

Deploy Secure Client with Umbrella Protection on Android via Zero-Touch MDM

Contents

Introduction

This document describes how to deploy Cisco Secure Client with the Umbrella module on Android devices using zero-touch deployment.

Background Information

You can deploy Cisco Secure Client with the Umbrella module on Android devices using zero-touch deployment through MDM solutions such as Workspace One, Cisco Meraki, or Microsoft Intune. This process enables seamless DNS-layer protection for apps and browser traffic, ensures Always On VPN is enabled, and eliminates user intervention for VPN and SEULA acceptance.

Prerequisites

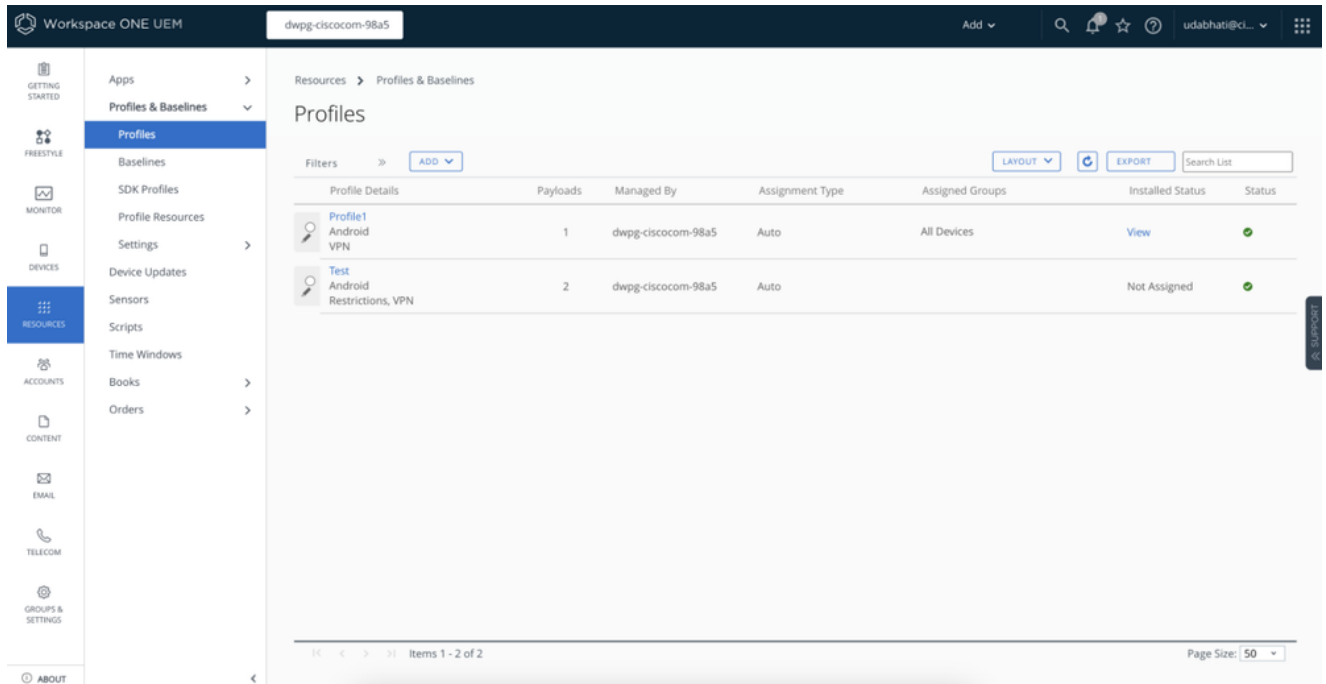
- Complete Android Enterprise Mobility Management (EMM) registration and device enrollment with work profile creation.
- The MDM app (Hub) must be visible under the work profile.
- Assign and install Cisco Secure Client only after publishing and installing the Always On VPN profile to Intelligent Hub.

Deployment Steps

A. Create the Always On VPN Profile

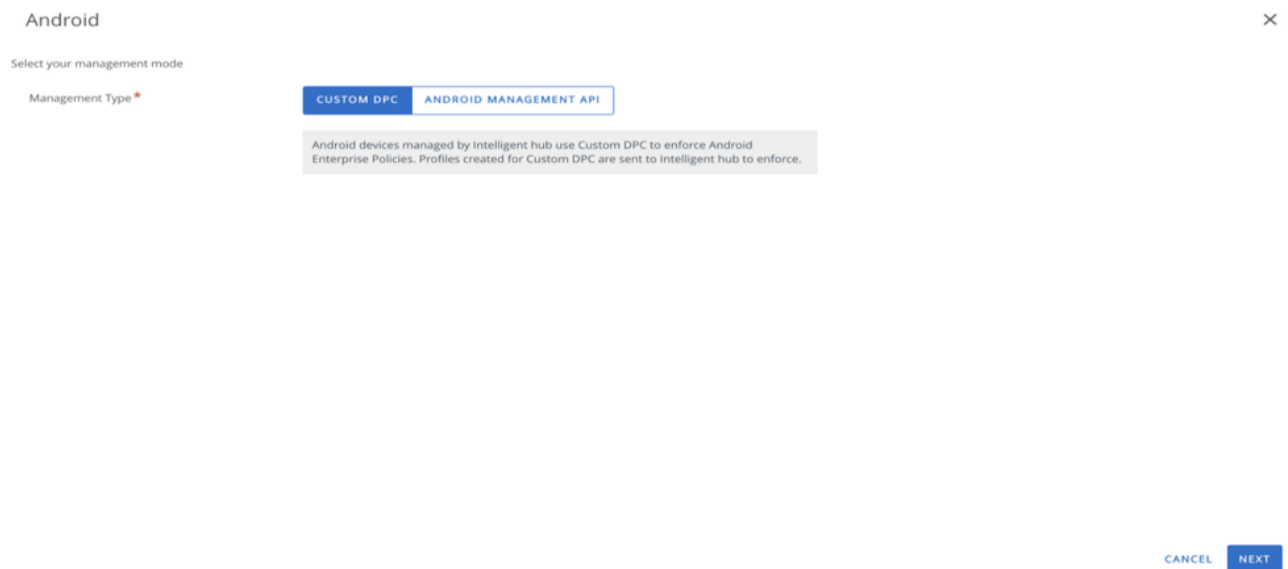
1. Navigate to Profiles:

- Go to **Resources > Profiles & Baselines > Profiles**.
- Click **Add** to create a new profile.



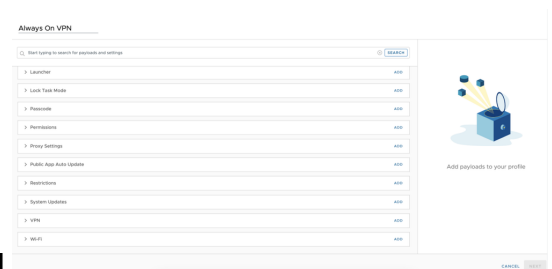
2. Profile Setup:

- Select **Android** as the platform.
- Choose the required **Management Type**.



3. Configure VPN Settings:

- In the profile section, go to **VPN Setting** and click **Add**.
- Fill in the required fields:
 - **Connection Type:** Cisco AnyConnect



- **Server:**cisco://local
- Enable**Always On VPN**and configure other properties as needed.
- Enable**Per-App VPN Rules**.
- Enable**Set Active**.
- Click**Next**.

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. Assign Profile:

- Leave the Smart Group empty.
- Assign the profile to the necessary devices.
- Select deployment values.
- Click**Save & Publish**.

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. Assign the Cisco Secure Client App

1. Add the App:

- Go to **Resources > Native > Public**.



- Add **Cisco Secure Client** from the Play Store if not already available.



2. App Assignment:

- Select the app and fill in required values.
- In the assignment section, create a new assignment.

Edit Application - Cisco Secure Client-AnyConnect

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

Details

Terms of Use

SDK

Name ^{*}

Cisco Secure Client-AnyConnect ⓘ

[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

UPLOAD

Categories

Start Typing to Select Category ... ⓘ

Supported Models

Android ⓘ

Is App Restricted to Silent Install

YES

NO ⓘ

Managed By

dwpg-ciscocom-98a5

SAVE & ASSIGN

CANCEL

3. Configure Distribution:

- Enter details in the Distribution section.

Cisco Secure Client-AnyConnect - Assignment

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-ciscocom-98a5) X

App Delivery Method ^{*}

☒ Auto

☐ On Demand ⓘ

Auto Update Priority

☐ Default

☒ High priority ⓘ

☐ Postpone (90 days) ⓘ

Pre-release Version

None ⓘ

CANCEL

CREATE

4. Enable Managed Access:

- In the **Restriction** tab, enable **Managed Access**.

Cisco Secure Client-AnyConnect - Assignment

- ✓ 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. Select Profile:

- In the **Tunnel** option, select the previously created profile ('Always On VPN') under **Android (Custom DPC)**.

Cisco Secure Client-AnyConnect - Assignment

- ✓ Distribution
- ✓ Restrictions
- Tunnel**
- ✓ Application Configuration
- ✓ Components Profile Configuration

Tunnel

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 ☒

Android Legacy Select a Profile... ⓘ

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

CANCEL SAVE

6. Application Configuration:

- Enter application configuration details such as **Org ID** and **Reg Token** from the Android Config

Managed Mobile Clients

To deploy Umbrella mobile coverage, download a configuration data file and use it to configure your MDM. For more information, see [Umbrella's iOS](#) and [Android Help](#).

IOS Android

Android Configuration File

Common Configuration

[Android Config](#) ⓘ

BACK DONE

File downloaded from the Umbrella Dashboard.

- Enable **Accept SEULA For Users** to bypass manual SEULA acceptance.
- Enable **Always On VPN Mode for Umbrella Protection Only** for seamless VPN management by Cisco Secure Client.
- Block users from creating new VPN connections (leave the Host field empty).

Cisco Secure Client-AnyConnect - Assignment

- Distribution
- Restrictions
- Tunnel
- Application Configuration**
- Components Profile Configuration

Application Configuration

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 ☒

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. Save and Publish:

- Save changes and publish the Cisco Secure Client app.

Cisco Secure Client-AnyConnect - Assignment

Details: Platform: Android Status: Active

Assignments Exclusions

Devices will receive application based on the configurations below. Devices with multiple assignments will receive policies in priority order. Adjusting the priority for a single assignment will automatically re-prioritize other assignments. Select the assignment to edit. Adding a new assignment will create a new tab at the bottom of the list.

ADD ASSIGNMENT

Priority	Assignment Name	Assignment	Smart Groups	App Delivery Method	EMM Managed Access
1	CCS	CCS	1	Auto	☒ Enabled

CANCEL PUBLISH

Cisco Secure Client-AnyConnect - Preview Assigned Devices

Assigned **1**

Newly added **0**

Newly removed **0**

Unchanged **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. Push the Umbrella Certificate:

- For instructions, see: [Push the Umbrella Certificate to Devices](#)