Deploy Secure Client with Umbrella Protection on Android via Zero-Touch MDM

Contents

Introduction

This document describes how to deploy Cisco Secure Client with the Umbrella module on Android devices using zero-touch deployment.

Background Information

You can deploy Cisco Secure Client with the Umbrella module on Android devices using zero-touch deployment through MDM solutions such as Workspace One, Cisco Meraki, or Microsoft Intune. This process enables seamless DNS-layer protection for apps and browser traffic, ensures Always On VPN is enabled, and eliminates user intervention for VPN and SEULA acceptance.

Prerequisites

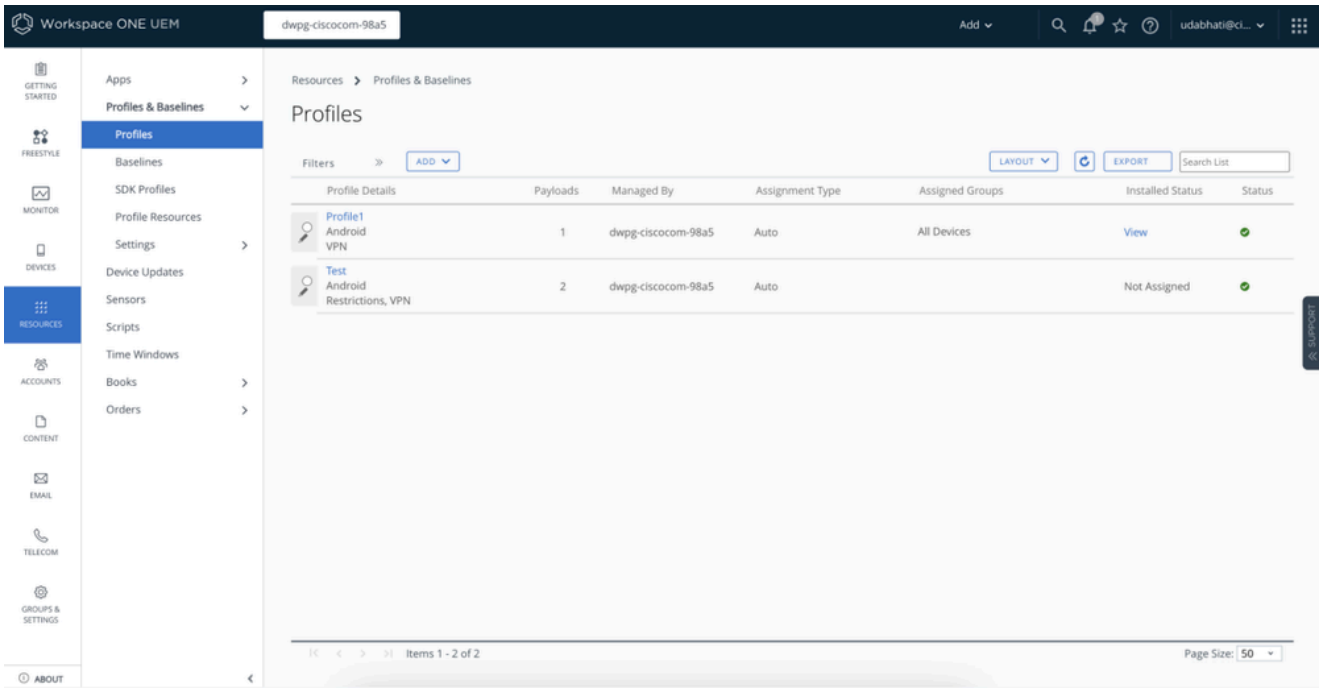
- Complete Android Enterprise Mobility Management (EMM) registration and device enrollment with work profile creation.
- The MDM app (Hub) must be visible under the work profile.
- Assign and install Cisco Secure Client only after publishing and installing the Always On VPN profile to Intelligent Hub.

Deployment Steps

A. Create the Always On VPN Profile

1. **Navigate to Profiles:**

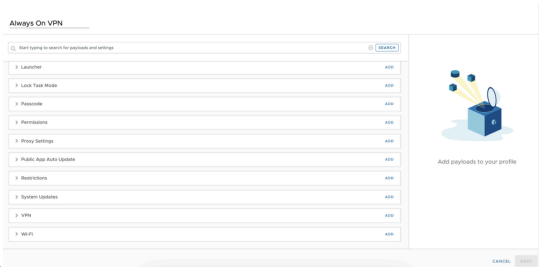
    - Go to**Resources > Profiles & Baselines > Profiles**.
    - Click**Add**to create a new profile.



2. **Profile Setup:**

- Select**Android**as the platform.
- Choose the required**Management Type**.

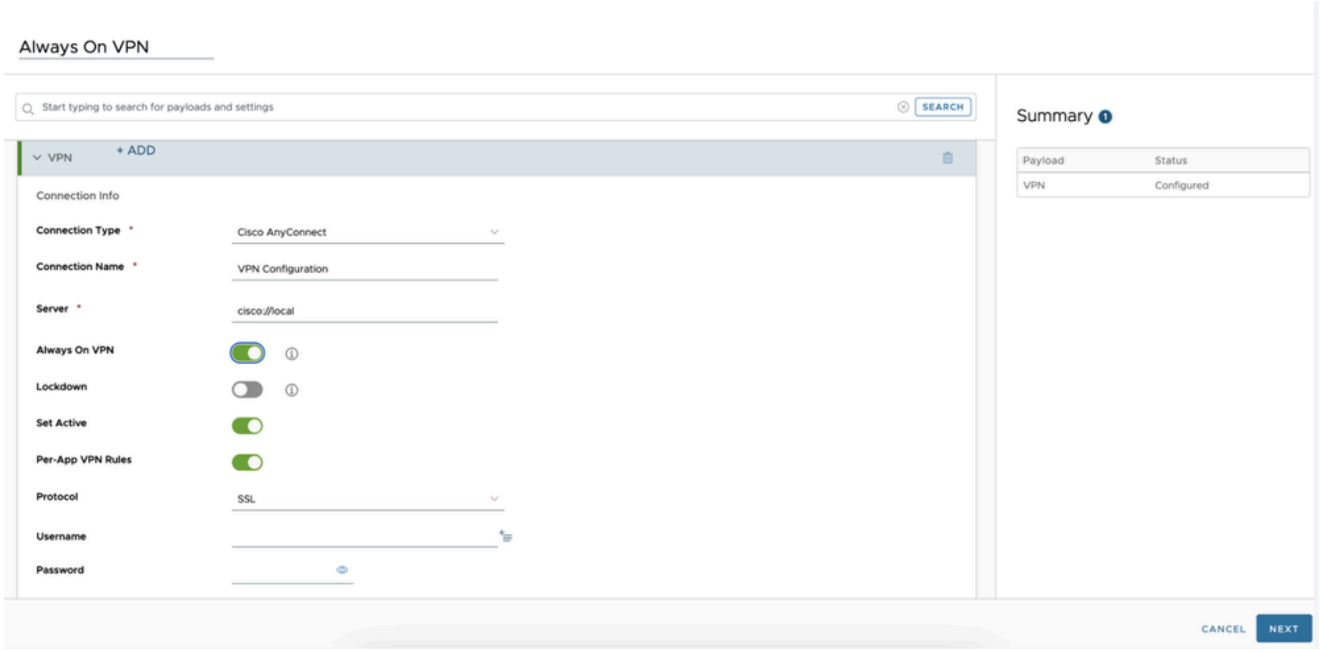
3. **Configure VPN Settings:**



- In the profile section, go to**VPN Setting**and click**Add**.
- Fill in the required fields:
  - **Connection Type:**Cisco AnyConnect

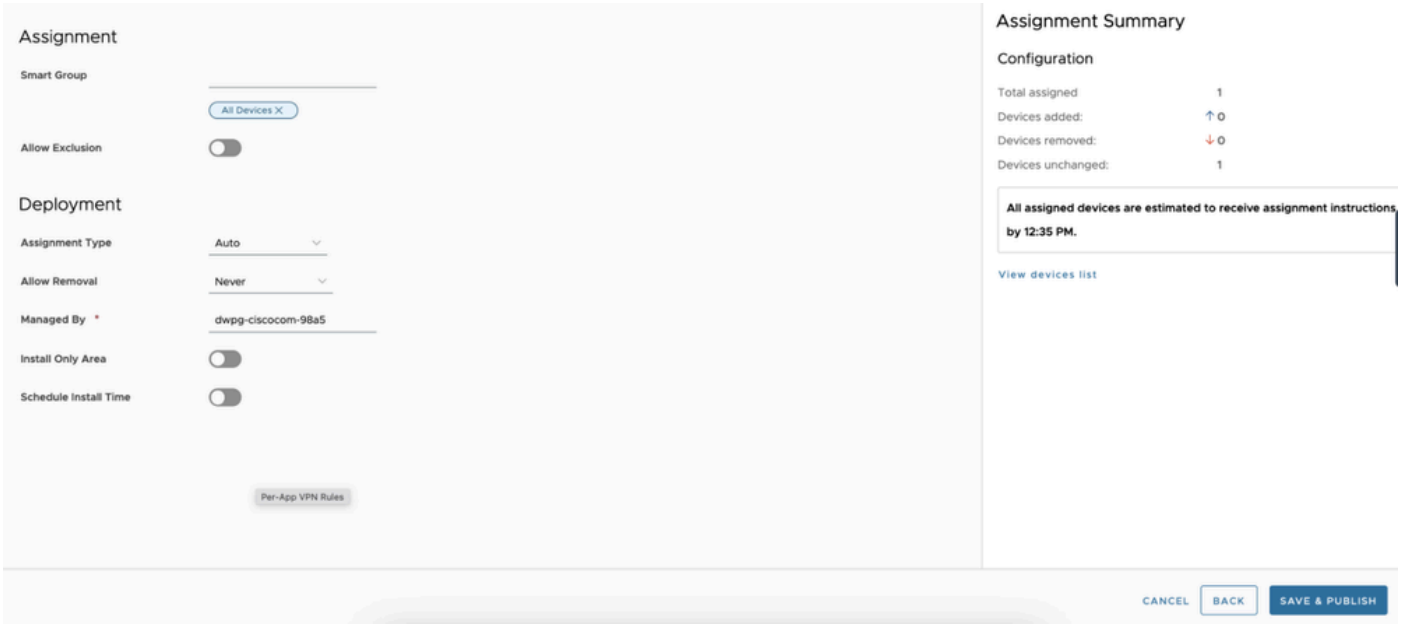
- **Server:**cisco://local
- Enable**Always On VPN**and configure other properties as needed.
- Enable**Per-App VPN Rules**.
- Enable**Set Active**.

- Click**Next**.



4. **Assign Profile:**

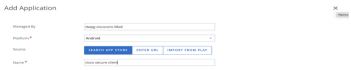
- Leave the Smart Group empty.
- Assign the profile to the necessary devices.
- Select deployment values.
- Click**Save & Publish**.



B. Assign the Cisco Secure Client App

1. **Add the App:**

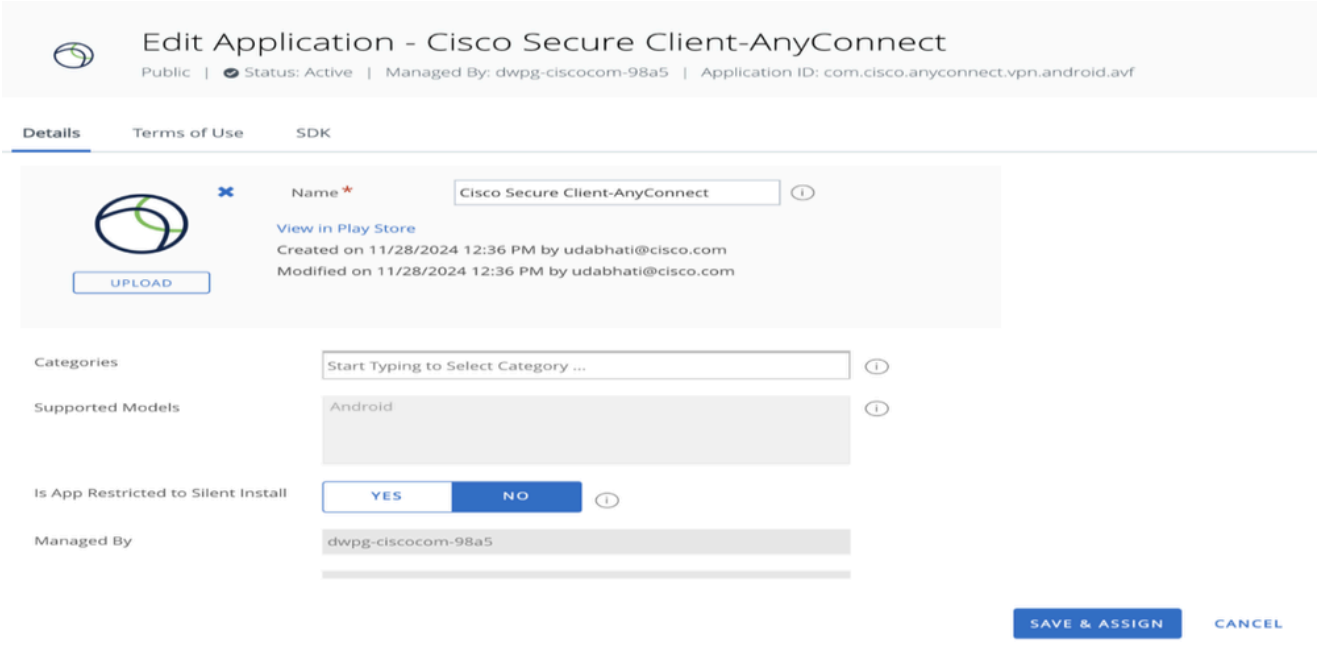
- Go to**Resources > Native > Public**.



- Add**Cisco Secure Client**from the Play Store if not already available.

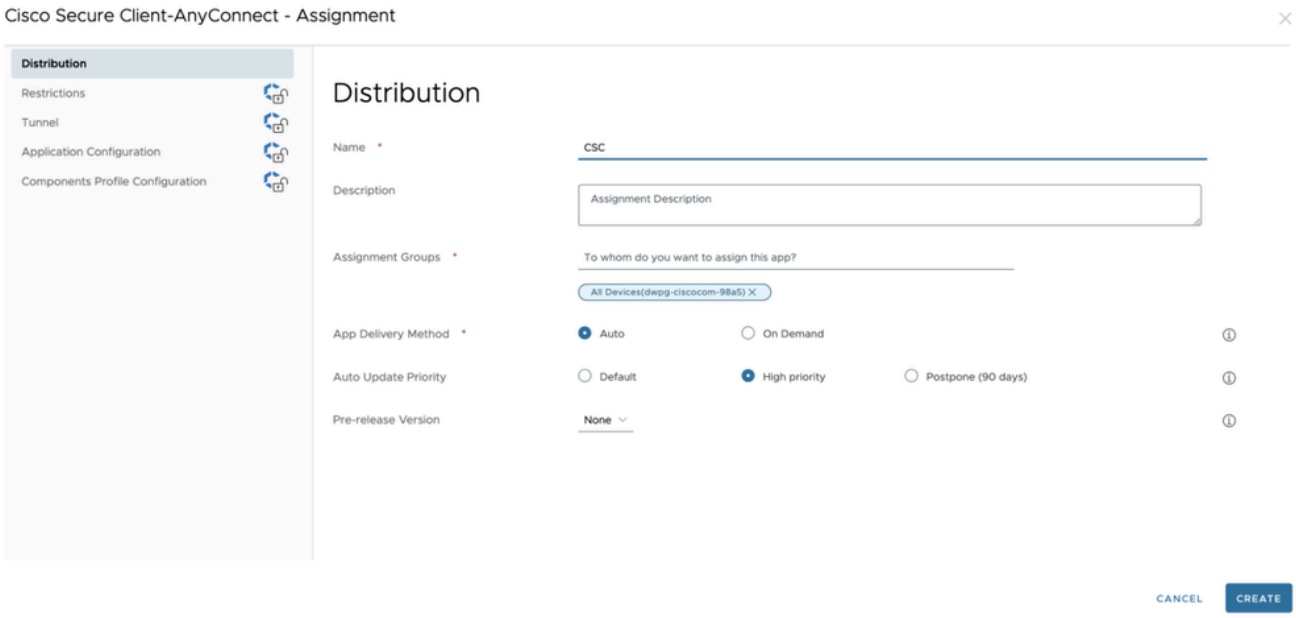
2. **App Assignment:**

- Select the app and fill in required values.
- In the assignment section, create a new assignment.



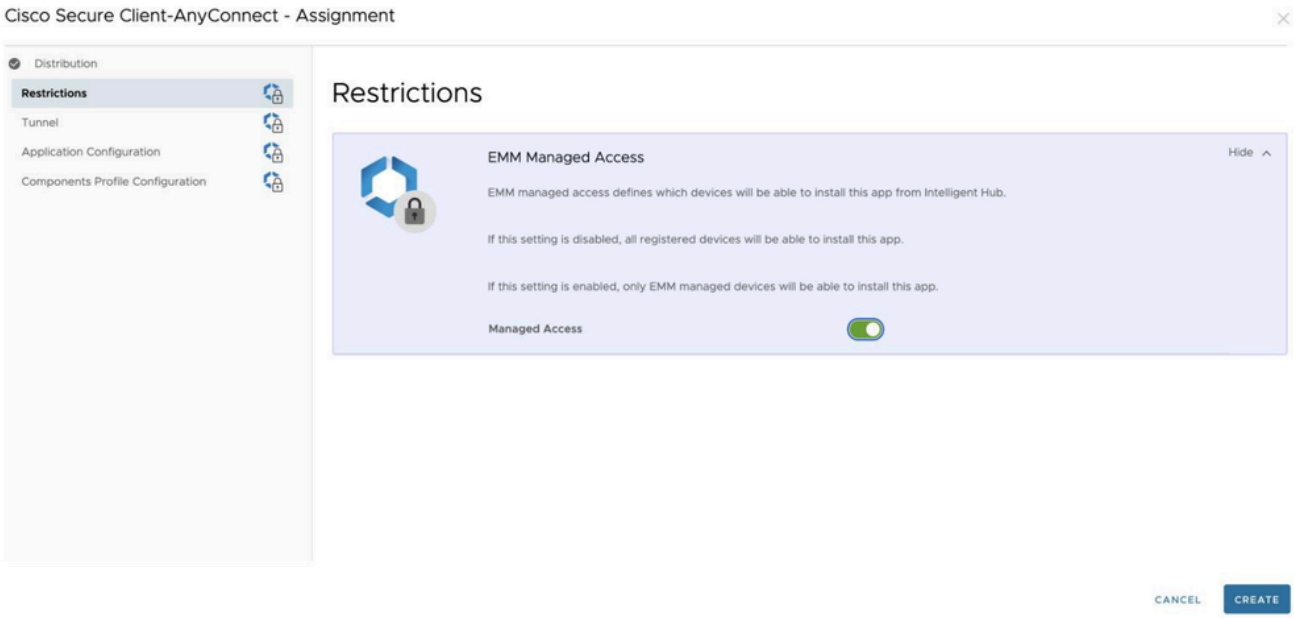
3. **Configure Distribution:**

- Enter details in the Distribution section.



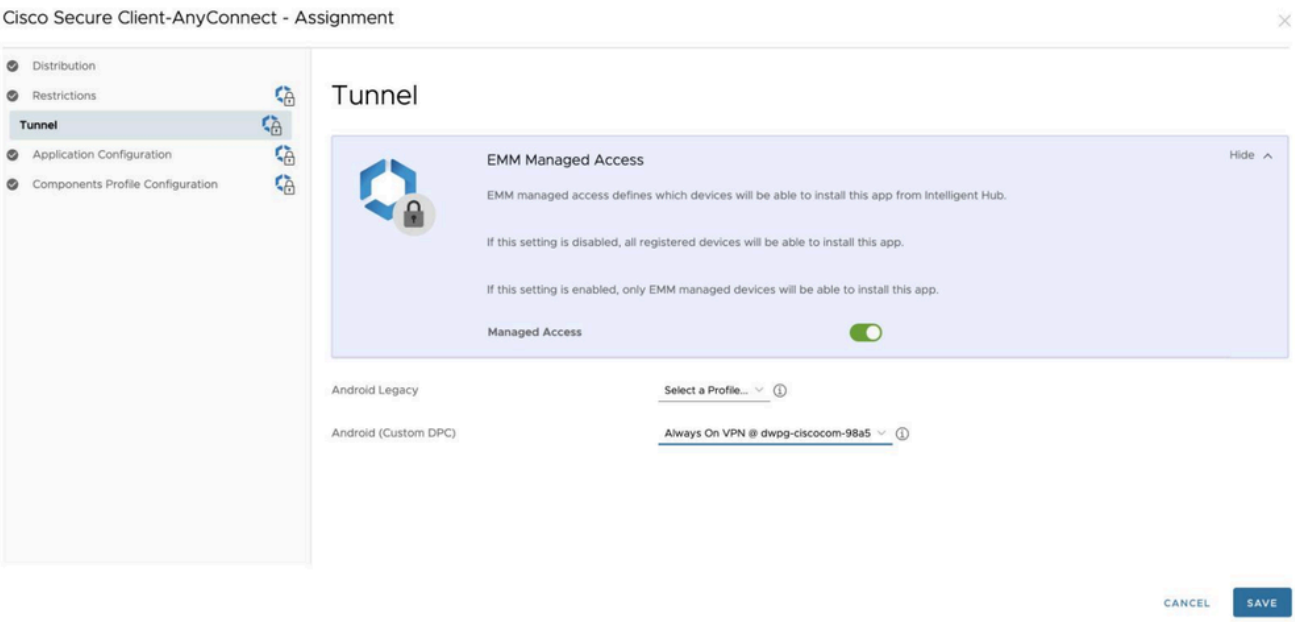
4. **Enable Managed Access:**

- In the**Restrictions**tab, enable**Managed Access**.



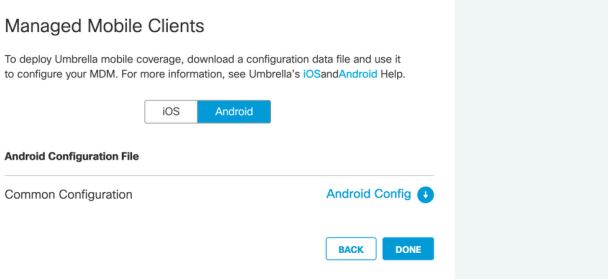
5. **Select Profile:**

- In the**Tunnel**option, select the previously created profile ('Always On VPN') under**Android (Custom DPC)**.



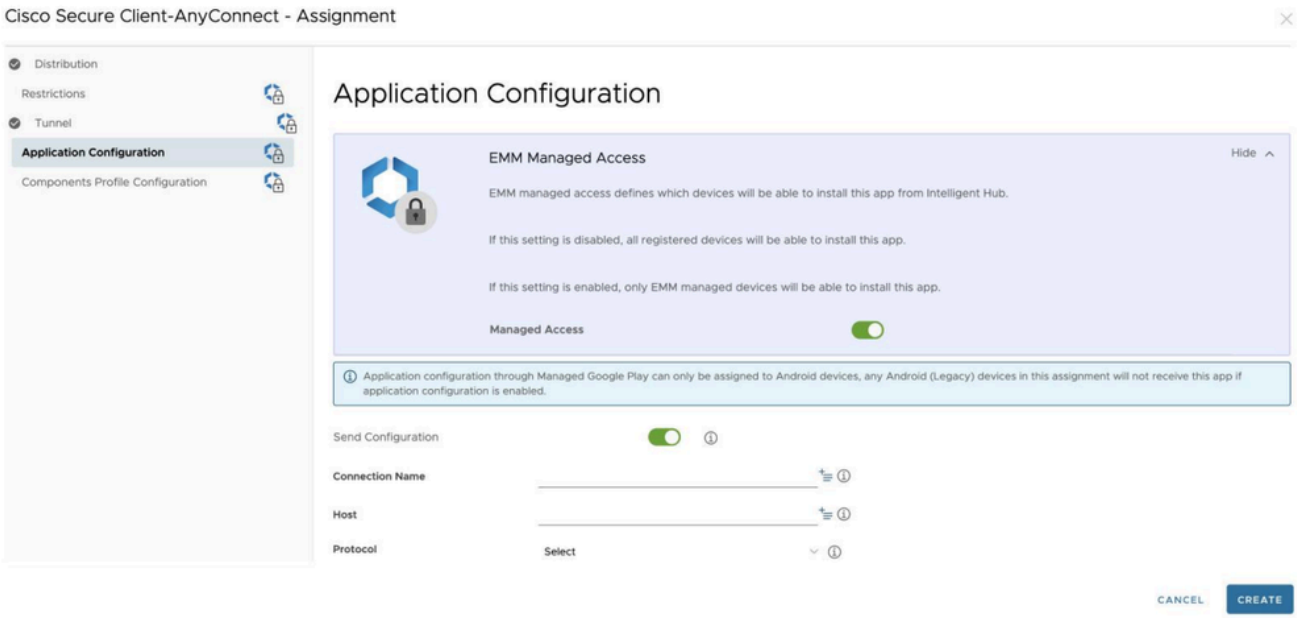
6. **Application Configuration:**

- Enter application configuration details such as**Org ID**and**Reg Token**from the Android Config

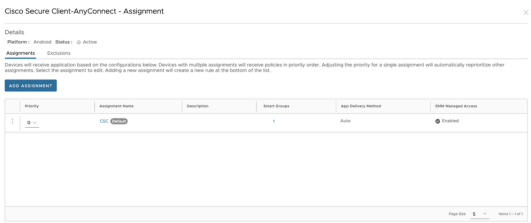


File downloaded from the Umbrella Dashboard.

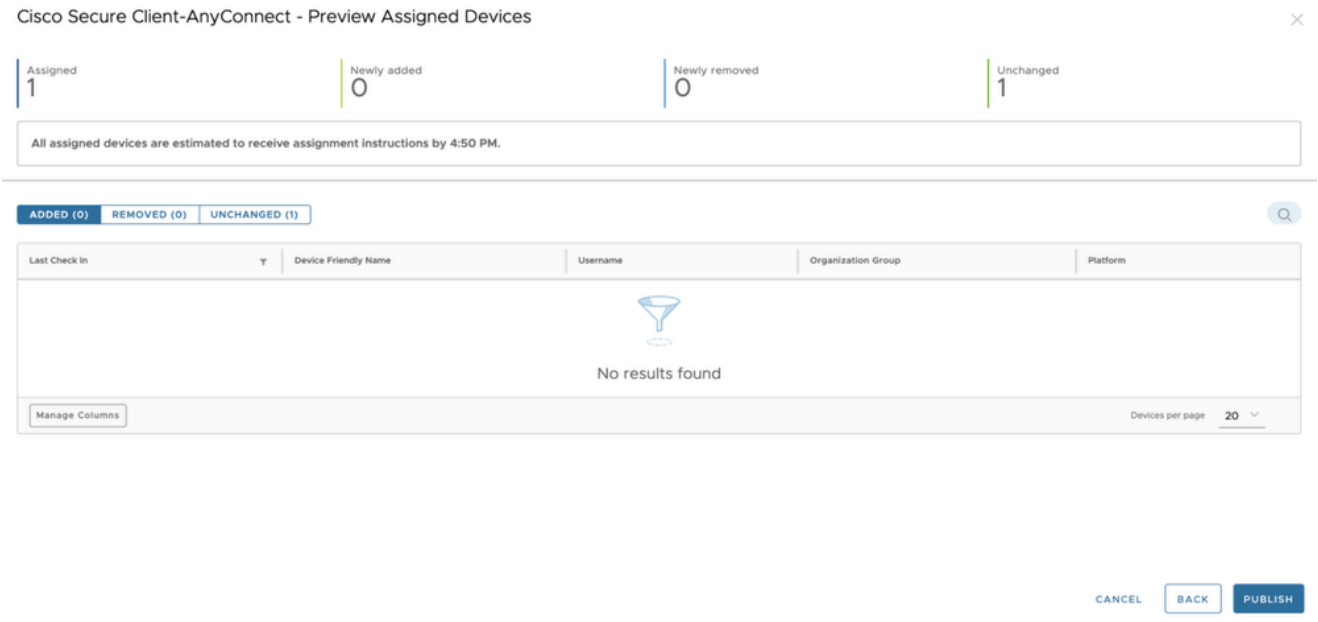
- Enable**Accept SEULA For Users**to bypass manual SEULA acceptance.
- Enable**Always On VPN Mode for Umbrella Protection Only**for seamless VPN management by Cisco Secure Client.
- Block users from creating new VPN connections (leave the Host field empty).



7. **Save and Publish:**



- Save changes and publish the Cisco Secure Client app.



8. **Push the Umbrella Certificate:**

- For instructions, see: Push the Umbrella Certificate to Devices