

Habilitar Aceitação Automática para VPN e SEULA no Cliente Seguro no Android via MDM

Contents

Introdução

Este documento descreve como configurar o Cisco Secure Client para aceitar automaticamente solicitações de VPN e SEULA para gerenciar pop-ups.

Overview

Você pode configurar o Cisco Secure Client para iniciar automaticamente e aceitar prompts de pop-up de VPN e SEULA (Contrato de Licença de Usuário Final de Software) sem interação do usuário em dispositivos Android usando soluções MDM, como Cisco Meraki e Microsoft Intune. Ao habilitar a VPN sempre ativa e definir a propriedade de aceitação SEULA em seu MDM, você elimina a necessidade de os usuários responderem à conexão VPN e aos pop-ups SEULA durante a implantação inicial.



Note: Para implantação automatizada com o Workspace One, consulte nossa documentação: [Implante o cliente Android: VMware Workspace ONE](#)

Configurações que afetam o lançamento inicial

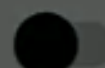
1. Solicitação de conexão VPN para Umbrella:

- O dispositivo deve aceitar uma solicitação de conexão para que a proteção Umbrella seja iniciada.
- Você pode aceitar isso automaticamente ao habilitar Always-OnVPN em sua configuração de MDM.



AnyConnect VPN

Disconnected



Connection request

Cisco Secure Client wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

 appears at the top of your screen when VPN is active.

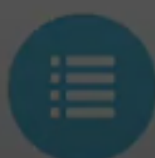
Cancel

OK



Checking connection state.

Please wait as this may take up to 30 seconds.



Details

Umbrella Statistics

user para aceitar automaticamente o contrato SEULA. Isso é independente da configuração da VPN Always-On.

The screenshot shows the Cisco Meraki Systems Manager configuration interface. On the left is a sidebar with navigation options: Network, MDM, Systems Manager, Insight, and Organization. The main area displays configuration settings for Umbrella. The settings are organized into sections with keys, types, and values. The 'accept_seula_for_user' key is highlighted with a red box. Below the settings is a 'Save' button.

Key	Type	Value
umbrella_org_id	Text	The organization id to which customer belongs and it is as seen in the configuration file downloaded from Cisco Umbrella dashboard.
umbrella_reg_token	Text	Umbrella Registration Token The unique regToken issued to a organization and the value is as seen in the configuration file downloaded from Cisco Umbrella dashboard.
umbrella_user_identity	Device: Name	Umbrella Identity (Mandatory for Umbrella) This is the user identity which is used for umbrella registration. e.g. iPad 1003
vpn_always_on_umbrella_only	Boolean	Enable Always-On VPN Mode for Umbrella Protection Only (Only applicable if using Umbrella) If set to true, always-on VPN will only apply Umbrella protection. If set to false, always-on VPN will apply to both Umbrella and remote access. True
accept_seula_for_user	Boolean	Accept SEULA for Users (Optional)- This will hide SEULA prompt that is normally displayed once after first install of the app. Use of this Cisco product ("Cisco Technology") is governed by the Cisco End User License Agreement and the Cisco Supplemental End User License Agreement... True

Importante: Se você iniciar o aplicativo antes de enviar a configuração de VPN sempre ativa, a janela pop-up de solicitação de conexão VPN ainda será exibida. Certifique-se de que a VPN Always-On esteja configurada e enviada por push antes da primeira inicialização para evitar isso.

Configurar a Aceitação Automática no Microsoft Intune

1. Crie um perfil de VPN e um perfil de restrições de dispositivo com a configuração de VPN sempre ativada.
2. Atribua esses perfis aos seus grupos-alvo.
3. Selecione um cliente VPN que suporte Always-On. Você pode escolher "Cisco AnyConnect" ou especificar um cliente "Personalizado" inserindo a ID do pacote do aplicativo na Google Play Store como "com.cisco.anyconnect.vpn.android.avf" (aplicativo Cisco AnyConnect VPN especificamente para dispositivos Android).

Home > Apps > App configuration policies > Cisco Secure Client Profile

Cisco Secure Client Profile | Properties

Search

Overview

Manage

Properties

Monitor

Device install status

Basics Edit

Name: Cisco Secure Client Profile

Description: Cisco Secure Client Profile

Device enrollment type: Managed devices

Platform: Android Enterprise

Profile Type: All Profile Types

Targeted app: Cisco Secure Client-AnyConnect

Settings Edit

Permissions: Not configured

Configuration Settings

Configuration key	Value type	Configuration value
Umbrella Identity	string	{{username}}
Enable Always-On VPN Mode for Umbrella Protection Only	bool	true
Umbrella Registration Token	string	
Umbrella Organization Id	string	
Accept SEULA for Users	bool	true

Connected apps: Enabled

Assignments Edit

Included groups

Group	Filter	Filter mode
All users	None	None
All devices	None	None

Excluded groups

Group
Android

4. Defina a propriedade de aceitação SEULA e a VPN sempre ativa.

Home > Devices | Android > Android | Configuration profiles >

Device restrictions

Android Enterprise

1 Basics 2 Configuration settings 3 Assignments 4 Review + create

Work profile settings

Password

System security

Connectivity

Always-on VPN ⓘ

Enable

Not configured

VPN client ⓘ

Cisco AnyConnect

Lockdown mode ⓘ

Enable

Not configured

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Devices | Android > Android | Configuration profiles > Always-On VPN >

Device restrictions

Android Enterprise

1 Basics

2 Review + save

Name *

Always-On VPN

Description

Platform

Android Enterprise

Profile type

Device restrictions

Properties

Basics [Edit](#)

Name	Always-On VPN
Description	No Description
Platform	Android Enterprise
Profile type	Device restrictions

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
All Users	None	None

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.