

Implemente Secure Client con protección Umbrella en Android a través de MDM sin intervención

Contenido

Introducción

Este documento describe cómo implementar Cisco Secure Client con el módulo Umbrella en dispositivos Android mediante la implementación sin intervención del usuario.

Antecedentes

Puede implementar Cisco Secure Client con el módulo Umbrella en dispositivos Android mediante la implementación sin intervención del usuario a través de soluciones de MDM como Workspace One, Cisco Meraki o Microsoft Intune. Este proceso permite una protección perfecta de la capa DNS para el tráfico de las aplicaciones y el navegador, garantiza que la función Always On VPN esté activada y elimina la intervención del usuario para la aceptación de VPN y SEULA.

Prerequisites

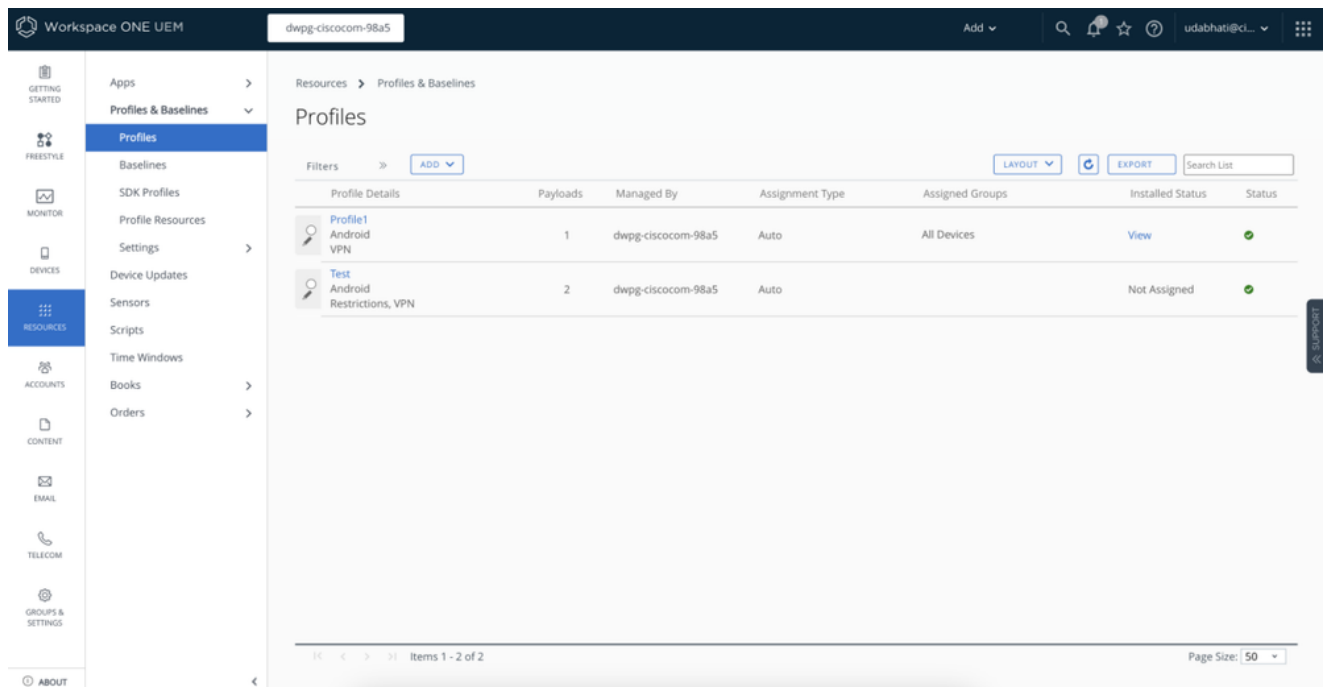
- Registro completo de Android Enterprise Mobility Management (EMM) e inscripción de dispositivos con creación de perfiles de trabajo.
- La aplicación MDM (concentrador) debe estar visible en el perfil de trabajo.
- Asigne e instale Cisco Secure Client solo después de publicar e instalar el perfil de VPN siempre activo en Intelligent Hub.

Pasos de implementación

A. Crear el perfil de VPN siempre activo

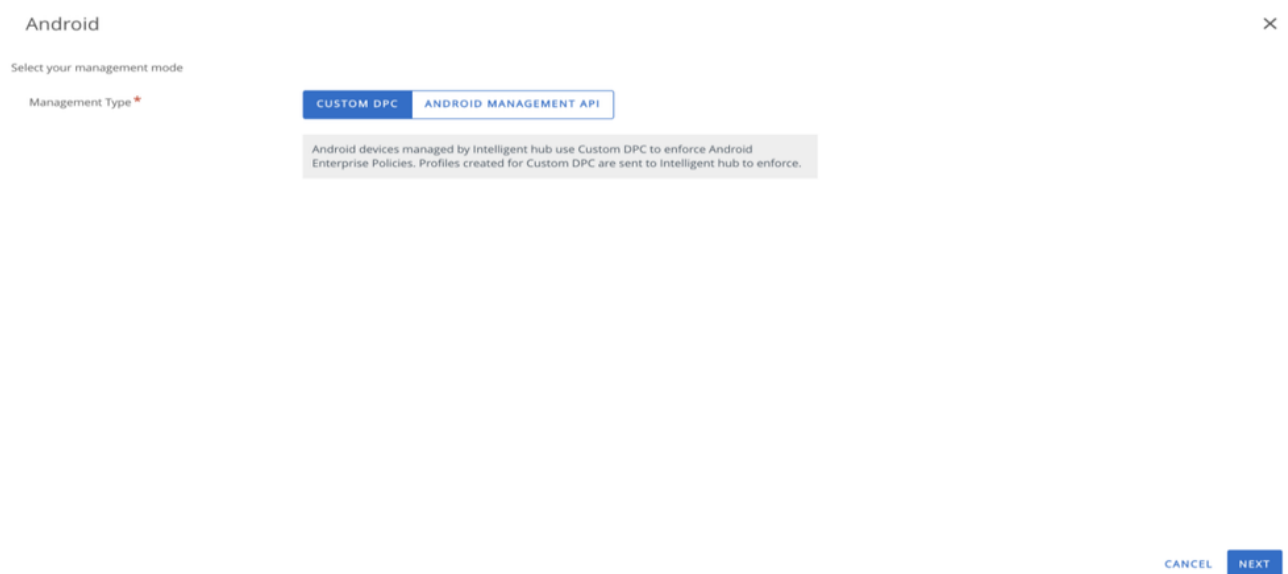
1. Vaya a Perfiles:

- Vaya a Recursos > Perfiles y líneas base > Perfiles.
- Haga clic en Agregar para crear un nuevo perfil.



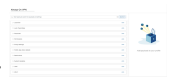
2. Configuración del perfil:

- Seleccione Androides en la plataforma.
- Elija el Tipo de administración requerido.



3. Configuración de los parámetros de VPN:

- En la sección de perfil, vaya a Configuración de VPN y haga clic en Agregar.
- Rellene los campos obligatorios:
 - Tipo de conexión: Cisco AnyConnect
 - Servidor: cisco://local
 - Habilite la VPN Always On y configure otras propiedades según sea necesario.
 - Habilite las reglas VPN por aplicación.
 - EnableSet Active.



- Haga clic en Siguiente.

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. Asignar perfil:

- Deje el grupo inteligente vacío.
- Asigne el perfil a los dispositivos necesarios.
- Seleccione los valores de implementación.
- Haga clic en Guardar y publicar.

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. Asignar la aplicación Cisco Secure Client

1. Agregue la aplicación:

- Vaya a Recursos > Nativos > Públicos.
- Agregue Cisco Secure Client desde Play Store si aún no está disponible.

Add Application

Managed By

Platform *

Source

Name *

2. Asignación de aplicaciones:

- Seleccione la aplicación y rellene los valores necesarios.
- En la sección de asignaciones, cree una nueva asignación.



Edit Application - Cisco Secure Client-AnyConnect

Public | Status: Active | Managed By: dwp-g-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. Configurar distribución:

- Introduzca los detalles en la sección Distribución.

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-ciscocon-98a5) X

App Delivery Method *

☒ Auto

☐ On Demand

Auto Update Priority

☐ Default

☒ High priority

☐ Postpone (90 days)

Pre-release Version

None

CANCEL

CREATE

4. Habilitar acceso administrado:

- En la ficha Restricciones, habilite Acceso administrado.

✓ 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. Seleccionar perfil:

- En la opción Túnel, seleccione el perfil creado anteriormente ('Always On VPN') en Android (DPC personalizado).

The screenshot shows the 'Tunnel' configuration page in the Cisco Secure Client-AnyConnect interface. On the left, a sidebar contains a list of configuration categories: Distribution, Restrictions, Tunnel (selected), Application Configuration, and Components Profile Configuration. The main content area is titled 'Tunnel' and features a section for 'EMM Managed Access'. This section includes a description: 'EMM managed access defines which devices will be able to install this app from Intelligent Hub.' It also provides two conditional instructions: 'If this setting is disabled, all registered devices will be able to install this app.' and 'If this setting is enabled, only EMM managed devices will be able to install this app.' Below this text, a toggle switch for 'Managed Access' is shown in the 'on' position. At the bottom of the main area, there are two rows for device profiles: 'Android Legacy' with a 'Select a Profile...' dropdown, and 'Android (Custom DPC)' with a dropdown showing 'Always On VPN @ dwpag-ciscocom-98a5'. In the bottom right corner, there are 'CANCEL' and 'SAVE' buttons.

6. Configuración de la aplicación:

- Introduzca los detalles de configuración de la aplicación, como el ID de la organización y el token de registro del archivo de configuración de Android descargado desde el

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

panel de Umbrella.

- EnableAccept SEULA For Users to bypass manual SEULA accept.
- Habilite el modo VPN siempre activo para la protección de paraguas solamente para la gestión de VPN sin problemas por parte de Cisco Secure Client.
- Bloquear a los usuarios para que no creen nuevas conexiones VPN (deje vacío el campo Host).

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 ⓘ

CANCEL CREATE

7. Guardar y publicar:

- Guarde los cambios y publique la aplicación Cisco Secure Client.

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. Introduzca el certificado de paraguas:

- Para obtener instrucciones, consulte: [Envío del certificado general a los dispositivos](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).