

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

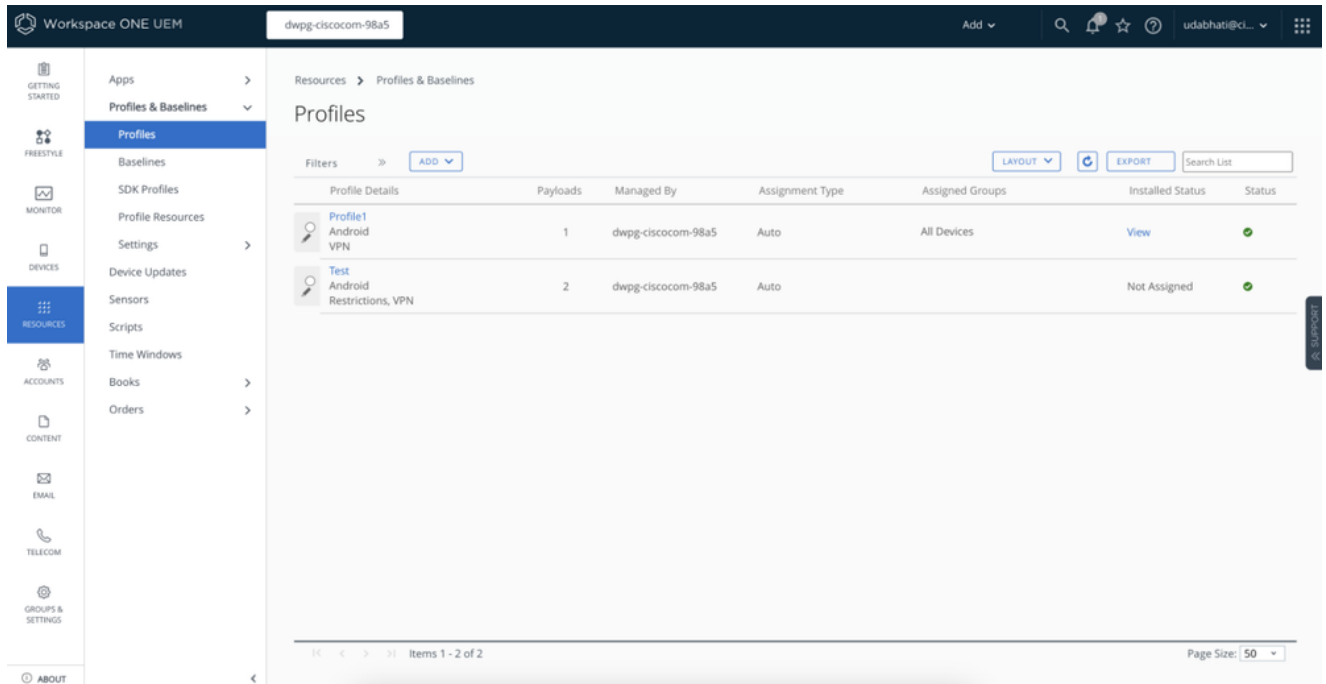
- Conclua o registro do Android Enterprise Mobility Management (EMM) e o registro do dispositivo com a criação do perfil de trabalho.
- O aplicativo MDM (Hub) deve estar visível no perfil de trabalho.
- Atribua e instale o Cisco Secure Client somente após publicar e instalar o perfil de VPN Always On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

Etapas de Implantação

A. Crie o perfil de VPN Always On

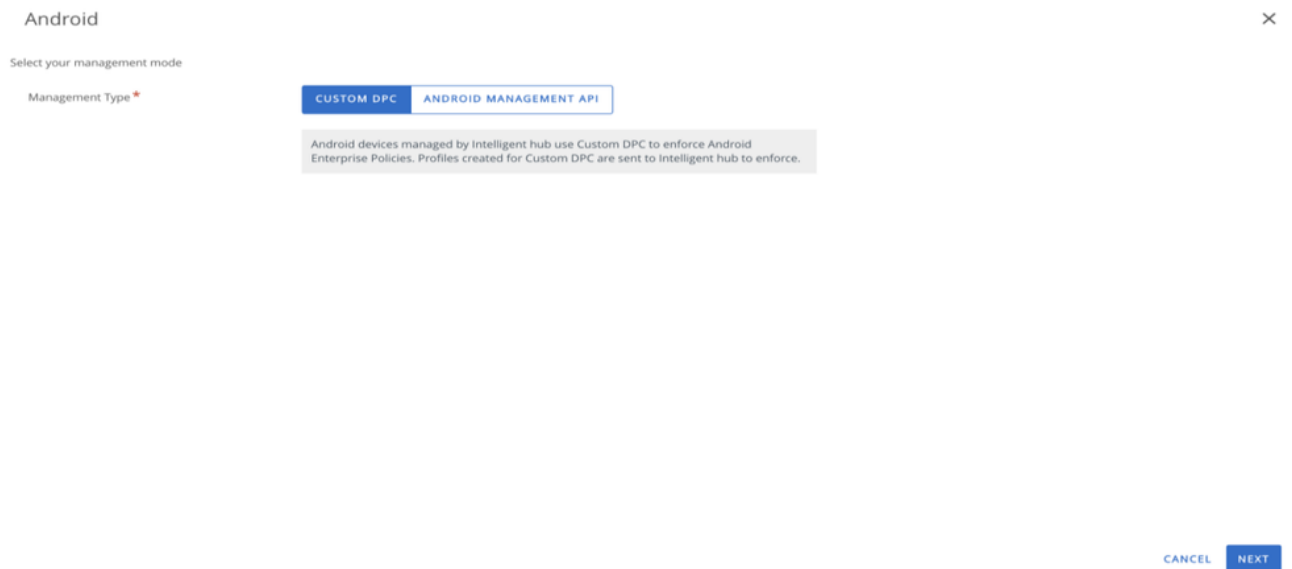
1. Navegue até Perfis:

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



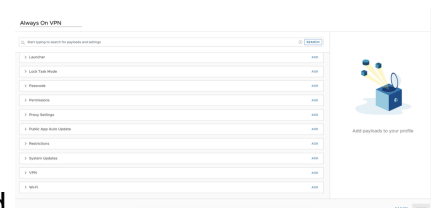
2. Configuração do perfil:

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



3. Configurar VPN:

- Na seção de perfil, vá para VPN 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.

Always On VPN

Start typing to search for payloads and settings

VPN + ADD

Connection Info

Connection Type * Cisco AnyConnect

Connection Name * VPN Configuration

Server * cisco://local

Always On VPN ☒

Lockdown ☐

Set Active ☒

Per-App VPN Rules ☒

Protocol SSL

Username

Password

Summary

Payload	Status
VPN	Configured

CANCEL NEXT

4. Atribuir perfil:

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

Assignment

Smart Group

All Devices X

Allow Exclusion ☐

Deployment

Assignment Type Auto

Allow Removal Never

Managed By * dwpg-ciscocom-98a5

Install Only Area ☐

Schedule Install Time ☐

Per-App VPN Rules

Assignment Summary

Configuration

Total assigned 1

Devices added: 0

Devices removed: 0

Devices unchanged: 1

All assigned devices are estimated to receive assignment instructions, by 12:35 PM.

View devices list

CANCEL BACK SAVE & PUBLISH

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.

Edit Application - Cisco Secure Client-AnyConnect
Public | Status: Active | Managed By: dwpj-ciscocom-98a5 | Application ID: com.cisco.anyconnect.vpn.android.avf

Details | Terms of Use | SDK

Name * Cisco Secure Client-AnyConnect ⓘ

[View in Play Store](#)
Created on 11/28/2024 12:36 PM by udabhati@cisco.com
Modified on 11/28/2024 12:36 PM by udabhati@cisco.com

Categories Start Typing to Select Category ... ⓘ

Supported Models Android ⓘ

Is App Restricted to Silent Install YES NO ⓘ

Managed By dwpj-ciscocom-98a5

SAVE & ASSIGN **CANCEL**

3. Configurar distribuição:

- Insira os detalhes na seção Distribuição.

Cisco Secure Client-AnyConnect - Assignment X

Distribution

Name * CSC

Description Assignment Description

Assignment Groups * To whom do you want to assign this app?
All Devices(dwpj-ciscocom-98a5) X

App Delivery Method * Auto On Demand ⓘ

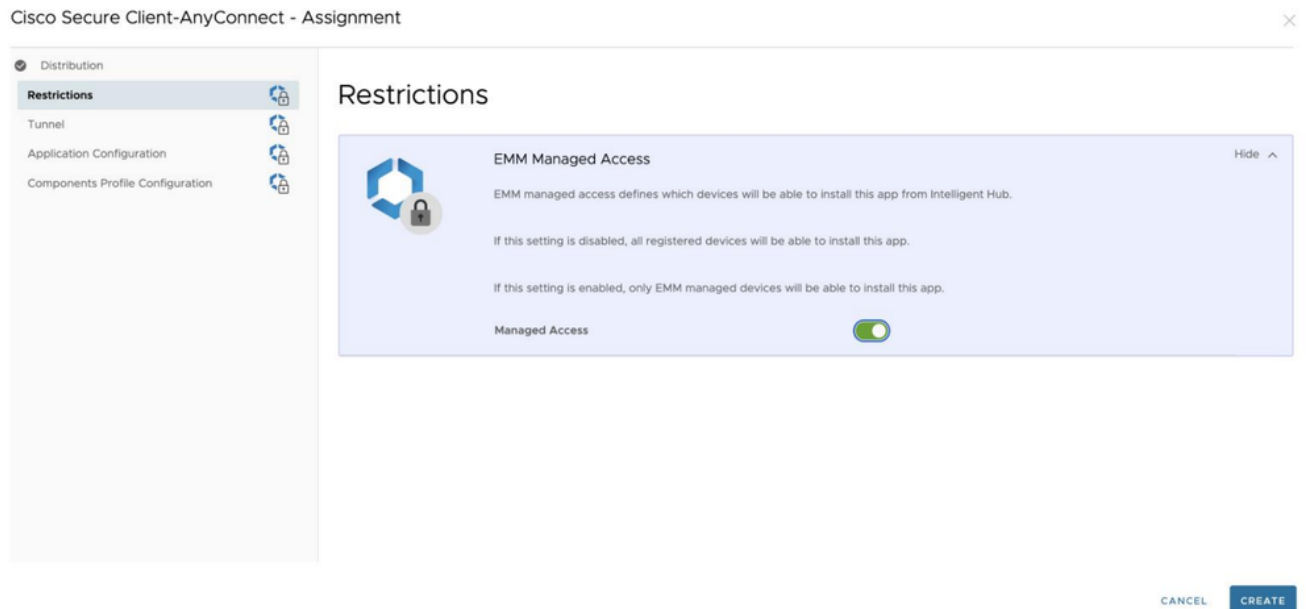
Auto Update Priority Default High priority Postpone (90 days) ⓘ

Pre-release Version None ⓘ

CANCEL **CREATE**

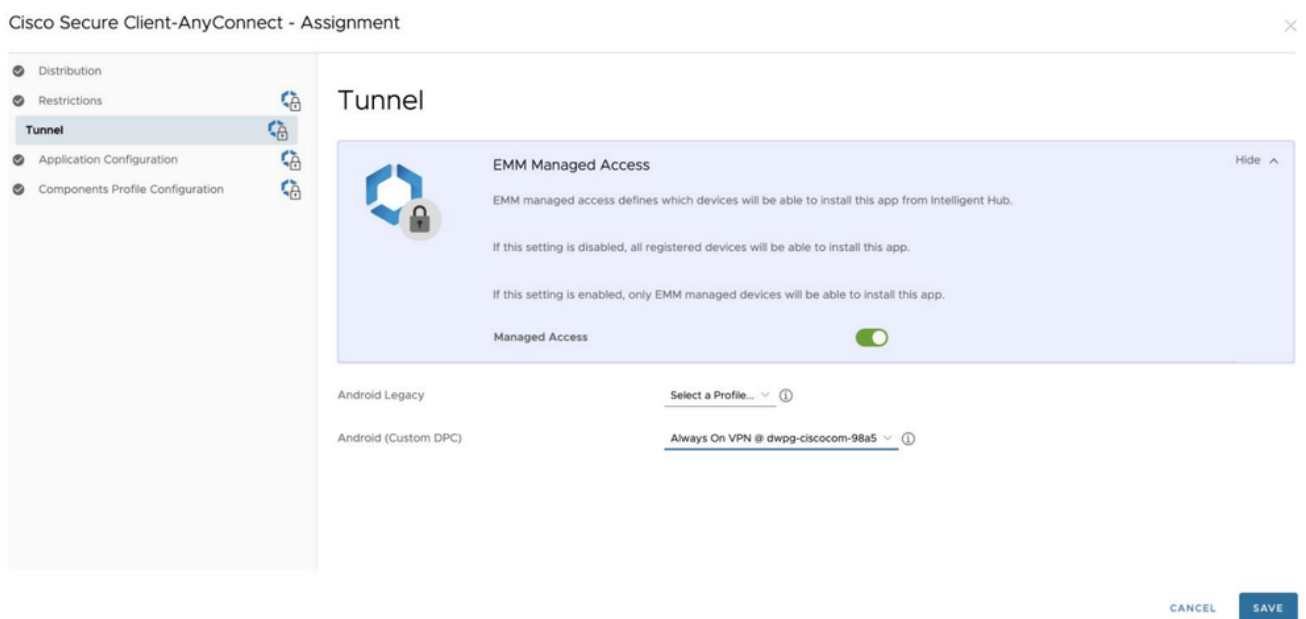
4. Habilitar acesso gerenciado:

- Na guia Restrictionsab, habiliteAcesso Gerenciado.



5. Selecionar perfil:

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

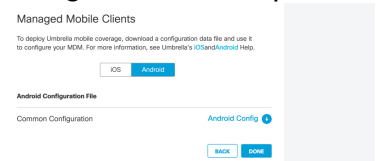


6. Configuração do aplicativo:

- Insira detalhes de configuração do aplicativo, como Org ID and Reg Token do arquivo

de configuração do Android baixado do Umbrella Dashboard.

- EnableAccept SEULA For User para 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).

Cisco Secure Client-AnyConnect - Assignment

- Distribution
- Restrictions
- Tunnel
- Application Configuration**
- Components Profile Configuration

Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access ☒

Application configuration through Managed Google Play can only be assigned to Android devices, any Android (Legacy) devices in this assignment will not receive this app if application configuration is enabled.

Send Configuration ☒ ⓘ

Connection Name ⓘ

Host ⓘ

Protocol Select ⓘ

CANCEL CREATE

7. Salvar e publicar:

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

Cisco Secure Client-AnyConnect - Preview Assigned Devices

Assigned **1**

Newly added **0**

Newly removed **0**

Unchanged **1**

All assigned devices are estimated to receive assignment instructions by 4:50 PM.

ADDED (0) REMOVED (0) UNCHANGED (1)

Last Check In	Device Friendly Name	Username	Organization Group	Platform
No results found				

Manage Columns

Devices per page **20**

CANCEL BACK PUBLISH

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.