

Abilita accettazione automatica per VPN e SEULA in Secure Client su Android tramite MDM

Sommario

Introduzione

Questo documento descrive come configurare Cisco Secure Client in modo che accetti automaticamente le richieste VPN e SEULA per gestire i popup.

Panoramica

È possibile configurare Cisco Secure Client in modo che si avvii automaticamente e accetti le richieste popup VPN e SEULA (Software End User License Agreement) essenziali senza interazione dell'utente sui dispositivi Android con soluzioni MDM come Cisco Meraki e Microsoft Intune. Abilitando la VPN Always-On e impostando la proprietà di accettazione SEULA in MDM, si elimina la necessità per gli utenti di rispondere alla connessione VPN e ai popup SEULA durante la distribuzione iniziale.



Nota: Per l'installazione zero-touch con Workspace One, vedere la documentazione:
[Distribuire il client Android: VMware Workspace ONE](#)

Impostazioni che influiscono sul lancio iniziale

1. Richiesta di connessione VPN per Umbrella:

- Per avviare la protezione Umbrella, il dispositivo deve accettare una richiesta di connessione.
- È possibile accettare automaticamente questa condizione abilitando Always-On VPN nella configurazione 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.

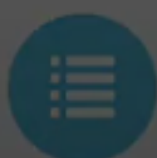
Cancel

OK



Checking connection state.

Please wait as this may take up to 30 seconds.



Details

Umbrella Statistics

userper accettare automaticamente il contratto SEULA. Ciò è indipendente dall'impostazione Always-On VPN.

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 VPN. The settings are organized into sections with 'Key', 'Type', and 'Value' fields. The 'umbrella_org_id' key is set to 'Text'. The 'umbrella_reg_token' key is set to 'Text'. The 'umbrella_user_identity' key is set to 'Device: Name' with the value 'e.g. iPad 1003'. The 'vpn_always_on_umbrella_only' key is set to 'Boolean' with the value 'True'. The 'accept_seula_for_user' key is set to 'Boolean' with the value 'True'. The 'accept_seula_for_user' key is highlighted with a red box. At the bottom of the configuration area 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	True
accept_seula_for_user	Boolean	True

Importante: Se si avvia l'app prima di eseguire il push della configurazione VPN Always-On, il popup della richiesta di connessione VPN continuerà a essere visualizzato. Verificare che la VPN Always-On sia configurata e sottoposta a push prima del primo avvio per evitare questa condizione.

Configurazione dell'accettazione automatica in Microsoft Intune

1. Creare un profilo VPN e un profilo di restrizioni dispositivo con l'impostazione VPN sempre attiva abilitata.
2. Assegnare questi profili ai gruppi target.
3. Selezionare un client VPN che supporti Always-On. È possibile scegliere "Cisco AnyConnect" o specificare un client "personalizzato" immettendo l'ID pacchetto dell'app nello store Google Play come "com.cisco.anyconnect.vpn.android.avf" (applicazione VPN Cisco AnyConnect specifica per dispositivi 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. Impostare la proprietà di accettazione SEULA e la VPN Always-On.

Home > Devices | Android > Android | Configuration profiles >

Device restrictions

Android Enterprise

✓ 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).