

Installazione di Secure Client con Umbrella Protection su Android tramite MDM Zero-Touch

Sommario

Introduzione

Questo documento descrive come distribuire Cisco Secure Client con il modulo Umbrella su dispositivi Android usando la distribuzione zero-touch.

Premesse

È possibile distribuire Cisco Secure Client con il modulo Umbrella su dispositivi Android utilizzando la distribuzione zero-touch tramite soluzioni MDM come Workspace One, Cisco Meraki o Microsoft Intune. Questo processo consente una protezione completa a livello DNS per le applicazioni e il traffico del browser, garantisce l'abilitazione della VPN Always On ed elimina l'intervento dell'utente per l'accettazione della VPN e della SEULA.

Prerequisiti

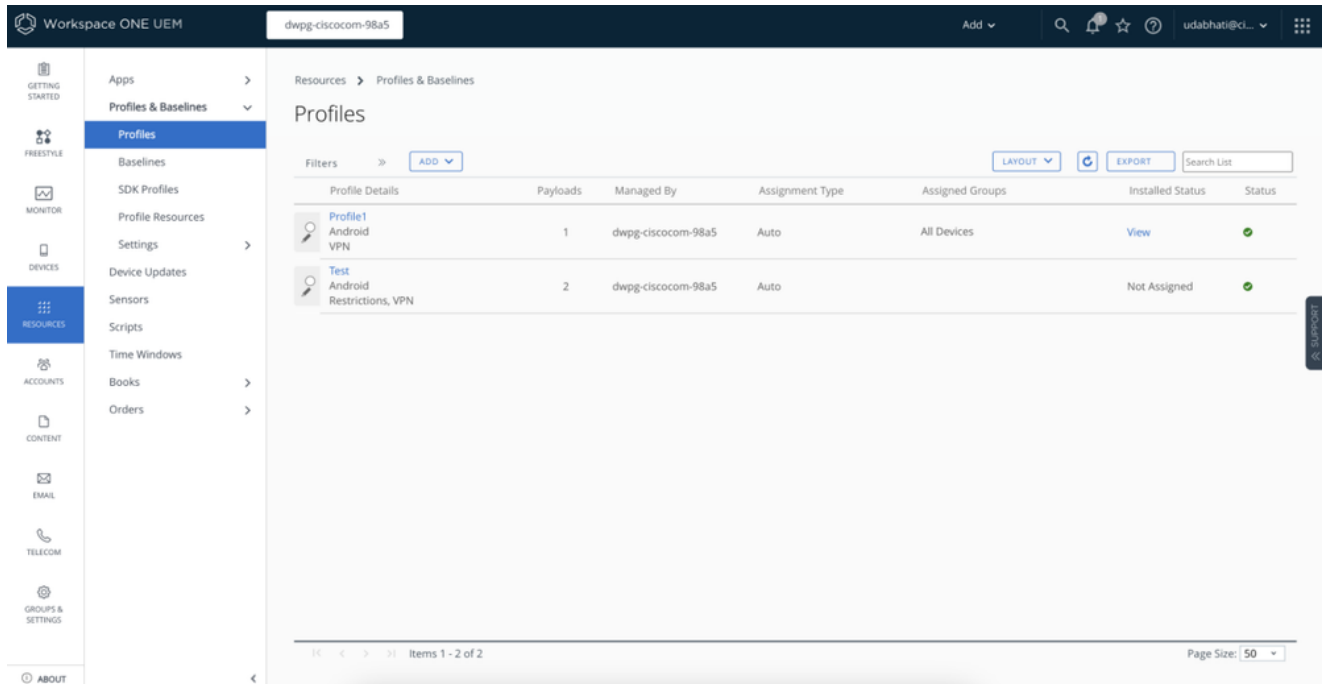
- Completamento della registrazione EMM (Android Enterprise Mobility Management) e della registrazione dei dispositivi con la creazione di profili di lavoro.
- L'app MDM (hub) deve essere visibile nel profilo di lavoro.
- Assegnare e installare Cisco Secure Client solo dopo la pubblicazione e l'installazione del profilo VPN Always On in Intelligent Hub.

Fasi di distribuzione

A. Creare il profilo VPN Always On

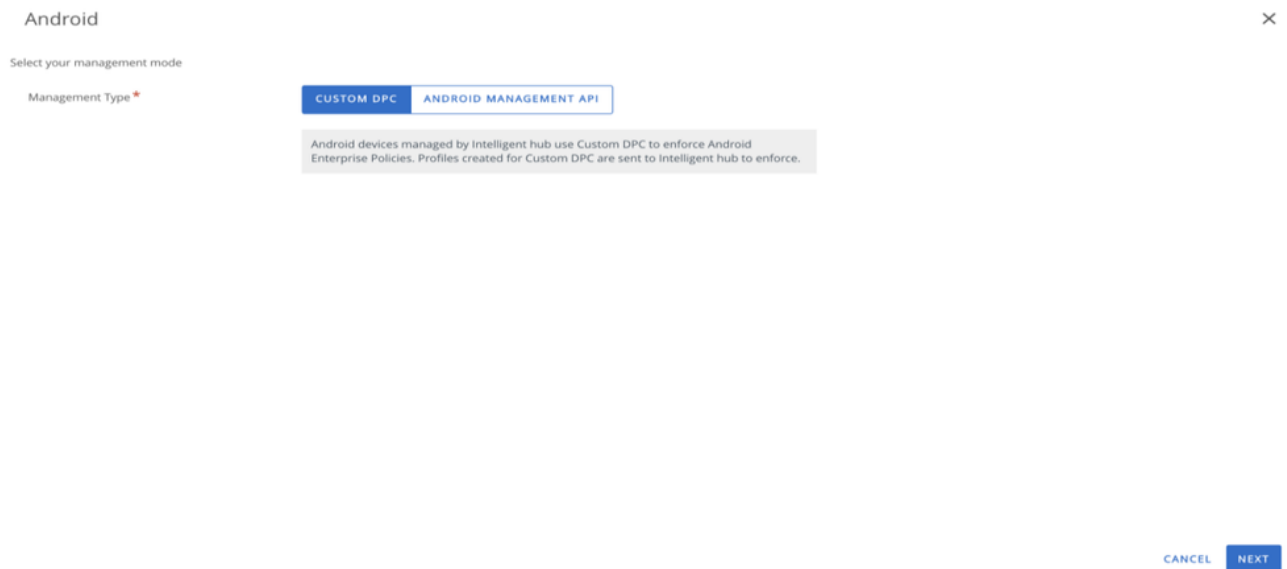
1. Passare a Profili:

- Selezionare Risorse > Profili e baseline > Profili.
- Fare clic su Aggiungi per creare un nuovo profilo.



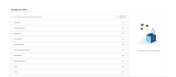
2. Impostazione profilo:

- Selezionate Androida come piattaforma.
- Scegliere il tipo di gestione richiesto.



3. Configurare le impostazioni VPN:

- Nella sezione del profilo, andare a Impostazioni VPN e fare clic su Aggiungi.
- Compilare i campi obbligatori:
 - Tipo di connessione: Cisco AnyConnect
 - Server: cisco://local
 - Abilitare la VPN Always On e configurare altre proprietà in base alle esigenze.
 - Abilita regole VPN per app.
 - EnableSet Attivo.



- Fare clic su Avanti.

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. Assegna profilo:

- Lasciare vuoto il gruppo smart.
- Assegnare il profilo ai dispositivi necessari.
- Selezionare i valori di distribuzione.
- Fare clic su Salva e pubblica.

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. Assegnazione dell'app Cisco Secure Client

1. Aggiungi l'app:

- Andare a Risorse > Native > Pubbliche.
- Aggiungere Cisco Secure Client dal Play Store, se non è già disponibile.

Add Application

Managed By

Platform *

Source

Name *

2. Assegnazione app:

- Selezionare l'app e immettere i valori richiesti.
- Nella sezione assegnazione creare una nuova assegnazione.



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



UPLOAD

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

YES

NO

Managed By

3. Configura distribuzione:

- Immettere i dettagli nella sezione Distribuzione.

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. Abilita accesso gestito:

- Nella scheda Restrictionstab, abilitare l'accesso gestito.

✓ 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. Seleziona profilo:

- Nell'opzione Tunneling, selezionare il profilo creato in precedenza ('Always On VPN') in Android (Custom DPC).

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-ciscocon-98a5 ⓘ

CANCEL SAVE

6. Configurazione applicazione:

- Immettere i dettagli di configurazione dell'applicazione, ad esempio ID organizzazione e Token reg, dal file di configurazione Android scaricato da Umbrella Dashboard.
- Abilitare Accetta SEULA per gli utenti in modo da ignorare l'accettazione manuale SEULA.
- Abilita la modalità VPN sempre attiva per la protezione degli ombrelli solo per una gestione VPN senza problemi da parte di Cisco Secure Client.
- Impedisce agli utenti di creare nuove connessioni VPN (lasciare vuoto il campo Host).

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. Salva e pubblica:

- Salva le modifiche e pubblica l'app Cisco Secure Client.

X

Assignments Exclusions

ADD ASSIGNMENT

CANCEL SAVE

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

CANCEL BACK PUBLISH

- Per istruzioni, vedere: [Invia certificato ombrello ai dispositivi](#)

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).