Configure Anyconnect PerApp VPN for iOS with Meraki System Manager

Contents

Introduction

This document describes how to configure PerApp VPN on Apple iOS devices managed by Meraki Mobile Device Manager (MDM), System Manager (SM).

Prerequisites

Requirements

- AnyConnect v4.0 Plus or Apex license.
- ASA 9.3.1 or later to support Per App VPN.
- Cisco Enterprise Application Selector tool available on Cisco.com

Components Used

The information in this document is based on these software versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

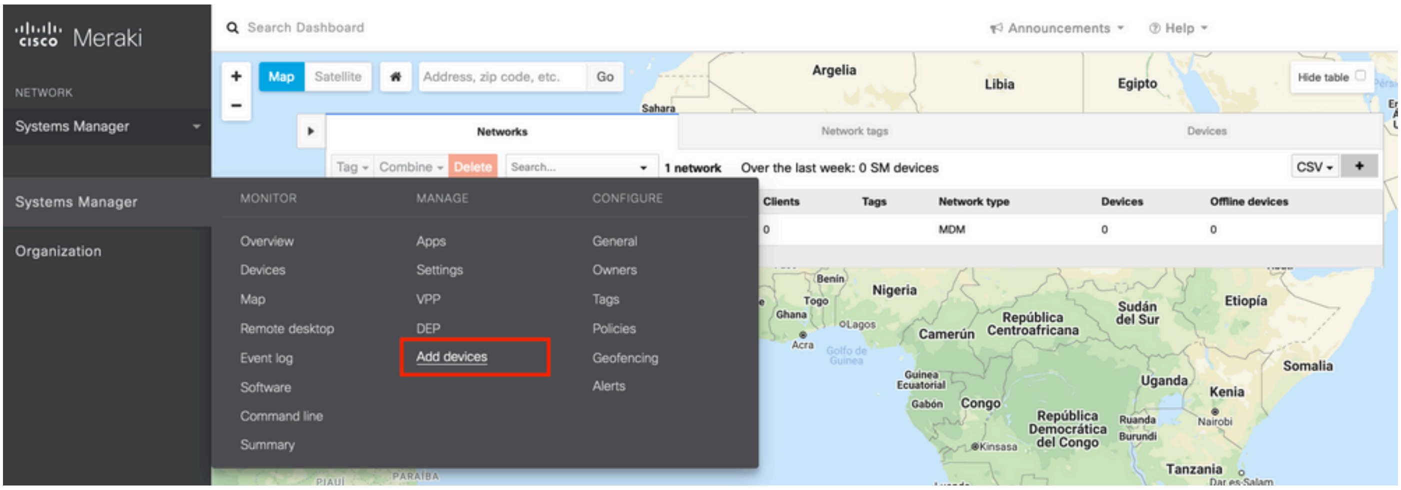
This document does not include the listed processes:

- SCEP CA Configuration on Systems Manager for client certificate generation
- PKCS12 client certificate generation for the iOS clients

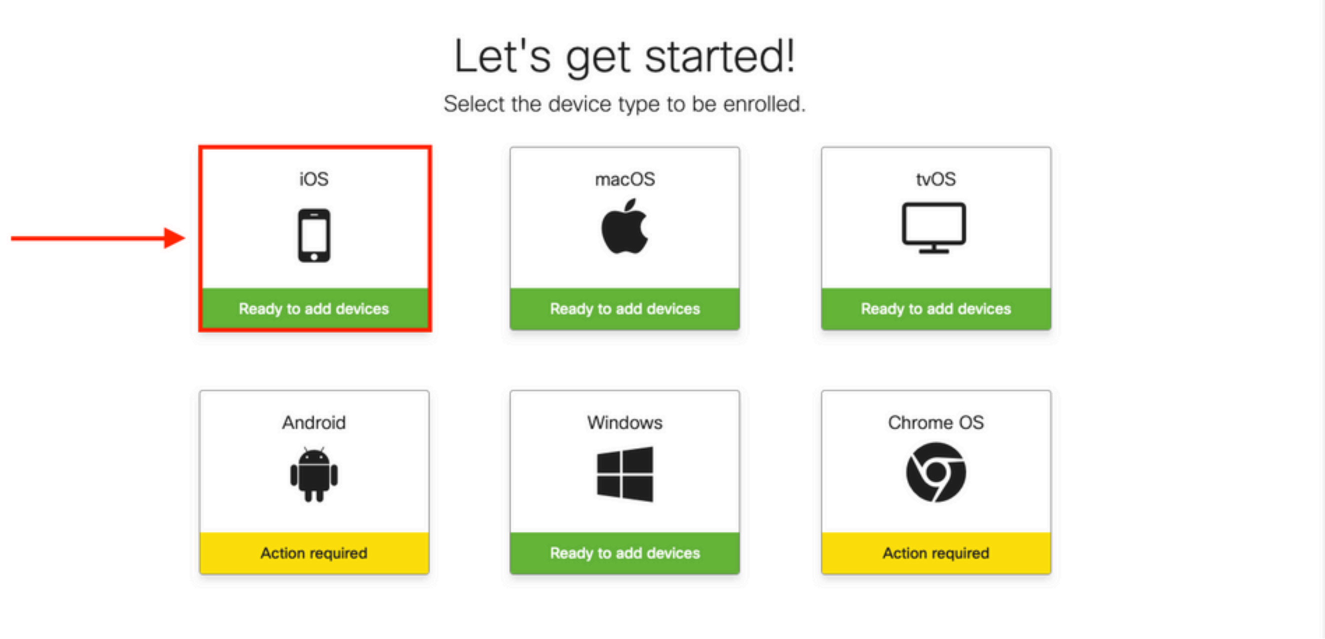
Configure

Step 1. Register iOS Device to Meraki Systems Manager

1.1. Navigate to **Systems Manager > Add Devices**

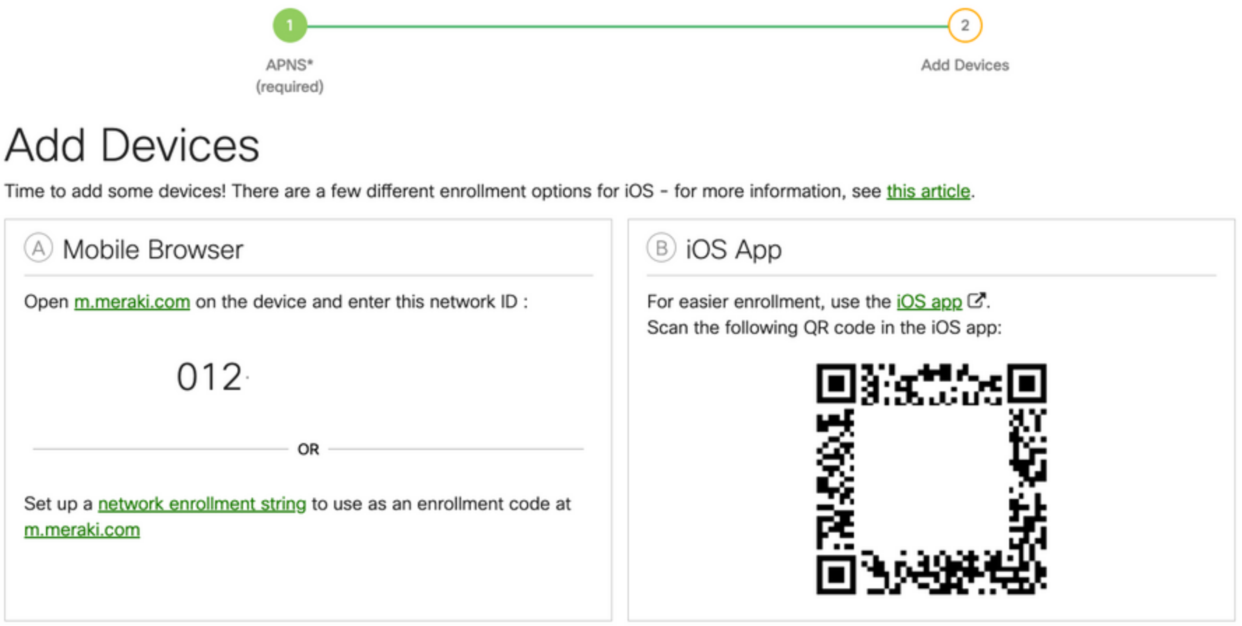


1.2. Click on the **iOS** option to start the enrollment.


Let's get started!

Select the device type to be enrolled.

1.3. Enroll the device via internet browser or scan the QR code with the camera. In this document, the camera was used for the enrollment process.



Add Devices

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

Ⓐ Mobile Browser

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

012[redacted]

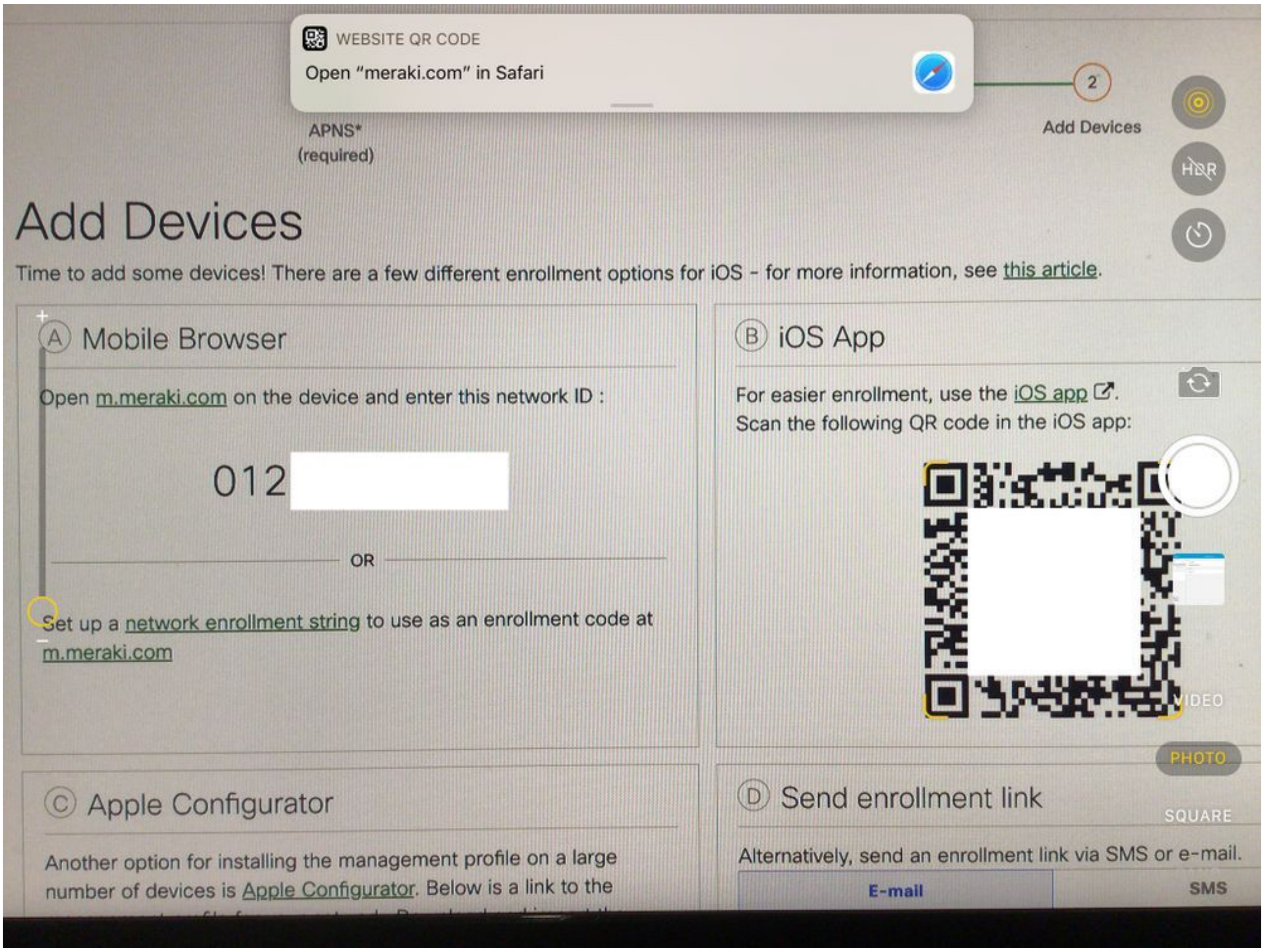
OR

Set up a network enrollment string to use as an enrollment code at m.meraki.com

Ⓑ iOS App

For easier enrollment, use the iOS app.
Scan the following QR code in the iOS app:

1.4. When the QR code is recognized by the camera, select the **Open "meraki.com" in Safari** notification that pops up.



Open “meraki.com” in Safari

Add Devices

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

Ⓐ Mobile Browser

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

012[redacted]

OR

Set up a network enrollment string to use as an enrollment code at m.meraki.com

Ⓑ iOS App

For easier enrollment, use the iOS app.
Scan the following QR code in the iOS app:

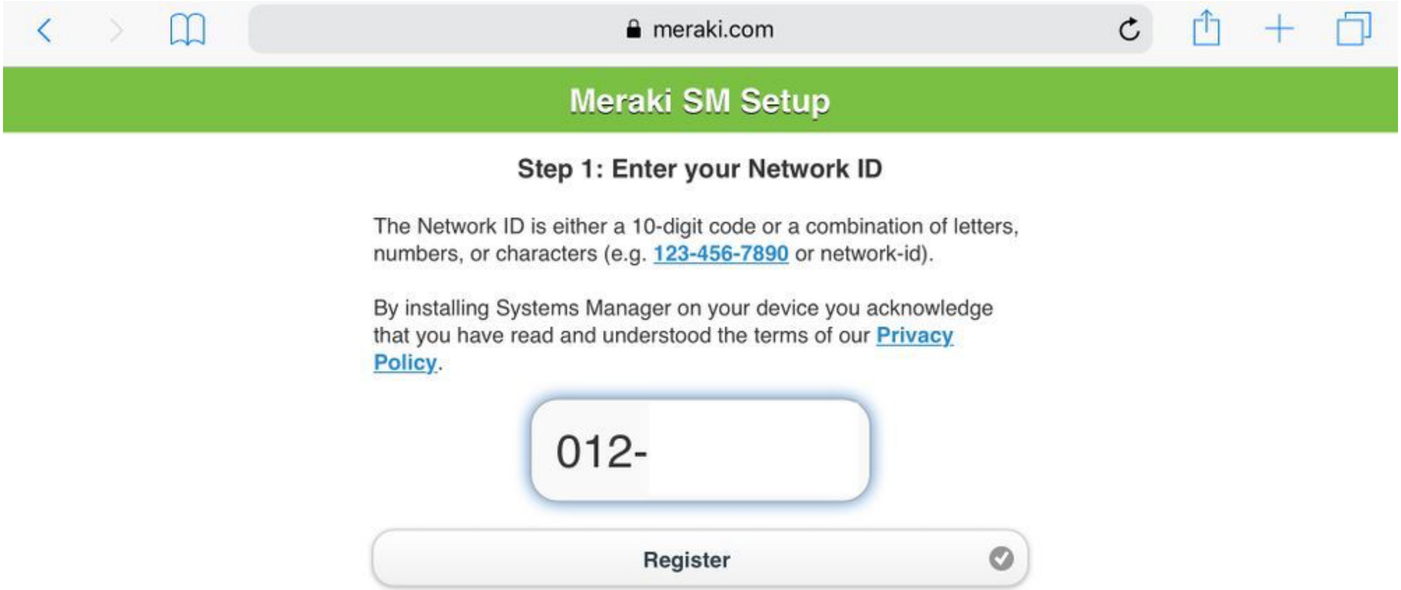
Ⓒ Apple Configurator

Another option for installing the management profile on a large number of devices is Apple Configurator. Below is a link to the

Ⓓ Send enrollment link

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

1.5. When prompted, select **Register**.


meraki.com

Meraki SM Setup

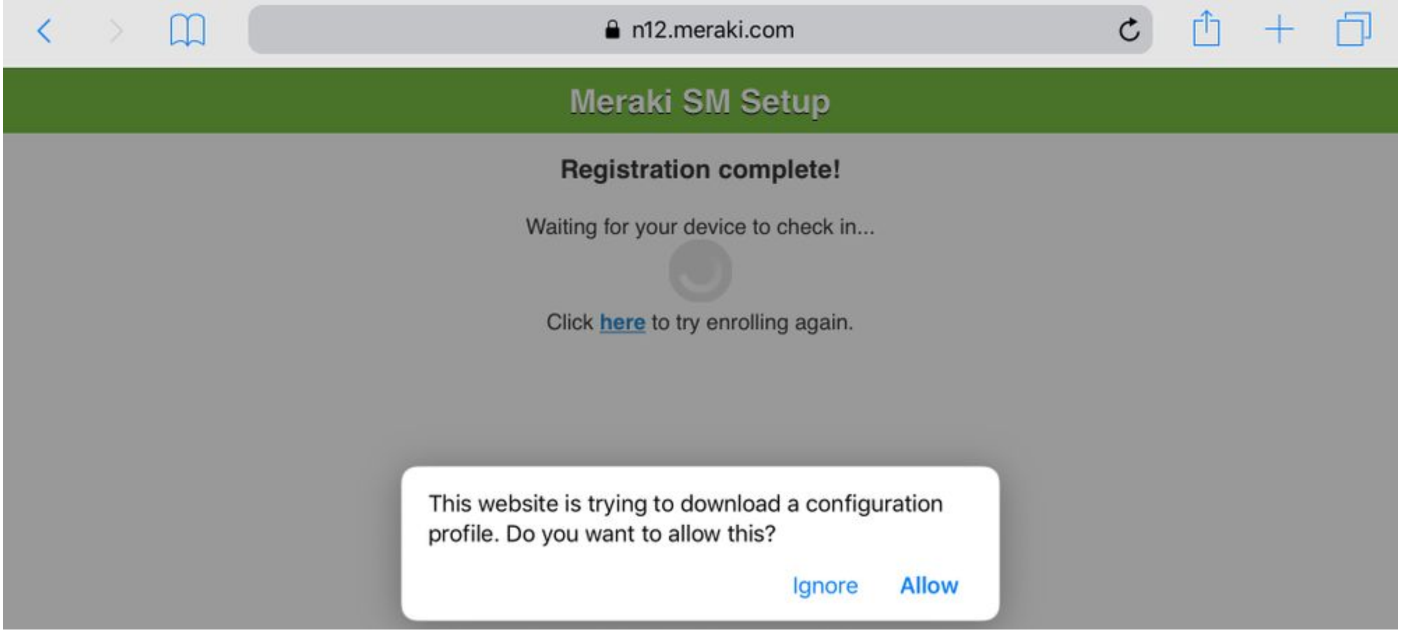
Step 1: Enter your Network ID

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.

012-

1.6. Select **Allow** in order to allow the device to download the MDM profile.


n12.meraki.com

Meraki SM Setup

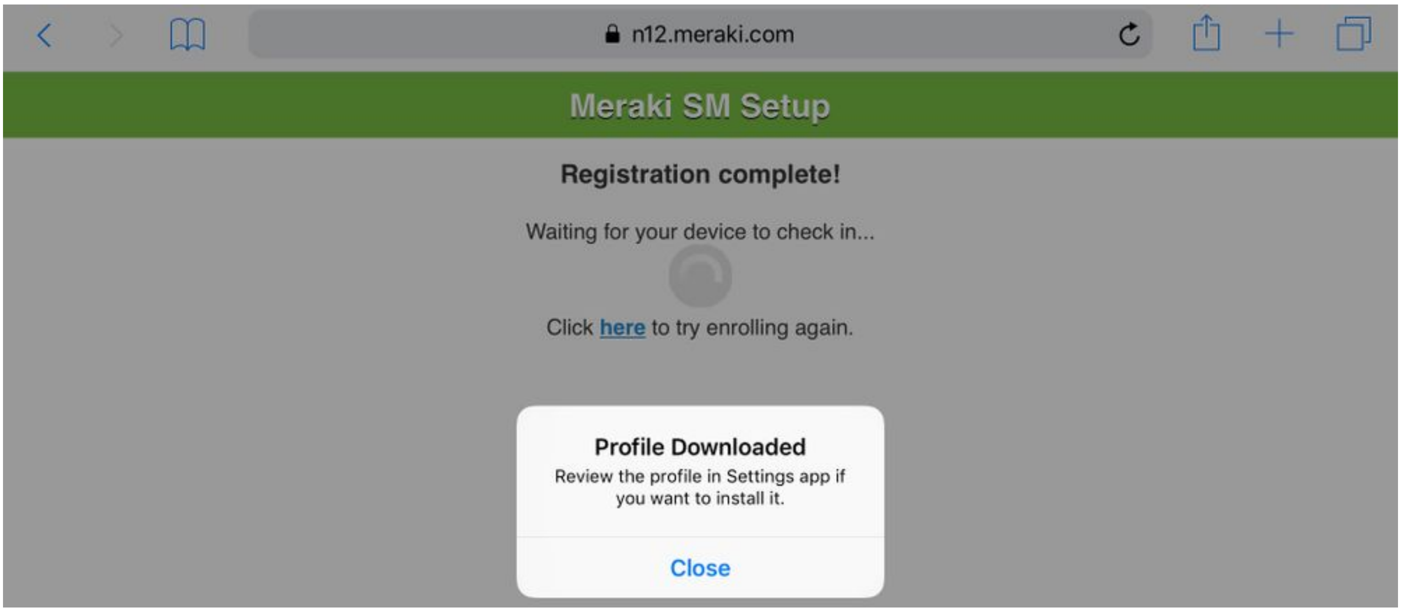
Registration complete!

Waiting for your device to check in...

Click here to try enrolling again.

This website is trying to download a configuration profile. Do you want to allow this?

1.7. Select **Close** to complete the download.


n12.meraki.com

Meraki SM Setup

Registration complete!

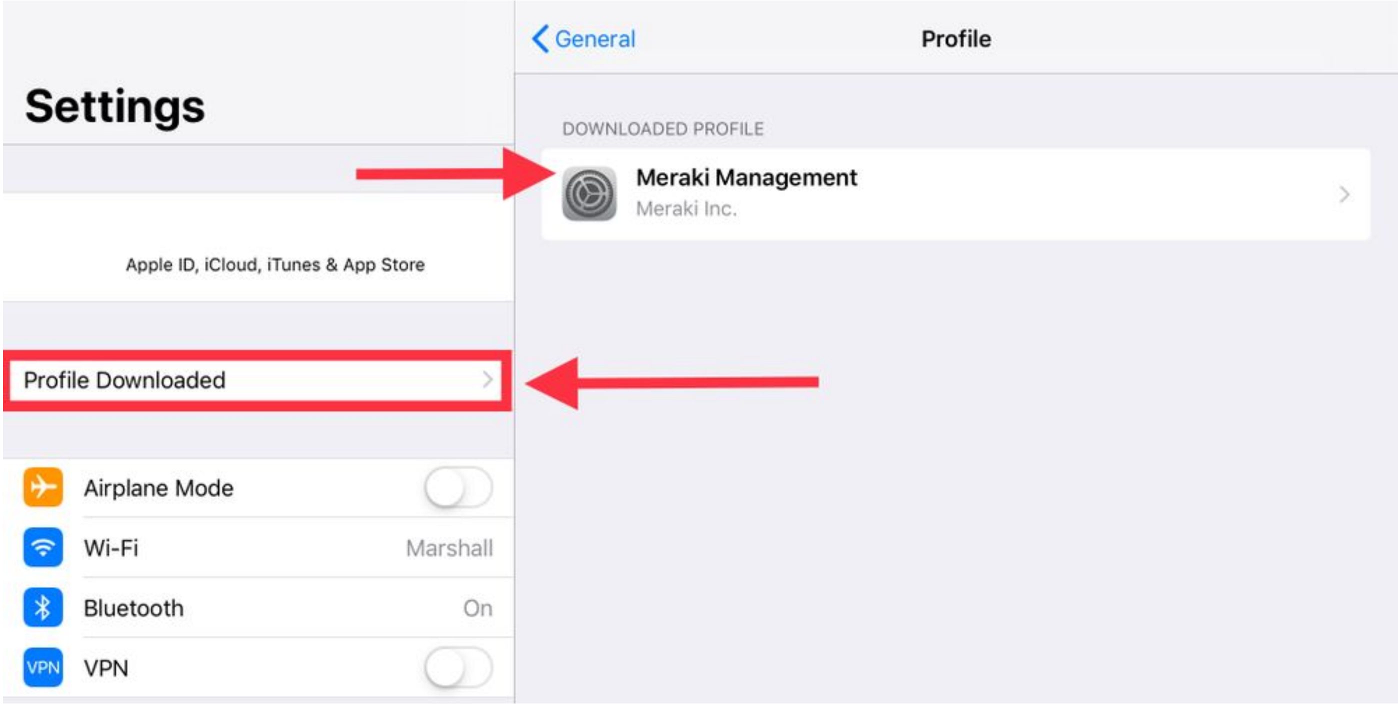
Waiting for your device to check in...

Click here to try enrolling again.

Profile Downloaded

Review the profile in Settings app if you want to install it.

1.8. Navigate to the iOS Settings App and locate the **Profile Downloaded** option in the left pane and select the **Meraki Management** section.



Settings

Apple ID, iCloud, iTunes & App Store

Profile Downloaded

Airplane Mode

Wi-Fi Marshall

Bluetooth On

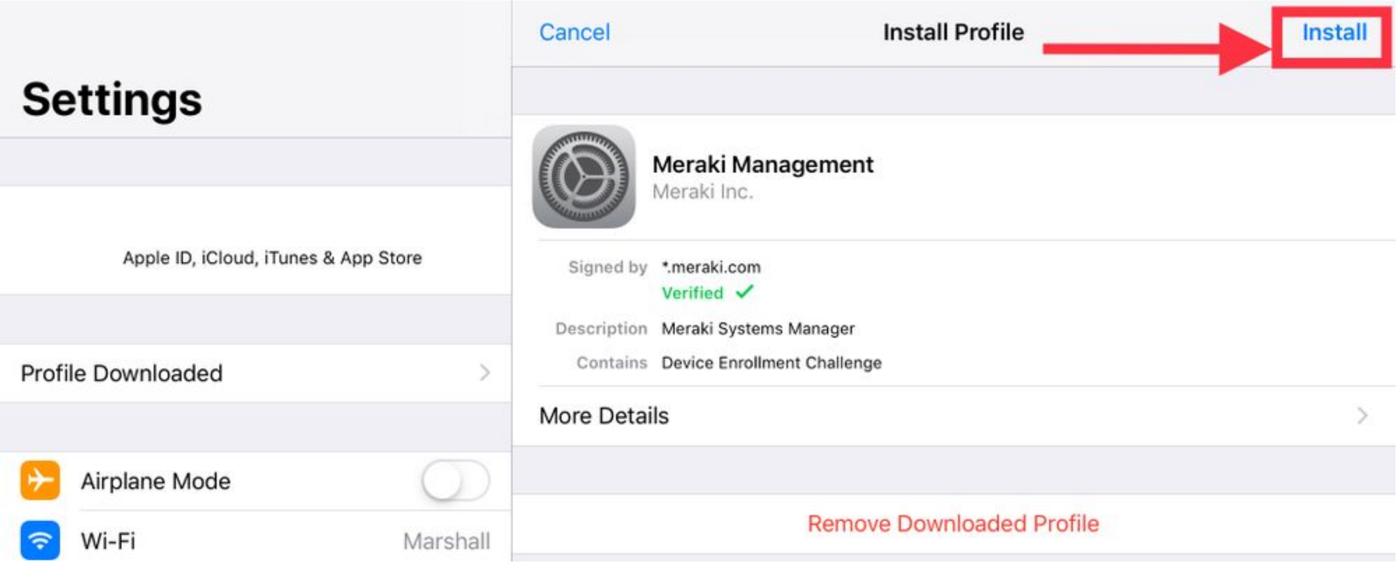
VPN

Profile

DOWNLOADED PROFILE

Meraki Management
Meraki Inc.

1.9. Select the **Install** option to install the MDM profile.



Settings

Apple ID, iCloud, iTunes & App Store

Profile Downloaded

Airplane Mode

Wi-Fi Marshall

Install Profile

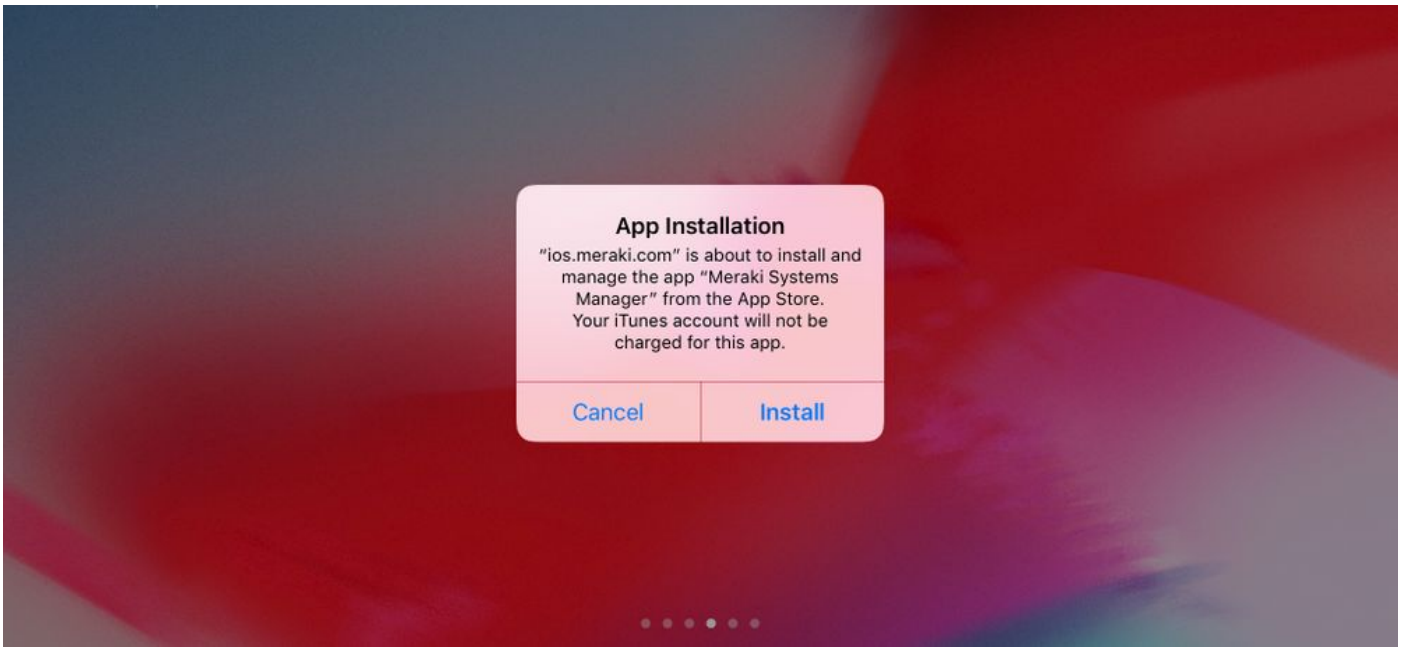
Meraki Management
Meraki Inc.

Signed by *.meraki.com
Verified ✓

Description Meraki Systems Manager

Contains Device Enrollment Challenge

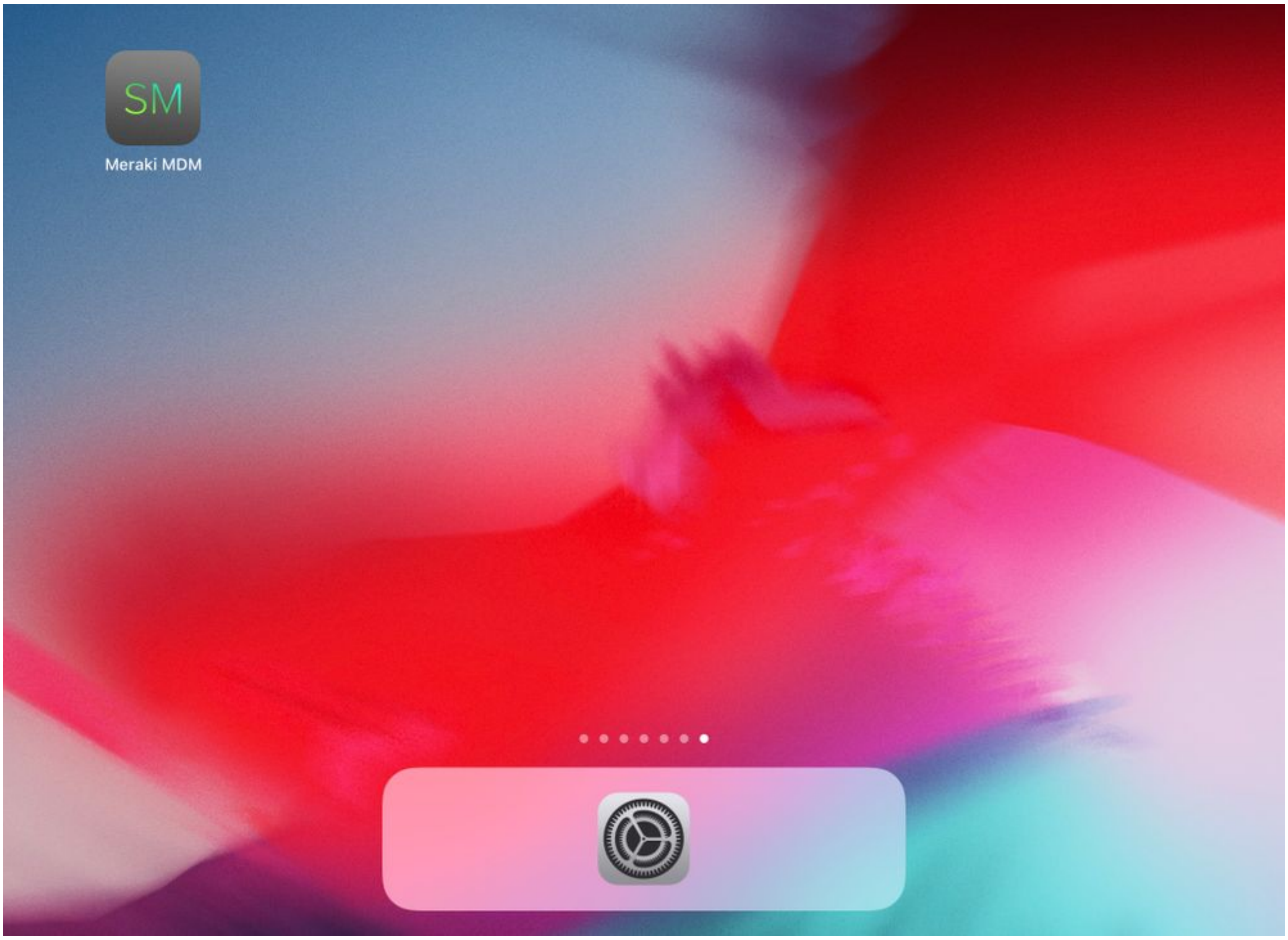
1.10. You must grant the access to **Install** the SM application.



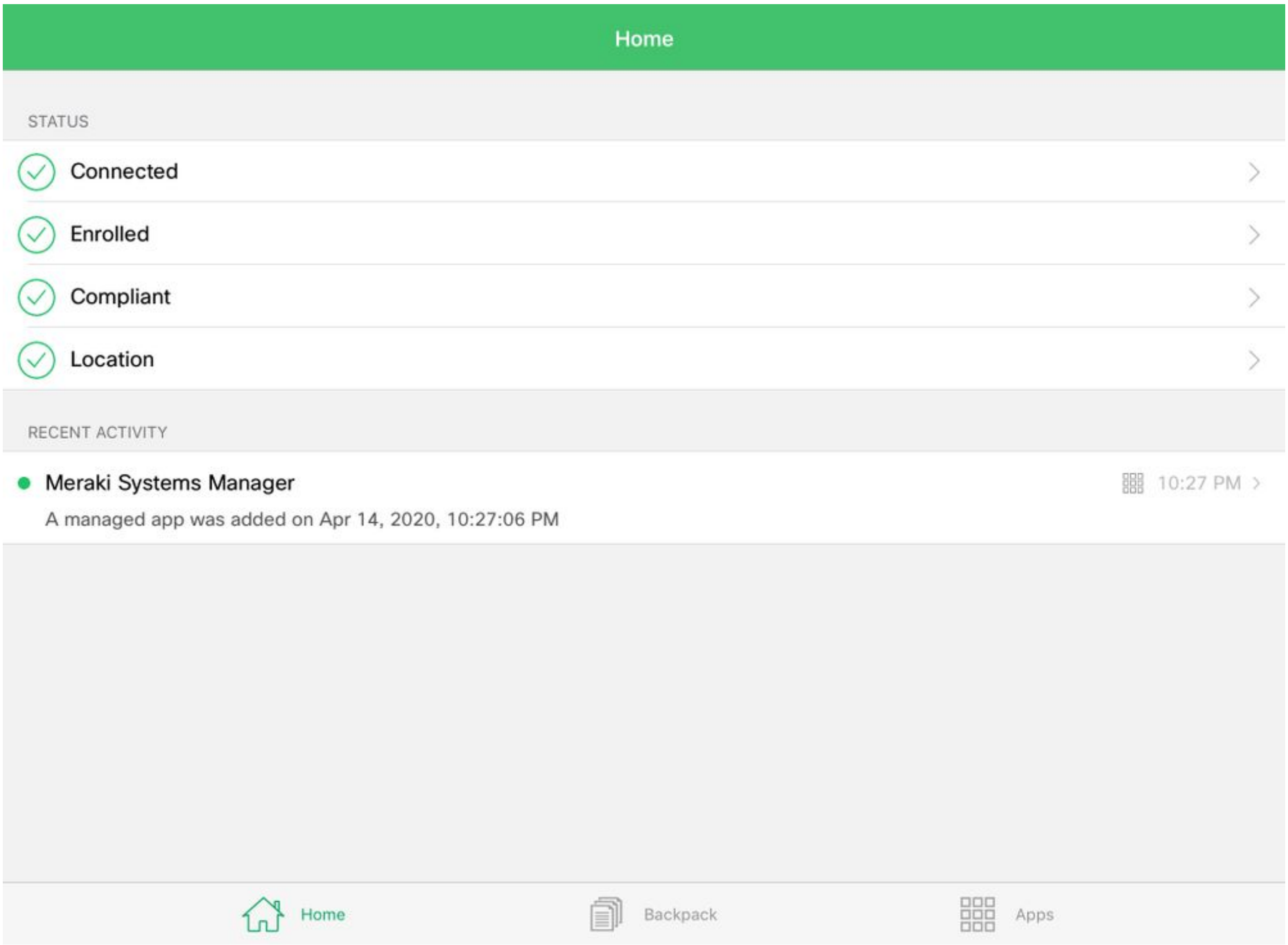
App Installation

"ios.meraki.com" is about to install and manage the app "Meraki Systems Manager" from the App Store. Your iTunes account will not be charged for this app.

1.11. Open the recently downloaded application called **Meraki MDM** located in the home screen.



1.12. Verify all the statuses have a green tick that confirms the enrollment is in complete.



Connected

Enrolled

Compliant

Location

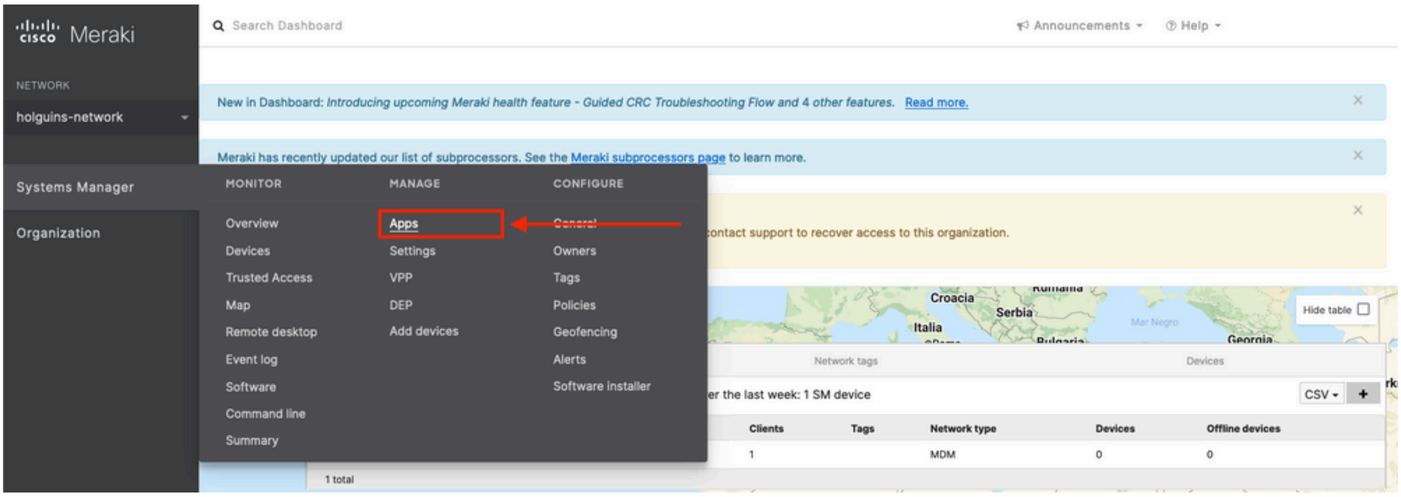
Meraki Systems Manager 10:27 PM

A managed app was added on Apr 14, 2020, 10:27:06 PM

Step 2. Setup Managed Apps

In order to setup the Tunneled Apps for PerApp later in this document, you need to manage those same applications via SM. In this configuration example, Firefox is intended to be tunneled via Per App, hence it is added to the managed Apps.

2.1. Navigate to **Systems Manager > Manage > Apps** in order to add the managed apps.



New in Dashboard: *Introducing upcoming Meraki health feature - Guided CRC Troubleshooting Flow and 4 other features.* Read more.

Meraki has recently updated our list of subprocessors. See the Meraki subprocessors page to learn more.

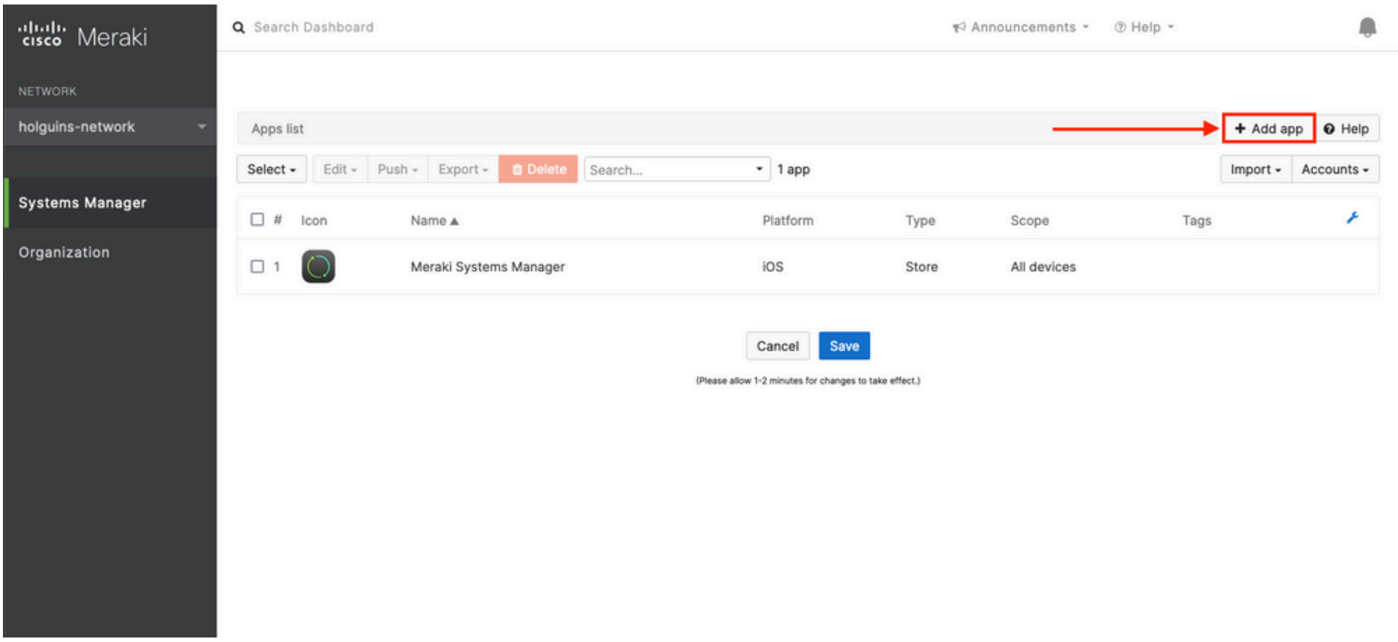
contact support to recover access to this organization.

er the last week: 1 SM device

Clients	Tags	Network type	Devices	Offline devices
1		MDM	0	0

1 total

2.2. Select the **Add app** option.



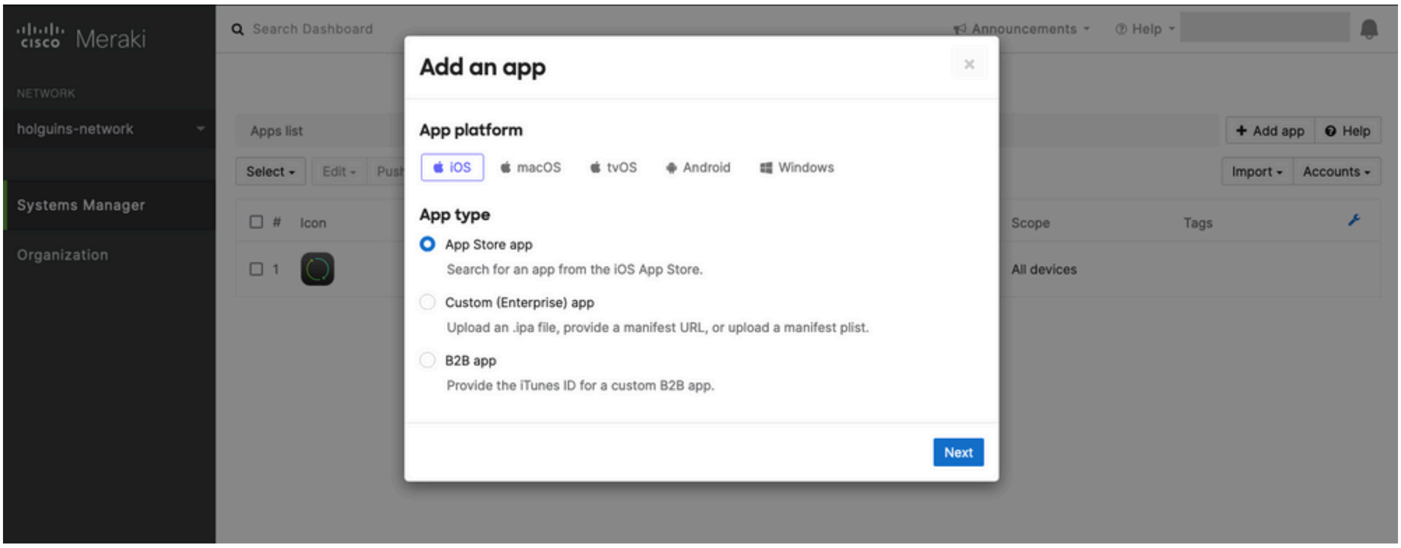
1 app

□ #	Icon	Name ▲	Platform	Type	Scope	Tags
□ 1		Meraki Systems Manager	iOS	Store	All devices	

(Please allow 1-2 minutes for changes to take effect.)

2.3. Select the type of application (App Store app, Custom, B2B) based on where the app is stored. Select **Next** once it is selected.

In this example the app is stored publicly in the App Store.



Add an app

App platform

iOS | macOS | tvOS | Android | Windows

App type

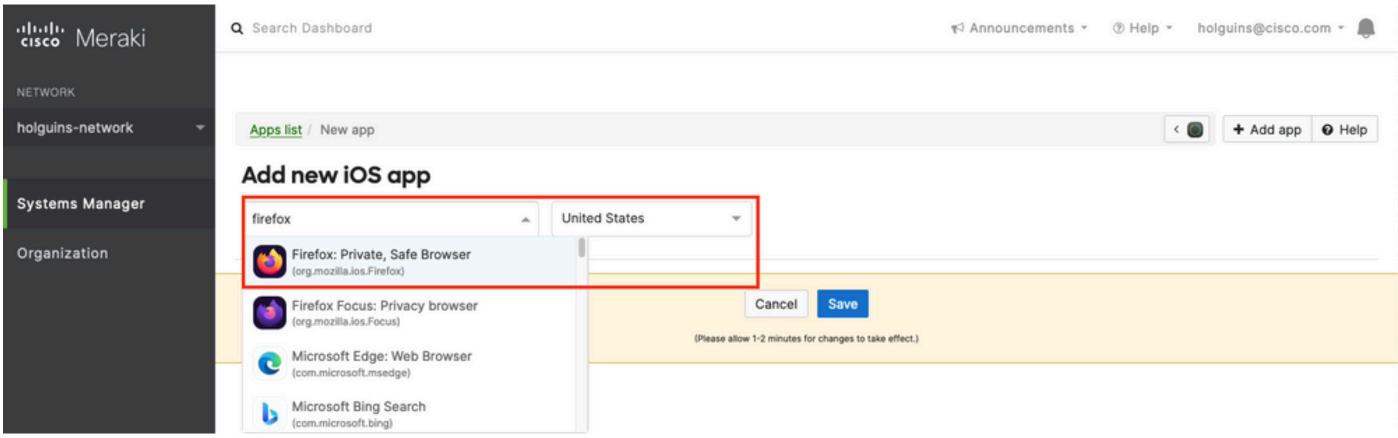
● App Store app
Search for an app from the iOS App Store.

○ Custom (Enterprise) app
Upload an .ipa file, provide a manifest URL, or upload a manifest plist.

○ B2B app
Provide the iTunes ID for a custom B2B app.

2.4. When prompted, search for the desired application and select the region from where the application is downloaded from. Select **Save** once the app is selected.

> **Note**: If the country does not match the Apple account's region, the user may experience problems with the application.



Add new iOS app

firefox | United States

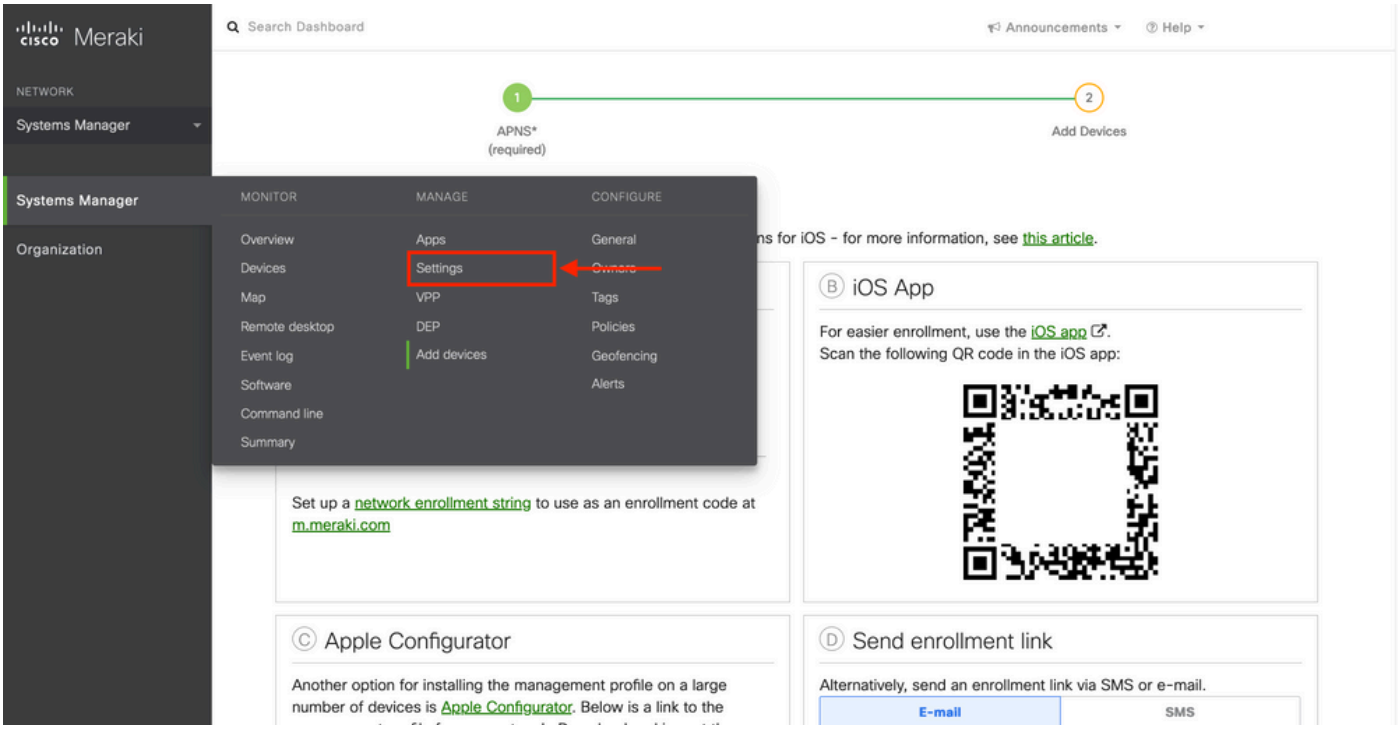
- Firefox: Private, Safe Browser (org.mozilla.ios.Firefox)
- Firefox Focus: Privacy browser (org.mozilla.ios.Focus)
- Microsoft Edge: Web Browser (com.microsoft.msedge)
- Microsoft Bing Search (com.microsoft.bing)

(Please allow 1-2 minutes for changes to take effect.)

2.5. Click **Save** once you select all the desired applications.

Step 3. Configure PerApp VPN profile

3.1. Navigate to **Systems Manager > Manage > Settings**



ns for iOS - for more information, see this article.

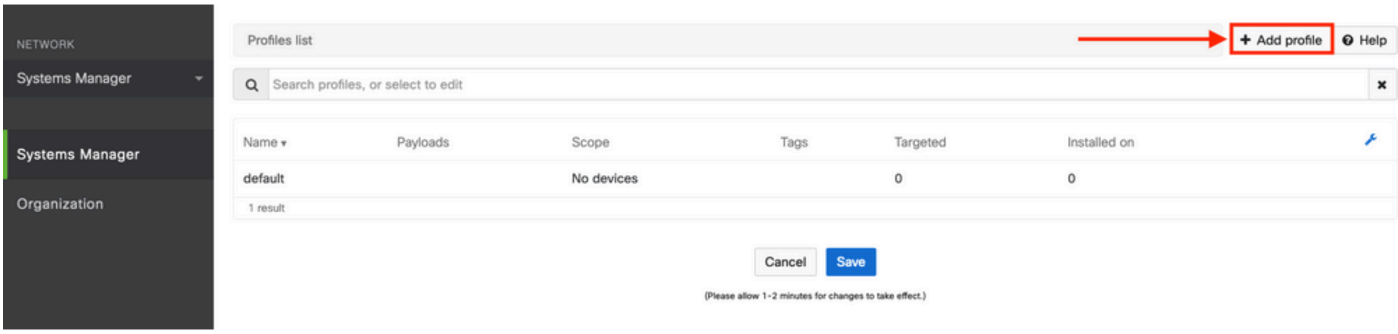
For easier enrollment, use the iOS app. Scan the following QR code in the iOS app:

Set up a network enrollment string to use as an enrollment code at m.meraki.com

Another option for installing the management profile on a large number of devices is Apple Configurator. Below is a link to the

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

3.2. Select the **Add profile** option.

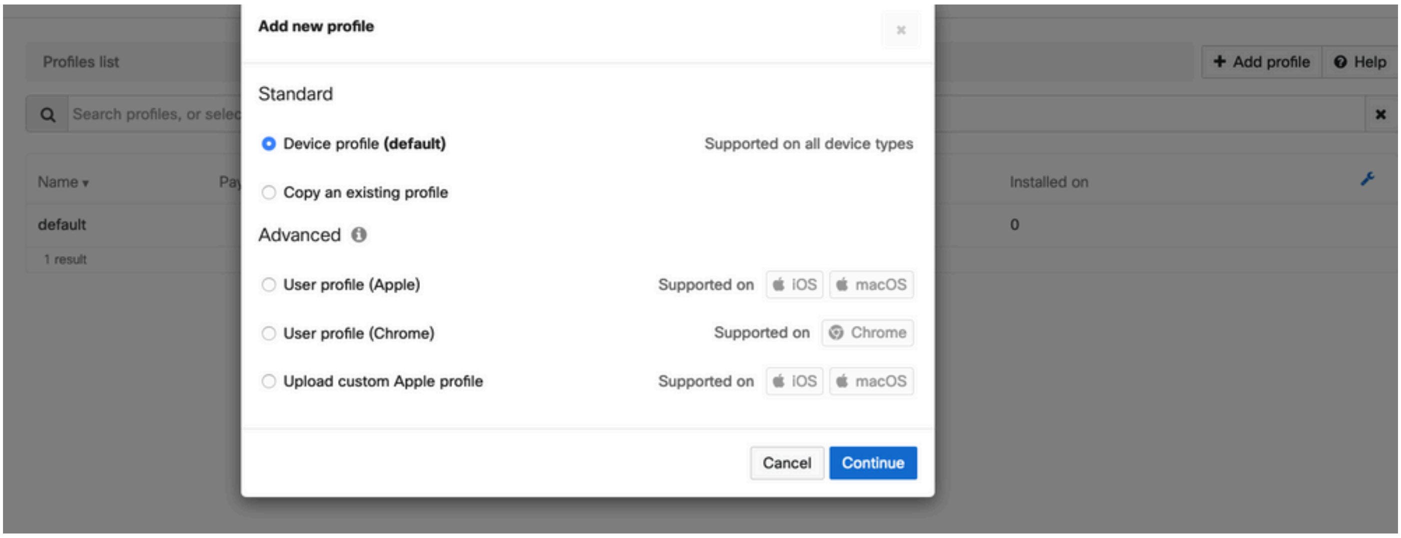


Name ▾	Payloads	Scope	Tags	Targeted	Installed on
default		No devices		0	0

1 result

(Please allow 1-2 minutes for changes to take effect.)

3.3. Select **Device profile (default)** and click **Continue.**



Add new profile

Standard

● Device profile **(default)** — Supported on all device types

○ Copy an existing profile

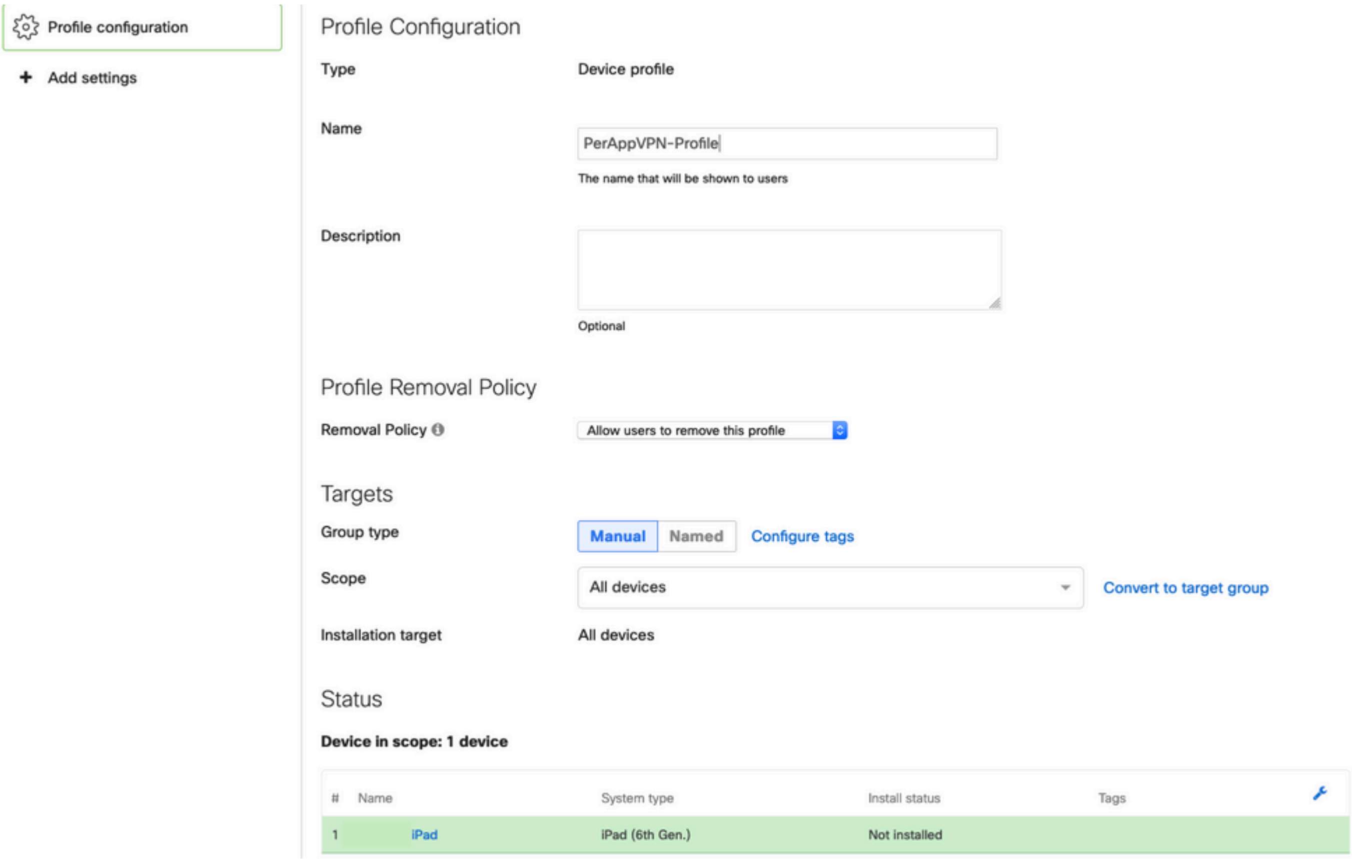
Advanced

○ User profile (Apple) — Supported on iOS macOS

○ User profile (Chrome) — Supported on Chrome

○ Upload custom Apple profile — Supported on iOS macOS

3.4. Once the **Profile Configuration** menu is displayed, write the **Name** and select the target devices under **Scope**.



Profile Configuration

Type: Device profile

Name: PerAppVPN-Profile

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

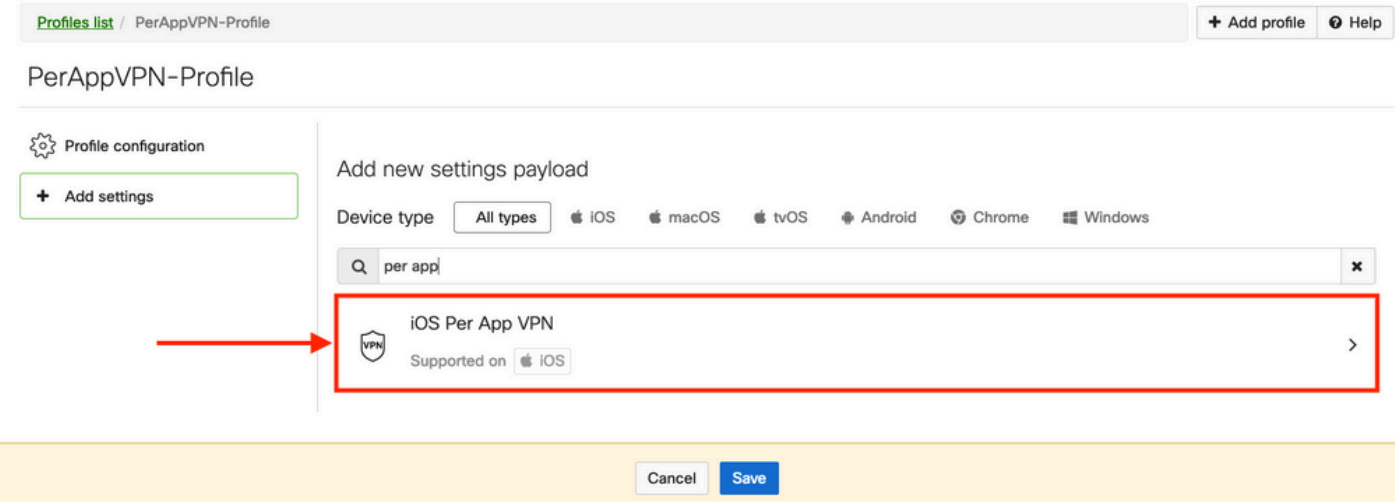
Installation target: All devices

Status

Device in scope: 1 device

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

3.5. Select **Add settings** and filter the types of profile by **iOS Per App VPN**, select the option as seen below.



Profiles list / PerAppVPN-Profile

+ Add profile | Help

PerAppVPN-Profile

Profile configuration

+ Add settings

Add new settings payload

Device type: All types | iOS | macOS | tvOS | Android | Chrome | Windows

per app

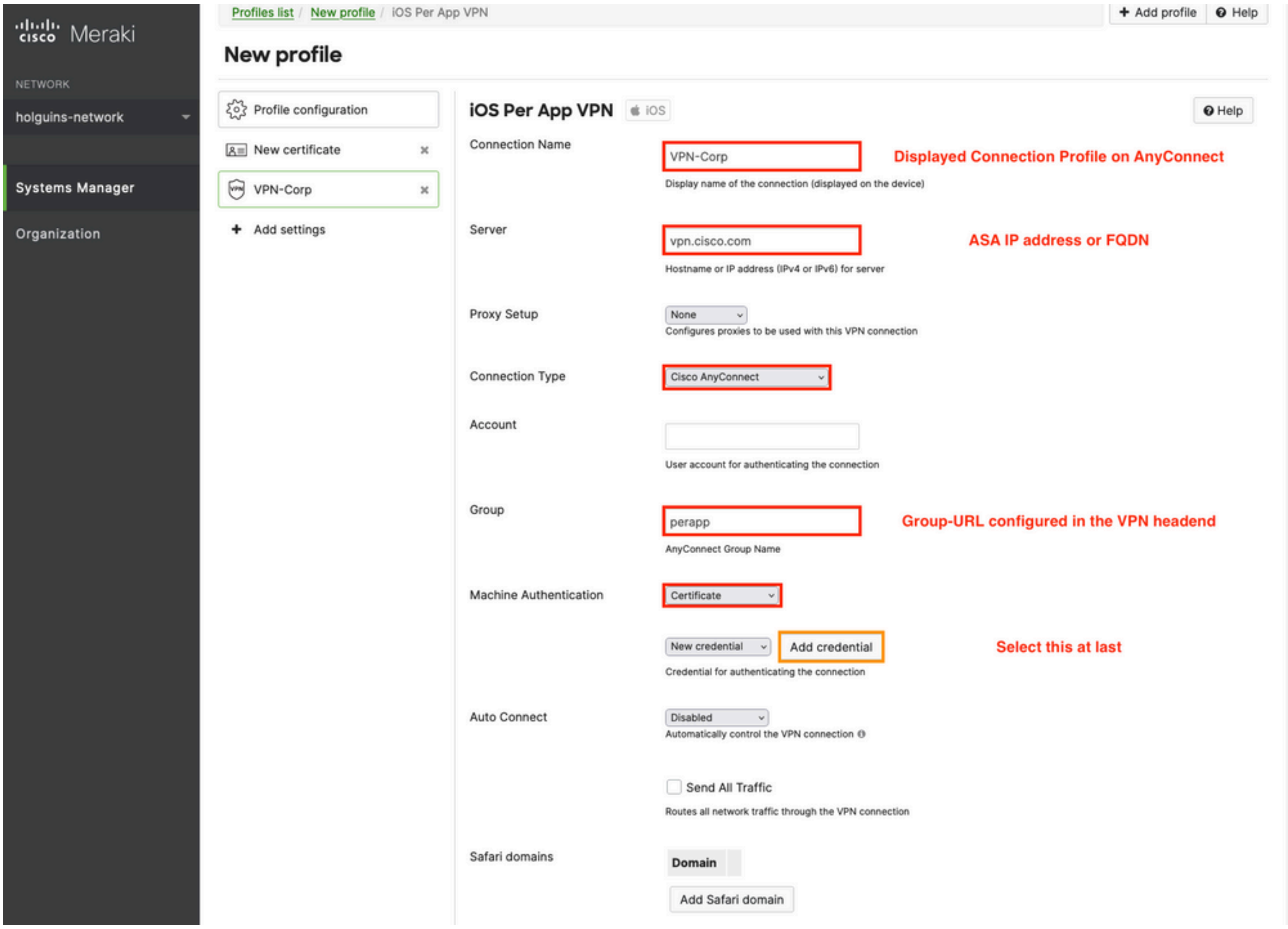
iOS Per App VPN
Supported on iOS

Cancel | Save

3.6. Once the menu is displayed, write the connection information based on the example below.

Systems Manager supports two certificate enrollments for these connections, SCEP and manual enrollment. In this example manual enrollment was used.

> **Note**: Select **Add credential** once you filled the text-boxes since this option takes you to a new menu to add a certificate file.



Profiles list / New profile / iOS Per App VPN

+ Add profile | Help

New profile

Profile configuration

New certificate ×

VPN-Corp ×

+ Add settings

iOS Per App VPN (iOS) | Help

Connection Name: VPN-Corp — Display name of the connection (displayed on the device) — **Displayed Connection Profile on AnyConnect**

Server: vpn.cisco.com — Hostname or IP address (IPv4 or IPv6) for server — **ASA IP address or FQDN**

Proxy Setup: None — Configures proxies to be used with this VPN connection

Connection Type: Cisco AnyConnect

Account: — User account for authenticating the connection

Group: perapp — AnyConnect Group Name — **Group-URL configured in the VPN headend**

Machine Authentication: Certificate

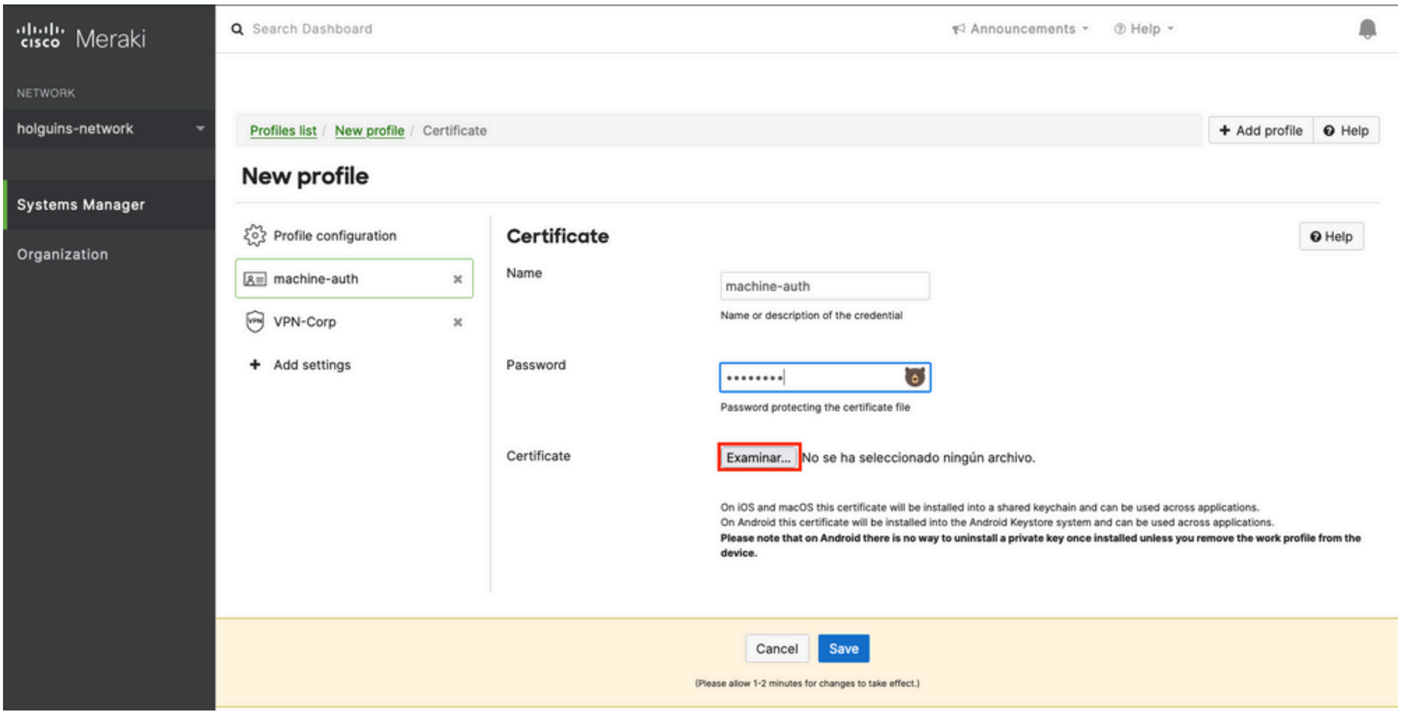
New credential | Add credential — Credential for authenticating the connection — **Select this at last**

Auto Connect: Disabled — Automatically control the VPN connection

□ Send All Traffic — Routes all network traffic through the VPN connection

Safari domains: Domain — Add Safari domain

3.7. Once you clicked on **Add credential** and you got redirected to the Certificate menu, write the **Name** of the Certificate, browse in your computer and look for the the **Password** that protects the .pfx file (encrypted certificate file).



New profile

Certificate

Name: machine-auth

Name or description of the credential

Password: ••••••••

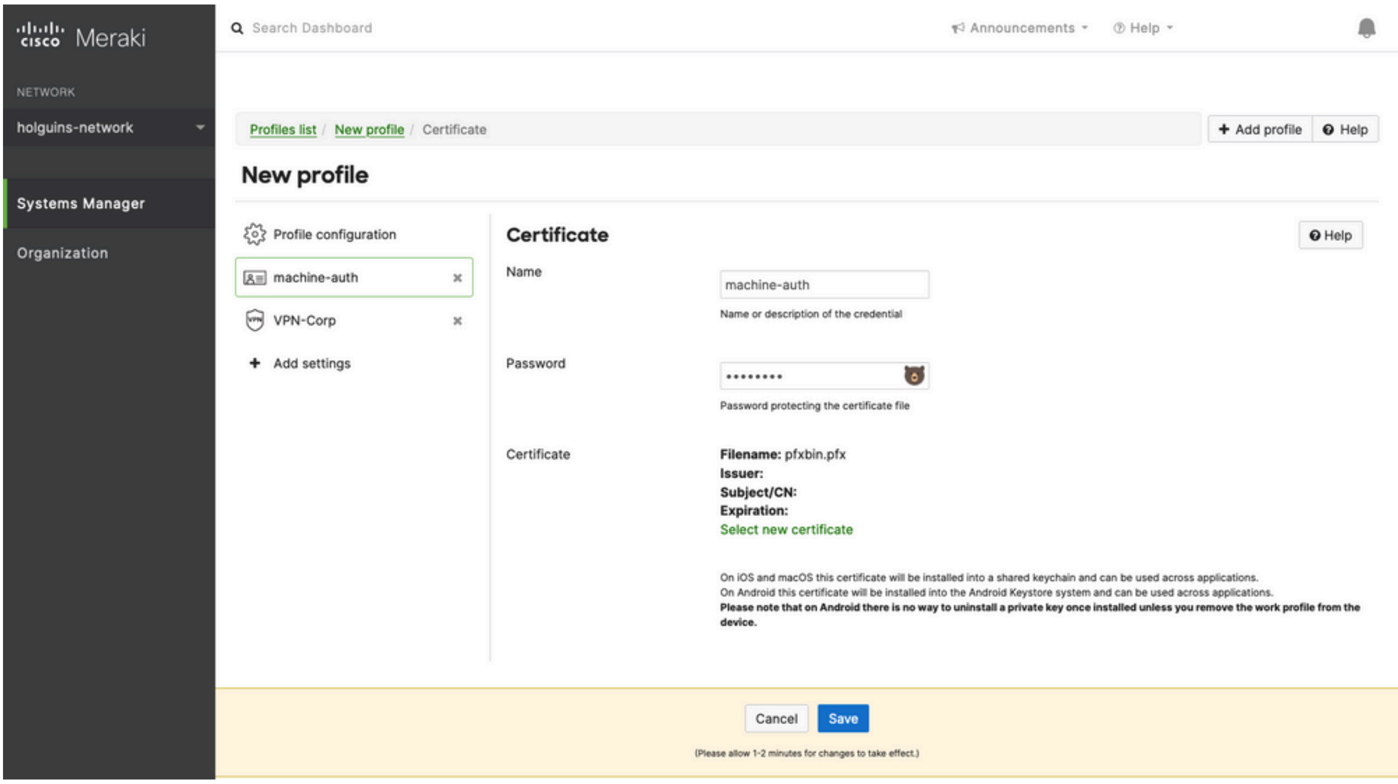
Password protecting the certificate file

Certificate: Examinar... No se ha seleccionado ningún archivo.

On iOS and macOS this certificate will be installed into a shared keychain and can be used across applications.
On Android this certificate will be installed into the Android Keystore system and can be used across applications.
Please note that on Android there is no way to uninstall a private key once installed unless you remove the work profile from the device.

(Please allow 1-2 minutes for changes to take effect.)

3.8. After the certificate is selected, the certificate filename is displayed.



New profile

Certificate

Name: machine-auth

Name or description of the credential

Password: ••••••••

Password protecting the certificate file

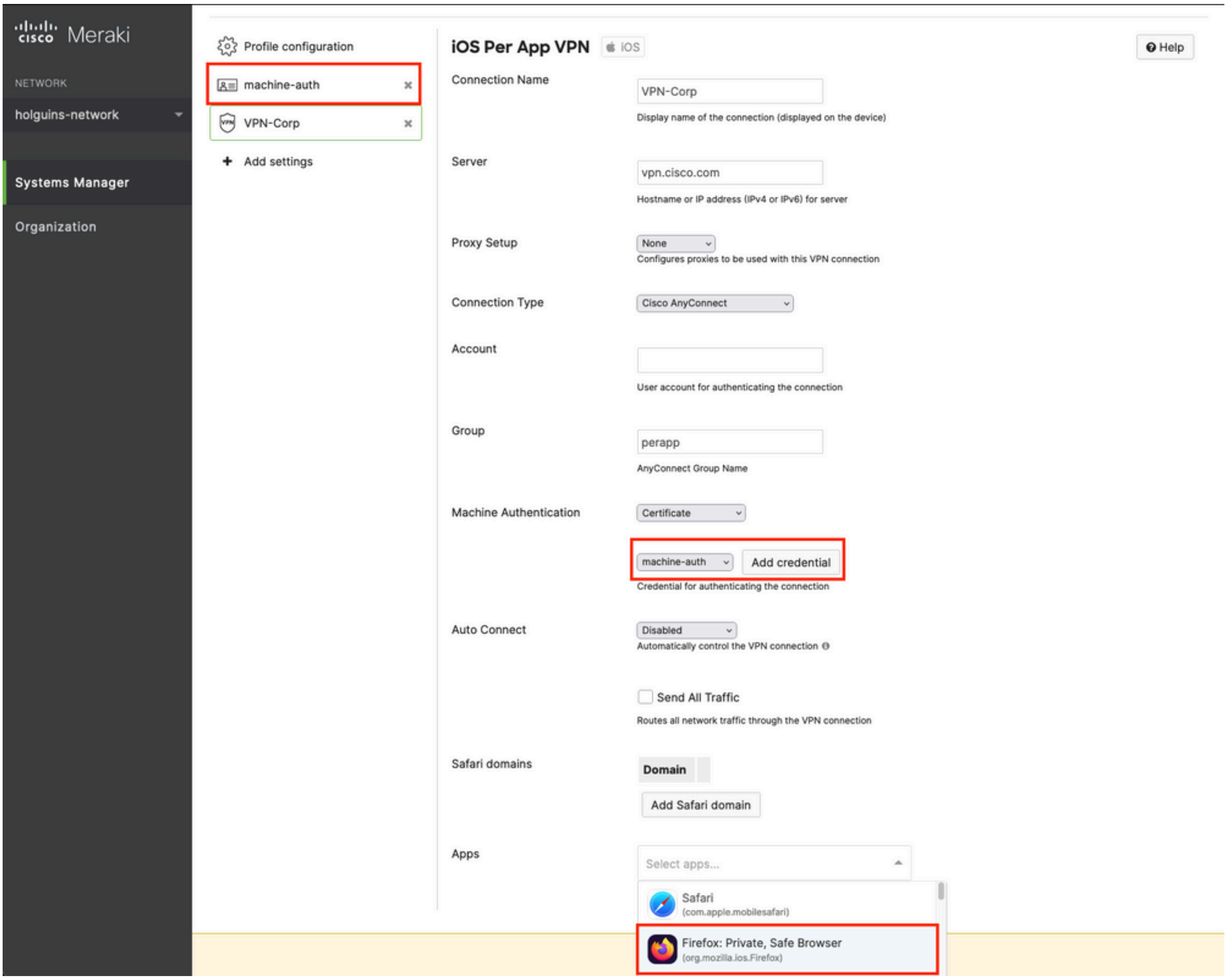
Certificate:
Filename: pfxbin.pfx
Issuer:
Subject/CN:
Expiration:
Select new certificate

On iOS and macOS this certificate will be installed into a shared keychain and can be used across applications.
On Android this certificate will be installed into the Android Keystore system and can be used across applications.
Please note that on Android there is no way to uninstall a private key once installed unless you remove the work profile from the device.

(Please allow 1-2 minutes for changes to take effect.)

3.9. Once you selected the certificate, navigate to the VPN profile you were previously on and select the recently imported credential and Select the tunneled App (Firefox in this case).

Click **Save** once this is completed.



iOS Per App VPN iOS

Connection Name: VPN-Corp
Display name of the connection (displayed on the device)

Server: vpn.cisco.com
Hostname or IP address (IPv4 or IPv6) for server

Proxy Setup: None
Configures proxies to be used with this VPN connection

Connection Type: Cisco AnyConnect

Account:
User account for authenticating the connection

Group: perapp
AnyConnect Group Name

Machine Authentication: Certificate
machine-auth Add credential
Credential for authenticating the connection

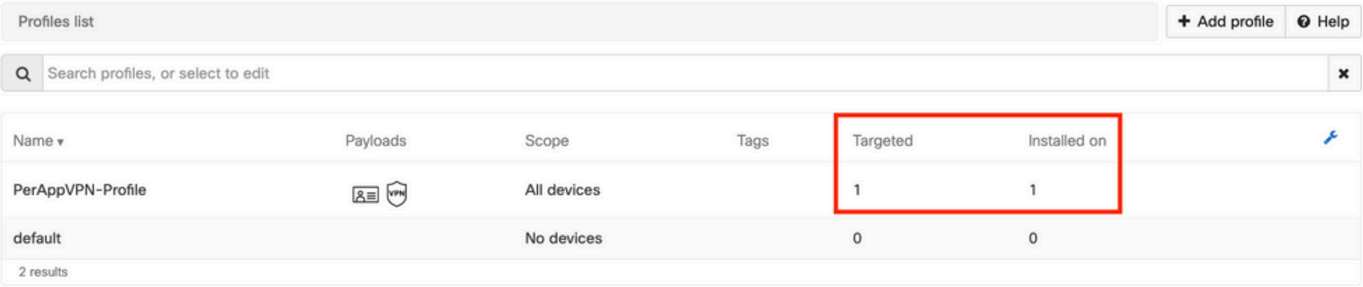
Auto Connect: Disabled
Automatically control the VPN connection

□ Send All Traffic
Routes all network traffic through the VPN connection

Safari domains: Domain
Add Safari domain

Apps: Select apps...
Safari (com.apple.mobilesafari)
Firefox: Private, Safe Browser (org.mozilla.ios.Firefox)

3.10. Verify the profile is installed on the target devices.



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

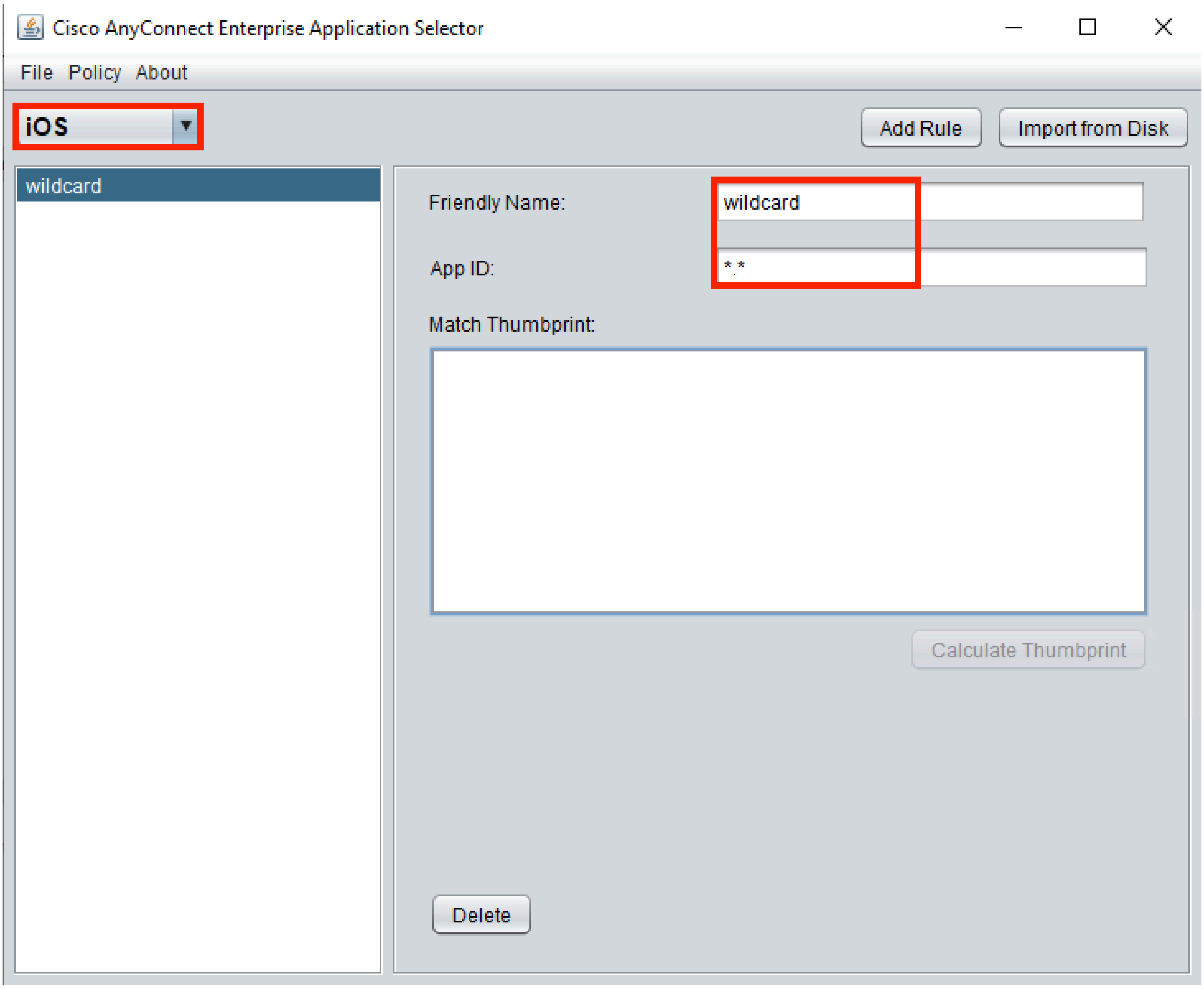
2 results

Step 4. App Selector Configuration

4.1. Download app selector from cisco website
https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0

> **Caution**: Run the application on a Windows machine. The results displayed are not be the expected when the tool is used on MacOS devices.

4.2. Open the java application. Select **iOS** from the dropdown menu, add a friendly name and ensure you type ***.*** in the **App ID**.

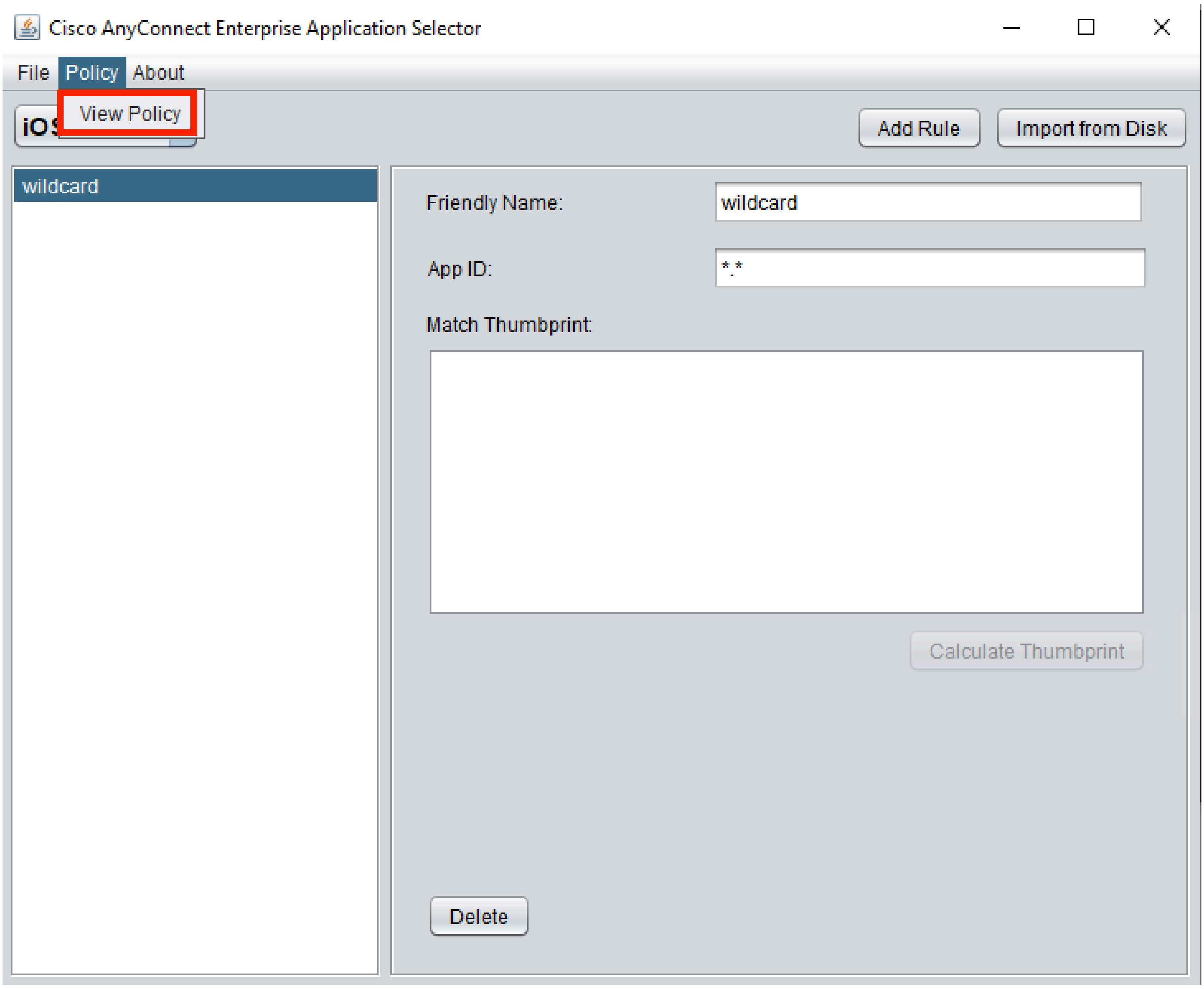


Friendly Name: wildcard

App ID: *.*

Match Thumbprint:

4.3. Navigate to **Policy** and select **View Policy**

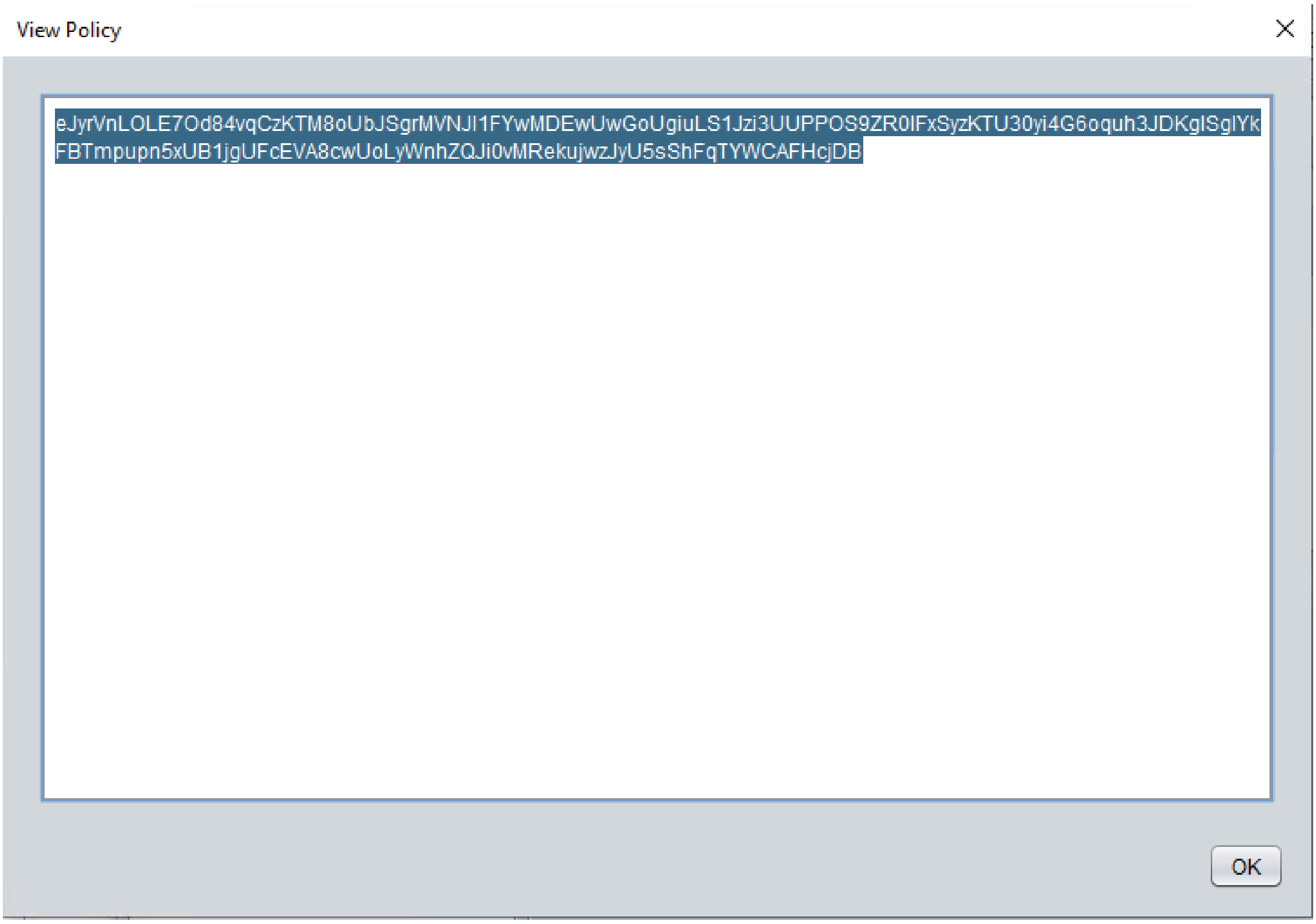


Friendly Name: wildcard

App ID: *.*

Match Thumbprint:

4.4. Copy the string displayed. (This is later used in the VPN headend configuration).



View Policy

```
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0lFxSyzKTU30yi4G6oquh3JDKglSgIYk
FBTmpupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB
```

Step 5. ASA Sample Per App VPN Configuration

```
conf t
webvpn
anyconnect-custom-attr perapp description PerAppVPN
anyconnect-custom-data perapp wildcard
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0lFxSyzKTU30yi4G6oquh3JDKglSg
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
```

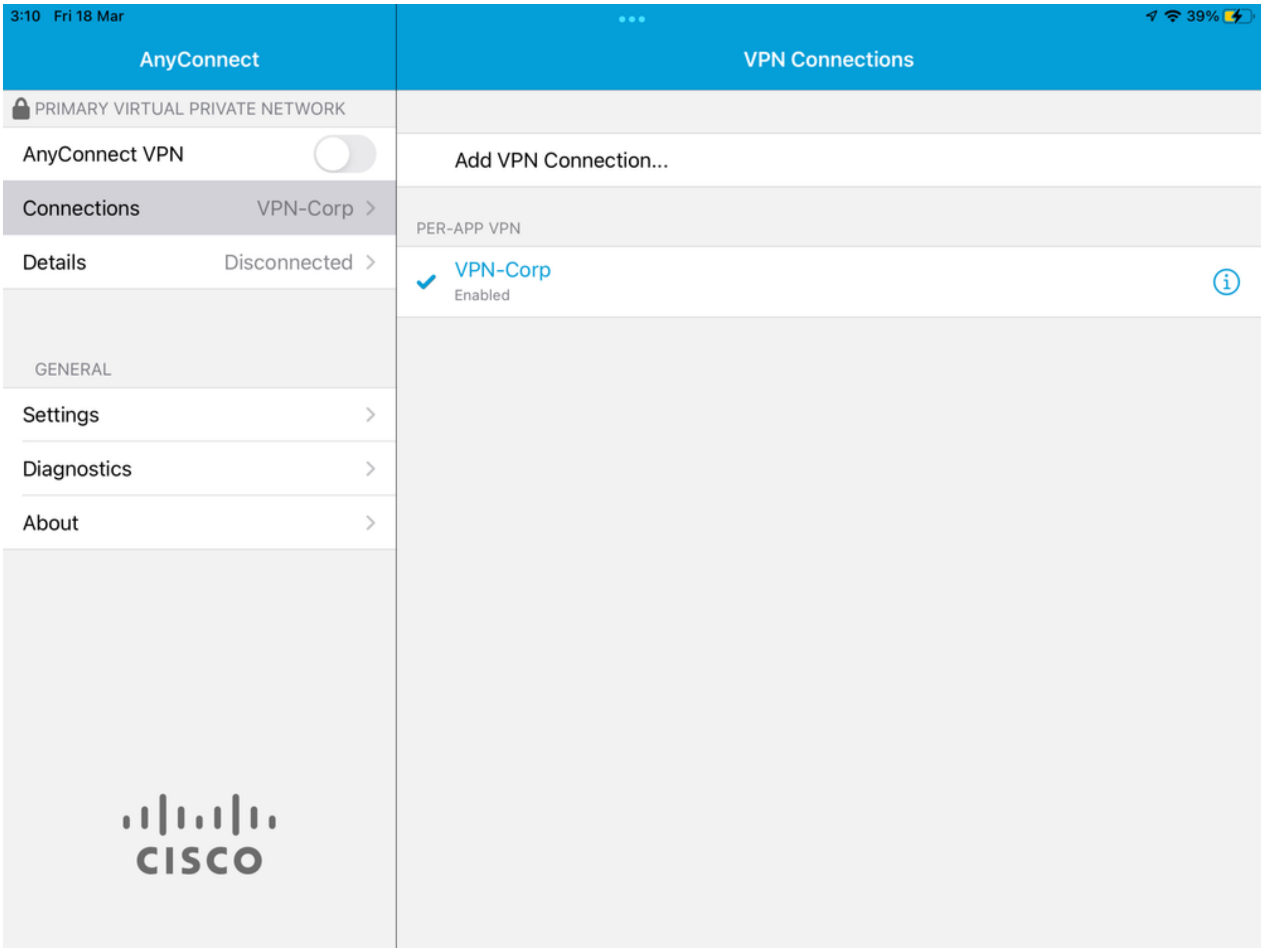
```
group-url https://vpn.cisco.com/perapp enable
```

Verify

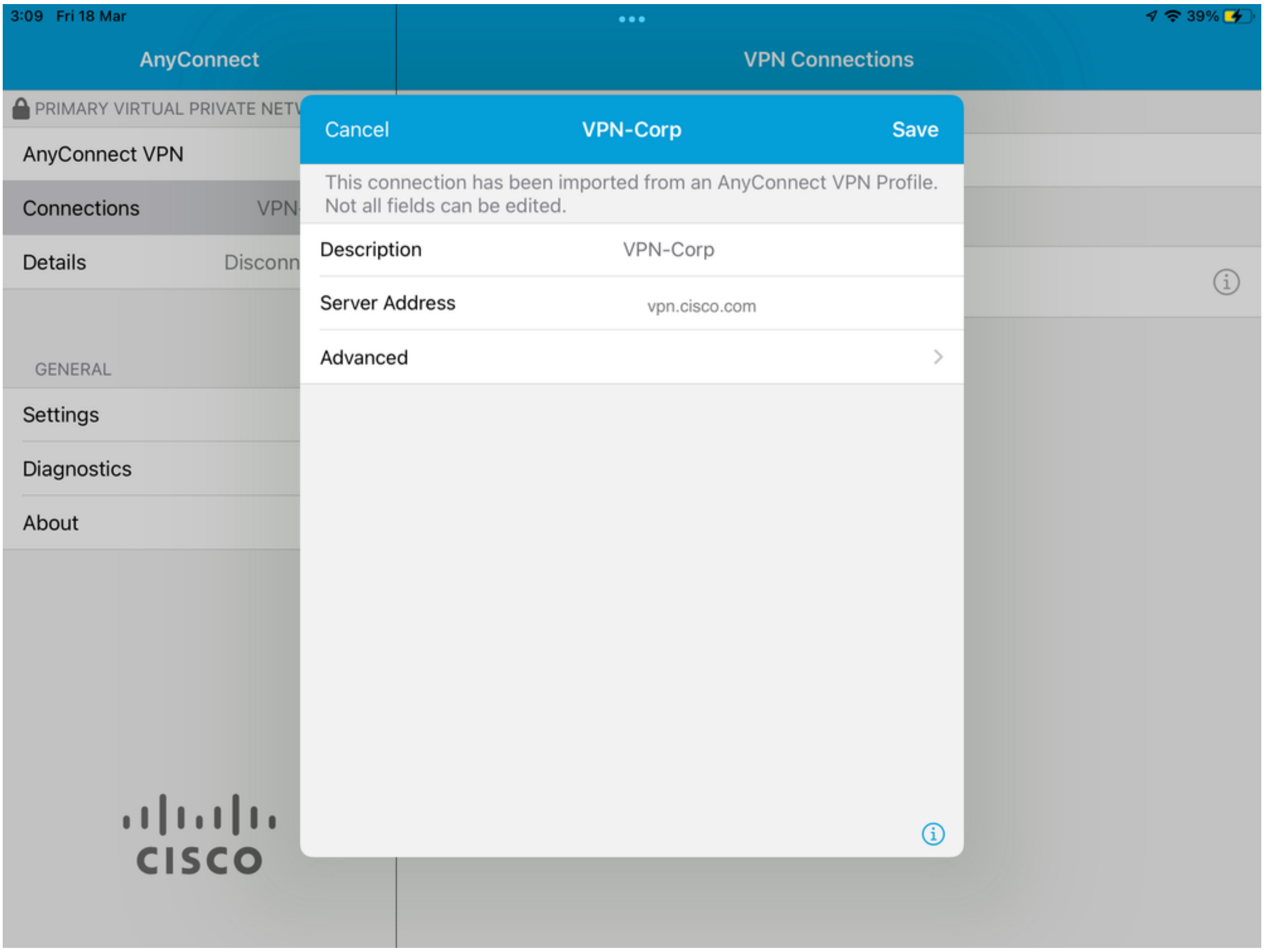
6. Verify Profile Installation on AnyConnect Application

6.1. Open the AnyConnect Application and select **Connections** in the left pane. The PerApp VPN profile must be displayed under a new section called **PER-APP VPN**.

Select the **i** to display the advanced settings.



6.2. Select the **Advanced** option.

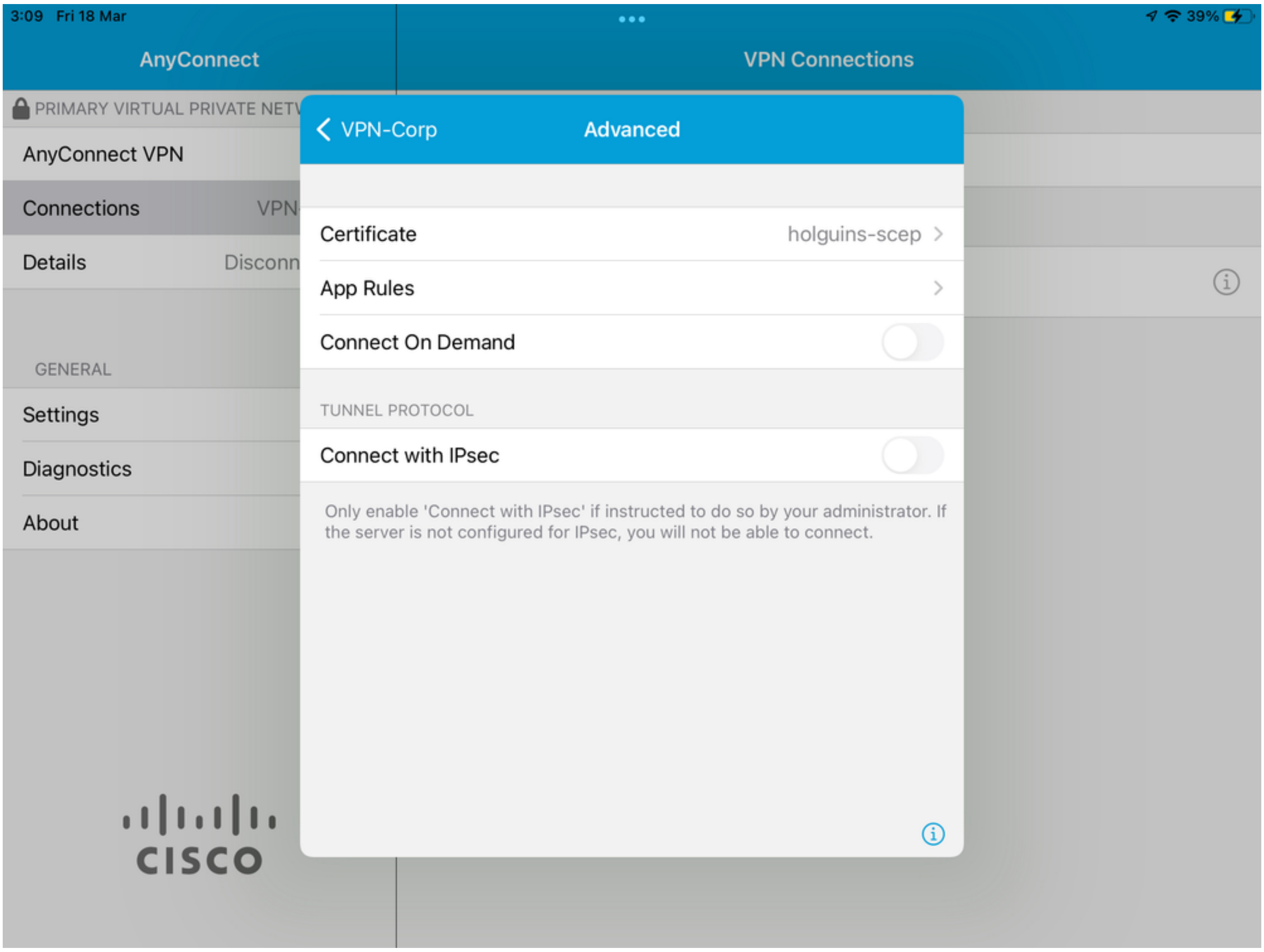


This connection has been imported from an AnyConnect VPN Profile. Not all fields can be edited.

Description VPN-Corp

Server Address vpn.cisco.com

6.3. Select the **App Rules** option.



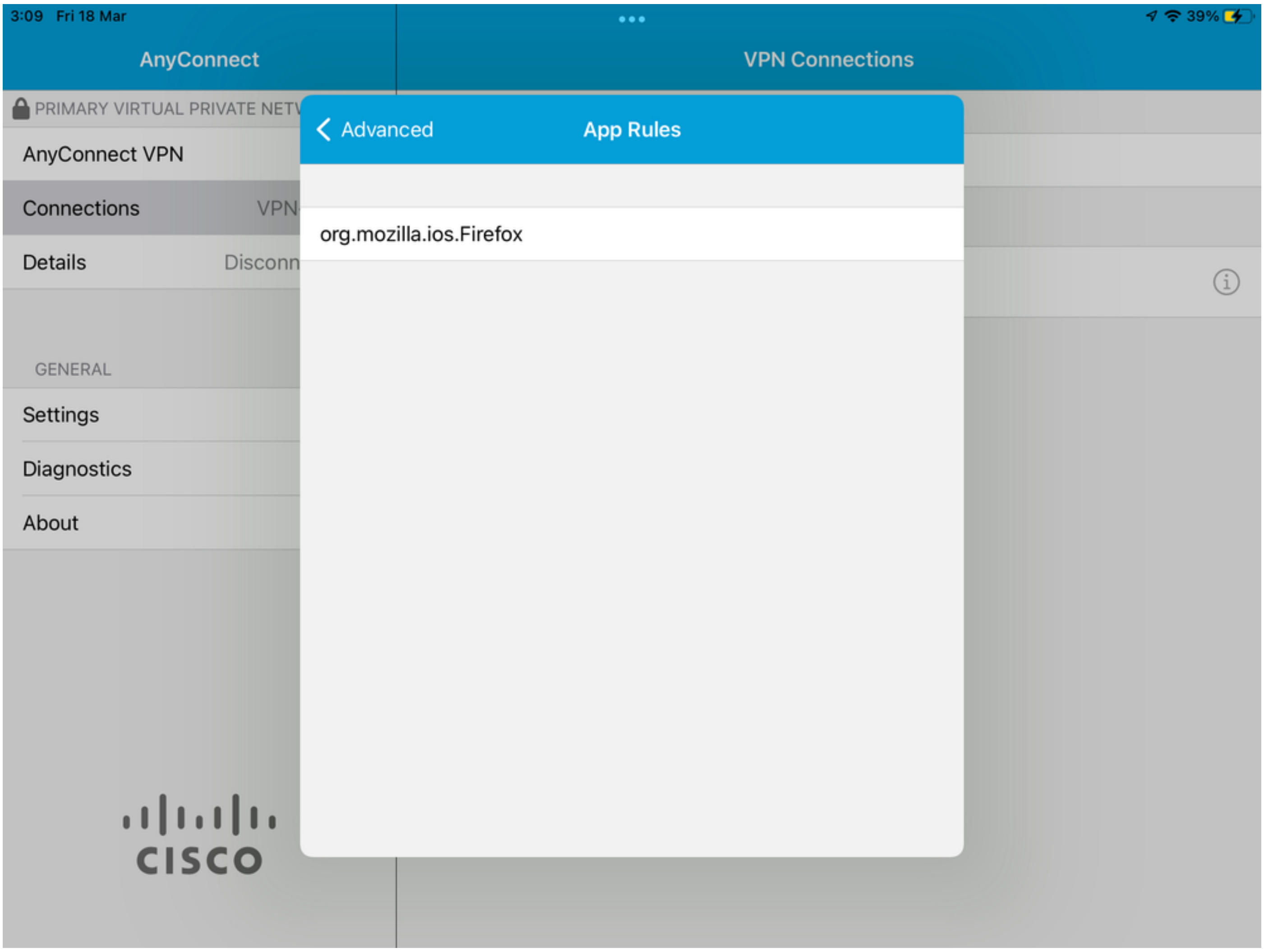
Certificate holguins-scep

Connect On Demand

Connect with IPsec

Only enable 'Connect with IPsec' if instructed to do so by your administrator. If the server is not configured for IPsec, you will not be able to connect.

6.4. Lastly, confirm the App Rule is installed. (Mozilla is the tunneled App desired in this document, so the app installation was successful).



org.mozilla.ios.Firefox

Troubleshoot

There are currently no specific troubleshooting steps for this document.