

Aktivieren Sie Auto-Accept für VPN und SEULA in Secure Client auf Android über MDM.

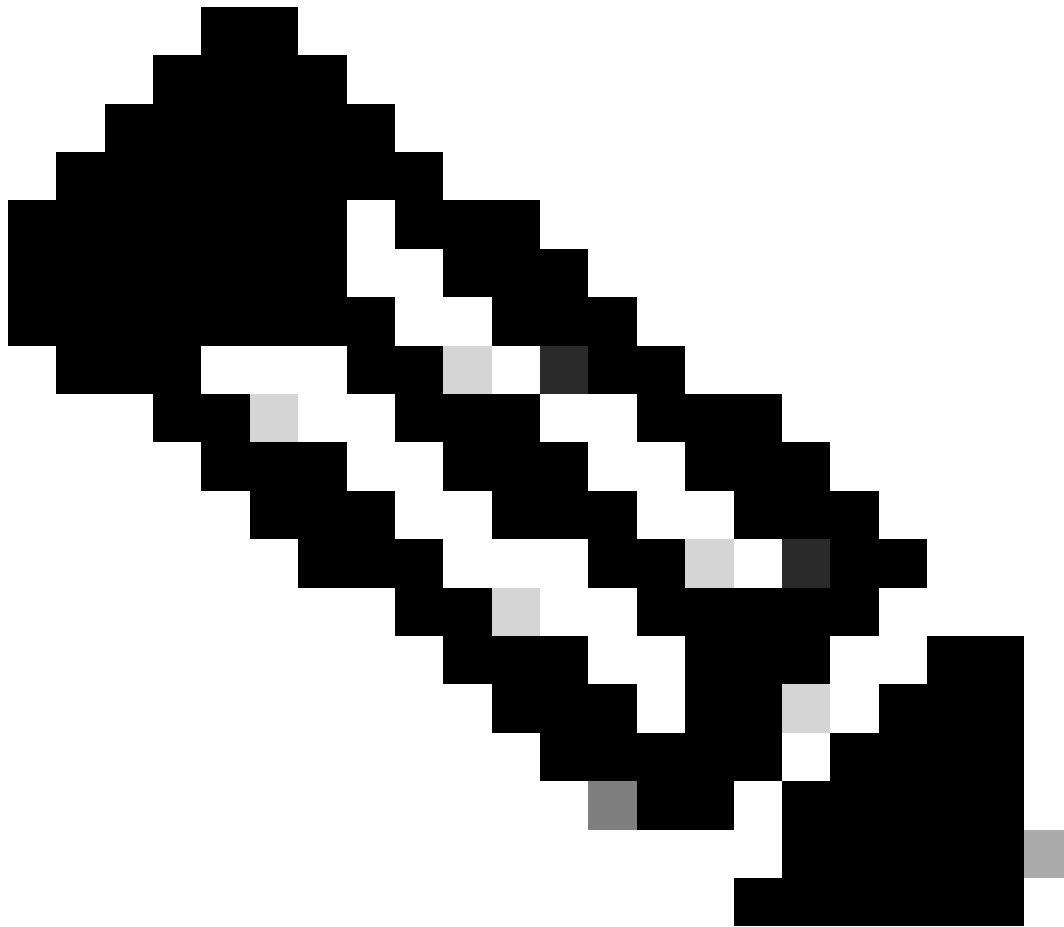
Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Cisco Secure Client so konfigurieren, dass VPN- und SEULA-Aufforderungen zur Verwaltung von Popup-Fenstern automatisch akzeptiert werden.

Überblick

Sie können den Cisco Secure Client so konfigurieren, dass er automatisch gestartet wird und wichtige VPN- und SEULA-Popup-Meldungen (Software End User License Agreement) ohne Benutzereingriff auf Android-Geräten akzeptiert, die MDM-Lösungen wie Cisco Meraki und Microsoft Intune verwenden. Durch die Aktivierung von Always-On VPN und die Einstellung der SEULA-Akzeptanz im MDM müssen Benutzer nicht mehr auf VPN-Verbindungen und SEULA-Popups bei der Erstbereitstellung reagieren.



Anmerkung: Informationen zur Bereitstellung ohne Benutzereingriffe mit Workspace One finden Sie in unserer Dokumentation: [Bereitstellen des Android-Clients: VMware Workspace ONE](#)

Einstellungen, die sich auf den ersten Start auswirken

1. VPN-Verbindungsanforderung für Umbrella:

- Das Gerät muss eine Verbindungsanfrage akzeptieren, damit Umbrella Protection gestartet werden kann.
- Sie können dies automatisch akzeptieren, indem Sie in Ihrer MDM-Konfiguration Always-On-VPN aktivieren.



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

userto auto-accept the SEULA agreement. Dies ist unabhängig von der Always-On-VPN-Einstellung.

The screenshot shows the Cisco Meraki Systems Manager configuration interface. On the left is a sidebar with navigation options: Network, MDM, Systems Manager (selected), Insight, and Organization. The main area displays configuration settings for Umbrella. The settings are organized into sections, each with a 'Key' dropdown, a 'Type' dropdown, and a 'Value' field. The 'accept_seula_for_user' key is highlighted with a red box. At the bottom, there are 'Cancel' and 'Save' buttons.

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

Wichtig: Wenn Sie die App starten, bevor Sie die Always-On-VPN-Konfiguration übertragen, wird das Popup-Fenster "VPN Connection Request" angezeigt. Stellen Sie sicher, dass das stets verfügbare VPN vor dem ersten Start konfiguriert und per Push bereitgestellt wird, um dies zu verhindern.

Konfigurieren von Auto-Accept in Microsoft Intune

1. Erstellen Sie ein VPN-Profil und ein Profil mit Geräteeinschränkungen, wobei die VPN-Einstellung "Always-On" aktiviert ist.
2. Weisen Sie diese Profile Ihren Zielgruppen zu.
3. Wählen Sie einen VPN-Client aus, der Always-On unterstützt. Sie können entweder "Cisco AnyConnect" wählen oder einen "Custom" Client angeben, indem Sie die Paket-ID der App im Google Play Store als "com.cisco.anyconnect.vpn.android.avf" (Cisco AnyConnect VPN-Anwendung speziell für Android-Geräte) eingeben.

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. Legen Sie die SEULA-Akzeptanzeigenschaft und das Always-On-VPN fest.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.