

Implementar el conector de seguridad con Intune

Contenido

[Introducción](#)

[Overview](#)

[Procedimiento](#)

[Limitaciones](#)

[Resolución de problemas](#)

[Registros](#)

Introducción

Este documento describe cómo implementar el Conector de seguridad mediante Intune.

Overview

Esta es una guía paso a paso sobre cómo obtener su dispositivo iOS/iPadOS MDM-manage a través de Intune, y enviar el perfil a través de Apple Configurator

También puede consultar nuestra documentación de [registro de Intune](#) y nuestra [guía PDF](#) aquí

Nota: este método muestra cómo realizar MDM en los dispositivos mediante Intune y Apple Configurator

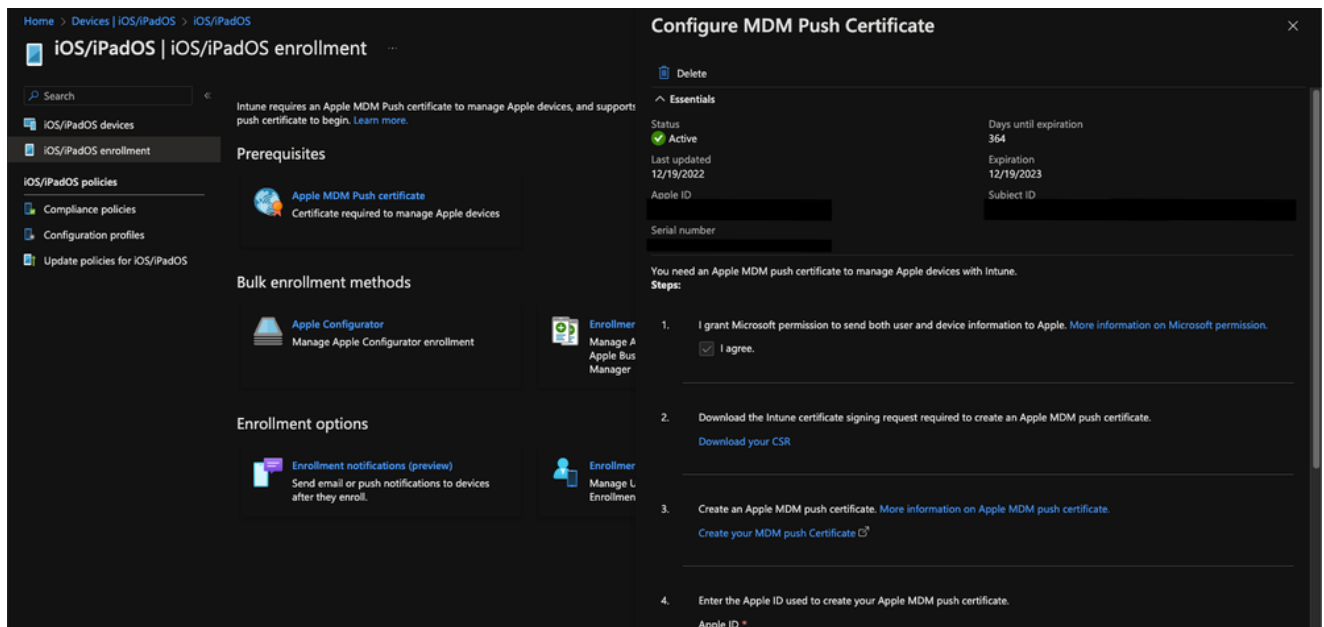
Notas Importantes:

Si está realizando una gestión de dispositivos móviles (MDM) en sus dispositivos supervisados a través de la aplicación Company Portal App, puede comenzar en el paso 14.

Este artículo se proporciona tal cual desde el 12/04/2023, la asistencia de Umbrella no garantiza que estas instrucciones sigan siendo válidas después de esta fecha y está sujeto a cambios según las actualizaciones de Microsoft Intune y Apple iOS.

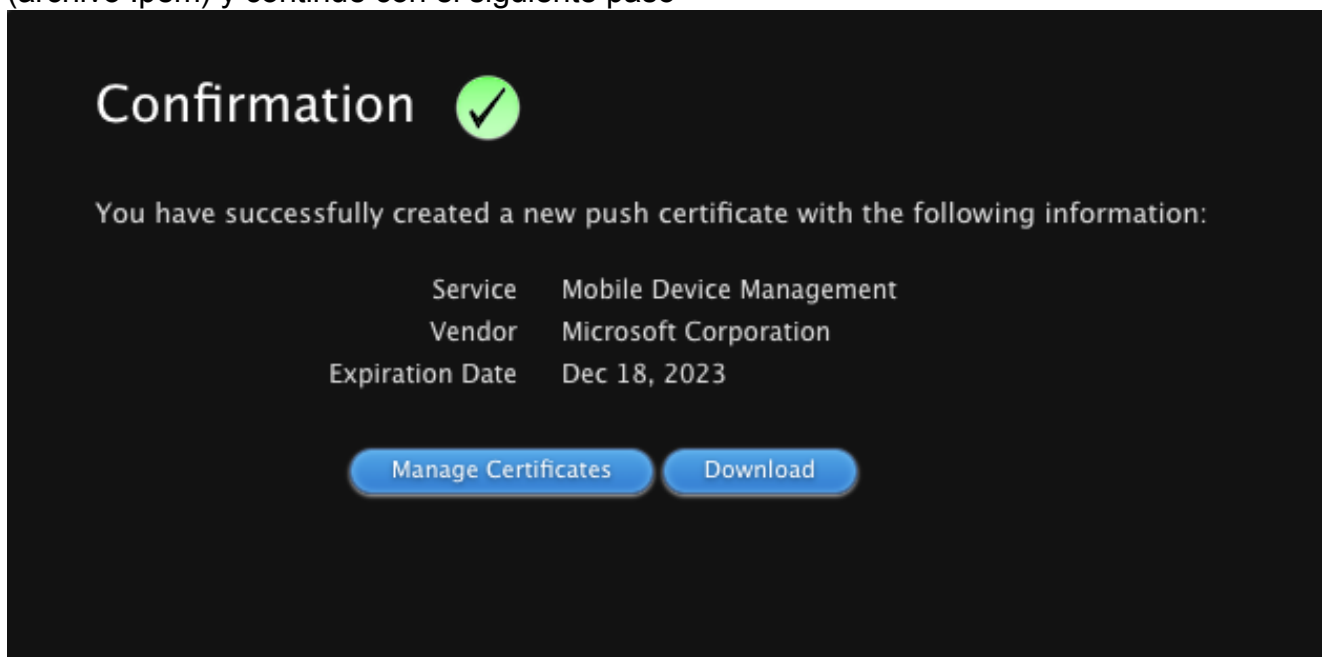
Procedimiento

1. Inicie sesión en el Portal de Azure y busque "Intune". También puede visitar https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/ e iniciar sesión
2. Una vez que esté en la página de inicio de Intune, vaya a Devices → iOS/iPadOS → iOS/iPadOS enrollment → Apple MDM Push certificate y haga clic en "Download your CSR" (Descargue su CSR)



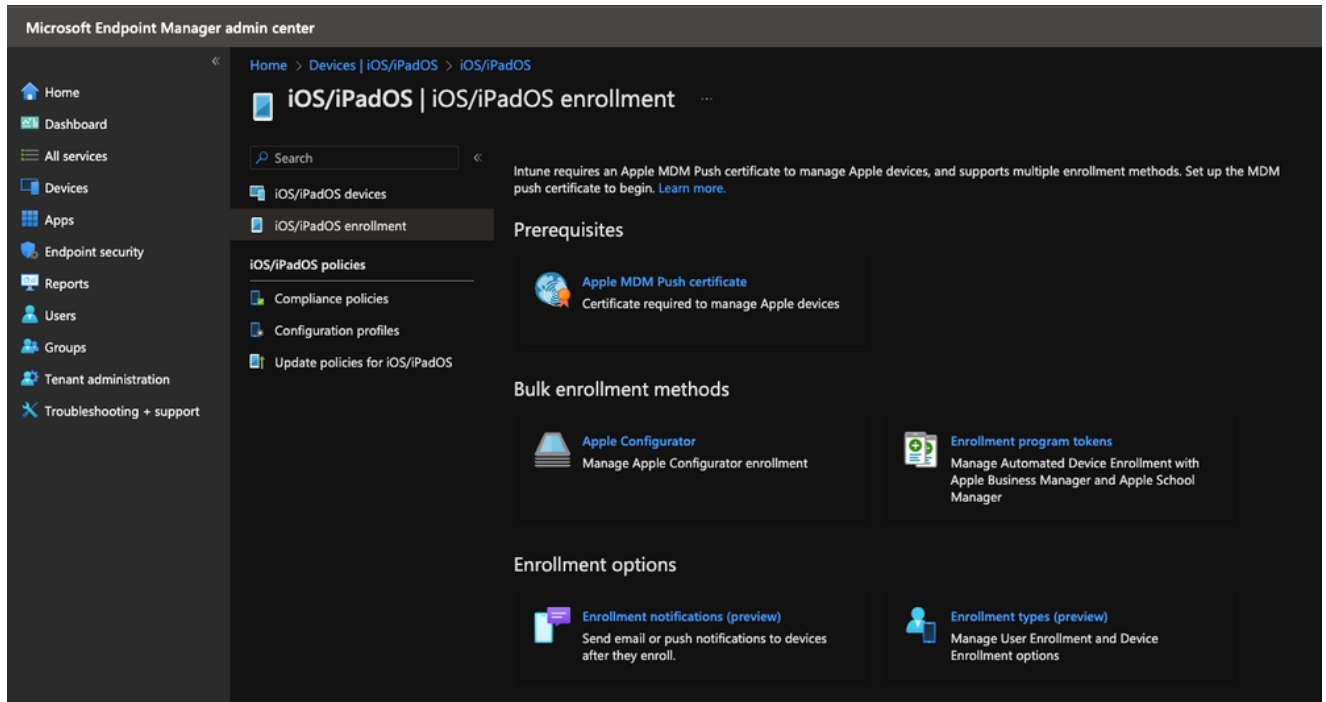
11752925317012

3. A continuación, haga clic en "Create your MDM push Certificate" (Crear certificado de inserción de MDM), que le redirigirá a <https://identity.apple.com/pushcert/>
4. En el portal de certificados push de Apple, vaya a "Crear un certificado" y cargue el archivo IntuneCSR.csr que acaba de descargar. Una vez que el archivo CSR se haya cargado correctamente, haga clic en "Descargar" para descargar el correo de privacidad mejorada (archivo .pem) y continúe con el siguiente paso



11752968667924

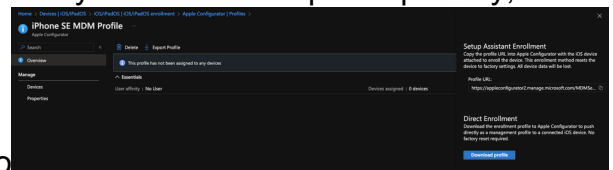
5. Introduzca la dirección de correo electrónico de la cuenta de ID de Apple que utilizó para iniciar sesión en el portal de certificados push de Apple y cargue el archivo .pem en "Apple MDM push certificate" y pulse "Cargar". Si la carga se realiza correctamente, verá las otras opciones para el desbloqueo "Métodos de inscripción masiva".



11752971407380

6. Vaya a Apple Configurator —> Profiles —> Create y cree un nuevo perfil. Dé un nombre significativo y para Afinidad de usuario seleccione "Inscribirse sin afinidad de usuario". Una vez creado el perfil, haga clic en el perfil recién creado y seleccione "Exportar perfil" y, a

continuación, "Descargar perfil" en el lado derecho



11753020728596

7. Descargue e inicie "Apple Configurator" en su macOS desde la App Store y conecte su teléfono a través de Lightning Cable. Haga clic con el botón derecho del ratón en su dispositivo dentro de Apple Configurator seleccione Add —> Profiles y luego seleccione el



archivo profile.mobileconfig que acaba de descargar

11753024446100

Alternativa de Windows: Utilidad de configuración del iPhone

8. Una vez finalizada la sincronización, en el dispositivo iOS/iPadOS, vaya a la aplicación Configuración y vaya a General —> VPN & Device Management —> Perfil de gestión

No SIM 

4:25 PM

@ 69% 



VPN & Device Management



VPN

Not Connected >

[Sign In to Work or School Account...](#)

DOWNLOADED PROFILE



Management Profile



Cancel

Install Profile

Install



Management Profile

Signed by IOSProfileSigning.manage.microsoft.com

Verified ✓

Description Install this profile to get access to your company apps

Contains Device Enrollment Challenge

More Details



Remove Downloaded Profile

Profile Installed

[Done](#)



Management Profile

Default Directory

Signed by IOSProfileSigning.manage.microsoft.com

Verified ✓

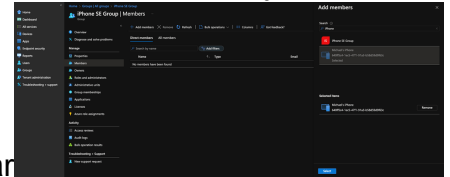
Description Install this profile to get access to your company apps

Contains Mobile Device Management
Device Identity Certificate
2 Certificates

More Details



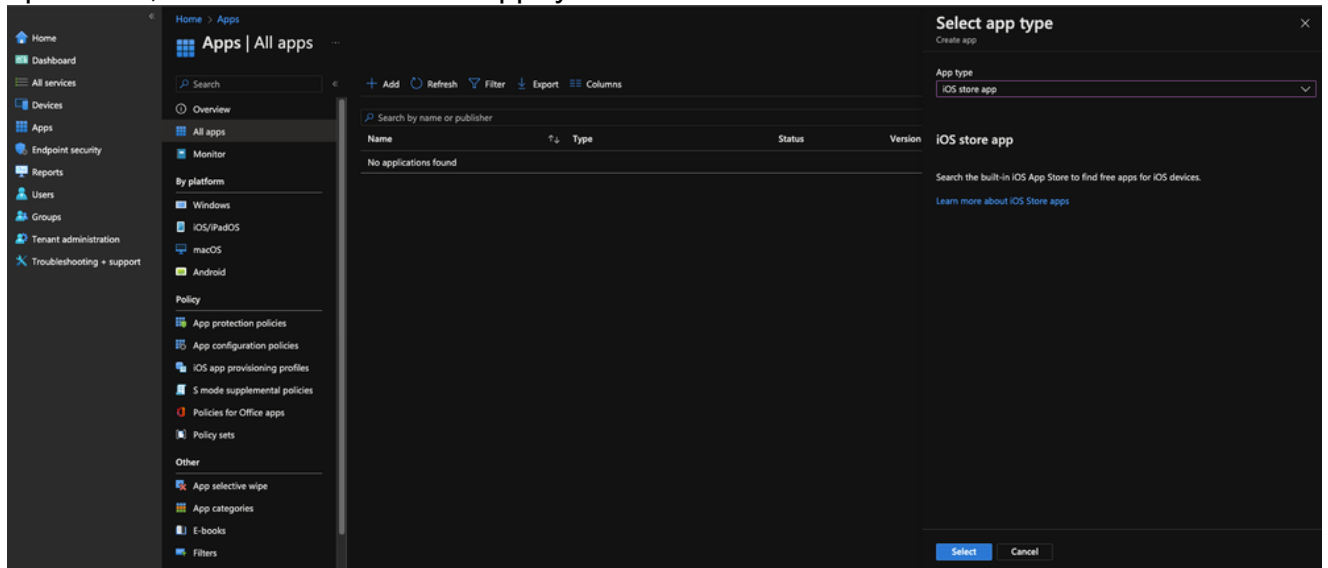
. Busque el dispositivo MDM en el que desea instalar la aplicación Cisco Security



Connector, en la lista y agréguelo al grupo que acaba de crear

11753692550036

14. Vaya a Aplicaciones —> Todas las aplicaciones —> Agregar. A continuación, para el tipo de aplicación, seleccione "iOS store app" y confirme haciendo clic en "Seleccionar"



11753797372436

15. Seleccione "Buscar App Store" e introduzca "Cisco Security Connector" en la barra de búsqueda y seleccione la aplicación "Cisco Security Connector" haciendo clic en "Seleccionar"

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

Select app * ⓘ Search the App Store

Name * ⓘ Cisco Security Connector

Description * ⓘ This application requires licenses for Cisco Clarity and/or Cisco Umbrella.

Publisher * ⓘ Cisco

Appstore URL https://apps.apple.com/us/app/cisco-security-connector/id1282518969?uo=4

Minimum operating system * ⓘ iOS 8.0

Applicable device type * ⓘ 2 selected

Category ⓘ 0 selected

Show this as a featured app in the Company Portal ⓘ Yes No

Information URL ⓘ Enter a valid url

Privacy URL ⓘ Enter a valid url

Developer ⓘ

Owner ⓘ

Previous Next

11753844054420

16. En Asignaciones, agregue el grupo que ha creado en los pasos anteriores que contiene su dispositivo MDM y, a continuación, continúe con Revisar y crear

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

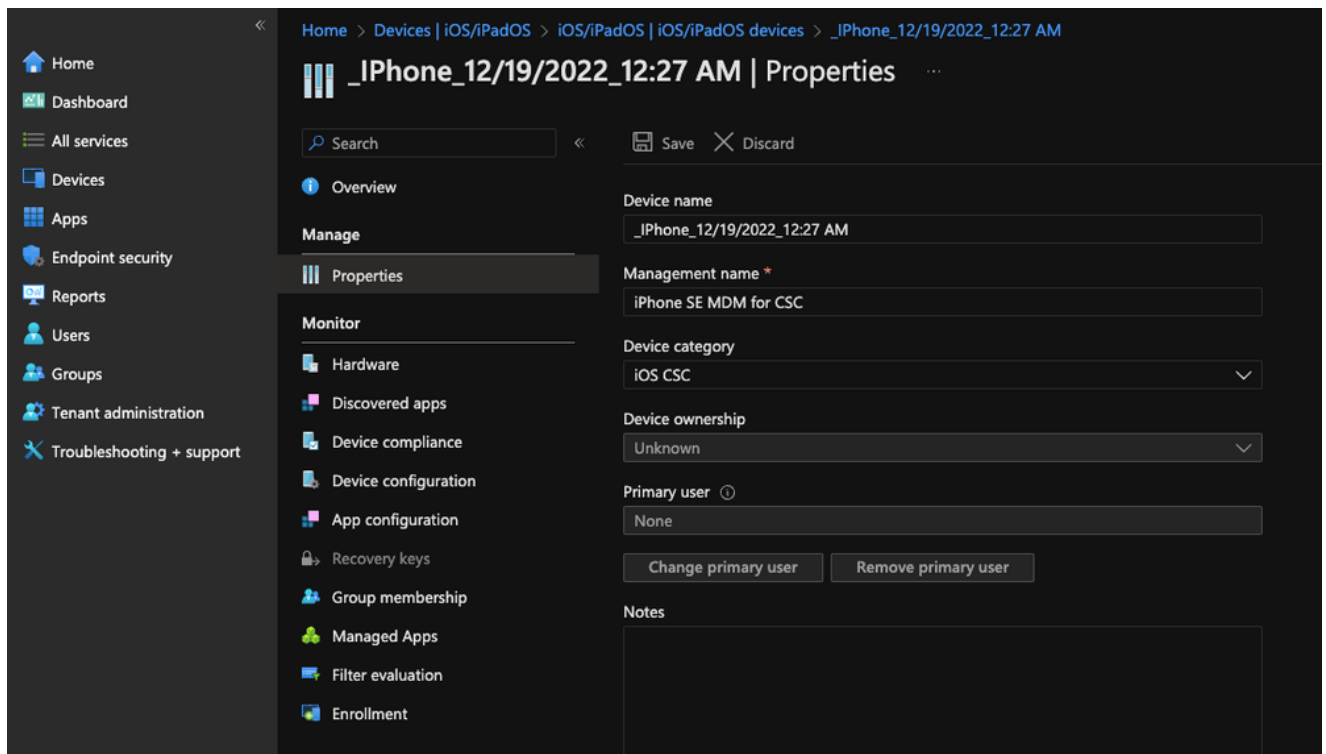
Required ⓘ

Group mode	Group	Filter mode	Filter	VPN	Uninstall on device re...	Install as removable	
⊕ Included	iPhone SE Group	None	None	None	No	Yes	...

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

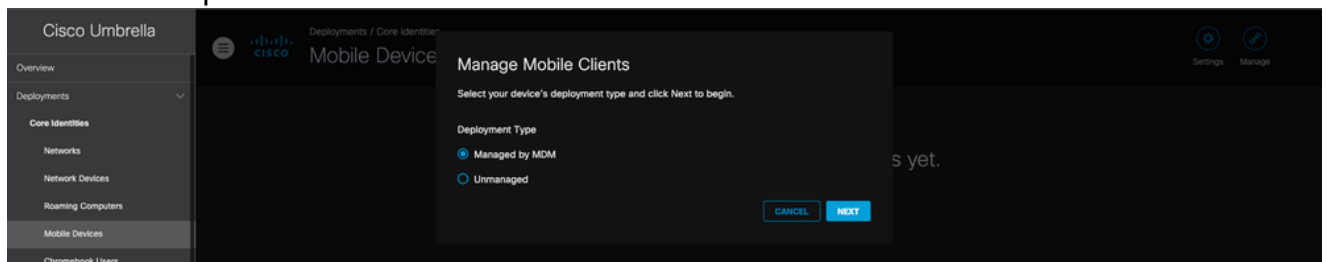
11753839516692

17. [Paso opcional] Vaya a Devices → iOS/iPadOS → iOS/iPadOS devices → Properties → Device Category, cree un perfil y asígnelo al dispositivo



11753916236820

18. Inicie sesión en el panel de Cisco Umbrella, en Implementaciones —> Identidades principales —> Dispositivos móviles —> parte superior derecha: Administrar —> Administrado por MDM



11753923081492

19. A continuación, vaya a iOS —> Descarga de configuración de Microsoft Intune. Introduzca la dirección de correo electrónico a la que desea que vayan los mensajes cuando los usuarios seleccionen "Informar de un problema" en la aplicación Cisco Security Connector

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

iOS Configuration File

Cisco Meraki

[Link MDM](#)

Apple

[Apple Config](#) 

IBM Maas360

[IBM Maas360 Config](#) 

Microsoft Intune

[Microsoft Intune Config](#) 

Jamf

[Jamf Config](#) 

MobiConnect

[MobiConnect Config](#) 

MobileIron

[MobileIron Config](#) 

Workspace ONE

[Workspace ONE Config](#) 

Common Config 

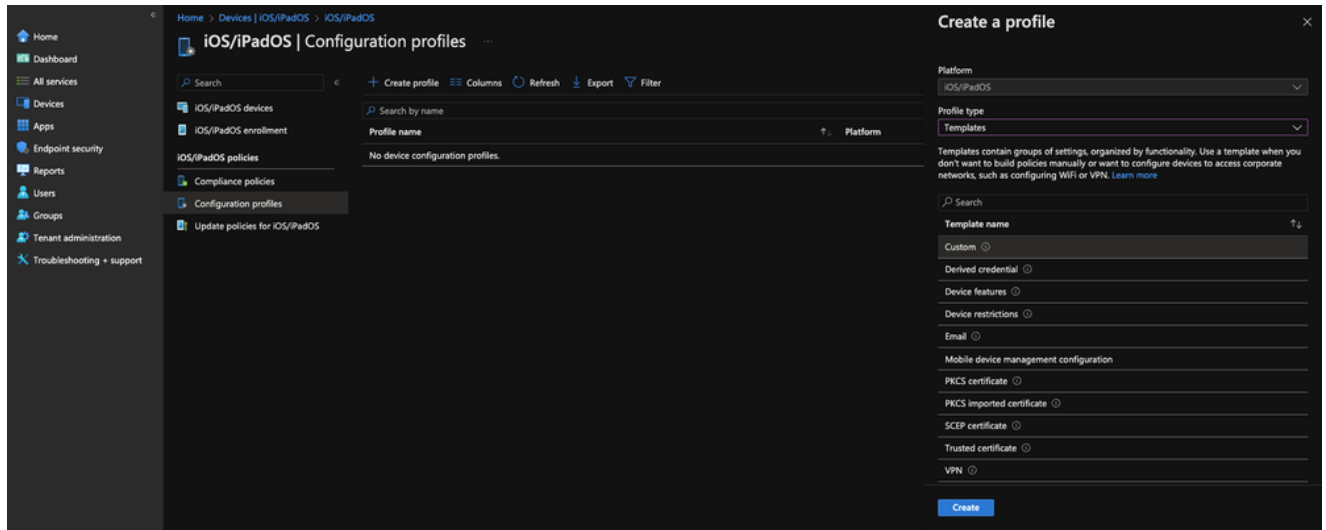
[iOS Config](#) 

BACK

DONE

11753924523540

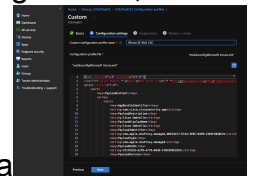
20. Vuelva al portal de Intune, en Dispositivos —> iOS/iPadOS —> Perfiles de configuración —> Crear perfil —> Plantillas —> Personalizado



11753988354964

21. Asigne un nombre descriptivo al perfil de configuración. En el Paso 2 - Configuración,

cargue el archivo XML que acaba de descargar del panel de Cisco Umbrella



11754000962196

22. En Asignaciones, asigne el grupo que ha creado anteriormente que contiene su dispositivo MDM y seleccione "Revisar y crear"
23. Vuelva a los dispositivos iOS/iPadOS y seleccione su dispositivo MDM y haga clic en sync en la parte superior y obtendrá una ventana emergente en su dispositivo MDM iOS/iPadOS para instalar la aplicación Cisco Security Connector

No SIM



4:30 AM



VPN & Device Management

VPN

VPN

Not Connected



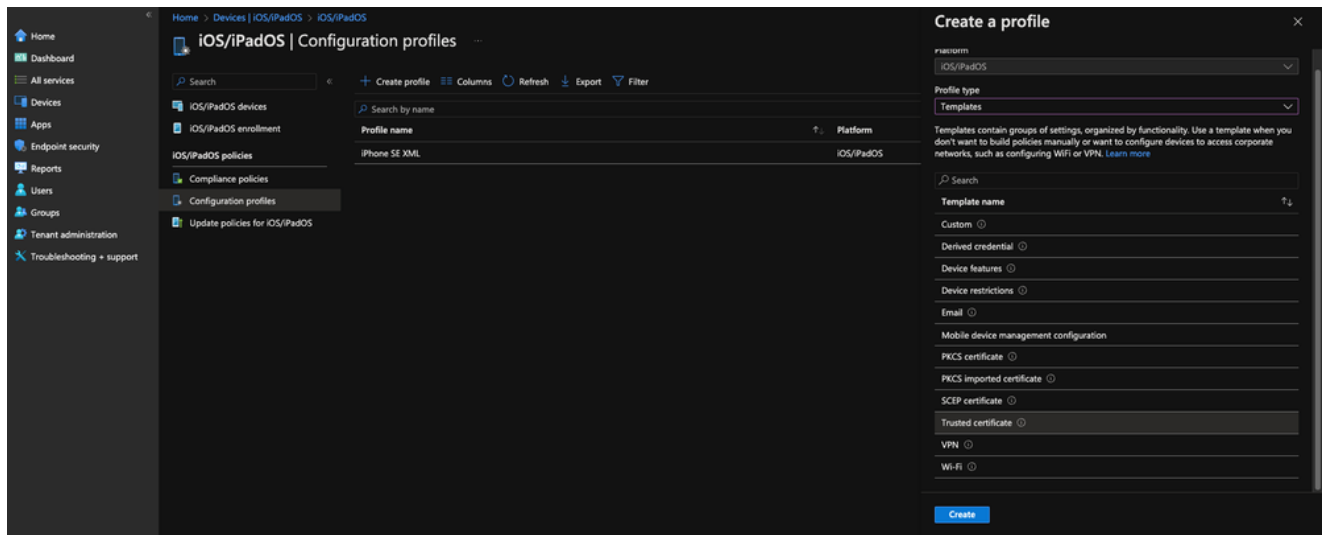
MOBILE DEVICE MANAGEMENT

App Installation

Default Directory is about to install and manage the app "Cisco Security Connector" from the App Store. Your iTunes account will not be charged for this app.

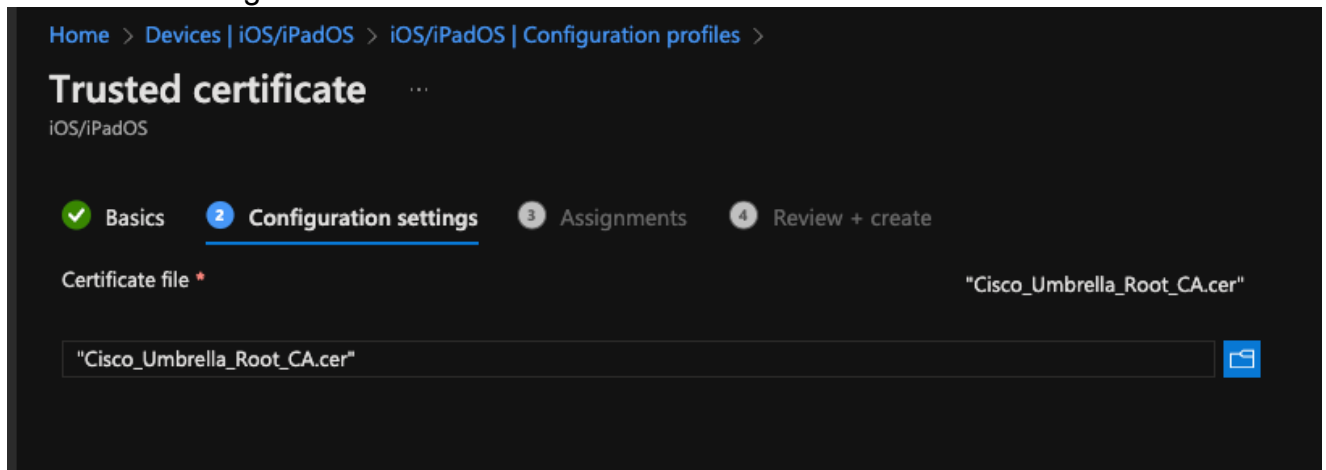
Cancel

Install



11754159037460

29. En el Paso 2 - Configuración de configuración, cargue el certificado raíz de Umbrella que acaba de descargar del Paso 27



11754204605460

30. Para el Paso 3 - Asignaciones, seleccione el grupo que contiene su dispositivo MDM iOS/iPadOS y haga clic en "Siguiente" y "Crear"
31. Vuelva a los dispositivos iOS/iPadOS, seleccione el dispositivo MDM y vuelva a pulsar la tecla de sincronización en la parte superior (como en el paso 24)
32. Cierre y vuelva a iniciar la aplicación Cisco Security Connector. Ahora verá el estado como "Protegido por paraguas"

No SIM 

4:41 AM



Status

DNS SECURITY



Protected by Umbrella



ENDPOINT VISIBILITY



Clarity Not Configured

No SIM



4:48 AM



Cisco Umbrella



Welcome to Umbrella!

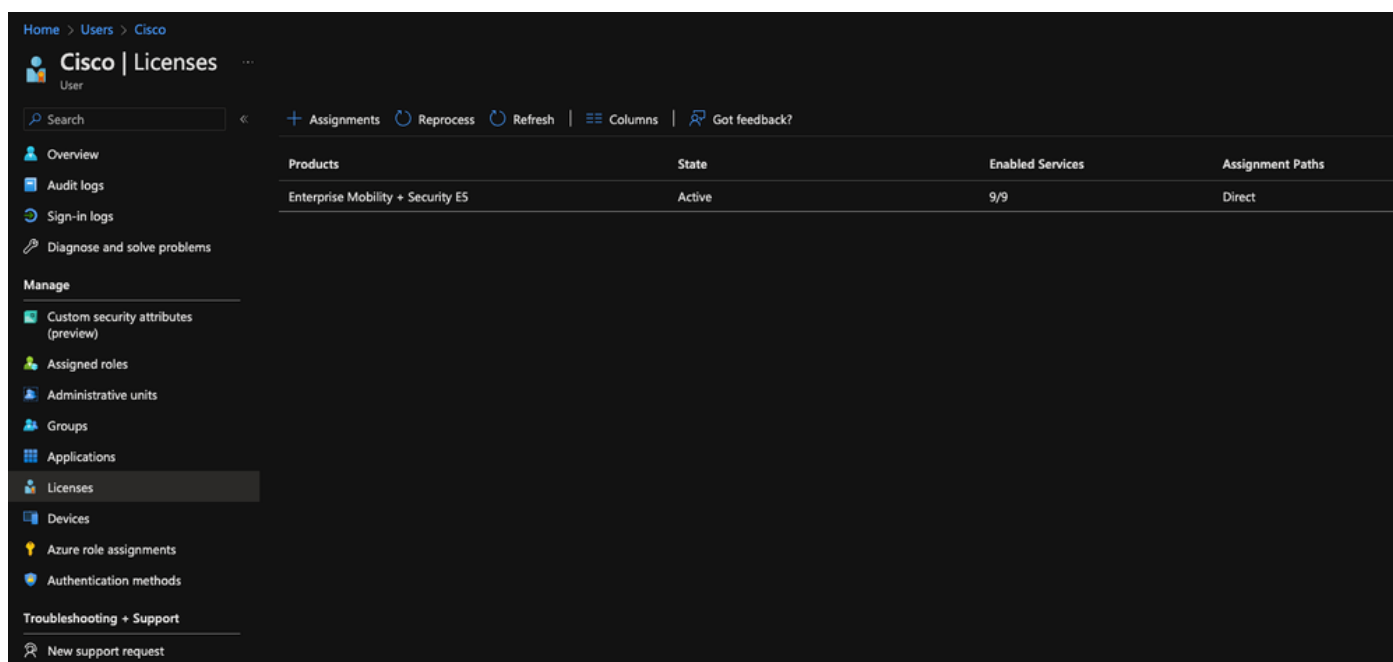
Your internet is faster,
more reliable and better
protected because
you're using Cisco
Umbrella.

- No puede tener ninguna configuración de "Aplicaciones restringidas" que restrinja la aplicación Umbrella ni ninguna configuración de "Mostrar u ocultar" para ocultar la aplicación Umbrella aplicada en el perfil de configuración del dispositivo.(En Intune admin center > Dispositivos > iOS/iPadOS > Configuración)

Resolución de problemas

- Cómo recopilar los registros de diagnóstico de Cisco Security Connector
- Error de registro de CSC "Informar de un problema" Función "Sin correo electrónico de administración"
- CSC: Estado "desprotegido" en las redes móviles

Si aparece un mensaje de error: "Nombre de usuario no reconocido. Este usuario no está autorizado a utilizar Microsoft Intune", vaya al Portal de Azure, en "Usuarios" y seleccione el nombre de usuario o la cuenta que está utilizando para configurar Intune, vaya a "Licencias" y asegúrese de que tiene una licencia de Intune activa asignada al usuario



Home > Users > Cisco

Cisco | Licenses

User

Search

Assignments Reprocess Refresh Columns Got feedback?

Products	State	Enabled Services	Assignment Paths
Enterprise Mobility + Security ES	Active	9/9	Direct

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

11754557401748

Registros

De forma predeterminada, la contraseña de los registros es bypass_email_filters. También se puede encontrar en el archivo UmbrellaProblemReport.txt

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).