

AnyConnect PerApp VPN voor iOS configureren met Meraki System Manager

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1. iOS-apparaat registreren bij Meraki Systems Manager](#)

[Stap 2. Beheerde apps instellen](#)

[Stap 3. PerApp VPN-profiel configureren](#)

[Stap 4. Configuratie van App Selector](#)

[Stap 5. ASA Sample per app VPN-configuratie](#)

[Verifiëren](#)

[6. Controleer de profielinstallatie op de AnyConnect-toepassing](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u PerApp VPN kunt configureren op Apple iOS-apparaten die worden beheerd door Meraki Mobile Device Manager (MDM), System Manager (SM).

Voorwaarden

Vereisten

- AnyConnect v4.0 Plus- of Apex-licentie.
- ASA 9.3.1 of hoger ter ondersteuning van Per App VPN.
- Cisco Enterprise Application Selector - tool beschikbaar op Cisco.com

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- ASA 5506W-X versie 9.15(1)10
- iPad iOS versie 15.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

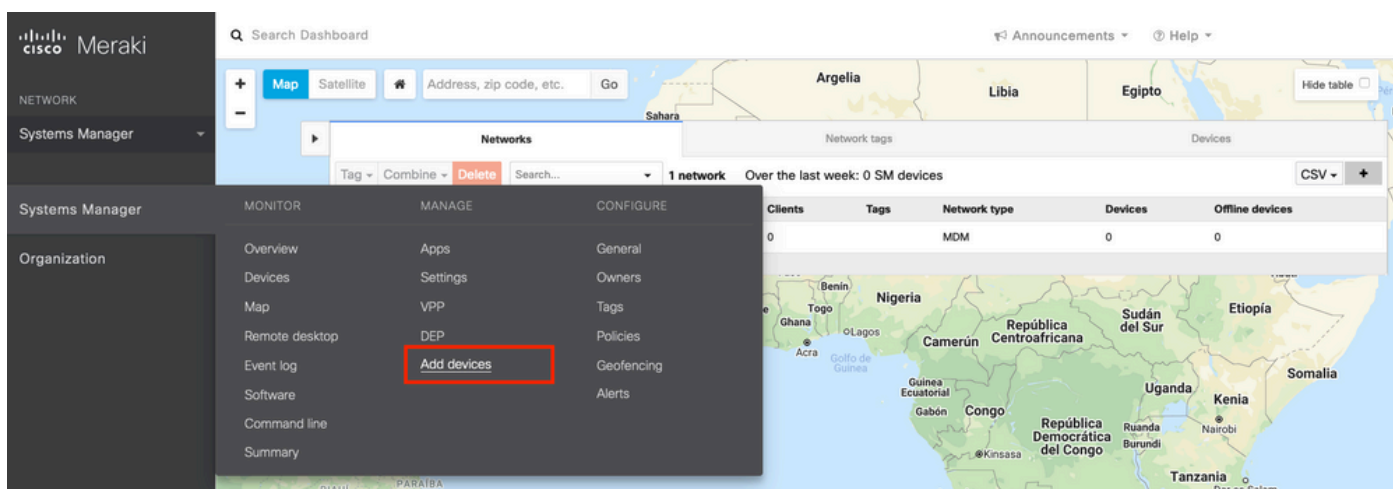
Dit document bevat niet de genoemde processen:

- SCEP CA-configuratie op Systems Manager voor het genereren van clientcertificaten
- PKCS12 clientcertificaat genereren voor de iOS-clients

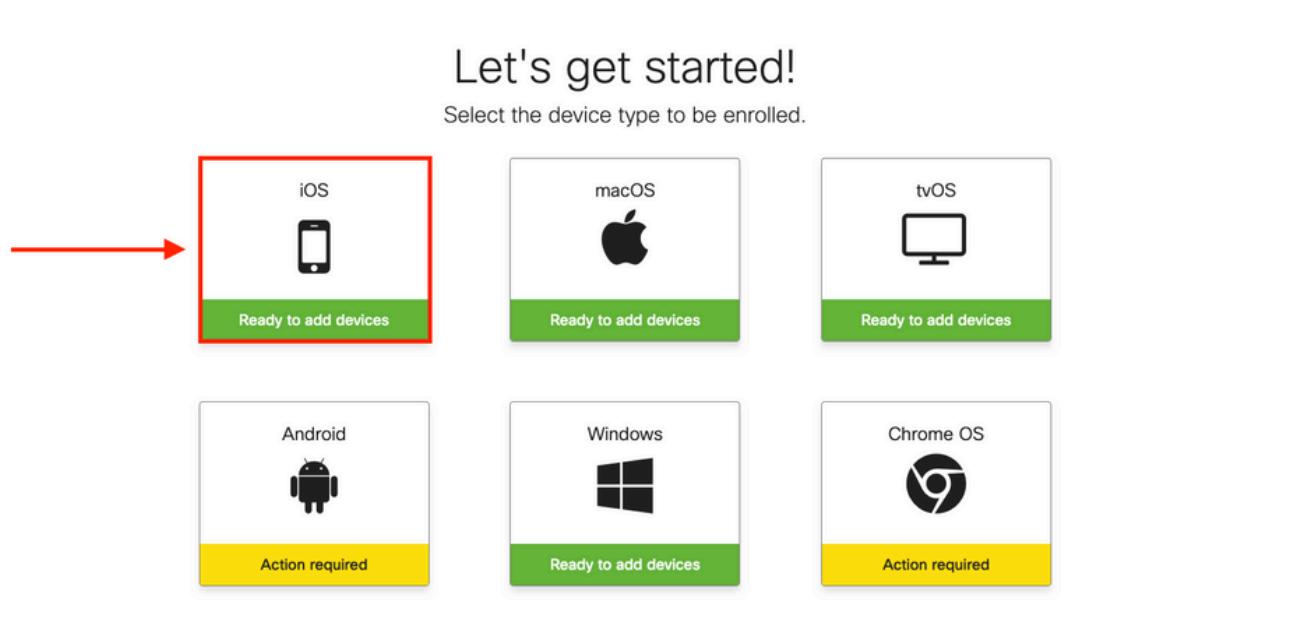
Configureren

Stap 1. iOS-apparaat registreren bij Meraki Systems Manager

1.1. Navigeren naar Systems Manager > Apparaten toevoegen



1.2. Klik op de iOS-optie om de inschrijving te starten.



1.3. Noteer het apparaat via internetbrowser of scan de QR-code met de camera. In dit document is de camera gebruikt voor het inschrijvingsproces.



Add Devices

Time to add some devices! There are a few different enrollment options for iOS - for more information, see [this article](#).

A Mobile Browser

Open m.meraki.com on the device and enter this network ID :

012


OR

Set up a [network enrollment string](#) to use as an enrollment code at m.meraki.com

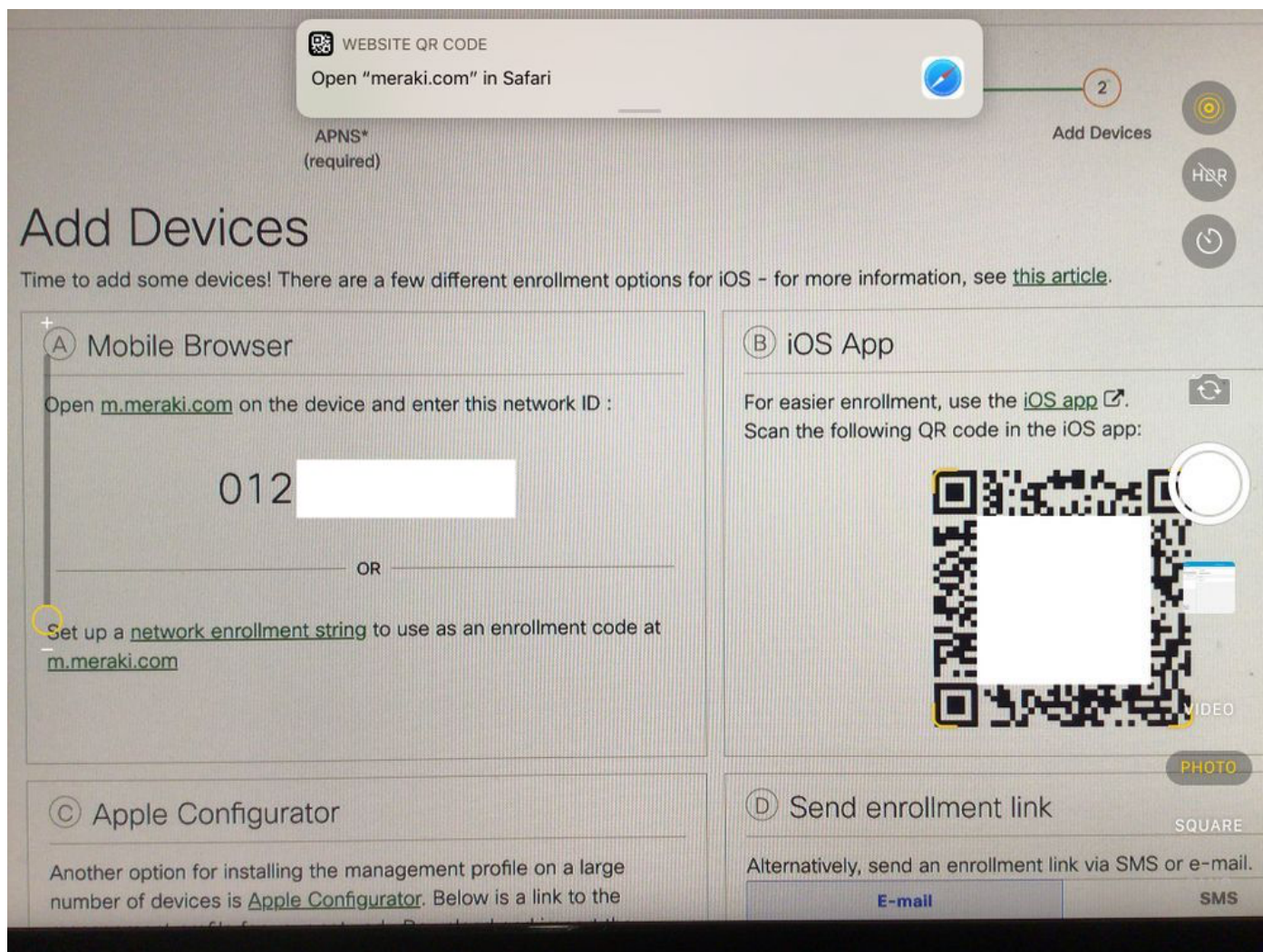
B iOS App

For easier enrollment, use the [iOS app](#).

Scan the following QR code in the iOS app:



1.4. Wanneer de QR-code wordt herkend door de camera, selecteert u de melding "meraki.com" openen in Safari.



1.5. Selecteer **Registreren** als u hierom wordt gevraagd.

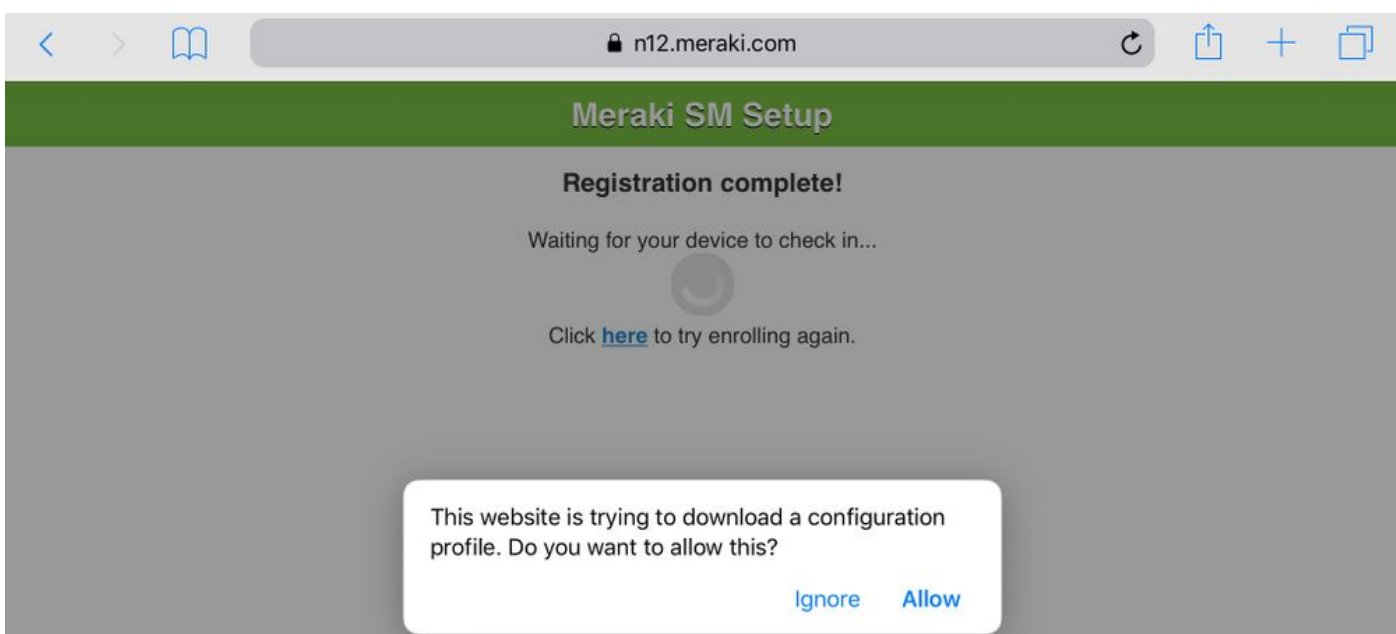


Step 1: Enter your Network ID

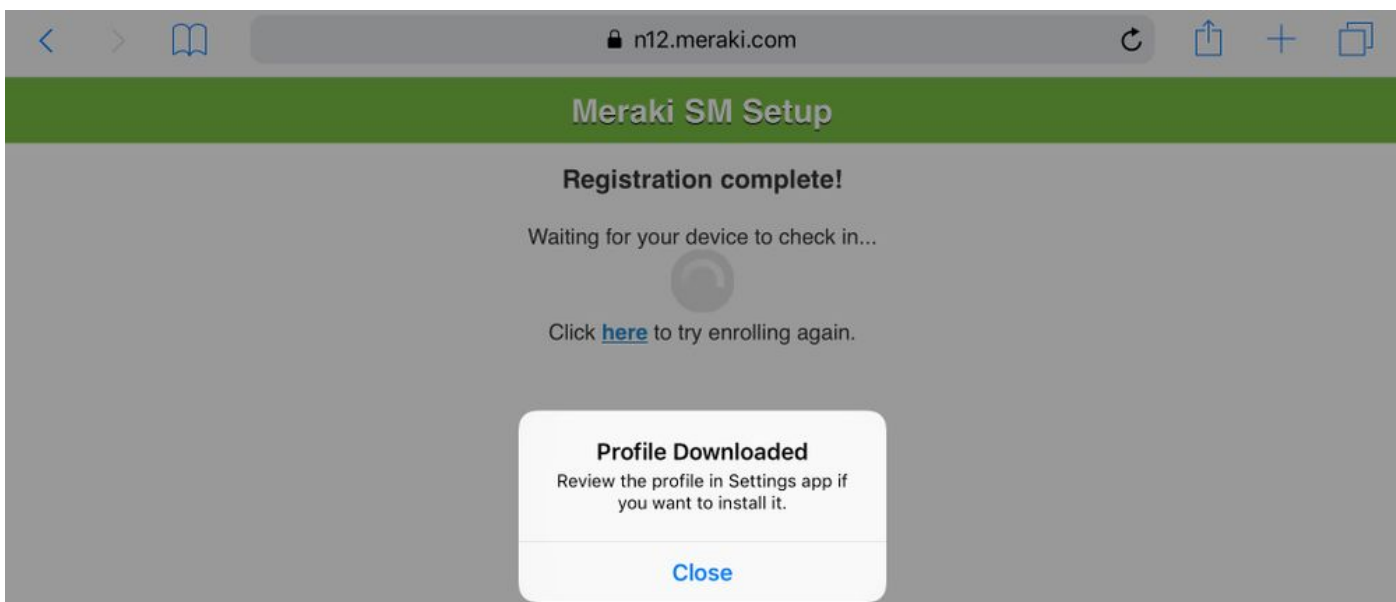
The Network ID is either a 10-digit code or a combination of letters, numbers, or characters (e.g. [123-456-7890](#) or network-id).

By installing Systems Manager on your device you acknowledge that you have read and understood the terms of our [Privacy Policy](#).

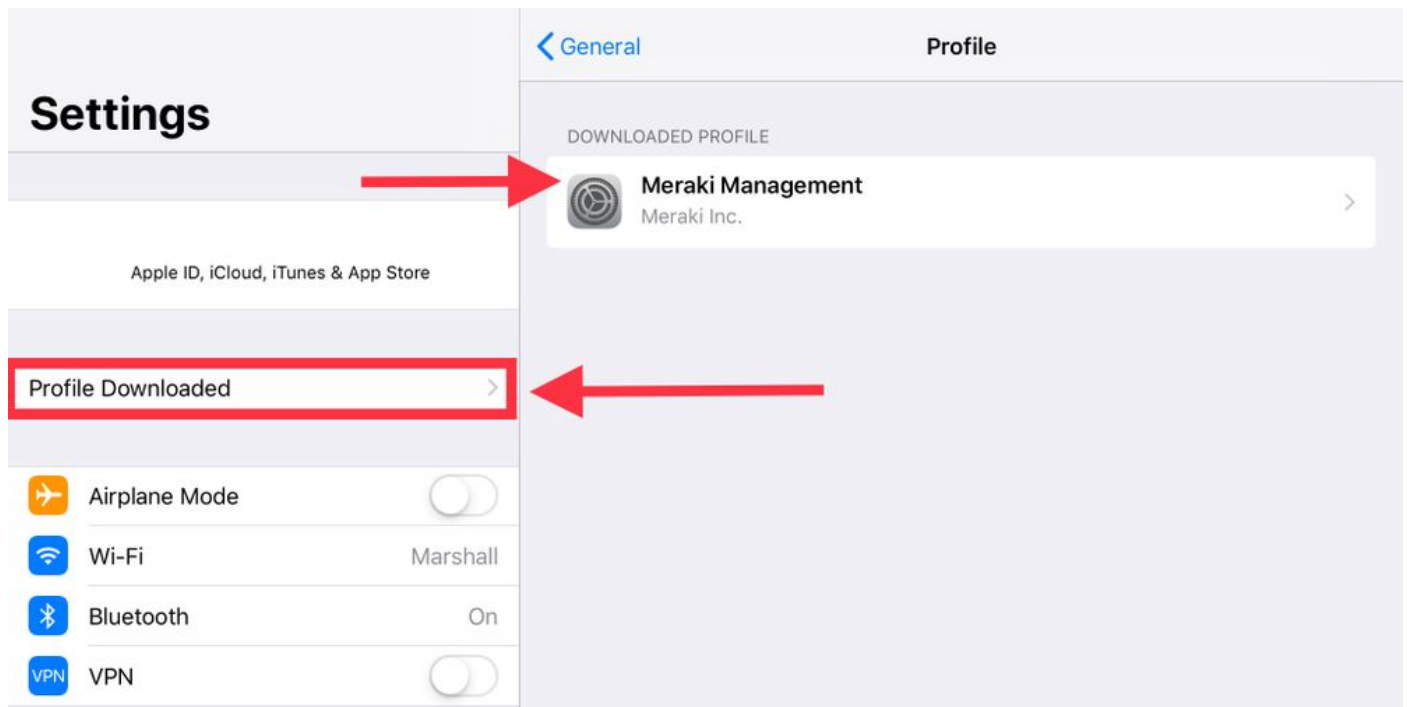
1.6. Selecteer **Toestaan** om het apparaat toe te staan om het MDM-profiel te downloaden.



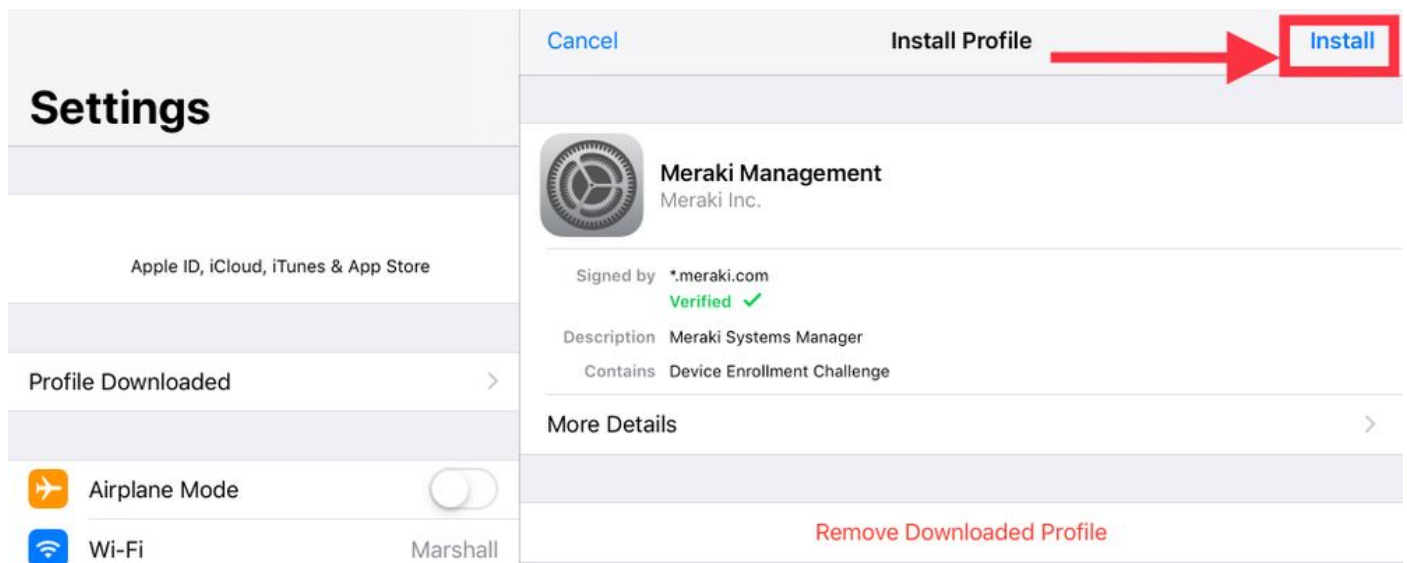
1.7. Selecteer **Sluiten** om het downloaden te voltooien.



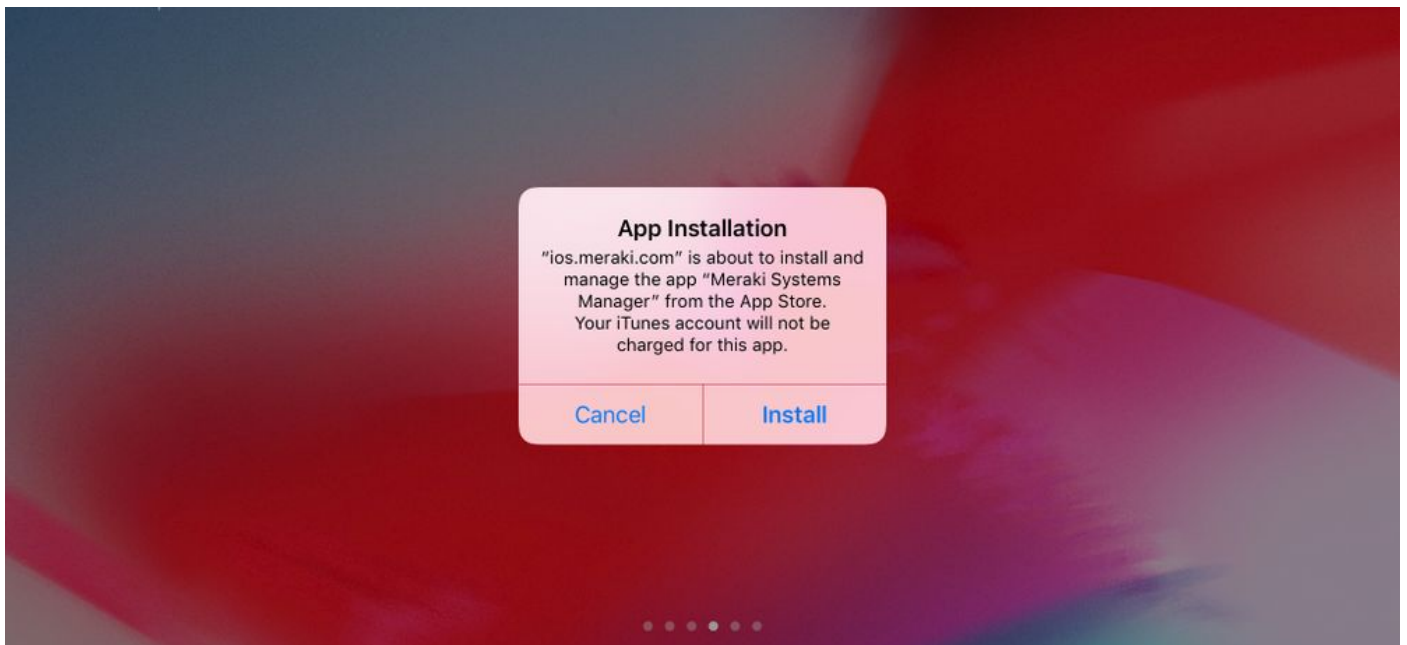
1.8. Navigeer naar de iOS-instellingenapp en zoek de optie **Profiel downloaden** in het linkerdeelvenster en selecteer de sectie **Meraki Management**.



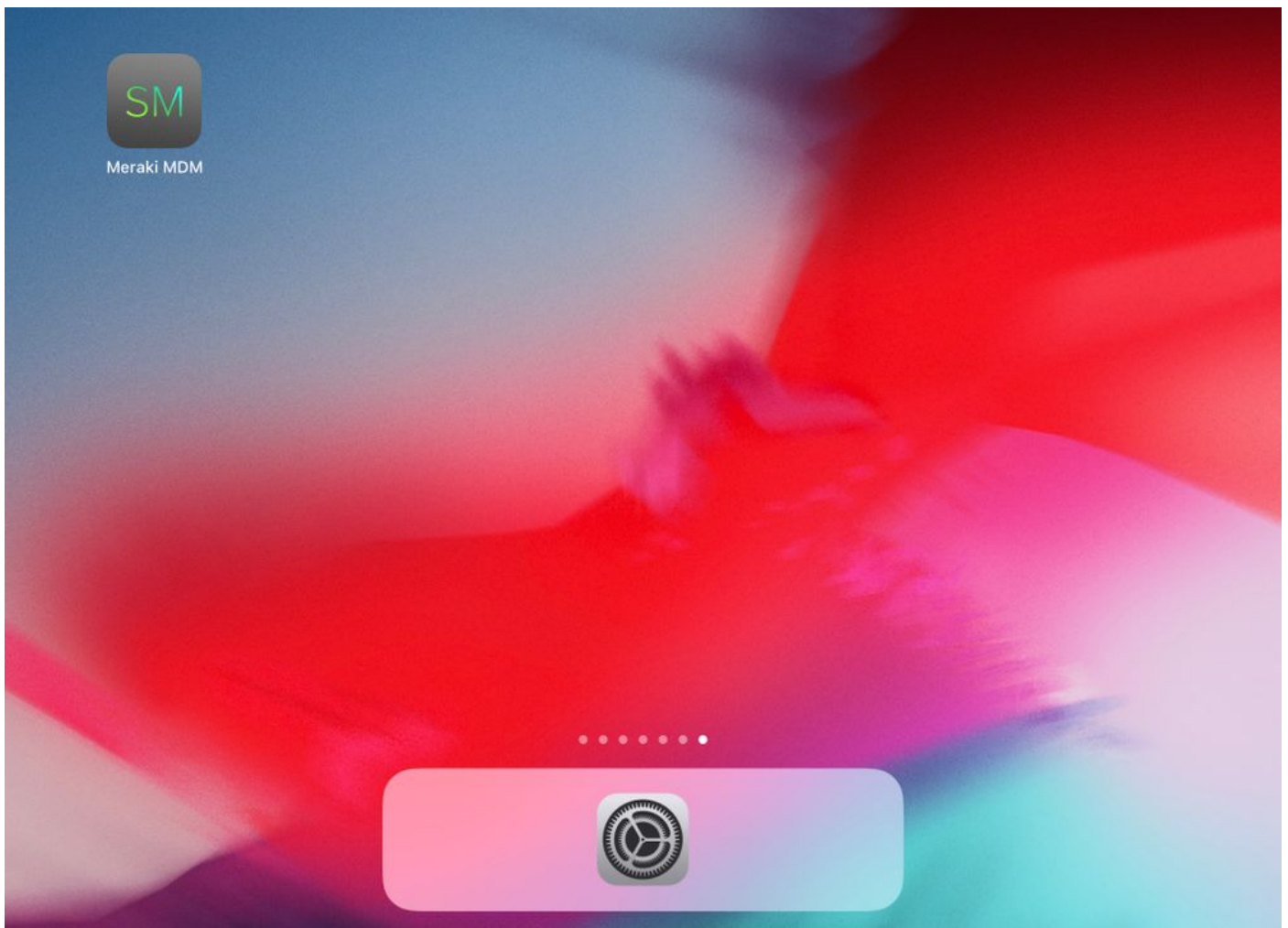
1.9. Selecteer de **installatieoptie** om het MDM-profiel te installeren.



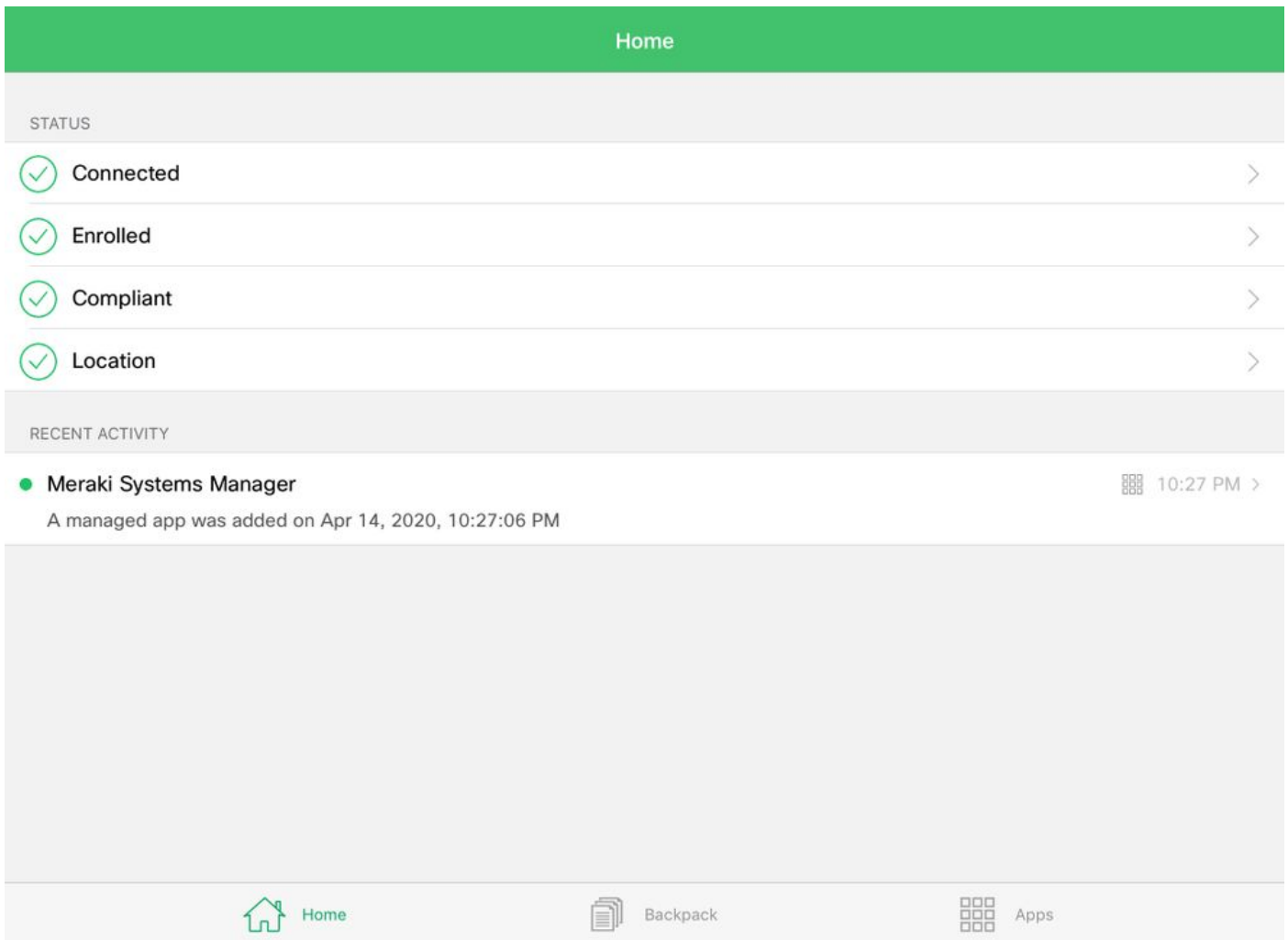
1.10. U moet toegang verlenen om de SM-toepassing te installeren.



1.11. Open de onlangs gedownloade applicatie **Meraki MDM** op het Homescherm.



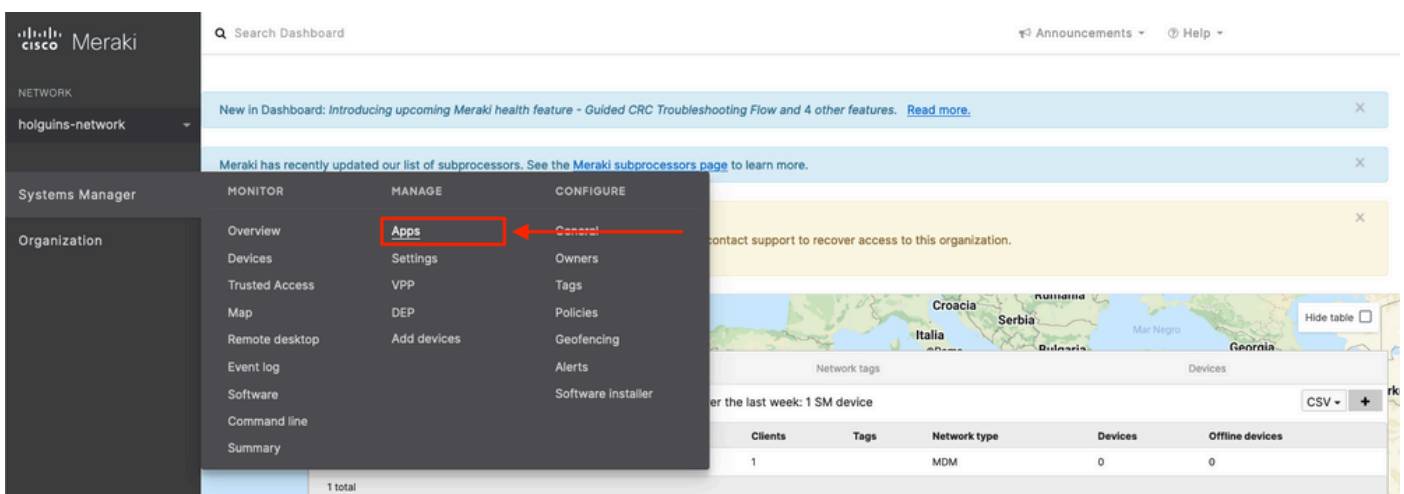
1.12. Controleer of alle statussen een groen vinkje hebben dat bevestigt dat de inschrijving volledig is.



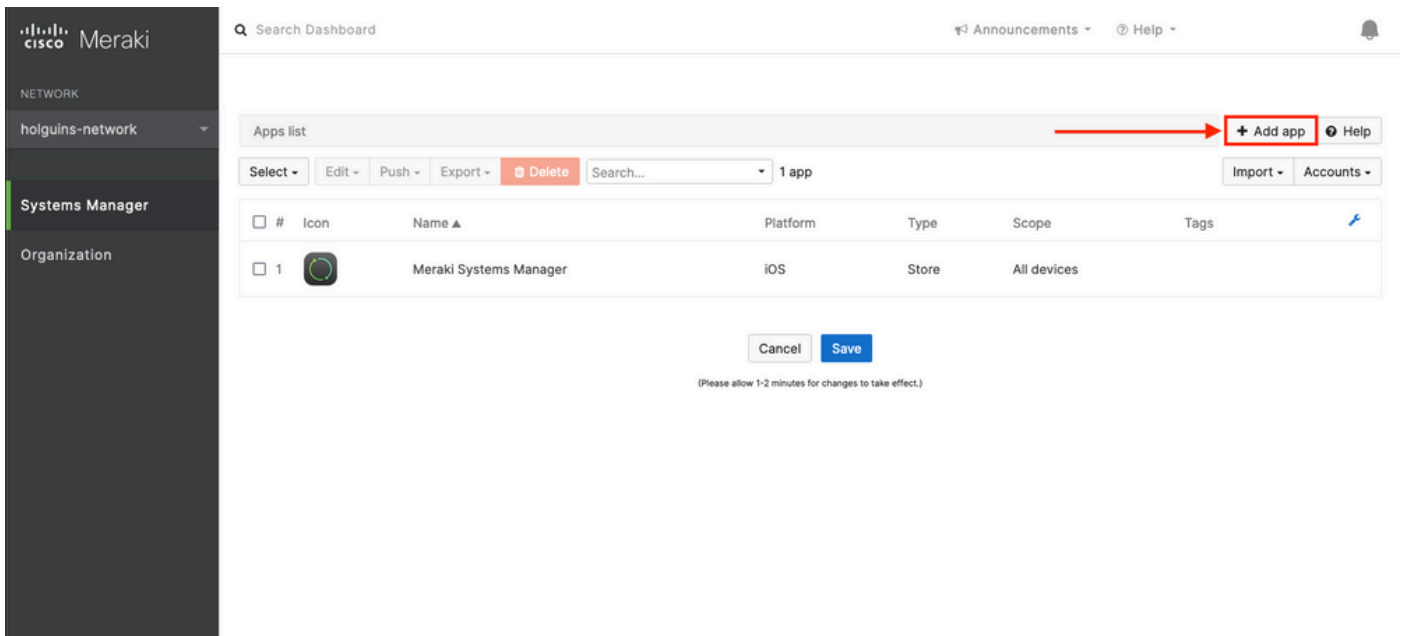
Stap 2. Beheerde apps instellen

Om de Tunneling Apps voor PerApp later in dit document te kunnen instellen, moet u diezelfde toepassingen via SM beheren. In dit configuratievoorbeeld is Firefox bedoeld om via Per App getunneld te worden, vandaar dat het wordt toegevoegd aan de beheerde Apps.

2.1. Navigeren naar **Systems Manager > Beheer > Apps** om de beheerde apps toe te voegen.

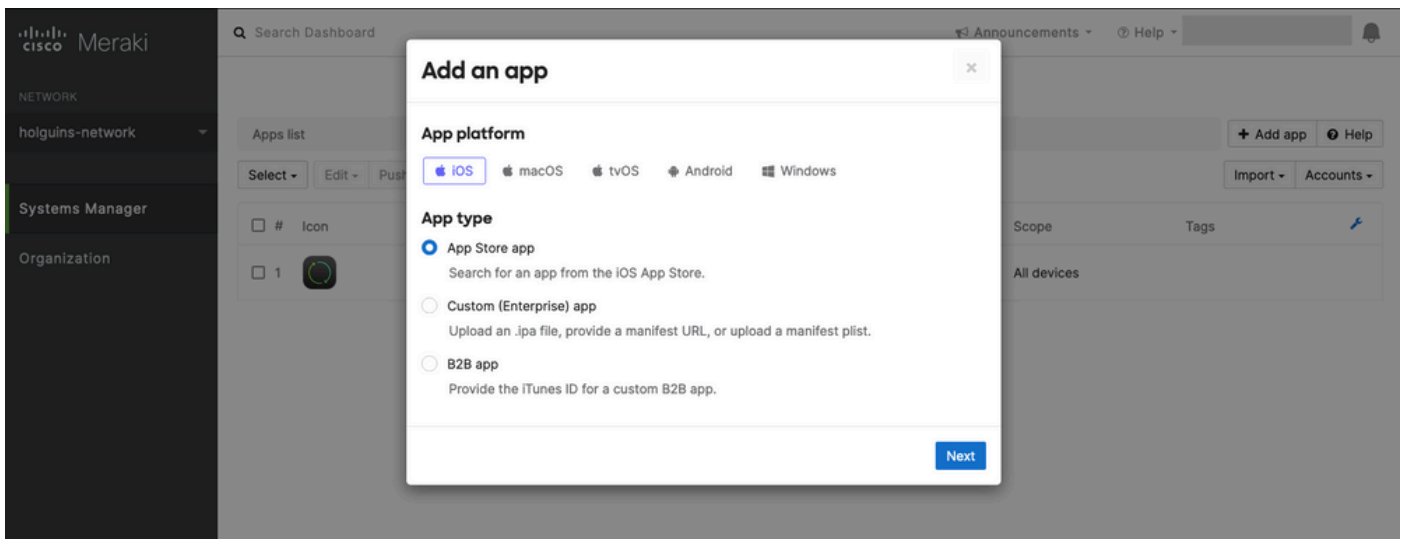


2.2. Selecteer de optie **Add app**.



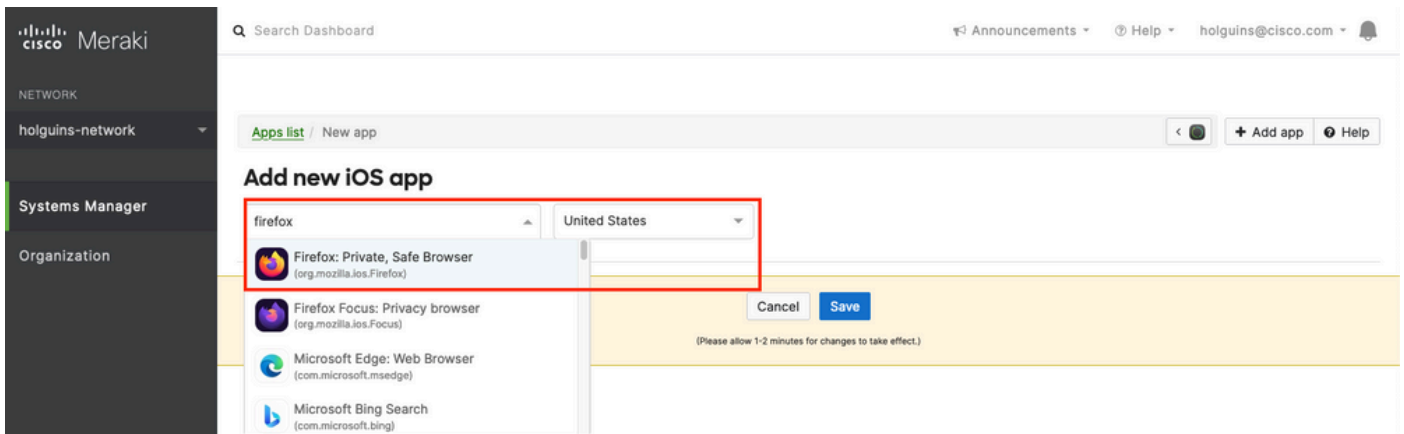
2.3. Selecteer het type toepassing (App Store-app, Custom, B2B) op basis van waar de app is opgeslagen. Selecteer **Volgende** zodra deze is geselecteerd.

In dit voorbeeld wordt de app publiekelijk opgeslagen in de App Store.



2.4. Zoek desgevraagd naar de gewenste applicatie en selecteer de regio waar de applicatie is gedownload. Selecteer **Opslaan** als de app is geselecteerd.

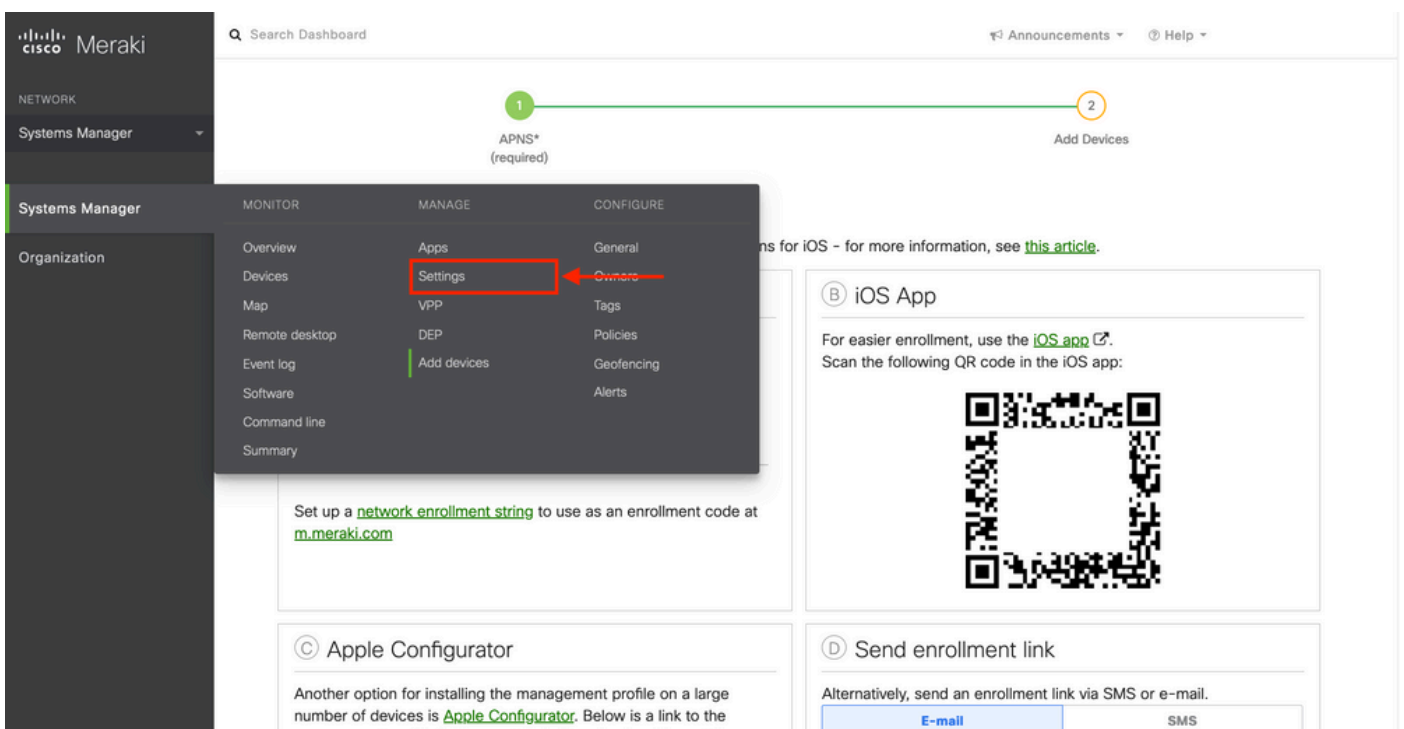
Opmerking: als het land niet overeenkomt met de regio van de Apple-account, kan de gebruiker problemen met de toepassing ondervinden.



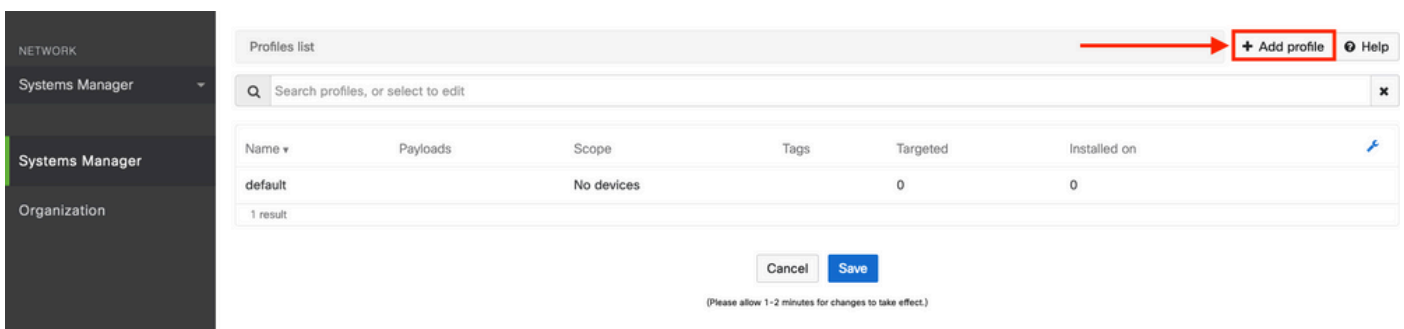
2.5. Klik op Opslaan als u alle gewenste toepassingen hebt geselecteerd.

Stap 3. PerApp VPN-profiel configureren

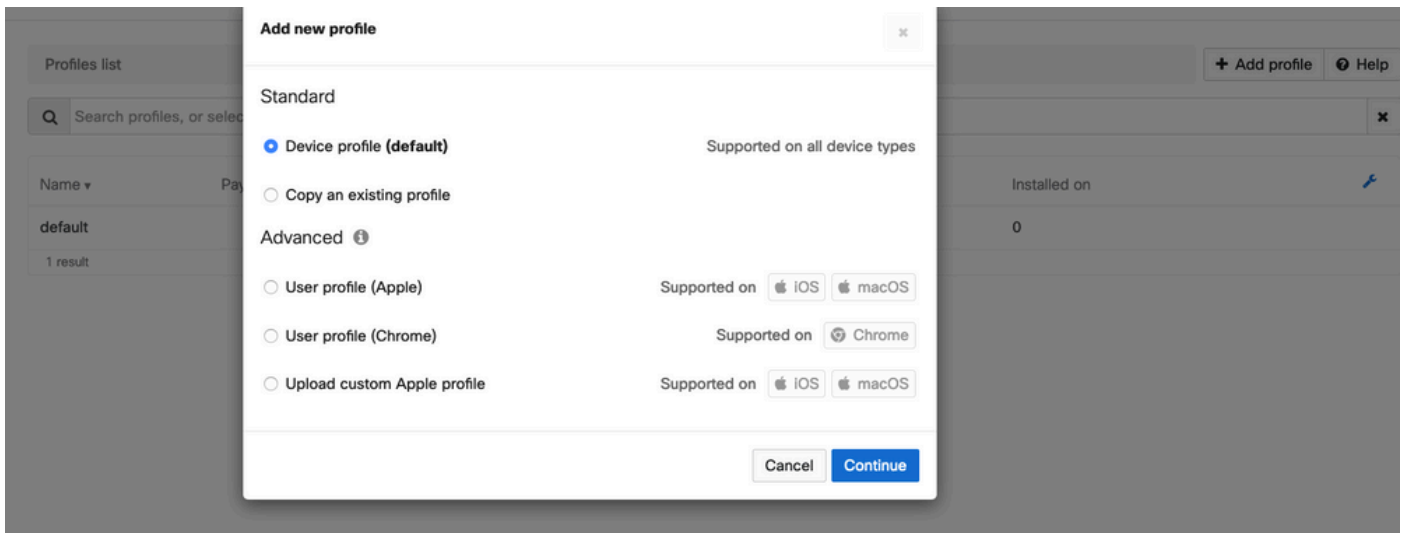
3.1. Navigeren naar Systems Manager > Beheer > Instellingen



3.2. Selecteer de optie Profiel toevoegen.



3.3. Selecteer Apparaatprofiel (standaard) en klik op Doorgaan.



3.4. Zodra het menu **Profielconfiguratie** wordt weergegeven, schrijft u de naam en selecteert u de doelapparaten onder **Bereik**.

⚙️ Profile configuration

Profile Configuration

Type Device profile

Name The name that will be shown to users

Description Optional

Profile Removal Policy

Removal Policy

Targets

Group type Manual Named Configure tags

Scope Convert to target group

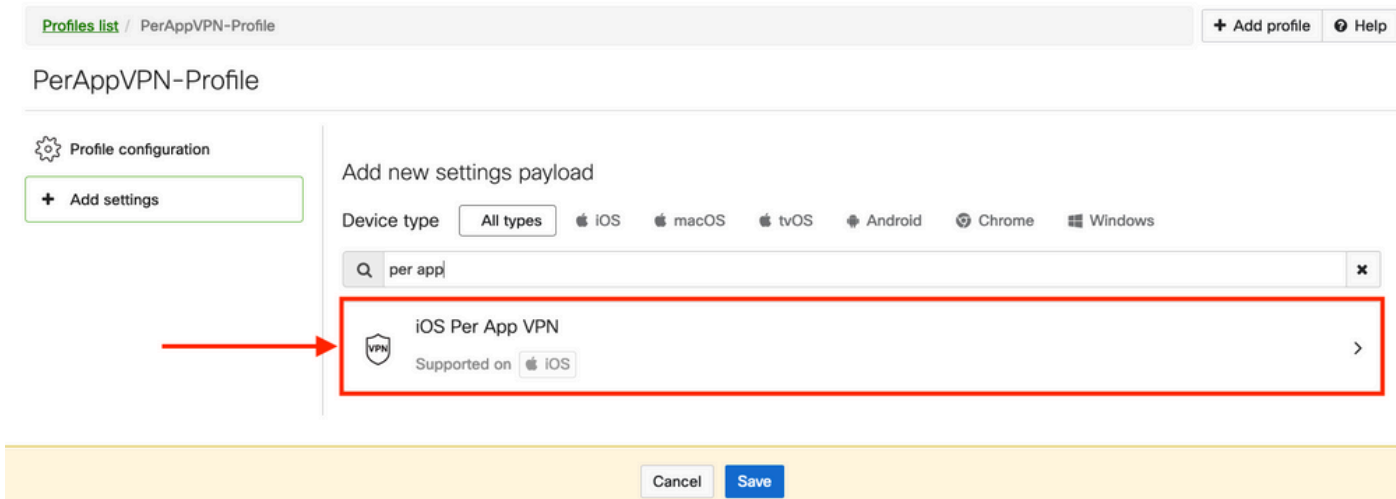
Installation target All devices

Status

Device in scope: 1 device

#	Name	System type	Install status	Tags
1	iPad	iPad (6th Gen.)	Not installed	

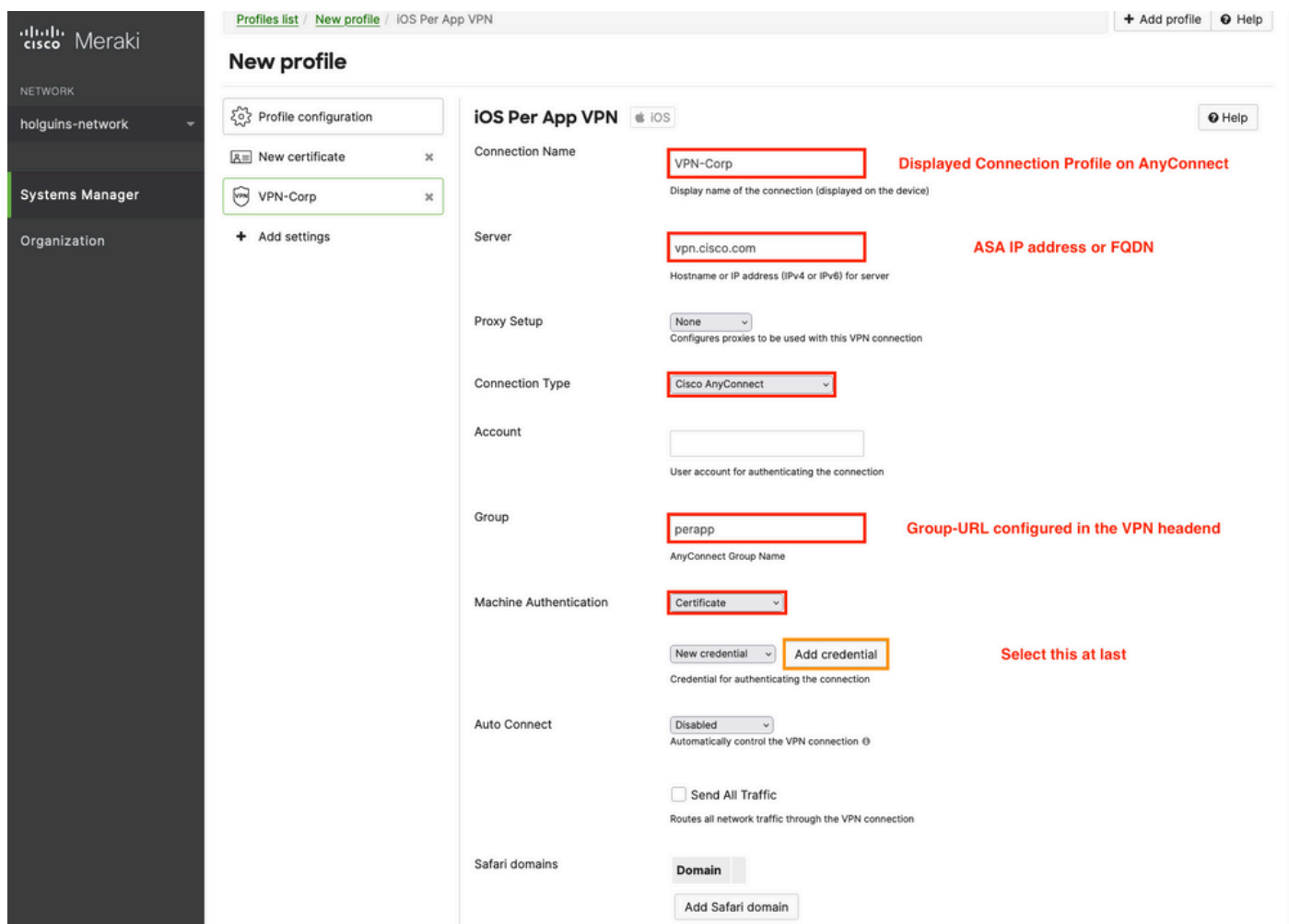
3.5. Selecteer **Instellingen toevoegen** en filter de soorten profiel door **iOS Per App VPN**, selecteer de optie zoals hieronder te zien.



3.6. Nadat het menu is weergegeven, schrijft u de verbindinginformatie naar aanleiding van het onderstaande voorbeeld.

Systems Manager ondersteunt twee certificaatschrijvingen voor deze verbindingen, SCEP en handmatige inschrijving. In dit voorbeeld werd handmatige inschrijving gebruikt.

Opmerking: Selecteer **Credentials toevoegen** nadat u de tekstvakken hebt ingevuld, omdat deze optie u naar een nieuw menu brengt om een certificaatbestand toe te voegen.



3.7. Zodra u op **Add credential** hebt geklikt en u bent doorgestuurd naar het certificaatmenu, schrijf de **naam** van het certificaat, blader door uw computer en zoek naar het **wachtwoord** dat het

bestand .pfx (versleuteld certificaatbestand) beschermt.

The screenshot shows the Meraki Systems Manager interface. On the left is a navigation sidebar with 'Systems Manager' selected. The main content area is titled 'New profile' and has a 'Certificate' tab selected. Under 'Profile configuration', there are two items: 'machine-auth' and 'VPN-Corp'. The 'Certificate' section contains the following fields:

- Name:** machine-auth
- Password:** A masked password field with a key icon.
- Certificate:** A red box highlights the text 'Examinar...' and the message 'No se ha seleccionado ningún archivo.' below it.

At the bottom, there are 'Cancel' and 'Save' buttons, and a note: '(Please allow 1-2 minutes for changes to take effect.)'

3.8. Nadat het certificaat is geselecteerd, wordt de bestandsnaam van het certificaat weergegeven.

This screenshot shows the same Meraki Systems Manager interface as above, but the 'Certificate' field now displays the following information:

- Filename:** pfxbin.pfx
- Issuer:**
- Subject/CN:**
- Expiration:** Select new certificate

The 'Save' button is highlighted in blue, indicating it is the active action.

3.9. Zodra u het certificaat hebt geselecteerd, navigeer dan naar het VPN-profiel waar u eerder op stond en selecteer de onlangs geïmporteerde referenties en selecteer de app voor tunnels (in dit geval Firefox).

Klik op **Opslaan** als dit is voltooid.

The screenshot shows the Meraki Systems Manager interface for configuring an iOS Per App VPN profile. The profile name is 'machine-auth'. The configuration includes a connection name 'VPN-Corp', server 'vpn.cisco.com', and connection type 'Cisco AnyConnect'. The machine authentication is set to 'Certificate' with the 'machine-auth' credential selected. The 'Firefox: Private, Safe Browser' app is selected in the 'Apps' list.

3.10. Controleer of het profiel op de doelapparaten is geïnstalleerd.

Profiles list + Add profile Help

Q Search profiles, or select to edit x

Name ▾	Payloads	Scope	Tags	Targeted	Installed on	
PerAppVPN-Profile		All devices		1	1	
default		No devices		0	0	

2 results

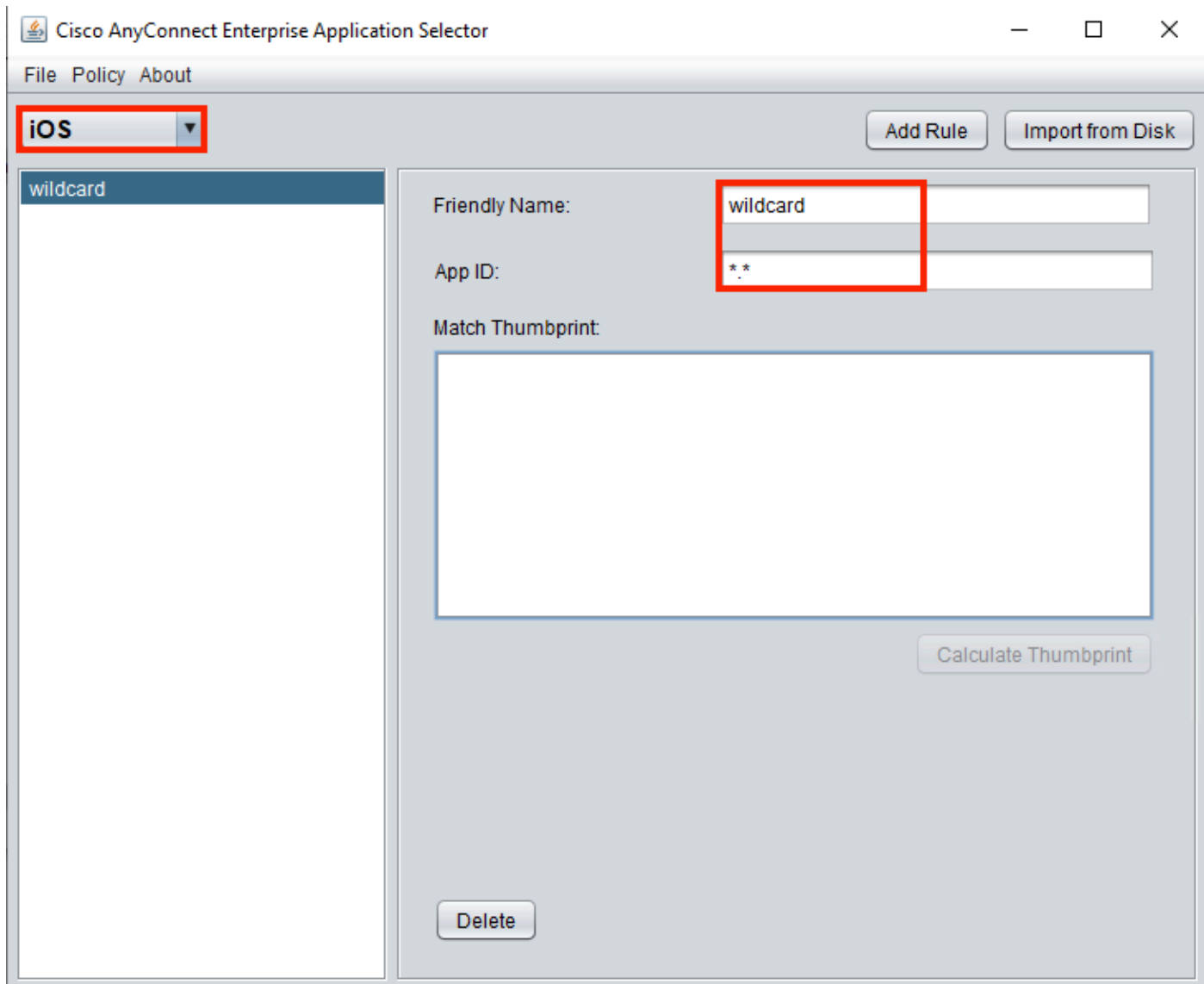
Stap 4. Configuratie van App Selector

4.1. App-kiezer downloaden vanaf Cisco-website

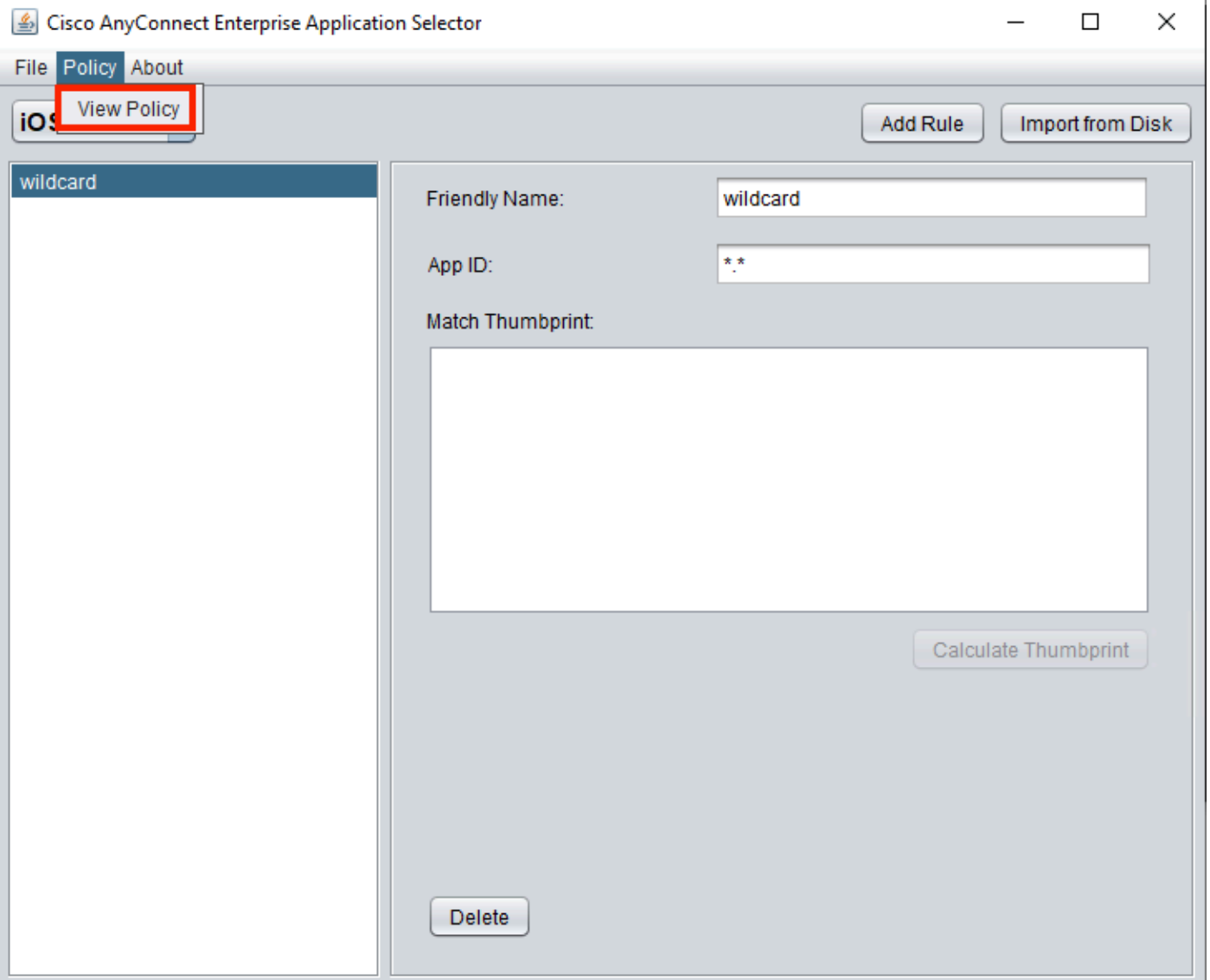
<https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0>

Waarschuwing: voer de toepassing uit op een Windows-machine. De weergegeven resultaten zijn niet de verwachte wanneer de tool wordt gebruikt op MacOS-apparaten.

4.2. Open de Java-toepassing. Selecteer **iOS** in het vervolkeuzemenu, voeg een vriendelijke naam toe en zorg ervoor dat u ***.*** in de **App-ID** typt.



4.3. Navigeer naar **Beleid** en selecteer **Beleid bekijken**



4.4. Kopieer de weergegeven string. (Dit wordt later gebruikt in de VPN head-end configuratie).

```
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSgIYk  
FBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB
```

OK

Stap 5. ASA Sample per app VPN-configuratie

```
conf t
webvpn
anyconnect-custom-attr perapp description PerAppVPN
anyconnect-custom-data perapp wildcard
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSgIYkFBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB

ip local pool vpnpool 10.204.201.20-10.204.201.30 mask 255.255.255.0

access-list split standard permit 172.168.0.0 255.255.0.0
access-list split standard permit 172.16.0.0 255.255.0.0

group-policy GP-perapp internal
group-policy GP-perapp attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
split-tunnel-all-dns disable
anyconnect-custom perapp value wildcard

tunnel-group perapp type remote-access
tunnel-group perapp general-attributes
address-pool vpnpool
default-group-policy GP-perapp
tunnel-group perapp webvpn-attributes
authentication certificate
group-alias perapp enable
```

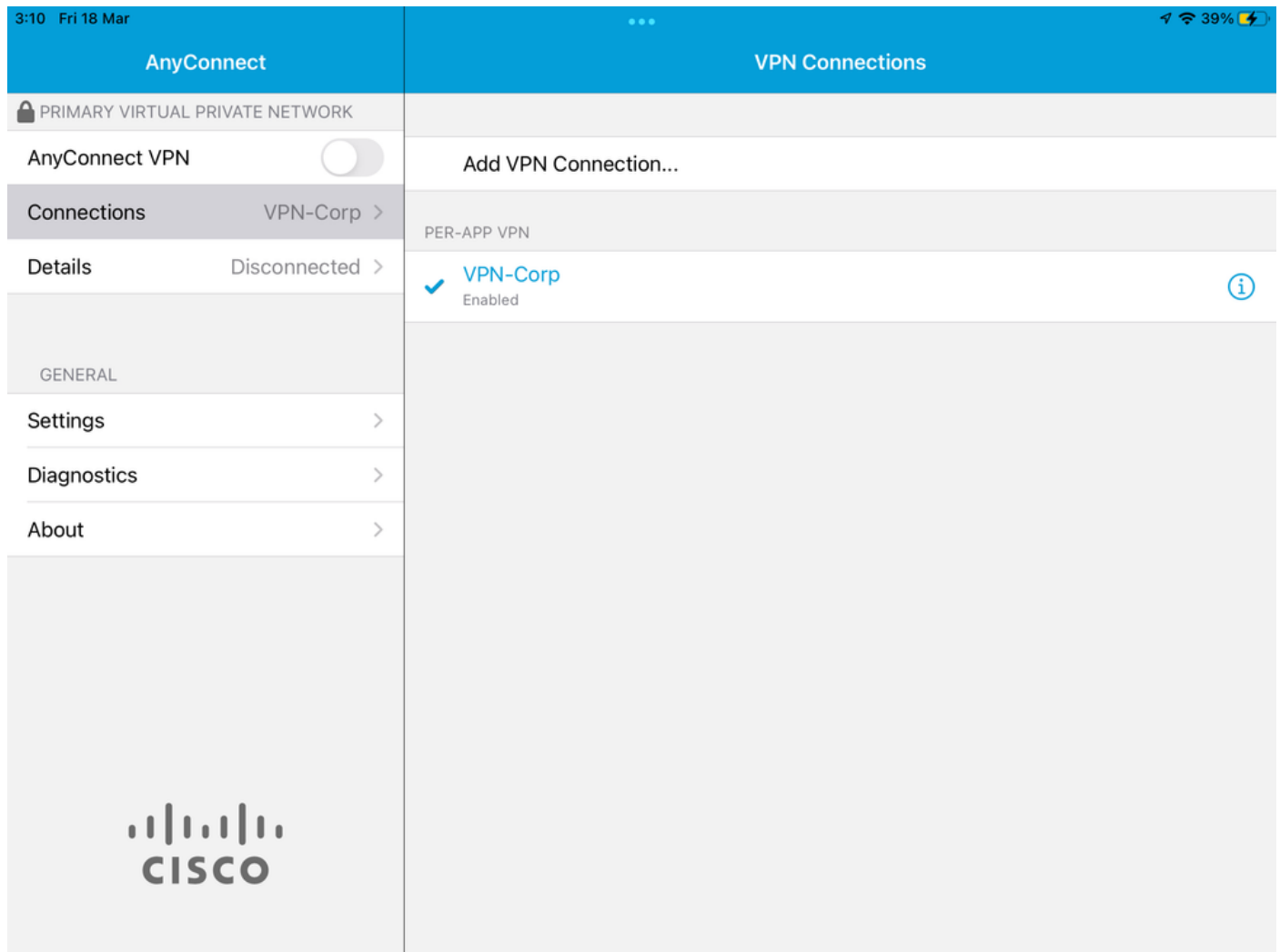

group-url https://vpn.cisco.com/perapp enable

Verifiëren

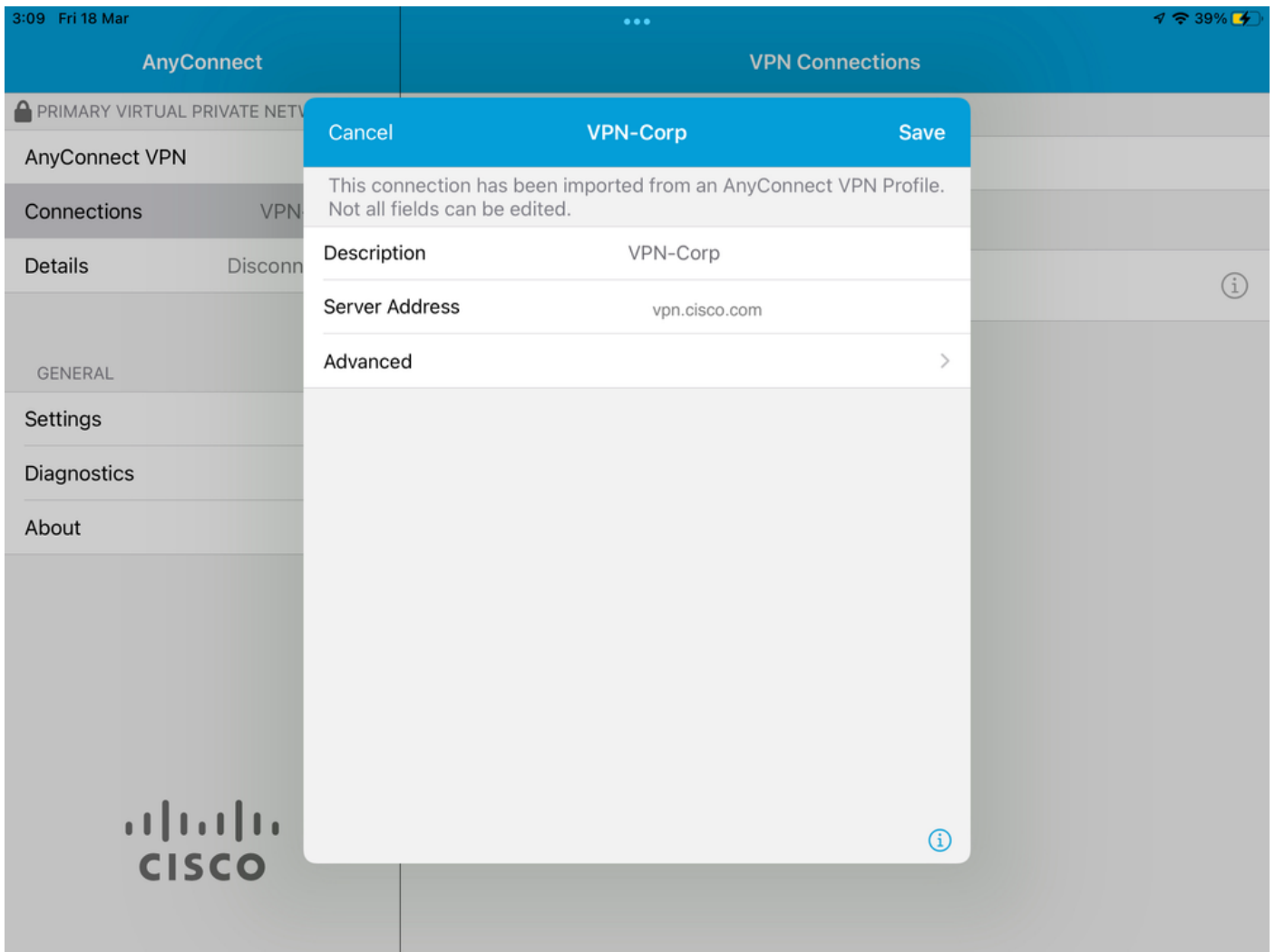
6. Controleer de profielinstallatie op de AnyConnect-toepassing

6.1. Open de AnyConnect-toepassing en selecteer **Verbindingen** in het linkerdeelvenster. Het PerApp VPN-profiel moet worden weergegeven onder een nieuwe sectie met de naam **PER-APP VPN**.

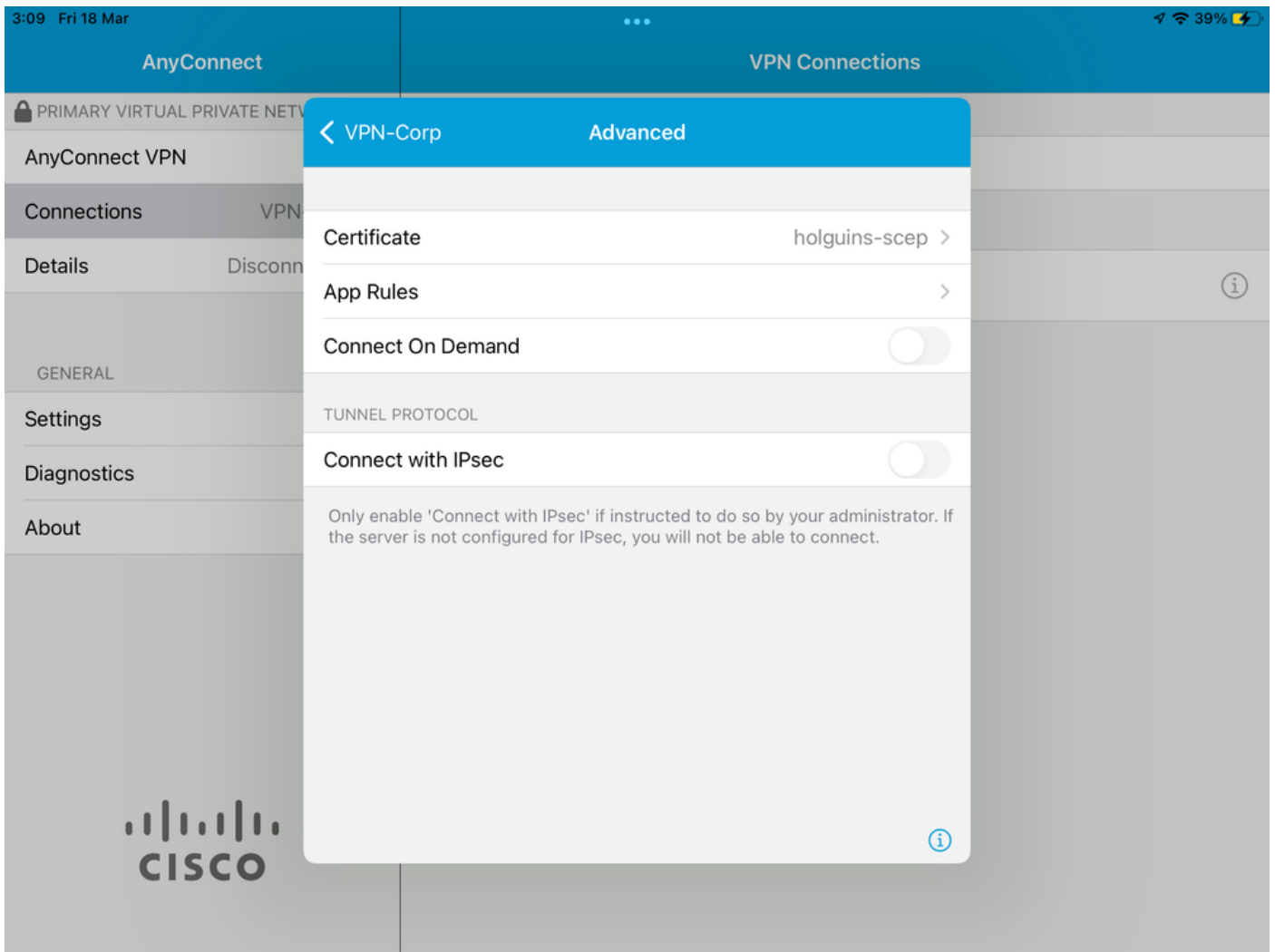
Selecteer de optie **I** om de geavanceerde instellingen weer te geven.



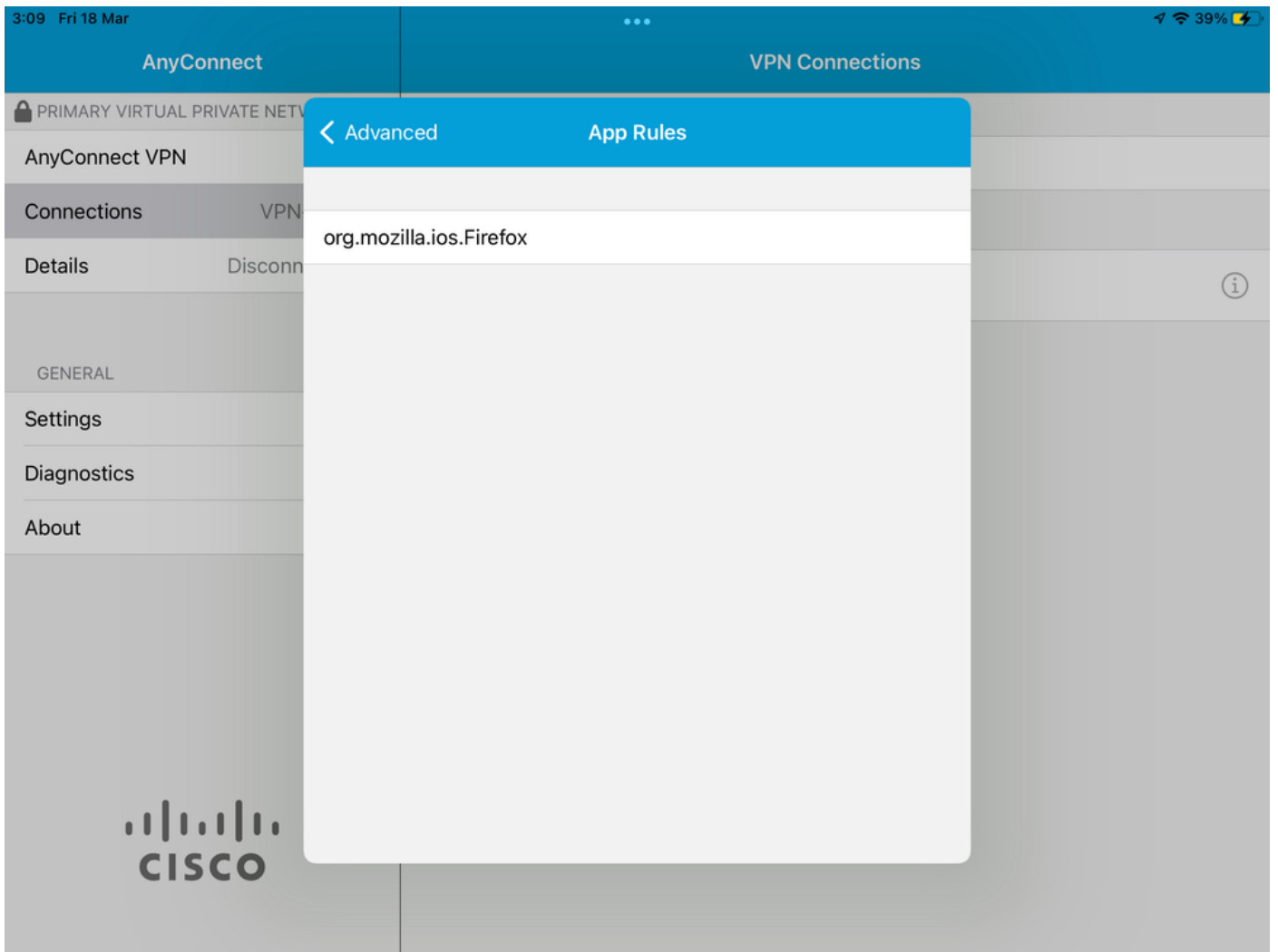
6.2. Selecteer de optie **Advanced**.



6.3. Selecteer de optie **App Rules**.



6.4. Bevestig ten slotte dat de App-regel is geïnstalleerd. (Mozilla is de app met tunnels die in dit document wordt gewenst, dus de app installatie was succesvol).



Problemen oplossen

Er zijn momenteel geen specifieke stappen voor probleemoplossing voor dit document.

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.