

Meraki System Managerを使用したiOS用 Anyconnect PerApp VPNの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ 1 : Cisco Meraki Systems ManagerへのiOSデバイスの登録](#)

[ステップ 2 : 管理対象アプリのセットアップ](#)

[ステップ 3 : PerApp VPNプロファイルの設定](#)

[ステップ 4 : アプリケーションセクタの設定](#)

[ステップ 5 : アプリケーションごとのASAのVPN設定例](#)

[確認](#)

[6. AnyConnectアプリケーションでのプロファイルインストールの確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Meraki Mobile Device Manager(MDM)、System Manager(SM)で管理されているApple iOSデバイスでPerApp VPNを設定する方法について説明します。

前提条件

要件

- AnyConnect v4.0 PlusまたはApexライセンス。
- Per App VPNをサポートするためのASA 9.3.1以降。
- Cisco Enterprise Application SelectorツールはCisco.comから入手できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- ASA 5506W-Xバージョン9.15(1)10
- iPad iOSバージョン15.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

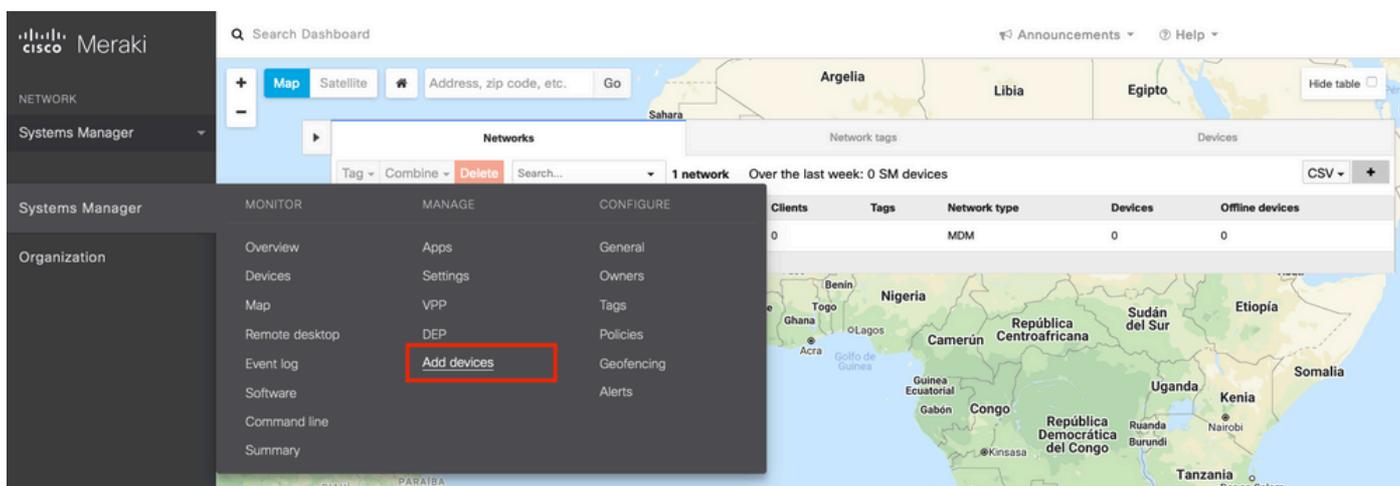
このドキュメントには、次に示すプロセスは含まれません。

- ・クライアント証明書を生成するためのシステムマネージャでのSCEP CAの設定
- ・iOSクライアント用のPKCS12クライアント証明書の生成

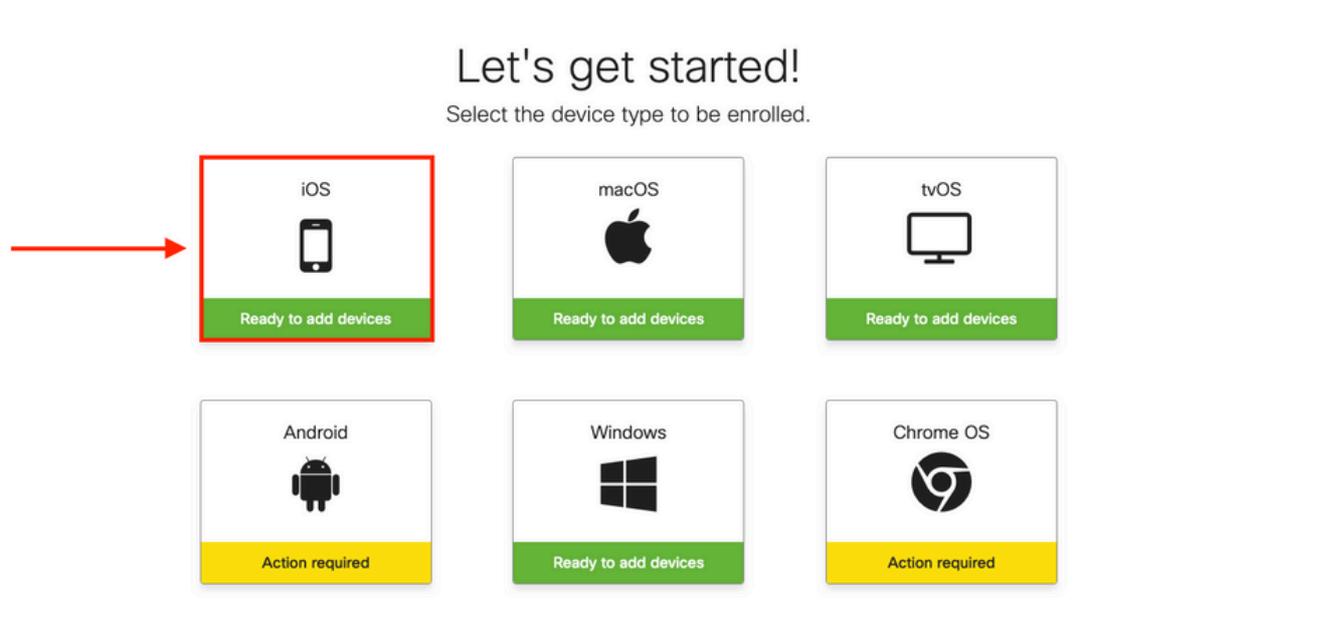
設定

ステップ 1 : Cisco Meraki Systems ManagerへのiOSデバイスの登録

1.1. [Systems Manager] > [Add Devices] に移動します。



1.2. [iOS] オプションをクリックして登録を開始します。



1.3. インターネットブラウザ経由でデバイスを登録するか、カメラでQRコードをスキャンします。このドキュメントでは、登録プロセスにカメラを使用しました。



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.カメラがQRコードを認識したら、ポップアップ表示されるSafariで「meraki.com」を開く通知を選択します。

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 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:



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](#) software.

D Send enrollment link

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

E-mail SMS

1.5.プロンプトが表示されたら、**Register**を選択します。

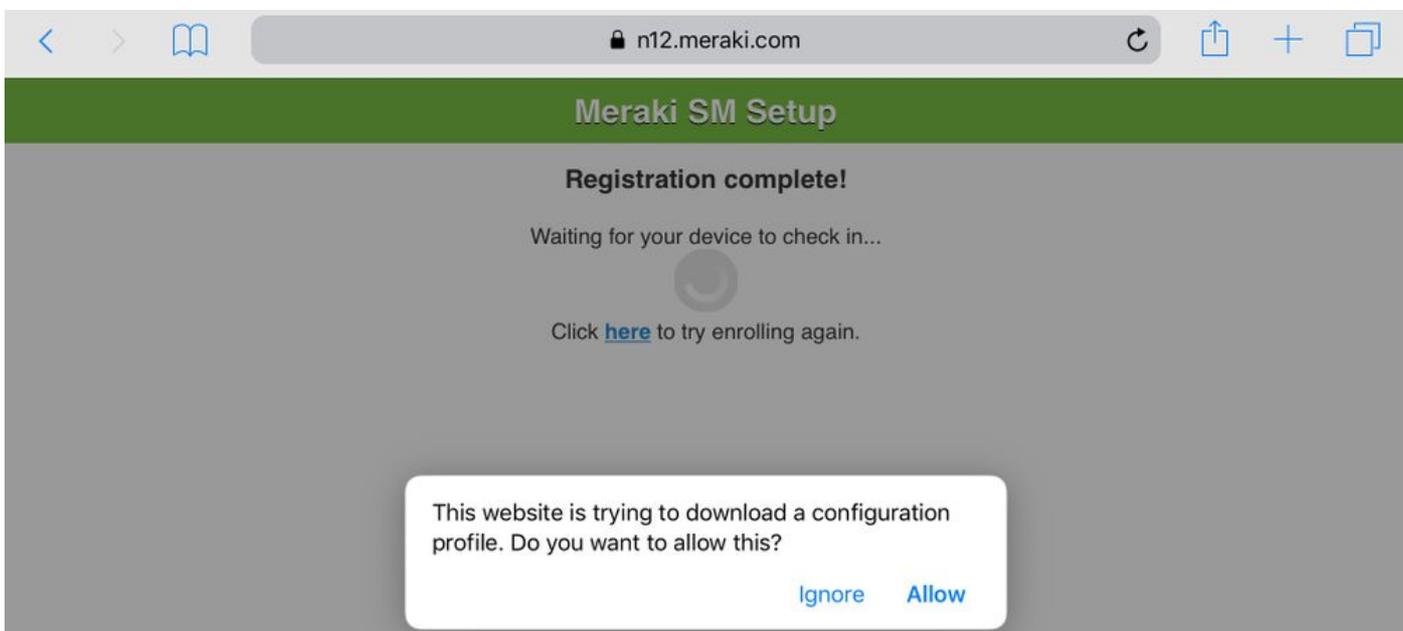


Step 1: Enter your Network ID

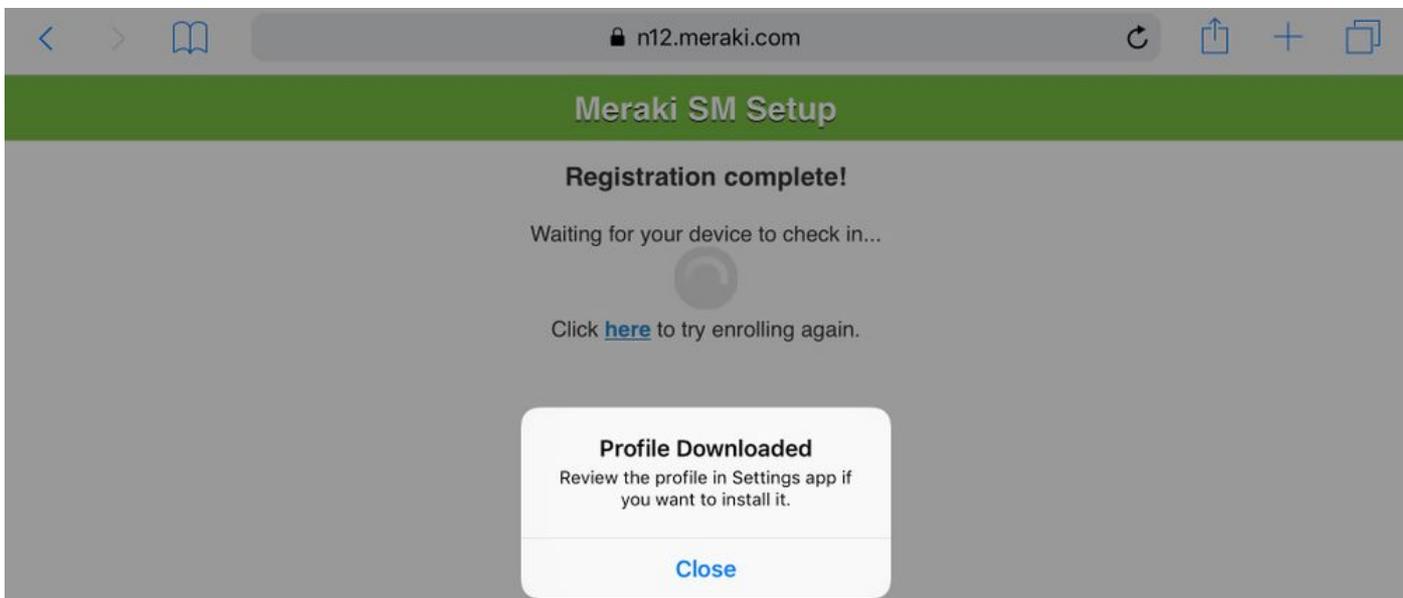
The Network ID is either a 10-digit code or a combination of letters, numbers, or characters (e.g. [123-456-7890](#) or network-id).

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

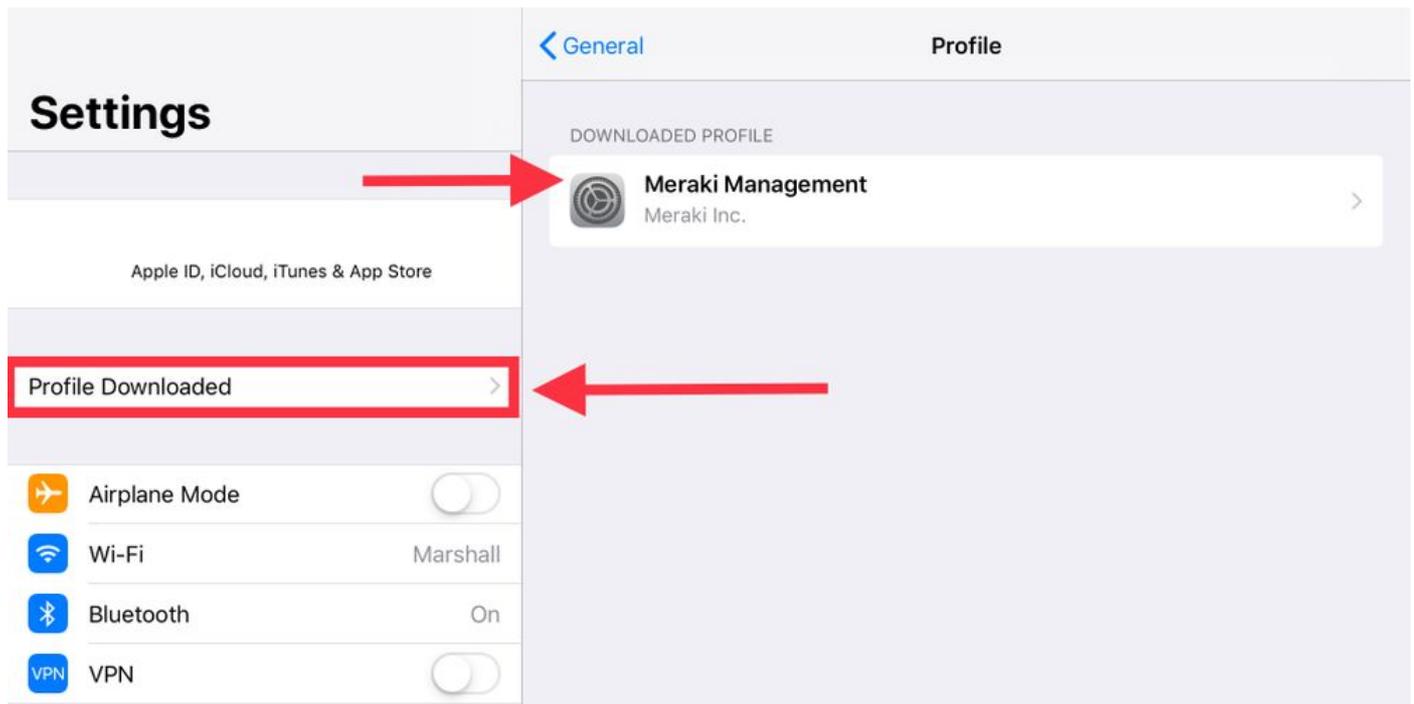
1.6. [Allow] を選択して、デバイスがMDMプロファイルをダウンロードできるようにします。



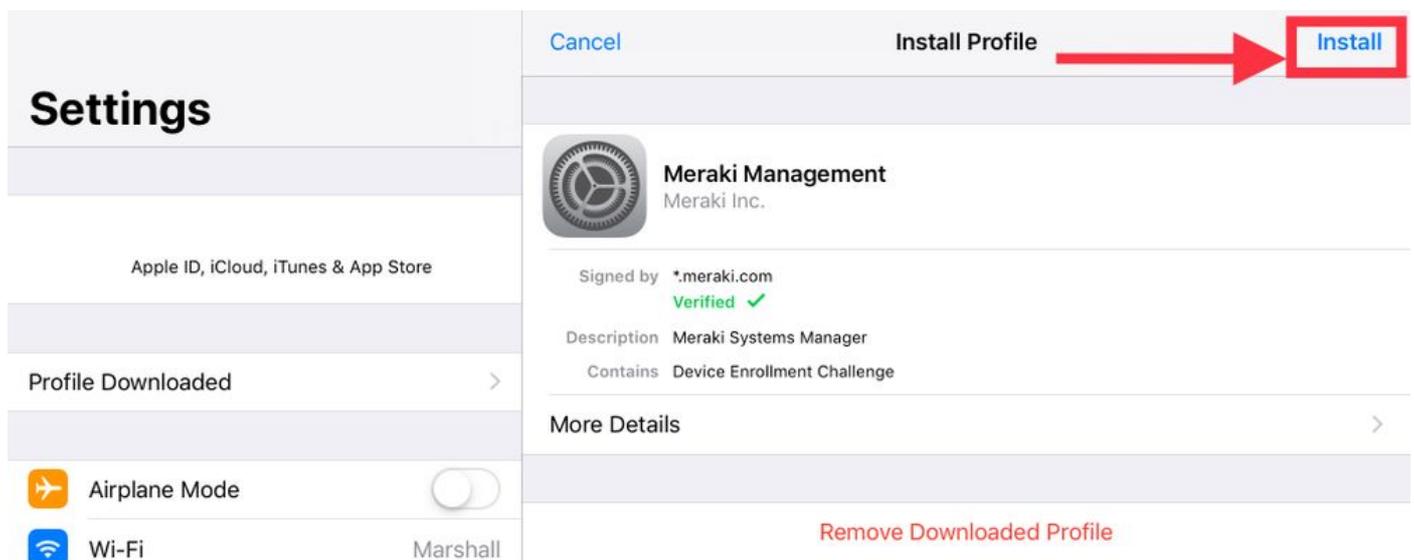
1.7. [Close] を選択してダウンロードを完了します。



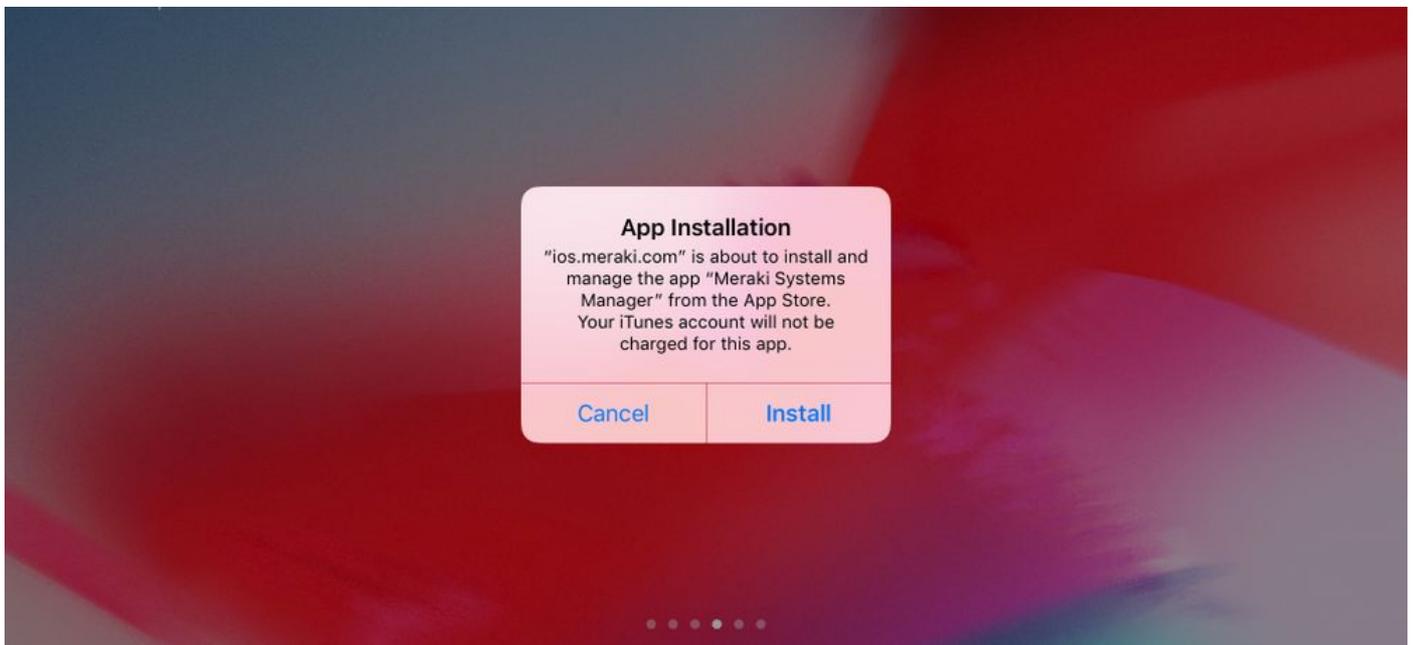
1.8. iOS Settings Appに移動し、左側のペインで**Profile Downloaded**オプションを見つけて、**Meraki Management**セクションを選択します。



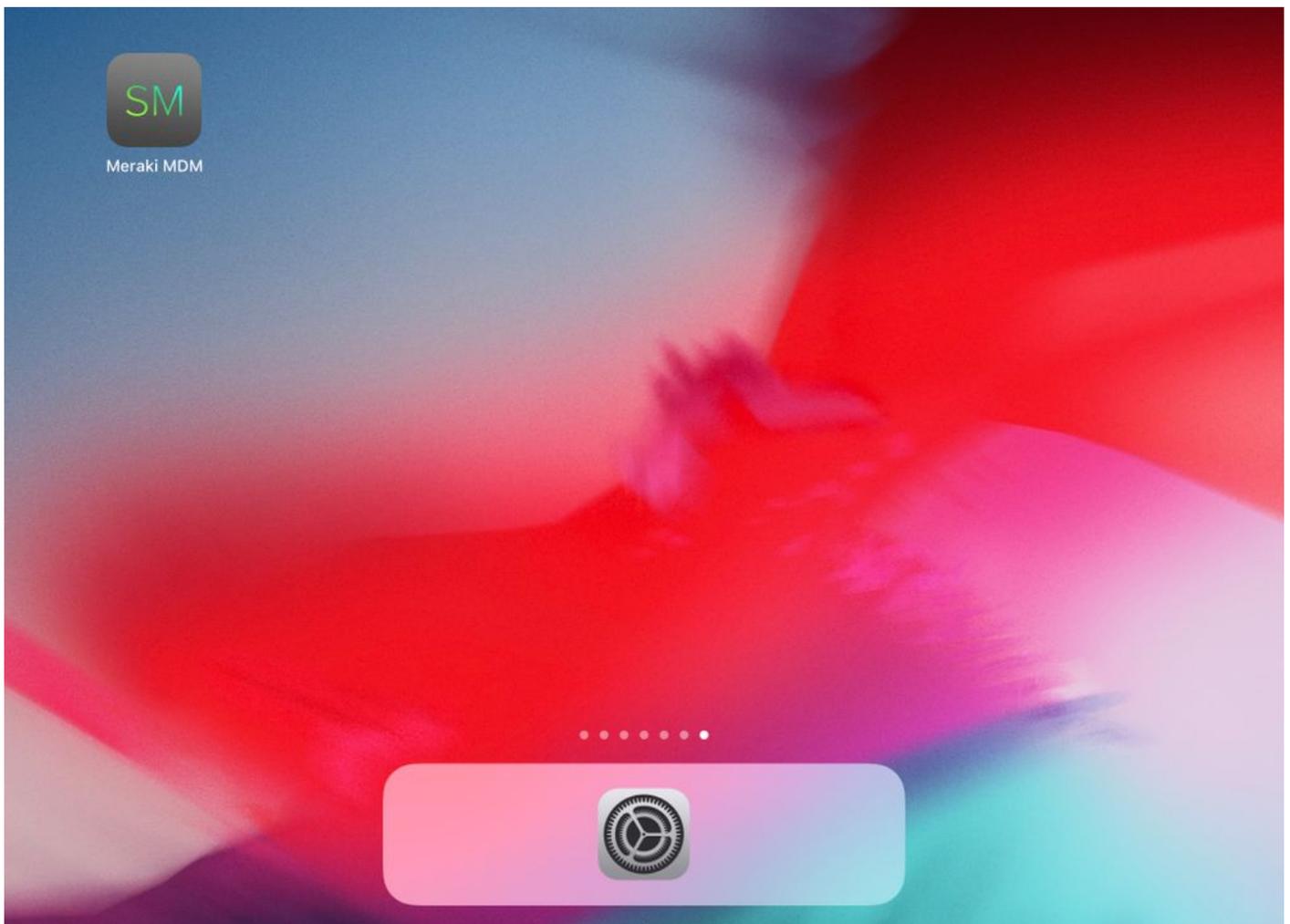
1.9. [Install] オプションを選択して、MDMプロファイルをインストールします。



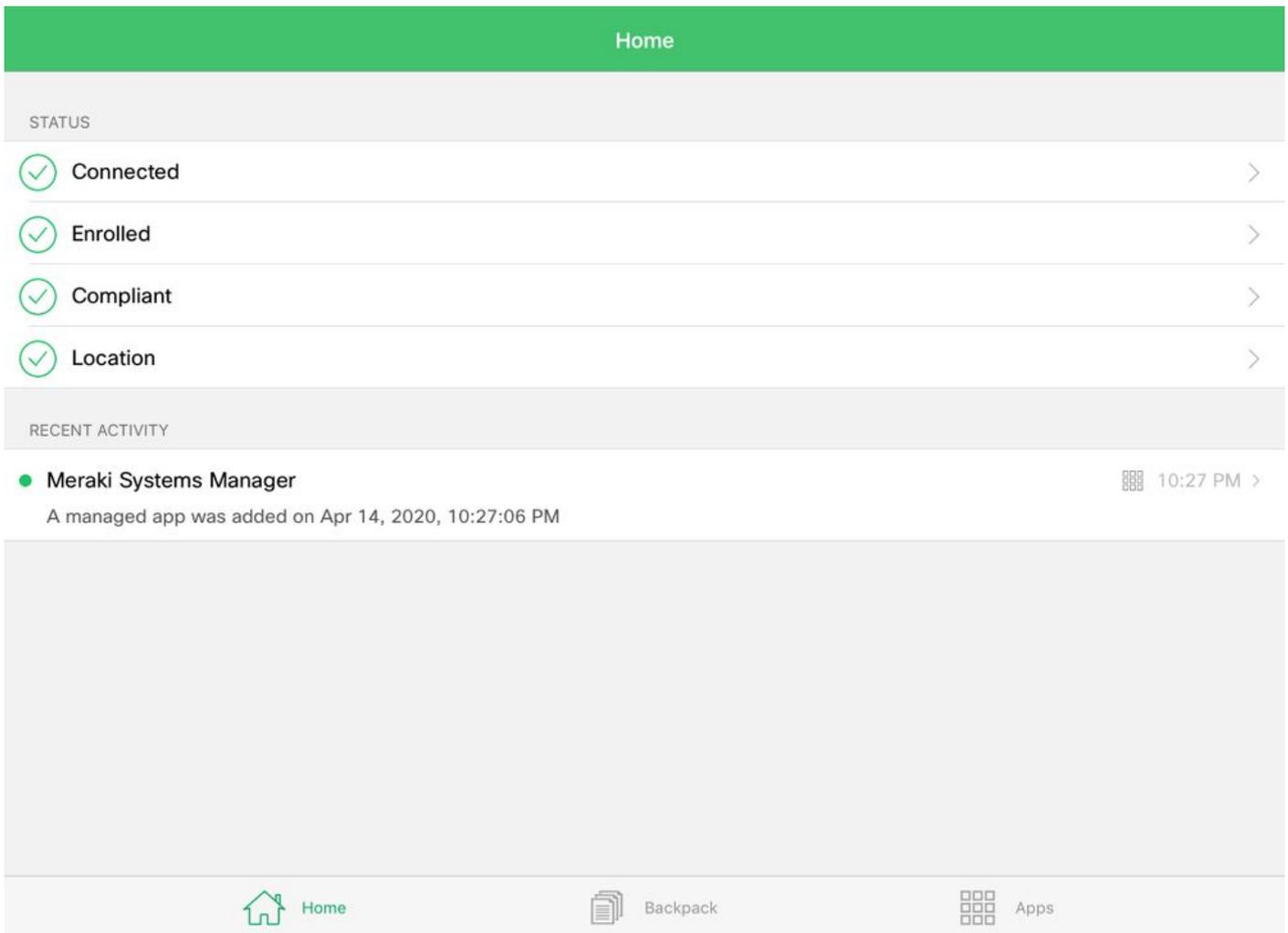
1.10. SMアプリケーションをインストールするためのアクセス権を付与する必要があります。



1.11. ホーム画面にある最近ダウンロードしたMeraki MDMというアプリケーションを開きます。



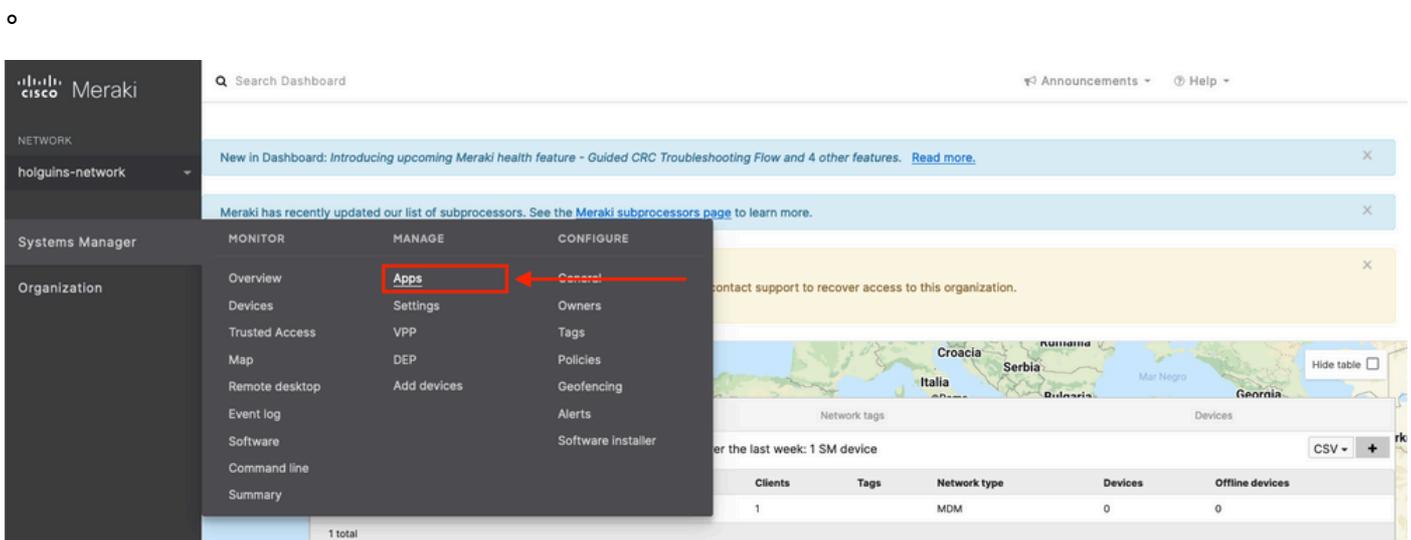
1.12. すべてのステータスに、登録が完了したことを示す緑色のチェックマークが付いていることを確認します。



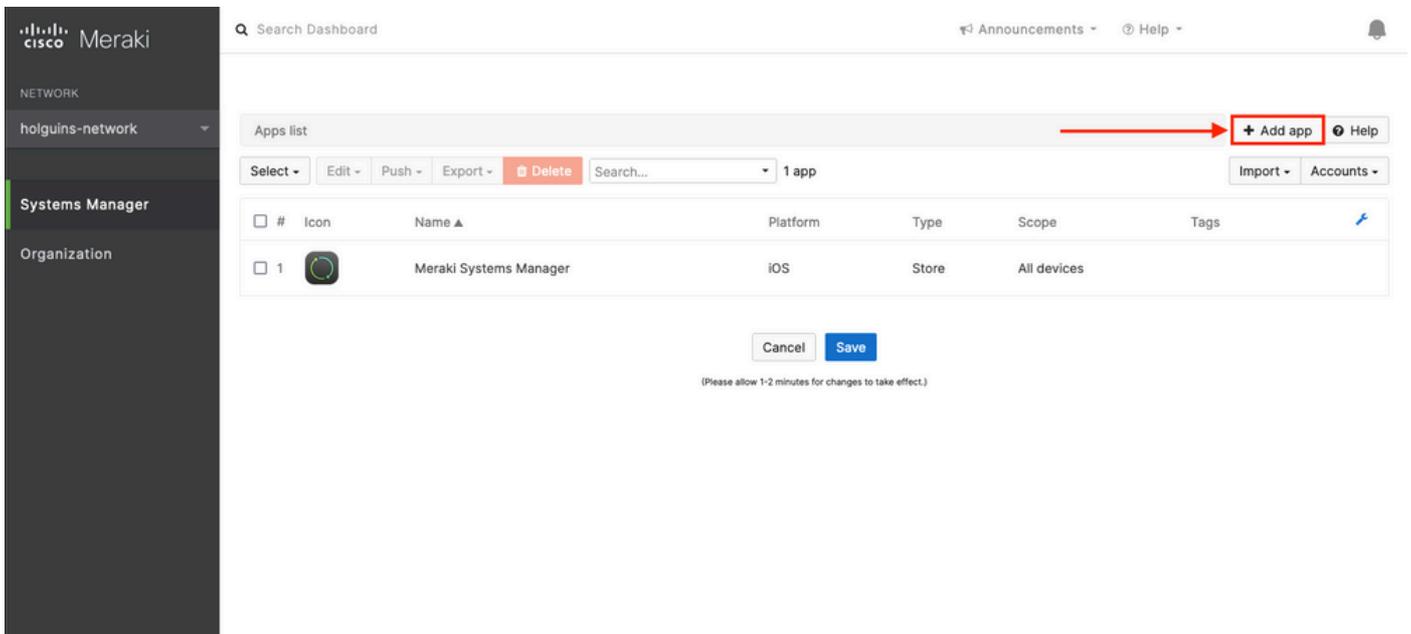
ステップ 2 : 管理対象アプリのセットアップ

このドキュメントの後半でPerApp用のトンネルアプリをセットアップするには、SMを介してこれらの同じアプリケーションを管理する必要があります。この設定例では、FirefoxはPer Appを介してトンネリングされることを意図しているため、管理対象アプリに追加されます。

2.1. [Systems Manager] > [Manage] > [Apps] に移動し、管理対象アプリケーションを追加します。

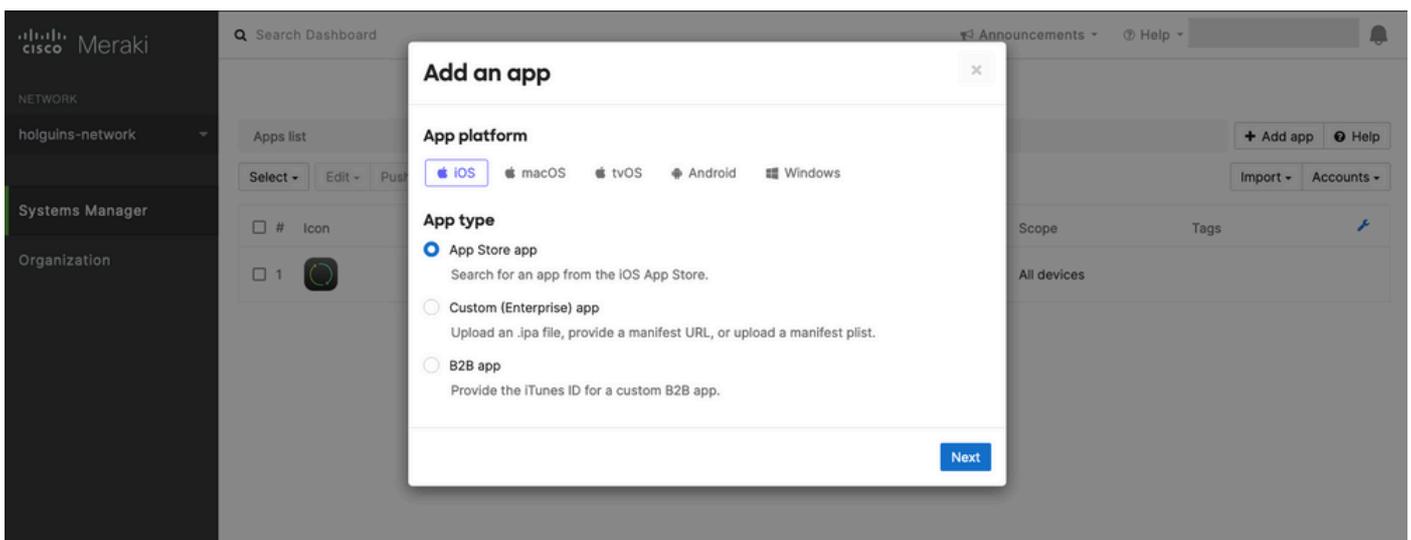


2.2. [Add app] オプションを選択します。



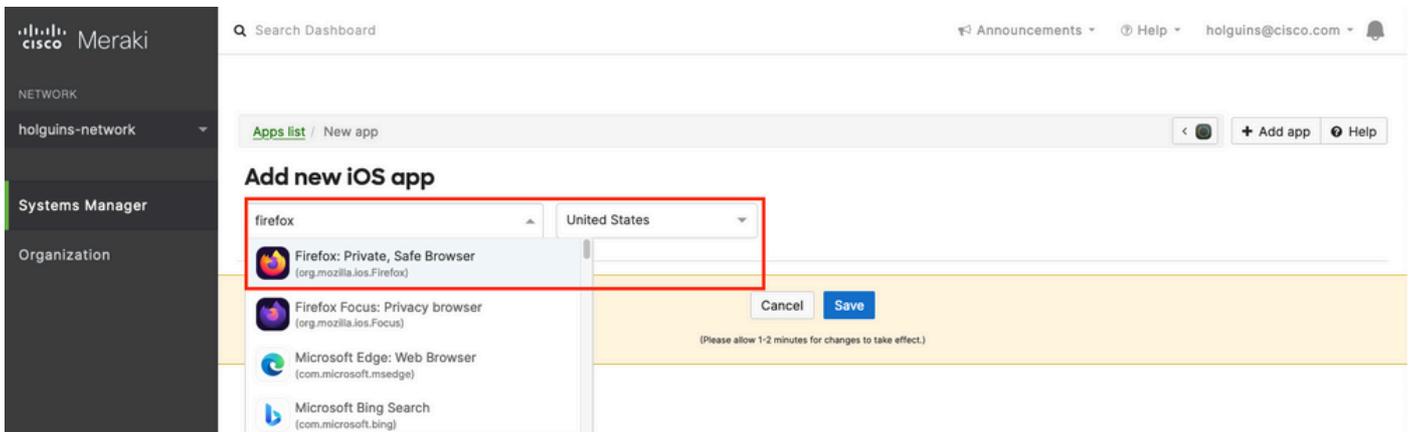
2.3.アプリケーションの種類 (App Storeアプリ、カスタム、B2B) をアプリの保存場所に基づいて選択します。選択したら、[Next] を選択します。

この例では、アプリケーションはApp Storeにパブリックに保存されます。



2.4.プロンプトが表示されたら、目的のアプリケーションを検索し、アプリケーションのダウンロード元のリージョンを選択します。アプリを選択したら、[Save] を選択します。

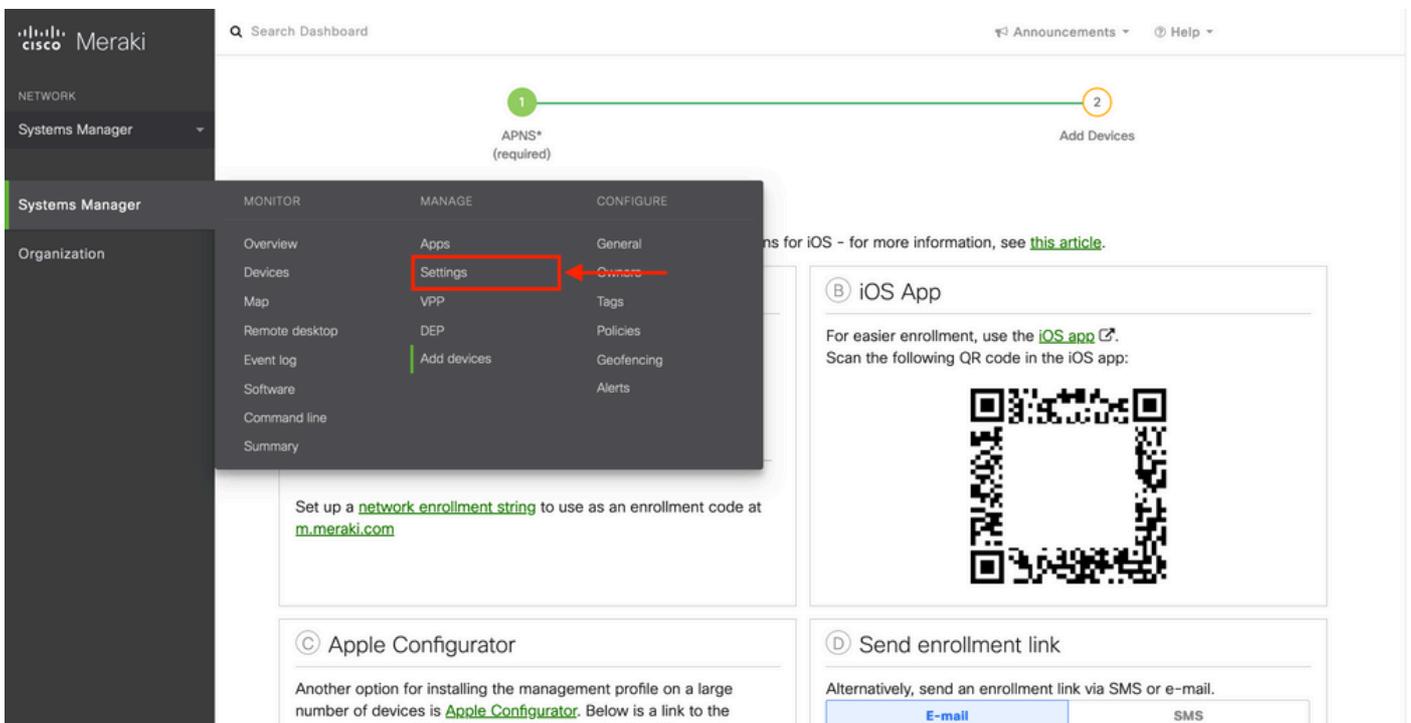
注：国がAppleアカウントの地域と一致しない場合は、アプリケーションで問題が発生する可能性があります。



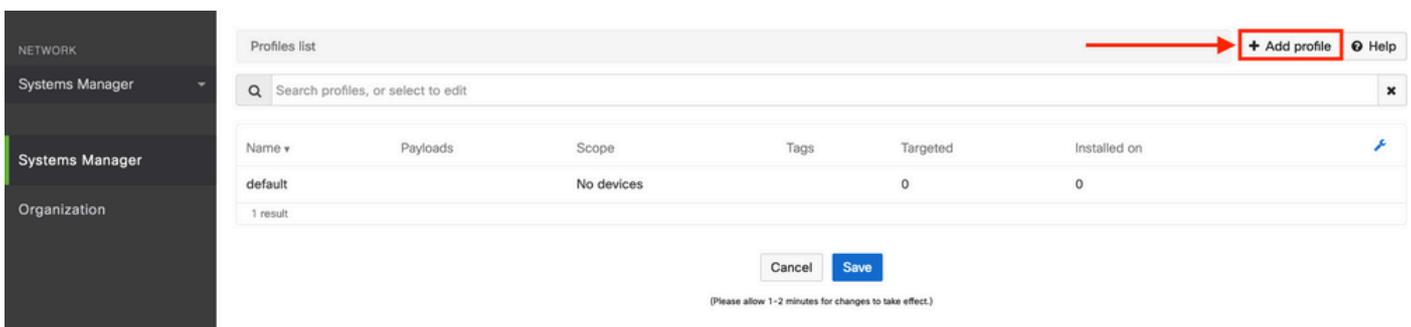
2.5. 目的のアプリケーションをすべて選択したら、[Save] をクリックします。

ステップ 3 : PerApp VPNプロファイルの設定

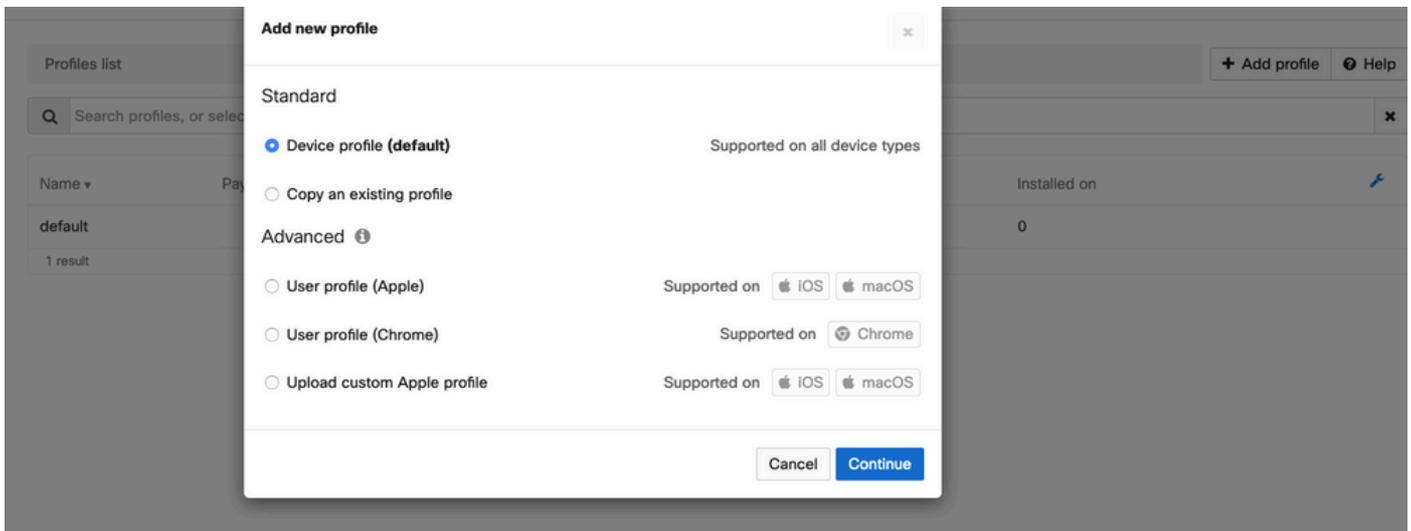
3.1. [システムマネージャ (Systems Manager)] > [管理 (Manage)] > [設定 (Settings)] に移動します



3.2. [Add profile] オプションを選択します。



3.3. [Device profile (default)] を選択し、[Continue] をクリックします。



3.4. [Profile Configuration] メニューが表示されたら、[Name] を入力し、[Scope] でターゲットデバイスを選択します。

⚙️ Profile configuration

Profile Configuration

Type Device profile

Name

The name that will be shown to users

Description

Optional

Profile Removal Policy

Removal Policy Allow users to remove this profile

Targets

Group type Manual Named Configure tags

Scope All devices Convert to target group

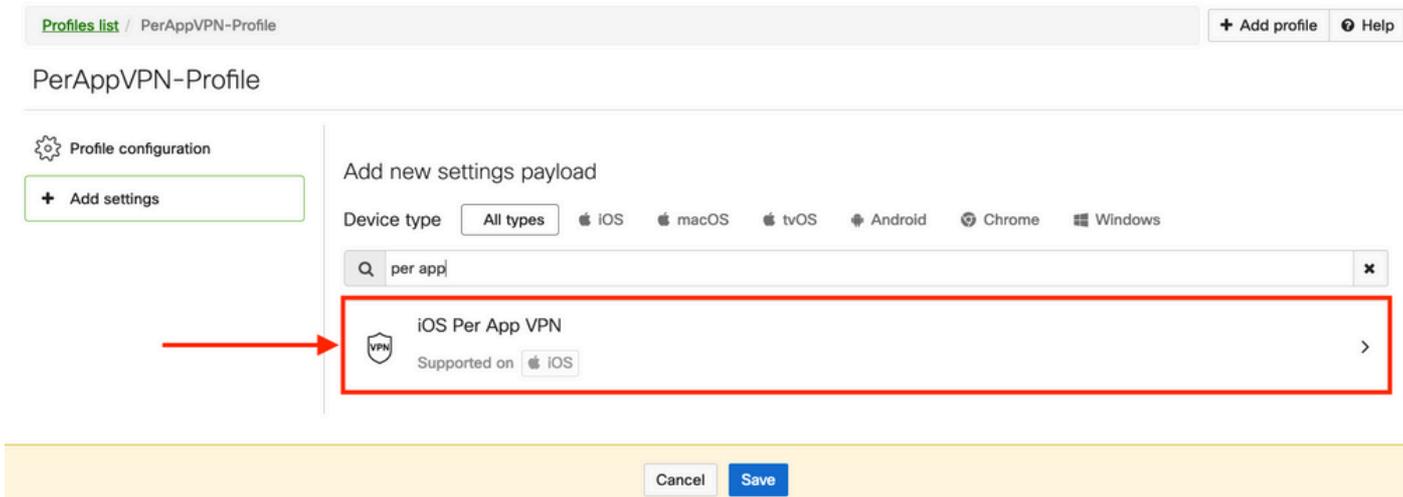
Installation target All devices

Status

Device in scope: 1 device

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

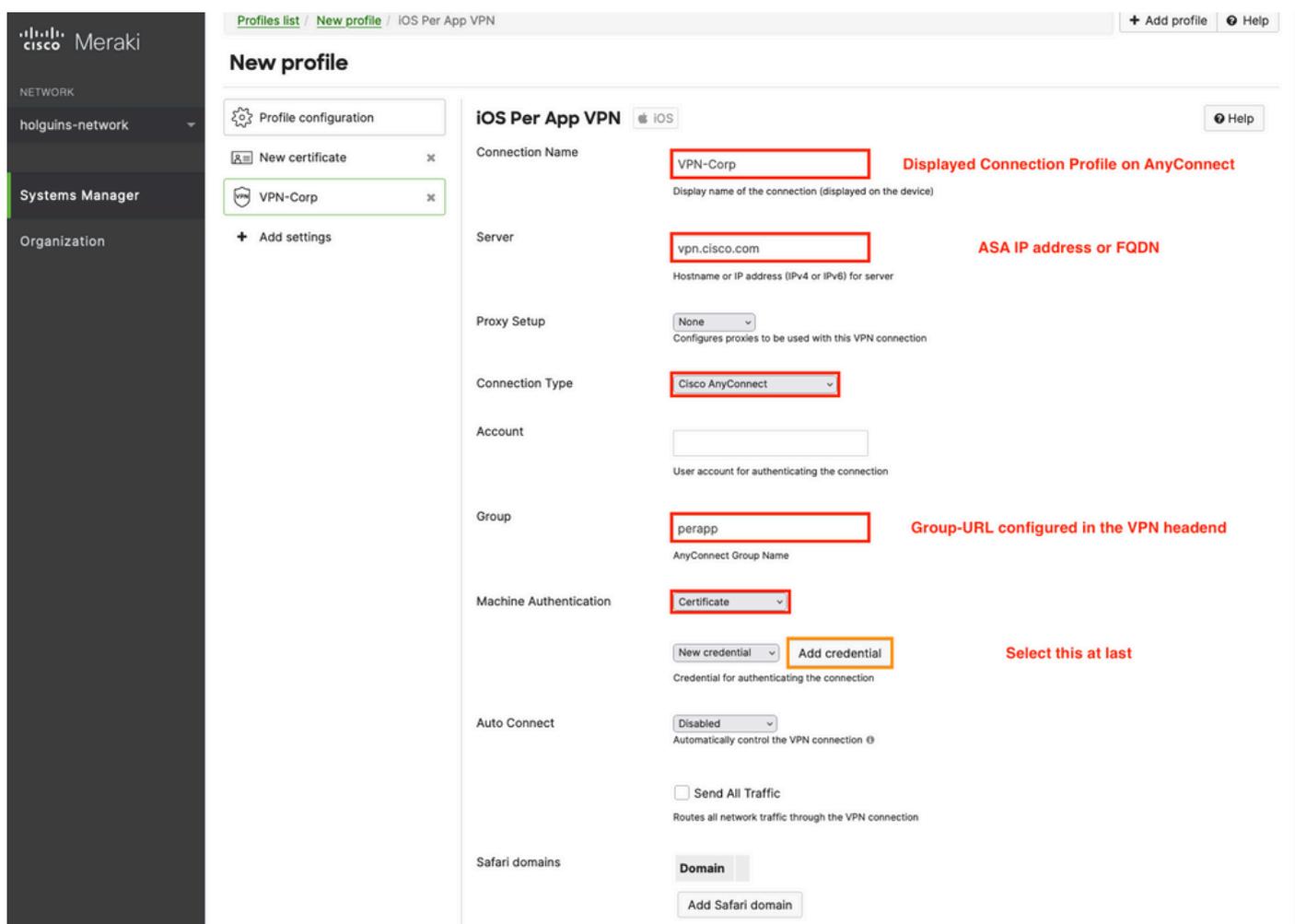
3.5. [Add settings] を選択し、プロファイルのタイプを[iOS Per App VPN] でフィルタリングして、次に示すオプションを選択します。



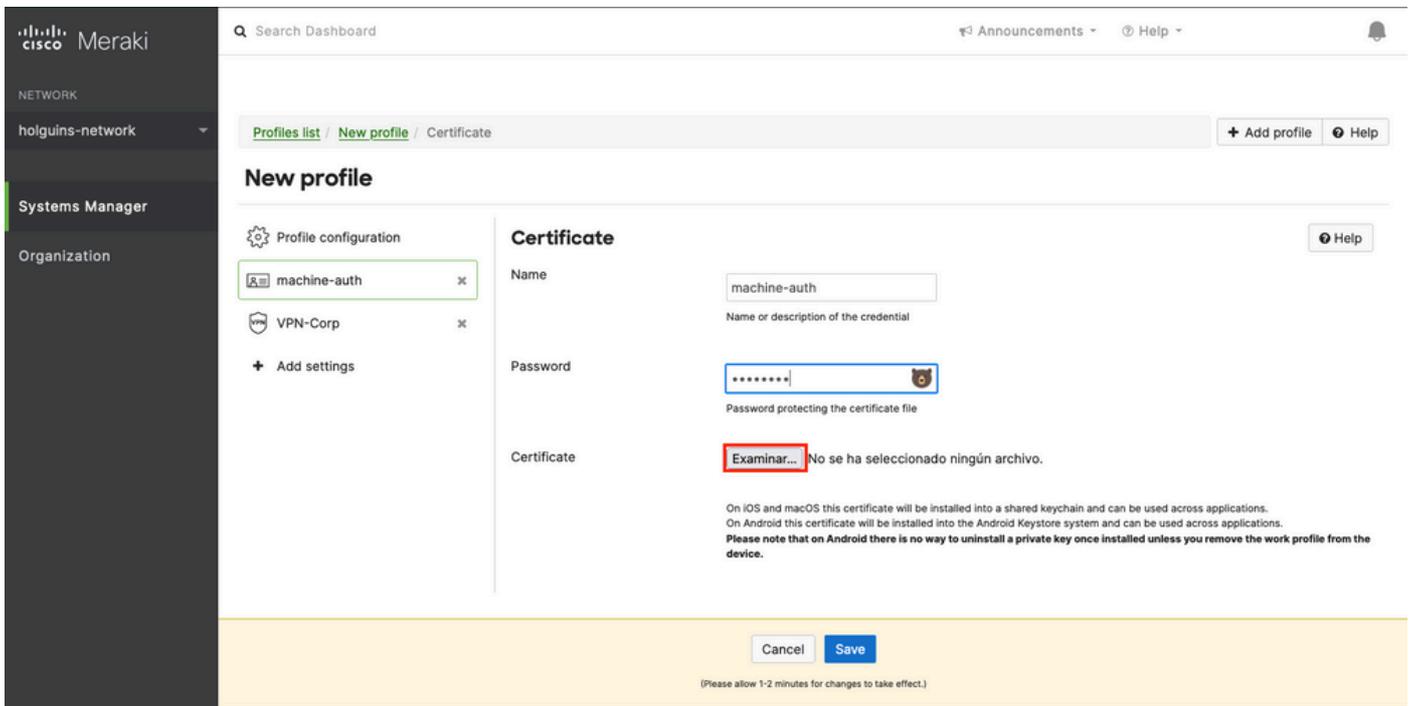
3.6. メニューが表示されたら、次の例に基づいて接続情報を書き込みます。

Systems Managerでは、これらの接続に対して、SCEPと手動登録という2つの証明書登録がサポートされています。この例では、手動登録が使用されています。

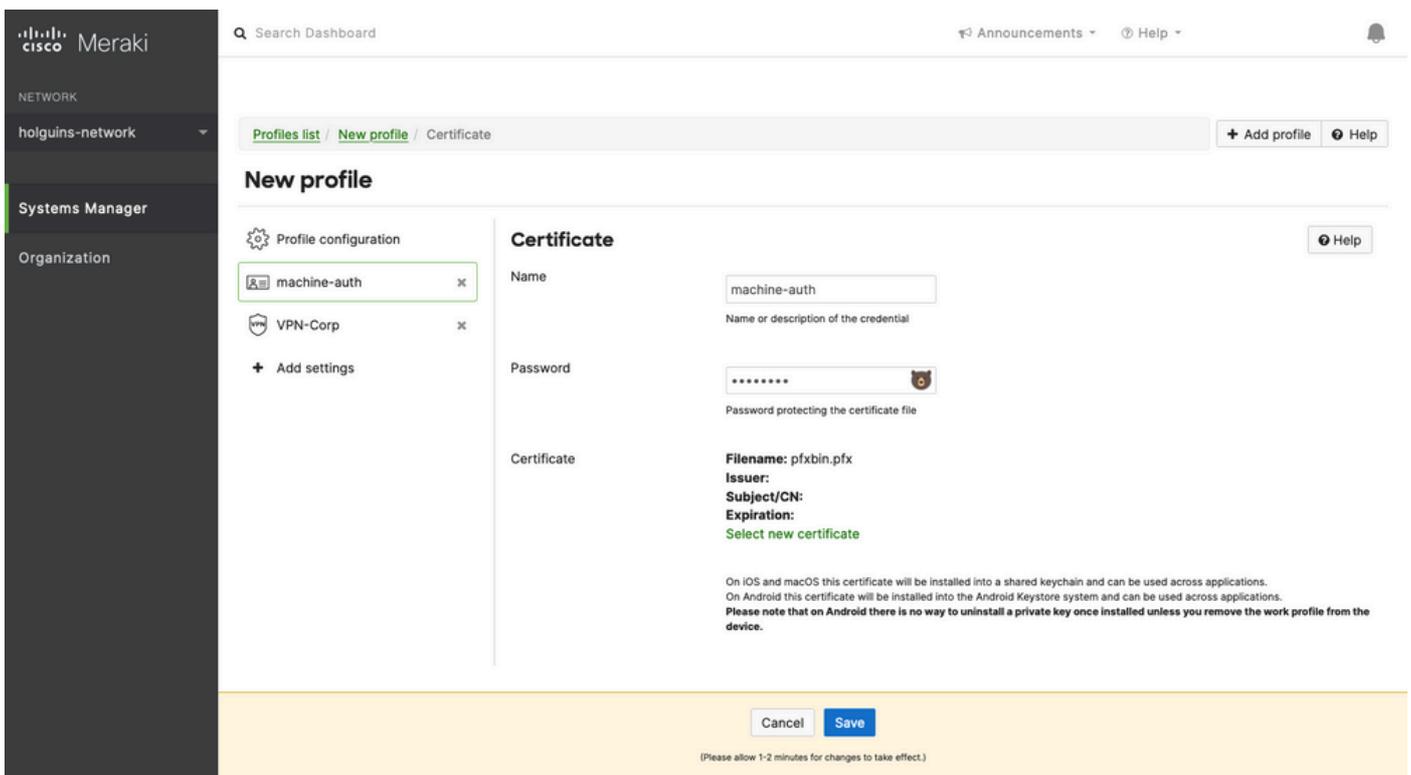
注：このオプションでは証明書ファイルを追加するための新しいメニューが表示されるため、テキストボックスに入力したら[Add credential]を選択します。



3.7. [クレデンシャルの追加(Add credential)] をクリックして[証明書(Certificate)]メニューにリダイレクトされたら、証明書の[名前(Name)]を入力し、コンピュータを参照して、.pfxファイル(暗号化された証明書ファイル)を保護する[パスワード>Password]を探します。



3.8.証明書が選択されると、証明書ファイル名が表示されます。



3.9.証明書を選択したら、以前使用していたVPNプロファイルに移動し、最近インポートしたクレデンシャルを選択し、トンネリングされたアプリを選択します（この場合はFirefox）。

これが完了したら、**Save**をクリックします。

The screenshot shows the Meraki Systems Manager interface for configuring an iOS Per App VPN profile. The left sidebar shows the navigation menu with 'Systems Manager' selected. The main content area is titled 'iOS Per App VPN' and includes the following fields:

- Profile configuration:** A list of profiles with 'machine-auth' highlighted in a red box.
- Connection Name:** VPN-Corp
- Server:** vpn.cisco.com
- Proxy Setup:** None
- Connection Type:** Cisco AnyConnect
- Account:** (empty)
- Group:** perapp
- Machine Authentication:** Certificate
- Machine Authentication:** machine-auth (dropdown) and Add credential (button) are highlighted in a red box.
- Auto Connect:** Disabled
- Send All Traffic:** (unchecked)
- Safari domains:** Domain (tab) and Add Safari domain (button)
- Apps:** A list of apps with 'Firefox: Private, Safe Browser' highlighted in a red box.

3.10. プロファイルがターゲットデバイスにインストールされていることを確認する。

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

2 results

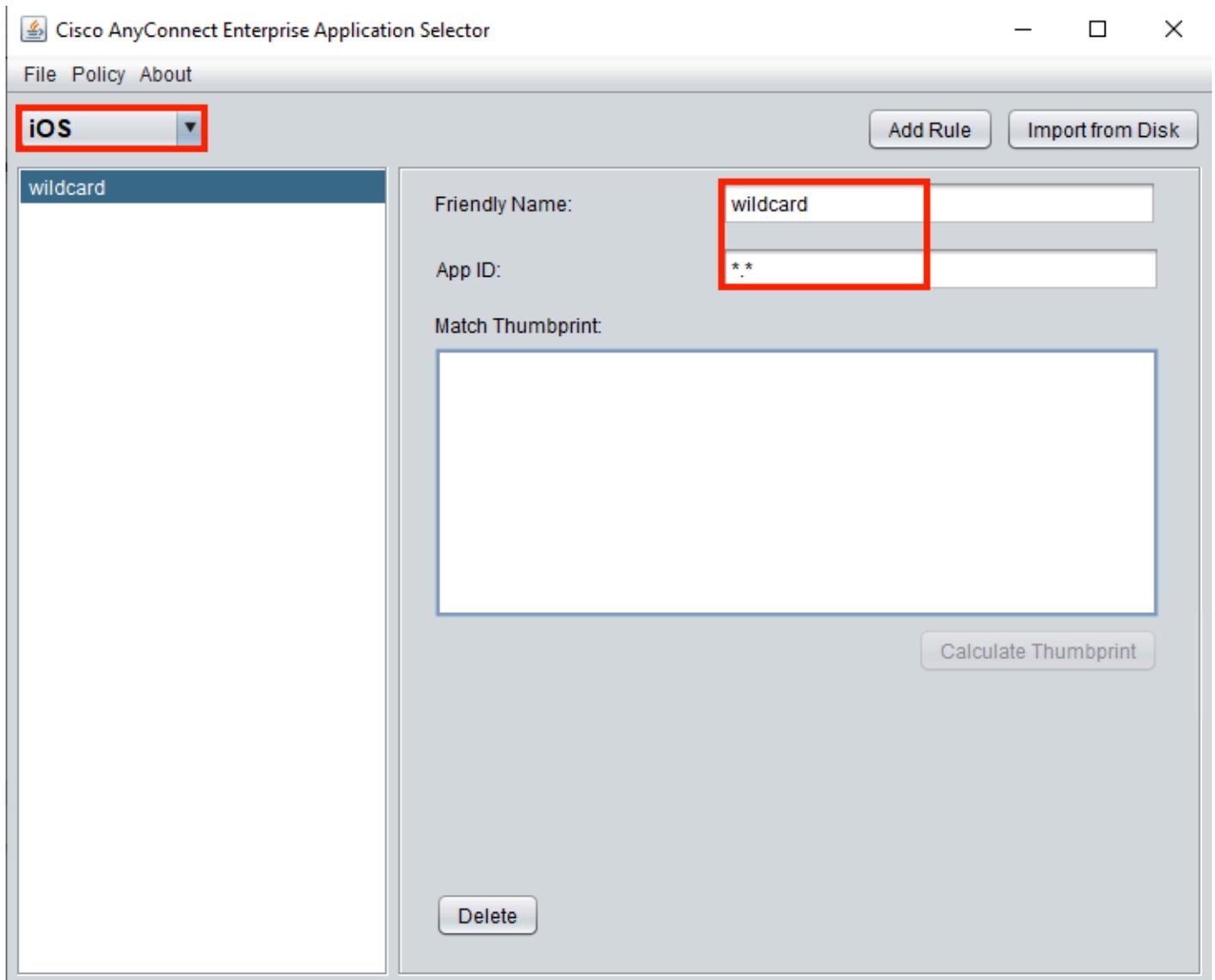
ステップ 4 : アプリケーションセレクタの設定

4.1. シスコのWebサイト

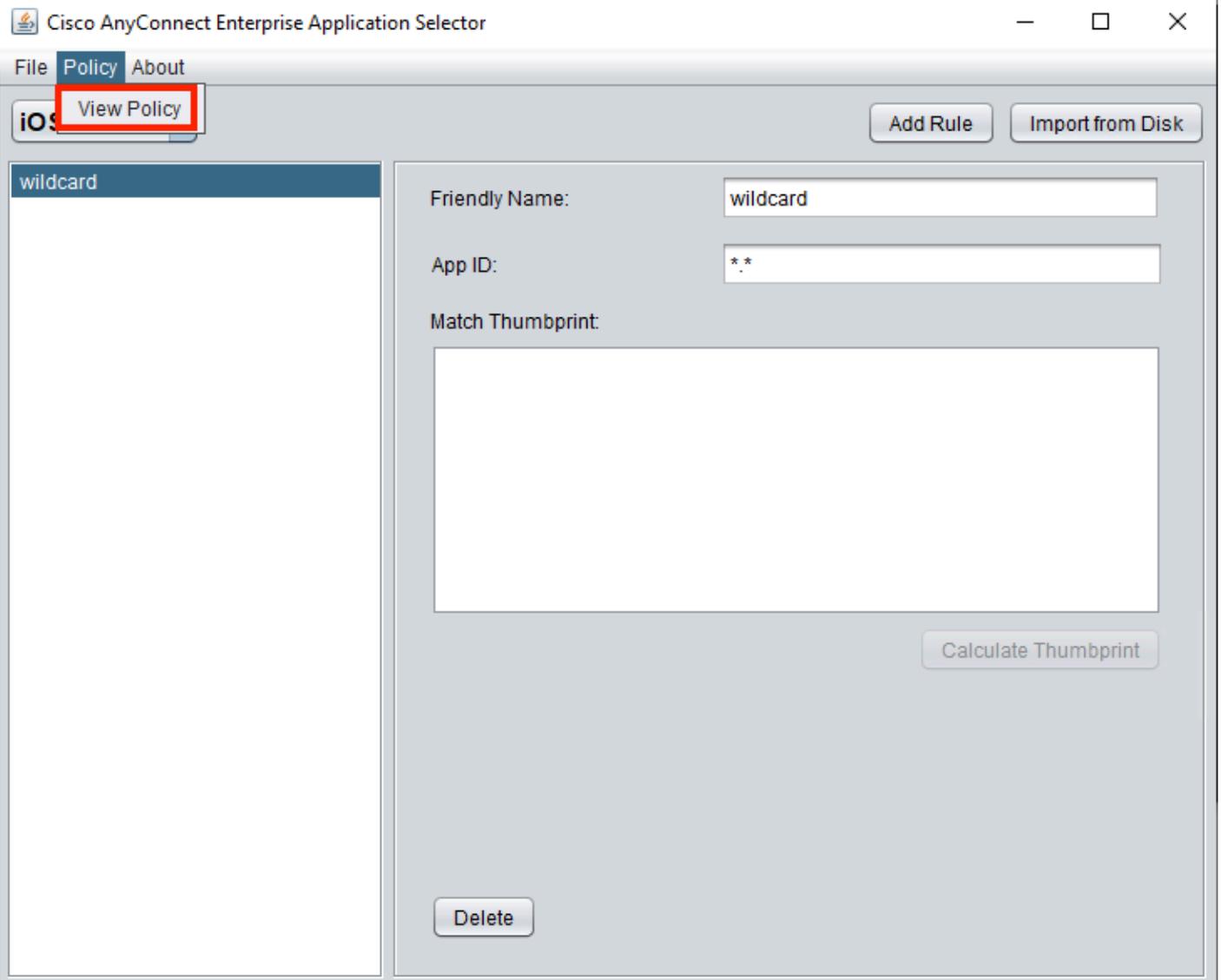
<https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0> から app selector をダウンロード [する](#)

注意: Windows マシンでアプリケーションを実行してください。表示される結果は、MacOS デバイスでツールを使用した場合に予想されるものではありません。

4.2. Java アプリケーションを開きます。ドロップダウンメニューから iOS を選択し、わかりやすい名前を追加して、App ID に *.* と入力します。



4.3. [Policy] に移動し、[View Policy] を選択します



4.4.表示された文字列をコピーする。(これは後でVPNヘッドエンド設定で使用されます)。

```
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSgIYk  
FBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB
```

OK

ステップ 5 : アプリケーションごとのASAのVPN設定例

```
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
```

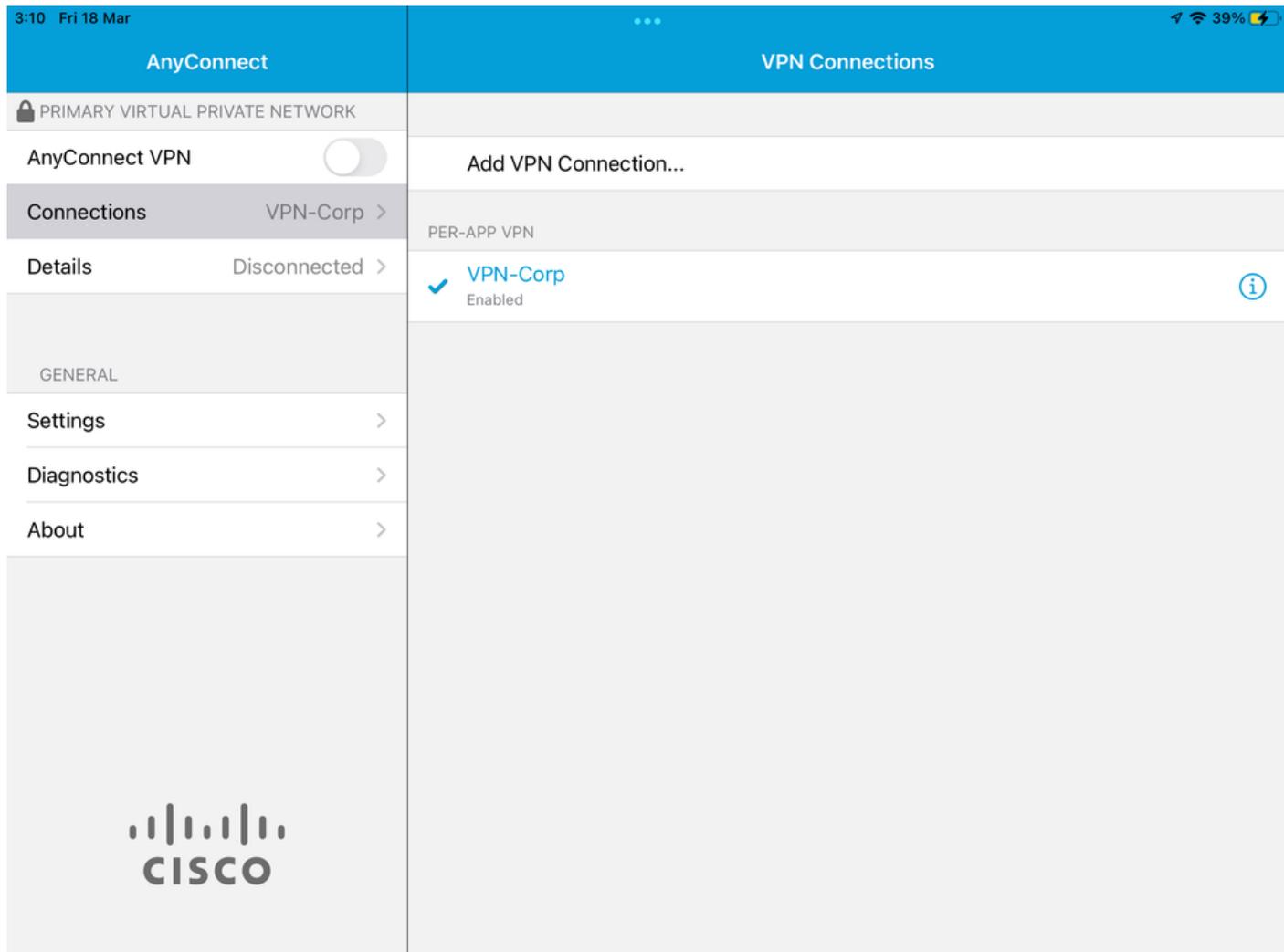
group-url https://vpn.cisco.com/perapp enable

確認

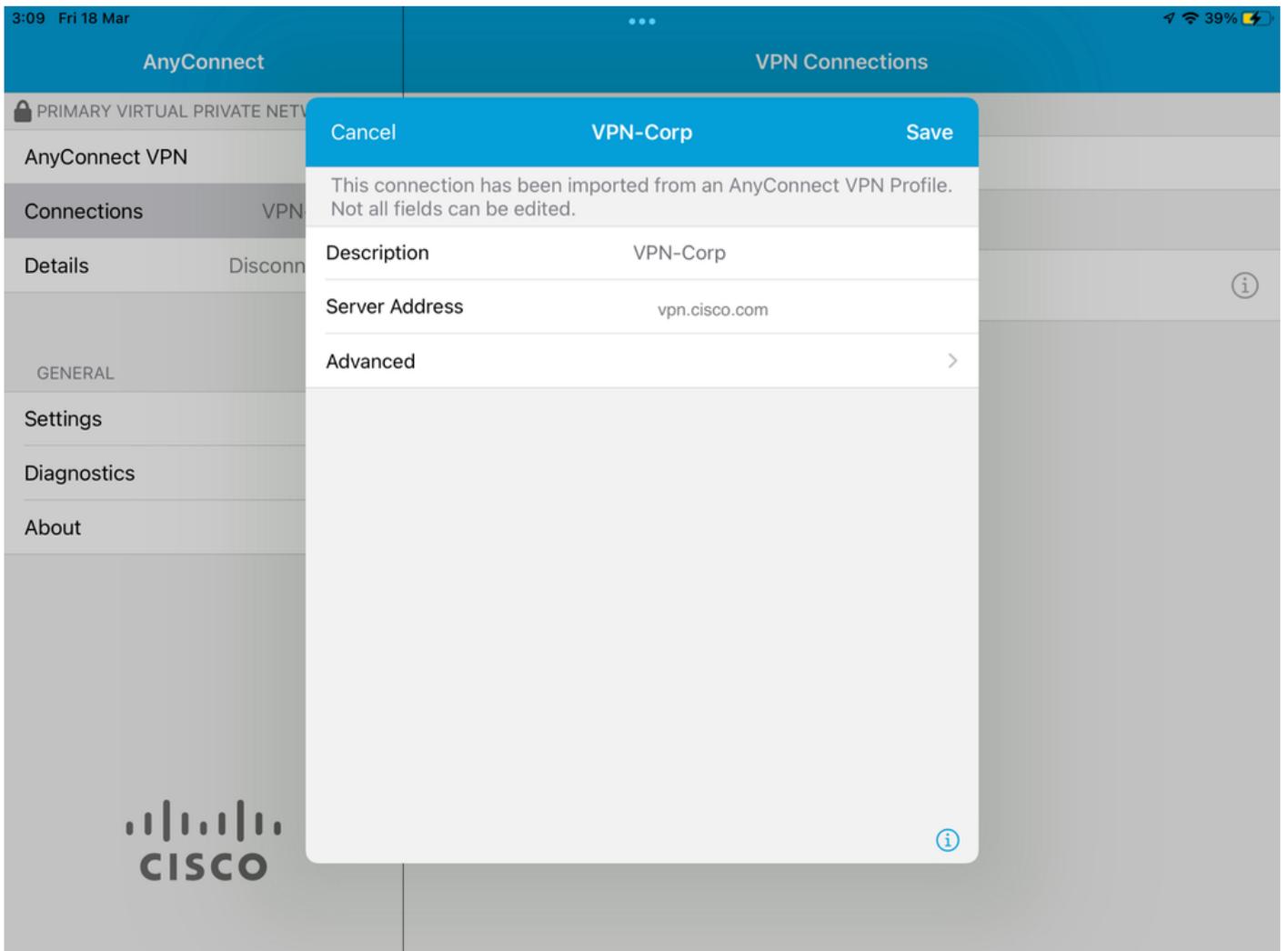
6. AnyConnectアプリケーションでのプロファイルインストールの確認

6.1. AnyConnectアプリケーションを開き、左側のペインで**Connections**を選択します。PerApp VPNプロファイルは、**PER-APP VPN**という名前の新しいセクションに表示される必要があります。

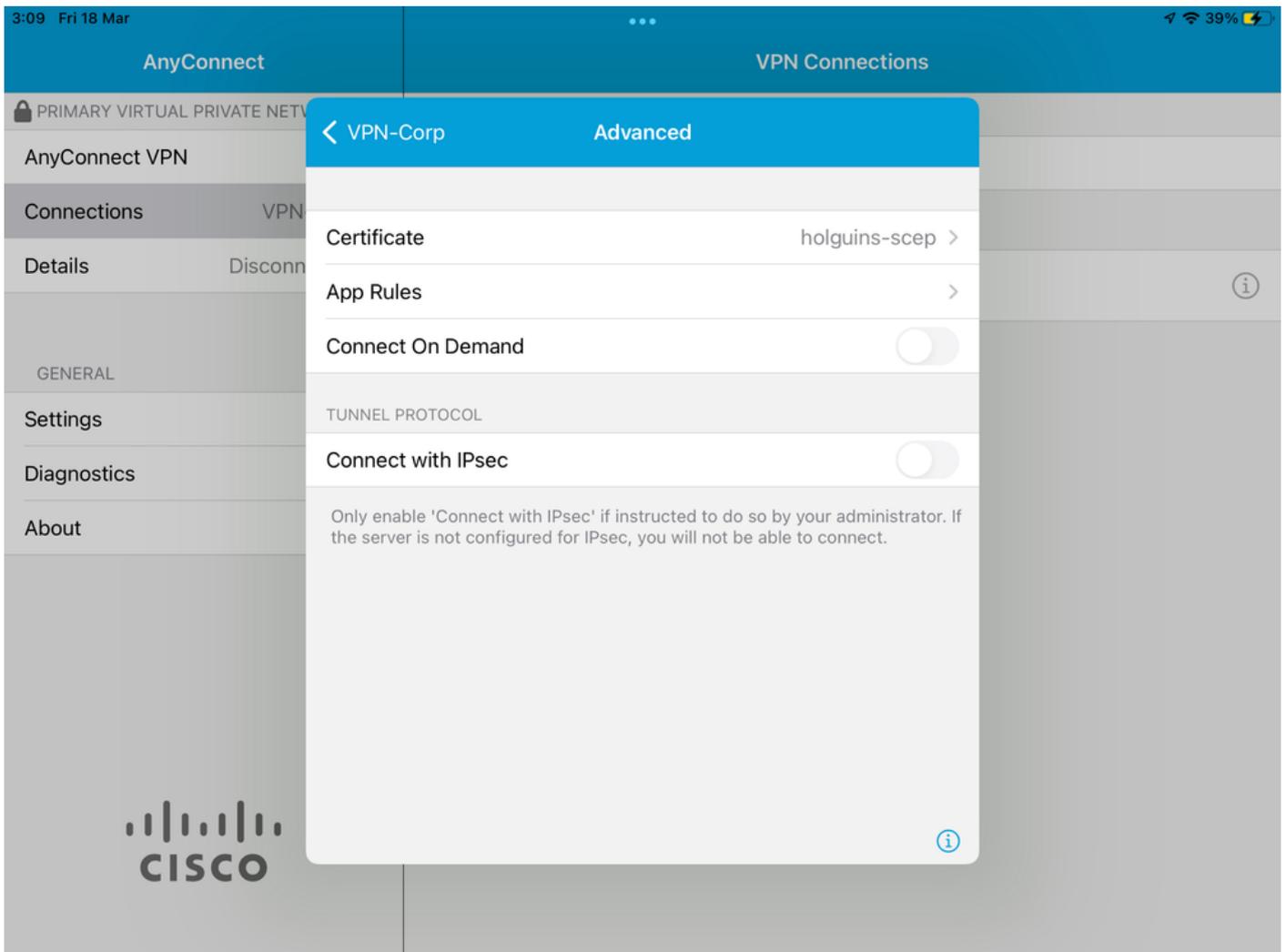
iを選択すると、詳細設定が表示されます。



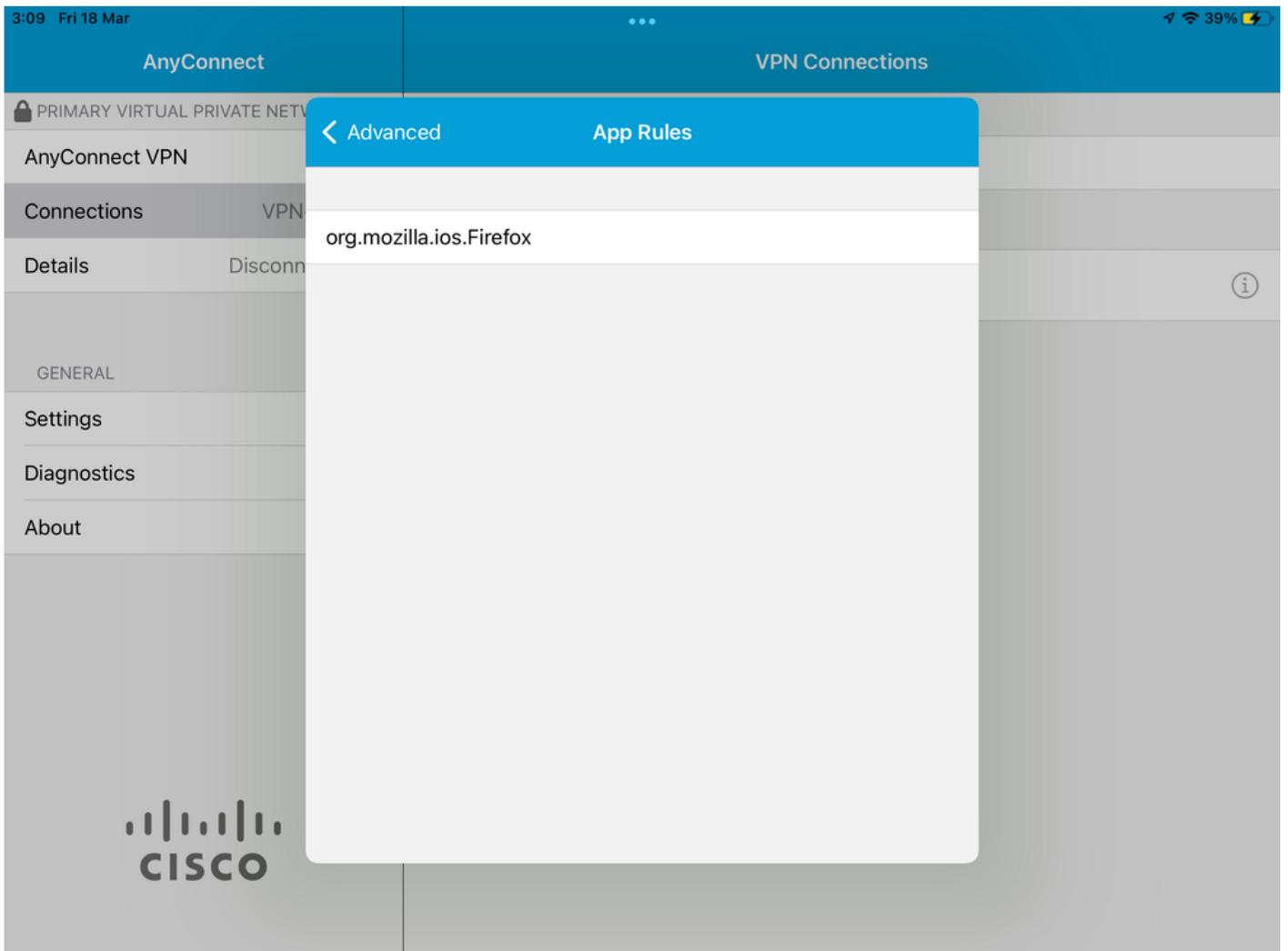
6.2. [Advanced] オプションを選択します。



6.3. [App Rules] オプションを選択します。



6.4.最後に、App Ruleがインストールされていることを確認します。(このドキュメントではMozillaが望ましいトンネル化されたAppであるため、Appのインストールは成功しました)。



トラブルシューティング

現在のところ、このドキュメントに固有のトラブルシューティング手順はありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。