Implante um cliente seguro com proteção abrangente no Android via MDM automatizado

Contents

Introdução

Este documento descreve como implantar o Cisco Secure Client com o módulo Umbrella em dispositivos Android usando a implantação automatizada.

Informações de Apoio

Você pode implantar o Cisco Secure Client com o módulo Umbrella em dispositivos Android usando implantação automatizada por meio de soluções MDM, como Workspace One, Cisco Meraki ou Microsoft Intune. Esse processo permite a proteção transparente da camada DNS para o tráfego de aplicativos e navegadores, garante que a VPN sempre ativa esteja habilitada e elimina a intervenção do usuário para aceitação de VPN e SEULA.

Pré-requisitos

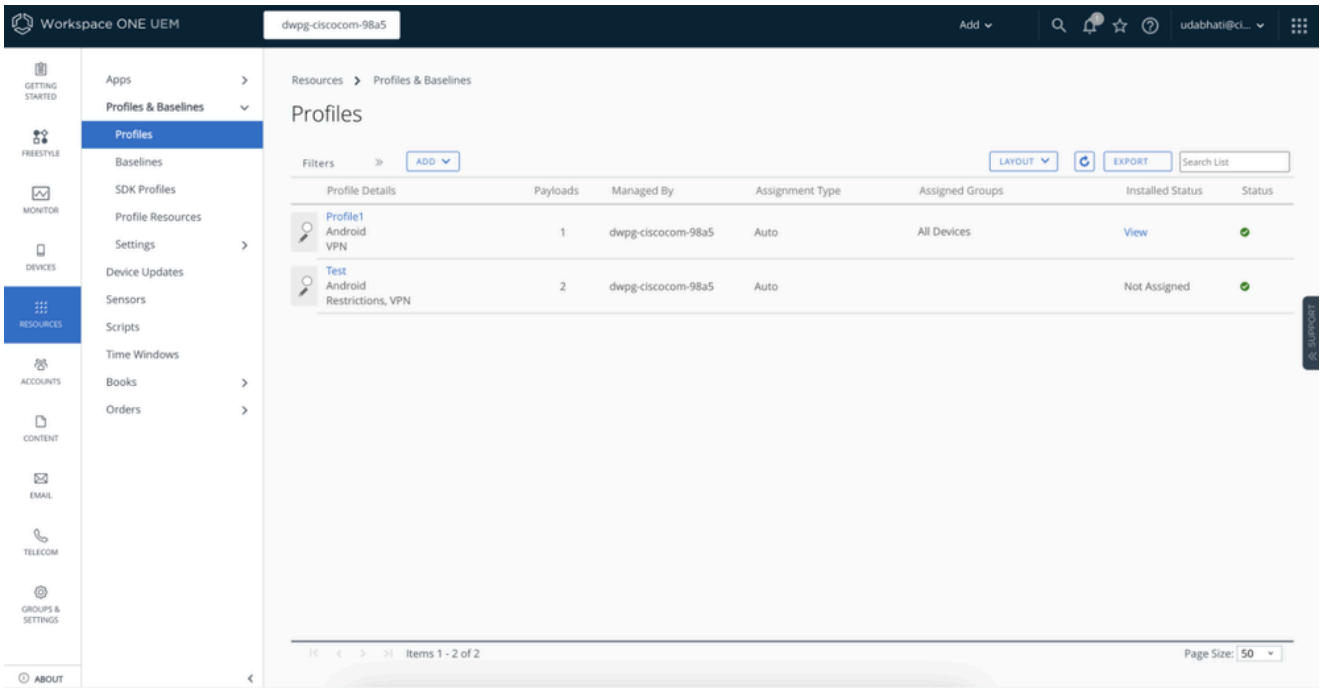
- Conclua o registro do Android Enterprise Mobility Management (EMM) e o registro do dispositivo com a criação do perfil de trabalho.
- O aplicativo MDM (Hub) deve estar visível no perfil de trabalho.
- Atribua e instale o Cisco Secure Client somente após publicar e instalar o perfil de VPN Always On no Intelligent Hub.

Etapas de Implantação

A. Crie o perfil de VPN Always On

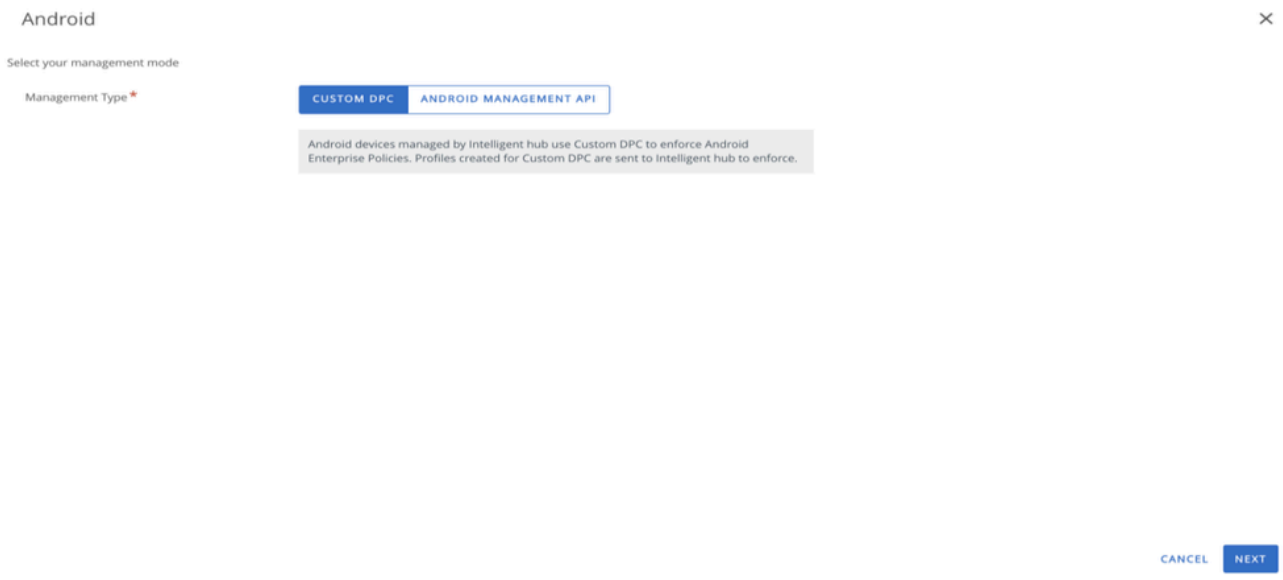
1. Navegue até Perfis:

    - Vá para Recursos > Perfis e Linhas de Base > Perfis.
    - Clique em Addpara criar um novo perfil.

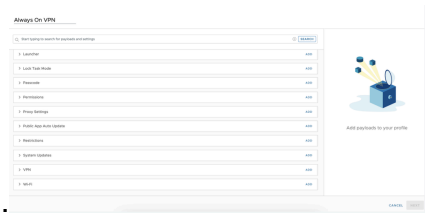


2. Configuração do perfil:

- Selecione Androidas na plataforma.
- Escolha o tipo de gerenciamento necessário.



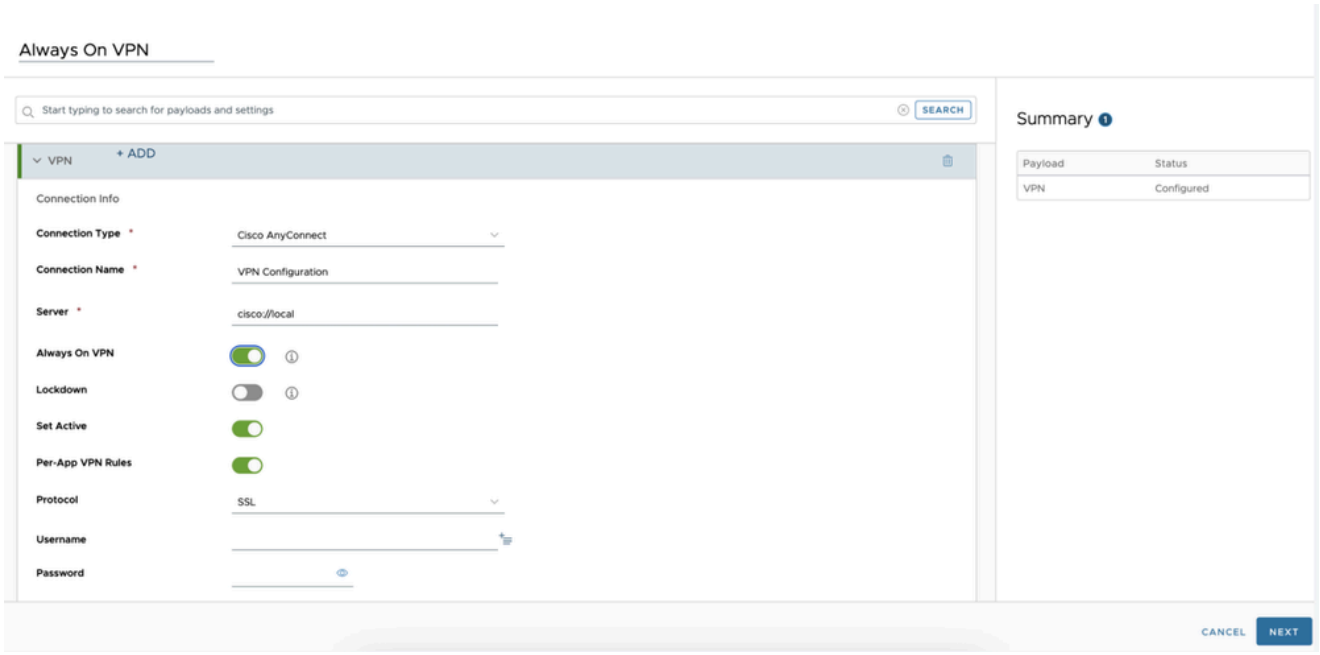
3. Configurar VPN:



- Na seção de perfil, vá paraVPN Settings e clique em Add.
- Preencha os campos obrigatórios:
  - Tipo de conexão:Cisco AnyConnect
  - Servidor:cisco://local

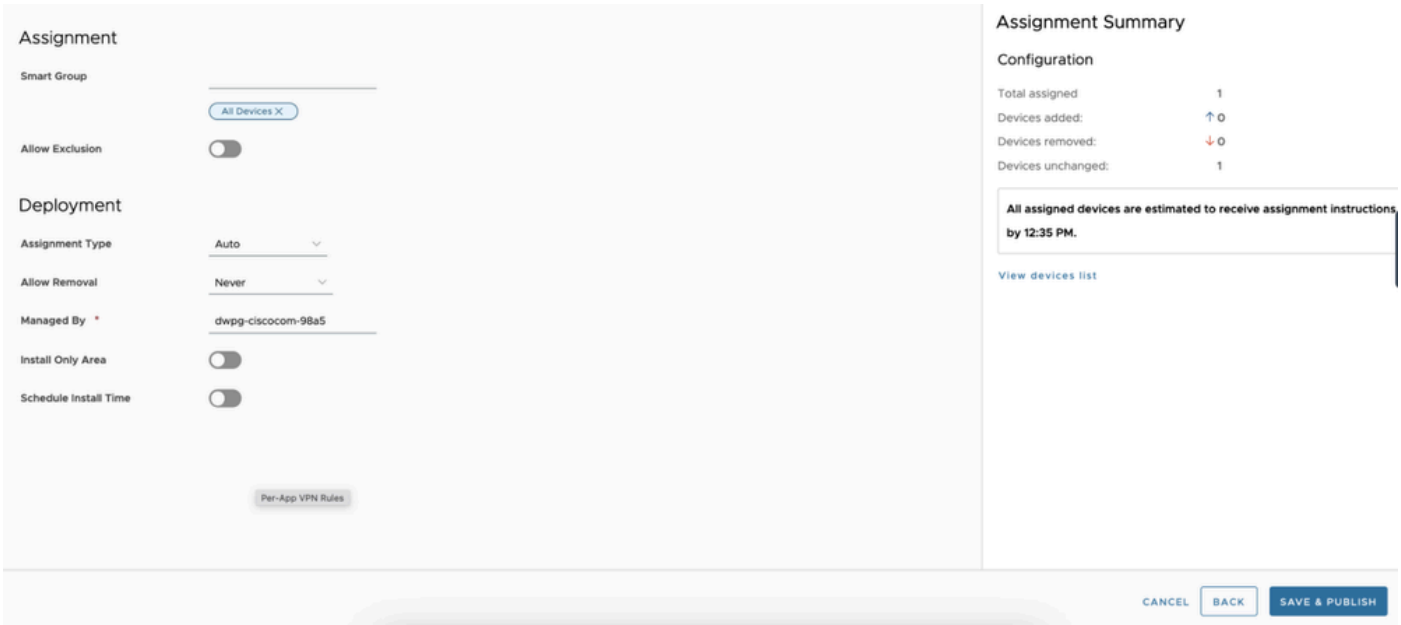
- Habilite a VPN Always On e configure outras propriedades conforme necessário.
- Habilitar Regras de VPN por Aplicativo.
- EnableSet Ativo.

- Clique em Avançar.



4. Atribuir perfil:

- Deixe o grupo inteligente vazio.
- Atribua o perfil aos dispositivos necessários.
- Selecione valores de implantação.
- Clique em Salvar e publicar.



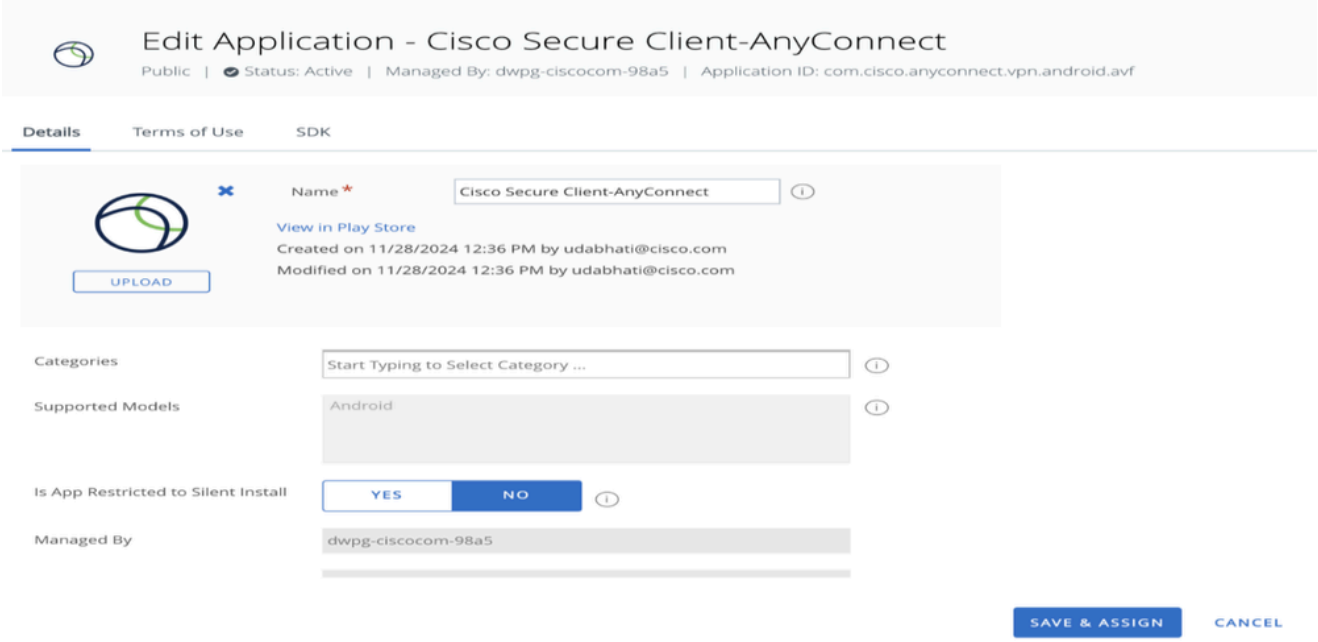
B. Atribua o aplicativo Cisco Secure Client

1. Adicione o aplicativo:

- Vá para Recursos > Nativo > Público.
- Adicione o Cisco Secure Client na Play Store se ainda não estiver disponível.

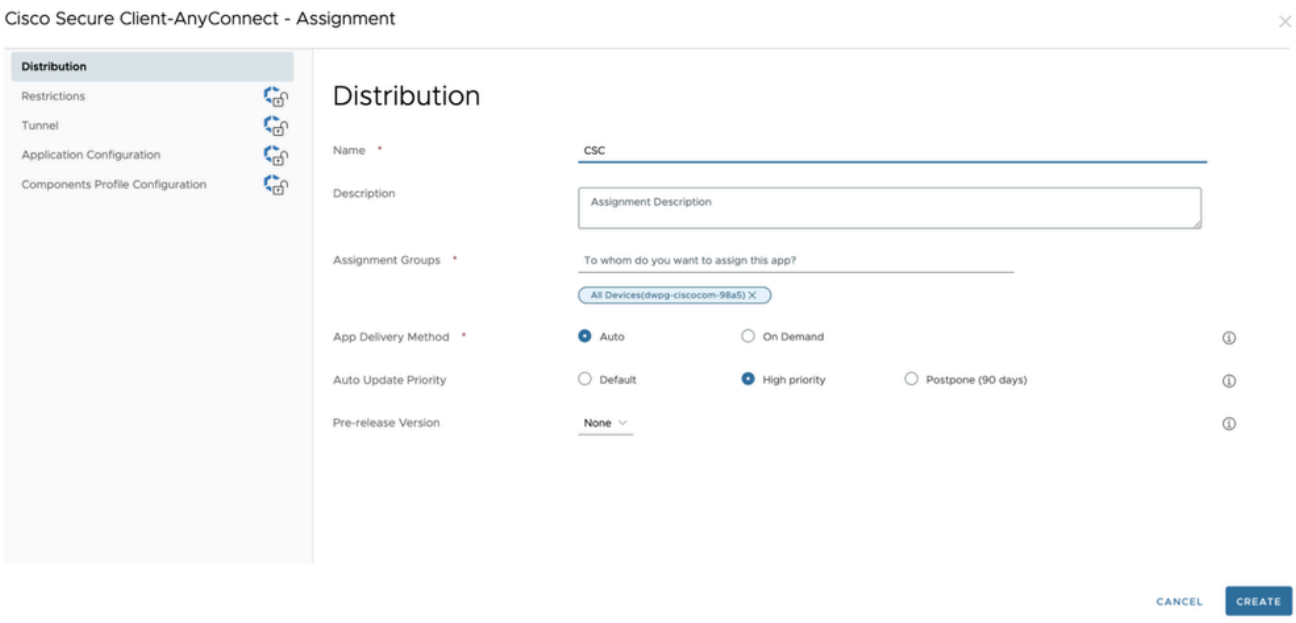
2. Atribuição de aplicativo:

- Selecione o aplicativo e preencha os valores necessários.
- Na seção de atribuição, crie uma nova atribuição.



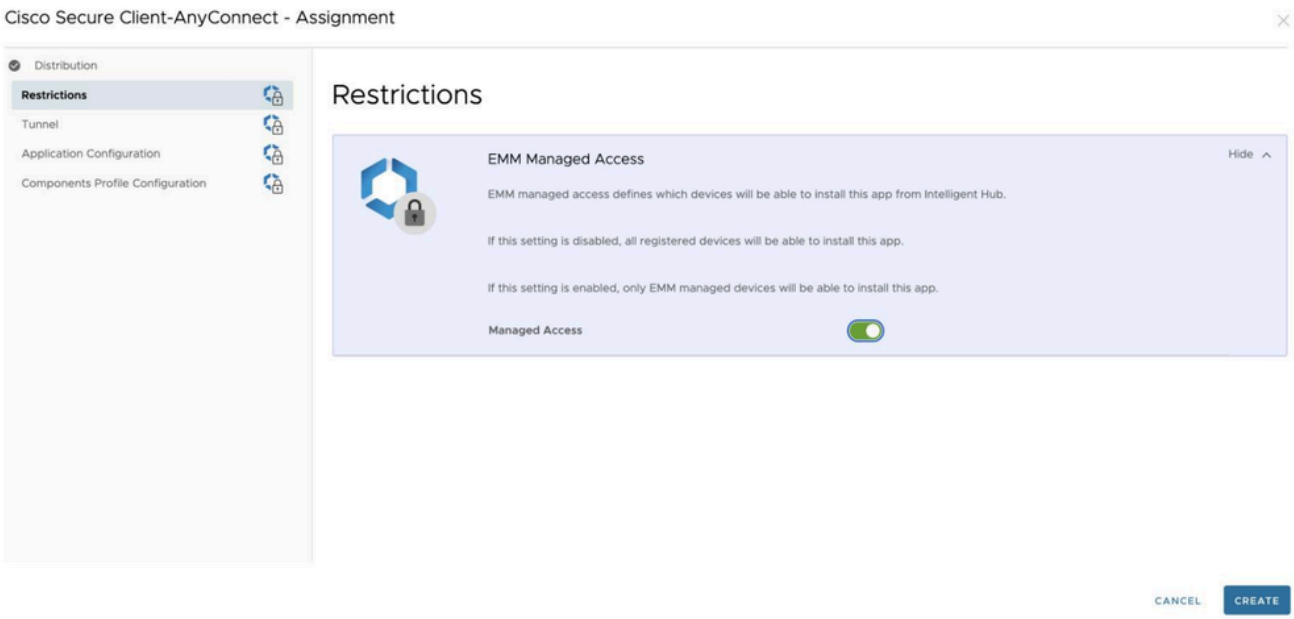
3. Configurar distribuição:

- Insira os detalhes na seção Distribuição.



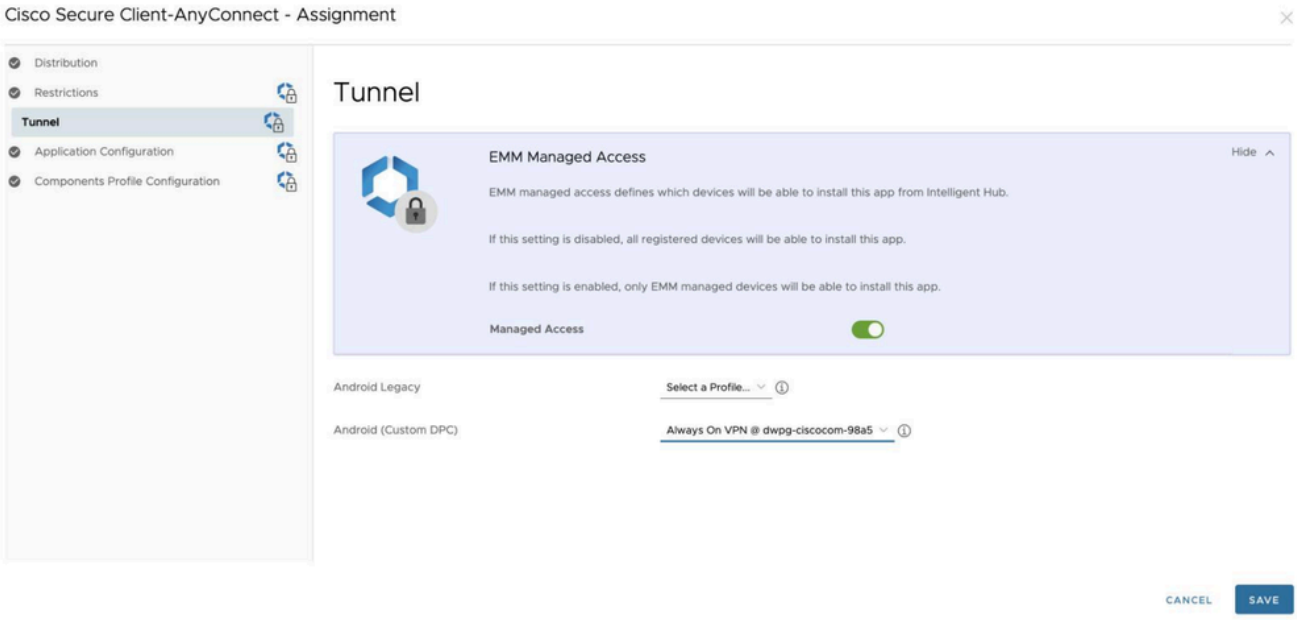
4. Habilitar acesso gerenciado:

- Na guia Restrictionsab, habiliteAcesso Gerenciado.



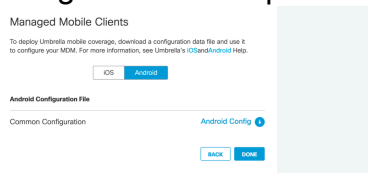
5. Selecionar perfil:

   - Na opçãode túnel, selecione o perfil criado anteriormente ('Always On VPN') em Android (DPC personalizado).



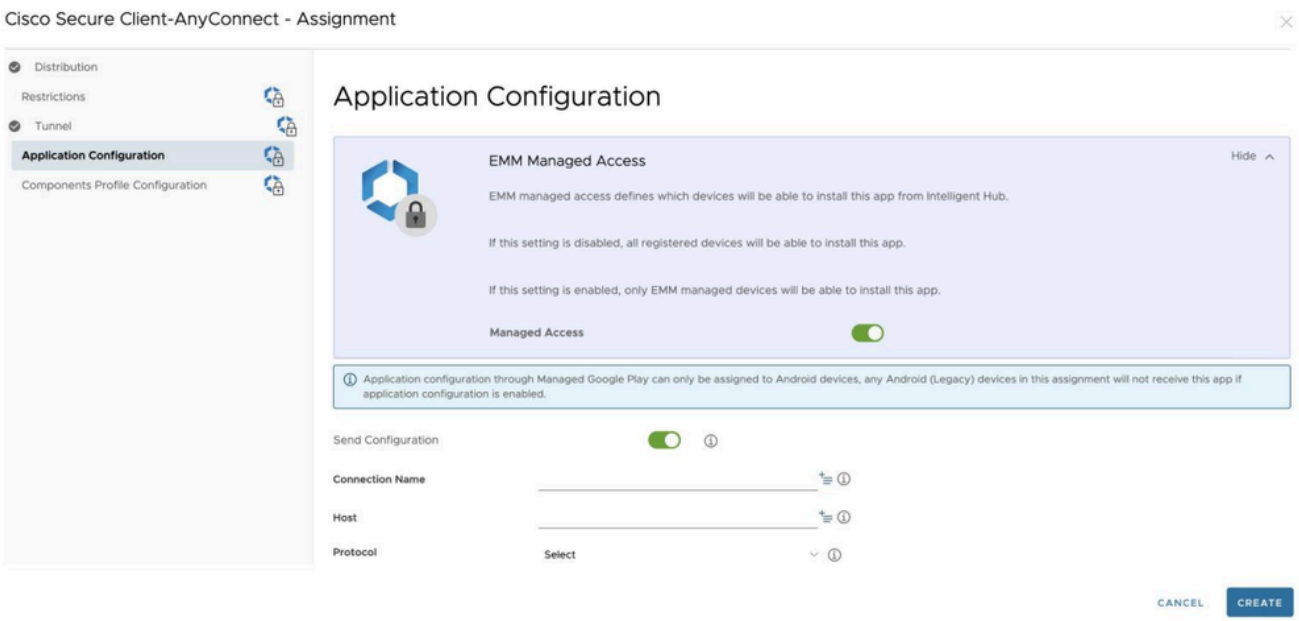
6. Configuração do aplicativo:

   - Insira detalhes de configuração do aplicativo, como Org IDandReg Token do arquivo

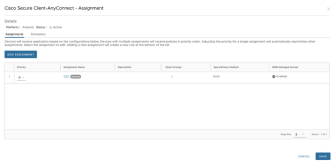


     de configuração do Android baixado do Umbrella Dashboard.
   - EnableAccept SEULA For Userpara ignorar a aceitação manual de SEULA.
   - Habilite o modo VPN sempre ativo somente para proteção de guarda-chuva para o gerenciamento de VPN transparente pelo Cisco Secure Client.

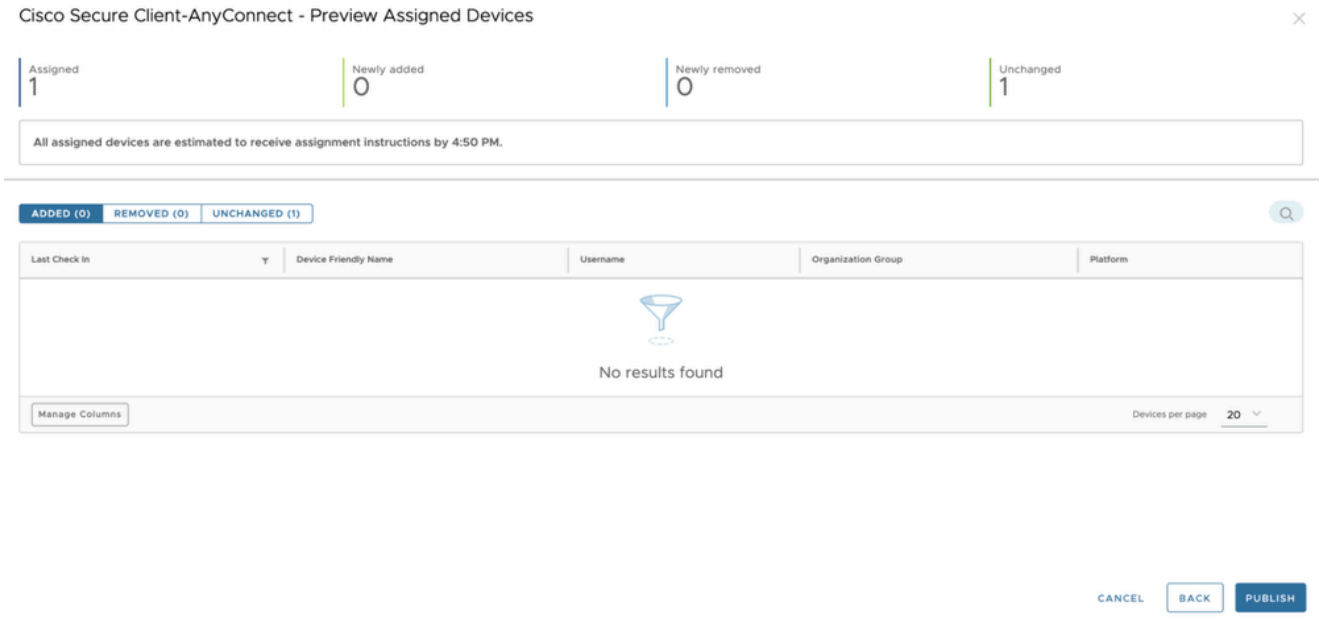
- Bloqueie a criação de novas conexões VPN pelos usuários (deixe o campo Host vazio).



7. Salvar e publicar:



- Salve as alterações e publique o aplicativo Cisco Secure Client.



8. Enviar o certificado do Umbrella:

- Para obter instruções, consulte: [Enviar o certificado do Umbrella para os dispositivos]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.