

Meraki System Manager를 사용하여 iOS용 Anyconnect PerApp VPN 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. Meraki Systems Manager에 iOS 디바이스 등록](#)

[2단계. 관리되는 앱 설정](#)

[3단계. PerApp VPN 프로파일 구성](#)

[4단계. 앱 선택기 컨피그레이션](#)

[5단계. ASA 샘플 퍼 앱\(Per App\) VPN 구성](#)

[다음을 확인합니다.](#)

[6. AnyConnect 애플리케이션에서 프로파일 설치 확인](#)

[문제 해결](#)

소개

이 문서에서는 Meraki MDM(Mobile Device Manager), SM(System Manager)에서 관리하는 Apple iOS 디바이스에서 PerApp VPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- AnyConnect v4.0 Plus 또는 Apex 라이선스.
- 퍼 앱(Per App) VPN을 지원하는 ASA 9.3.1 이상
- Cisco Enterprise Application Selector 툴: Cisco.com

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

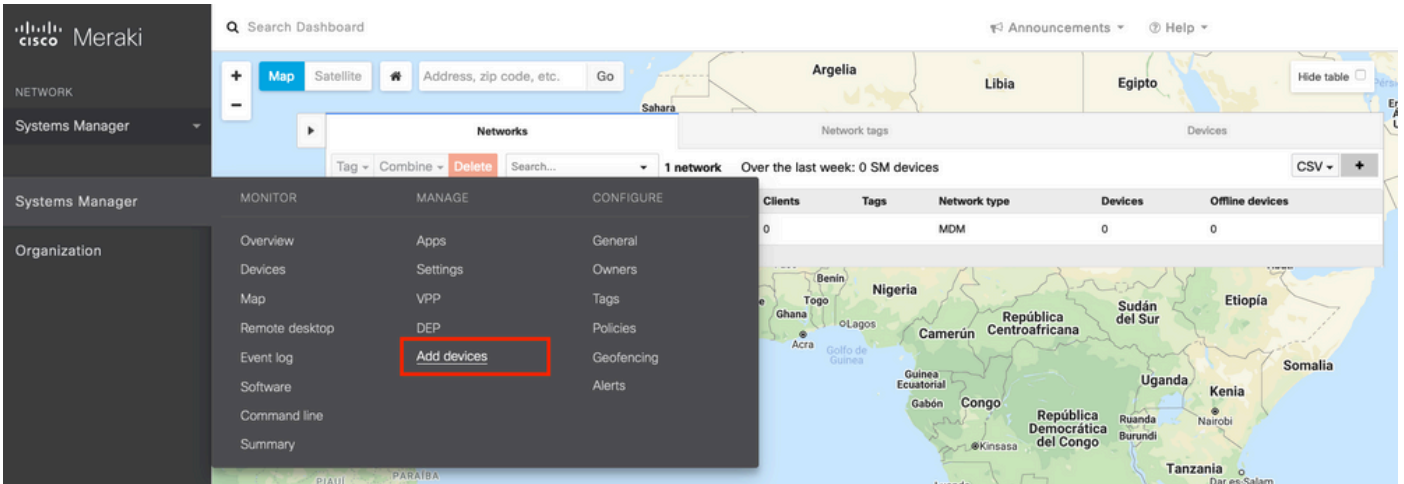
이 문서에는 나열된 프로세스는 포함되지 않습니다.

- 클라이언트 인증서 생성을 위한 Systems Manager의 SCEP CA 컨피그레이션
- iOS 클라이언트에 대한 PKCS12 클라이언트 인증서 생성

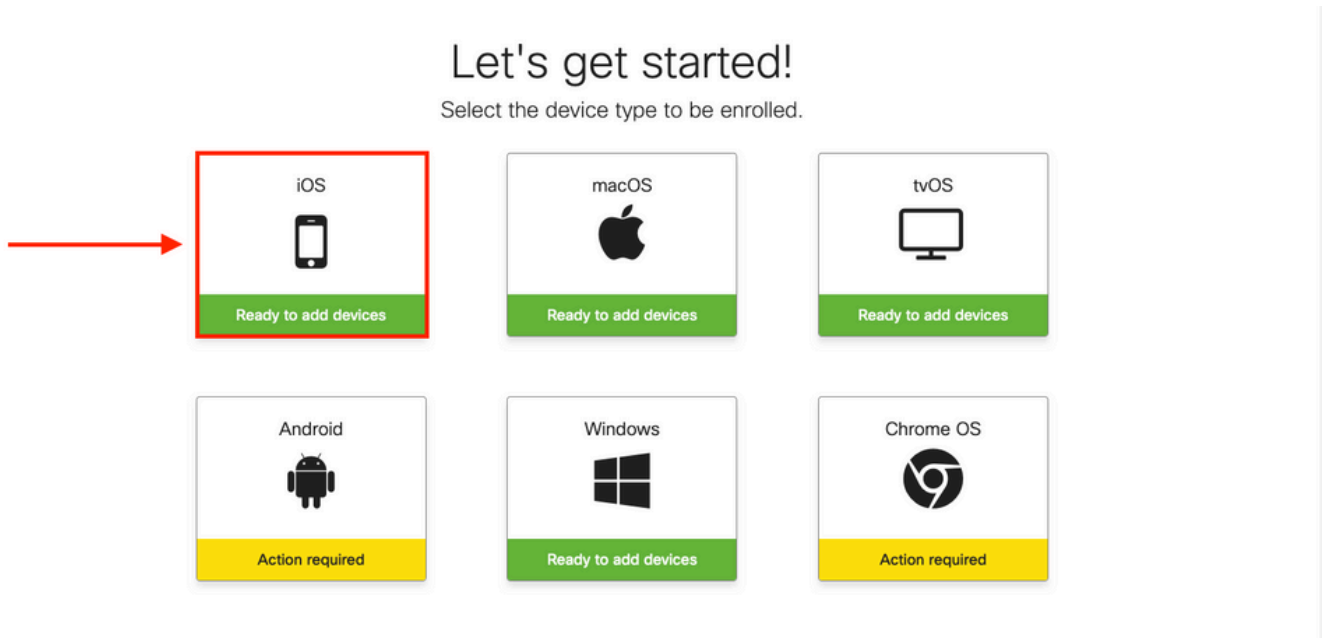
구성

1단계. Meraki Systems Manager에 iOS 디바이스 등록

1.1. Systems Manager > Add Devices(디바이스 추가)로 이동합니다



1.2. iOS 옵션을 클릭하여 등록을 시작합니다.



1.3. 인터넷 브라우저를 통해 장치를 등록하거나 카메라로 QR 코드를 스캔합니다. 본 문서에서는 등록 과정에 카메라를 사용하였습니다.

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 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

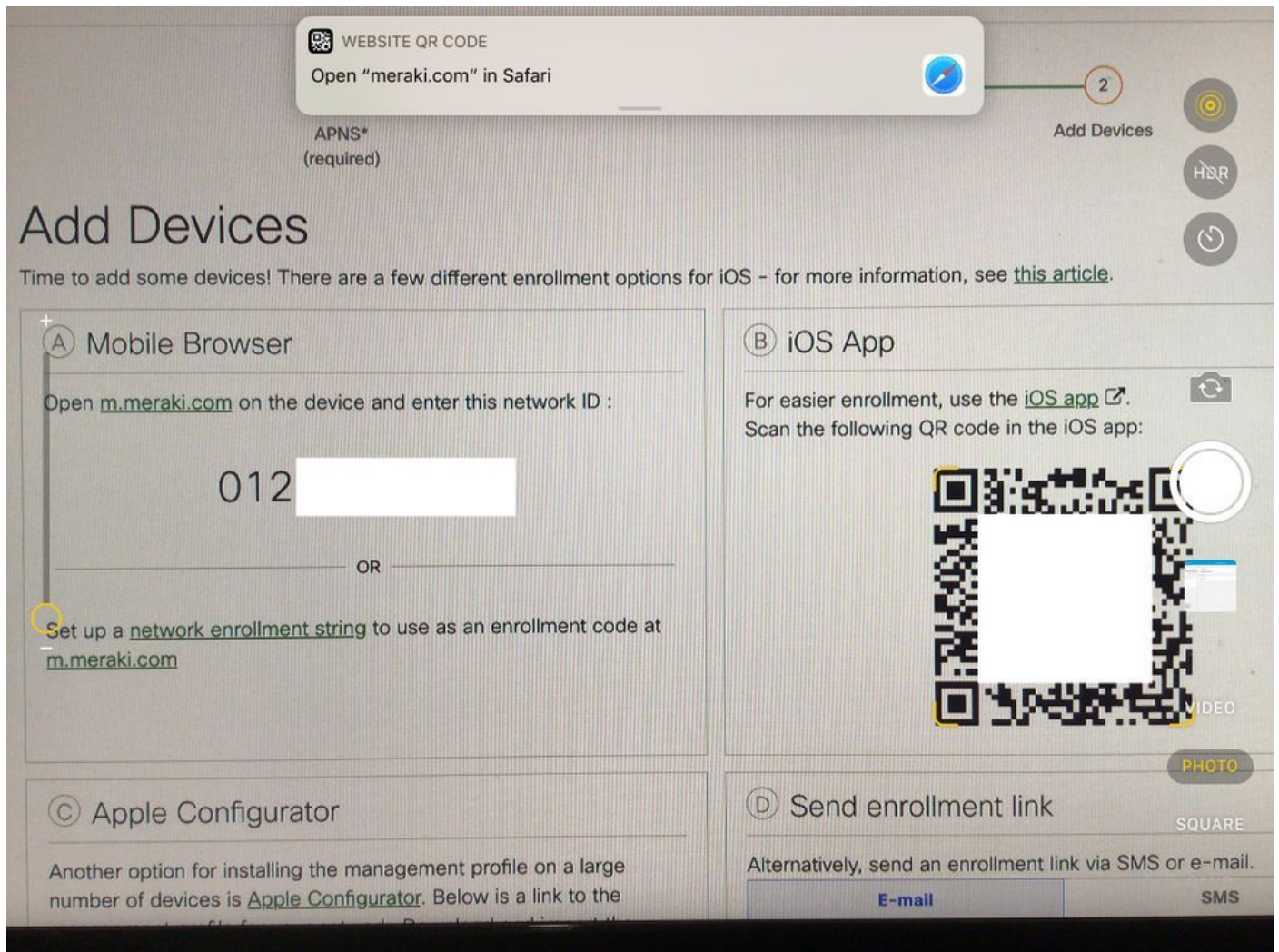
B iOS App

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

Scan the following QR code in the iOS app:



1.4. 카메라에서 QR 코드를 인식하면 Safari 알림에서 팝업되는 Open "meraki.com"을 선택합니다.



The screenshot shows the 'Add Devices' screen on an iPhone. At the top, a Safari notification bubble says 'WEBSITE QR CODE' and 'Open "meraki.com" in Safari'. Below the notification, the 'Add Devices' screen is visible. It has a '1' next to 'APNS* (required)' and a '2' next to 'Add Devices'. The screen is divided into four sections: 'A Mobile Browser', 'B iOS App', 'C Apple Configurator', and 'D Send enrollment link'. In the 'A Mobile Browser' section, the network ID '012' is partially obscured by a white box. In the 'B iOS App' section, a QR code is shown with a camera icon overlaid on it. In the 'D Send enrollment link' section, there are buttons for 'E-mail' and 'SMS'. The 'PHOTO' button is also visible at the bottom right.

1.5. 프롬프트가 표시되면 등록을 선택합니다.

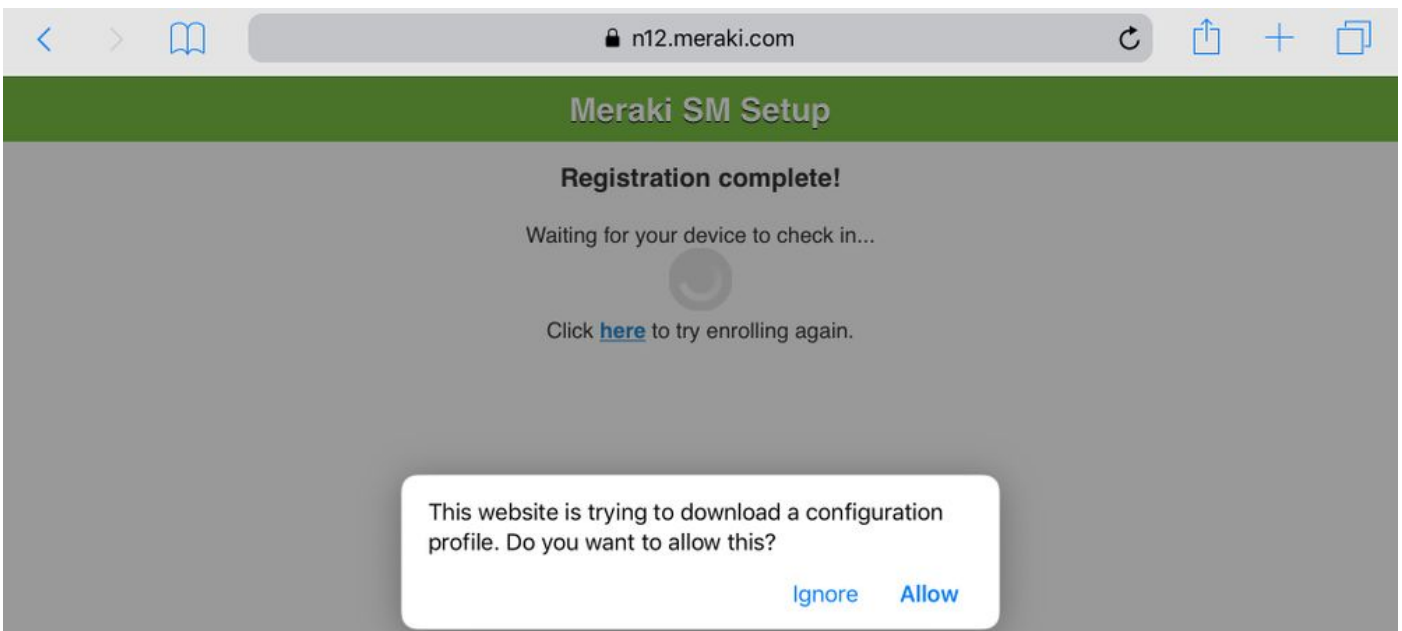


Step 1: Enter your Network ID

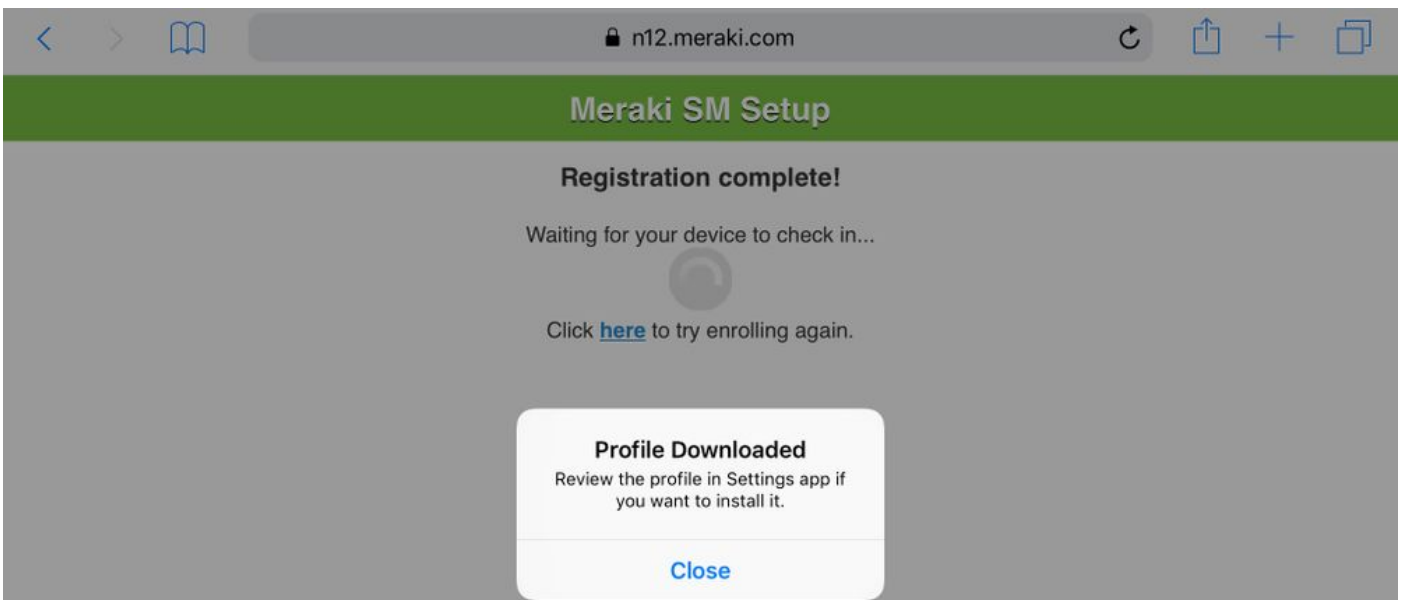
The Network ID is either a 10-digit code or a combination of letters, numbers, or characters (e.g. [123-456-7890](#) or network-id).

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

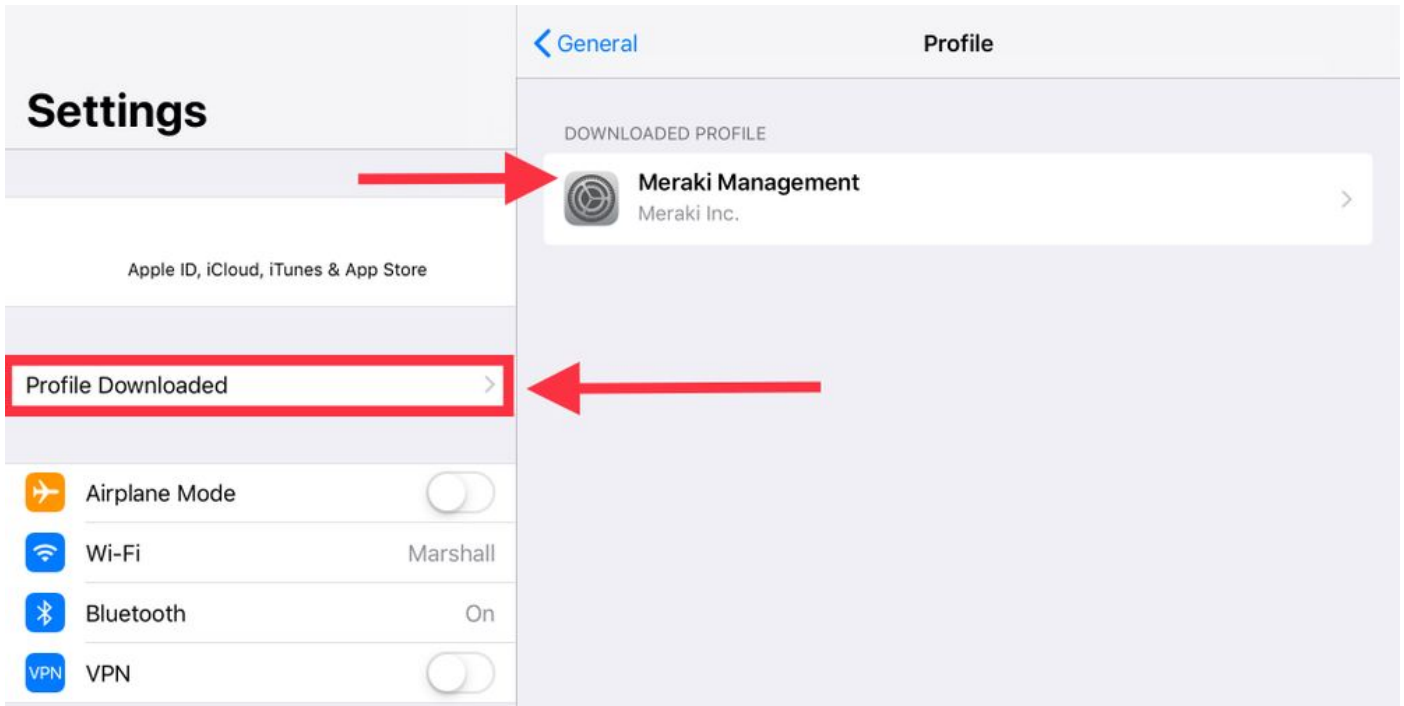
1.6. 장치가 MDM 프로필을 다운로드 할 수 있도록 하려면 Allow(허용)를 선택합니다.



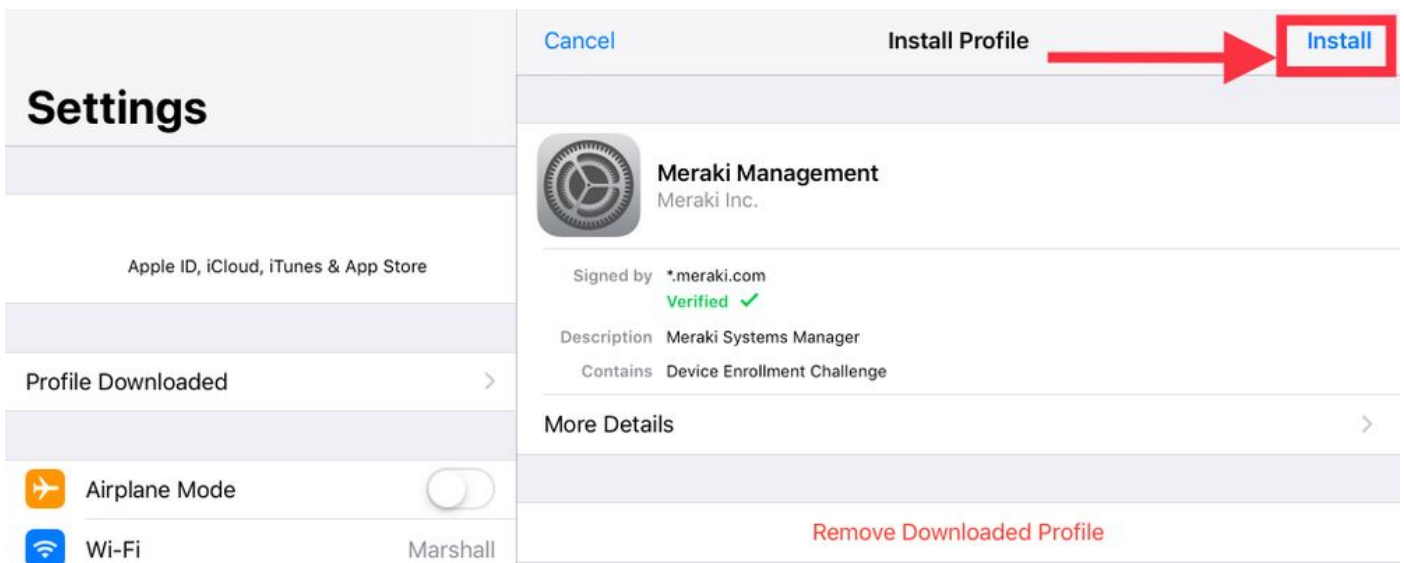
1.7. [닫기]를 선택하여 다운로드를 완료합니다.



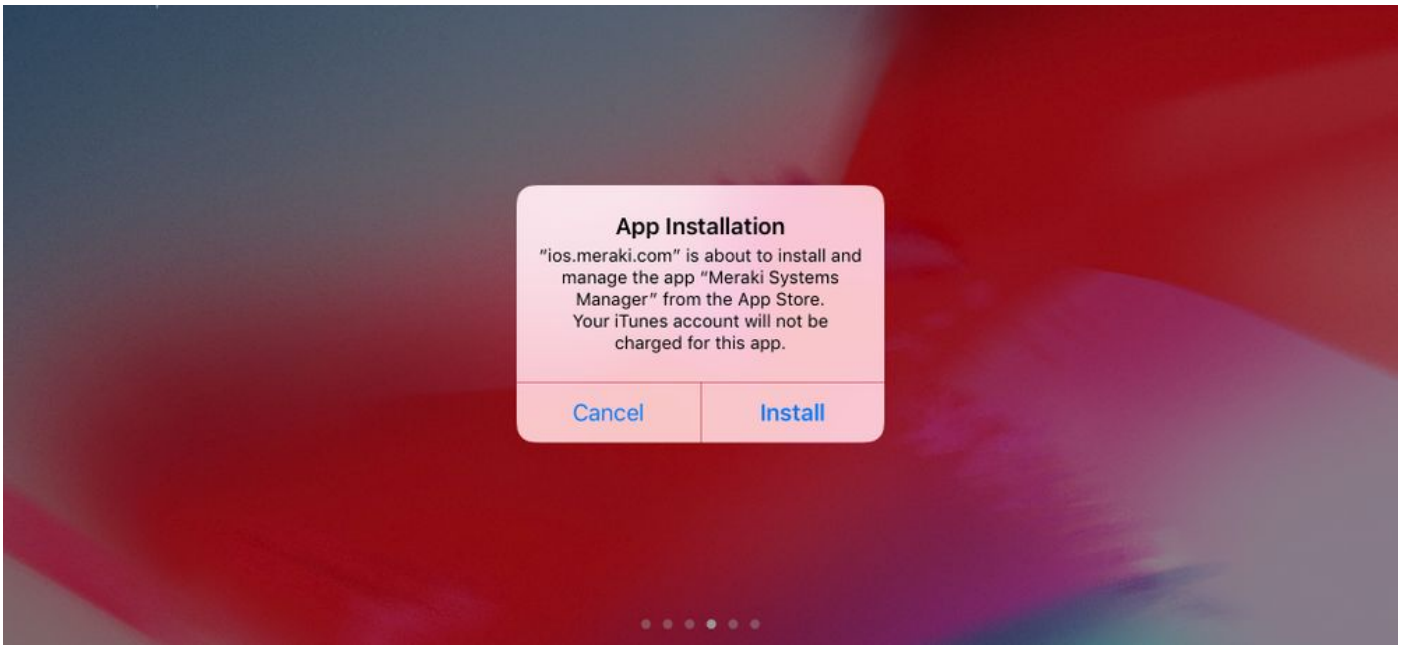
1.8. iOS 설정 앱으로 이동하여 왼쪽 창에서 **Profile Downloaded(프로필 다운로드)** 옵션을 찾은 다음 **Meraki Management(Meraki 관리)** 섹션을 선택합니다.



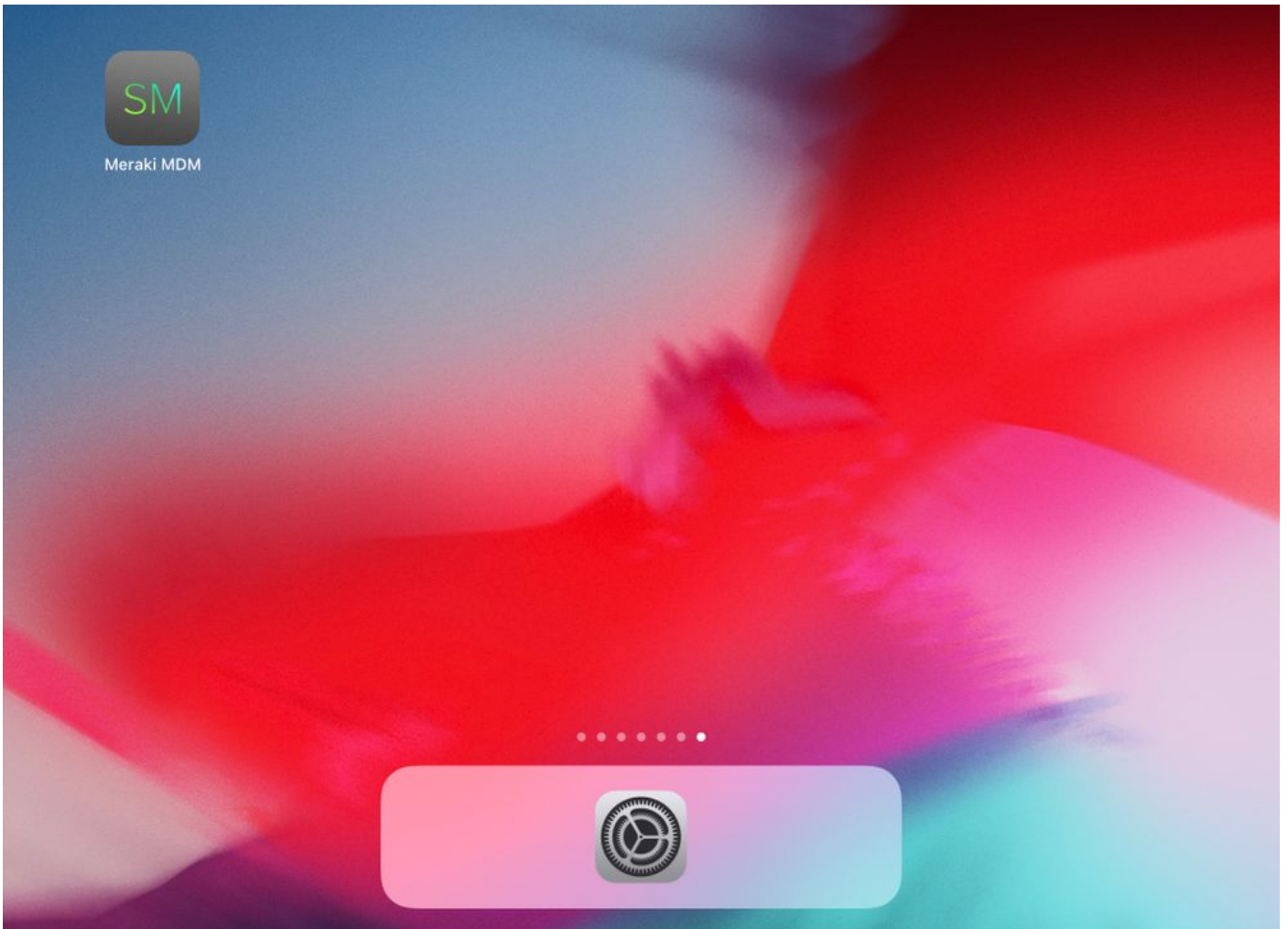
1.9. MDM 프로필을 설치하려면 설치 옵션을 선택합니다.



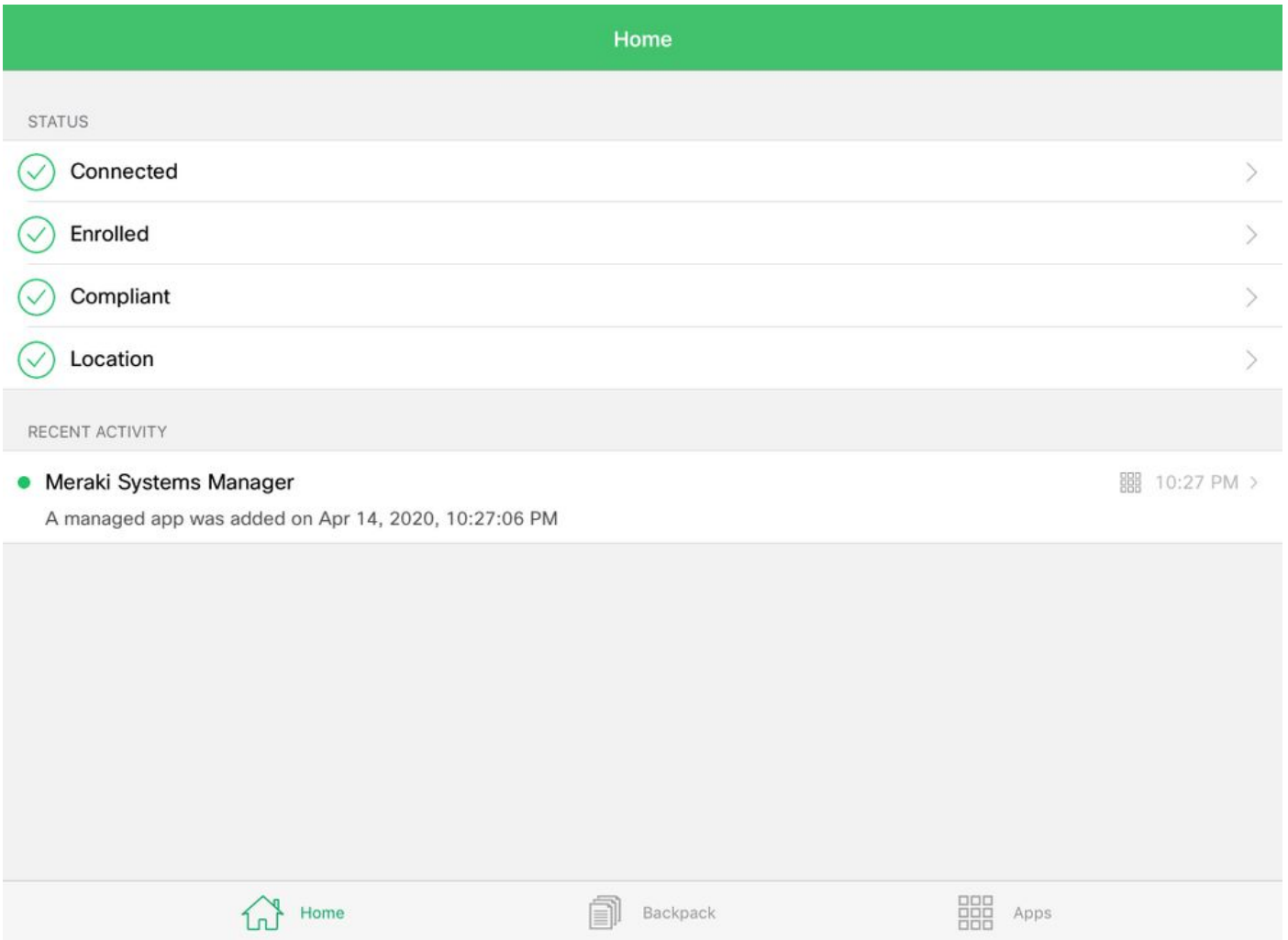
1.10. SM 응용 프로그램 설치 액세스 권한을 부여해야 합니다.



1.11. 홈 화면에 있는 Meraki MDM이라는 최근 다운로드한 애플리케이션을 엽니다.



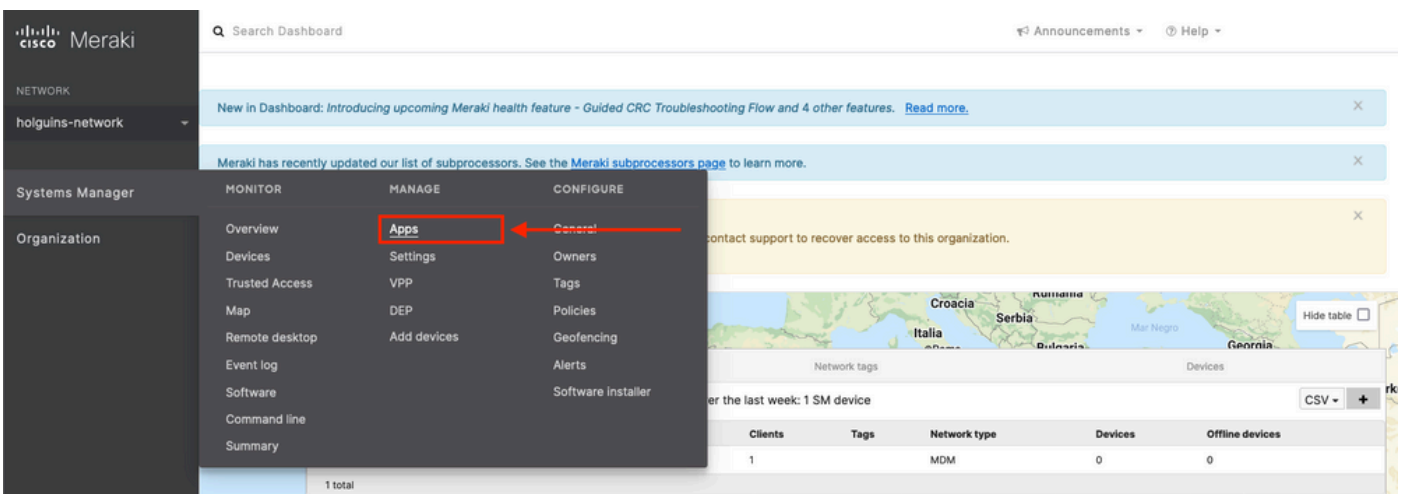
1.12. 모든 상태가 녹색으로 표시되어 등록이 완료되었음을 확인합니다.



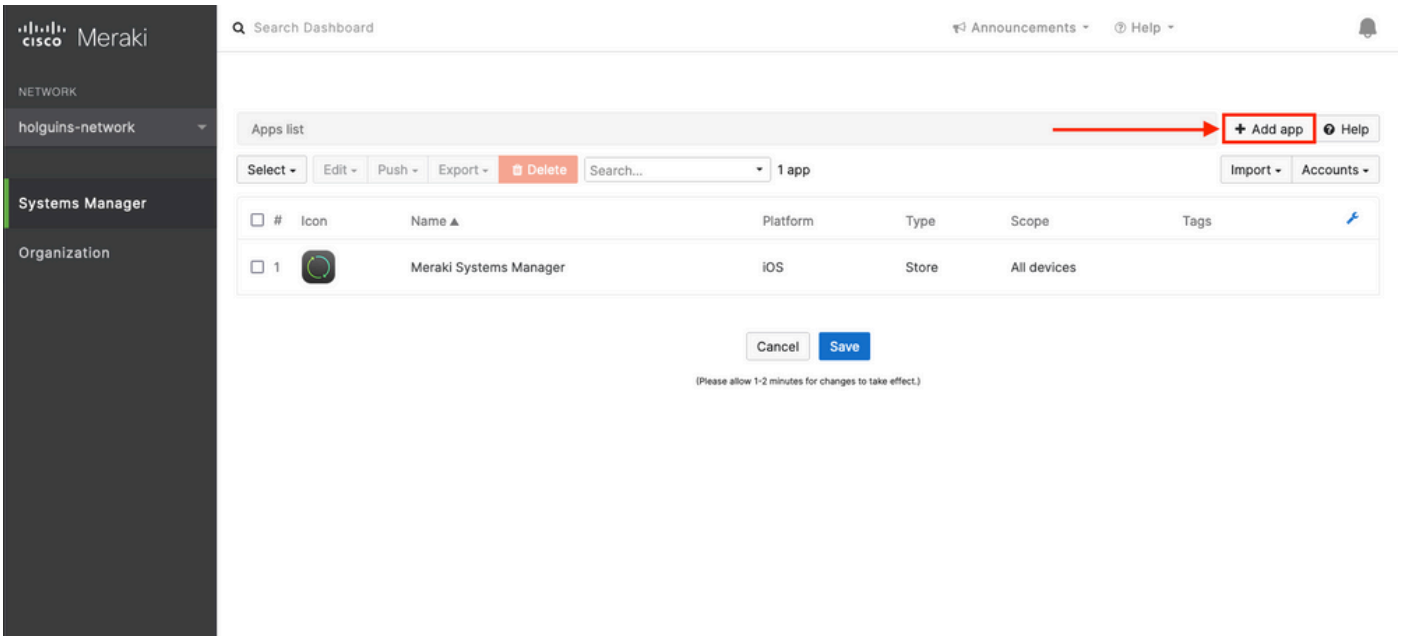
2단계. 관리되는 앱 설정

이 문서의 뒷부분에 나오는 PerApp용 터널링된 앱을 설정하려면 SM을 통해 동일한 애플리케이션을 관리해야 합니다. 이 컨피그레이션 예에서는 Firefox가 퍼 앱(Per App)을 통해 터널링되므로 관리되는 앱에 추가됩니다.

2.1. **Systems Manager > Manage > Apps**로 이동하여 관리되는 앱을 추가합니다.

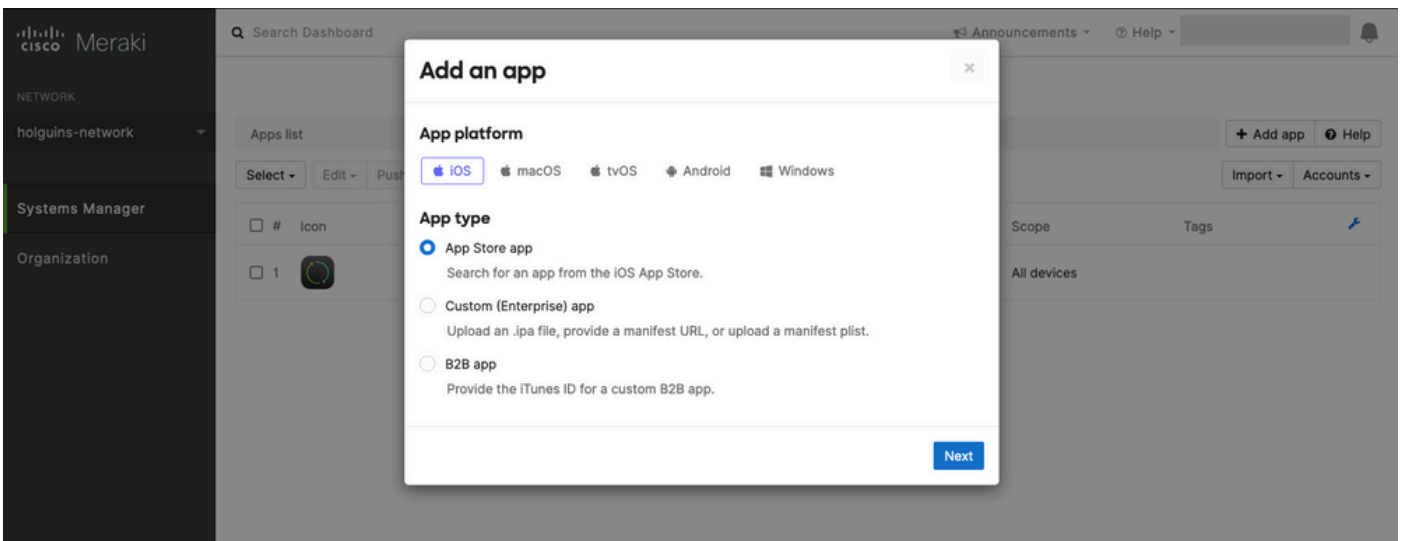


2.2. **앱 추가 옵션**을 선택합니다.



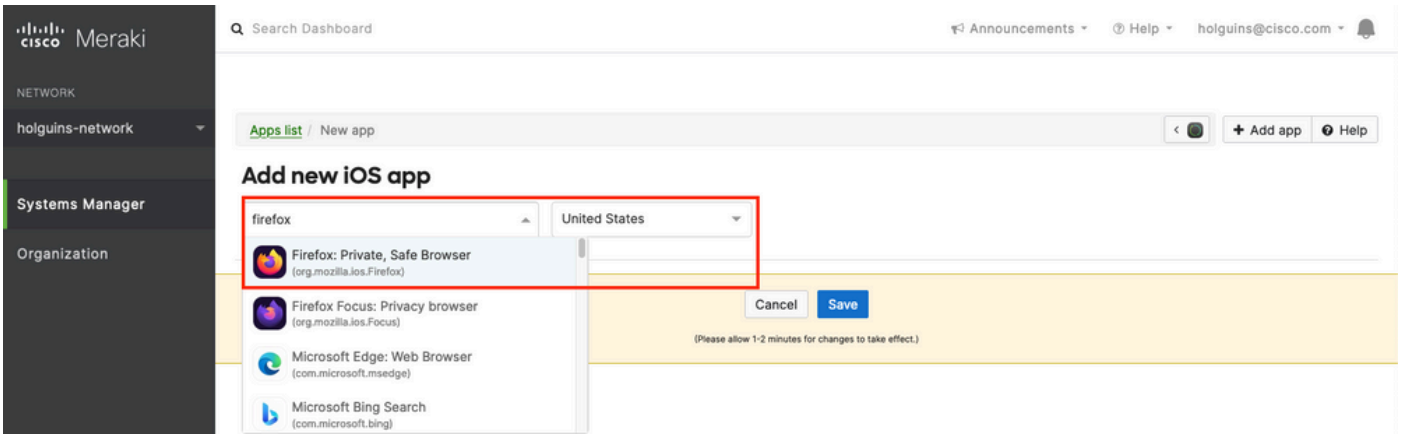
2.3. 앱이 저장된 위치에 따라 애플리케이션 유형(App Store 앱, 사용자 지정, B2B)을 선택합니다. 다음을 선택한 후 선택합니다.

이 예에서는 앱이 App Store에 공개적으로 저장됩니다.



2.4. 메시지가 표시되면 원하는 애플리케이션을 검색하고 애플리케이션이 다운로드되는 지역을 선택합니다. 앱을 선택한 후 저장을 선택합니다.

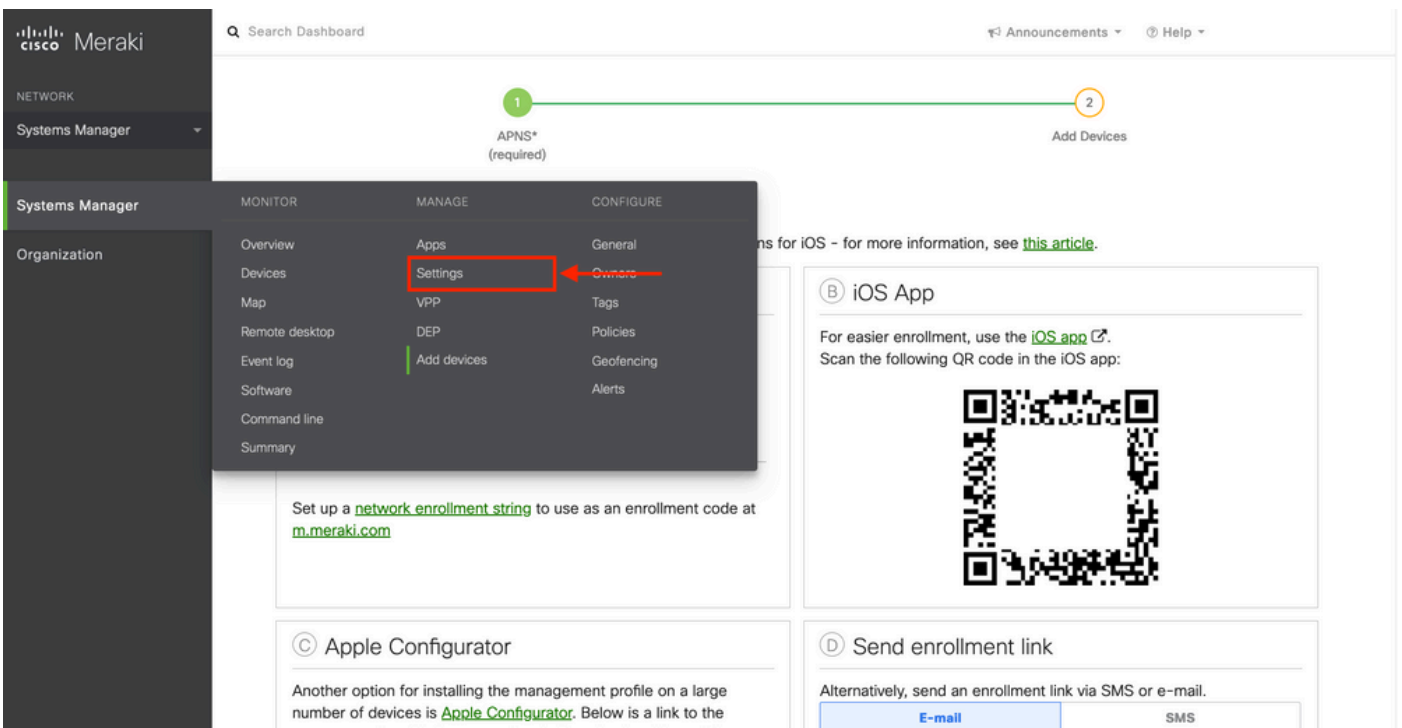
참고: 국가가 Apple 계정의 지역과 일치하지 않을 경우 사용자가 애플리케이션에 문제가 발생할 수 있습니다.



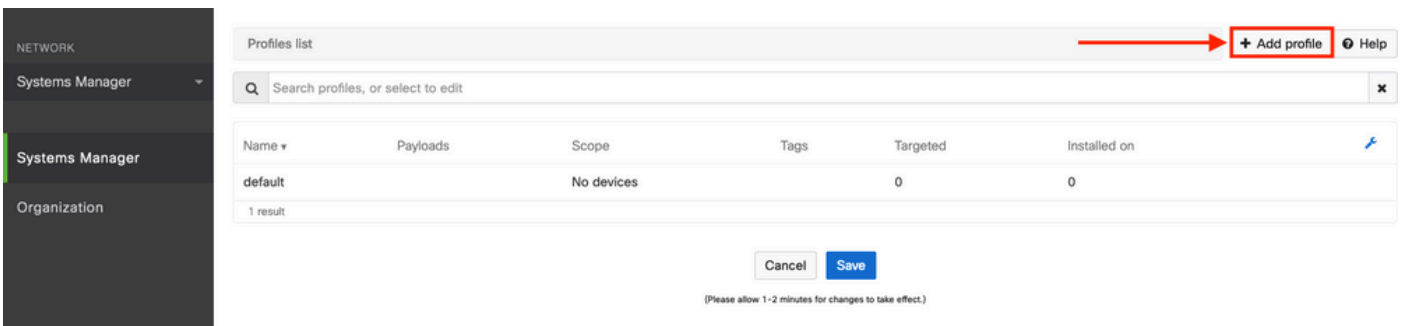
2.5. 원하는 응용 프로그램을 모두 선택한 후 저장을 클릭합니다.

3단계. PerApp VPN 프로파일 구성

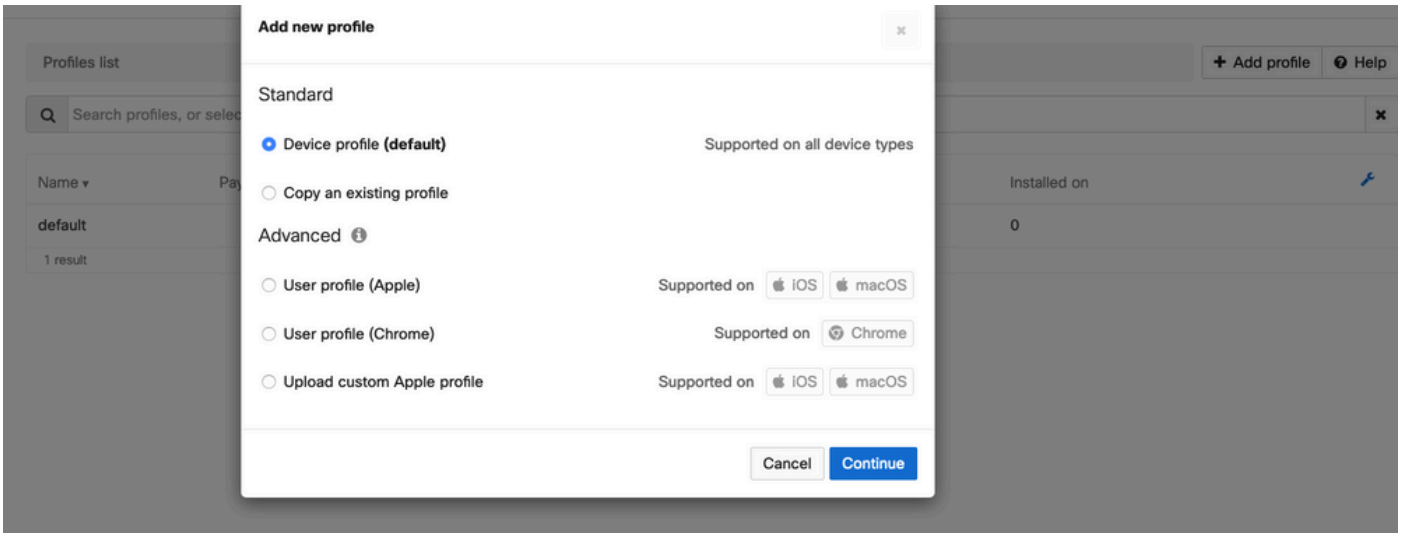
3.1. Systems Manager > Manage > Settings로 이동합니다



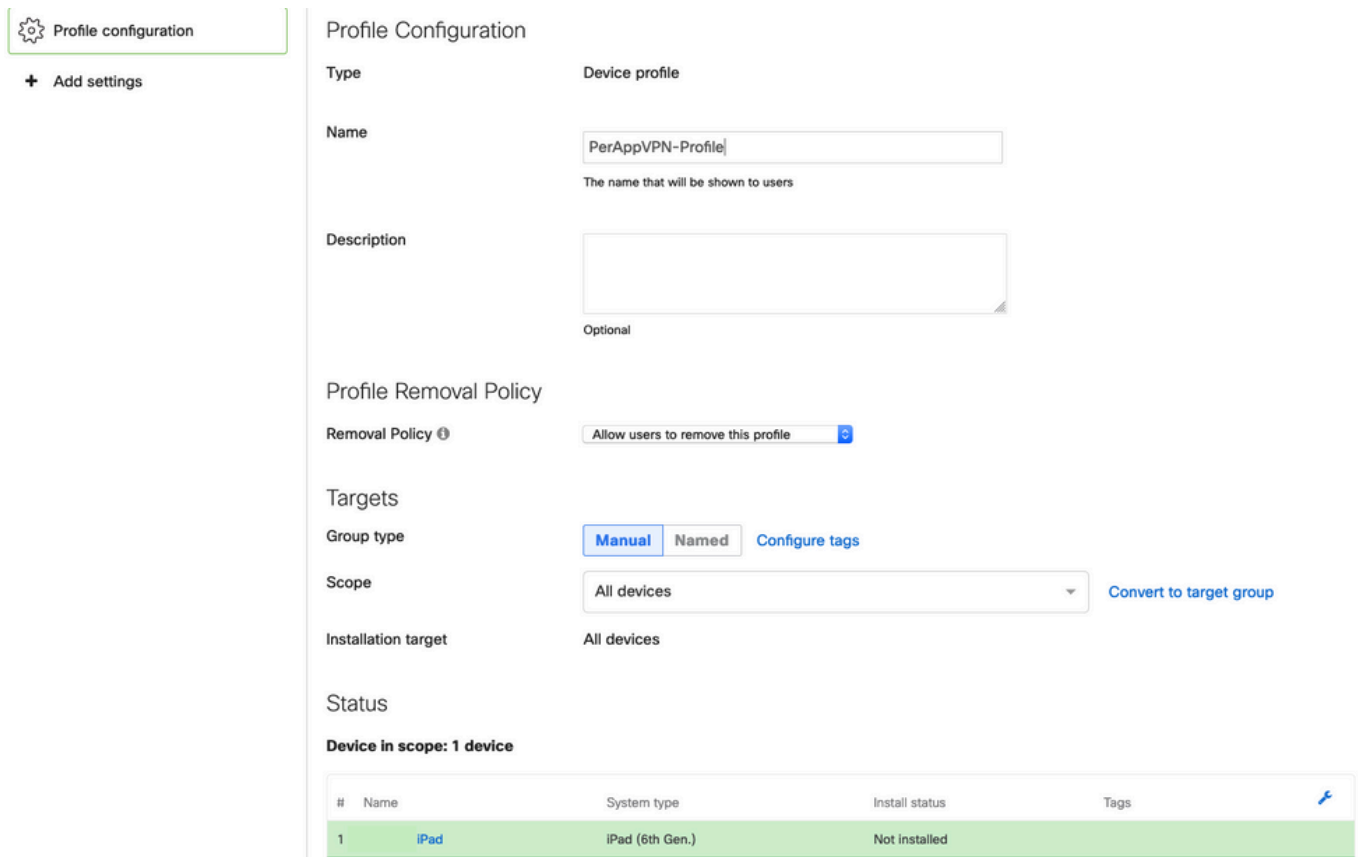
3.2. 프로파일 추가 옵션을 선택합니다.



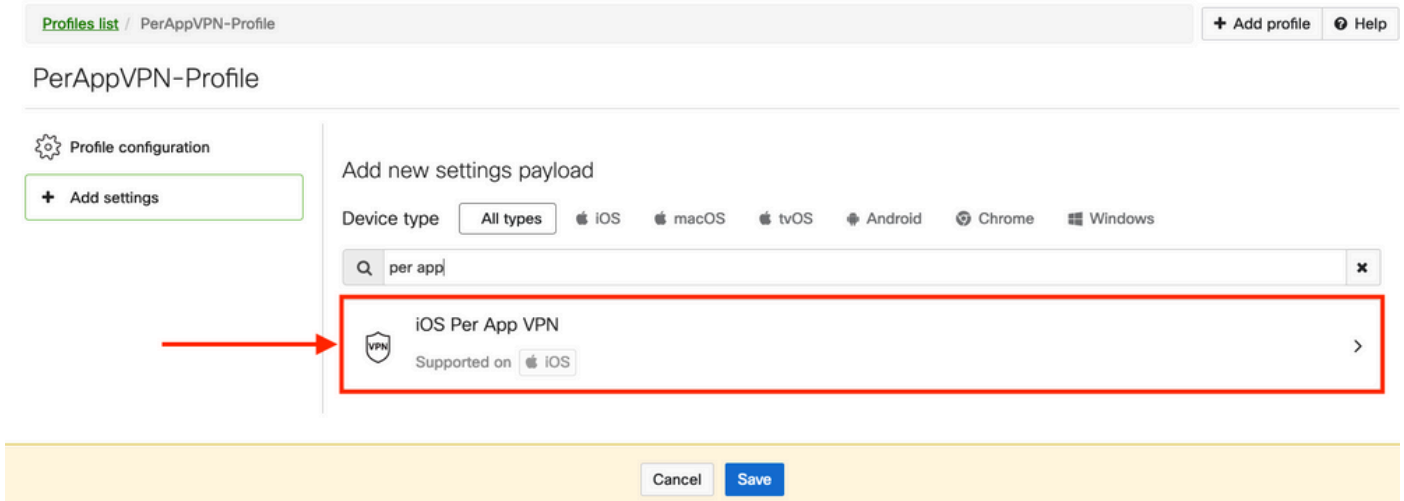
3.3. Device profile (default)(디바이스 프로파일(기본값))을 선택하고 Continue(계속)를 클릭합니다.



3.4. Profile Configuration(프로필 컨피그레이션) 메뉴가 표시되면 Name(이름)을 쓰고 Scope(범위) 아래에서 대상 디바이스를 선택합니다.



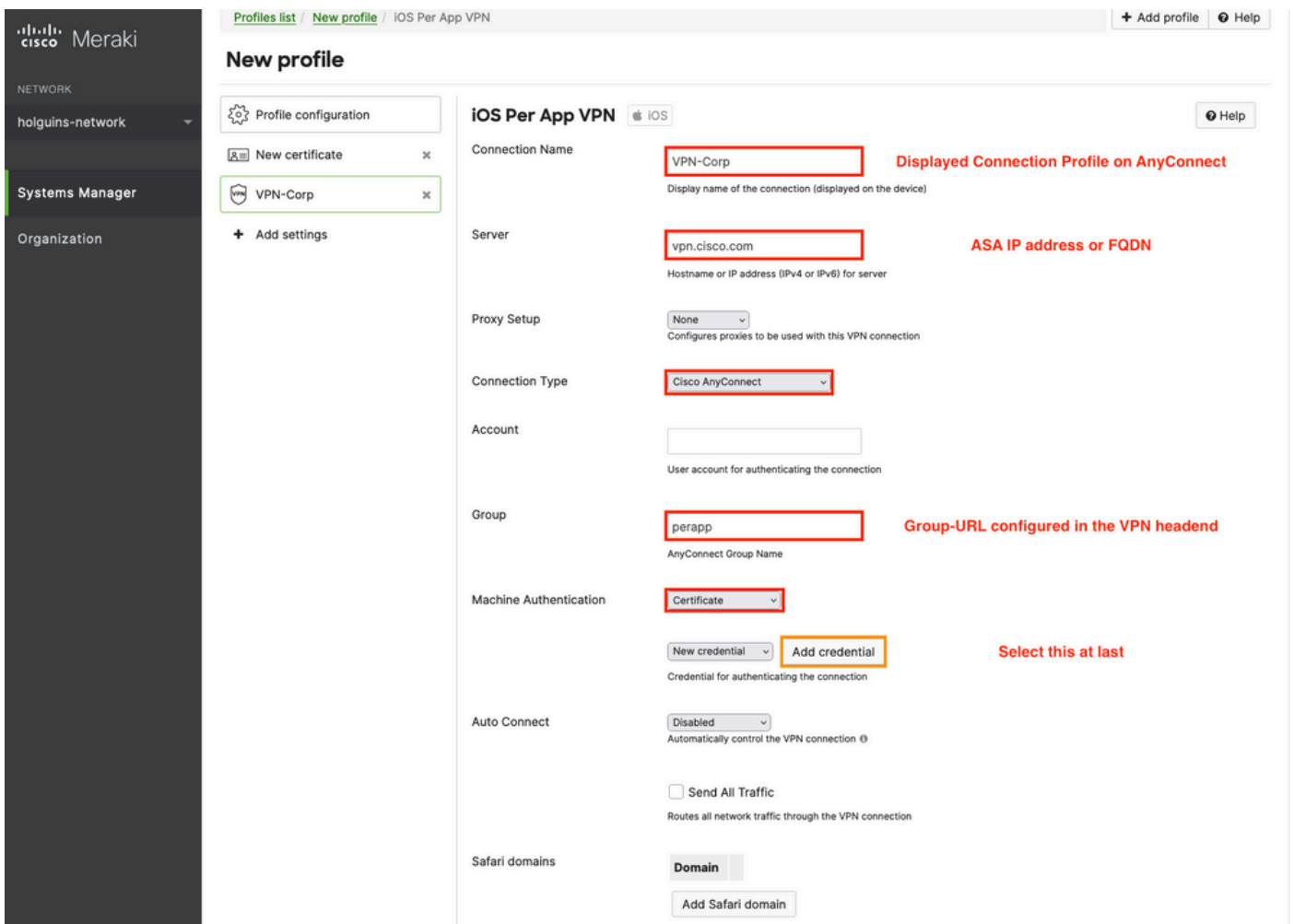
3.5. Add settings(설정 추가)를 선택하고 iOS Per App VPN(iOS 퍼 앱 VPN)으로 프로필 유형을 필터링한 다음 아래 표시된 대로 옵션을 선택합니다.



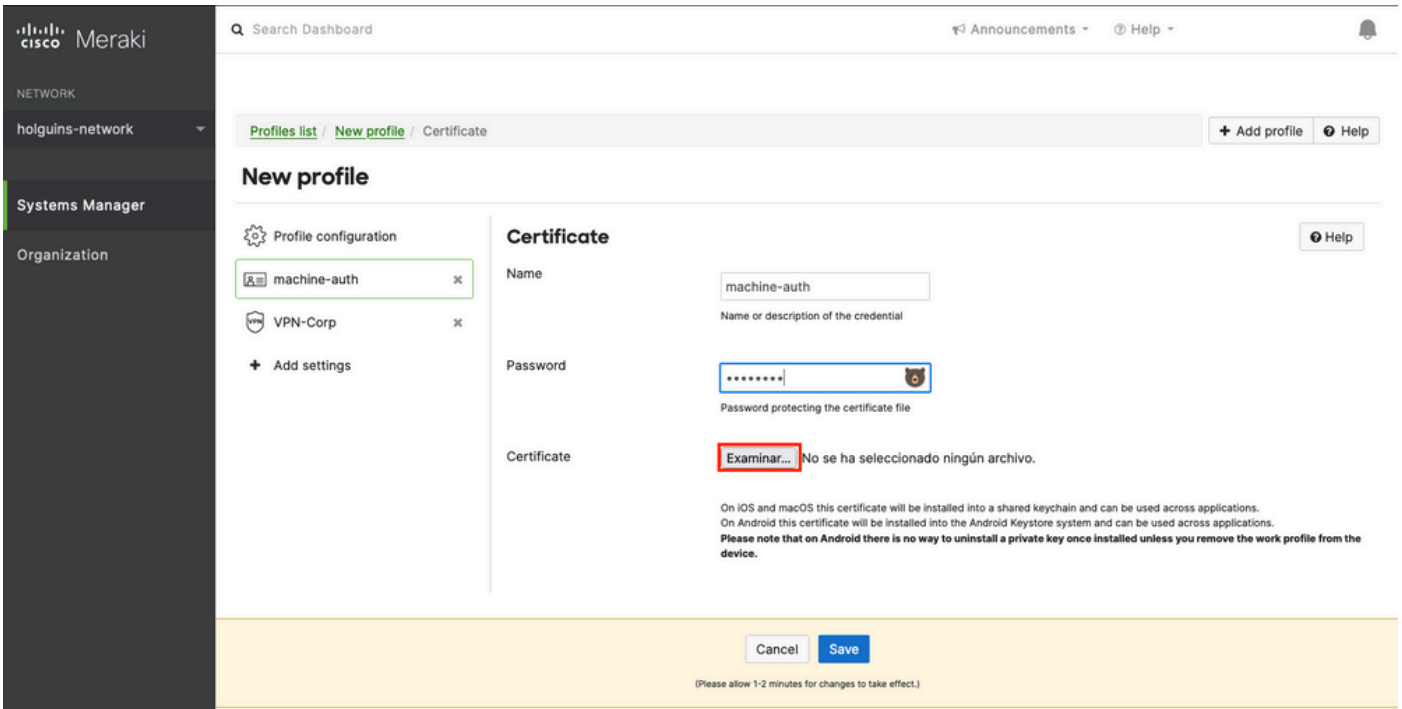
3.6. 메뉴가 표시되면 아래 예제를 기준으로 연결 정보를 작성합니다.

Systems Manager는 이러한 연결에 대해 SCEP 및 수동 등록의 두 가지 인증서 등록을 지원합니다. 이 예에서는 수동 등록이 사용되었습니다.

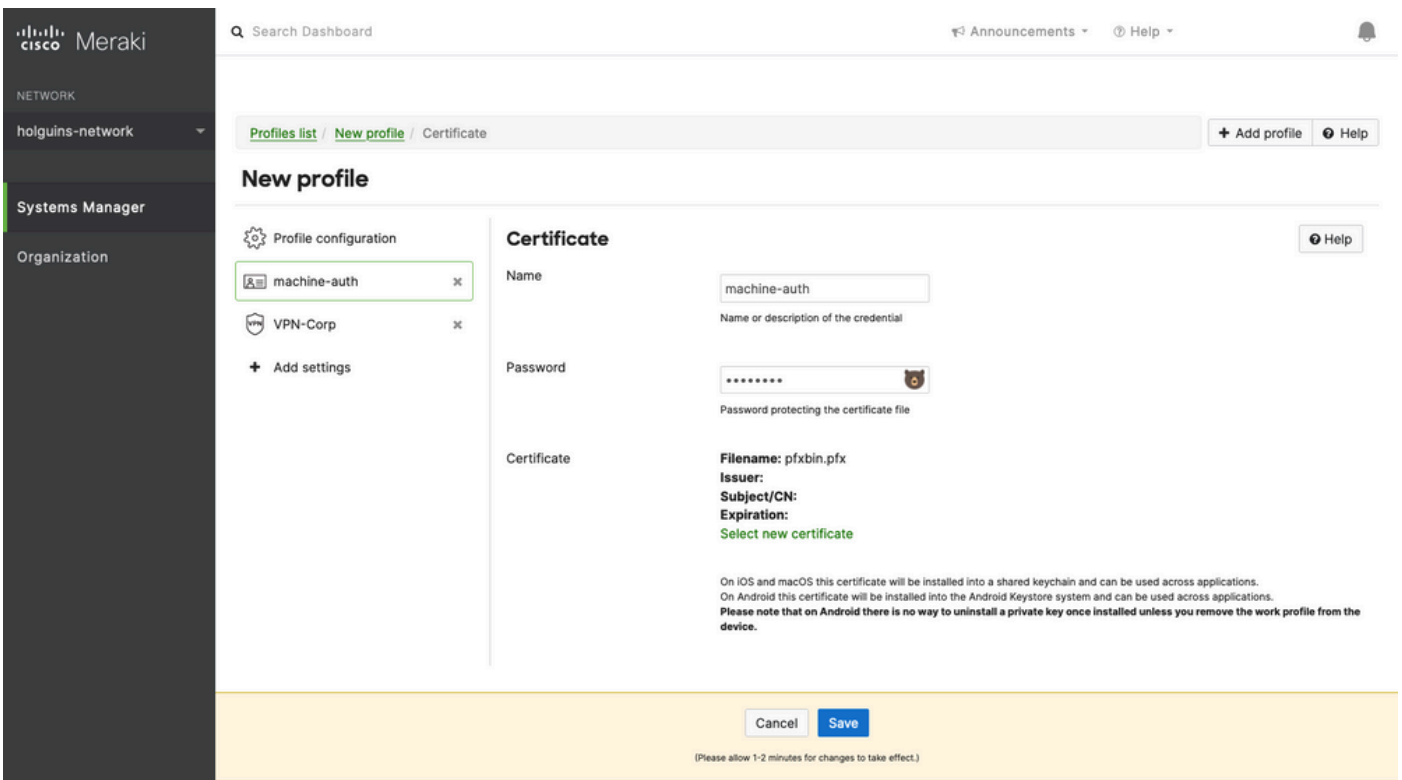
참고: 이 옵션을 사용하면 새 메뉴로 이동하여 인증서 파일을 추가할 수 있으므로 텍스트 상자를 채운 후 Add credential(인증서 추가)을 선택합니다.



3.7. 자격 증명 추가를 클릭하고 Certificate(인증서) 메뉴로 리디렉션되면 인증서의 이름을 쓰고 컴퓨터에서 검색하여 .pfx 파일(암호화된 인증서 파일)을 보호하는 암호를 찾습니다.

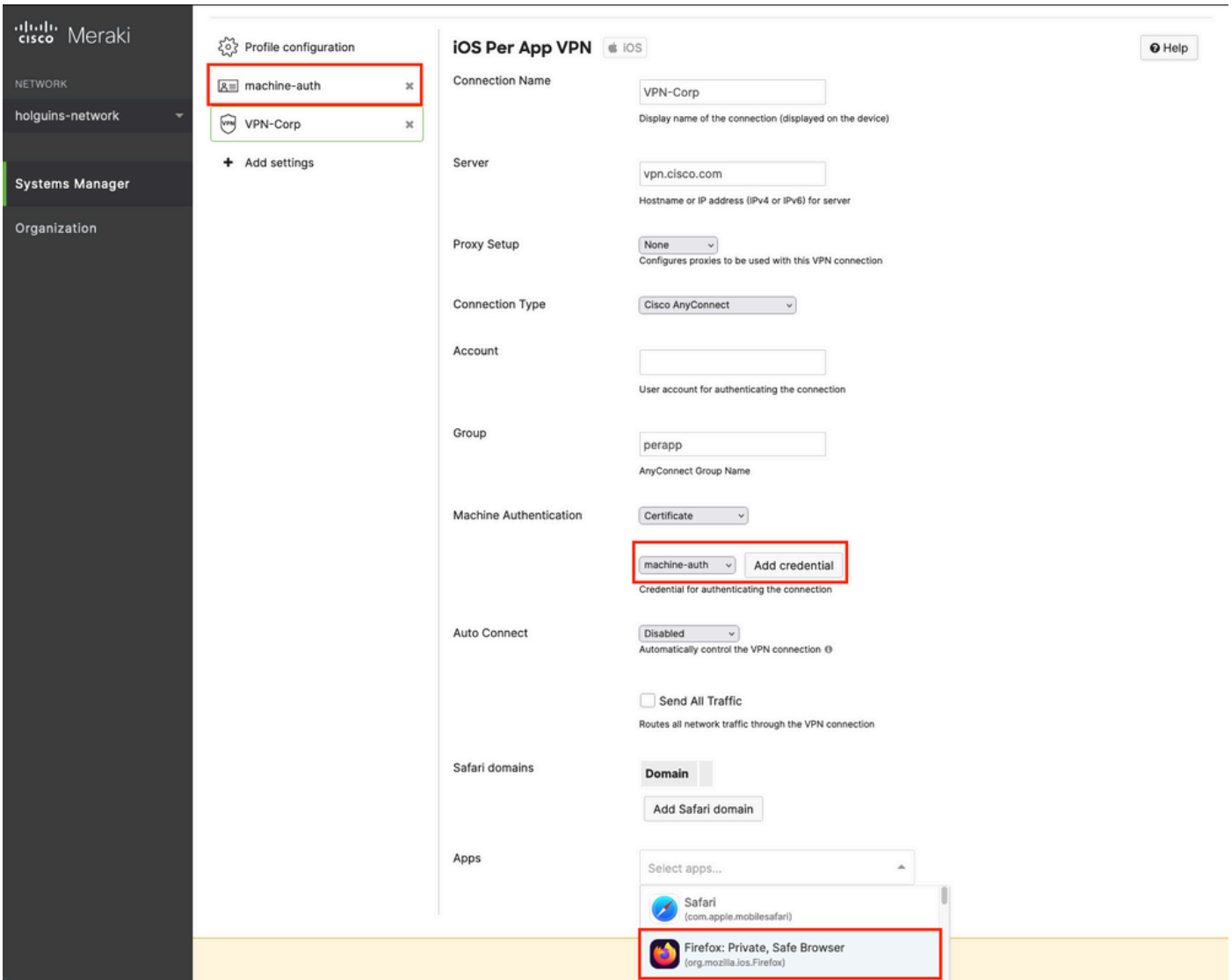


3.8. 인증서를 선택하면 인증서 파일 이름이 표시됩니다.



3.9. 인증서를 선택한 후에는 이전에 사용했던 VPN 프로파일로 이동하여 최근에 가져온 자격 증명을 선택하고 터널링된 앱(이 경우 Firefox)을 선택합니다.

이 작업이 완료되면 Save(저장)를 클릭합니다.



3.10. 프로파일이 대상 장치에 설치되어 있는지 확인합니다.

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

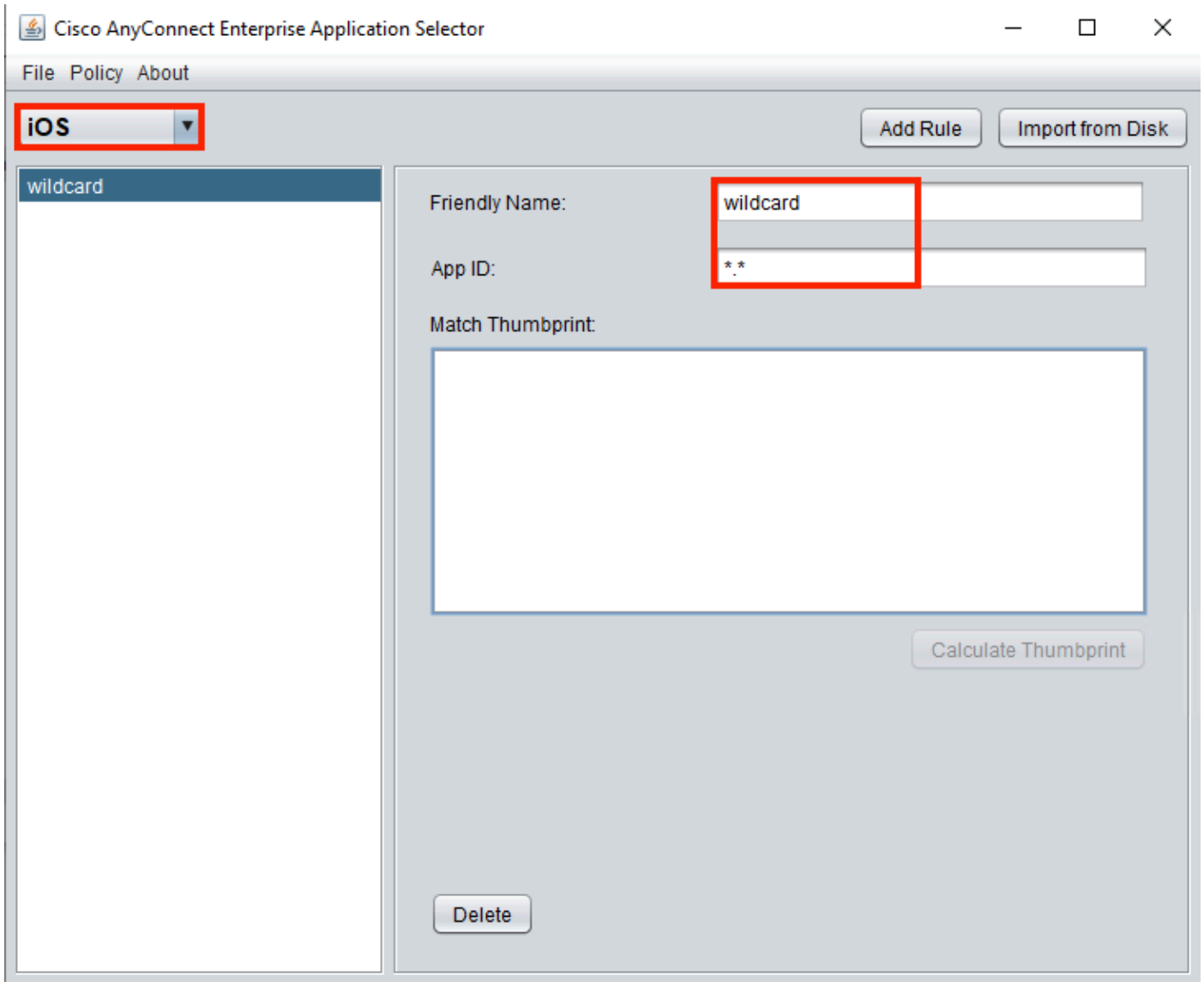
4단계. 앱 선택기 컨피그레이션

4.1. cisco 웹 사이트에서 앱 선택기 다운로드

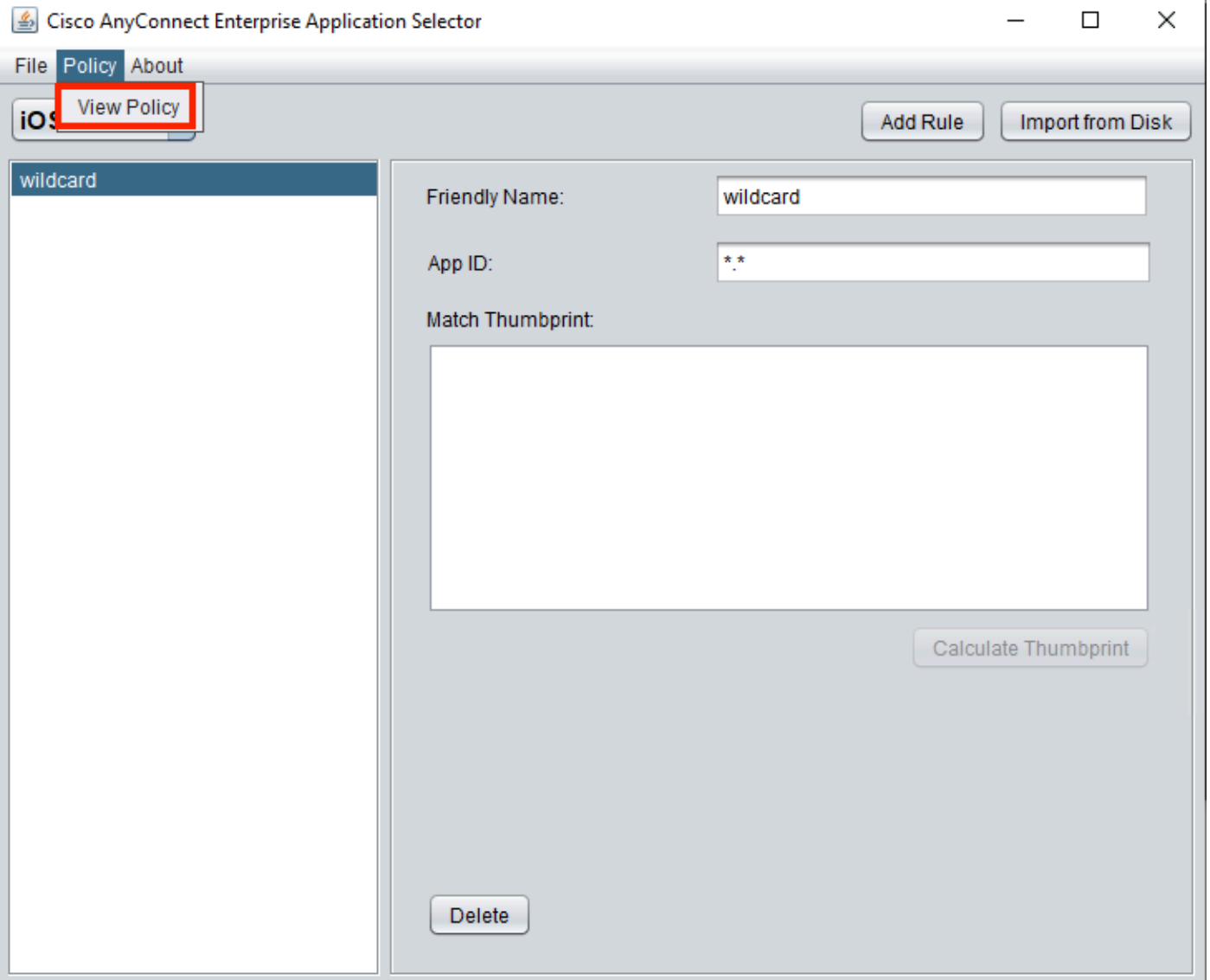
<https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0>

주의: Windows 컴퓨터에서 응용 프로그램을 실행합니다. MacOS 디바이스에서 툴을 사용할 경우 표시되는 결과는 예상과 다릅니다.

4.2. java 응용 프로그램을 엽니다. 드롭다운 메뉴에서 iOS를 선택하고 이름을 추가한 다음 앱 ID에 *.*를 입력합니다.



4.3. Policy(정책)로 이동하고 View Policy(정책 보기)를 선택합니다



4.4. 표시된 문자열을 복사합니다. (이는 나중에 VPN 헤드엔드 컨피그레이션에서 사용됩니다.)

```
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSglYk  
FBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB
```

OK

5단계. ASA 샘플 퍼 앱(Per App) VPN 구성

```
conf t
webvpn
anyconnect-custom-attr perapp description PerAppVPN
anyconnect-custom-data perapp wildcard
eJyrVnLOLE7Od84vqCzKTM8oUbJSgrMVNJI1FYwMDEwUwGoUgiuLS1Jzi3UUPPOS9ZR0IFxSyzKTU30yi4G6oquh3JDKglSg  
lYkFBTmPupn5xUB1jgUFcEVA8cwUoLyWnhZQJi0vMRekujwzJyU5sShFqTYWCAFHcjDB

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
```

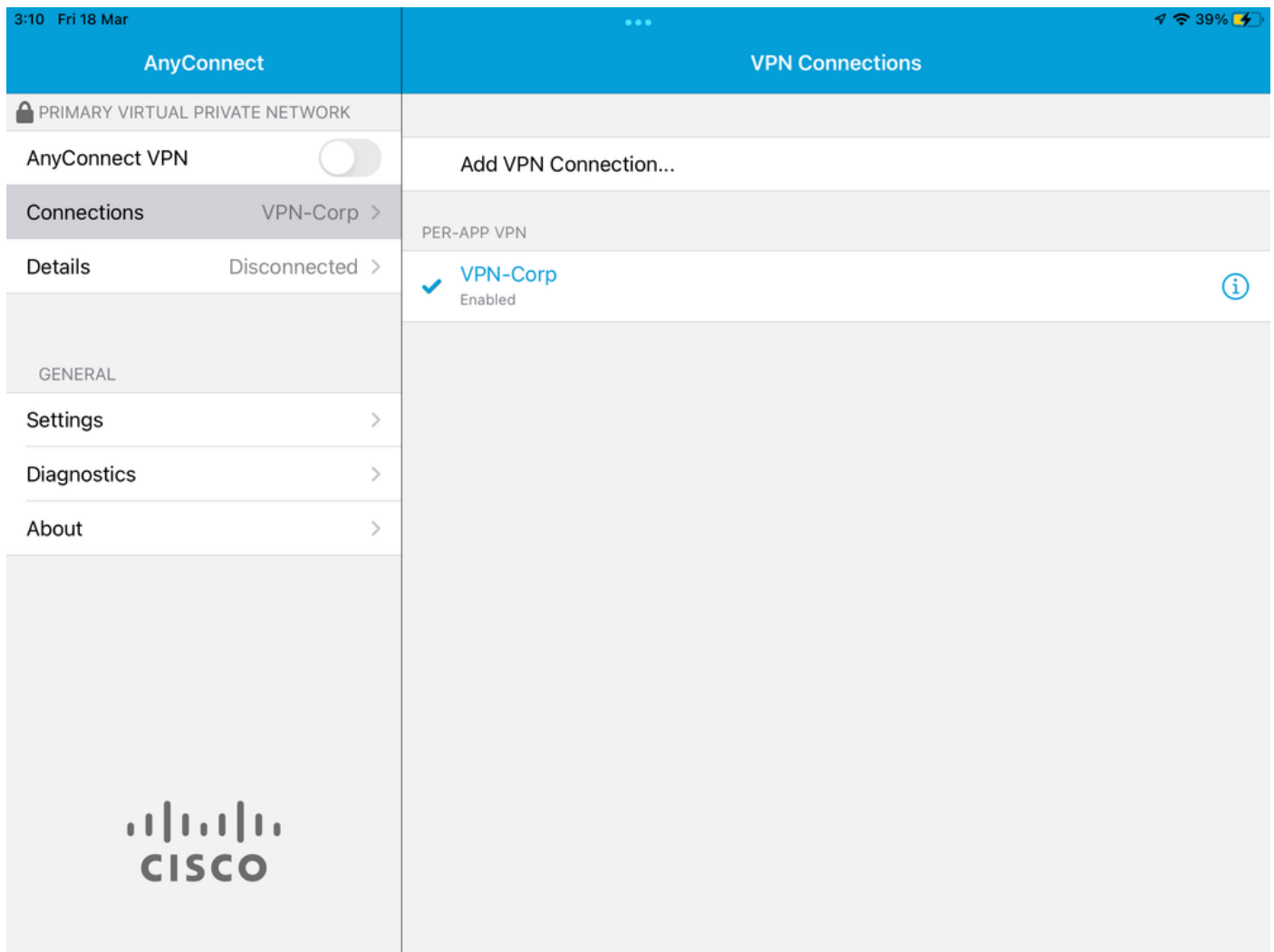

group-url https://vpn.cisco.com/perapp enable

다음을 확인합니다.

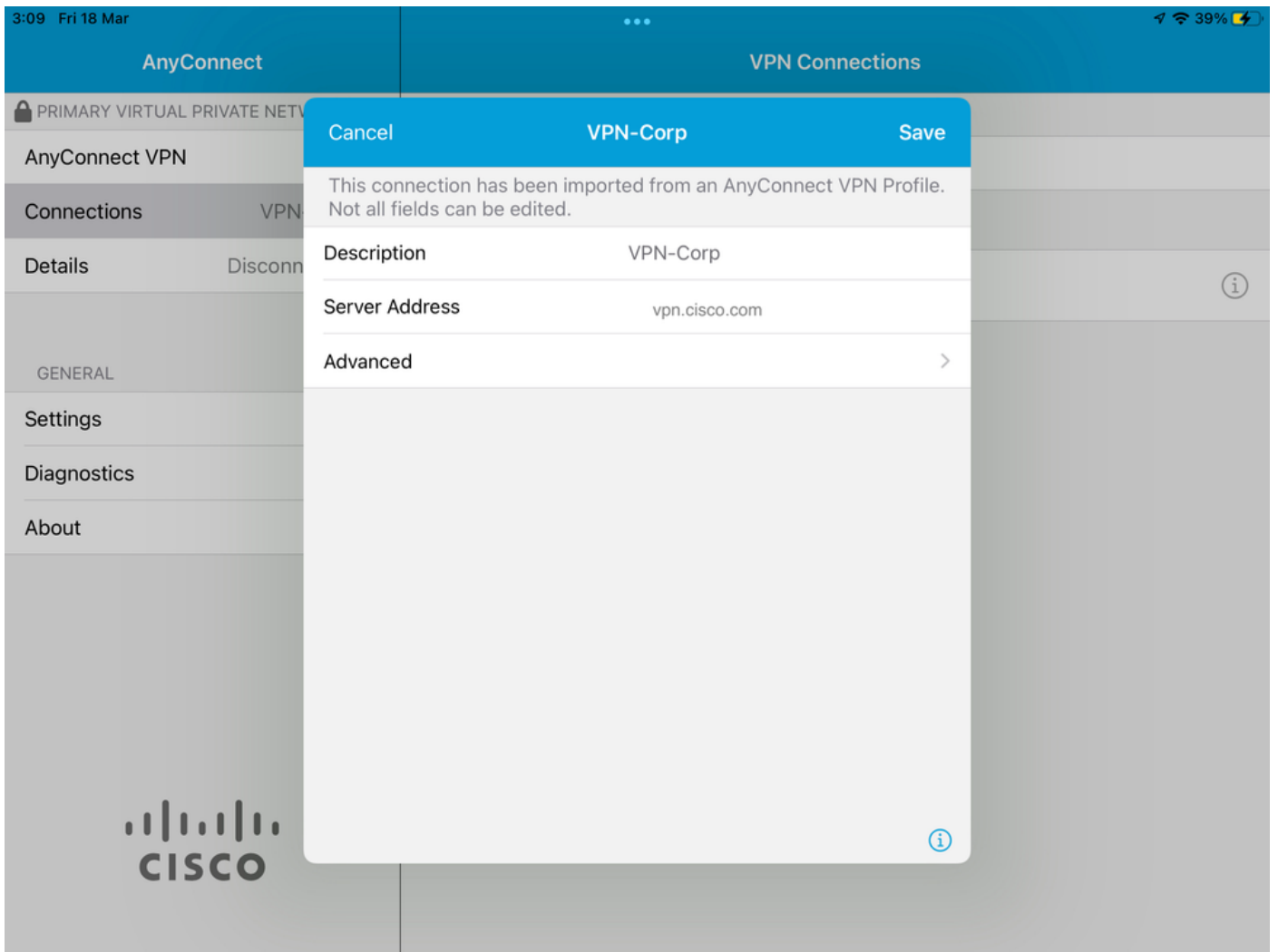
6. AnyConnect 애플리케이션에서 프로파일 설치 확인

6.1. AnyConnect 애플리케이션을 열고 왼쪽 창에서 **Connections**를 선택합니다. PerApp VPN 프로파일은 PER-APP VPN이라는 새 섹션 아래에 표시되어야 합니다.

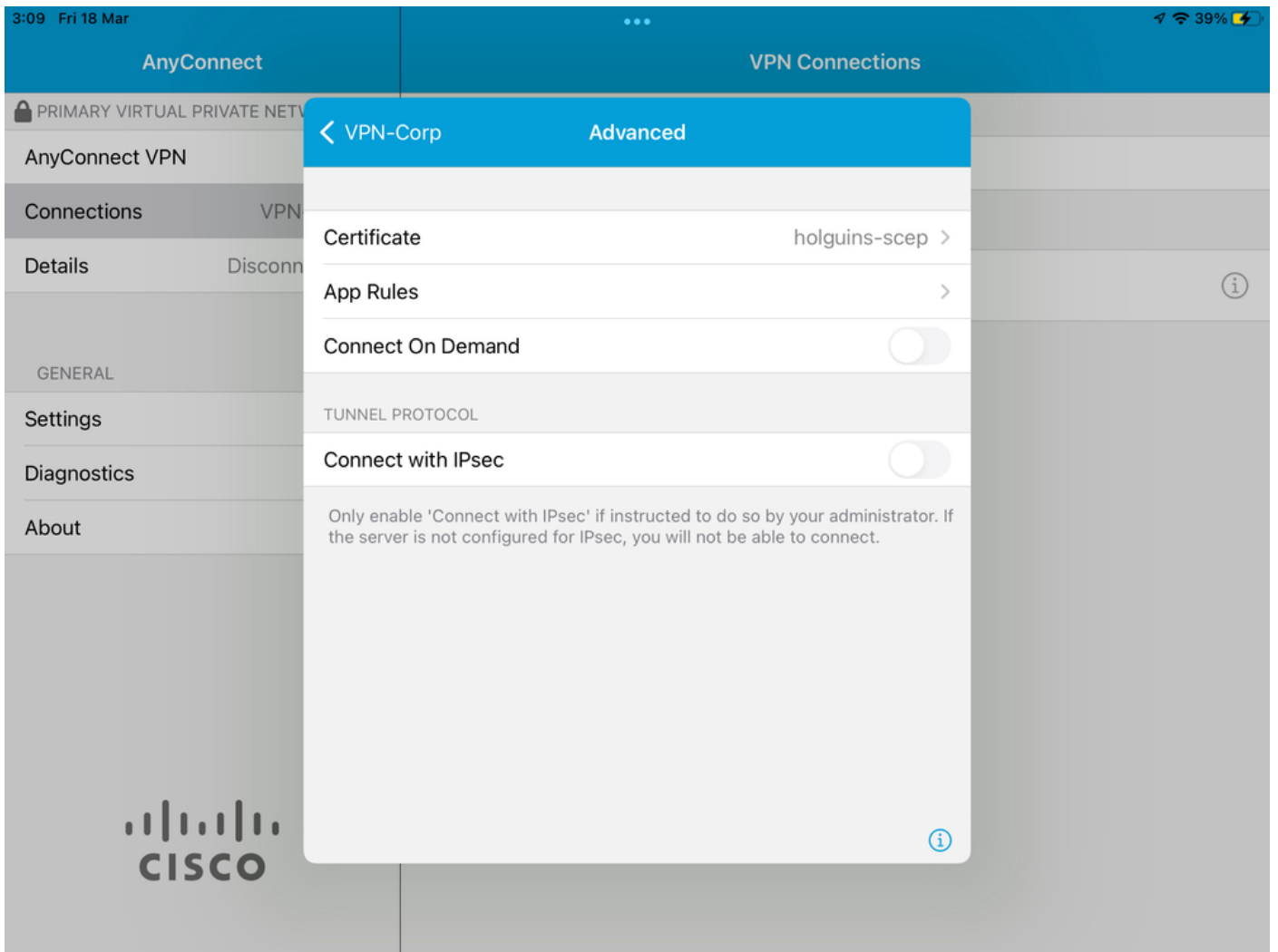
고급 설정을 표시하려면 **i**를 선택합니다.



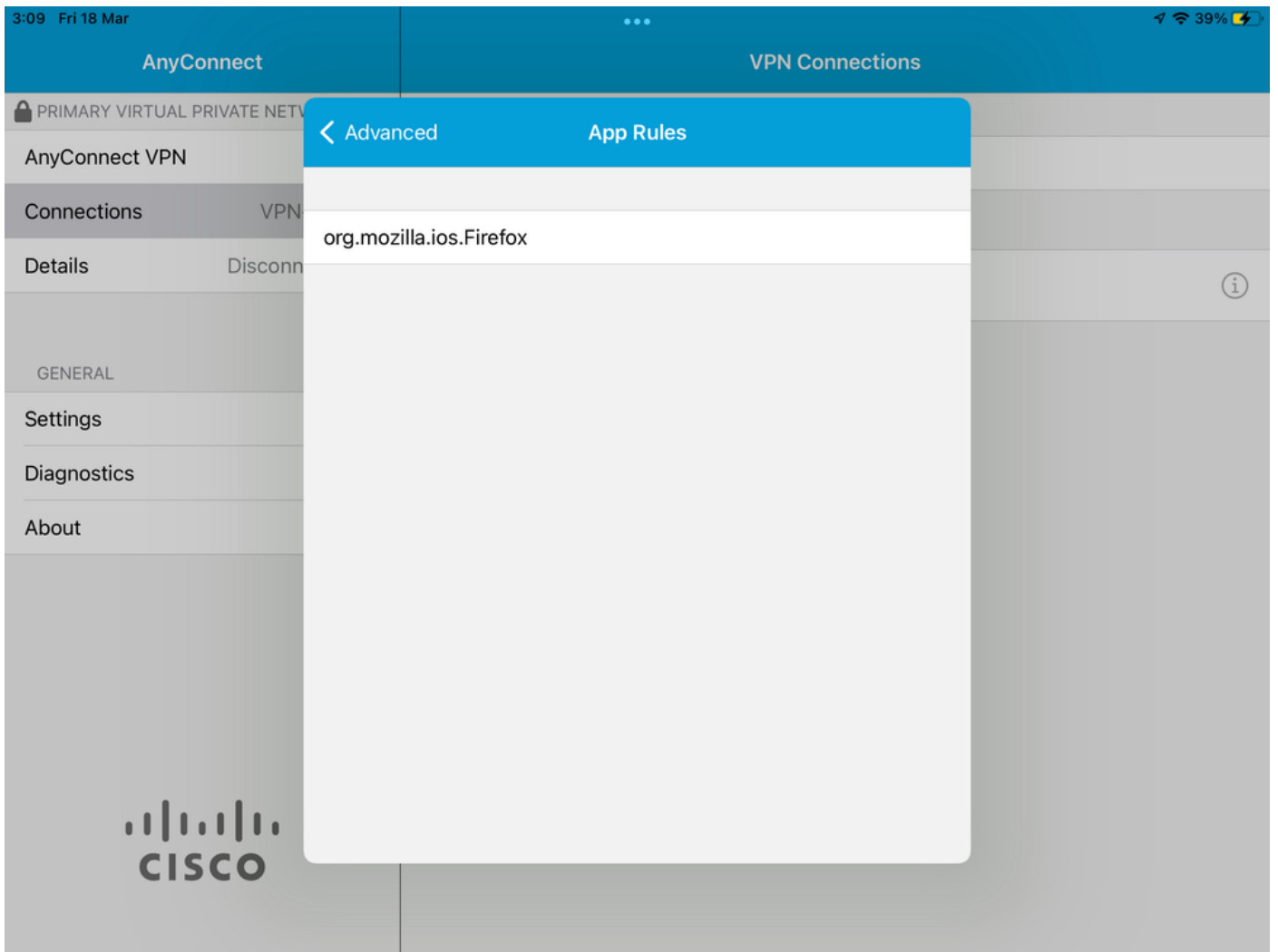
6.2. 고급 옵션을 선택합니다.



6.3. App Rules(앱 규칙) 옵션을 선택합니다.



6.4. 마지막으로 앱 규칙이 설치되었는지 확인합니다. (Mozilla는 이 문서에서 원하는 터널링된 앱이므로 앱 설치가 성공했습니다.)



문제 해결

현재 이 문서에 대한 구체적인 트러블슈팅 단계가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.