

Bereitstellung eines sicheren Clients mit Umbrella Protection unter Android über Zero-Touch-MDM

Inhalt

Einleitung

Dieses Dokument beschreibt die Bereitstellung von Cisco Secure Client mit dem Umbrella-Modul auf Android-Geräten ohne Benutzereingriffe.

Hintergrundinformationen

Sie können Cisco Secure Client mit dem Umbrella-Modul auf Android-Geräten mithilfe von MDM-Lösungen wie Workspace One, Cisco Meraki oder Microsoft Intune ohne Benutzereingriffe bereitstellen. Dieser Prozess ermöglicht einen nahtlosen DNS-Layer-Schutz für Anwendungen und Browser-Datenverkehr, stellt sicher, dass Always On VPN aktiviert ist, und eliminiert Benutzereingriffe für die VPN- und SEULA-Akzeptanz.

Voraussetzungen

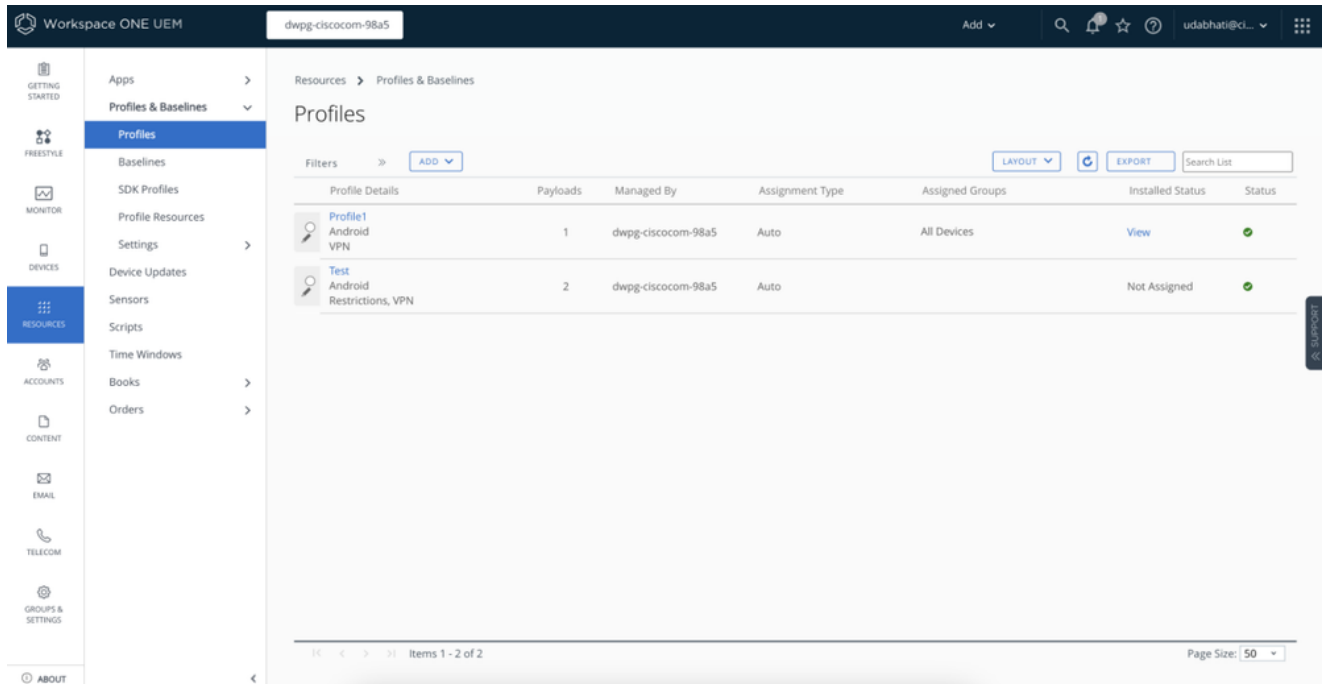
- Vollständige Android Enterprise Mobility Management (EMM)-Registrierung und Geräteanmeldung mit Erstellung von Arbeitsprofilen
- Die MDM-App (Hub) muss unter dem Arbeitsprofil sichtbar sein.
- Weisen Sie Cisco Secure Client nur nach der Veröffentlichung und Installation des Always On VPN-Profiles auf dem Intelligent Hub zu, und installieren Sie es.

Bereitstellungsschritte

A. Erstellen Sie das stets verfügbare VPN-Profil.

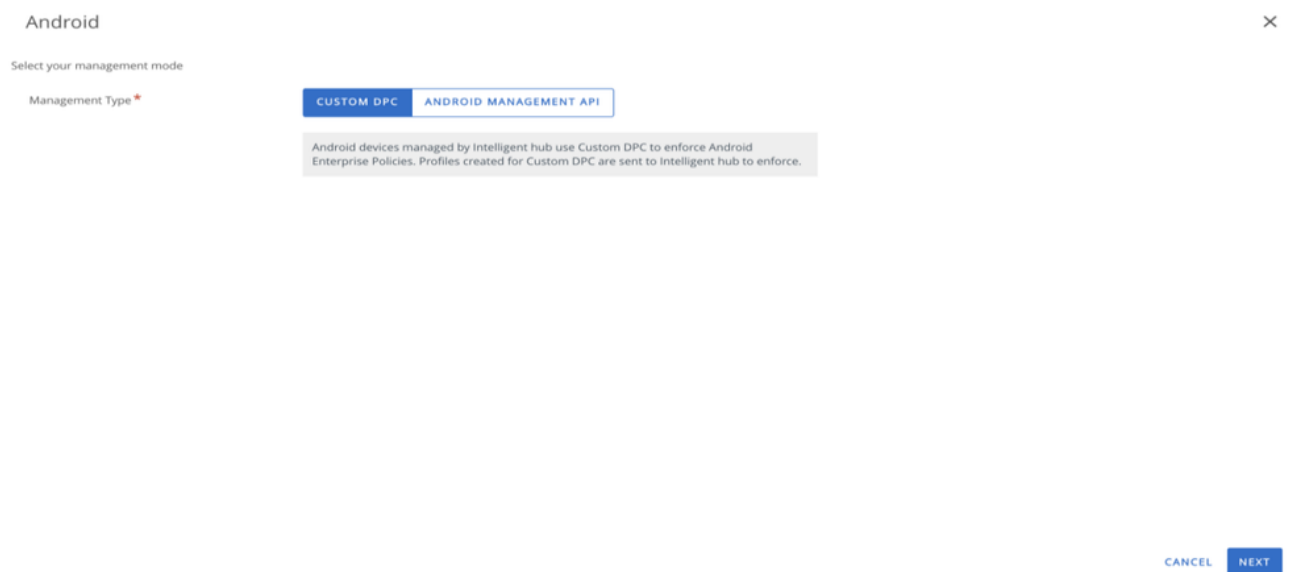
1. Zu Profilen navigieren:

- Gehen Sie zu Resources > Profiles & Baselines > Profiles.
- Klicken Sie auf Hinzufügen, um ein neues Profil zu erstellen.



2. Profil-Setup:

- Wählen Sie Android als Plattform aus.
- Wählen Sie den erforderlichen Verwaltungstyp aus.



3. VPN-Einstellungen konfigurieren:

- Gehen Sie im Profilabschnitt zu VPN Settings, und klicken Sie auf Add.
- Füllen Sie die erforderlichen Felder aus:
 - Verbindungstyp: Cisco AnyConnect
 - Server: cisco://local
 - Aktivieren Sie das Always On-VPN, und konfigurieren Sie bei Bedarf weitere Eigenschaften.



- Aktivieren Sie anwendungsspezifische VPN-Regeln.
- AktivierenAktiv setzen.
- Klicken Sie auf Weiter.

Always On VPN

Start typing to search for payloads and settings

VPN + ADD

Connection Info

Connection Type * Cisco AnyConnect

Connection Name * VPN Configuration

Server * cisco//local

Always On VPN ☒

Lockdown ☐

Set Active ☒

Per-App VPN Rules ☒

Protocol SSL

Username

Password

Summary

Payload	Status
VPN	Configured

CANCEL NEXT

4. Profil zuweisen:

- Lassen Sie die Smart Group leer.
- Weisen Sie das Profil den erforderlichen Geräten zu.
- Auswählen von Bereitstellungswerten.
- Klicken Sie auf Speichern und veröffentlichen.

Assignment

Smart Group

All Devices X

Allow Exclusion ☐

Deployment

Assignment Type Auto

Allow Removal Never

Managed By * dwpg-ciscocom-98a5

Install Only Area ☐

Schedule Install Time ☐

Per-App VPN Rules

Assignment Summary

Configuration

Total assigned 1

Devices added: ↑ 0

Devices removed: ↓ 0

Devices unchanged: 1

All assigned devices are estimated to receive assignment instructions by 12:35 PM.

View devices list

CANCEL BACK SAVE & PUBLISH

B. Zuweisen der Cisco Secure Client-Anwendung

1. App hinzufügen:

- Gehen Sie zu Resources > Native > Public.
- Fügen Sie Cisco Secure Client aus dem Play Store hinzu, falls dies noch nicht möglich

Add Application

Managed By

Platform *

Source

Name *

Native

ist.

NEXT CANCEL

2. Anwendungszuweisung:

- Wählen Sie die App aus, und geben Sie die erforderlichen Werte ein.
- Erstellen Sie im Zuordnungsabschnitt eine neue Zuweisung.



Edit Application - Cisco Secure Client-AnyConnect

Public | Status: Active | Managed By: dwpj-ciscocom-98a5 | Application ID: com.cisco.anyconnect.vpn.android.avf

Details Terms of Use SDK



Name * ⓘ

[View in Play Store](#)

Created on 11/28/2024 12:36 PM by udabhati@cisco.com

Modified on 11/28/2024 12:36 PM by udabhati@cisco.com

Categories ⓘ

Supported Models ⓘ

Is App Restricted to Silent Install ⓘ

Managed By

3. Konfiguration der Verteilung:

- Geben Sie Details im Abschnitt "Distribution" ein.

Distribution

Restrictions

Tunnel

Application Configuration

Components Profile Configuration

Distribution

Name *

CSC

Description

Assignment Description

Assignment Groups *

To whom do you want to assign this app?

All Devices(dwpg-cisco.com-98a5) X

App Delivery Method *

☒ Auto

☐ On Demand

Auto Update Priority

☐ Default

☒ High priority

☐ Postpone (90 days)

Pre-release Version

None

CANCEL

CREATE

4. Managed Access aktivieren:

- Aktivieren Sie auf der Registerkarte Restrictions den verwalteten Zugriff.

✓ Distribution

Restrictions

Tunnel

Application Configuration

Components Profile Configuration

Restrictions



EMM Managed Access

Hide ^

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access

☒

CANCEL

CREATE

5. Profil auswählen:

- Wählen Sie in der Tunneloption das zuvor erstellte Profil ('Always On VPN') unter Android (Custom DPC) aus.

Cisco Secure Client-AnyConnect - Assignment

☒ Distribution
☒ Restrictions
☒ Tunnel
☒ Application Configuration
☒ Components Profile Configuration

Tunnel



EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access ☒

Android Legacy Select a Profile... ⓘ

Android (Custom DPC) Always On VPN @ dwpq-ciscocom-98a5 ⓘ

CANCEL SAVE

6. Anwendungskonfiguration:

- Geben Sie Details zur Anwendungskonfiguration wie Org-ID und Reg-Token in die Android-Konfigurationsdatei ein, die vom Umbrella Dashboard heruntergeladen wurde.
- Aktivieren/Akzeptieren der SEULA Für Benutzer, um die manuelle Annahme der SEULA zu umgehen.
- Stets verfügbarer VPN-Modus nur für Umbrella Protection zur nahtlosen VPN-Verwaltung durch Cisco Secure Client.
- Blockiert die Erstellung neuer VPN-Verbindungen durch Benutzer (lässt das Feld Host leer).

Cisco Secure Client-AnyConnect - Assignment

☒ Distribution
☒ Restrictions
☒ Tunnel
☒ Application Configuration
☒ Components Profile Configuration

Application Configuration



EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access ☒

ⓘ Application configuration through Managed Google Play can only be assigned to Android devices, any Android (Legacy) devices in this assignment will not receive this app if application configuration is enabled.

Send Configuration ☒ ⓘ

Connection Name ⓘ

Host ⓘ

Protocol Select ⓘ

CANCEL CREATE

7. Speichern und veröffentlichen:

- Speichern Sie die Änderungen, und veröffentlichen Sie die Cisco Secure Client-App.

Assigned
1Newly added
0Newly removed
0Unchanged
1

All assigned devices are estimated to receive assignment instructions by 4:50 PM.

ADDED (0) REMOVED (0) UNCHANGED (1)



Last Check In	Device Friendly Name	Username	Organization Group	Platform
 No results found				

Manage Columns

Devices per page 20

CANCEL

BACK

PUBLISH

8. Schieben Sie das Umbrella Certificate:

- Anweisungen hierzu finden Sie unter: [Umbrella-Zertifikat auf Geräte übertragen](#)

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.