

Beveiligingsconnector implementeren met Intune

Inhoud

[Inleiding](#)

[Overzicht](#)

[Procedure](#)

[Beperkingen](#)

[Probleemoplossing](#)

[Logboeken](#)

Inleiding

In dit document wordt beschreven hoe u de beveiligingsconnector kunt implementeren met Intune.

Overzicht

Dit is een stap-voor-stap handleiding over hoe u uw iOS / iPadOS-apparaat MDM-beheren via Intune, en druk op het profiel via Apple Configurator

U kunt ook verwijzen naar onze [Intune Registratie](#) documentatie en [PDF-gids](#) hier

Opmerking: deze methode laat u zien hoe u uw MDM-apparaten kunt gebruiken via Intune en Apple Configurator

Belangrijke opmerkingen:

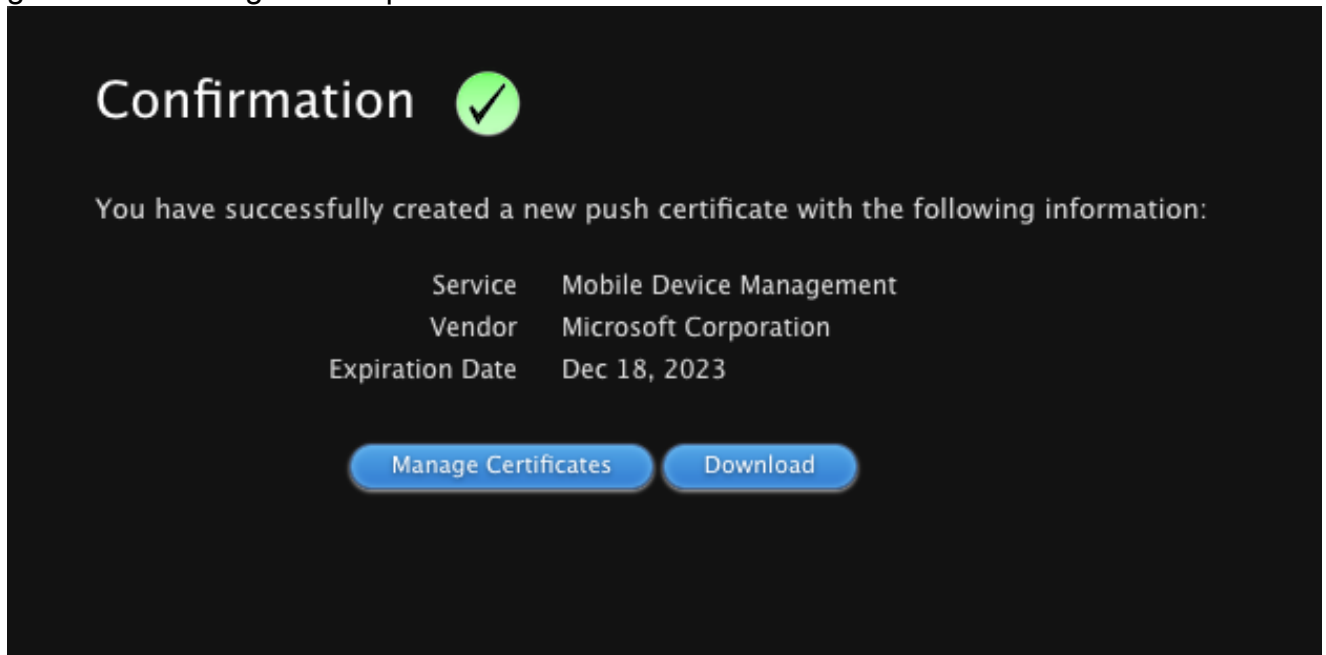
Als u MDM-ing uw begeleid apparaten via de Company Portal App, dan kunt u beginnen bij stap 14.

Dit artikel wordt geleverd vanaf 04/12/2023, Umbrella-ondersteuning garandeert niet dat deze instructies na deze datum geldig blijven en kan worden gewijzigd op basis van updates van Microsoft Intune en Apple iOS.

Procedure

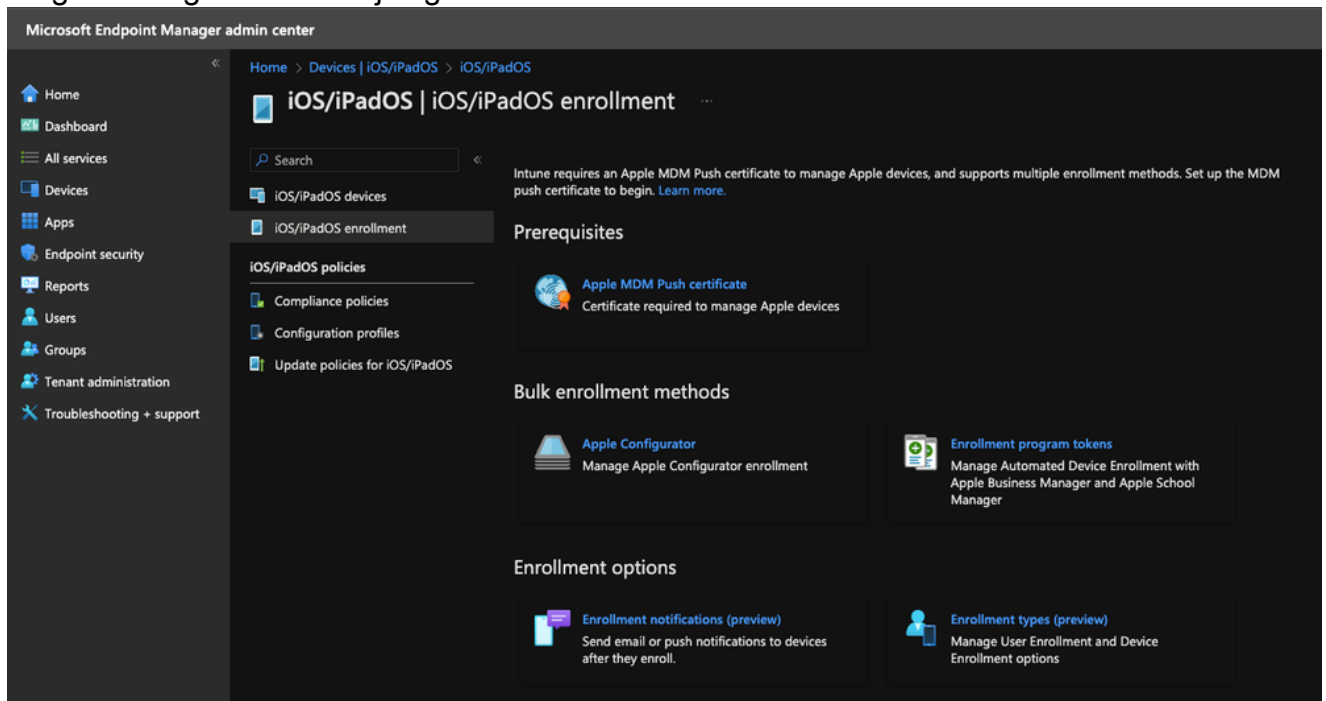
1. Log in op de Azure Portal en zoek naar "Intune". U kunt ook naar https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/ gaan en inloggen
2. Zodra u op de Intune-startpagina bent, gaat u naar Apparaten --> iOS/iPadOS --> iOS/iPadOS-inschrijving --> Apple MDM Push-certificaat en klikt u op "Download uw CSR" 
- 11752925317012
3. Klik vervolgens op "Create your MDM push Certificate", die u doorverwijst naar <https://identity.apple.com/pushcert/>

4. Ga op het Apple Push Certificates Portal naar "Create a Certificate" en upload het zojuist gedownloadte IntuneCSR.csr-bestand. Zodra het CSR-bestand succesvol is geüpload, klikt u op "Downloaden" om het bestand Privacy Enhanced Mail (.pem) te downloaden en door te gaan naar de volgende stap



11752968667924

5. Voer het e-mailadres van uw Apple ID-account in dat u hebt gebruikt om u aan te melden bij het Apple Push Certificates Portal en upload het .pem-bestand onder "Apple MDM push certificate" en druk op "Upload". Als de upload succesvol is, ziet u de andere opties voor de ontgrendeling "Bulkinschrijvingsmethoden".



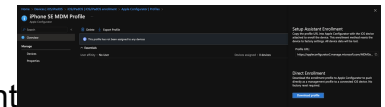
11752971407380

6. Ga naar Apple Configurator --> Profielen --> Een nieuw profiel maken. Geef het een zinvolle naam en selecteer "Inschrijven zonder gebruikersaffiniteit" voor gebruikersaffiniteit. Zodra

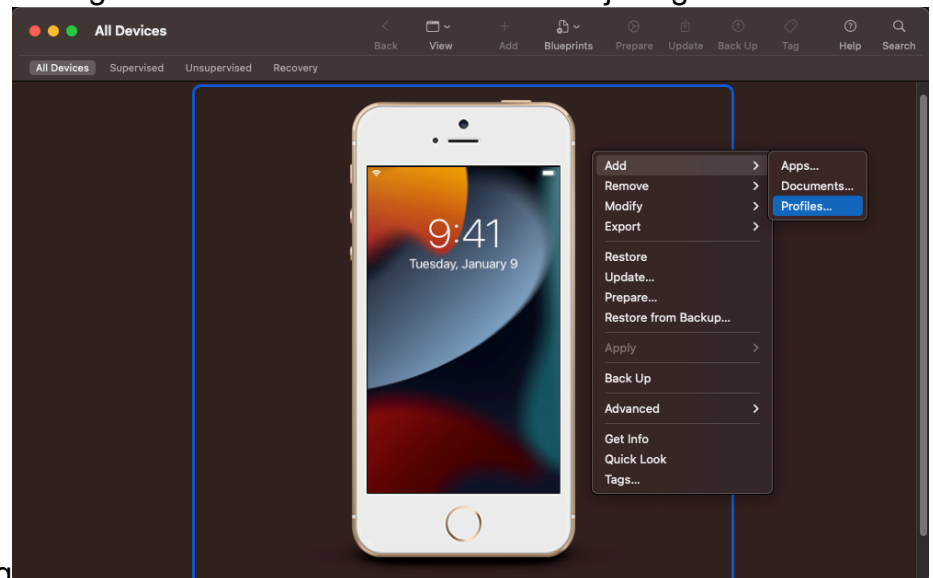
dat profiel is gemaakt, klikt u in uw nieuw aangemaakte profiel en selecteert u "Profiel

exporteren" en vervolgens "Profiel downloaden" aan de rechterkant

11753020728596



7. Download en start "Apple Configurator" op uw macOS vanuit de App Store en sluit uw telefoon aan via de Lightning-kabel. Klik met de rechtermuisknop op uw apparaat in Apple Configurator en selecteer Toevoegen --> Profielen en selecteer het zojuist gedownloade



bestand profile.mobileconfig

11753024446100

Windows Alternatief: iPhone Configuration Utility

8. Zodra de synchronisatie is voltooid, gaat u op uw iOS / iPadOS-apparaat naar de app Instellingen en gaat u naar Algemeen -> VPN en apparaatbeheer -> Beheerprofiel

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 ✓

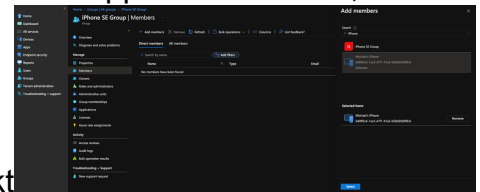
Description Install this profile to get access to your company apps

Contains Mobile Device Management
Device Identity Certificate
2 Certificates

More Details



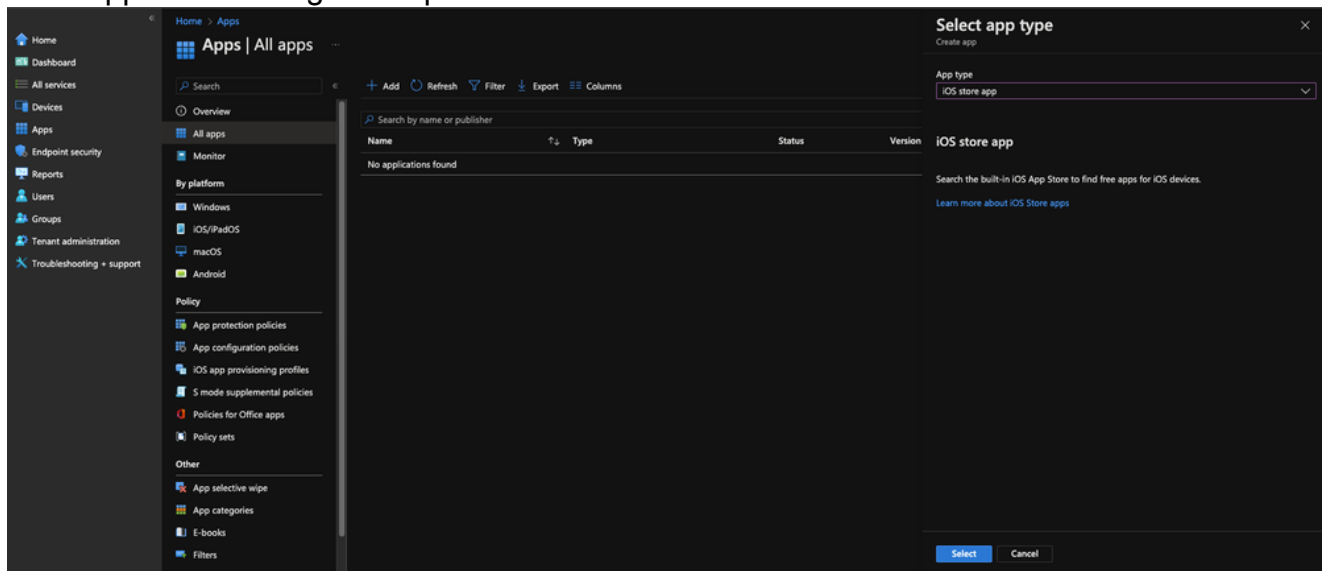
. Zoek uw MDM-apparaat waarop u de Cisco Security Connector-app wilt installeren, in de



lijst en voeg het toe aan de groep die u zojuist hebt gemaakt

11753692550036

14. Ga naar Apps --> Alle apps --> Toevoegen. Selecteer vervolgens voor het type App "iOS store app" en bevestig door op "Selecteren" te klikken



11753797372436

15. Selecteer "Zoeken naar App Store" en voer "Cisco Security Connector" in de zoekbalk in en selecteer de app "Cisco Security Connector" door op "Selecteren" te klikken

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. Voeg onder Toewijzingen de groep toe die u in de eerdere stappen hebt gemaakt en die uw MDM-apparaat bevat en ga vervolgens verder met Bekijken en maken

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

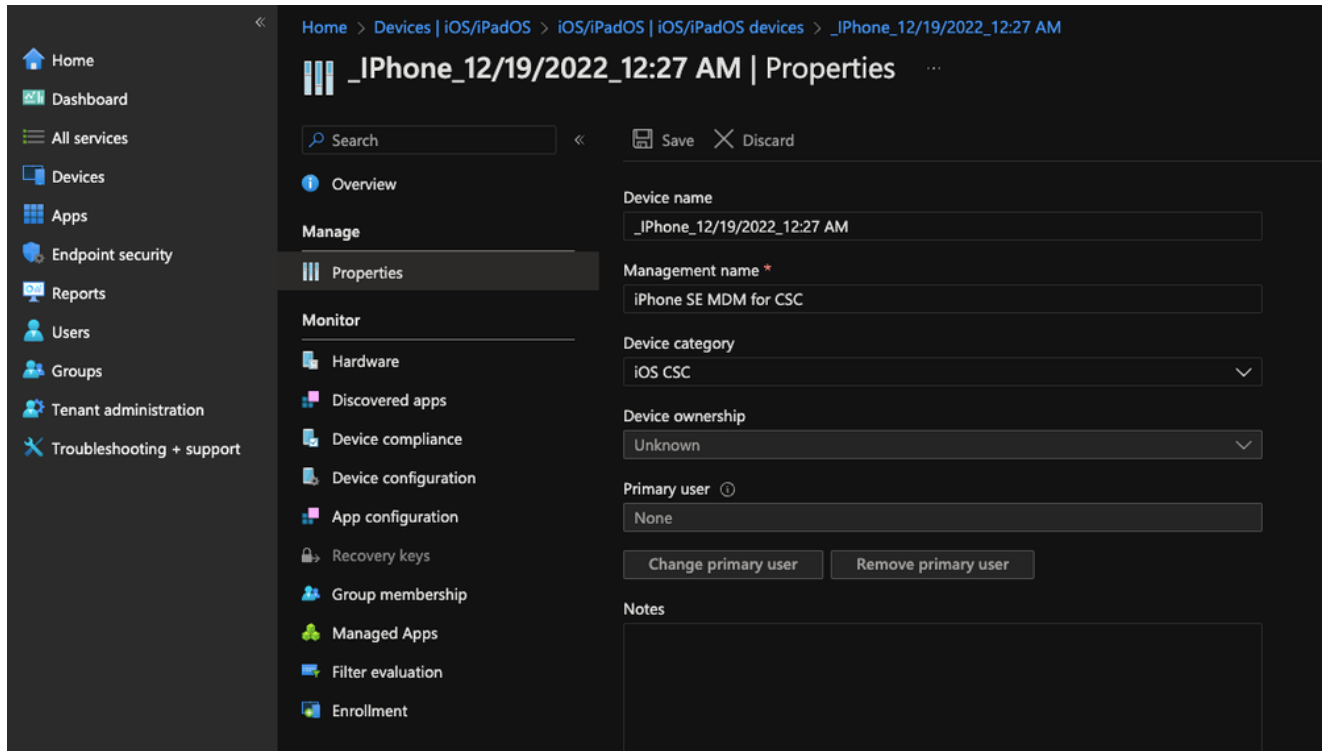
Required ⓘ

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 ⓘ

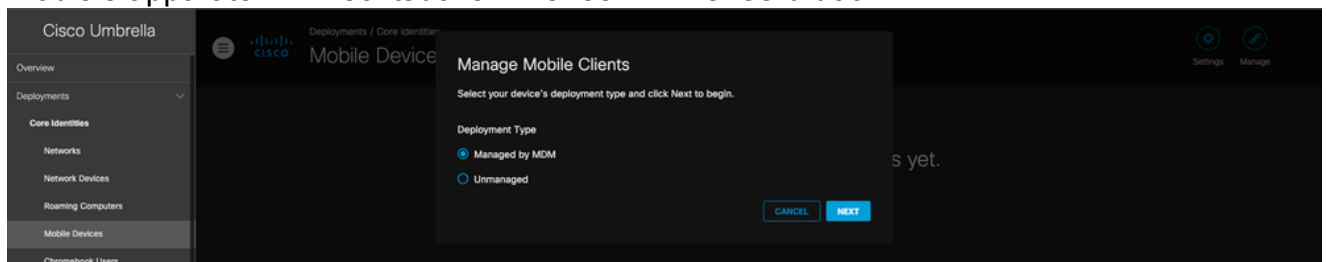
11753839516692

17. [Optionele stap] Ga naar Apparaten --> iOS/iPadOS --> iOS/iPadOS-apparaten --> Eigenschappen --> Apparaatcategorie, maak een profiel en wijs het toe aan het apparaat



11753916236820

18. Meld u aan bij uw Cisco Umbrella-dashboard onder Implementaties --> Core Identities --> Mobiele apparaten --> rechtsboven: Beheer --> Beheerd door MDM



11753923081492

19. Ga dan naar iOS --> Microsoft Intune Config download. Voer het e-mailadres in waarnaar u e-mails wilt sturen wanneer gebruikers "Een probleem melden" selecteren in de Cisco Security Connector-app

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 

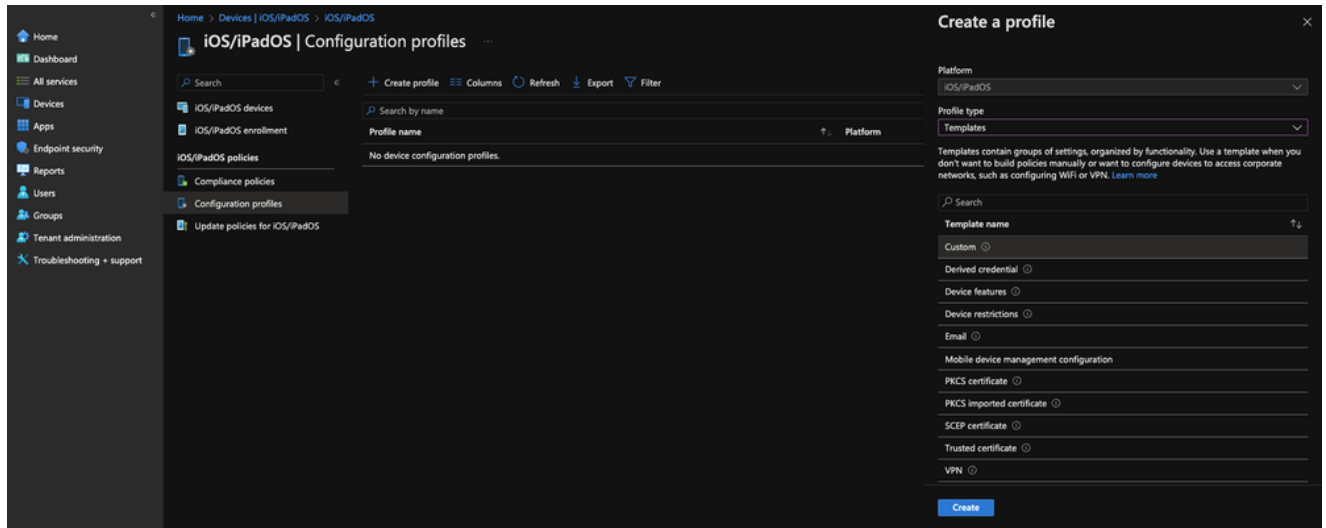
[iOS Config](#) 

BACK

DONE

11753924523540

20. Ga terug naar uw Intune-portal, onder Apparaten --> iOS/iPadOS --> Configuratieprofielen --> Profiel maken --> Sjablonen --> Aangepast



11753988354964

21. Geef het een zinvolle naam voor uw configuratieprofiel. In stap 2 - Configuratie-instellingen, upload het XML-bestand dat u zojuist hebt gedownload van uw Cisco Umbrella-dashboard

11754000962196

22. Wijs onder Toewijzingen de groep toe die u eerder hebt gemaakt en die uw MDM-apparaat bevat en selecteer "Bekijken en maken"
23. Ga terug naar iOS / iPadOS-apparaten en selecteer uw MDM-apparaat en druk bovenaan op synchroniseren en u krijgt een pop-up op uw MDM iOS / iPadOS-apparaat om de Cisco Security Connector-app te installeren

No SIM



4:30 AM



VPN & Device Management

VPN

VPN

Not Connected



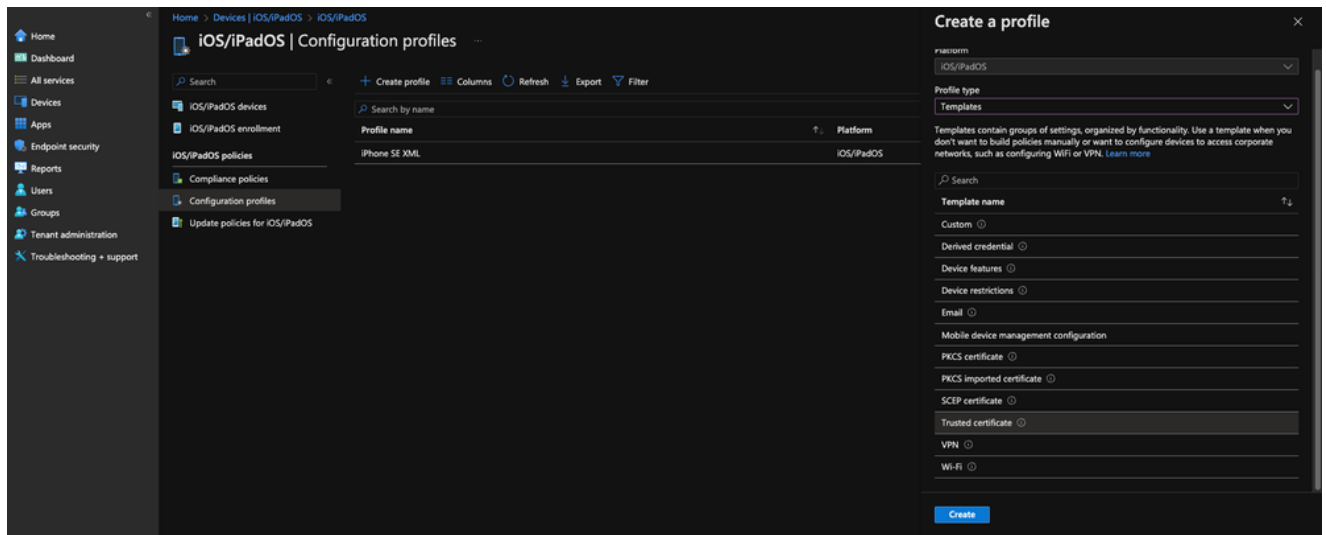
MOBILE DEVICE MANAGEMENT

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.

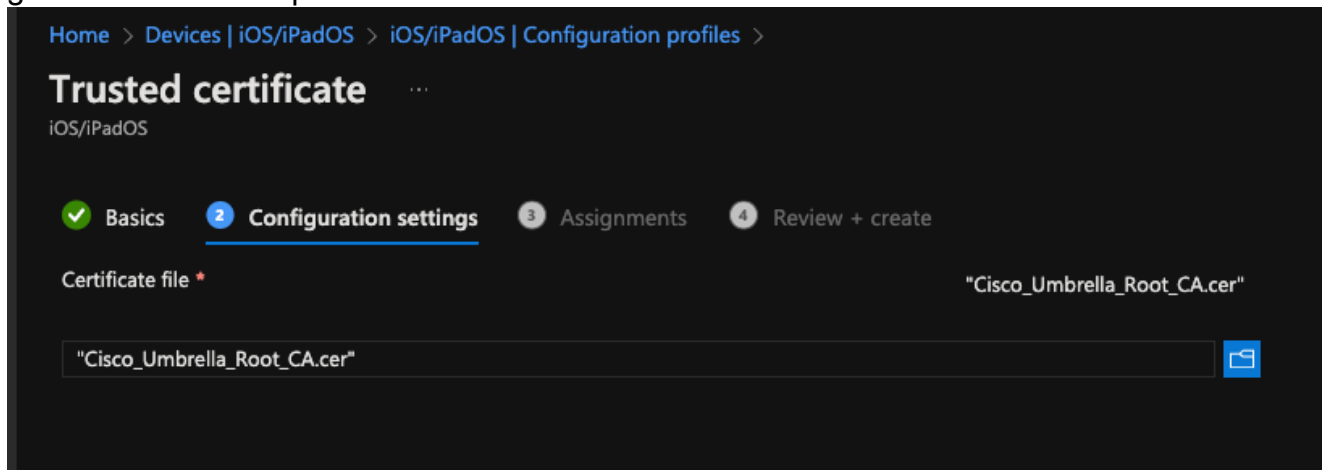
Cancel

Install



11754159037460

29. In stap 2 - Configuratie-instellingen, upload het Umbrella Root Certificate dat u zojuist hebt gedownload van stap 27



11754204605460

30. Voor Stap 3 - Toewijzingen, selecteer de groep die uw MDM iOS / iPadOS-apparaat bevat en klik op "Volgende" en "Maken"
31. Ga terug naar iOS / iPadOS-apparaten en selecteer uw MDM-apparaat en druk nogmaals op synchroniseren bovenaan (zoals stap 24)
32. Sluit de Cisco Security Connector-app en start deze opnieuw. U ziet nu de status "Beschermd door paraplu"

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!

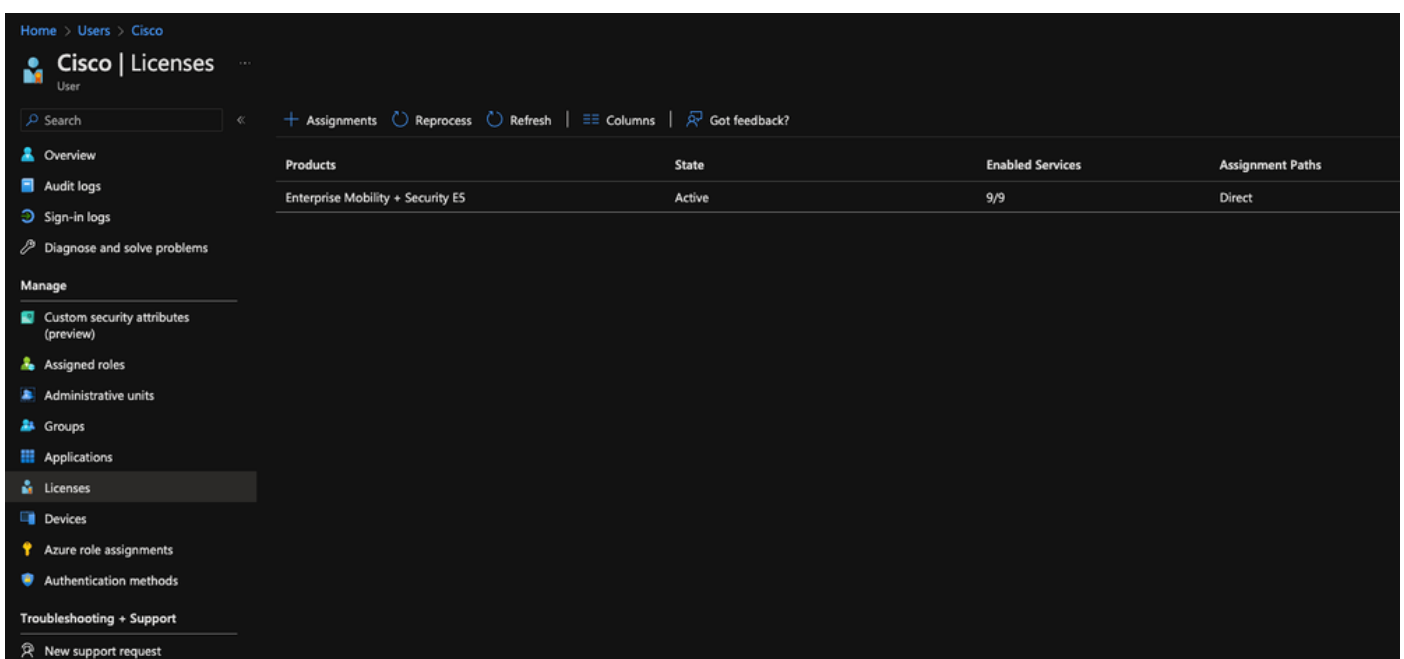
Your internet is faster,
more reliable and better
protected because
you're using Cisco
Umbrella.

- U kunt geen instelling "Beperkte apps" hebben die de Umbrella-app beperkt en/of een instelling "Weergeven of verbergen" om de Umbrella-app te verbergen die is toegepast in uw apparaatconfiguratieprofiel. (Onder uw Intune-beheercentrum > Apparaten > iOS/iPadOS > Configuratie)

Probleemoplossing

- Hoe Cisco Security Connector Diagnostics Logs te verzamelen
- CSC-log "Een probleem melden"-functie "Geen e-mail van beheerder"-fout
- CSC: status "Onbeschermd" op mobiele netwerken

Als u een fout krijgt: "Gebruikersnaam niet herkend. Deze gebruiker is niet bevoegd om Microsoft Intune te gebruiken, ga naar de Azure Portal, onder "Gebruikers" en selecteer de gebruikersnaam of account die u gebruikt om Intune te configureren, ga naar "Licenties" en zorg ervoor dat u een actieve Intune-licentie hebt toegewezen aan de gebruiker



Home > Users > Cisco

Cisco | Licenses

User

Search < + Assignments Reprocess Refresh Columns Got feedback?

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

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

11754557401748

Logboeken

Standaard is het wachtwoord voor de logs `bypass_email_filters`. Dit kan ook worden gevonden in de `UmbrellaProblemReport.txt`

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.