

Activer l'acceptation automatique pour VPN et SEULA dans le client sécurisé sur Android via MDM

Table des matières

Introduction

Ce document décrit comment configurer Cisco Secure Client pour accepter automatiquement les invites VPN et SEULA pour gérer les fenêtres publicitaires intempestives.

Aperçu

Vous pouvez configurer Cisco Secure Client pour qu'il se lance automatiquement et accepte les invites contextuelles essentielles VPN et SEULA (Software End User License Agreement) sans interaction de l'utilisateur sur les appareils Android utilisant des solutions MDM telles que Cisco Meraki et Microsoft Intune. En activant Always-On VPN et en définissant la propriété d'acceptation SEULA dans votre MDM, vous éliminez le besoin pour les utilisateurs de répondre à la connexion VPN et aux fenêtres contextuelles SEULA lors du déploiement initial.



Remarque : Pour un déploiement sans intervention avec Workspace One, consultez notre documentation : [Déployez le client Android : VMware Workspace ONE](#)

Paramètres ayant un impact sur le lancement initial

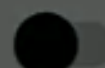
1. Demande de connexion VPN pour Umbrella :

- Le périphérique doit accepter une demande de connexion pour que la protection Umbrella démarre.
- Vous pouvez l'accepter automatiquement en activant **Always-On VPN** dans votre configuration 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.

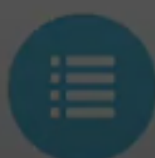
Cancel

OK



Checking connection state.

Please wait as this may take up to 30 seconds.



Details

Umbrella Statistics

userpour accepter automatiquement le contrat SEULA. Ce paramètre est indépendant du paramètre VPN Always-On.

The screenshot shows the Meraki Systems Manager interface. On the left is a navigation menu with 'Network MDM', 'Systems Manager', 'Insight', and 'Organization'. The main area displays configuration settings for VPN. The settings are organized into sections with 'Key', 'Type', and 'Value' fields. The 'vpn_always_on_umbrella_only' setting is a Boolean toggle set to 'On'. The 'accept_seula_for_user' setting is a Boolean toggle set to 'On' and is highlighted with a red box. At the bottom, there are 'Cancel' and 'Save' buttons.

Key	Type	Value
umbrella_org_id	Text	
umbrella_reg_token	Text	
umbrella_user_identity	Device: Name	e.g. iPad 1003
vpn_always_on_umbrella_only	Boolean	On
accept_seula_for_user	Boolean	On

Important : Si vous lancez l'application avant de pousser la configuration VPN Always-On, la fenêtre contextuelle de demande de connexion VPN s'affiche toujours. Assurez-vous que le VPN Always-On est configuré et activé avant le premier lancement pour éviter cela.

Configurer l'acceptation automatique dans Microsoft Intune

1. Créez un profil VPN et un profil de restrictions de périphérique avec le paramètre VPN Always-On activé.
2. Attribuez ces profils à vos groupes cibles.
3. Sélectionnez un client VPN qui prend en charge la fonctionnalité Always-On. Vous pouvez choisir « Cisco AnyConnect » ou spécifier un client « personnalisé » en entrant l'ID de package de l'application dans le magasin Google Play sous la forme « com.cisco.anyconnect.vpn.android.avf » (application VPN Cisco AnyConnect spécifiquement pour les appareils 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. Définissez la propriété d'acceptation SEULA et le VPN Always-On.

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.