

# Konfigurieren von AnyConnect PerApp VPN für iOS mit Meraki System Manager

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Registrieren des iOS-Geräts bei Meraki Systems Manager](#)

[Schritt 2: Verwaltete Anwendungen einrichten](#)

[Schritt 3: Konfigurieren des ProApp-VPN-Profiles](#)

[Schritt 4: Konfiguration der Anwendungsauswahl](#)

[Schritt 5: ASA - Beispiel-VPN-Konfiguration pro Anwendung](#)

[Überprüfung](#)

[6. Überprüfen der Profilinstallation auf der AnyConnect-Anwendung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird die Konfiguration von PerApp VPN auf Apple iOS-Geräten beschrieben, die vom Meraki Mobile Device Manager (MDM) oder System Manager (SM) verwaltet werden.

## Voraussetzungen

### Anforderungen

- AnyConnect v4.0 Plus- oder Apex-Lizenz
- ASA 9.3.1 oder höher zur Unterstützung von anwendungsbasiertem VPN
- Das Cisco Enterprise Application Selector-Tool finden Sie unter Cisco.com

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Hintergrundinformationen

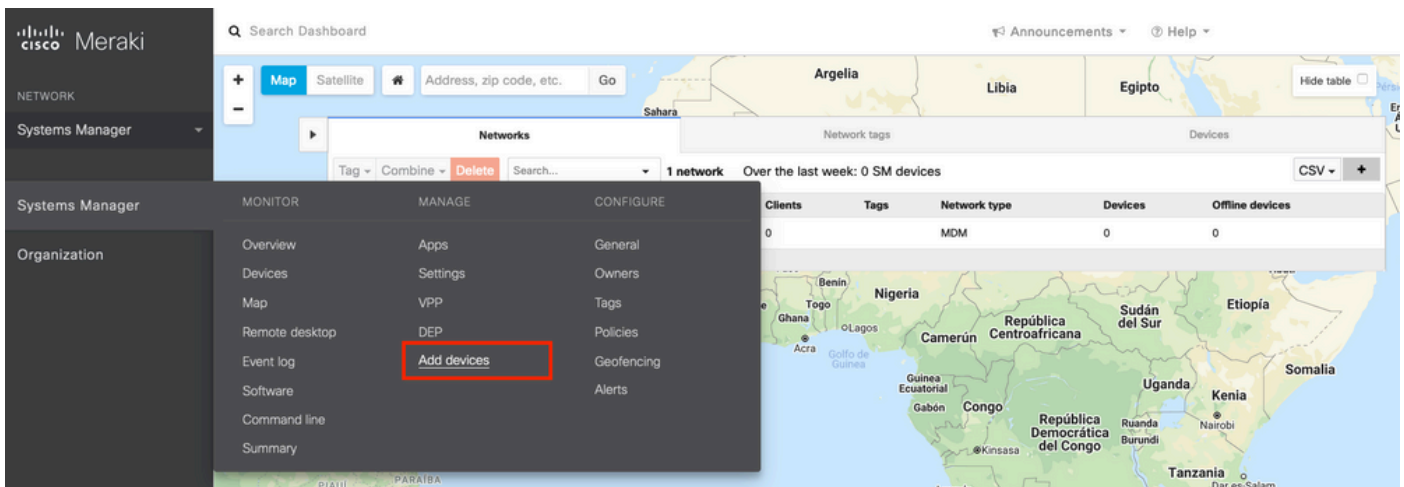
Die folgenden Prozesse sind in diesem Dokument nicht aufgeführt:

- SCEP-Zertifizierungsstellenkonfiguration auf Systems Manager für Clientzertifikatgenerierung
- PKCS12-Client-Zertifikatgenerierung für die iOS-Clients

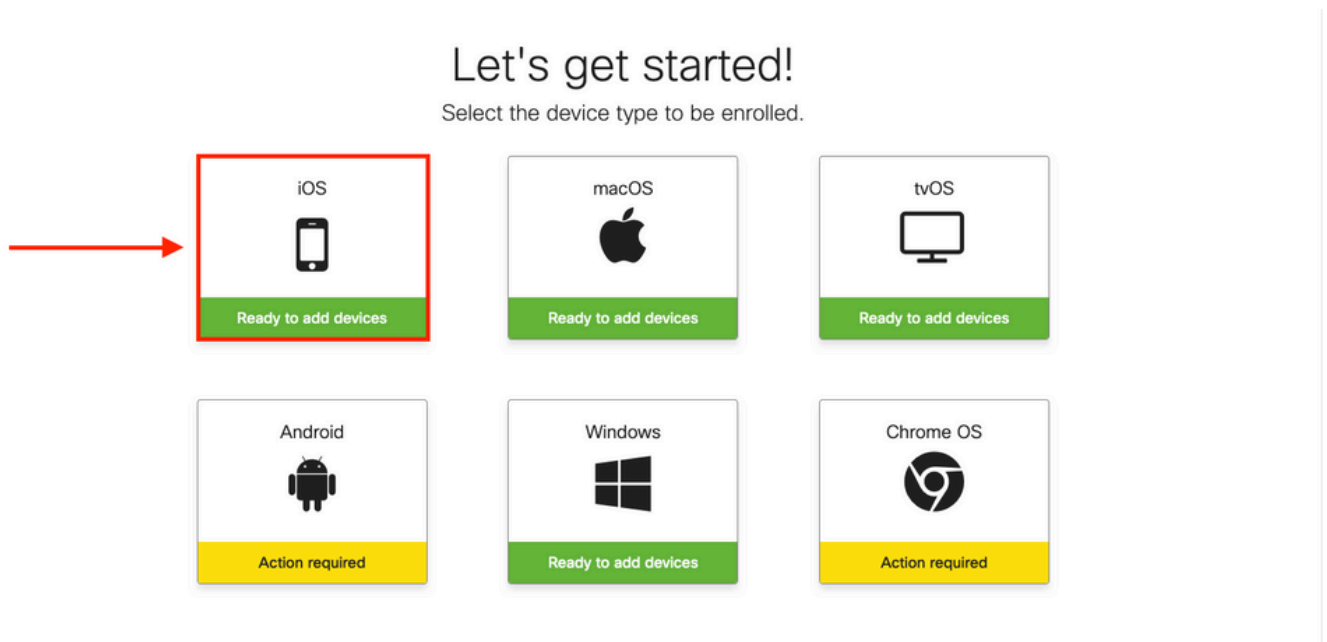
## Konfigurieren

### Schritt 1: Registrieren des iOS-Geräts bei Meraki Systems Manager

1.1. Navigieren Sie zu **Systems Manager > Geräte hinzufügen**.



1.2. Klicken Sie auf die **iOS**-Option, um die Registrierung zu starten.



1.3. Registrieren Sie das Gerät per Internet-Browser oder scannen Sie den QR-Code mit der Kamera. In diesem Dokument wurde die Kamera für den Registrierungsprozess verwendet.

1  
APNS\*  
(required)

2  
Add Devices

## 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](https://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](https://m.meraki.com)

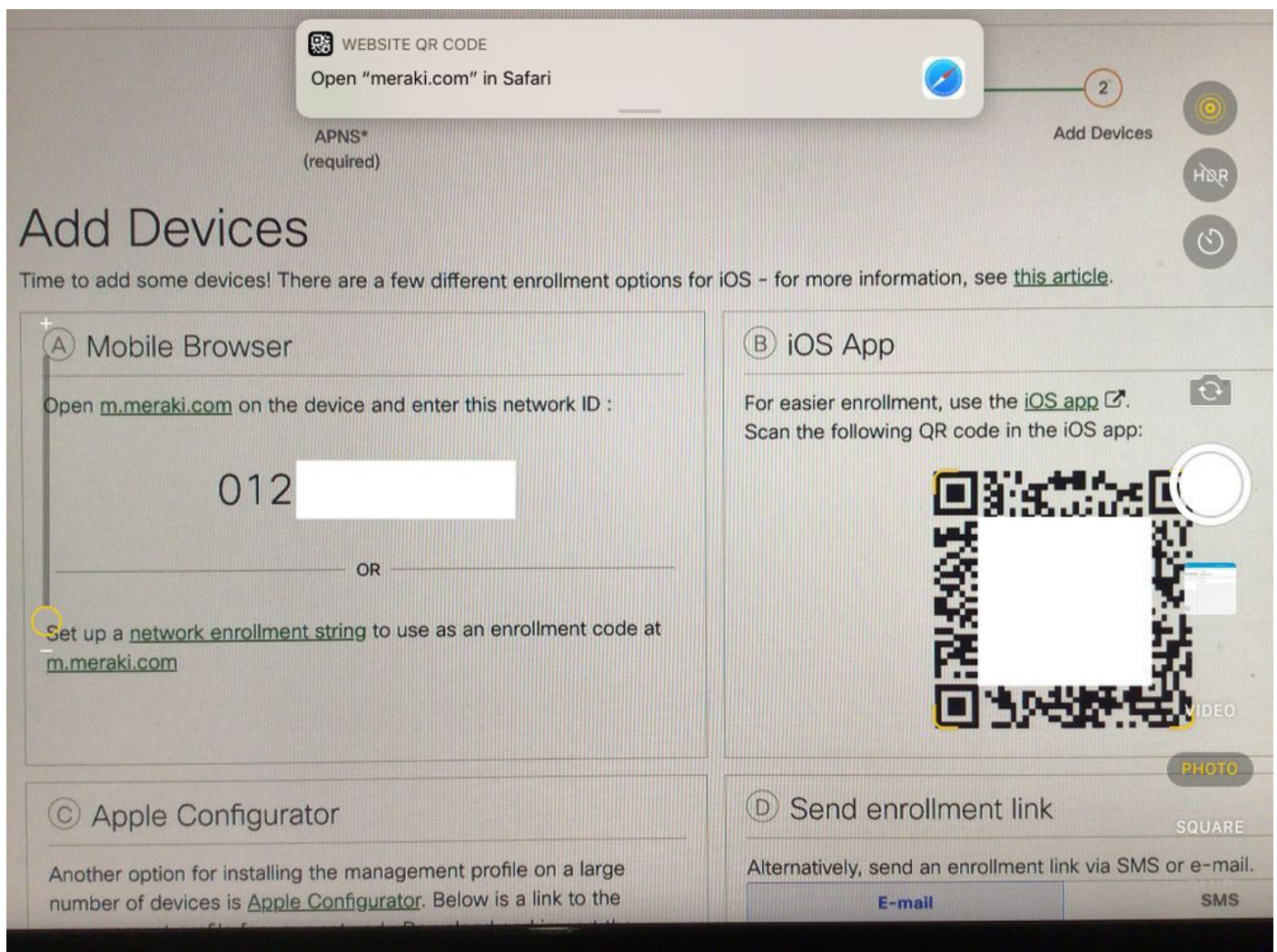
**B** iOS App

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

Scan the following QR code in the iOS app:



1.4. Wenn der QR-Code von der Kamera erkannt wird, wählen Sie die Meldung "meraki.com" in Safari öffnen, die erscheint.



WEBSITE QR CODE  
Open "meraki.com" in Safari

APNS\*  
(required)

Add Devices

## 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](https://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](https://m.meraki.com)

**B** iOS App

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

Scan the following QR code in the iOS app:

**C** Apple Configurator

Another option for installing the management profile on a large number of devices is [Apple Configurator](#). Below is a link to the [Apple Configurator](#) page.

**D** Send enrollment link

Alternatively, send an enrollment link via SMS or e-mail.

E-mail      SMS

1.5. Wählen Sie **Registrieren**, wenn Sie dazu aufgefordert werden.

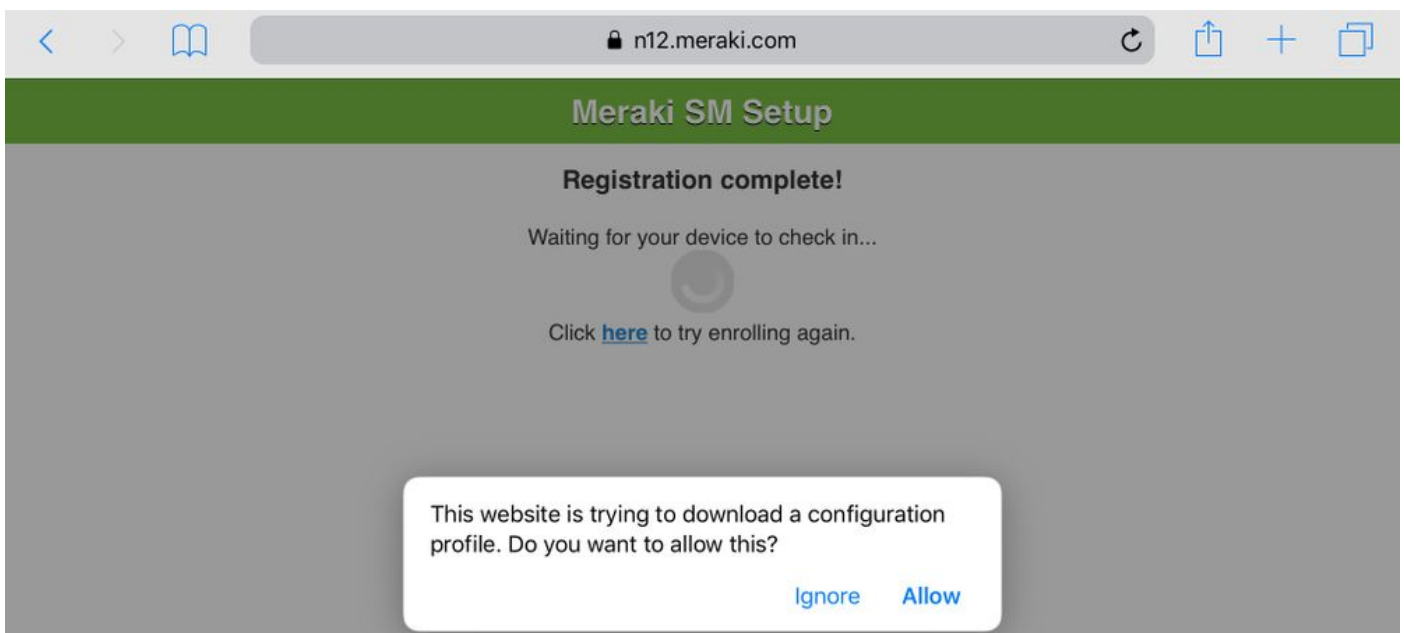


### Step 1: Enter your Network ID

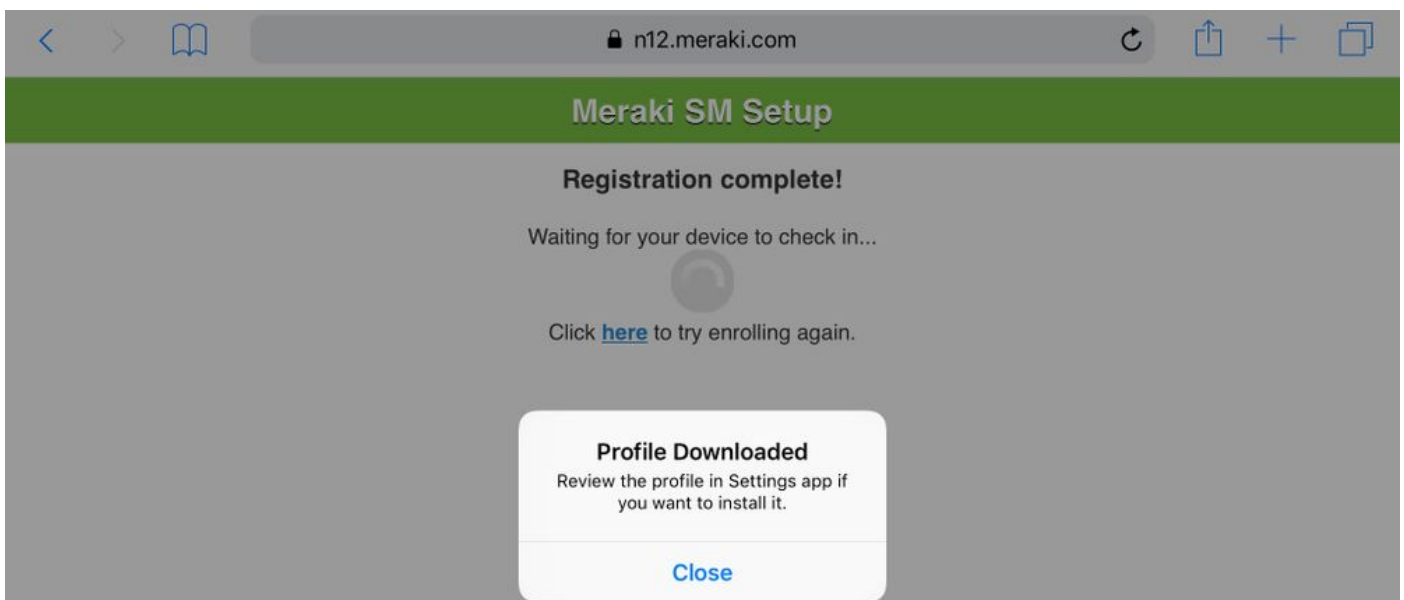
The Network ID is either a 10-digit code or a combination of letters, numbers, or characters (e.g. [123-456-7890](#) or network-id).

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

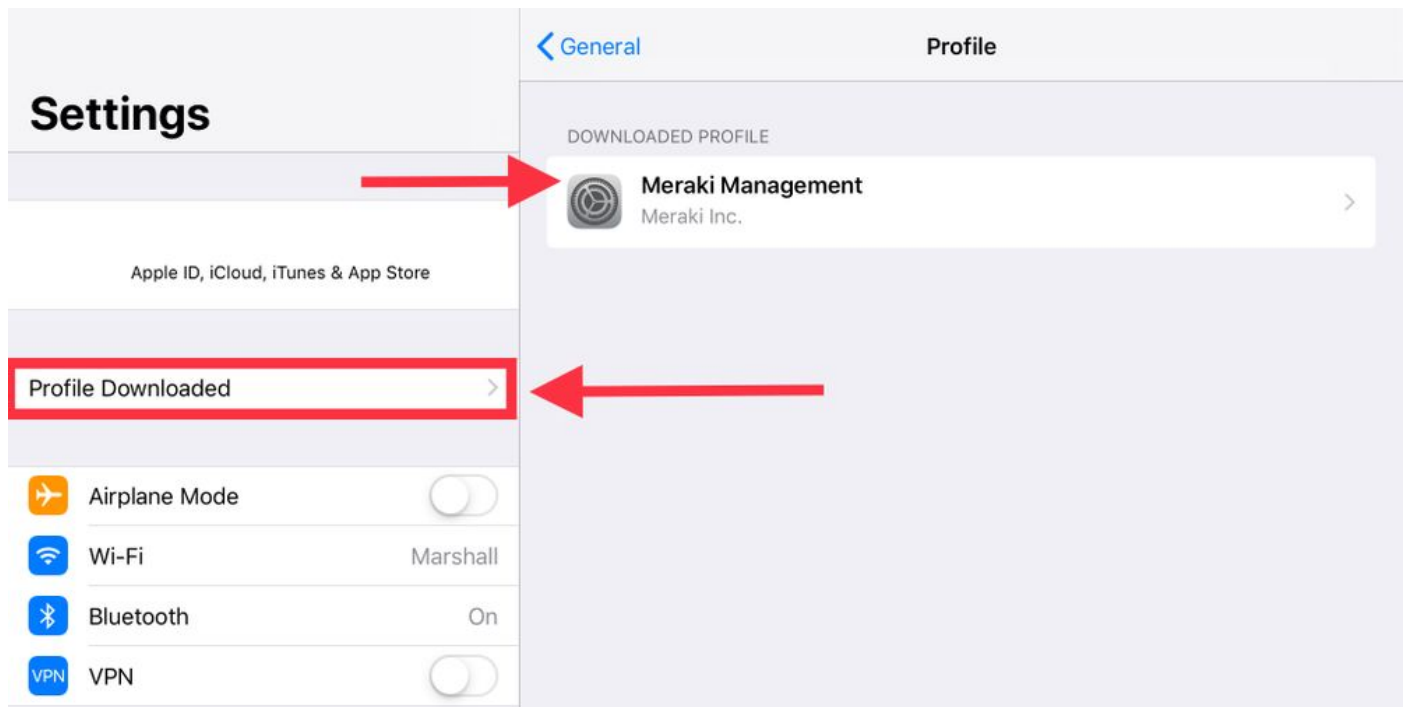
1.6. Wählen Sie **Zulassen**, damit das Gerät das MDM-Profil herunterladen kann.



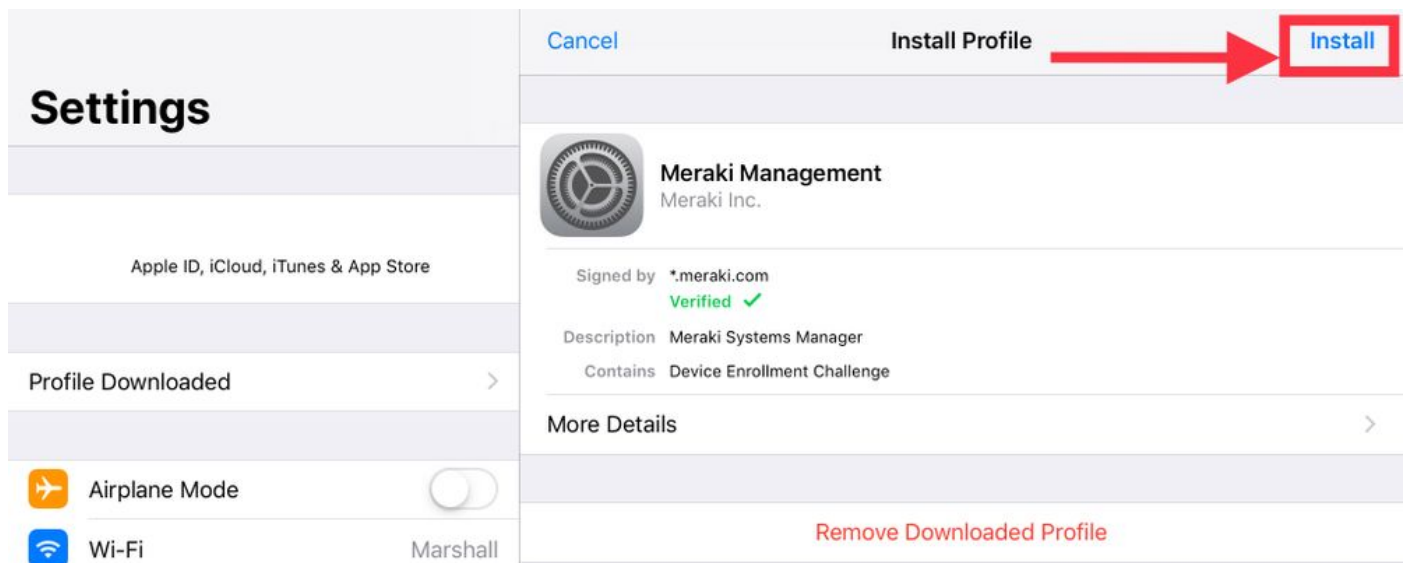
1.7. Wählen Sie **Schließen**, um den Download abzuschließen.



1.8. Navigieren Sie zur App "iOS Settings" (iOS-Einstellungen), suchen Sie im linken Bereich nach der Option "Profile Downloaded" (Profil heruntergeladen), und wählen Sie den Abschnitt "Meraki Management" aus.

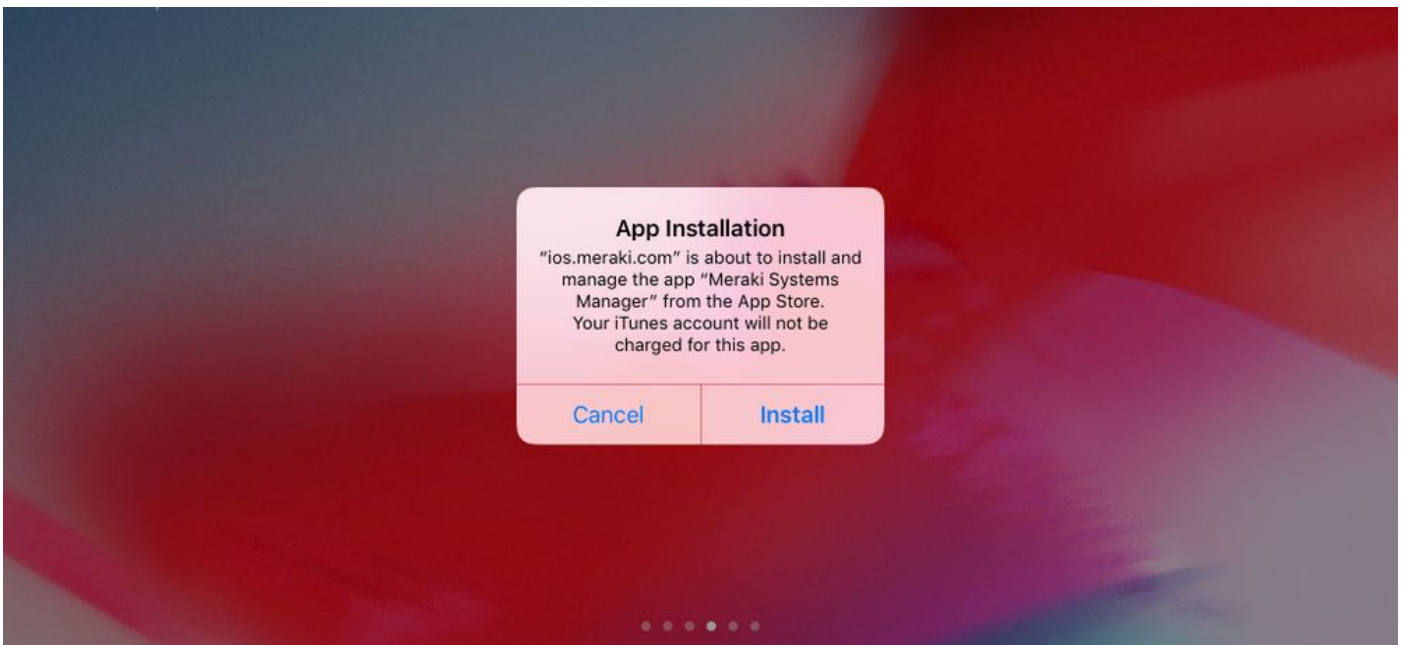


1.9. Wählen Sie die Option **Install (Installieren)**, um das MDM-Profil zu installieren.

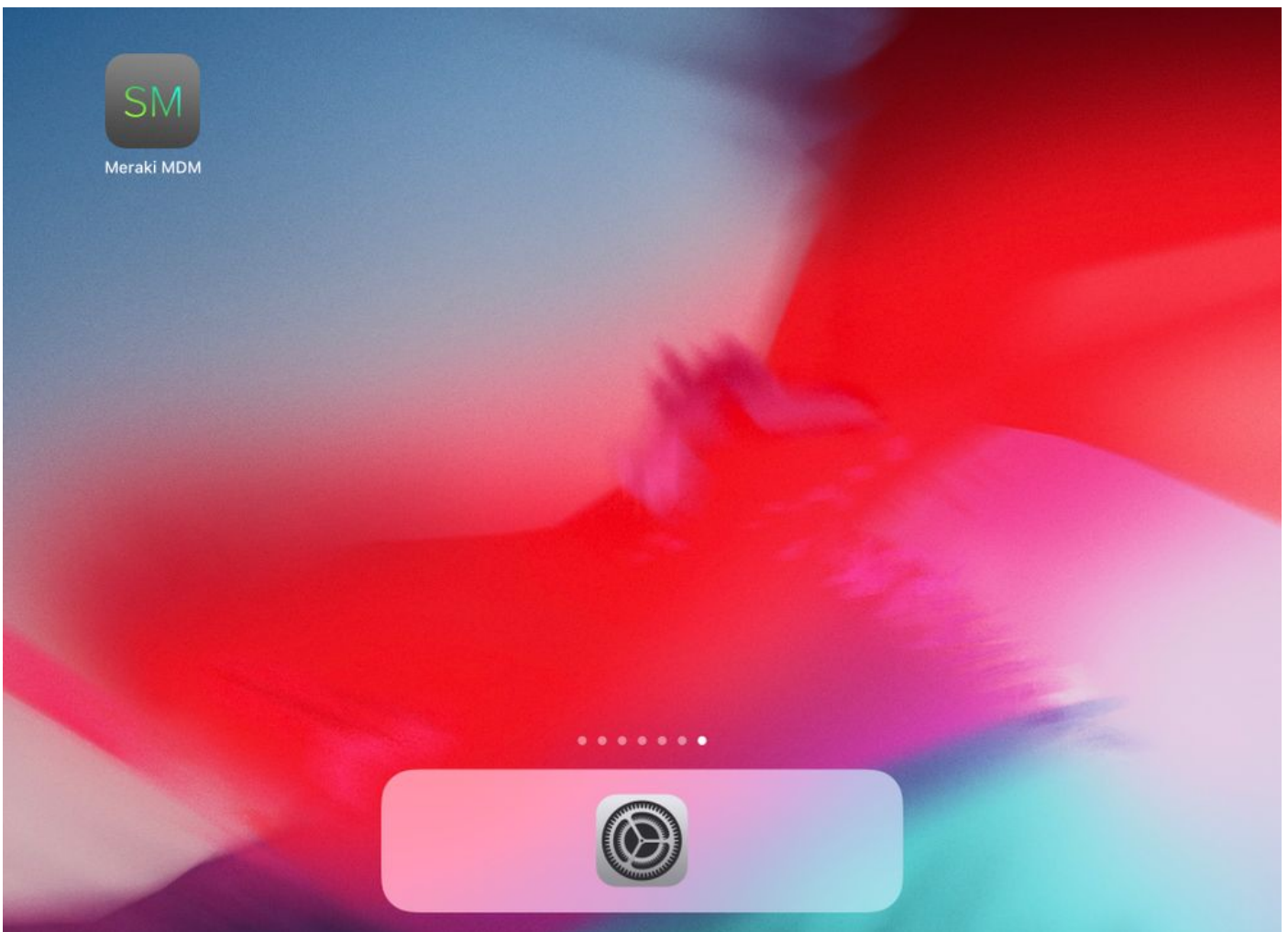


1.10. Sie müssen den Zugriff auf die SM-Anwendung **installieren** erteilen.

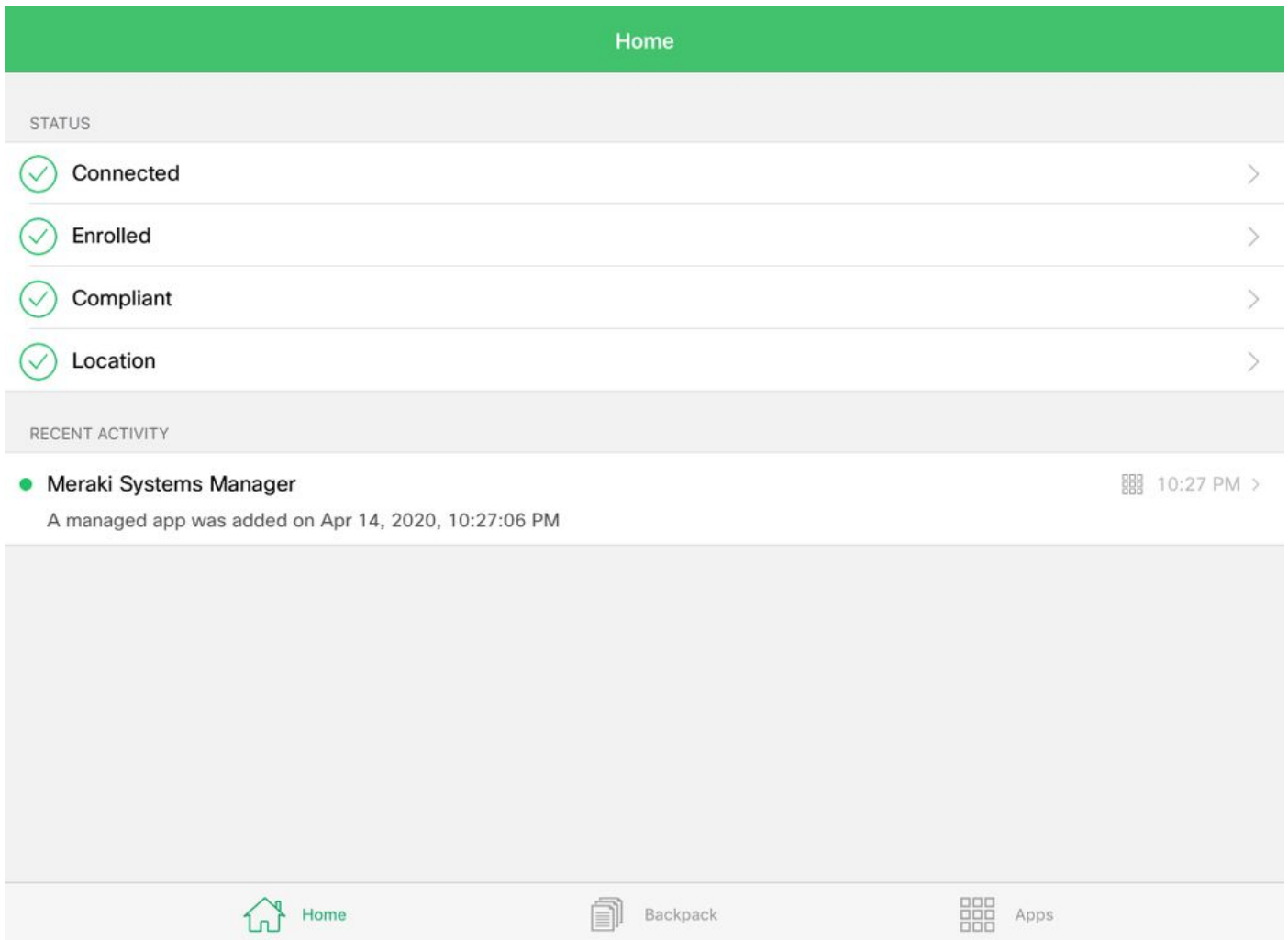




1.11. Öffnen Sie die kürzlich heruntergeladene Anwendung **Meraki MDM**, die sich auf dem Hauptbildschirm befindet.



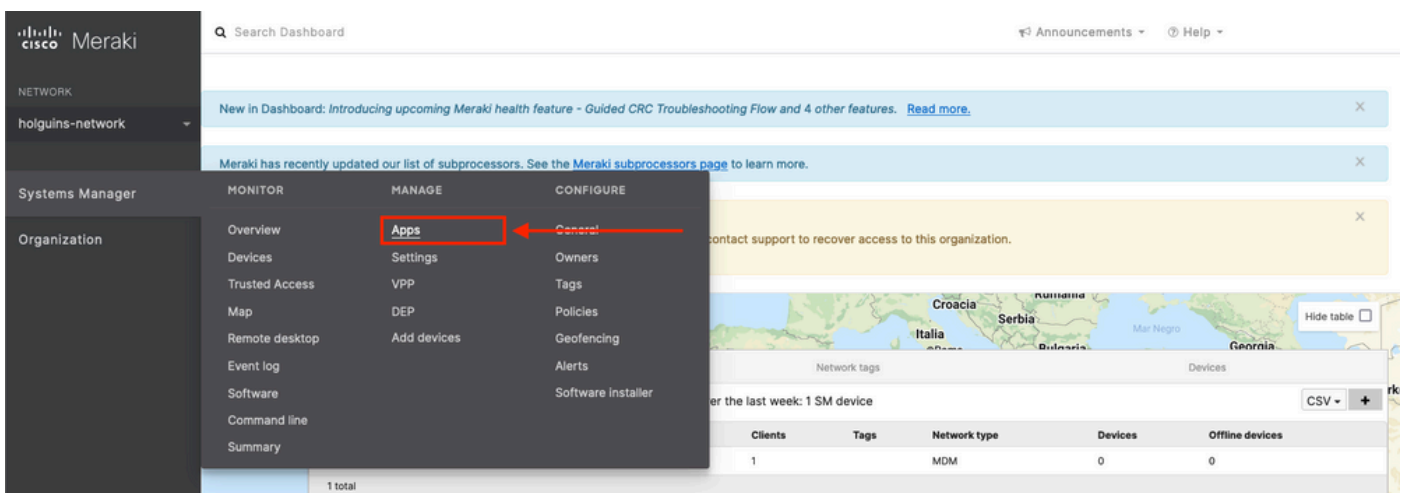
1.12. Vergewissern Sie sich, dass alle Status mit einem grünen Häkchen versehen sind, das bestätigt, dass die Registrierung abgeschlossen ist.



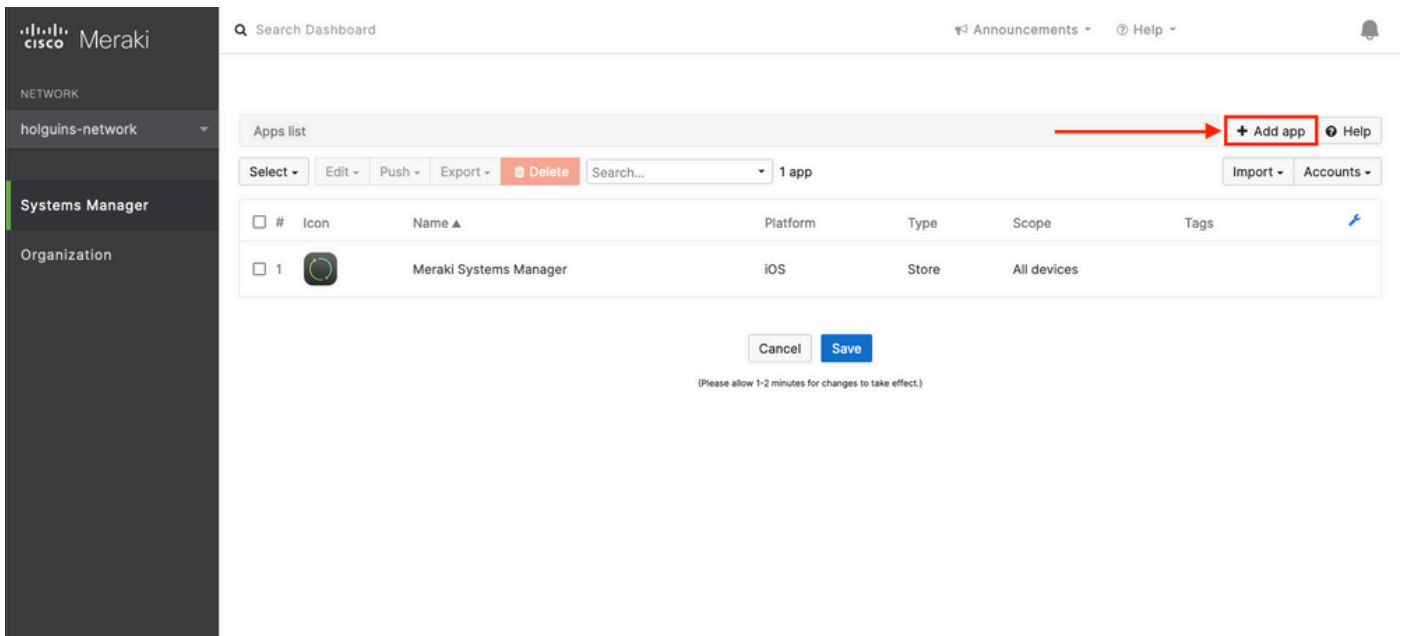
## Schritt 2: Verwaltete Anwendungen einrichten

Um die tunnelten Apps für PerApp später in diesem Dokument einzurichten, müssen Sie dieselben Anwendungen über SM verwalten. In diesem Konfigurationsbeispiel soll Firefox per App getunnelt werden und wird daher den verwalteten Apps hinzugefügt.

2.1. Navigieren Sie zu **Systems Manager > Manage > Apps**, um die verwalteten Apps hinzuzufügen.

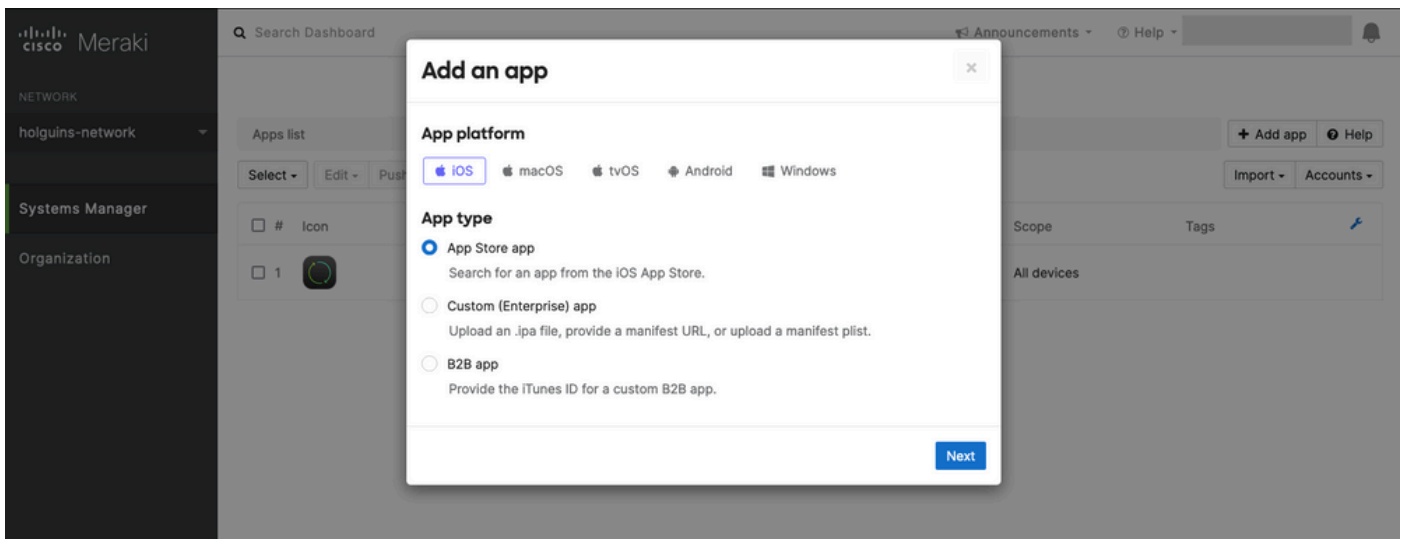


2.2. Wählen Sie die Option **App hinzufügen**.



2.3. Wählen Sie den Anwendungstyp (App Store, Custom, B2B), je nachdem, wo die App gespeichert ist. Wählen Sie nach der Auswahl die Option **Weiter** aus.

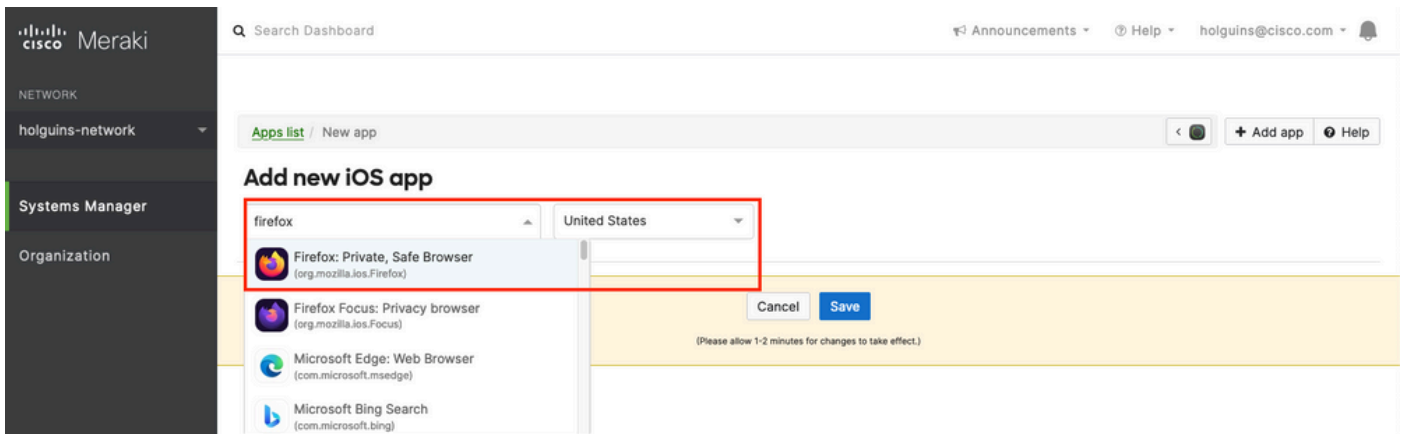
In diesem Beispiel wird die App öffentlich im App Store gespeichert.



2.4. Suchen Sie bei entsprechender Aufforderung nach der gewünschten Anwendung, und wählen Sie die Region aus, aus der die Anwendung heruntergeladen werden soll. Wählen Sie **Speichern** aus, sobald die App ausgewählt wurde.

**Hinweis:** Wenn das Land nicht mit der Region des Apple-Kontos übereinstimmt, kann es zu Problemen mit der Anwendung kommen.

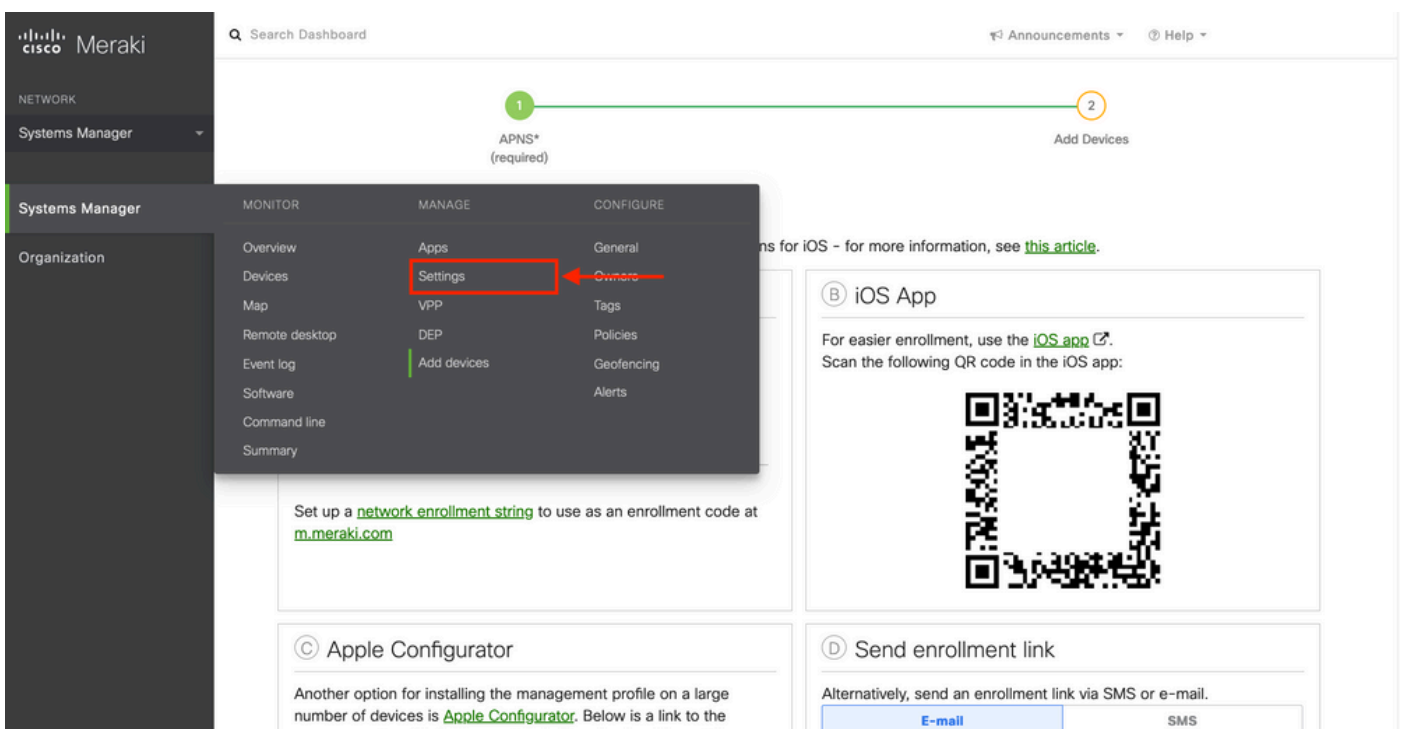




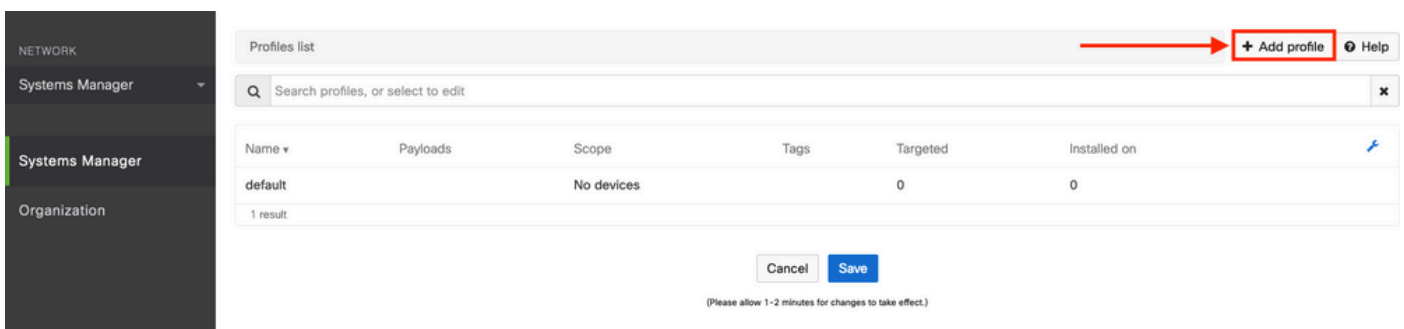
2.5. Klicken Sie auf **Speichern**, sobald Sie alle gewünschten Anwendungen ausgewählt haben.

## Schritt 3: Konfigurieren des ProApp-VPN-Profiles

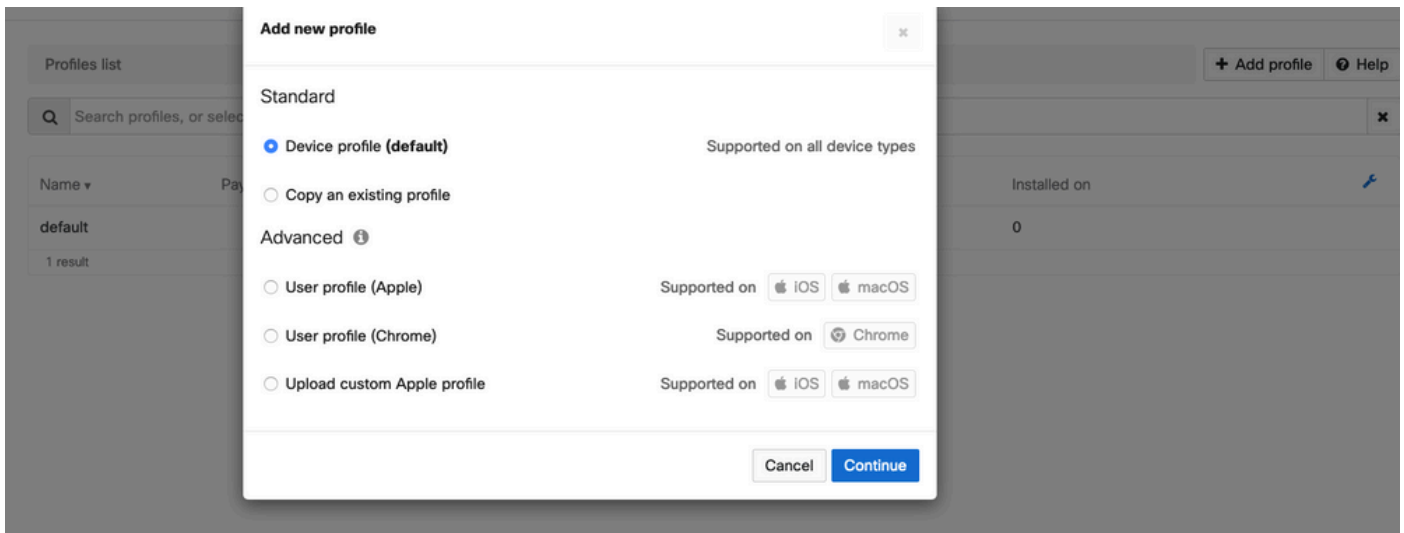
3.1. Navigieren Sie zu **Systems Manager > Manage > Settings**



3.2. Wählen Sie die Option **Profil hinzufügen**.



3.3. Wählen Sie **Geräteprofil (Standard)** aus, und klicken Sie auf **Weiter**.



3.4. Wenn das Menü **Profile Configuration (Profilkonfiguration)** angezeigt wird, geben Sie den **Namen ein**, und wählen Sie die Zielgeräte unter **Scope (Bereich)** aus.

⚙️ 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

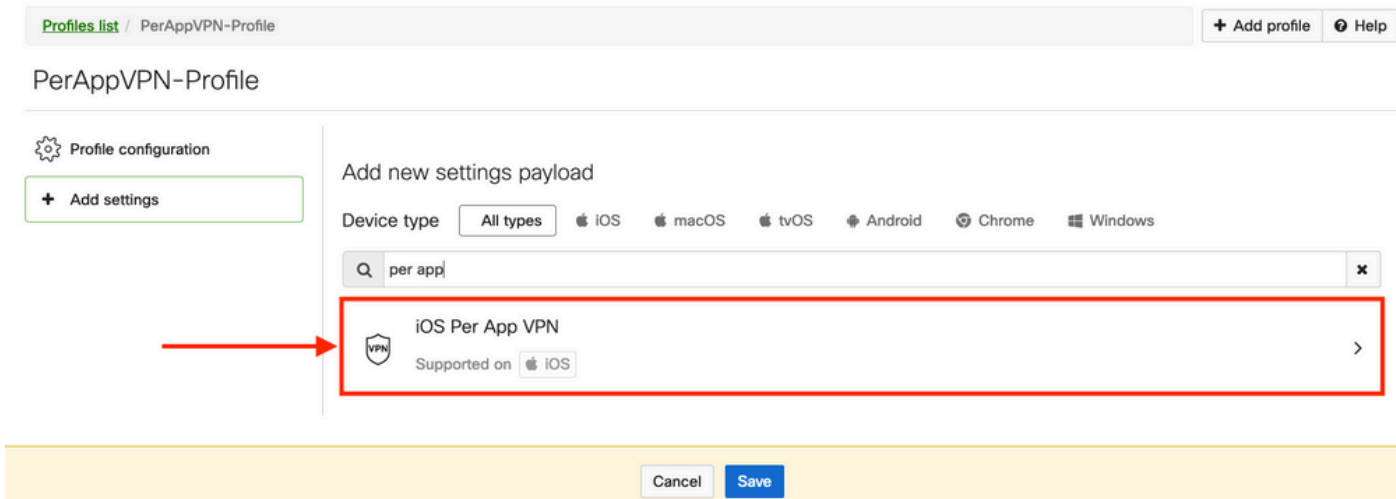
**Installation target** All devices

**Status**

**Device in scope: 1 device**

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

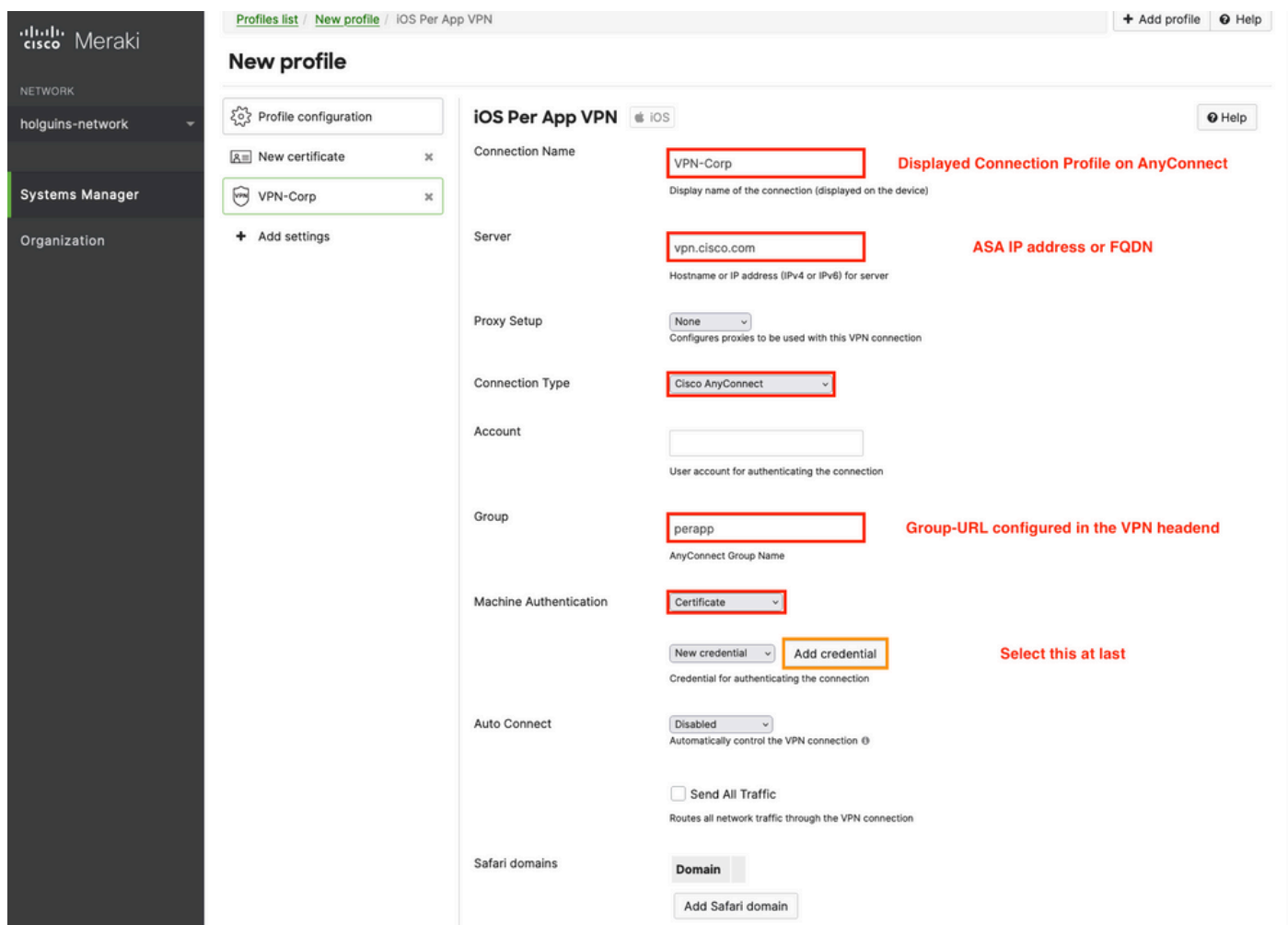
3.5. Wählen Sie **Einstellungen hinzufügen** und filtern Sie die Profiltypen nach **iOS Pro App VPN**, wählen Sie die Option wie unten gesehen.



3.6. Sobald das Menü angezeigt wird, schreiben Sie die Verbindungsinformationen basierend auf dem Beispiel unten.

Systems Manager unterstützt zwei Zertifikatregistrierungen für diese Verbindungen, SCEP und manuelle Registrierung. In diesem Beispiel wurde die manuelle Registrierung verwendet.

**Hinweis:** Wählen Sie **Anmeldeinformationen hinzufügen**, nachdem Sie die Textfelder ausgefüllt haben, da Sie mit dieser Option in ein neues Menü zum Hinzufügen einer Zertifikatsdatei gelangen.



3.7. Nachdem Sie auf **Anmeldeinformationen hinzufügen** geklickt und zum Menü Zertifikat

weitergeleitet wurden, schreiben Sie den **Namen** des Zertifikats, suchen Sie auf Ihrem Computer nach dem **Kenntwort**, das die PFX-Datei schützt (verschlüsselte Zertifikatsdatei).

The screenshot shows the Meraki dashboard interface. On the left is a navigation sidebar with 'Meraki', 'NETWORK', 'holguins-network', 'Systems Manager', and 'Organization'. The main content area is titled 'New profile' and has a breadcrumb 'Profiles list / New profile / Certificate'. Below this is a 'Profile configuration' section with 'machine-auth' and 'VPN-Corp' selected. The 'Certificate' section contains a 'Name' field with 'machine-auth', a 'Password' field with masked characters, and a 'Certificate' field with a red box around 'Examinar...' and the text 'No se ha seleccionado ningún archivo.' Below the fields are 'Cancel' and 'Save' buttons and a note: '(Please allow 1-2 minutes for changes to take effect.)'

3.8. Nach der Auswahl des Zertifikats wird der Dateiname des Zertifikats angezeigt.

This screenshot is similar to the previous one but shows the 'Certificate' field updated. It now displays 'Filename: pfxbin.pfx', 'Issuer:', 'Subject/CN:', and 'Expiration: Select new certificate'. The 'Cancel' and 'Save' buttons and the note '(Please allow 1-2 minutes for changes to take effect.)' are still present at the bottom.

3.9. Nachdem Sie das Zertifikat ausgewählt haben, navigieren Sie zum zuvor verwendeten VPN-Profil, und wählen Sie die kürzlich importierten Anmeldeinformationen aus, und wählen Sie die getunnelte App aus (in diesem Fall Firefox).

Klicken Sie nach Abschluss dieses Vorgangs auf **Speichern**.

3.10. Überprüfen Sie, ob das Profil auf den Zielgeräten installiert ist.

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

## Schritt 4: Konfiguration der Anwendungsauswahl

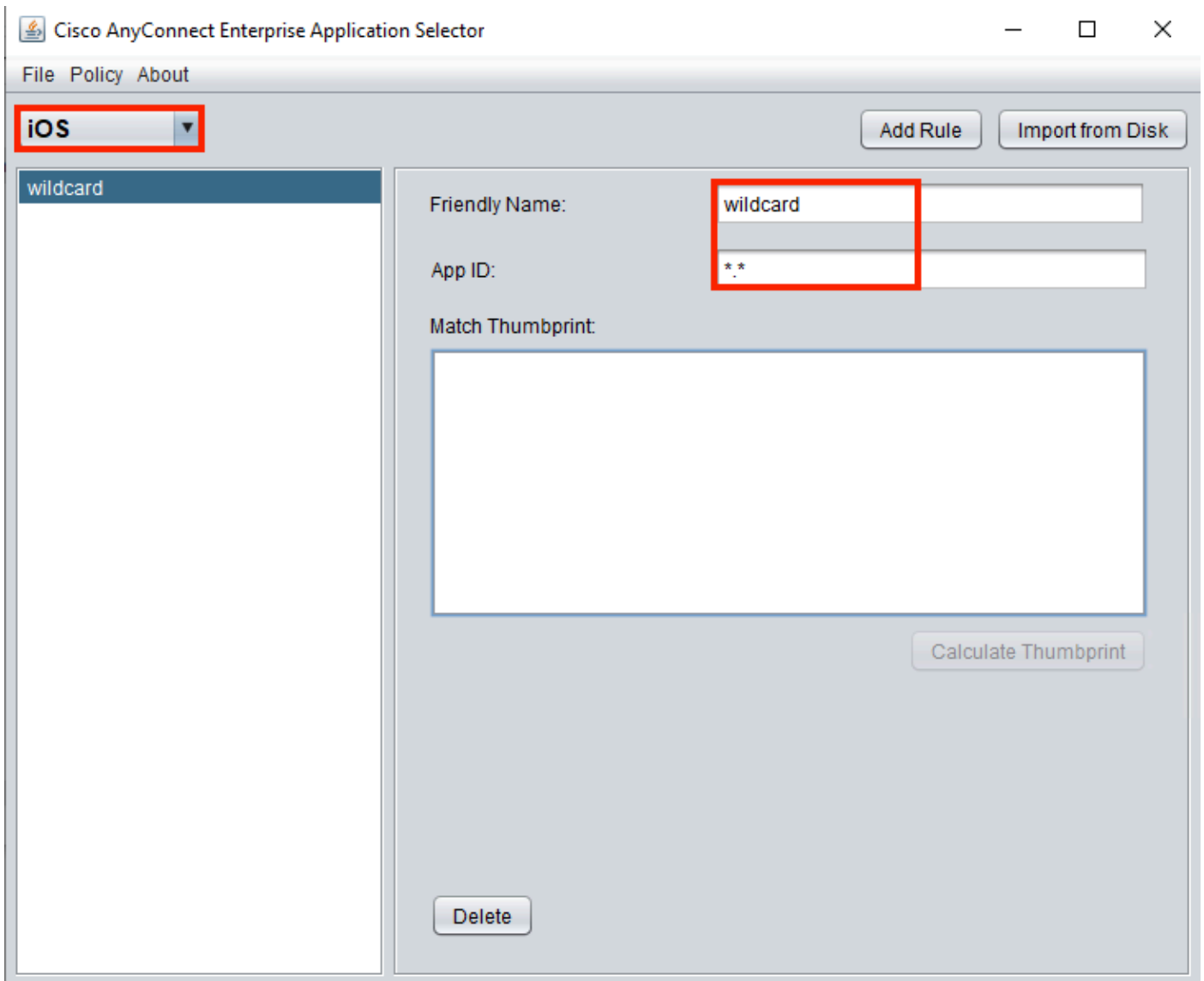
4.1. App Selector von der Cisco Website herunterladen

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

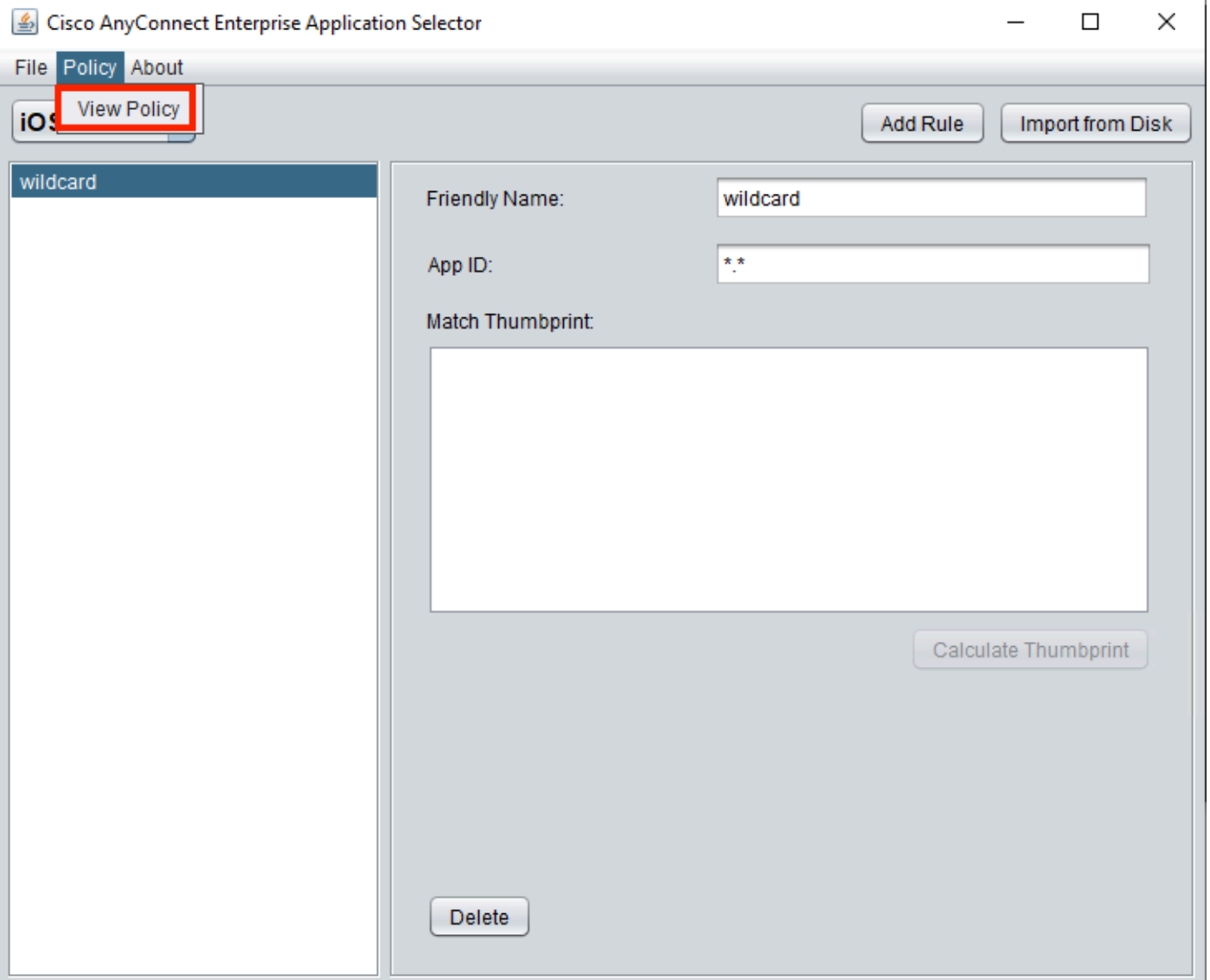
**Achtung:** Führen Sie die Anwendung auf einem Windows-Computer aus. Die angezeigten Ergebnisse sind nicht die erwarteten, wenn das Tool auf MacOS-Geräten verwendet wird.

4.2. Öffnen Sie die Java Anwendung. Wählen Sie **iOS** aus dem Dropdown-Menü aus, fügen Sie einen Anzeigenamen hinzu, und stellen Sie sicher, dass Sie **.\*** in die **App-ID** eingeben.





4.3. Navigieren Sie zu **Richtlinie**, und wählen Sie **Richtlinie anzeigen** aus.



4.4. Kopieren Sie die angezeigte Zeichenfolge. (Dies wird später in der VPN-Headend-Konfiguration verwendet.)

```
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSgIYk
FBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB
```

OK

## Schritt 5: ASA - Beispiel-VPN-Konfiguration pro Anwendung

```
conf t
webvpn
anyconnect-custom-attr perapp description PerAppVPN
anyconnect-custom-data perapp wildcard
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSg
IYkFBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB

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
```

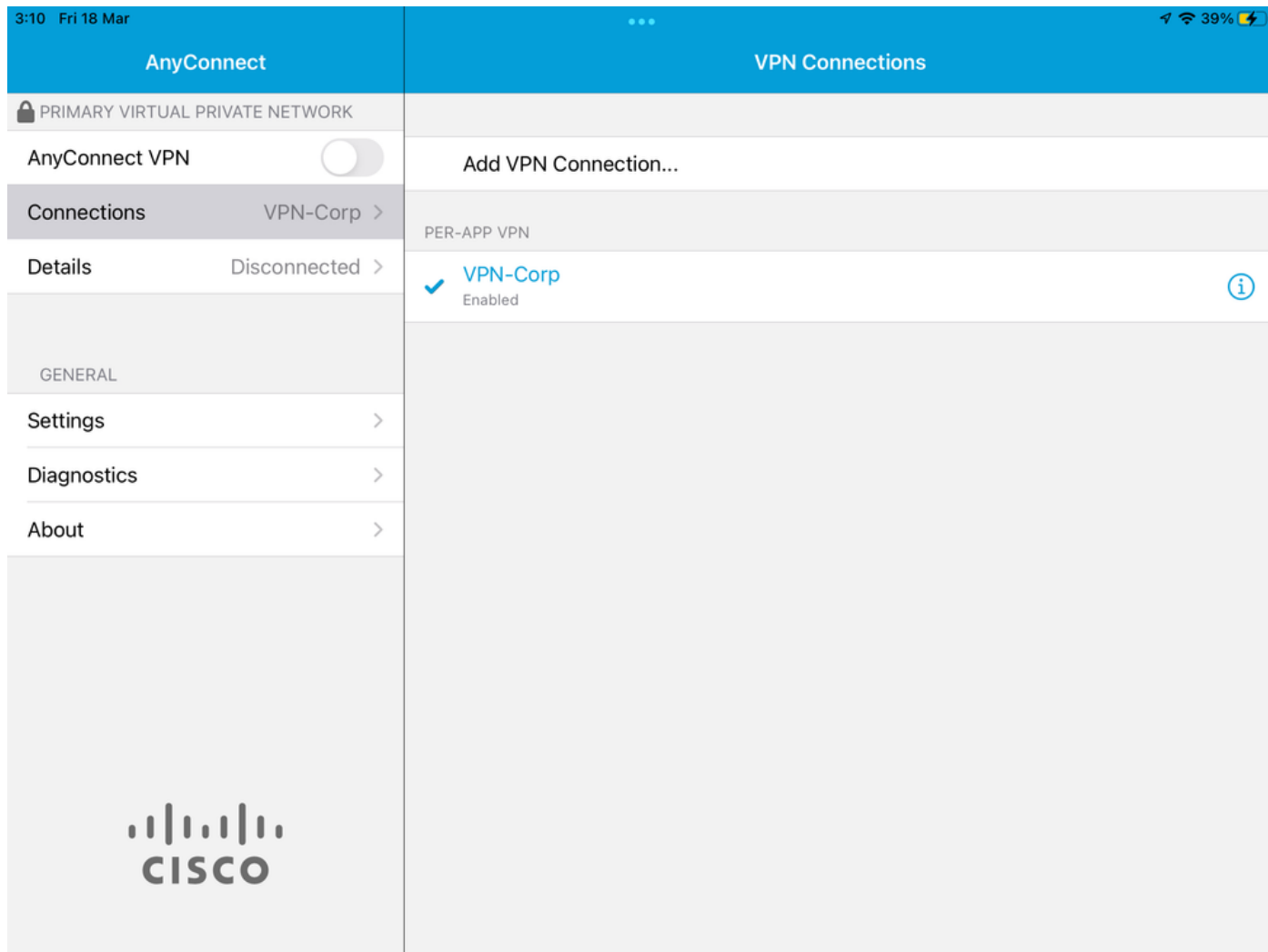
group-url https://vpn.cisco.com/perapp enable

# Überprüfung

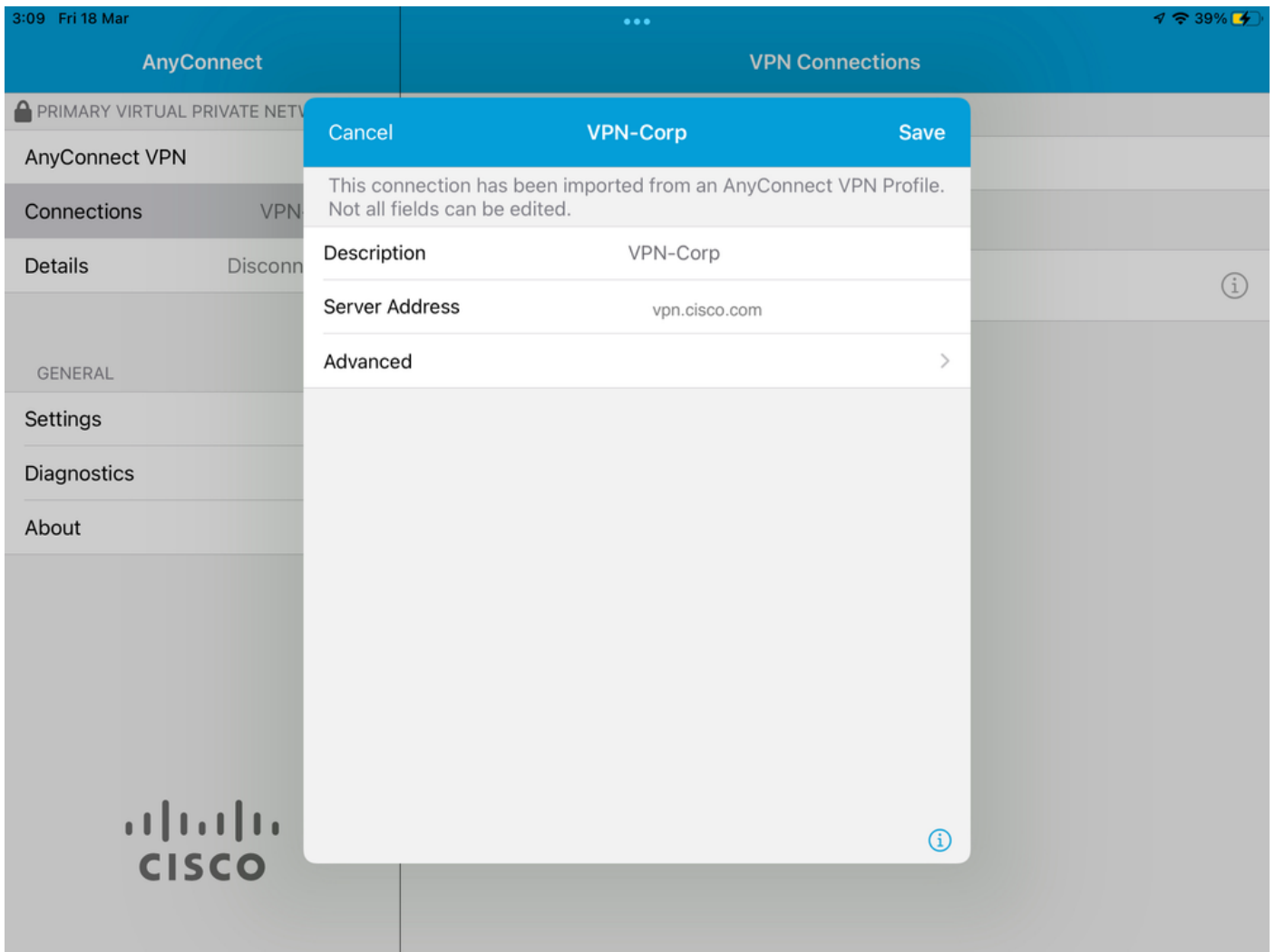
## 6. Überprüfen der Profilinstallation auf der AnyConnect-Anwendung

6.1. Öffnen Sie die AnyConnect-Anwendung, und wählen Sie im linken Bereich **Verbindungen aus**. Das PerApp VPN-Profil muss in einem neuen Abschnitt mit der Bezeichnung **PER-APP VPN** angezeigt werden.

Wählen Sie das **i** aus, um die erweiterten Einstellungen anzuzeigen.

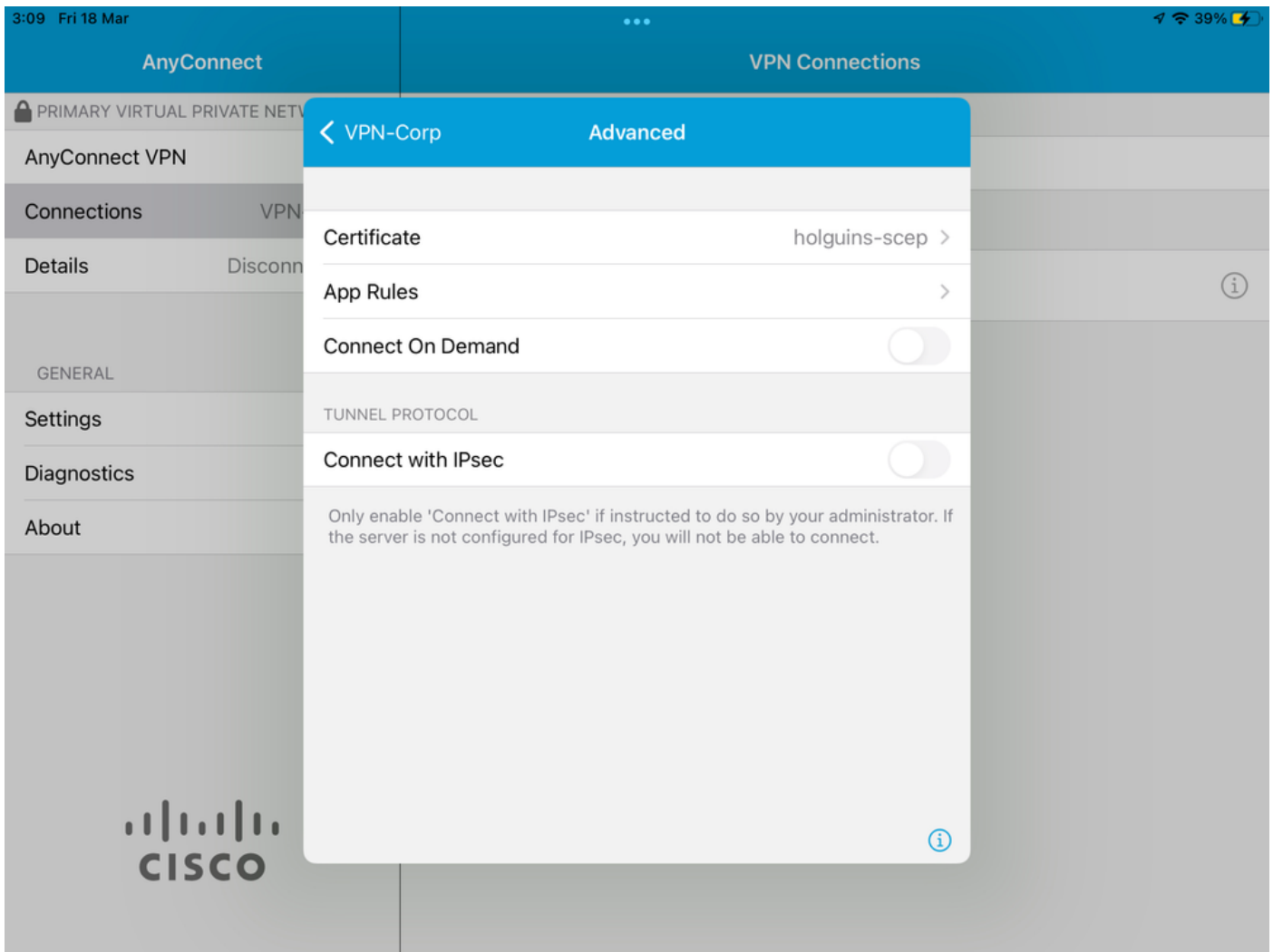


6.2. Wählen Sie die Option **Erweitert**.

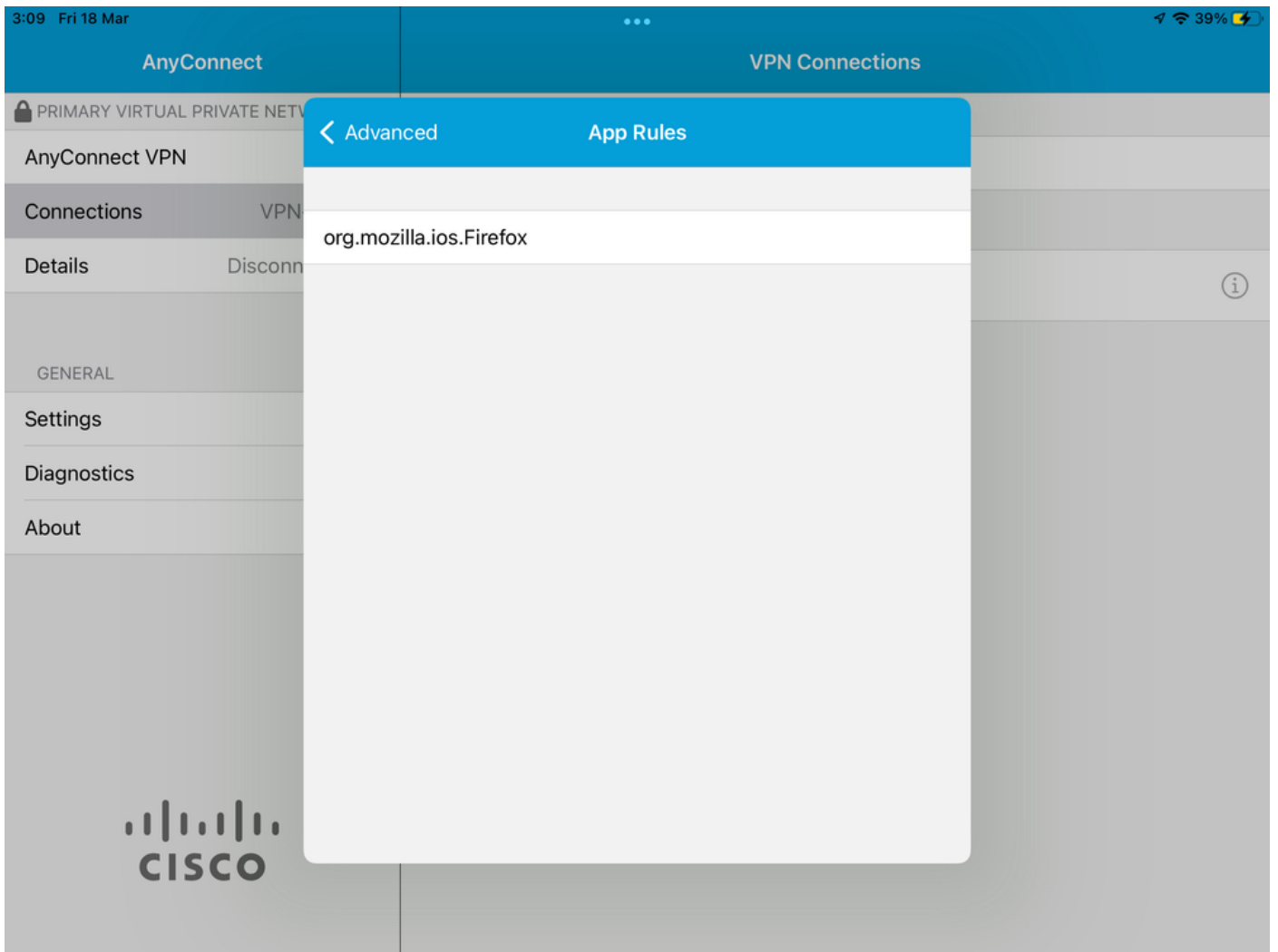


6.3. Wählen Sie die Option **App Rules**.





6.4. Überprüfen Sie abschließend, ob die App-Regel installiert ist. (Mozilla ist die getunnelte App, die in diesem Dokument gewünscht wird, daher war die App-Installation erfolgreich).



## Fehlerbehebung

Derzeit gibt es keine spezifischen Schritte zur Fehlerbehebung für dieses Dokument.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.