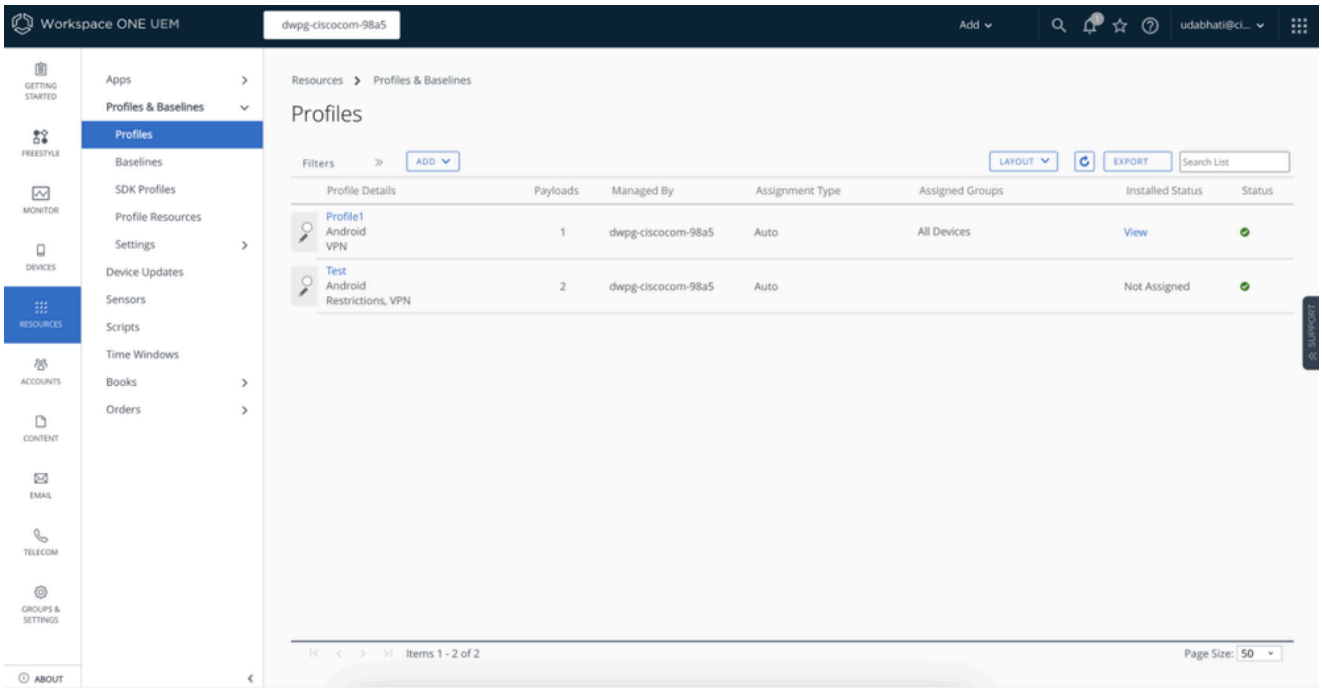
- Inscrivez-vous et inscrivez-vous à Android Enterprise Mobility Management (EMM) en créant un profil de travail.
- L'application MDM (concentrateur) doit être visible sous le profil de travail.
- Attribuez et installez Cisco Secure Client uniquement après la publication et l'installation du profil Always On VPN sur le concentrateur intelligent.

Étapes de déploiement

A. Créer le profil VPN Always On

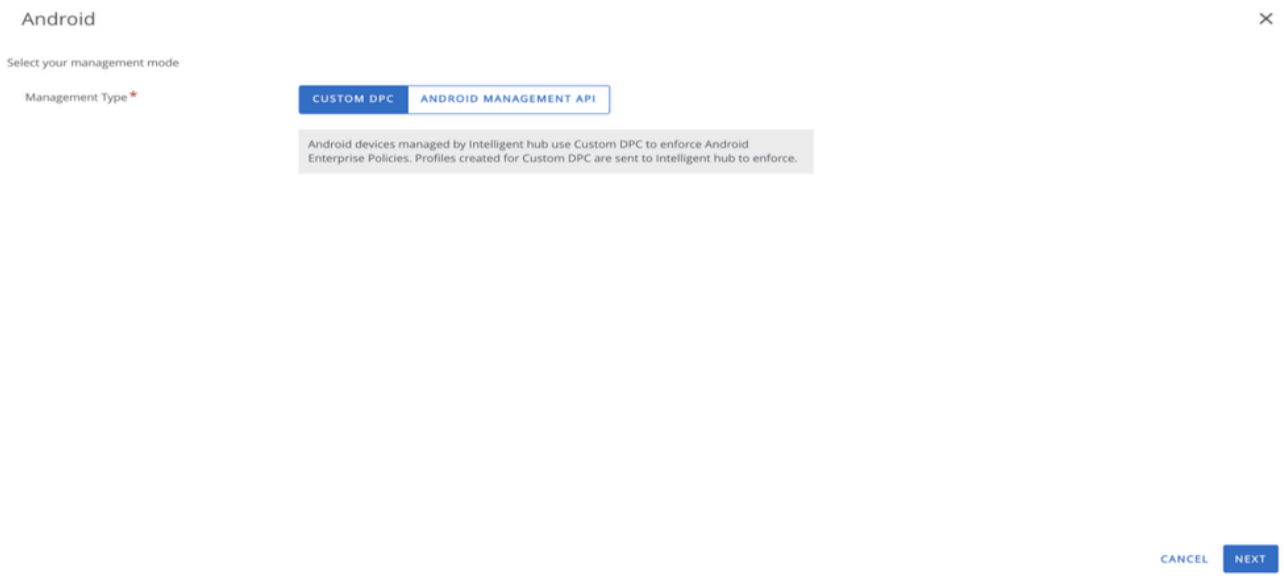
1. Accédez à Profils :

    - Accédez à Ressources > Profils et lignes de base > Profils.
    - Cliquez sur Ajouter pour créer un nouveau profil.

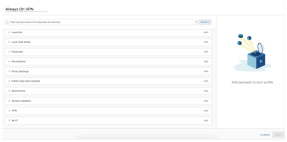


2. Configuration du profil :

- Sélectionnez Android comme plate-forme.
- Sélectionnez le type de gestion requis.

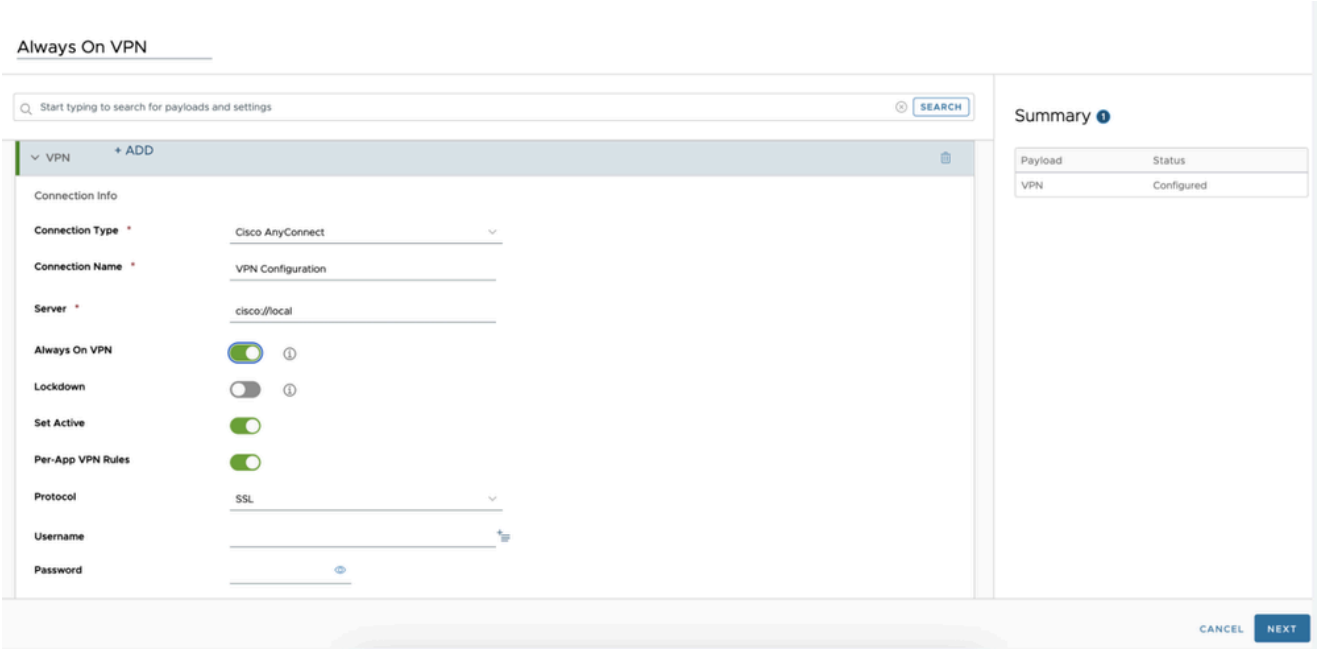


3. Configuration des paramètres VPN :



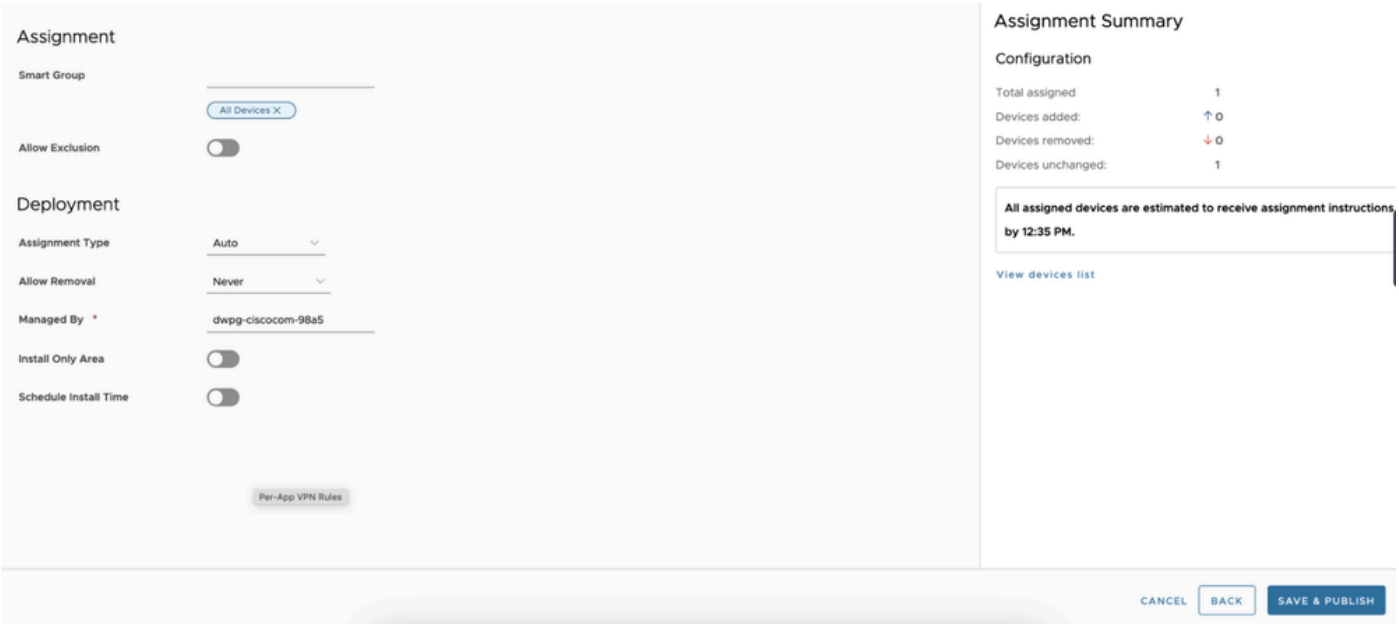
- Dans la section Profile, accédez à VPN Settings et cliquez sur Add.
- Renseignez les champs obligatoires :
  - Type de connexion:Cisco AnyConnect
  - Serveur : cisco://local
  - EnableAlways On VPN et configurez d'autres propriétés si nécessaire.

    - Activer les règles VPN par application.
    - EnableSet Active.
- Cliquez sur Suivant.



4. Attribuer un profil :

    - Laissez le groupe intelligent vide.
    - Attribuez le profil aux périphériques nécessaires.
    - Sélectionnez les valeurs de déploiement.
    - Cliquez sur Enregistrer et publier.



B. Attribution de l'application Cisco Secure Client

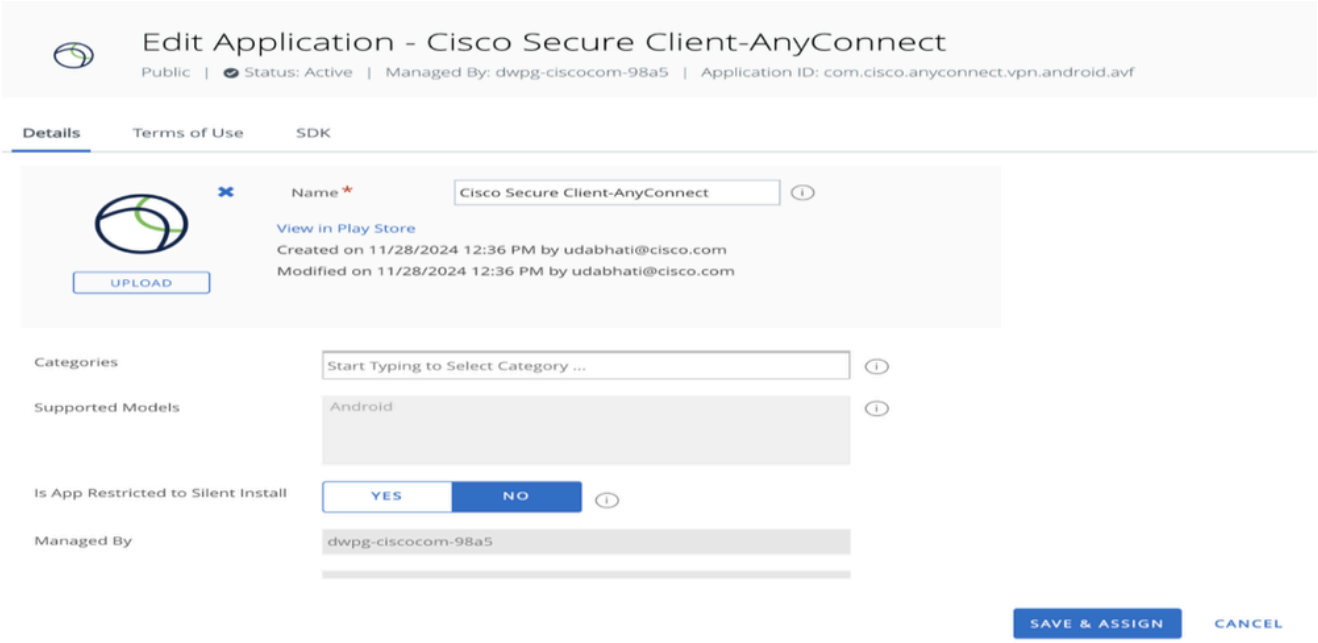
1. Ajouter l'application :

- Accédez à Ressources > Natif > Public.

- Ajoutez Cisco Secure Client à partir du Play Store si ce n'est pas déjà fait.

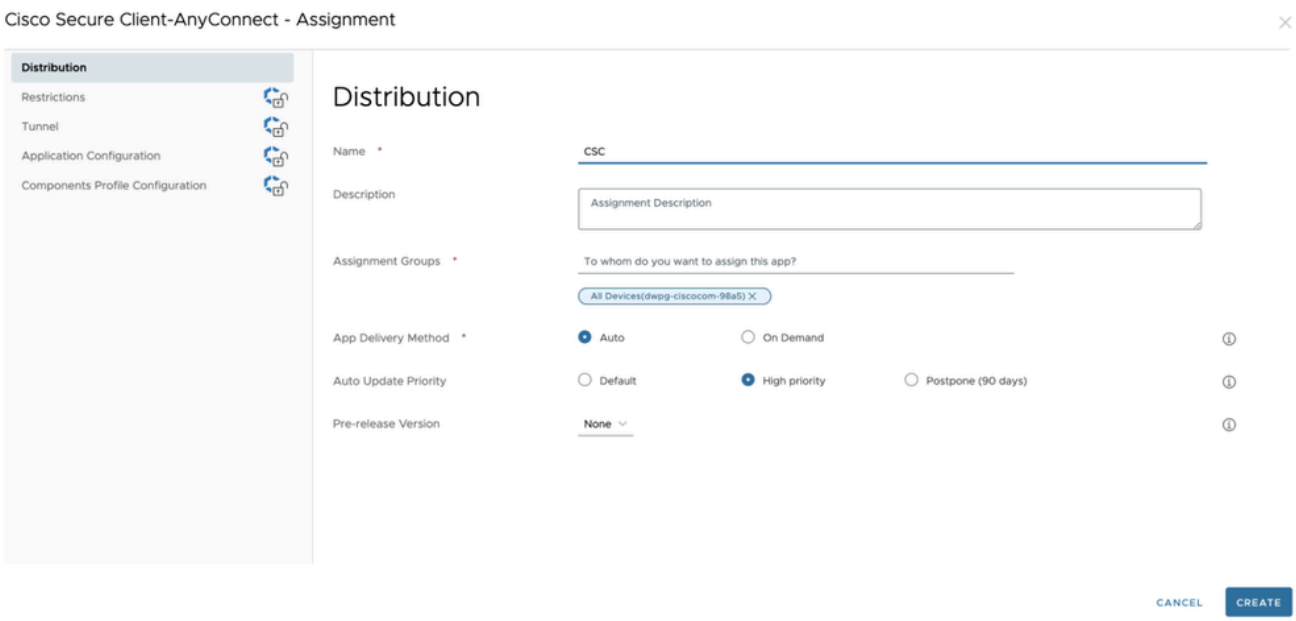
2. Affectation d'application :

- Sélectionnez l'application et renseignez les valeurs requises.
- Dans la section Affectation, créez une nouvelle affectation.



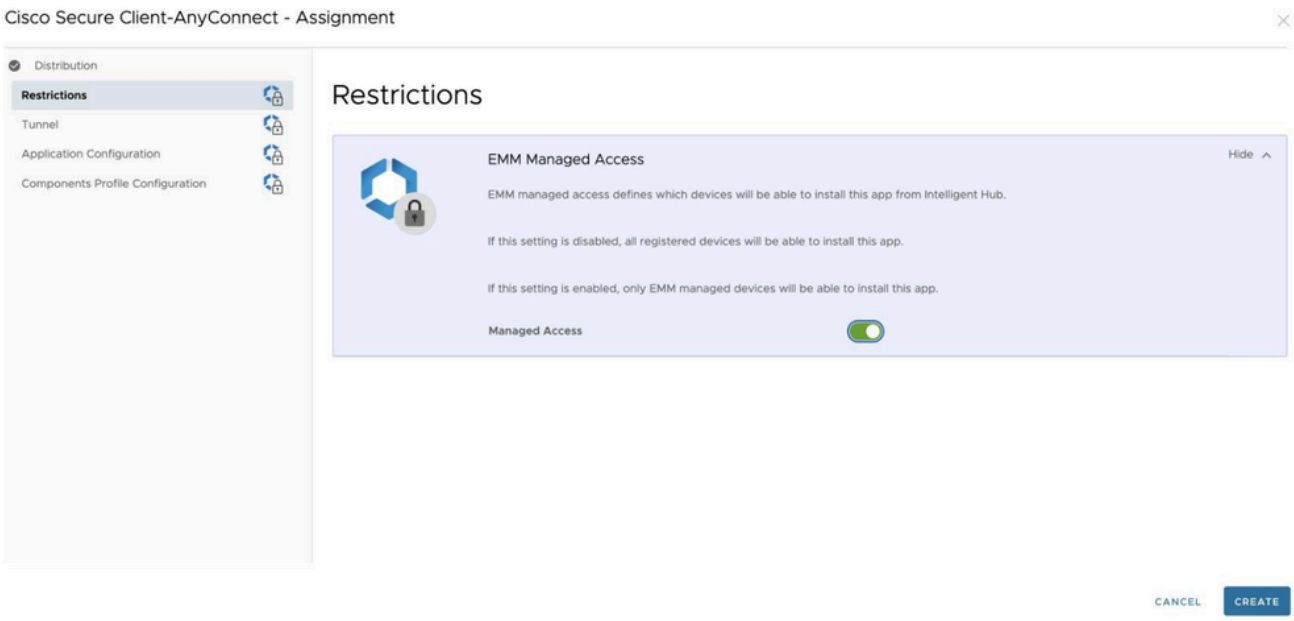
3. Configurer la distribution :

- Saisissez les détails dans la section Distribution.



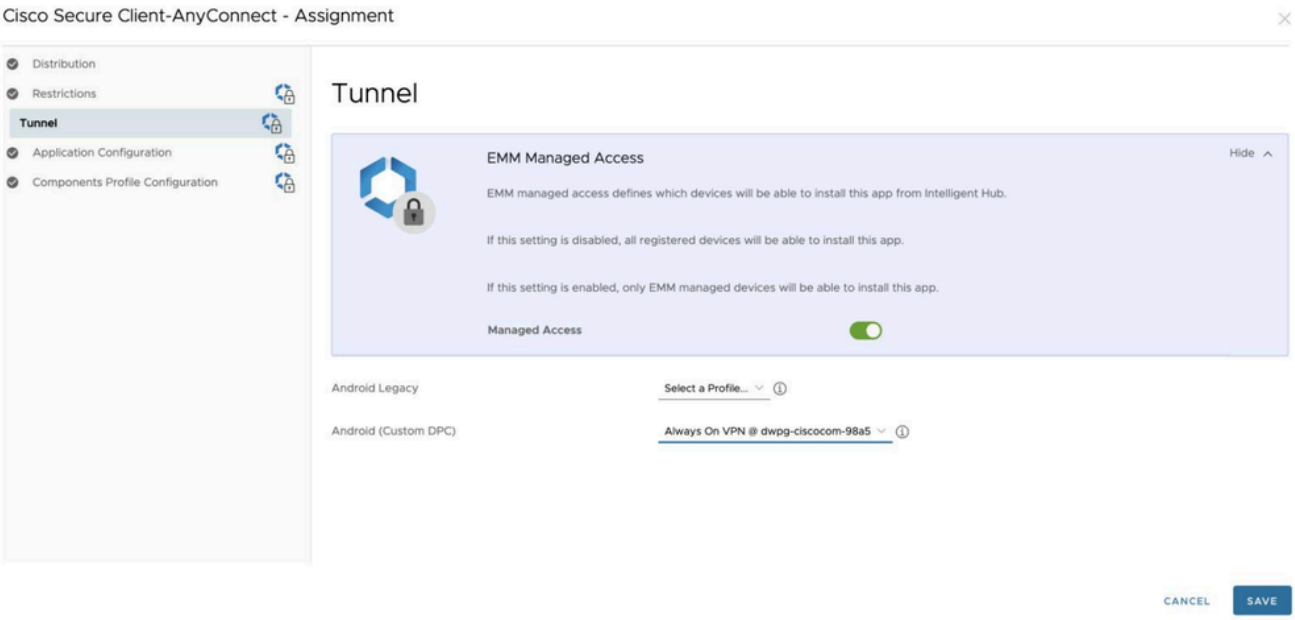
4. Activer l'accès géré :

- Dans l'ongletRestrictions, activezAccès géré.



5. Sélectionner un profil :

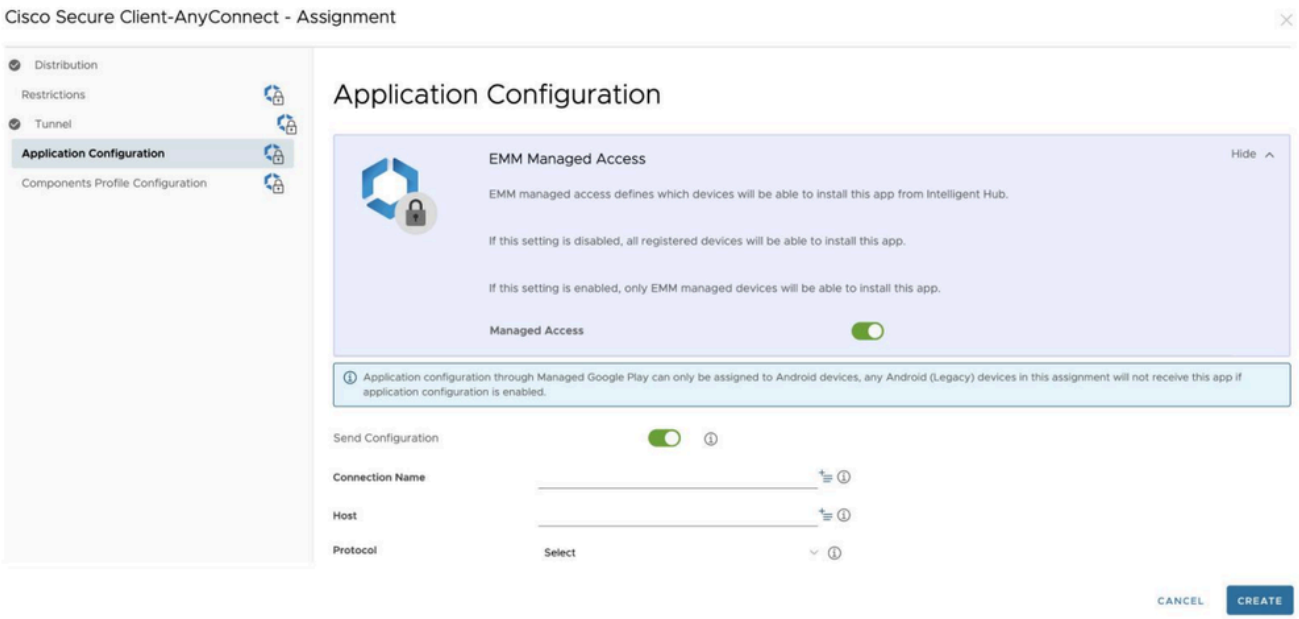
- Dans l'option Tunnel, sélectionnez le profil précédemment créé (« Always On VPN ») sous Android (Custom DPC).



6. Configuration des applications :

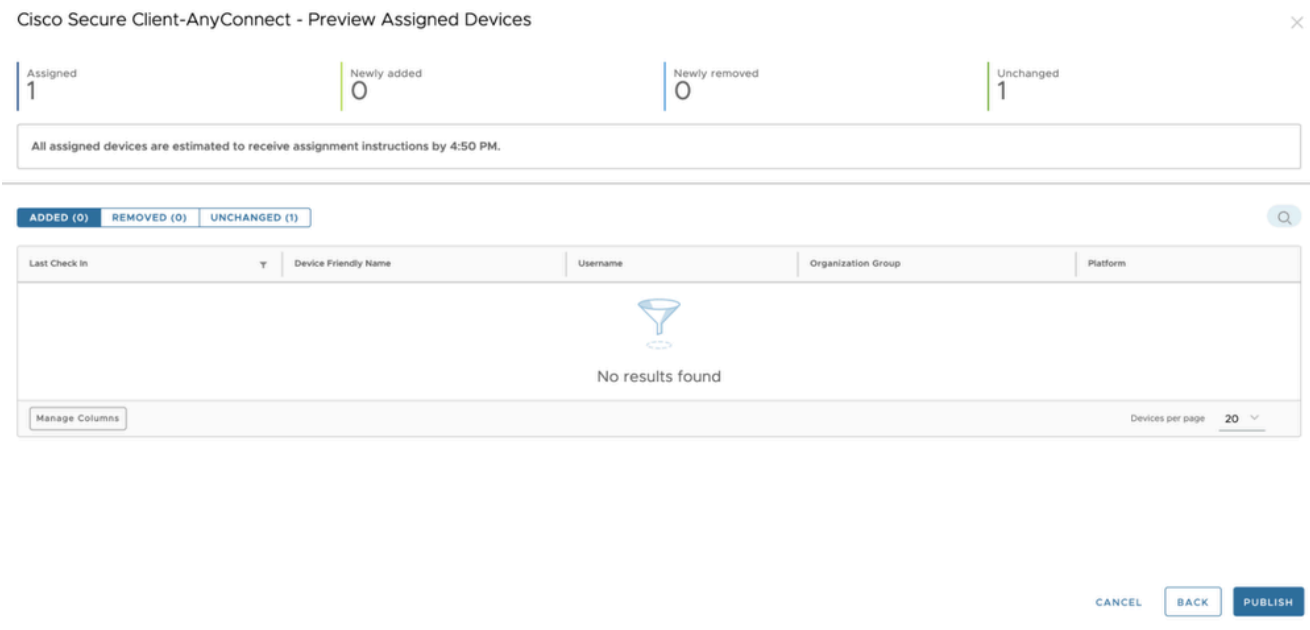
- Entrez les détails de configuration de l'application tels que Org IDandReg Token dans le fichier de configuration Android téléchargé à partir du tableau de bord Umbrella.
- EnableAccept SEULA : permet aux utilisateurs de contourner l'acceptation SEULA manuelle.
- Activer le mode VPN Always On pour la protection Umbrella Only pour une gestion VPN transparente par Cisco Secure Client.

- Empêchez les utilisateurs de créer de nouvelles connexions VPN (laissez le champ Hôte vide).



7. Enregistrer et publier :

- Enregistrez les modifications et publiez l'application Cisco Secure Client.



8. Push the Umbrella Certificate :

- Pour obtenir des instructions, voir : [Diffuser le certificat-cadre aux périphériques]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.