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

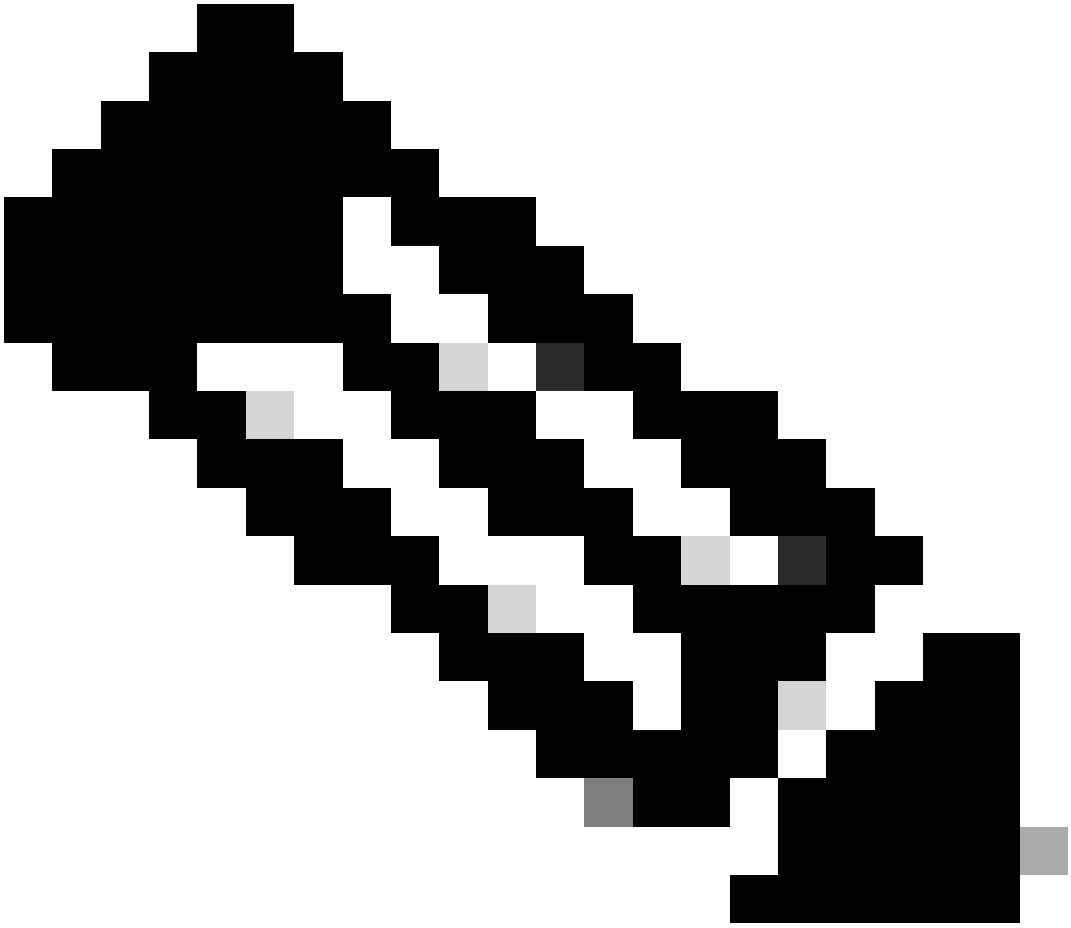
Inhalt

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

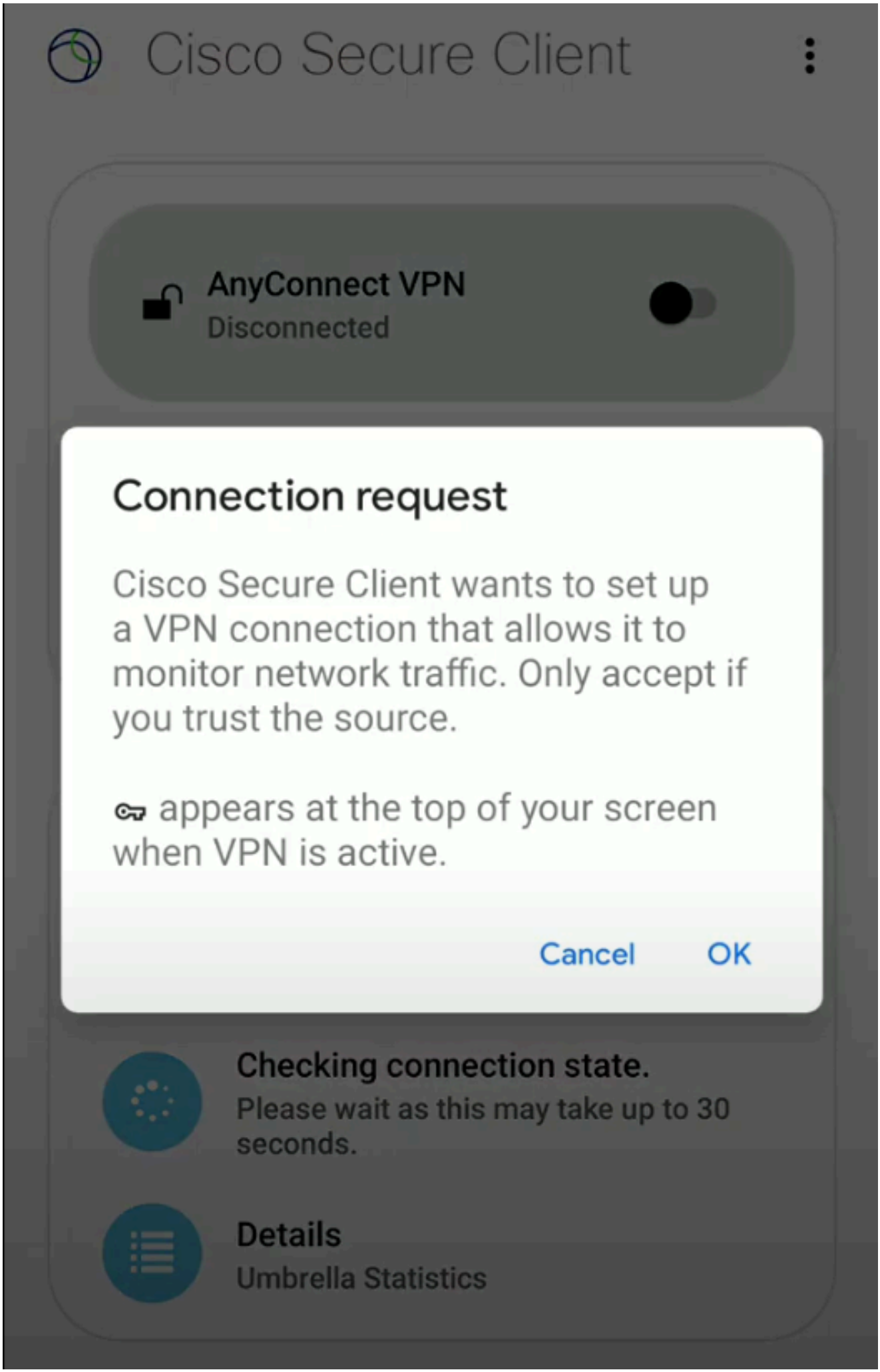
Sie können den Cisco Secure Client so konfigurieren, dass er automatisch gestartet wird und wichtige VPN- und SEULA-Popup-Meldungen (Software End User License Agreement) ohne Benutzereingriff auf Android-Geräten akzeptiert, die MDM-Lösungen wie Cisco Meraki und Microsoft Intune verwenden. Durch die Aktivierung 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]

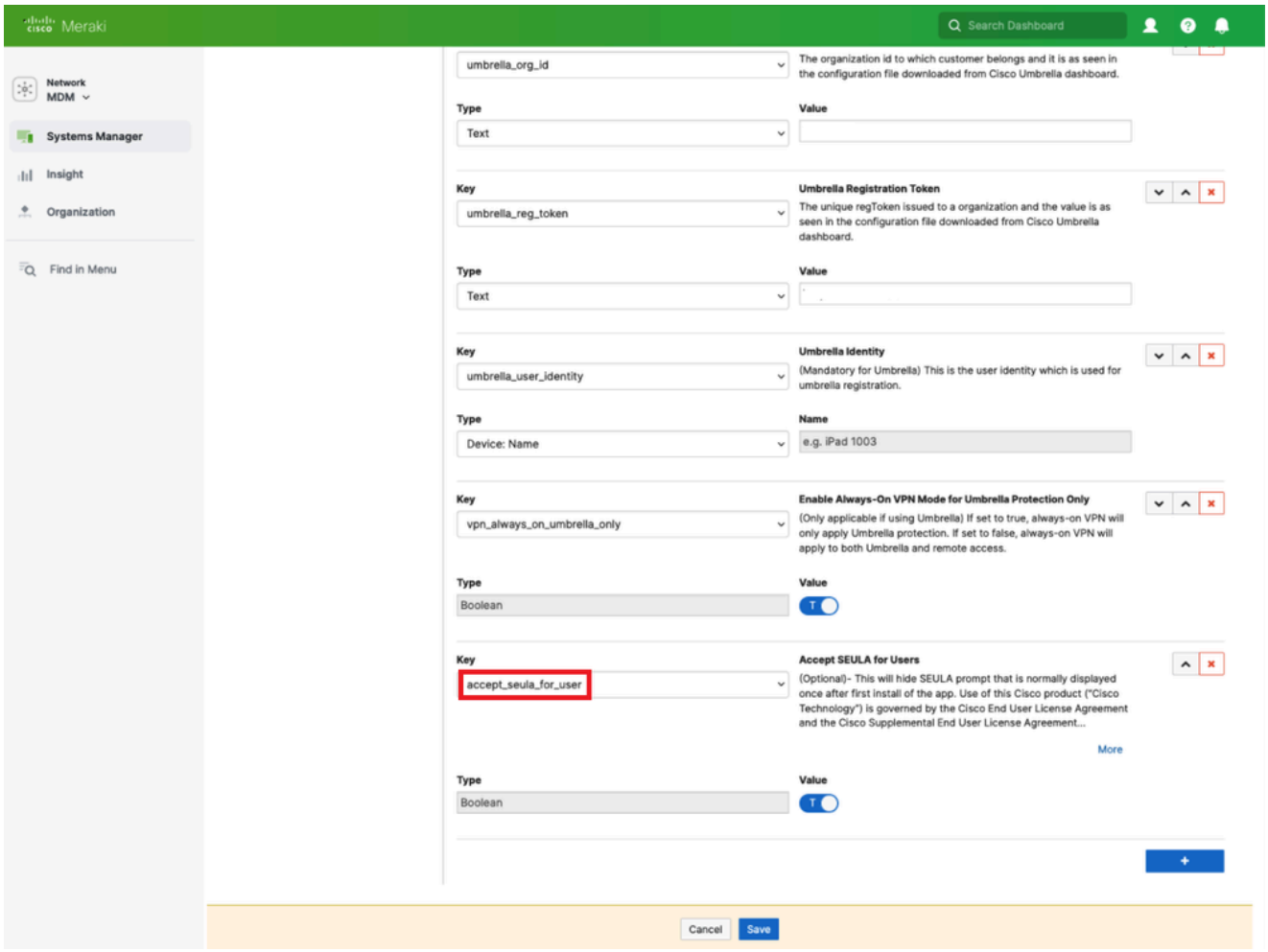
Einstellungen, die sich auf den ersten Start auswirken

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.



2. SELLA-Annahme:

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



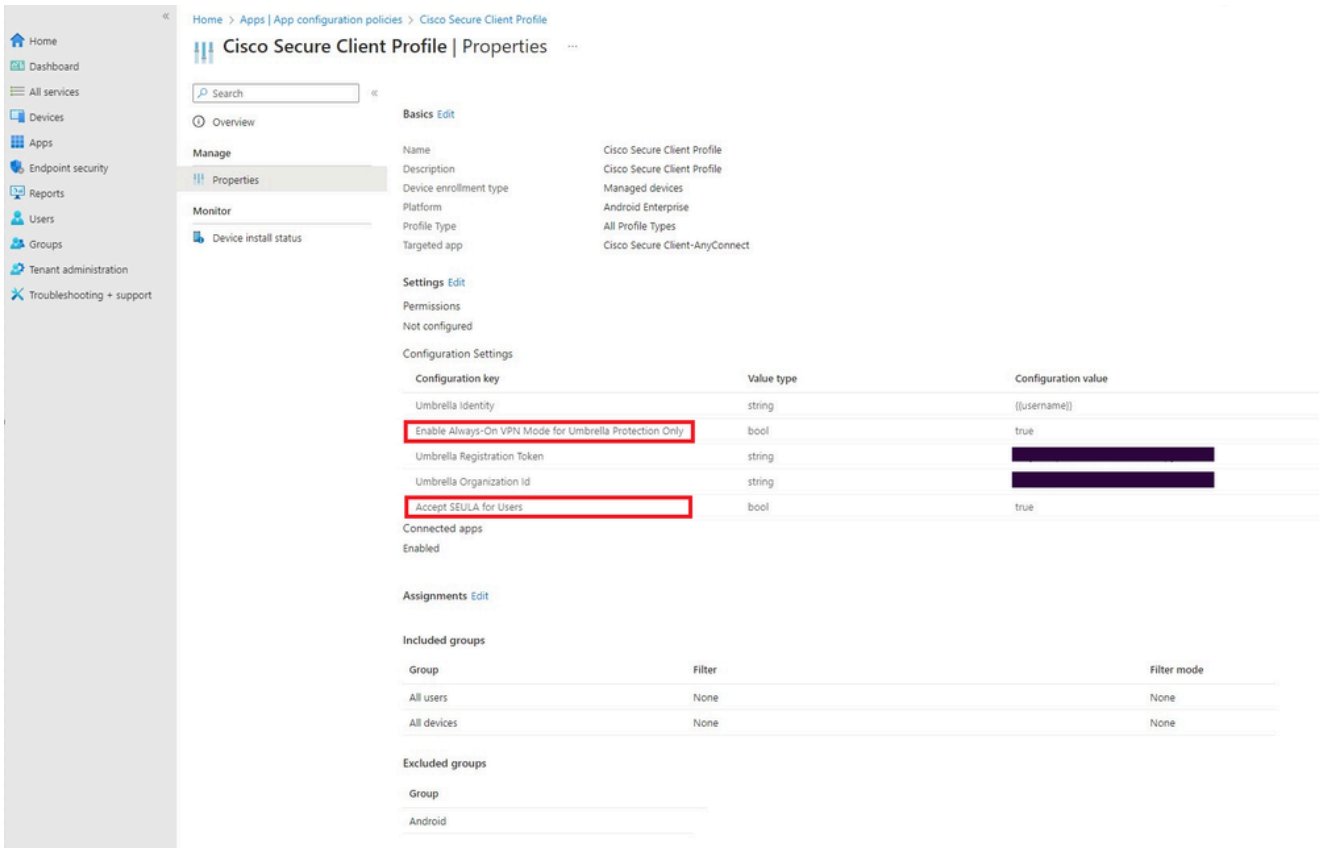
Wichtig: Wenn Sie die App starten, bevor Sie die Always-On-VPN-Konfiguration übertragen, wird das Popup-Fenster "VPN Connection Request" angezeigt. Stellen Sie sicher, dass das stets verfügbare VPN vor dem ersten Start konfiguriert und per Push bereitgestellt wird, um dies zu verhindern.

Konfigurieren von Auto-Accept in Microsoft Intune

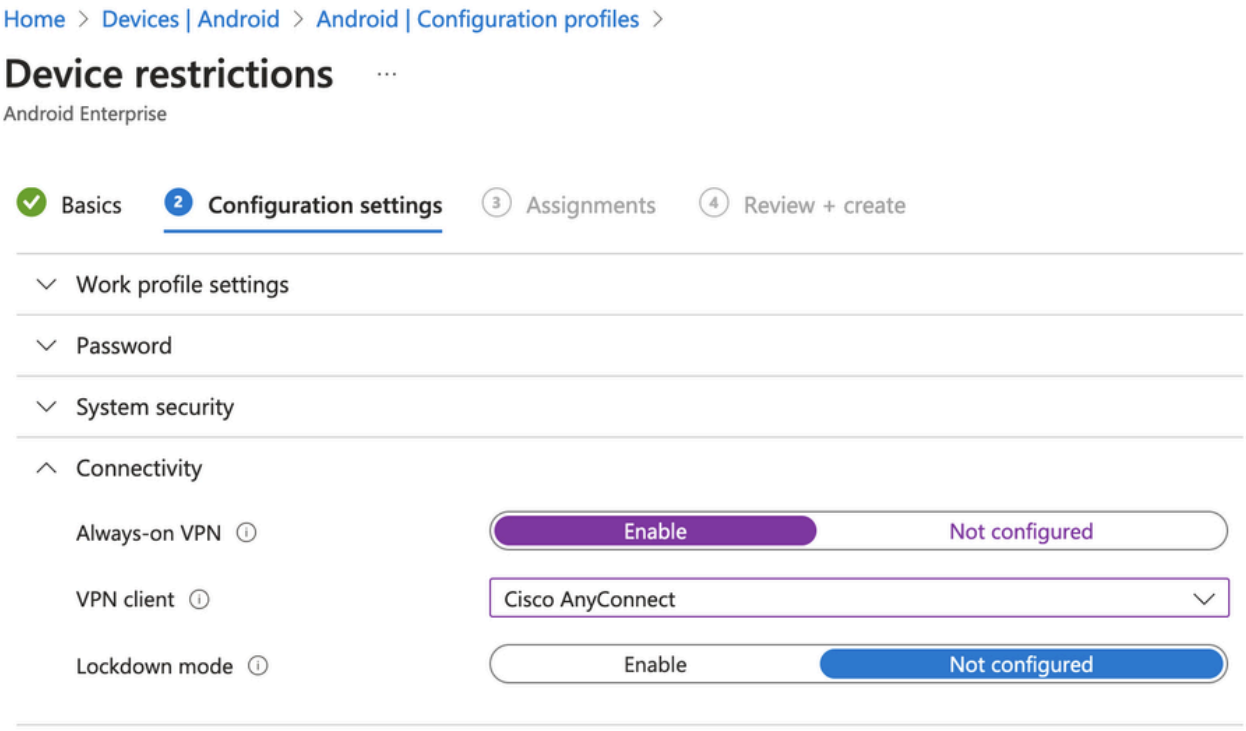
1. Erstellen Sie ein VPN-Profil und ein Profil mit Geräteeinschränkungen, wobei die VPN-Einstellung "Always-On" aktiviert ist.

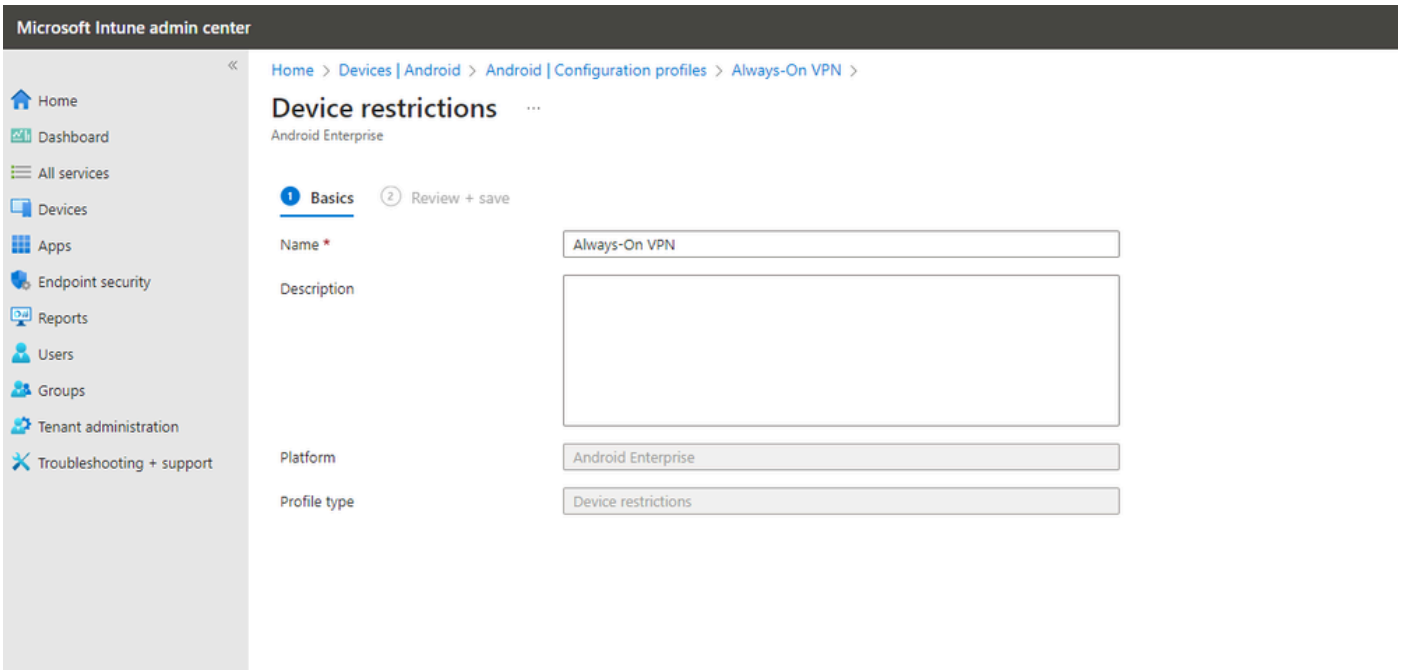
2. Weisen Sie diese Profile Ihren Zielgruppen zu.

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.



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





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.