

MDM経由でAndroidのSecure ClientのVPNおよびSEULAの自動受け入れを有効にする

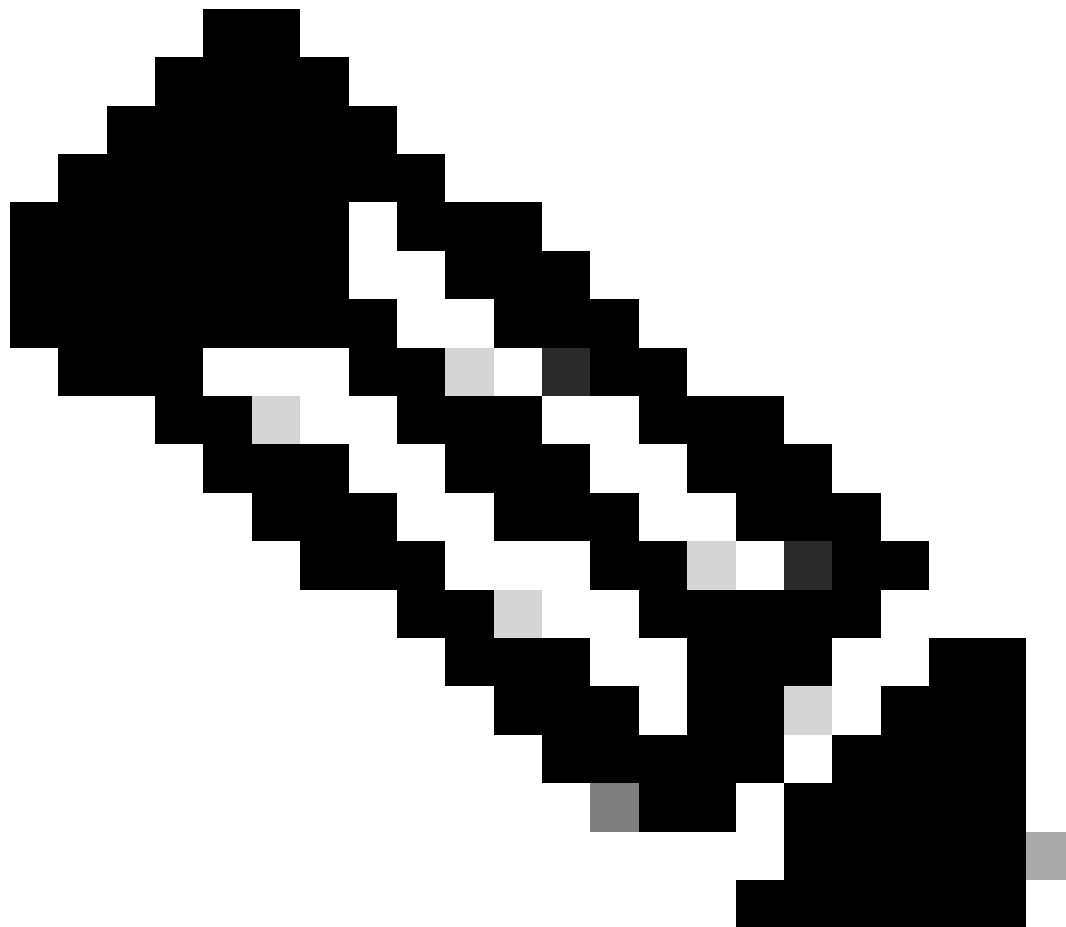
内容

はじめに

このドキュメントでは、ポップアップを管理するために、VPNおよびSEULAプロンプトを自動的に受け入れるようにCisco Secure Clientを設定する方法について説明します。

概要

Cisco MerakiやMicrosoft IntuneなどのMDMソリューションを使用するAndroidデバイスでは、ユーザの操作なしで、必須のVPNおよびSEULA（ソフトウェアエンドユーザライセンス契約）のポップアッププロンプトを自動的に起動して受け入れるように、Cisco Secure Clientを設定できます。Always-On VPNを有効にし、MDMでSEULA受け入れプロパティを設定することで、初期導入時にユーザがVPN接続およびSEULAポップアップに応答する必要がなくなります。



注:Workspace Oneによるゼロタッチ導入については、次のドキュメントを参照してください。[Androidクライアントの導入：VMware Workspace ONE](#)

初期起動に影響する設定

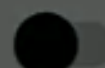
1. UmbrellaのVPN接続要求：

- Umbrella保護を開始するには、デバイスで接続要求を受け入れる必要があります。
- MDM設定でAlways-On VPNを有効にすると、これを自動的に受け入れることができます。



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.

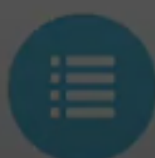
Cancel

OK



Checking connection state.

Please wait as this may take up to 30 seconds.



Details

Umbrella Statistics

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。