使用Meraki系統管理器配置iOS的Anyconnect PerApp VPN

目錄

簡介

本文檔介紹如何在由Meraki流動裝置管理器(MDM)和系統管理器(SM)管理的Apple iOS裝置上配置PerApp VPN。

必要條件

需求

- AnyConnect v4.0 Plus或Apex許可證。
- ASA 9.3.1或更高版本，支援每應用VPN。
- Cisco.com上提供了思科企業應用選擇器工具

採用元件

本檔案中的資訊是根據以下軟體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

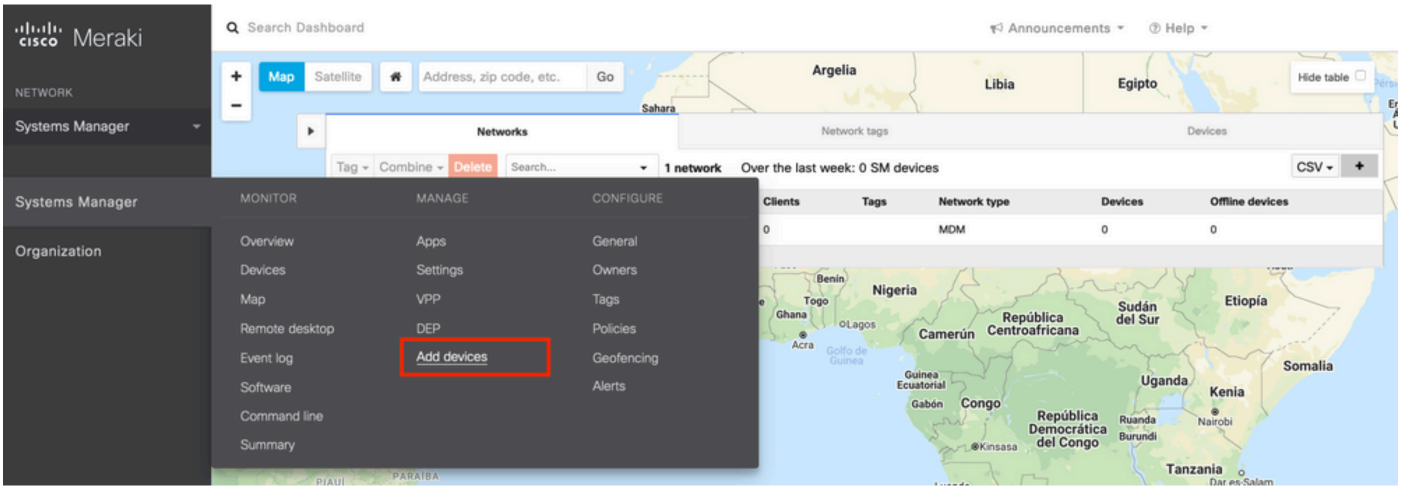
本文檔不包括列出的進程：

- Systems Manager上的SCEP CA配置，用於生成客戶端證書
- 為iOS客戶端生成PKCS12客戶端證書

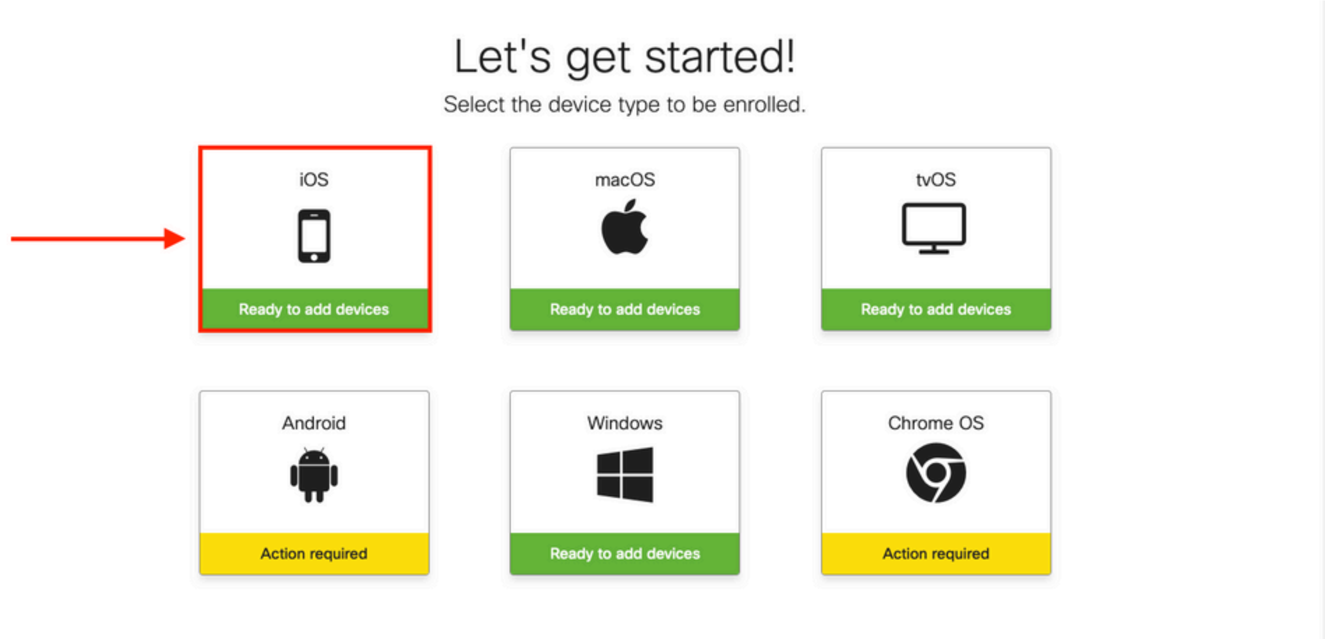
設定

步驟1.將iOS裝置註冊到Meraki系統管理器

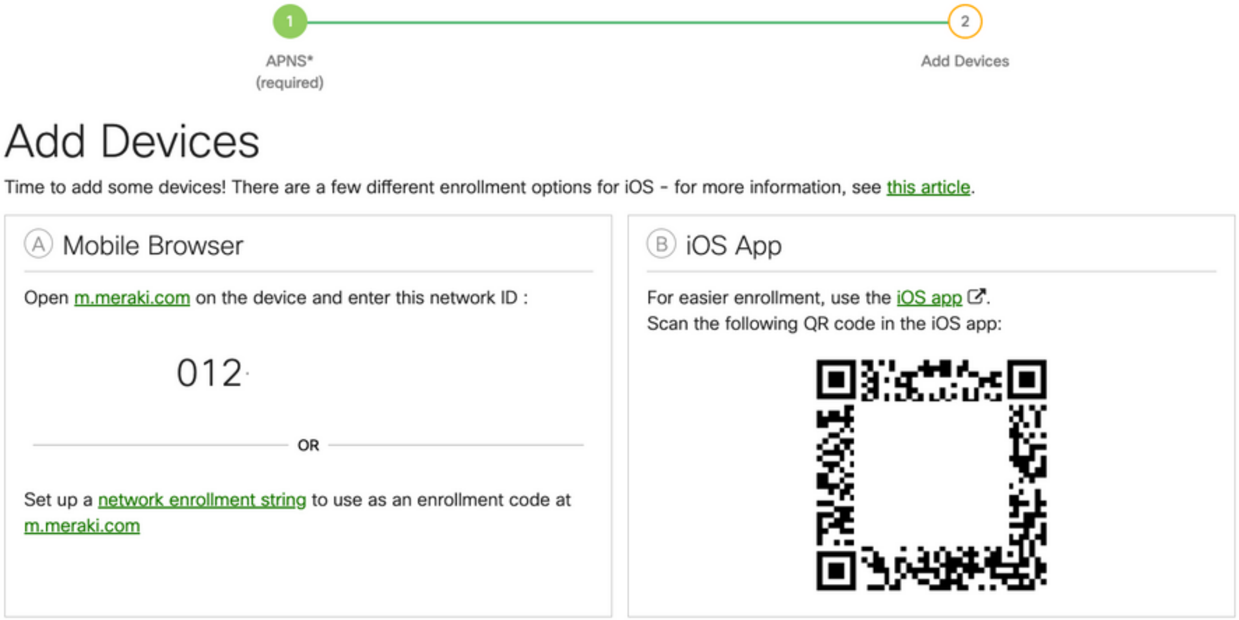
1.1.導航到**Systems Manager > Add Devices**



1.2.按一下**iOS**選項開始註冊。



1.3.通過網際網路瀏覽器註冊裝置或使用監視器掃描QR碼。在本文檔中，使用監視器進行註冊過程。



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]

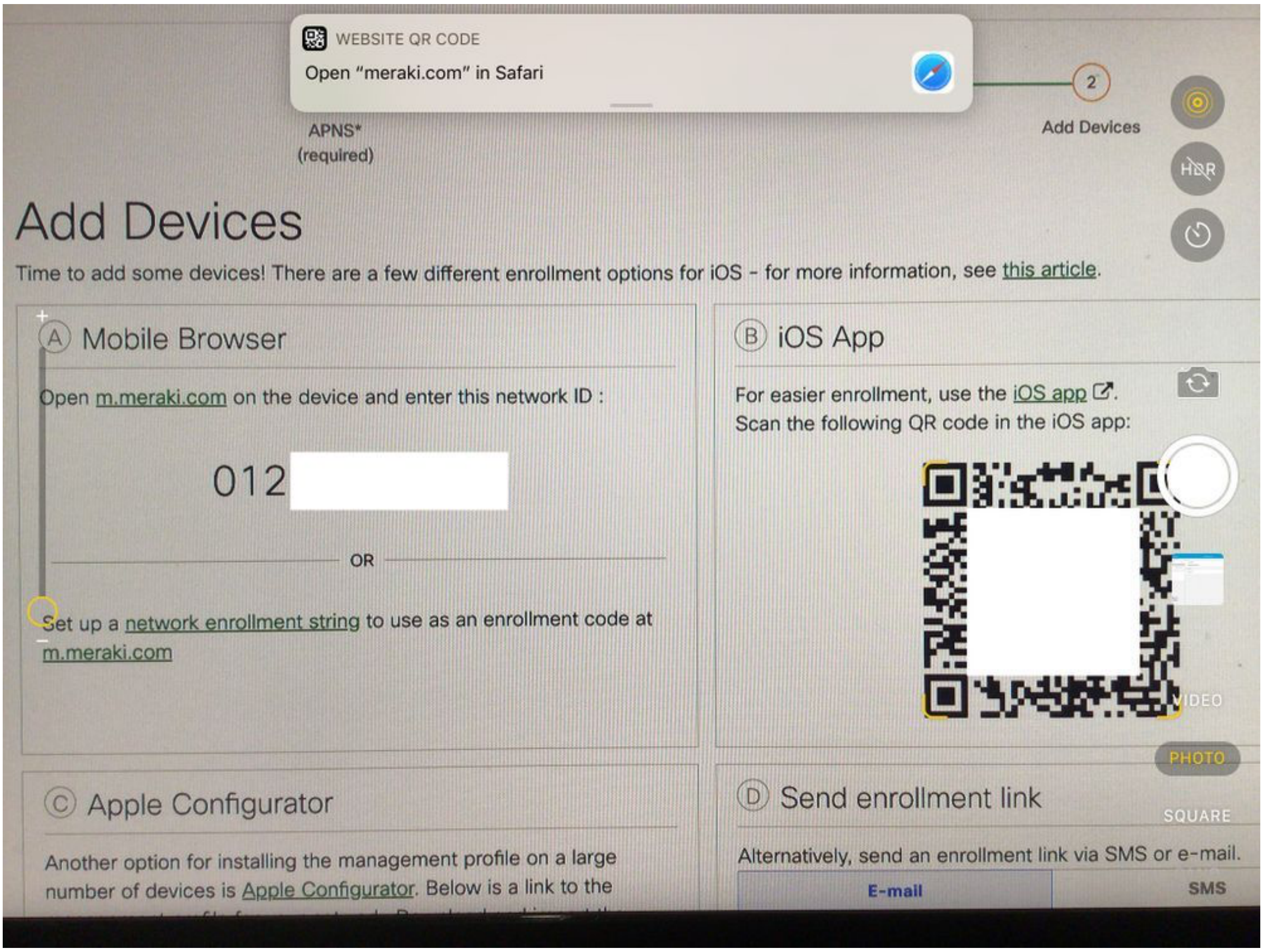
OR

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.當監視器識別QR代碼時，請在彈出的Safari通知中選擇**Open** "meraki.com"。



WEBSITE QR CODE
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

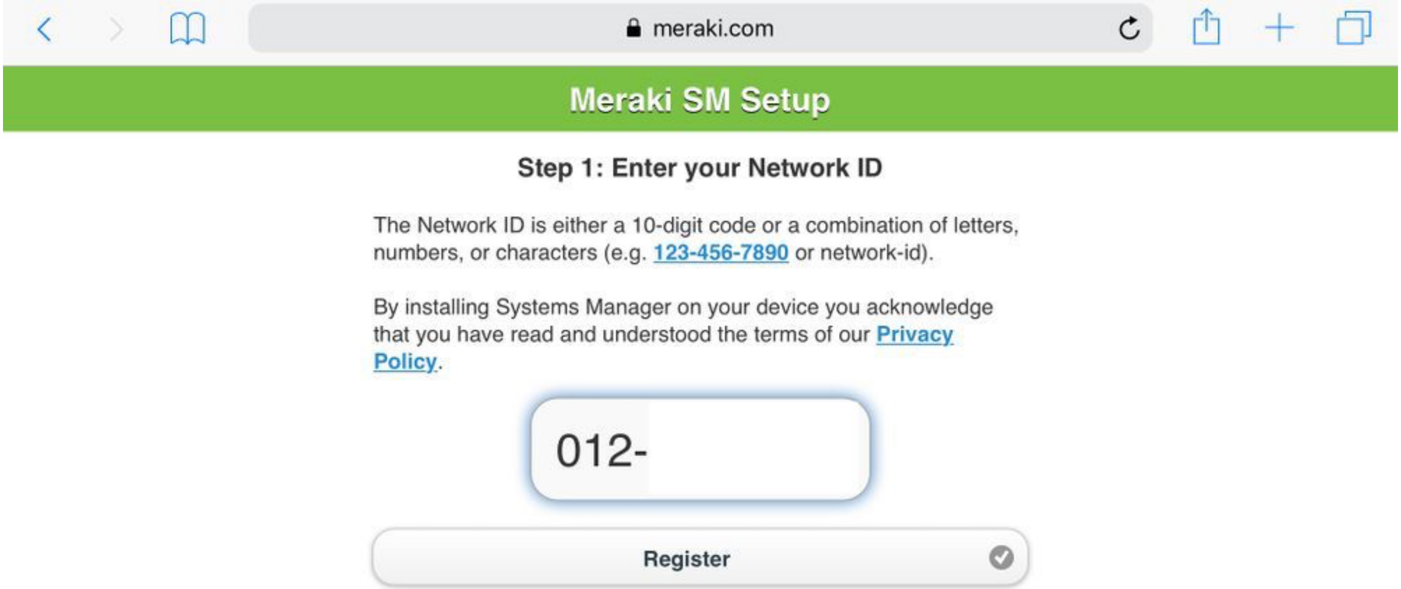
Another option for installing the management profile on a large number of devices is Apple Configurator. Below is a link to the

Ⓓ Send enrollment link

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

E-mail SMS

1.5.出現提示時，選擇**Register**。



meraki.com

Meraki SM Setup

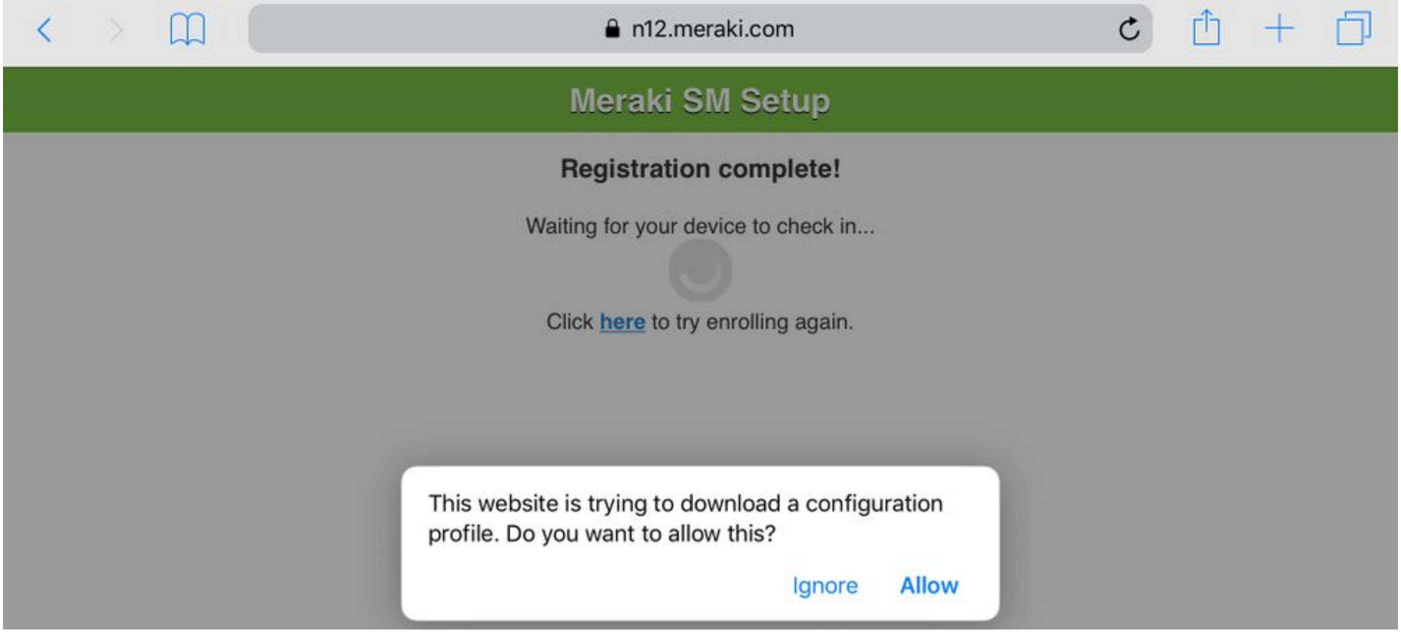
Step 1: Enter your Network ID

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.選擇Allow以允許裝置下載MDM配置檔案。



n12.meraki.com

Meraki SM Setup

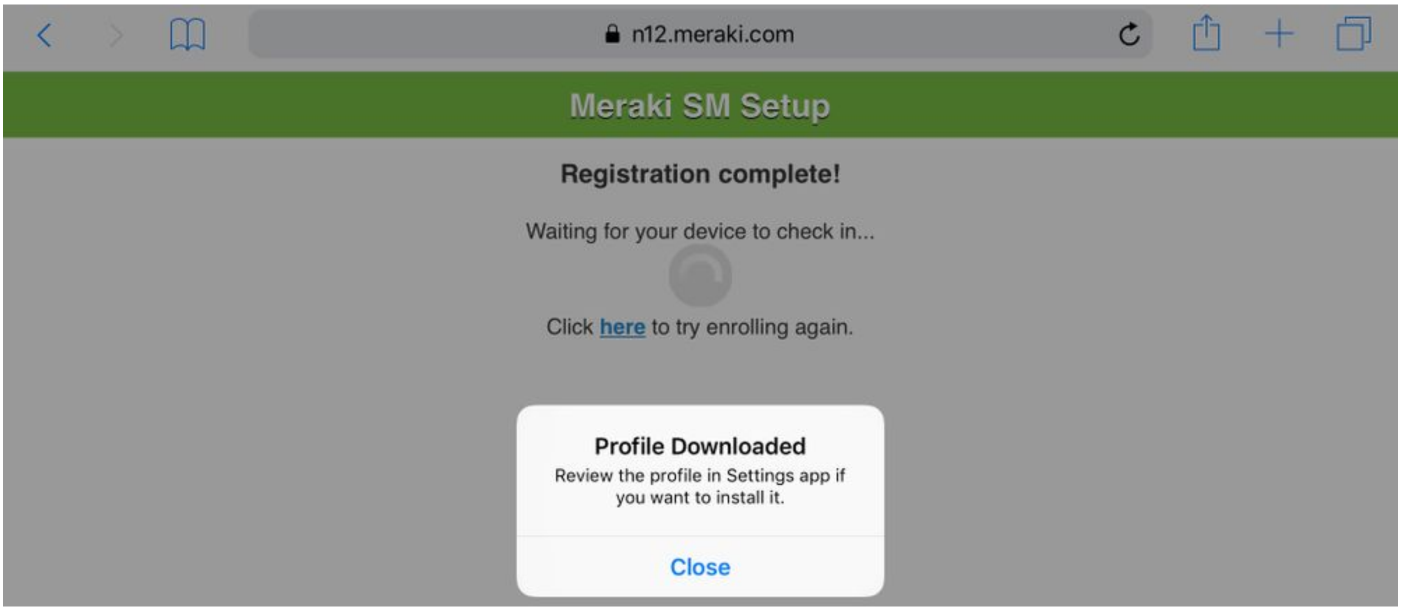
Registration complete!

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.選擇Close以完成下載。



n12.meraki.com

Meraki SM Setup

Registration complete!

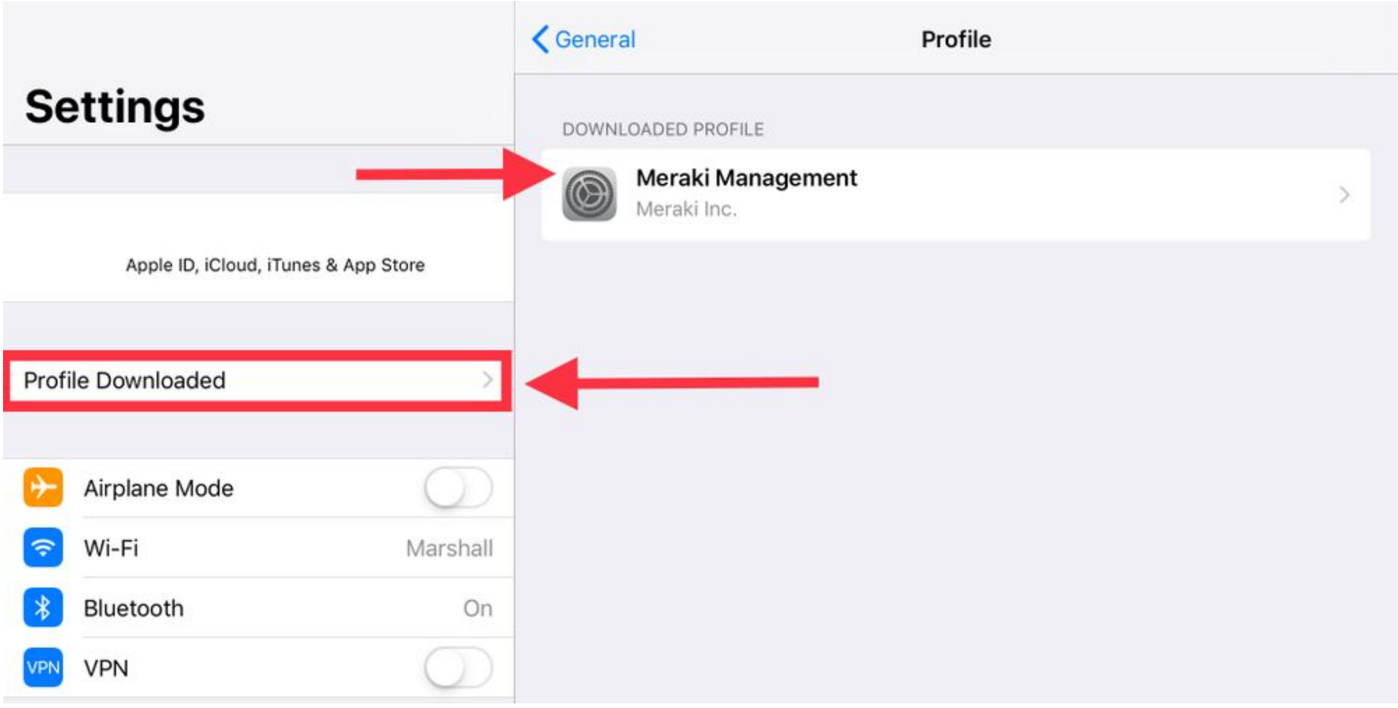
Waiting for your device to check in...

Click here to try enrolling again.

Profile Downloaded

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

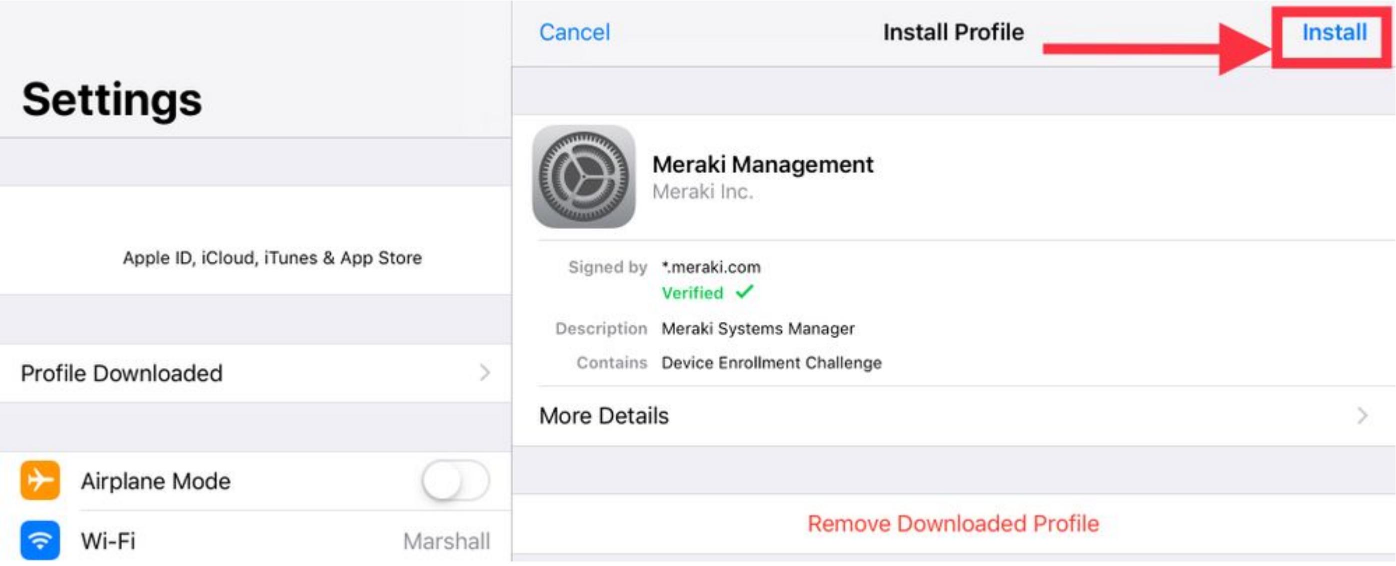
1.8.導航到iOS設定應用，在左窗格中找到**Profile Downloaded**選項，然後選擇**Meraki Management**部分。



Wi-Fi: Marshall

Bluetooth: On

1.9.選擇**Install**選項以安裝MDM配置檔案。



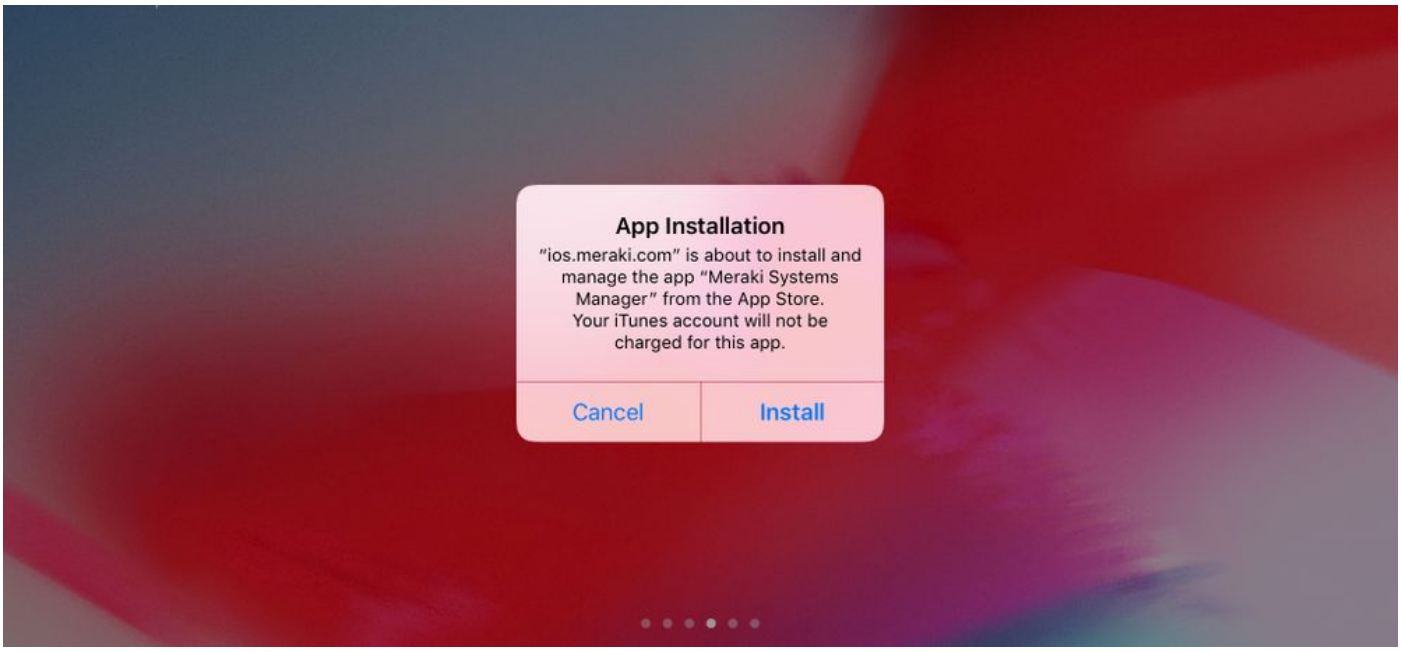
Wi-Fi: Marshall

Signed by *.meraki.com
Verified ✓

Description Meraki Systems Manager

Contains Device Enrollment Challenge

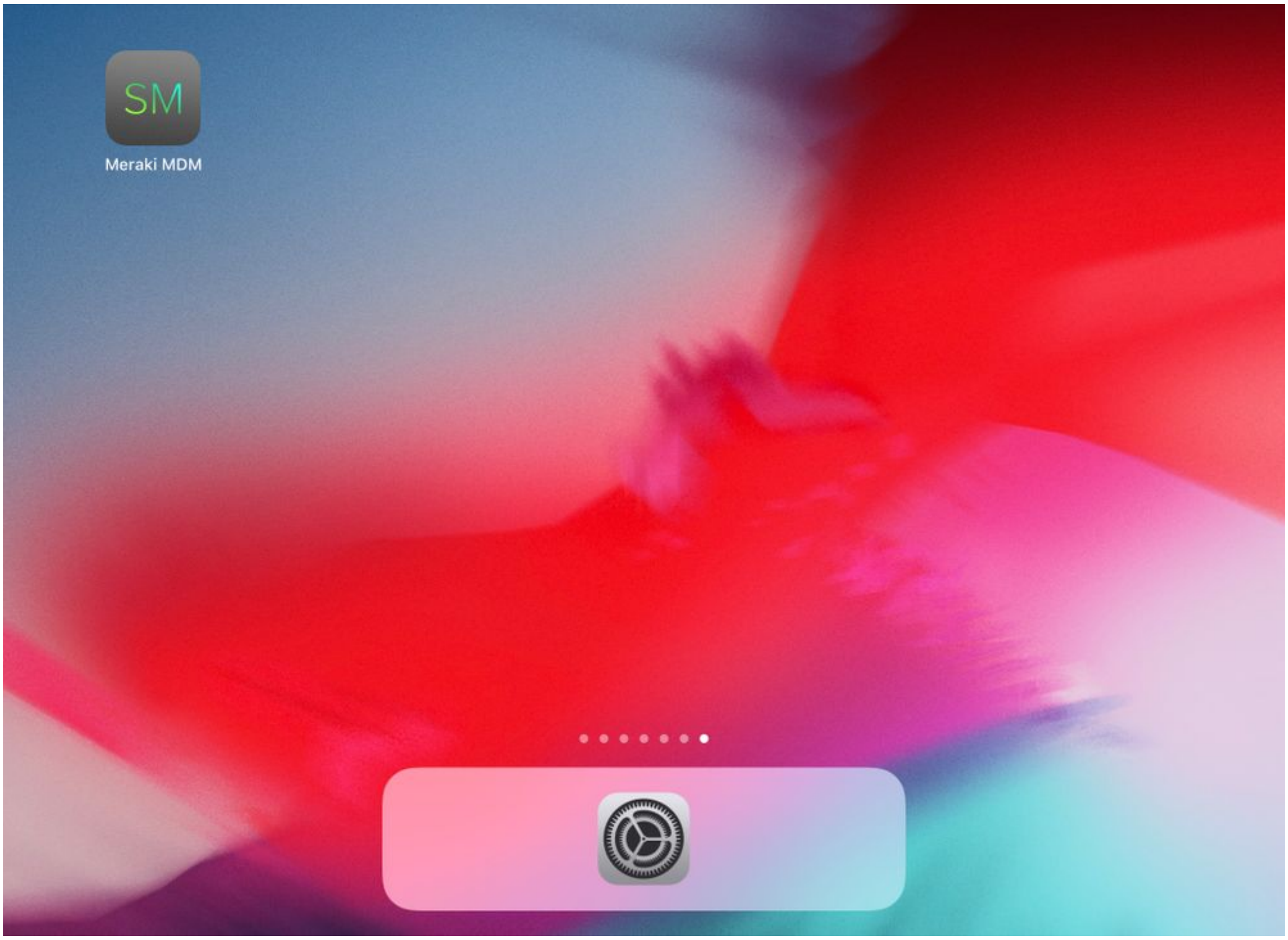
1.10.您必須授予訪問**安裝SM**應用程式的許可權。



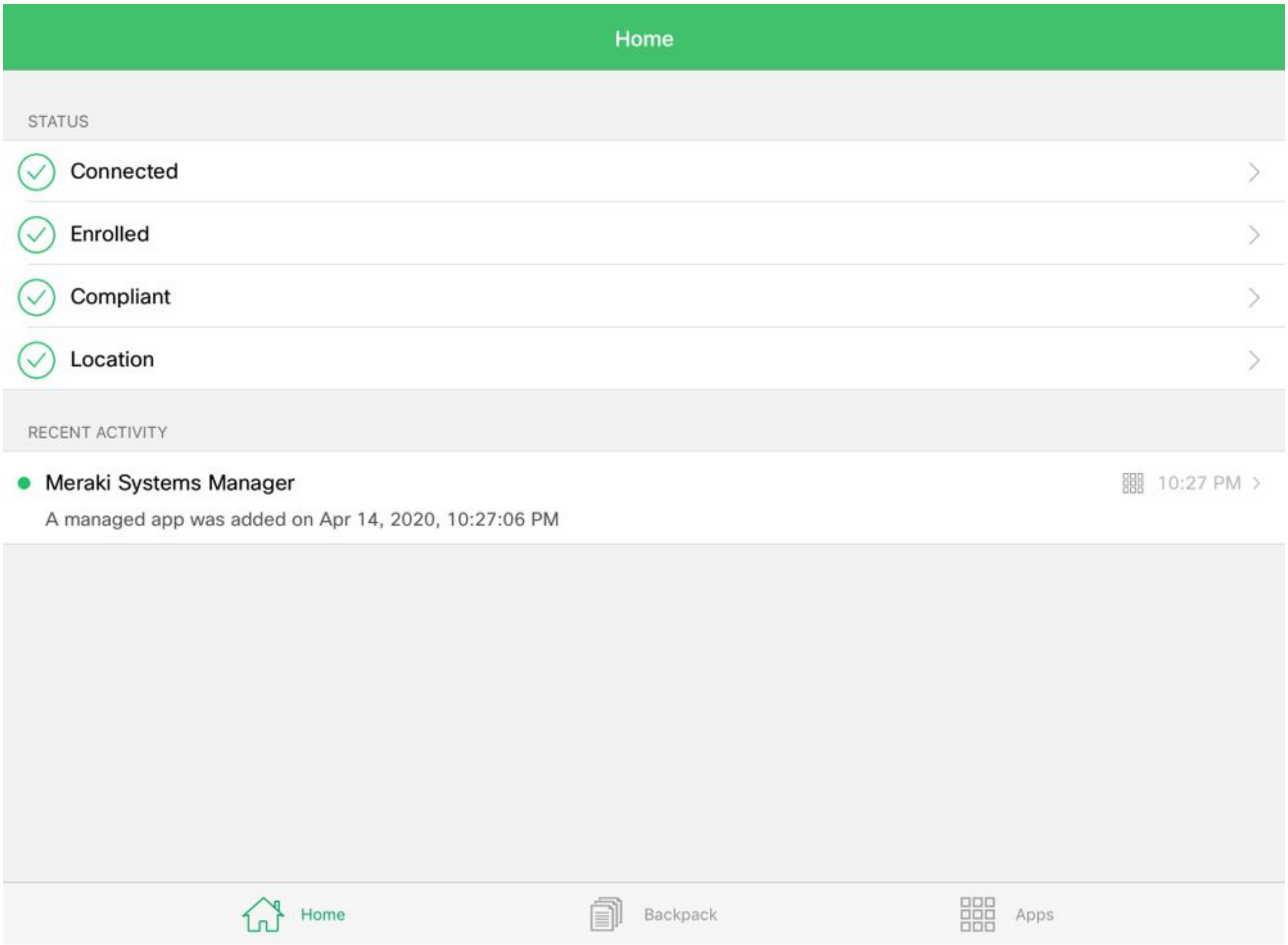
App Installation

"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.開啟位於主螢幕中的最近下載的應用程式Meraki MDM。



1.12.檢驗所有狀態是否都有一個綠色勾選標籤，以確認登記已完成。



Home

STATUS

Connected

Enrolled

Compliant

Location

RECENT ACTIVITY

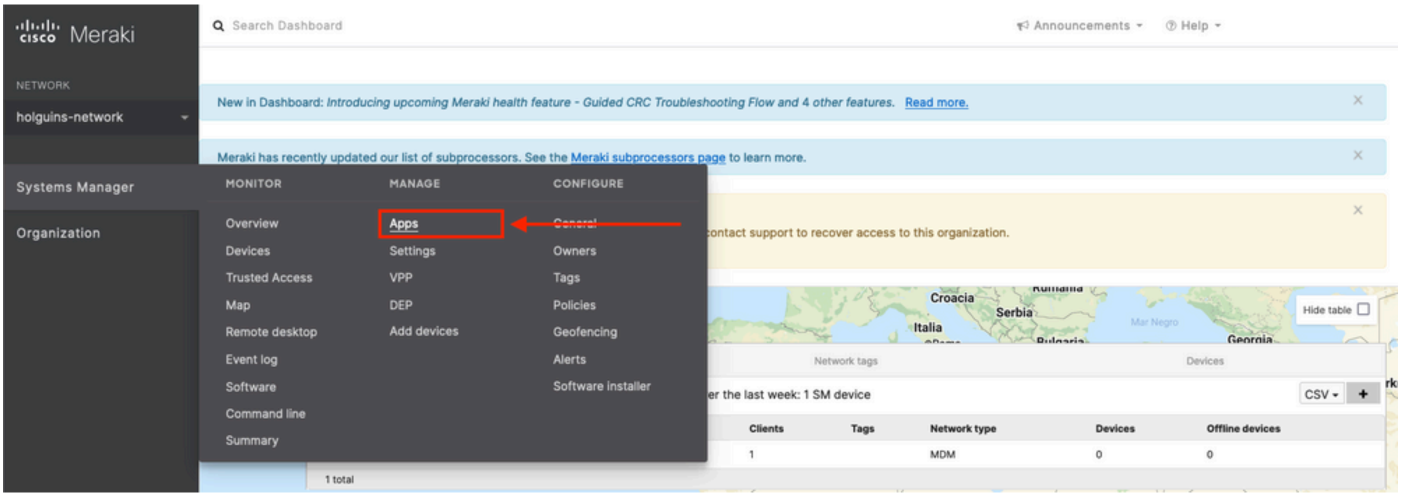
Meraki Systems Manager 10:27 PM

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

步驟2.設定託管應用

為了稍後在本文檔中設定PerApp的隧道應用，您需要通過SM管理這些相同的應用。在此配置示例中，Firefox旨在通過Per App進行隧道化，因此會將其新增到託管應用中。

2.1.導航到**Systems Manager > Manage > Apps**以新增託管應用。



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.

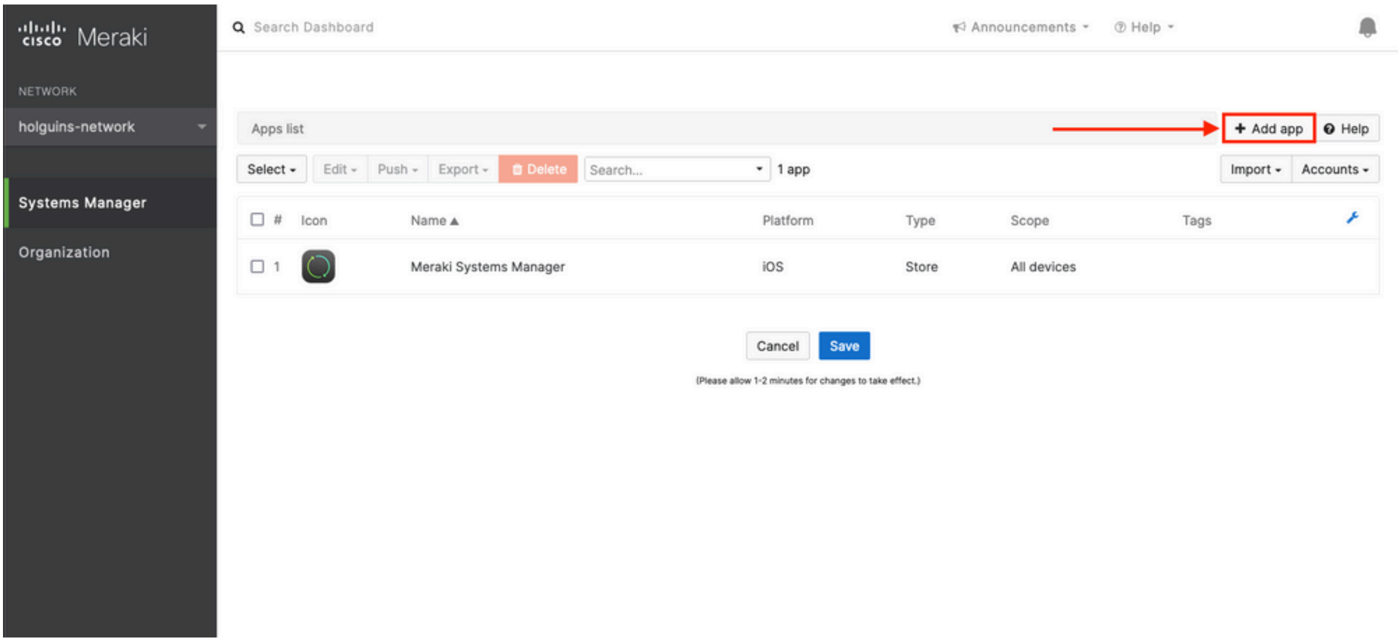
contact support to recover access to this organization.

er the last week: 1 SM device

Clients	Tags	Network type	Devices	Offline devices
1		MDM	0	0

1 total

2.2.選擇**Add app** 選項。

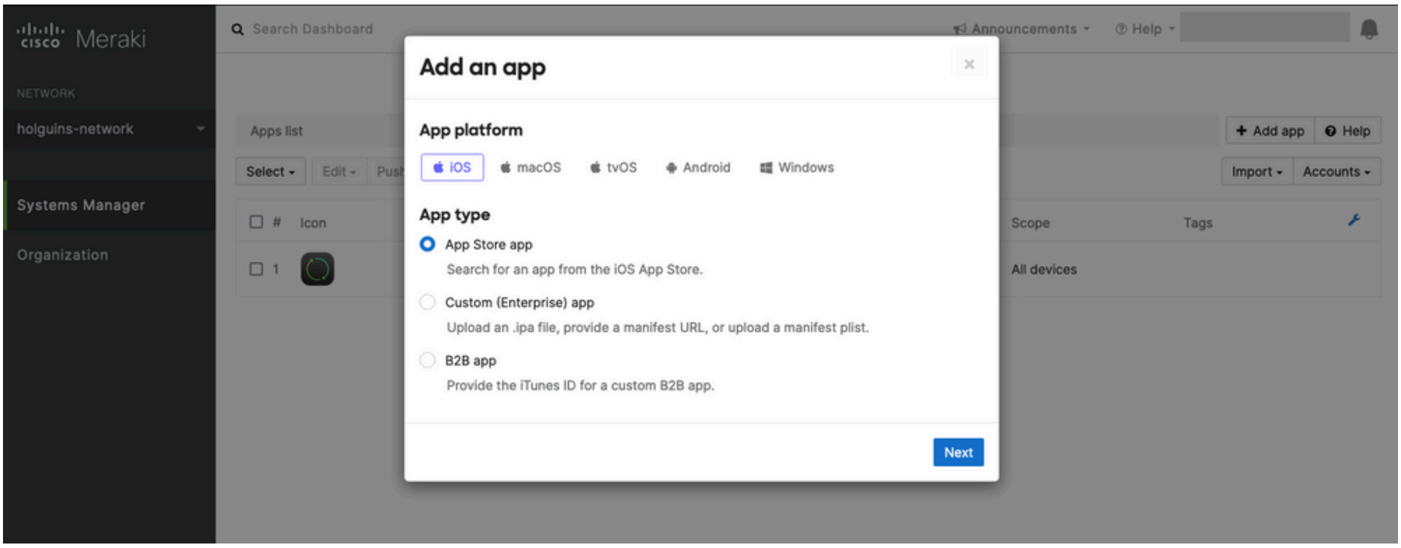


#	Icon	Name ▲	Platform	Type	Scope	Tags
1		Meraki Systems Manager	iOS	Store	All devices	

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

2.3.根據應用程式的儲存位置選擇應用程式的型別（App Store應用程式、自定義應用程式、B2B）。選擇後選擇**Next**。

在此示例中，應用會公開儲存在App Store中。

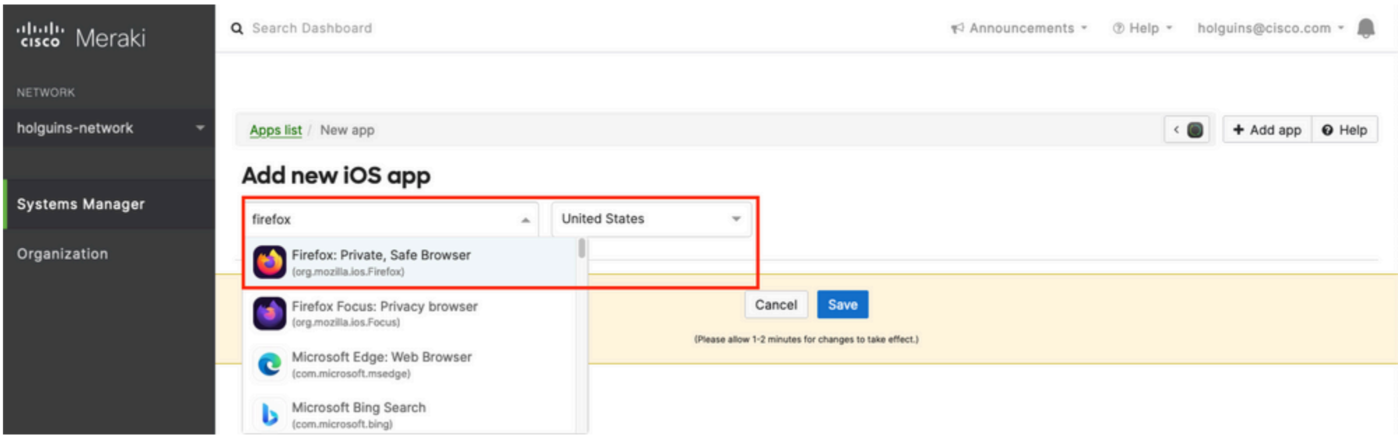


App type

- ● 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.出現提示時，搜尋所需的應用程式，並選擇從中下載應用程式的區域。選擇應用後選擇**Save**。

注意：如果國家/地區與Apple帳戶的區域不匹配，則使用者可能會遇到應用程式問題。



Add new iOS app

firefox | United States

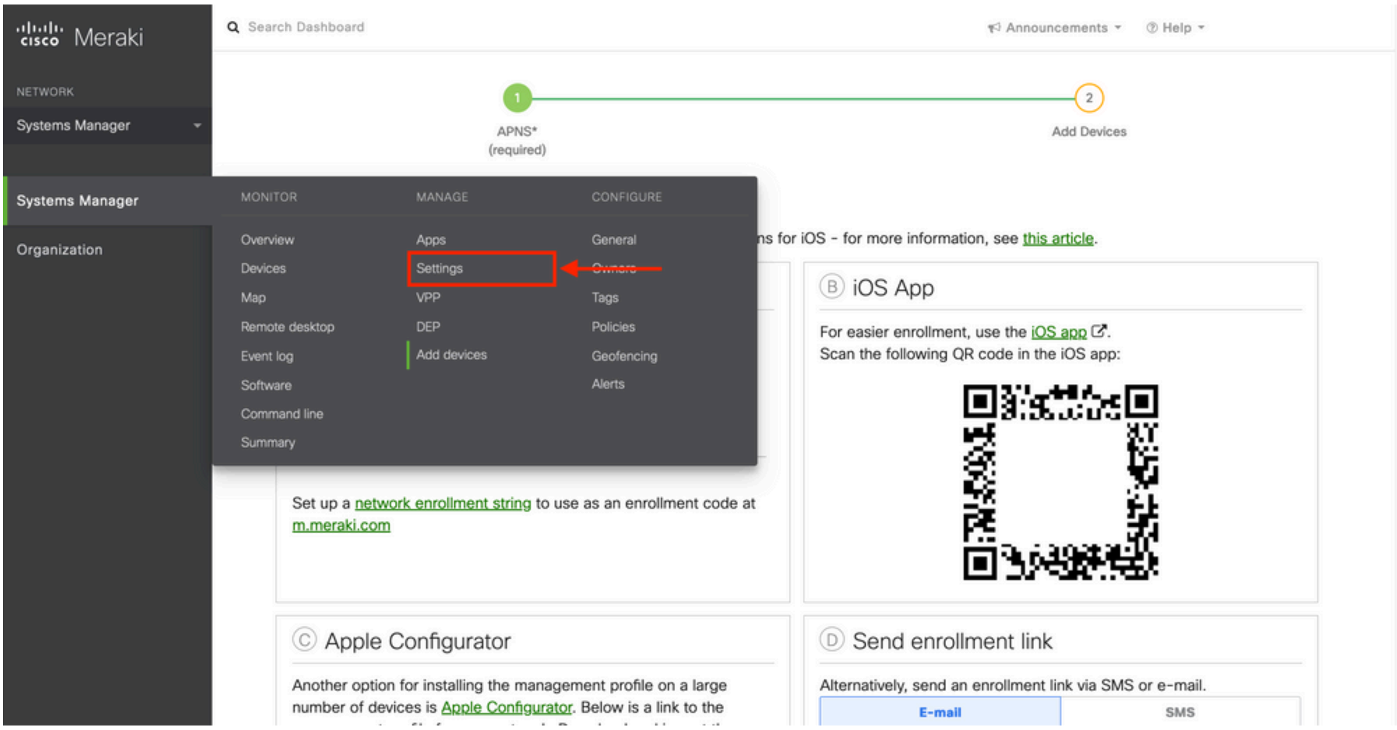
- Firefox: Private, Safe Browser (org.mozilla.ios.Firefox)
- Firefox Focus: Privacy browser (org.mozilla.ios.Focus)
- Microsoft Edge: Web Browser (com.microsoft.msedge)
- Microsoft Bing Search (com.microsoft.bing)

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

2.5.選擇所有所需的應用程式後，按一下Save。

步驟3.配置PerApp VPN配置檔案

3.1.導航到Systems Manager > Manage > Settings



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

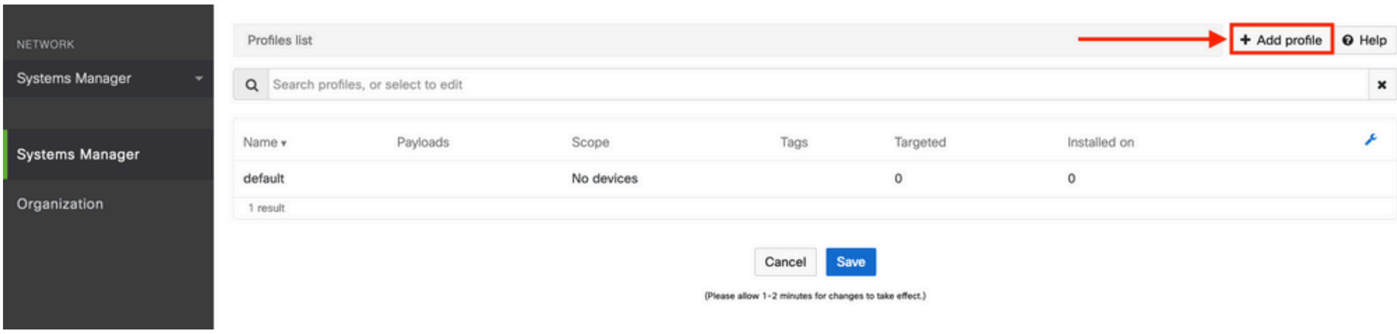
For easier enrollment, use the iOS app. Scan the following QR code in the iOS app:

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.選擇Add profile 選項。

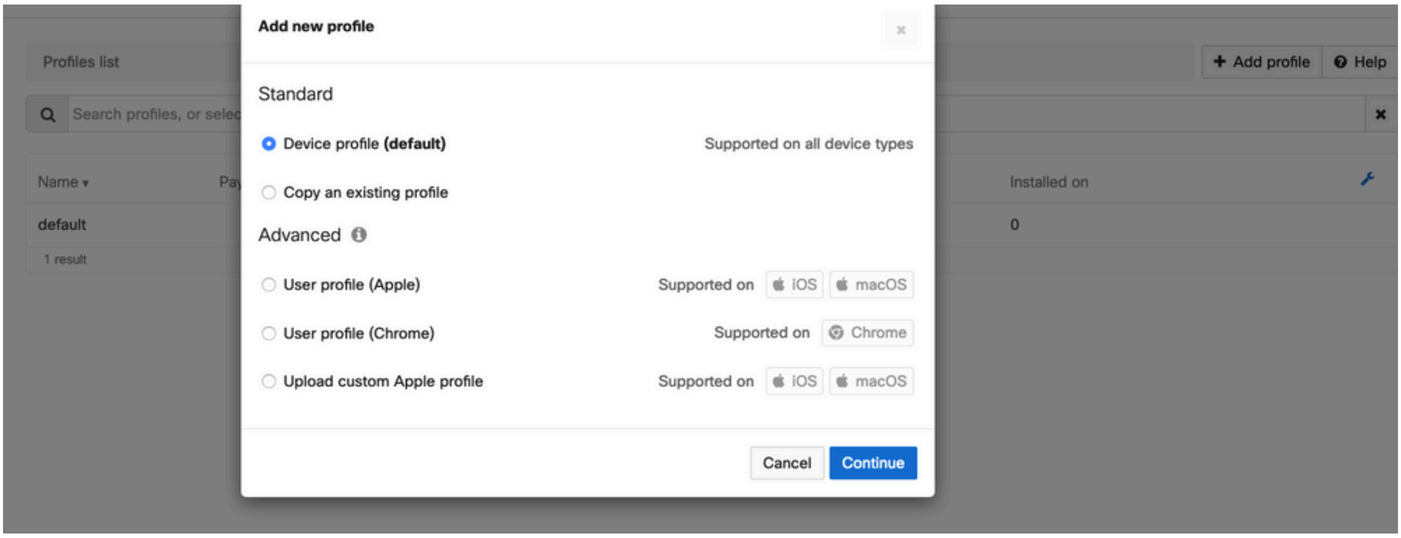


Name ▾	Payloads	Scope	Tags	Targeted	Installed on
default		No devices		0	0

1 result

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

3.3.選擇Device profile（預設）並按一下Continue。



Add new profile

Standard

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

○ Copy an existing profile

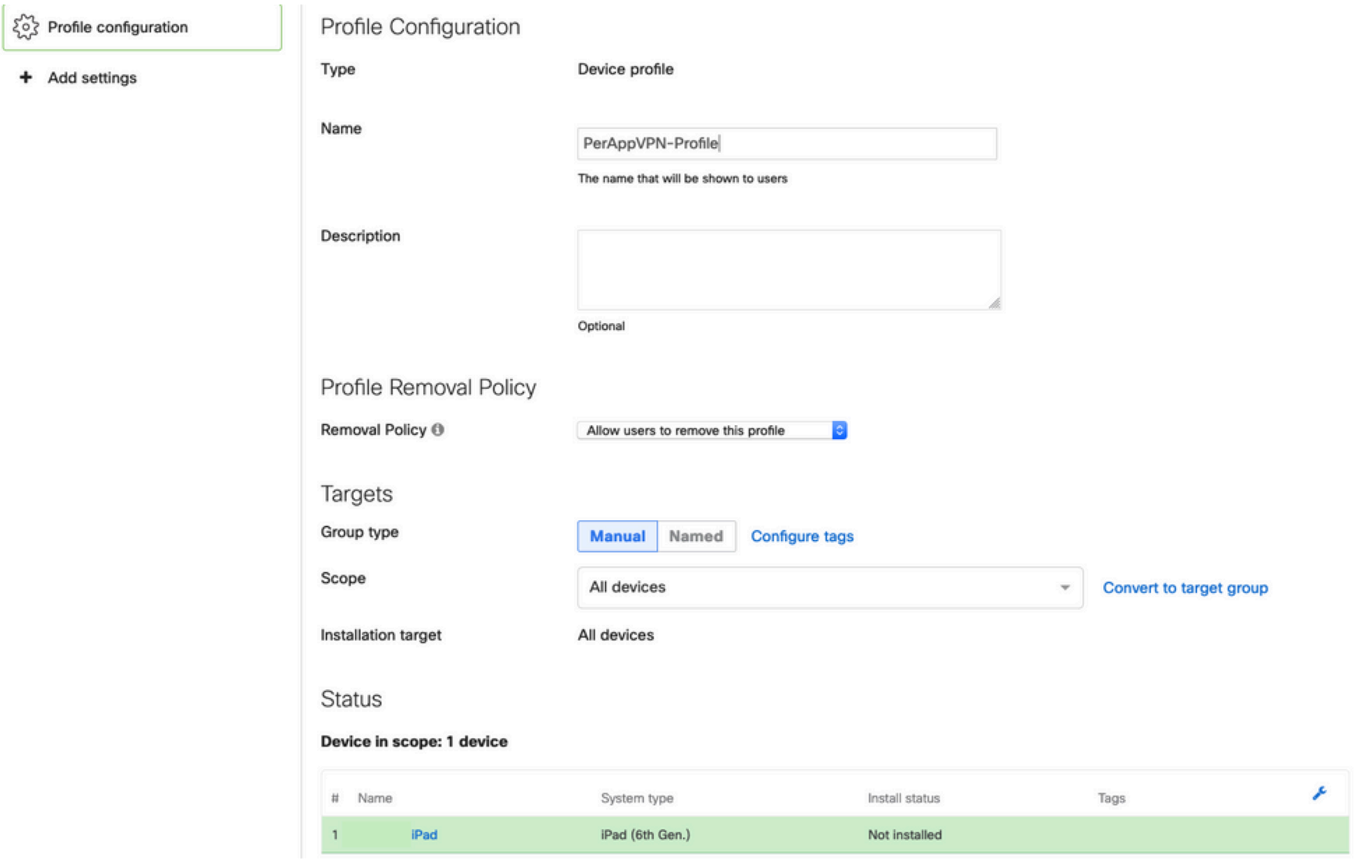
Advanced

○ User profile (Apple) — Supported on iOS macOS

○ User profile (Chrome) — Supported on Chrome

○ Upload custom Apple profile — Supported on iOS macOS

3.4.顯示**Profile Configuration**選單後，寫入**Name**，然後在**Scope**下選擇目標裝置。



Profile configuration

+ Add settings

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

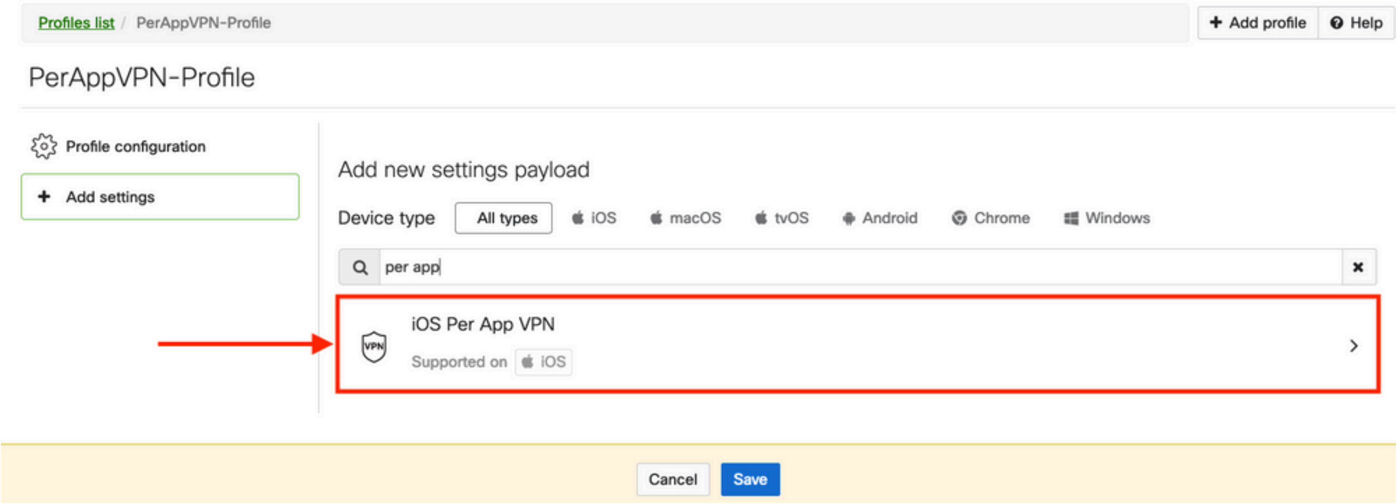
Installation target: All devices

Status

Device in scope: 1 device

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

3.5.選擇**Add settings**並按**iOS Per App VPN**過濾配置檔案型別，選擇如下所示的選項。



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

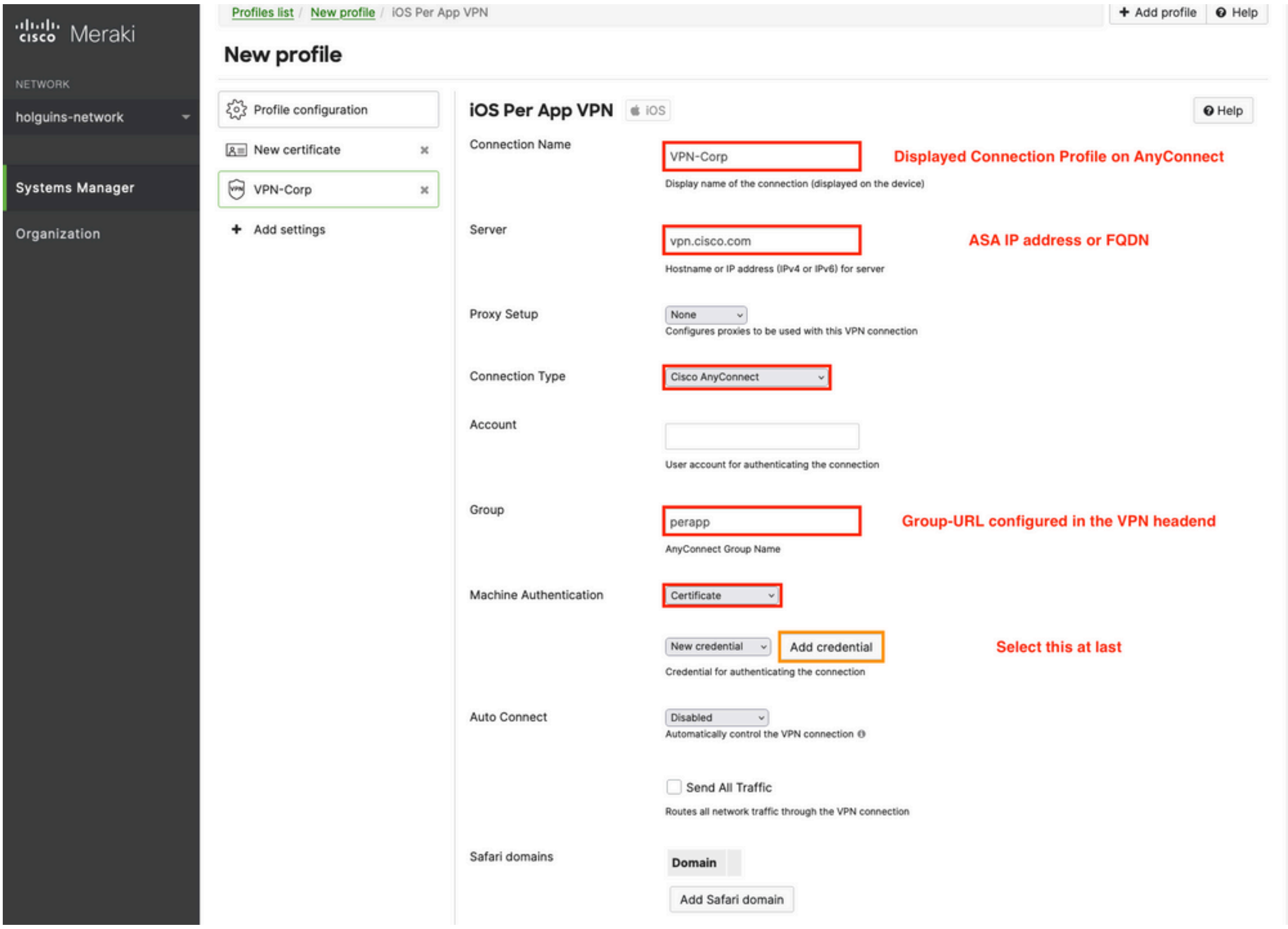
Supported on iOS

Cancel | Save

3.6.顯示選單後，根據以下示例編寫連線資訊。

Systems Manager支援這些連線的兩個證書註冊：SCEP和手動註冊。在此示例中，使用手動註冊。

> **注意**：一旦填滿文本框，請選擇**Add credential，因為此選項會將您帶到一個新選單以新增證書檔案。**



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

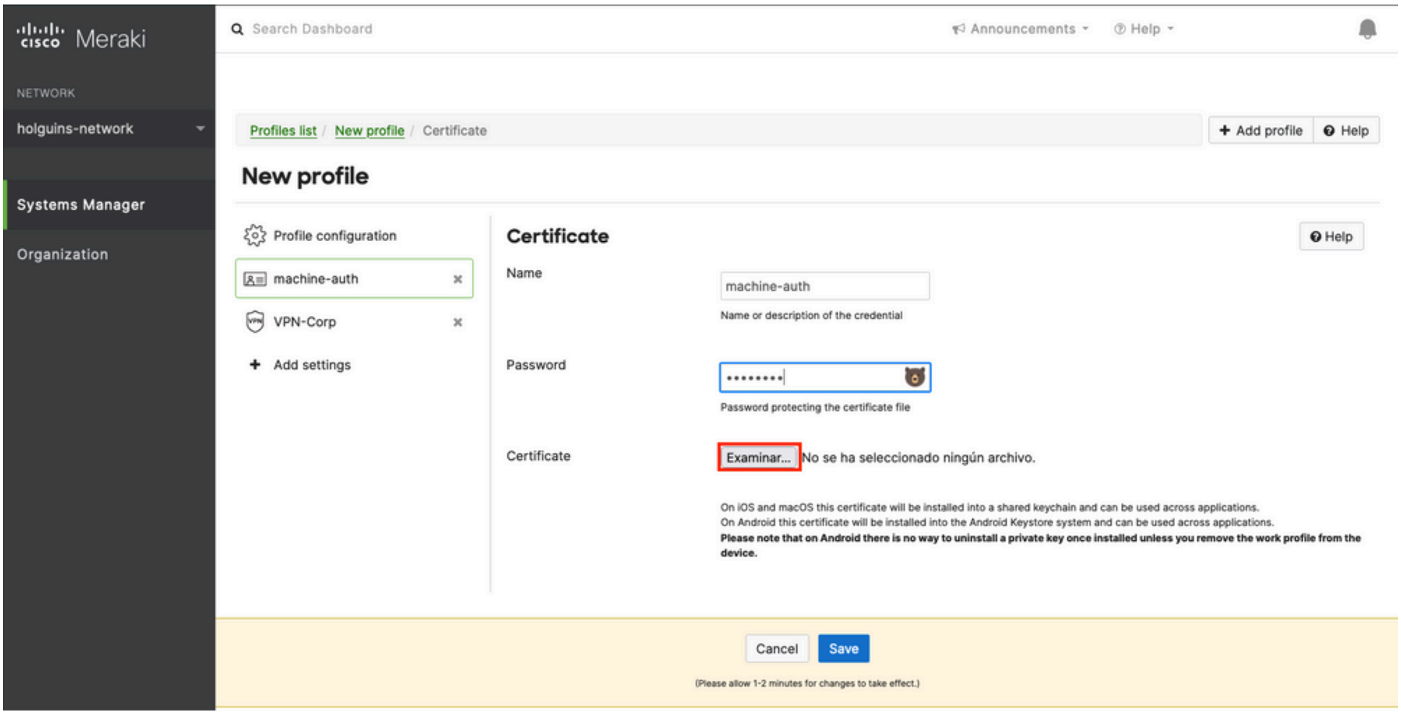
New credential — Add credential — Credential for authenticating the connection — Select this at last

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.按一下Add credential並重定向到「證書」選單後，請寫入證書的Name，在電腦中瀏覽並查詢保護.pfx檔案（加密證書檔案）的Password。



Name: machine-auth — Name or description of the credential

Password: •••••••• — Password protecting the certificate file

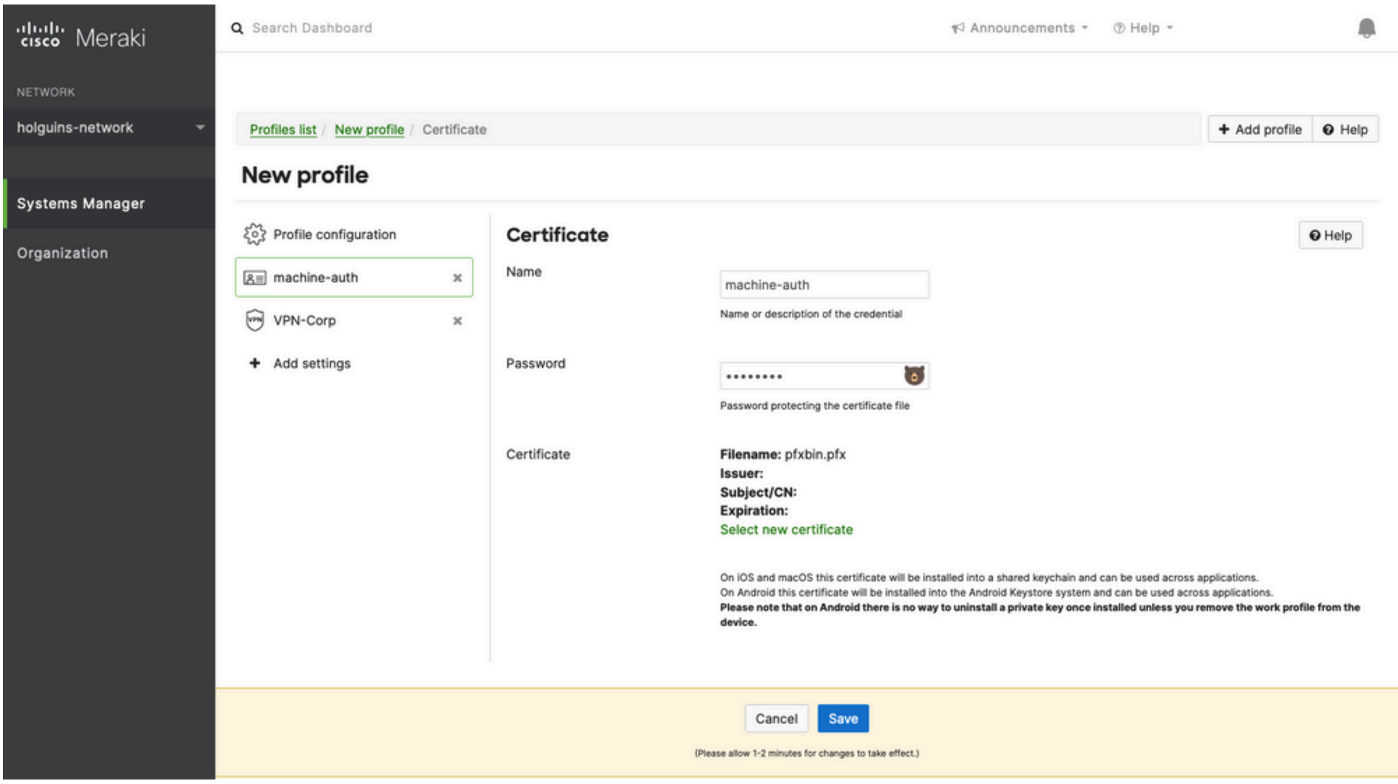
Certificate: Examinar... No se ha seleccionado ningún archivo.

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.

Cancel | Save

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

3.8.選擇證書後，將顯示證書檔名。



New profile

Certificate

Name: machine-auth

Name or description of the credential

Password: ••••••••

Password protecting the certificate file

Certificate

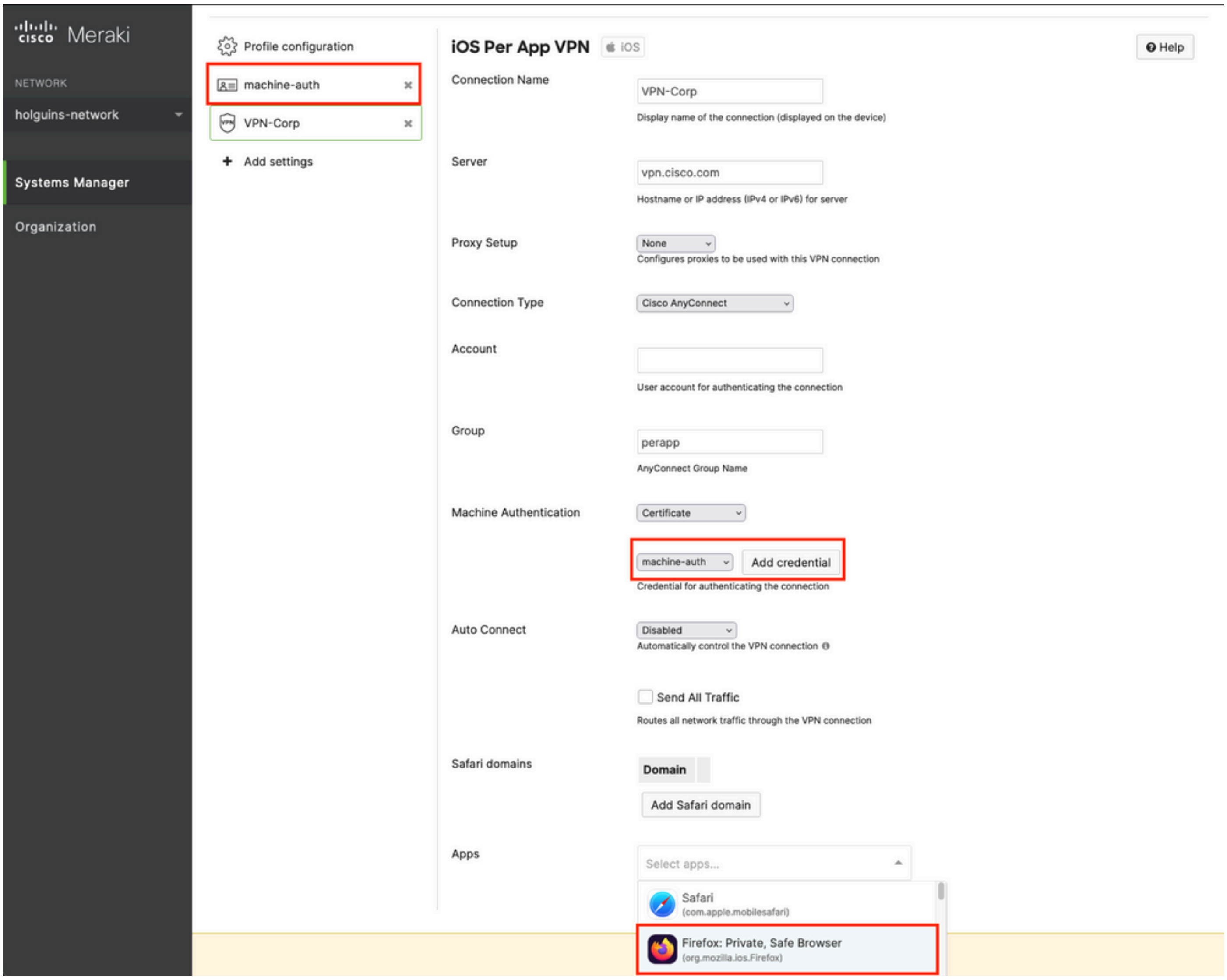
Filename: pfxbin.pfx
Issuer:
Subject/CN:
Expiration:
Select new certificate

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.選擇證書後，導航到您先前使用的VPN配置檔案，選擇最近匯入的憑證並選擇隧道應用（本例中為Firefox）。

完成此操作後，按一下**Save**。



iOS Per App VPN

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

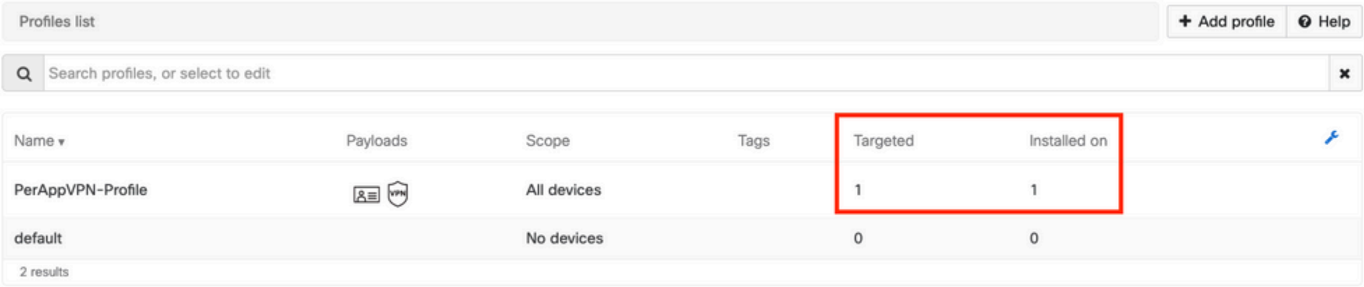
Auto Connect: Disabled
Automatically control the VPN connection

□ 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.驗證目標裝置上是否已安裝配置檔案。



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

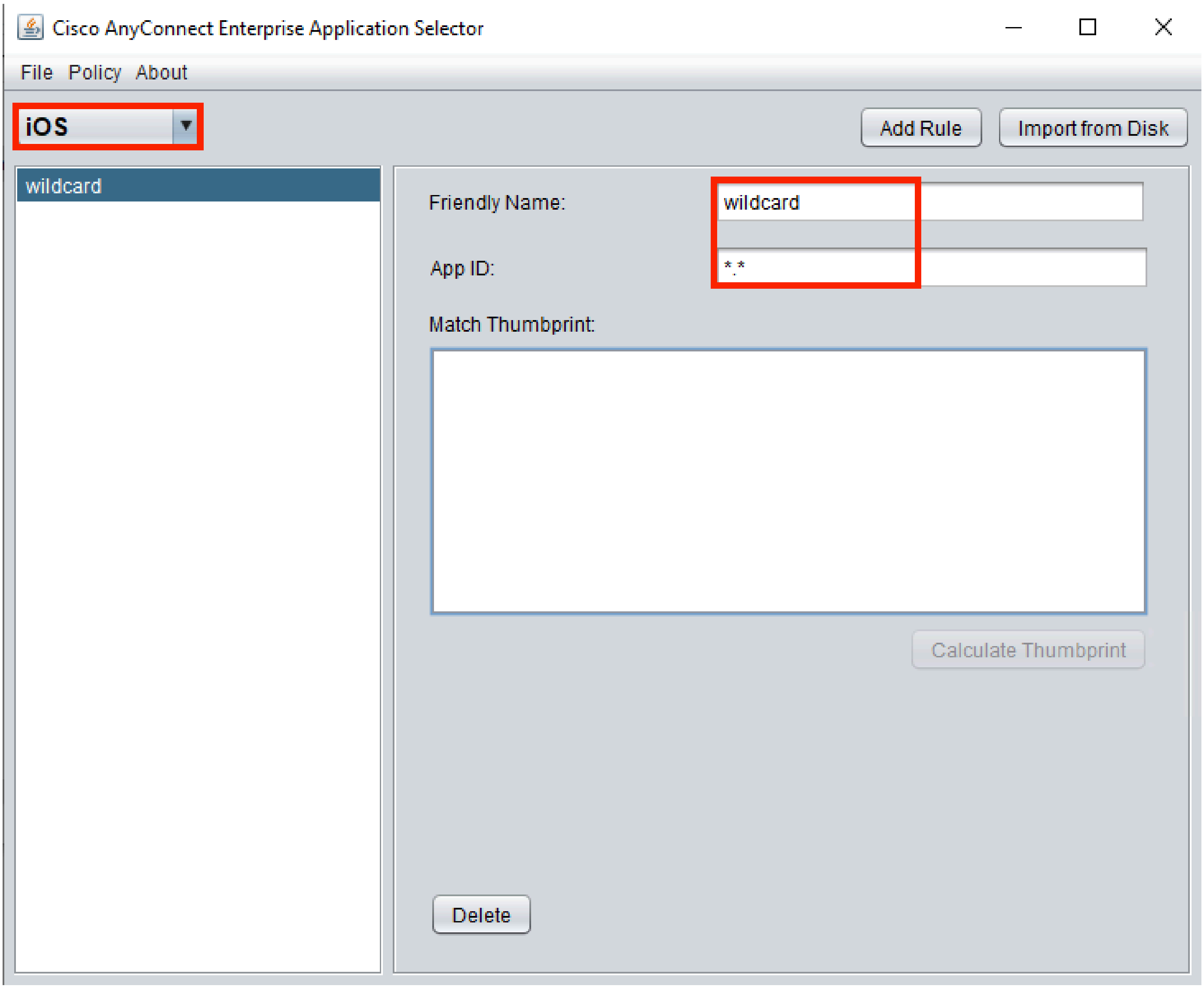
2 results

步驟4.應用選擇器配置

4.1.從思科網站下載應用選擇器
https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0

> **注意**：在Windows電腦上運行應用程式。在MacOS裝置上使用該工具時，顯示的結果不符合預期。

4.2.開啟java應用程式。從下拉選單中選擇**iOS**，新增一個友好名稱，並確保在**App ID**中鍵入***.***。



iOS

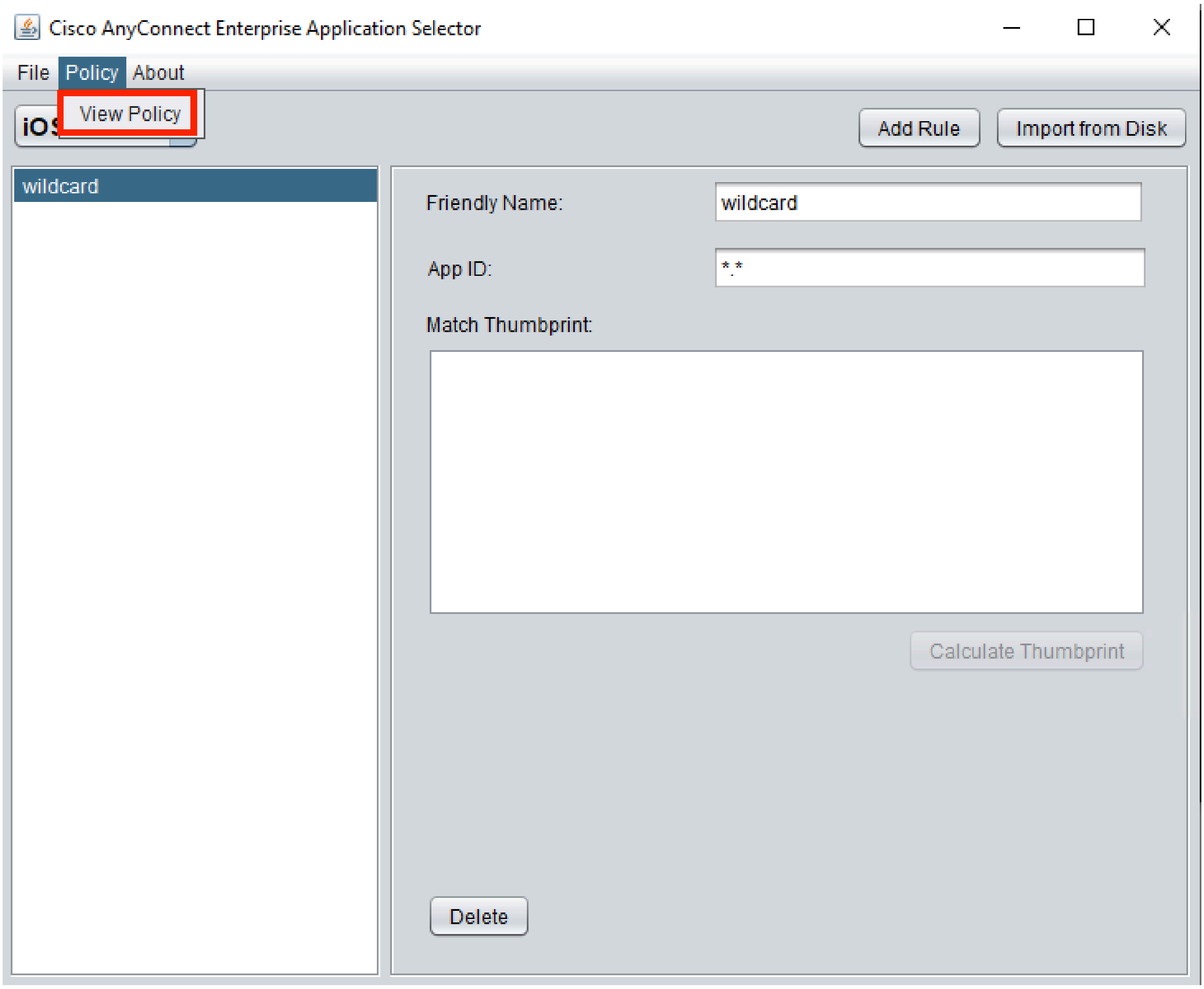
wildcard

Friendly Name: wildcard

App ID: *.*

Match Thumbprint:

4.3.導航到**Policy**，然後選擇**View Policy**



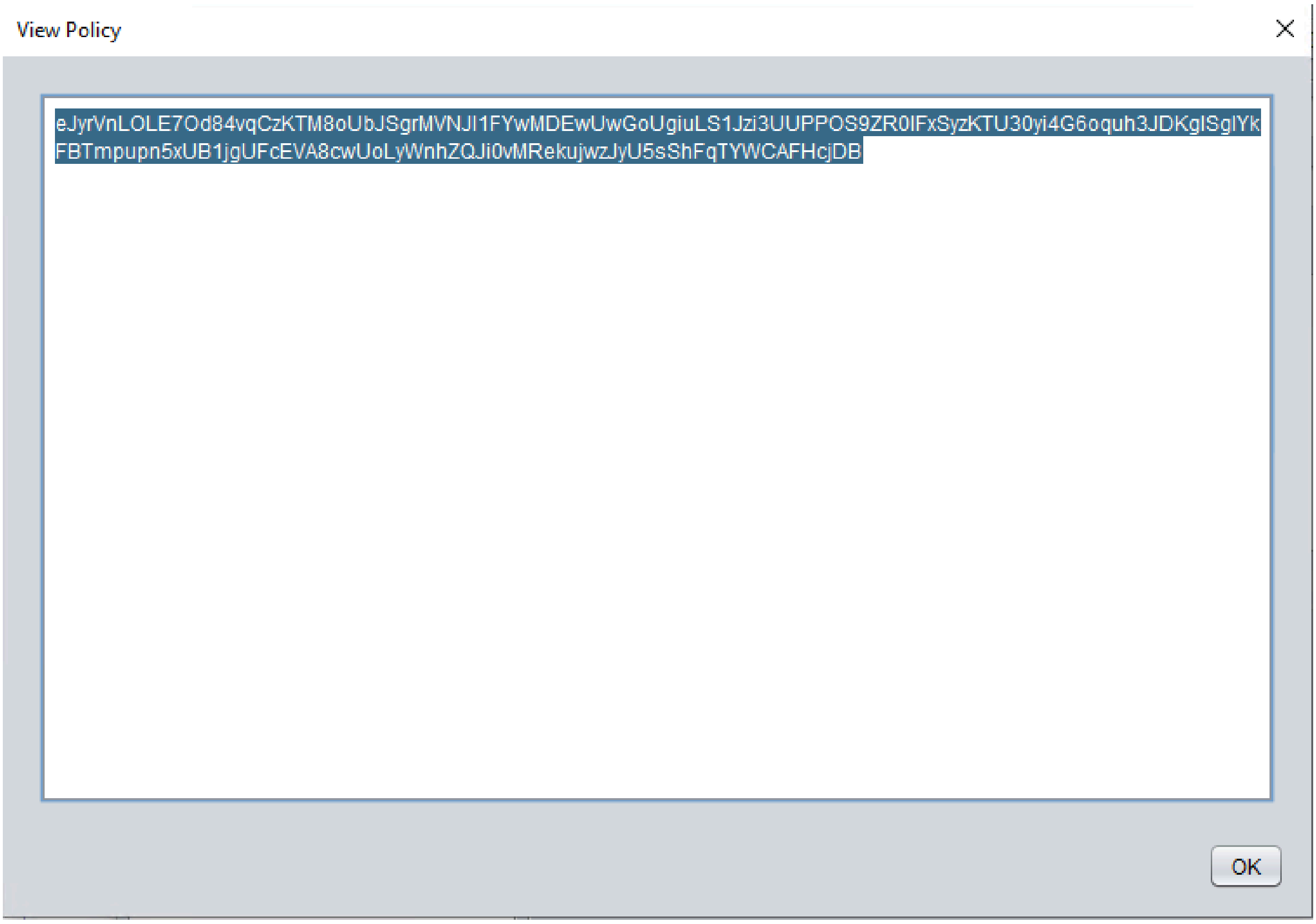
wildcard

Friendly Name: wildcard

App ID: *.*

Match Thumbprint:

4.4.複製顯示的字串。（稍後將在VPN頭端配置中使用此功能）。



View Policy

eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0lFxSyzKTU30yi4G6oquh3JDKglSgIYk
FBTmpupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB

步驟5.每個應用VPN配置的ASA示例

```
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
```

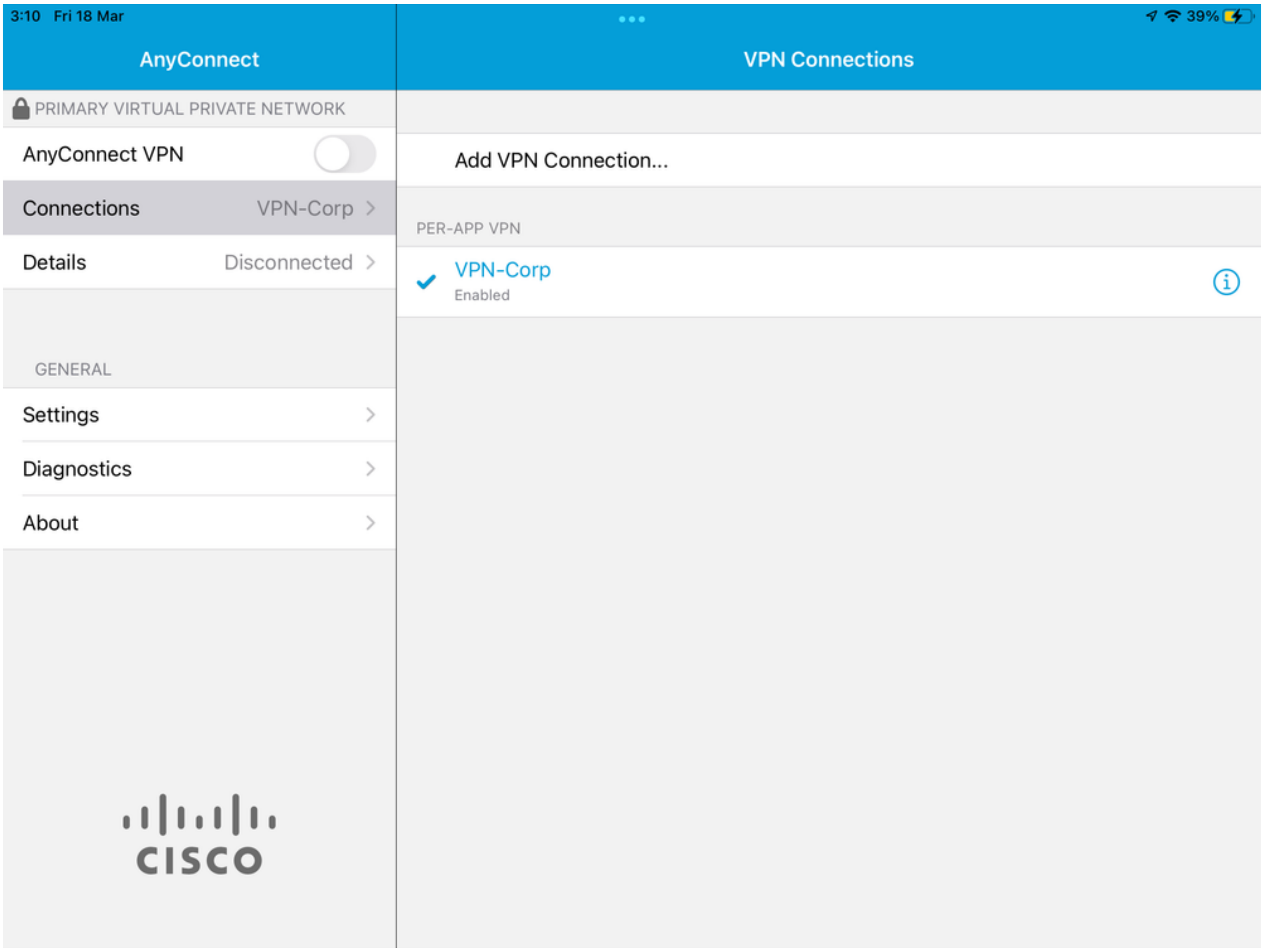
```
group-url https://vpn.cisco.com/perapp enable
```

驗證

6.驗證AnyConnect應用程式上的配置檔案安裝

6.1.開啟AnyConnect應用程式，然後在左側窗格中選擇**Connections**。PerApp VPN配置檔案必須顯示在名為**PER-APP VPN**的新部分下。

選擇**i**以顯示高級設定。



3:10 Fri 18 Mar

39%

AnyConnect

VPN Connections

PRIMARY VIRTUAL PRIVATE NETWORK

AnyConnect VPN

Connections VPN-Corp >

Details Disconnected >

GENERAL

Settings >

Diagnostics >

About >

Add VPN Connection...

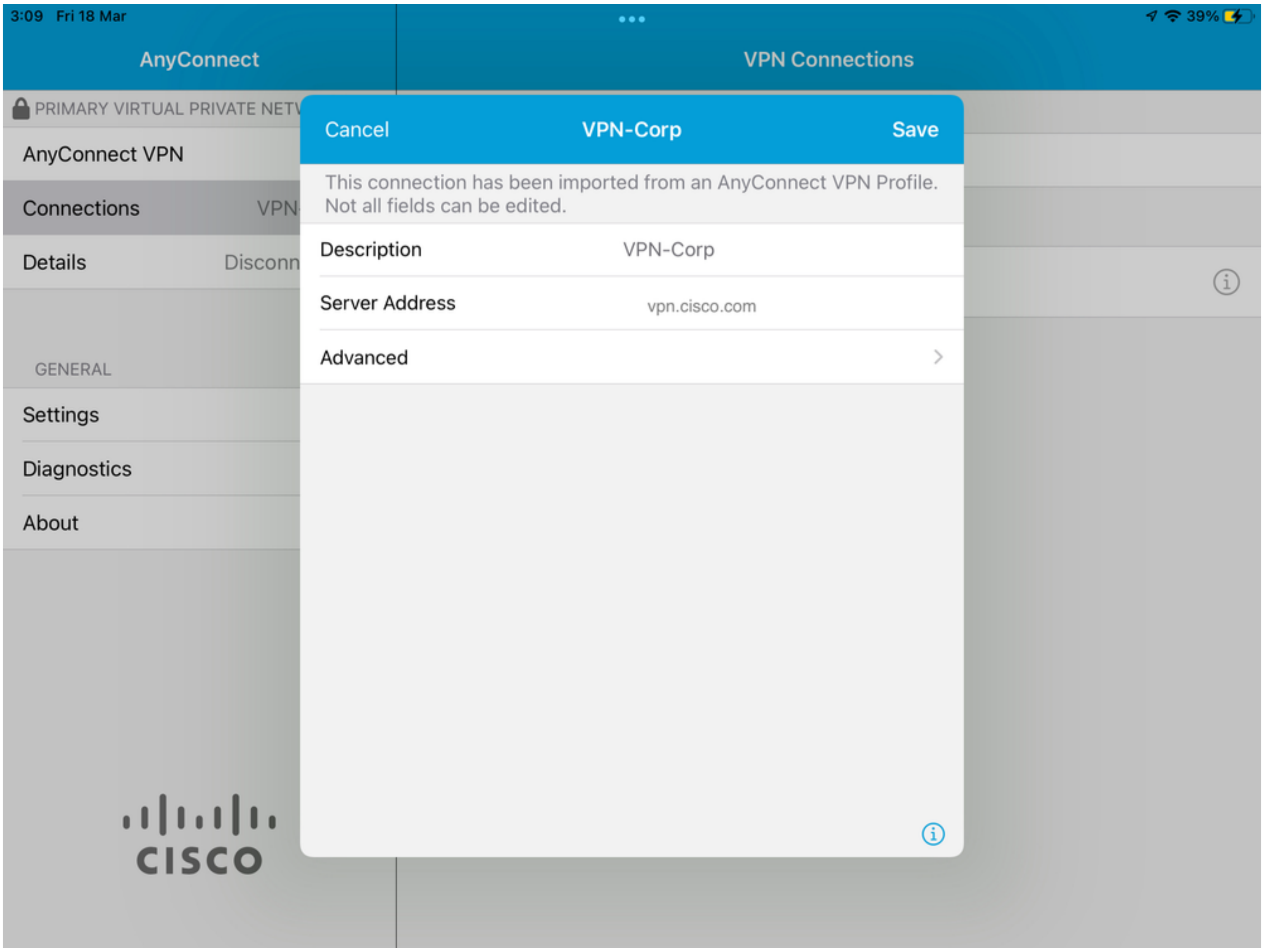
PER-APP VPN

✓ VPN-Corp

Enabled

ⓘ

6.2.選擇**Advanced**選項。



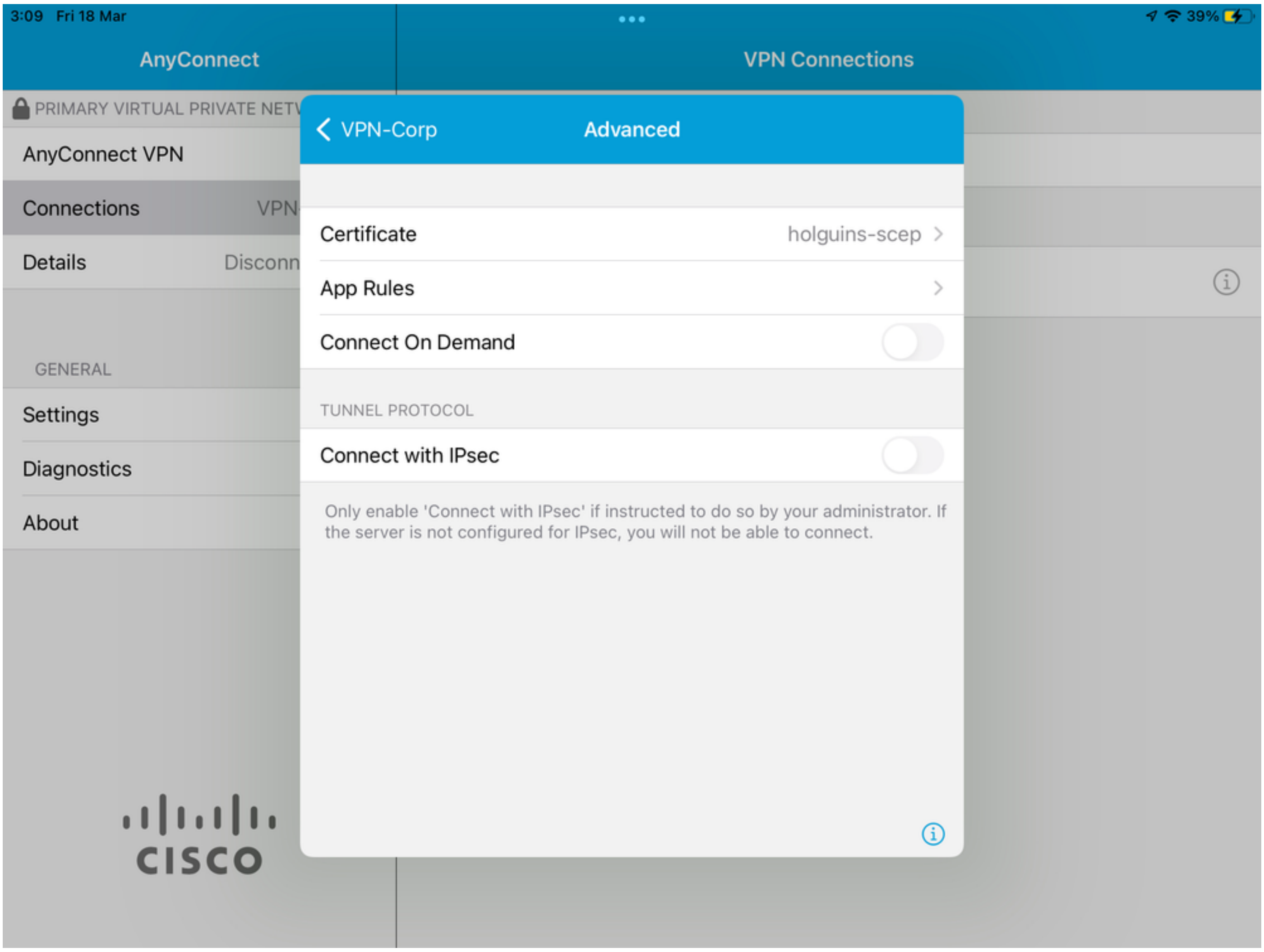
This connection has been imported from an AnyConnect VPN Profile. Not all fields can be edited.

Description VPN-Corp

Server Address vpn.cisco.com

Advanced

6.3.選擇**App Rules**選項。



Certificate holguins-scep

App Rules

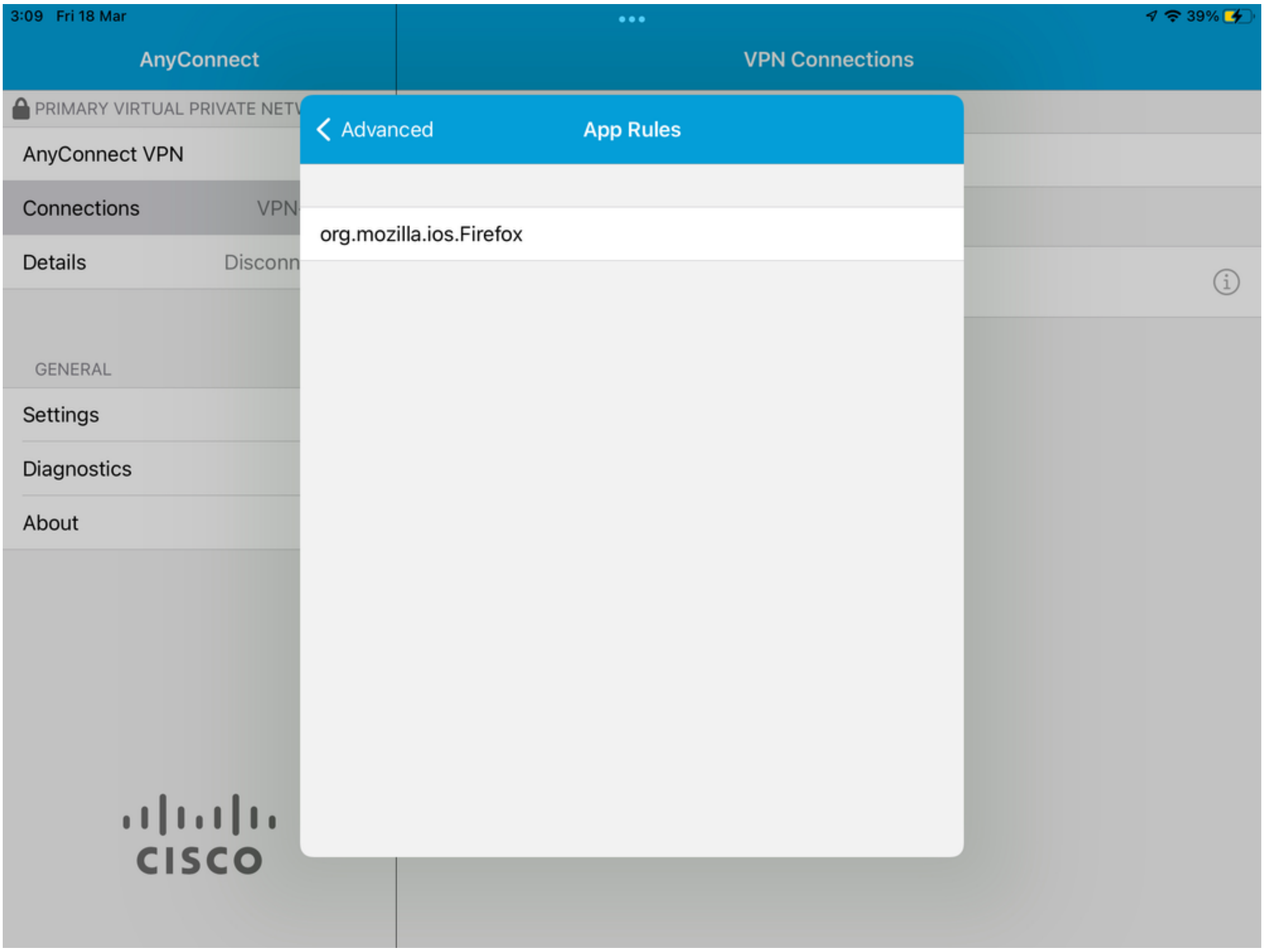
Connect On Demand

TUNNEL PROTOCOL

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.最後，確認已安裝應用規則。（Mozilla是本文檔中所需的隧道化應用，因此應用安裝成功）。



org.mozilla.ios.Firefox

疑難排解

目前沒有適用於本文的具體疑難排解步驟。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。