# Enable Auto-Accept for VPN and SEULA in Secure Client on Android via MDM

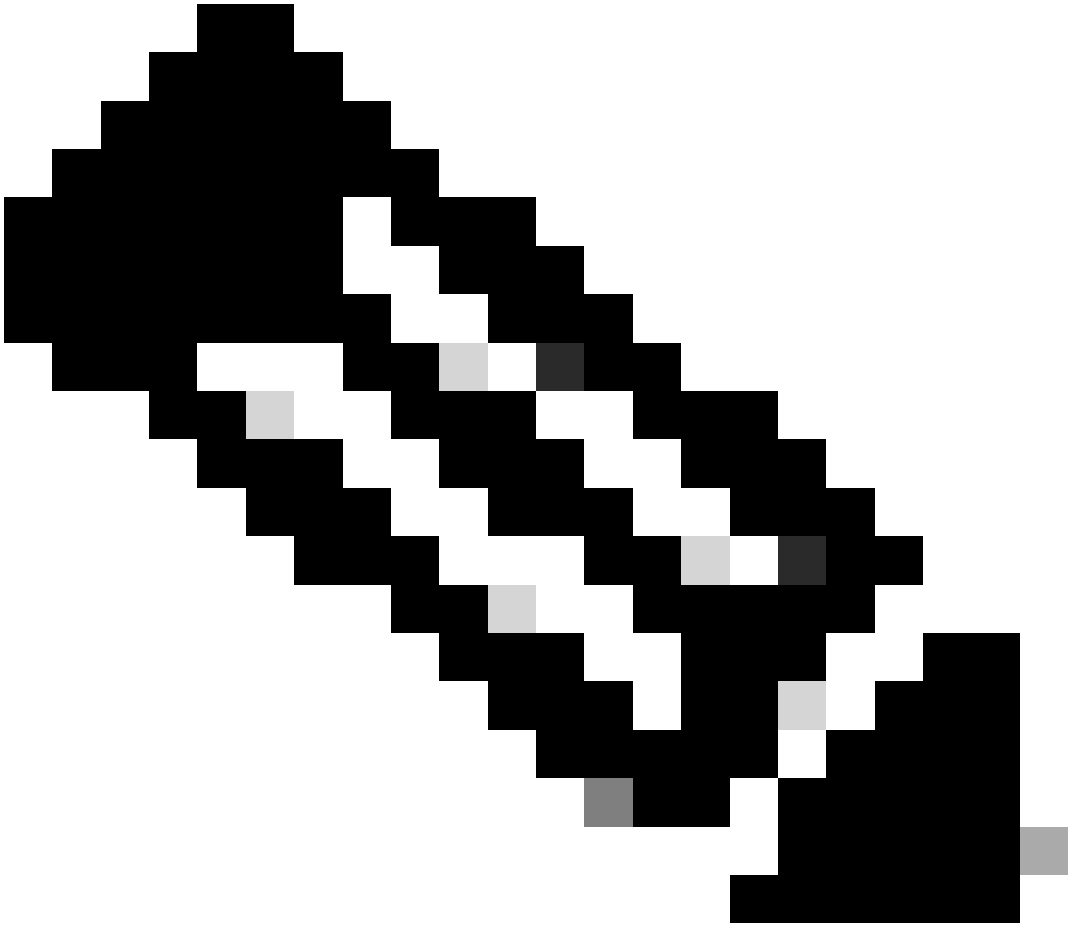
## Contents

## Introduction

This document describes how to configure Cisco Secure Client to automatically accept VPN and SEULA prompts to manage pop-ups.

## Overview

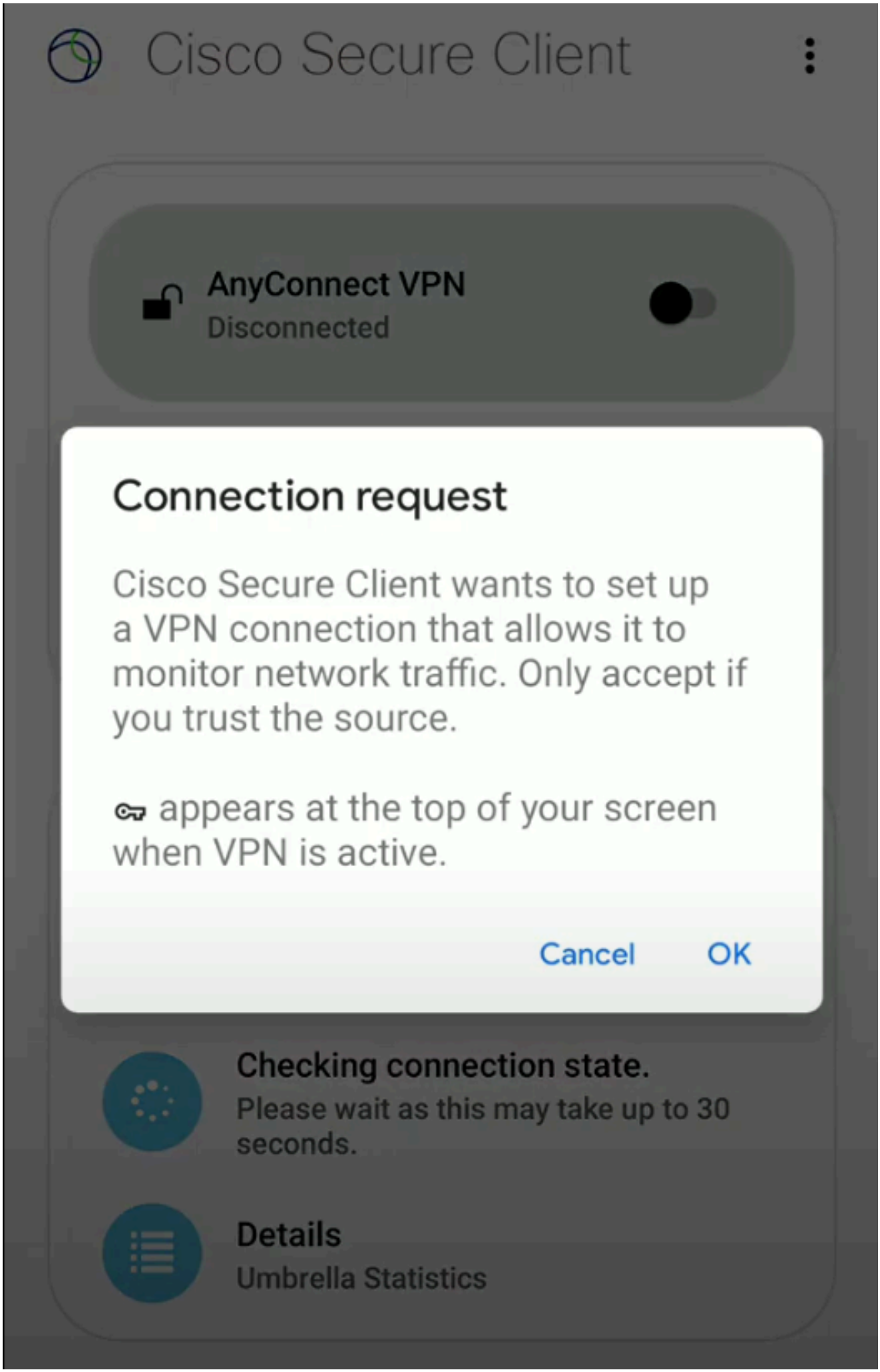
You can configure Cisco Secure Client to launch automatically and accept essential VPN and SEULA (Software End User License Agreement) pop-up prompts without user interaction on Android devices using MDM solutions such as Cisco Meraki and Microsoft Intune. By enabling Always-On VPN and setting the SEULA acceptance property in your MDM, you eliminate the need for users to respond to VPN connection and SEULA pop-ups during initial deployment.



**Note**: For zero-touch deployment with Workspace One, see our documentation: Deploy the Android Client: VMware Workspace ONE

## Settings Impacting Initial Launch

1. **VPN Connection Request for Umbrella:**
    - The device must accept a connection request for Umbrella protection to start.
    - You can auto-accept this by enabling**Always-On VPN**in your MDM configuration.

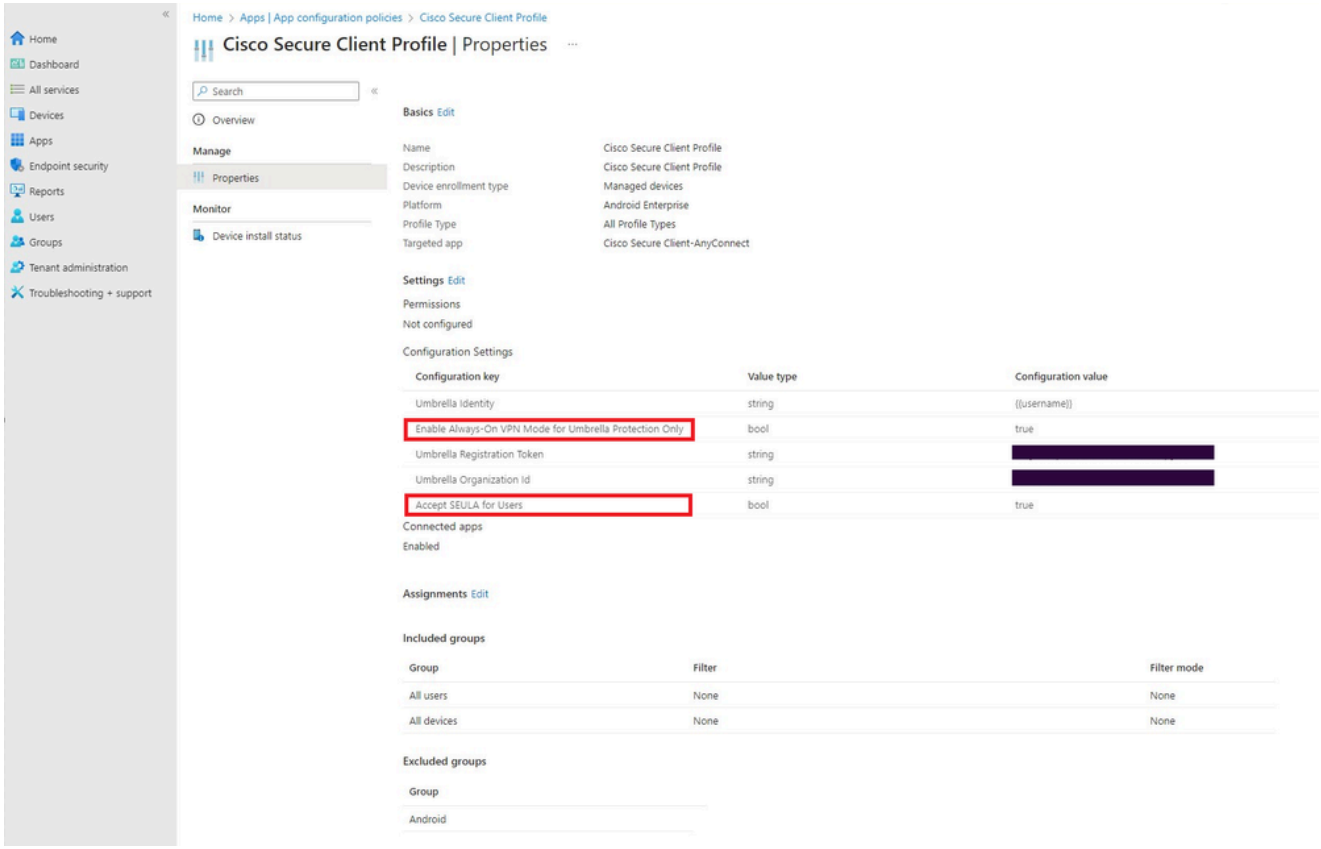



2. **SEULA Acceptance:**

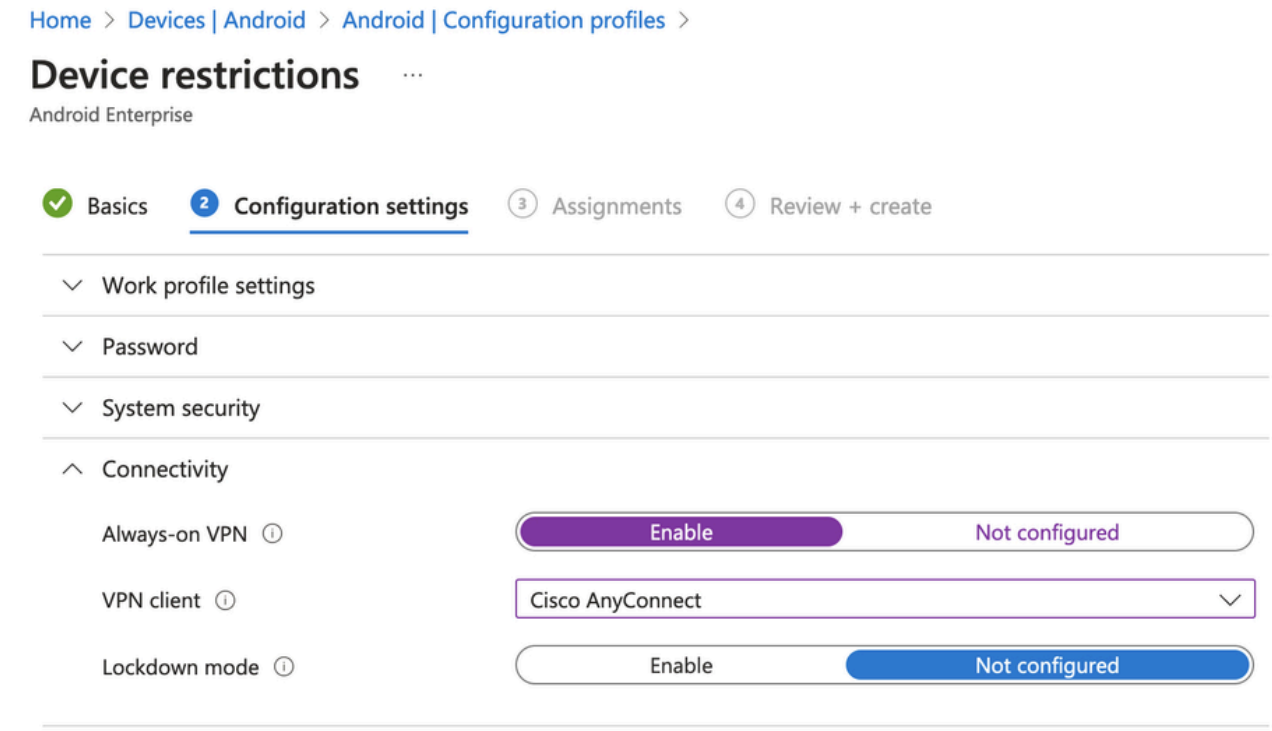
If you launch the app before pushing the Always-On VPN configuration, the VPN connection request pop-up will still appear. Ensure Always-On VPN is configured and pushed before first launch to prevent this.

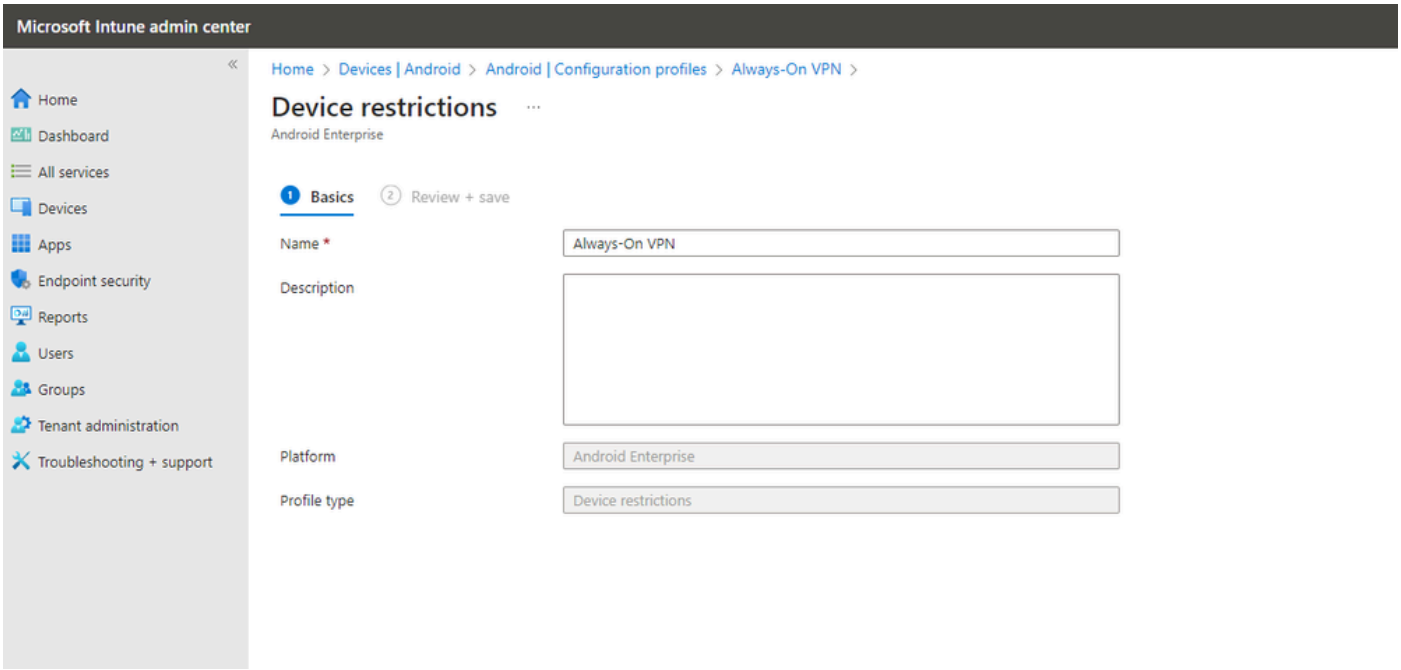
# Configure Auto-Accept in Microsoft Intune

1. Create a VPN profile and a device restrictions profile with the Always-On VPN setting enabled.
2. Assign these profiles to your target groups.
3. Select a VPN client that supports Always-On. You can choose either "Cisco AnyConnect" or specify a "Custom" client by entering the package ID of the app in the Google Play store as "com.cisco.anyconnect.vpn.android.avf" (Cisco AnyConnect VPN application specifically for Android devices).




4. Set the SEULA acceptance property and Always-On VPN.


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 |