# 通过零接触MDM在Android上部署具有Umbrella保护的安全客户端

## 目录

## 简介

本文档介绍如何使用零接触部署在Android设备上部署带有Umbrella模块的Cisco Secure Client。

## 背景信息

您可以通过MDM解决方案（如Workspace One、Cisco Meraki或Microsoft Intune）使用零接触部署在Android设备上部署带有Umbrella模块的Cisco Secure Client。此过程可实现对应用和浏览器流量的无缝DNS层保护，确保启用永远在线VPN，并消除用户对VPN和SEULA接受的干预。

## 先决条件

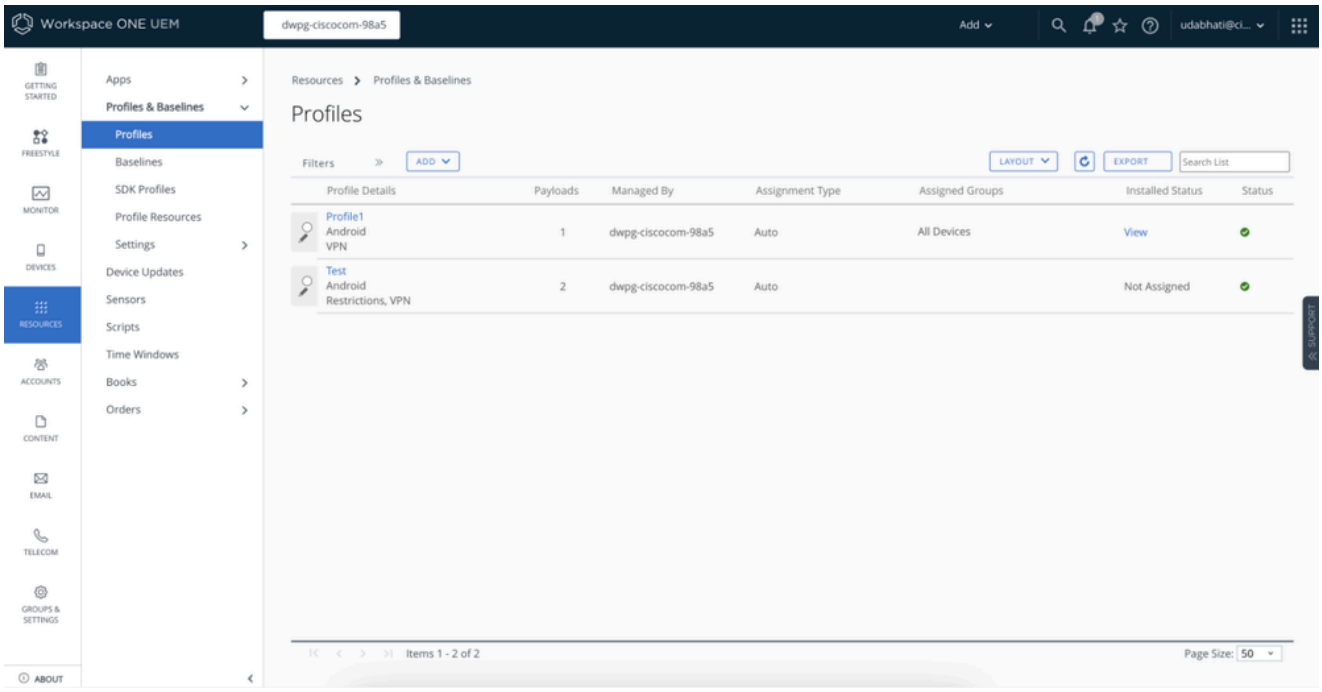
- 通过创建工作配置文件完成Android企业移动管理(EMM)注册和设备注册。
- MDM应用(Hub)必须在工作配置文件下可见。
- 仅在发布和安装Always On VPN配置文件到Intelligent Hub之后分配和安装Cisco Secure Client。

## 部署步骤

### A.创建Always On VPN配置文件

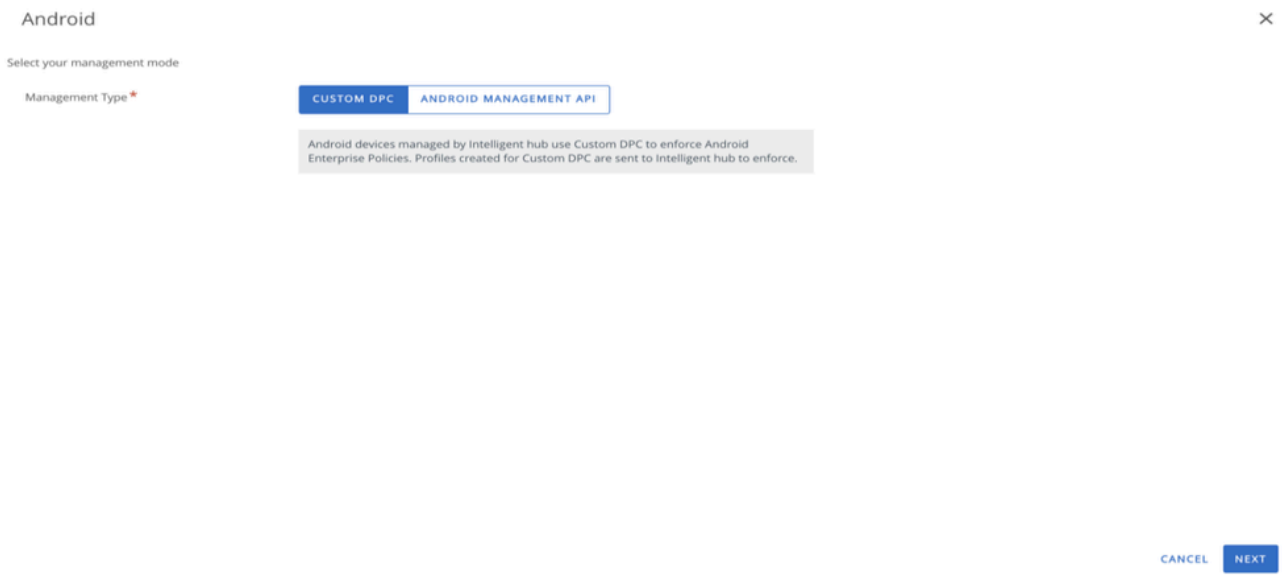
1. 导航至配置文件：

    - 转至Resources > Profiles & Baselines > Profiles。
    - 点击Add以创建新配置文件。

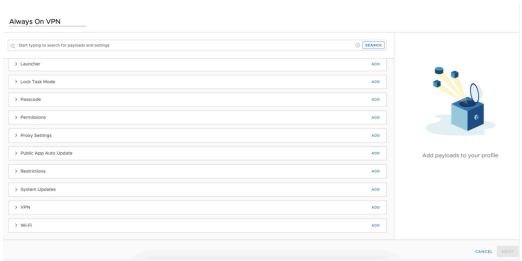



2. 配置文件设置：

- 选择Android作为平台。
- 选择requiredManagement Type。



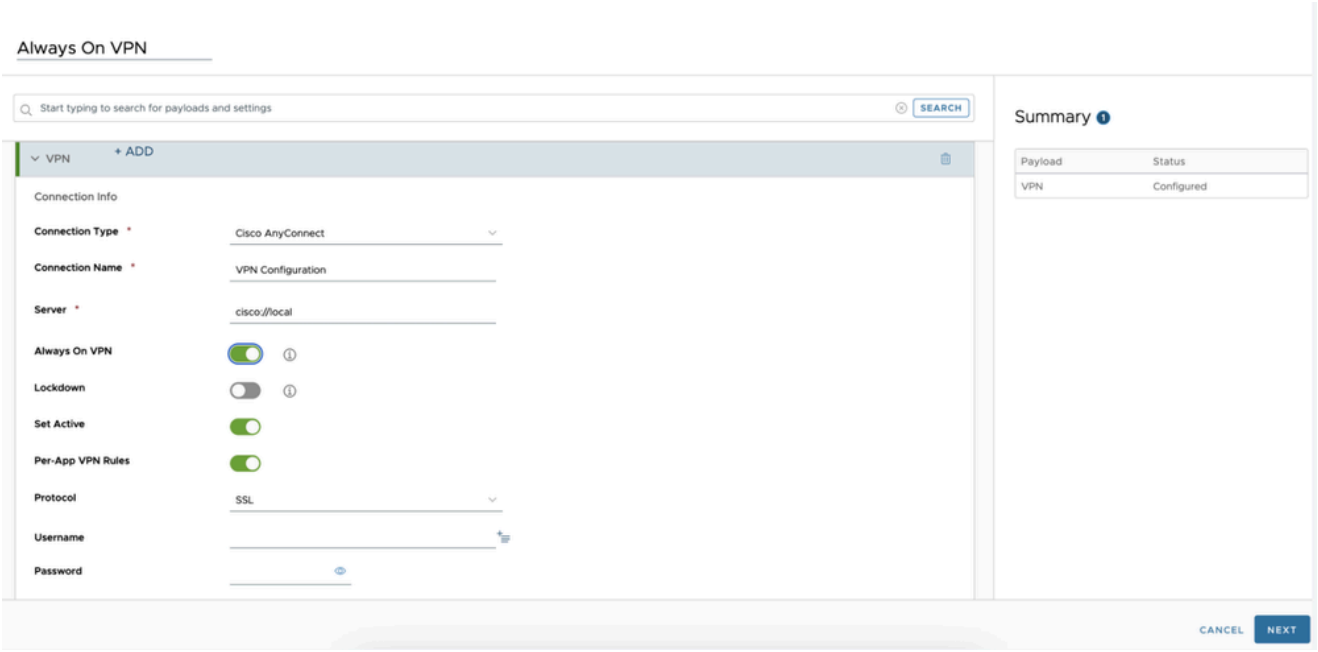

3. 配置VPN设置：




- 在profile部分，转至VPN Settings，然后单击Add。
- 填写必填字段：
  - 连接类型:Cisco AnyConnect

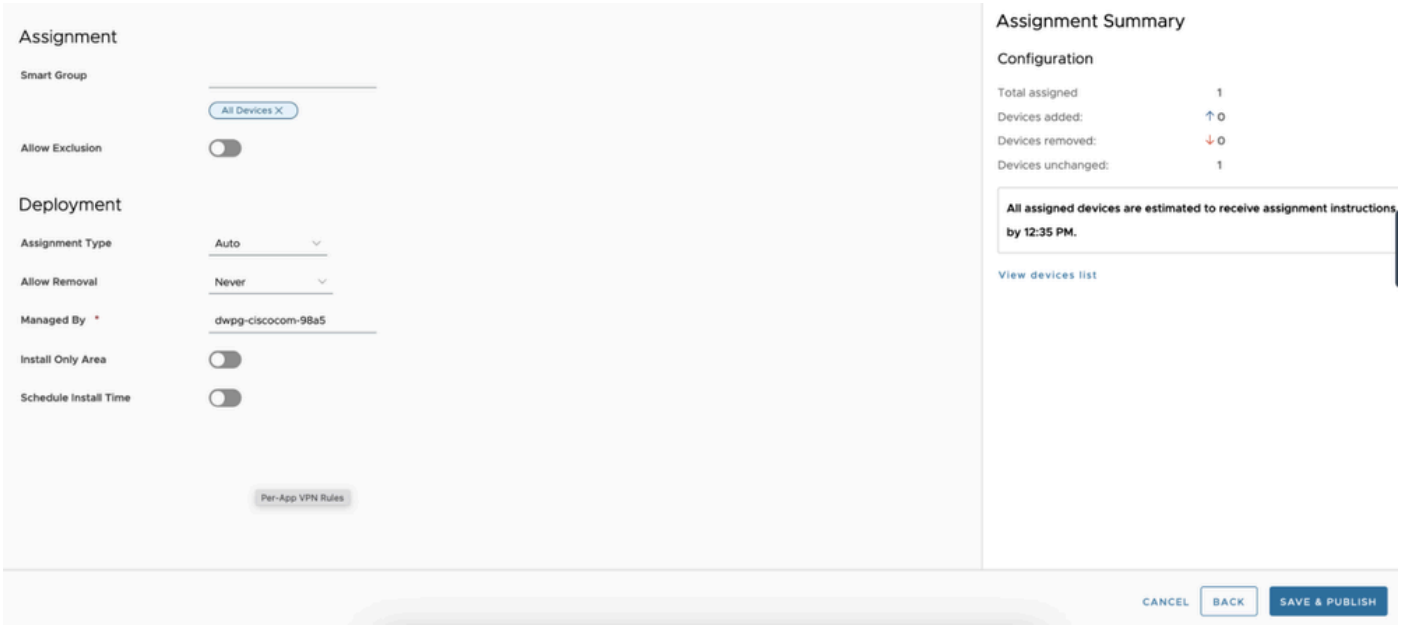
- 服务器：cisco://local
- EnableAlways On VPN并根据需要配置其他属性。
- EnablePer-App VPN规则。
- EnableSet Active。

- 点击Next。




4. 分配配置文件：

- 将智能组留空。
- 将配置文件分配到必要的设备。
- 选择部署值。
- 点击保存并发布。




B.分配思科安全客户端应用

1. 添加应用：

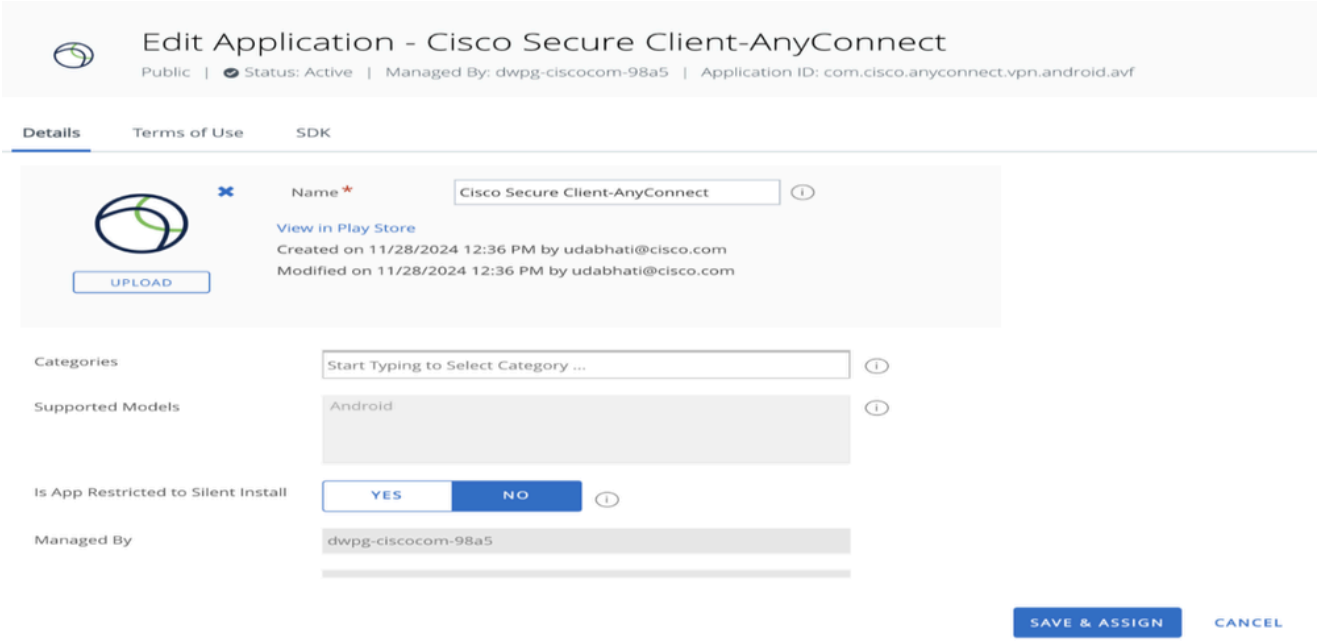
   - 转至Resources > Native > Public。

   - 从Play Store添加Cisco Secure Client（如果尚不可用）。



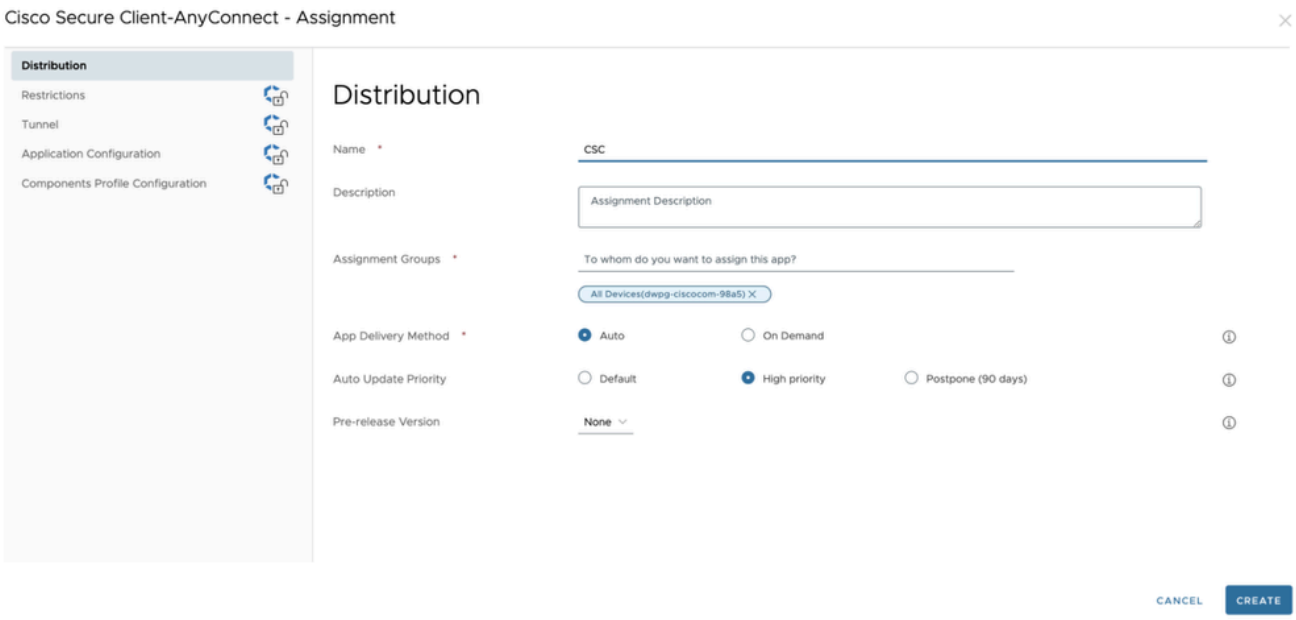
2. 应用分配：

   - 选择应用并填写所需的值。
   - 在“作业”部分中，创建新作业。



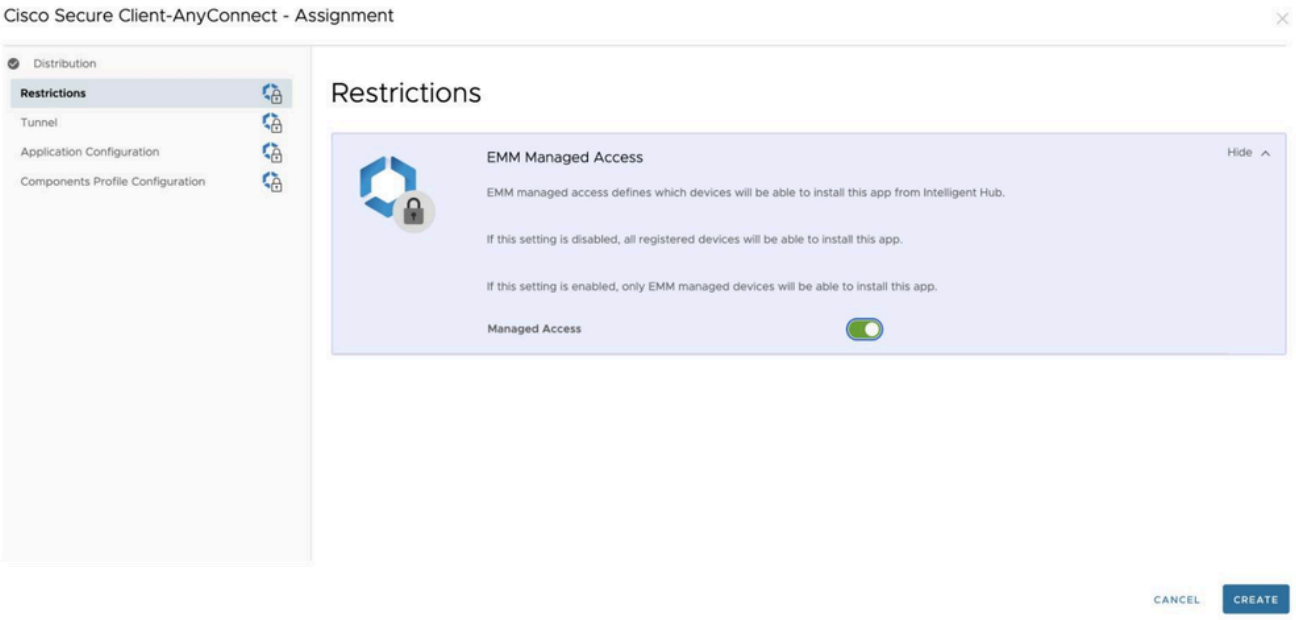

3. 配置分布：

   - 在Distribution部分输入详细信息。



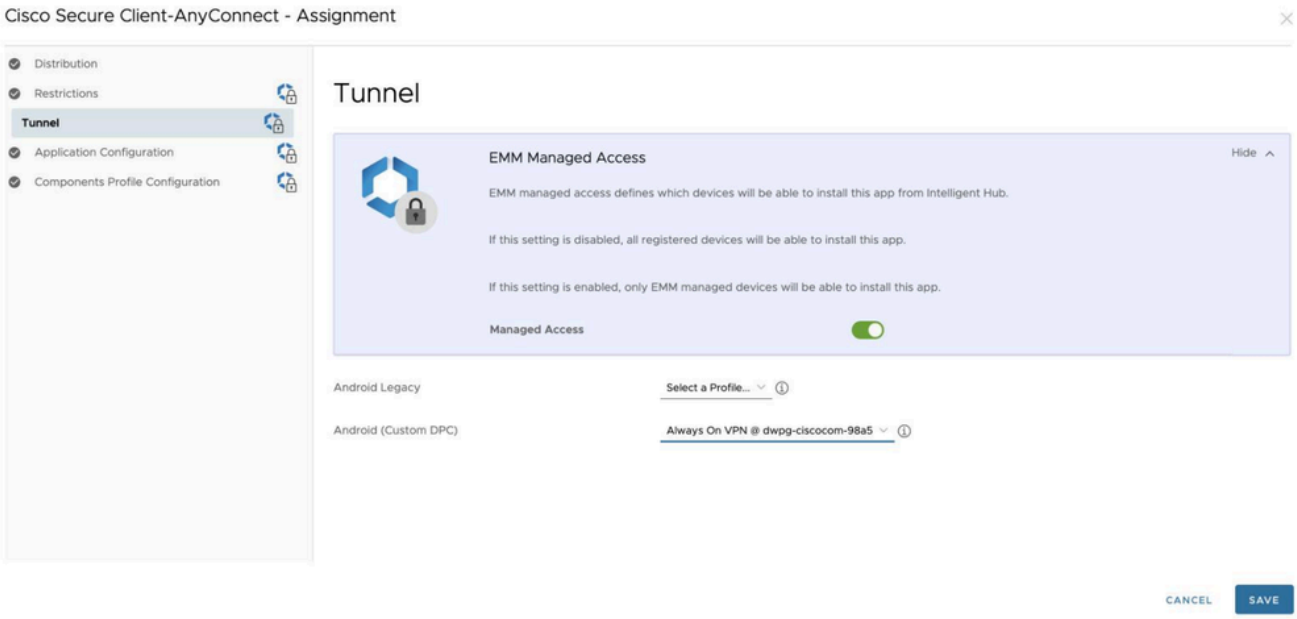

4. 启用托管访问：

- 在Restrictionstab中，enableManaged Access。



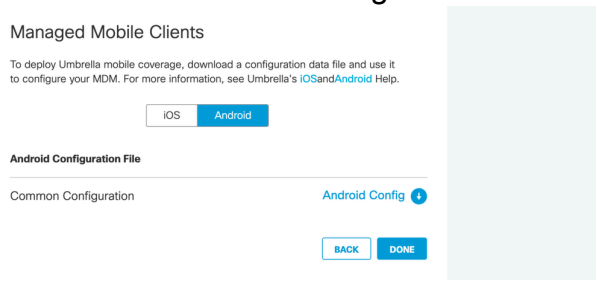

5. 选择配置文件:

- 在Tunneloption中，选择Android（自定义DPC）下先前创建的配置文件(“始终在VPN上”)。

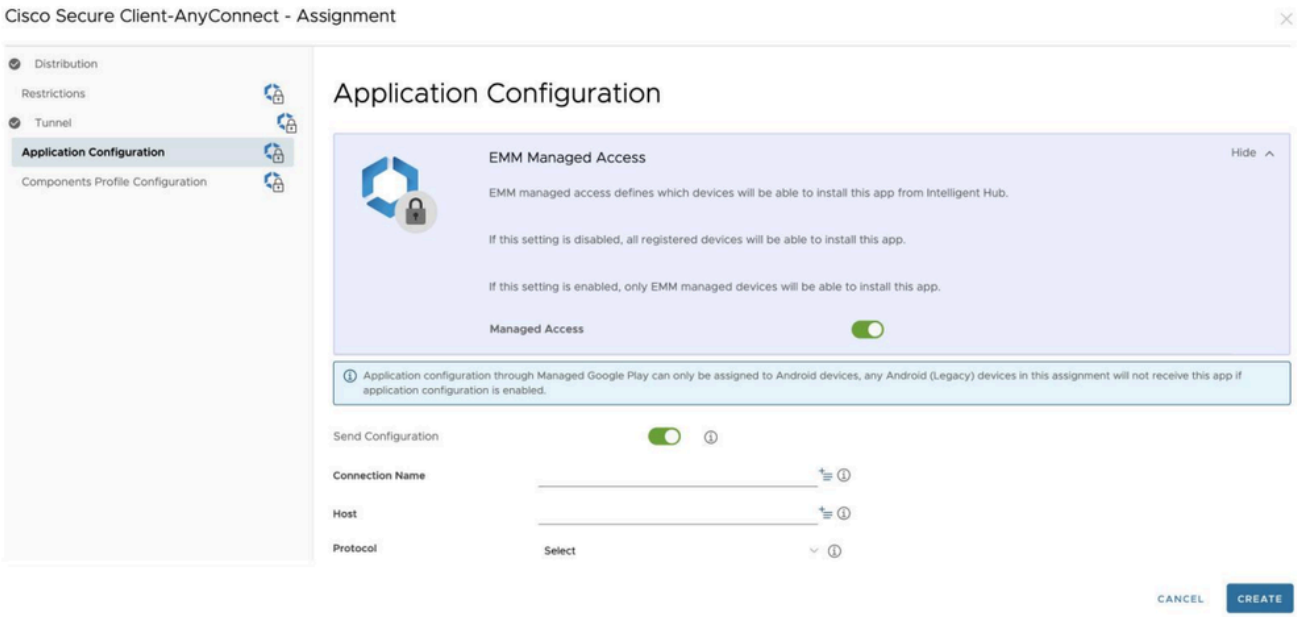



6. 应用配置：

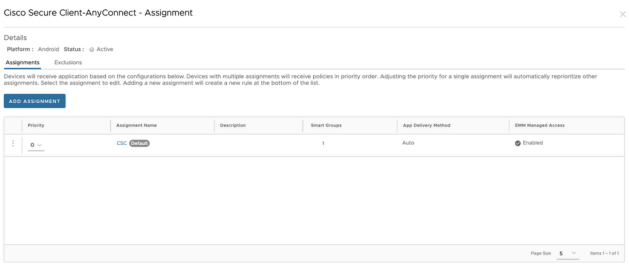
- 输入应用配置详细信息，例如Org ID和RegTokenfrom the Android Config File




downloaded from the Umbrella Dashboard。
- EnableAccept SEULA for Users以绕过手动SEULA接受。
- EnableAlways On VPN Mode for Umbrella Protection Only for seamless VPN management by Cisco Secure Client。
- 阻止用户创建新的VPN连接（将Host字段留空）。

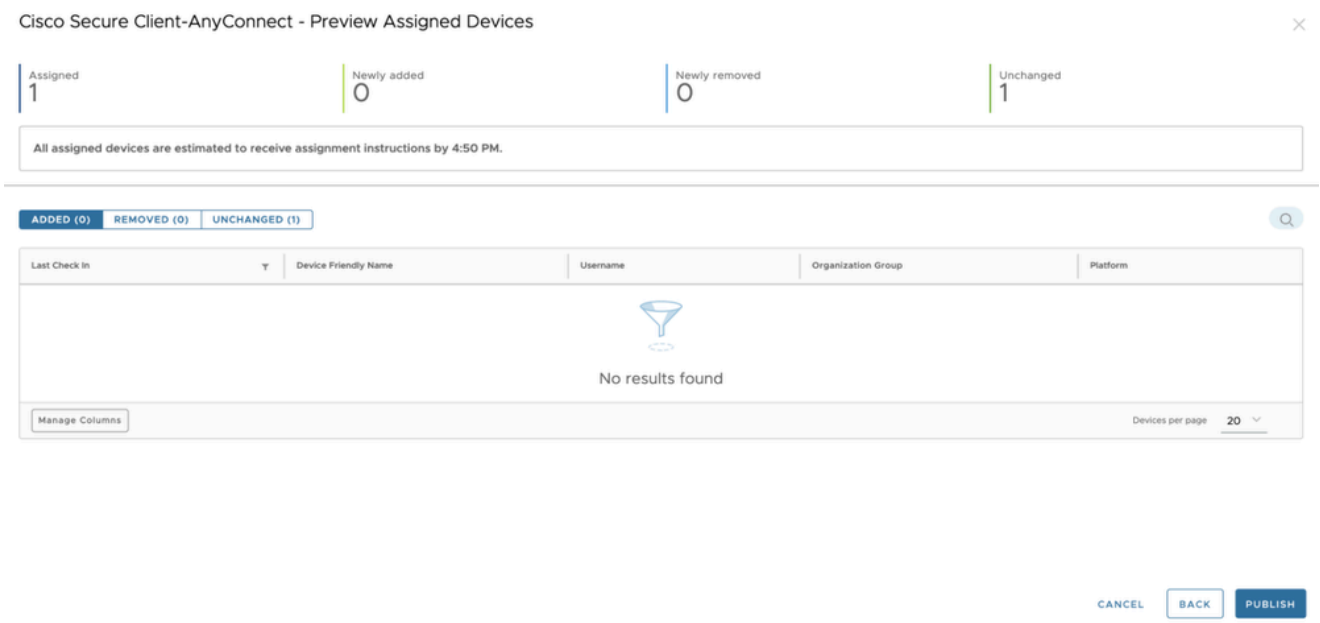


7. 保存并发布：




- 保存更改并发布Cisco Secure Client应用。







8. 推送Umbrella证书：

- 有关说明，请参阅：[将Umbrella证书推送到设备]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。