Configuración de Anyconnect PerApp VPN para iOS con Meraki System Manager

Contenido

Introducción

Este documento describe cómo configurar PerApp VPN en dispositivos Apple iOS administrados por Meraki Mobile Device Manager (MDM), System Manager (SM).

Prerequisites

Requirements

- Licencia AnyConnect v4.0 Plus o Apex.
- ASA 9.3.1 o posterior para admitir VPN por aplicación.
- Herramienta Cisco Enterprise Application Selector disponible en Cisco.com

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

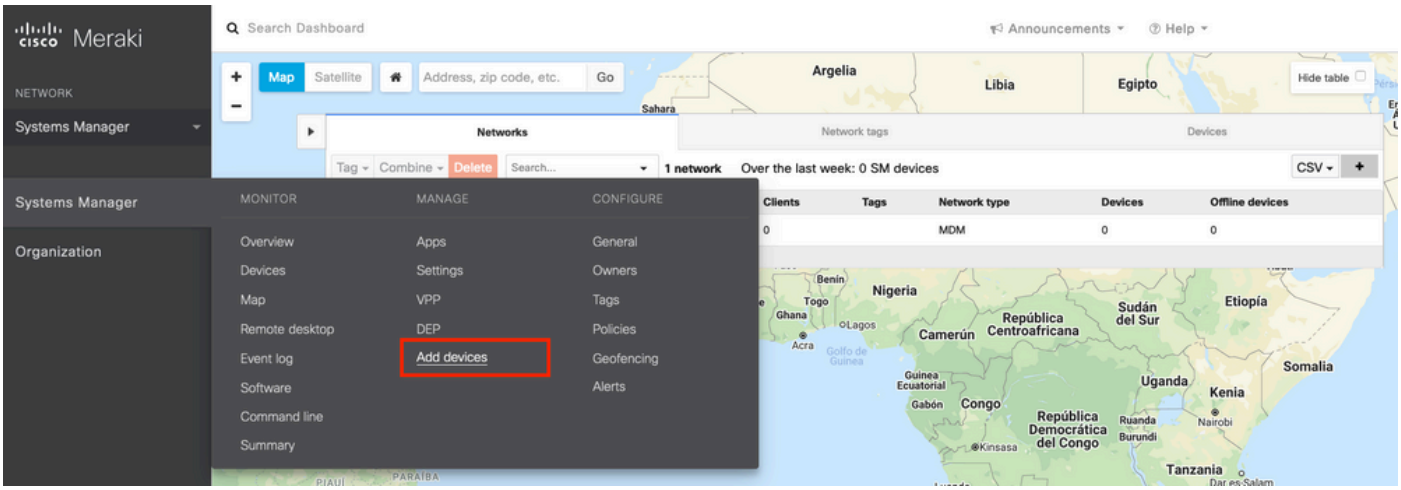
Este documento no incluye los procesos enumerados:

- Configuración de CA de SCEP en Systems Manager para la generación de certificados de cliente
- Generación de certificados de cliente PKCS12 para los clientes iOS

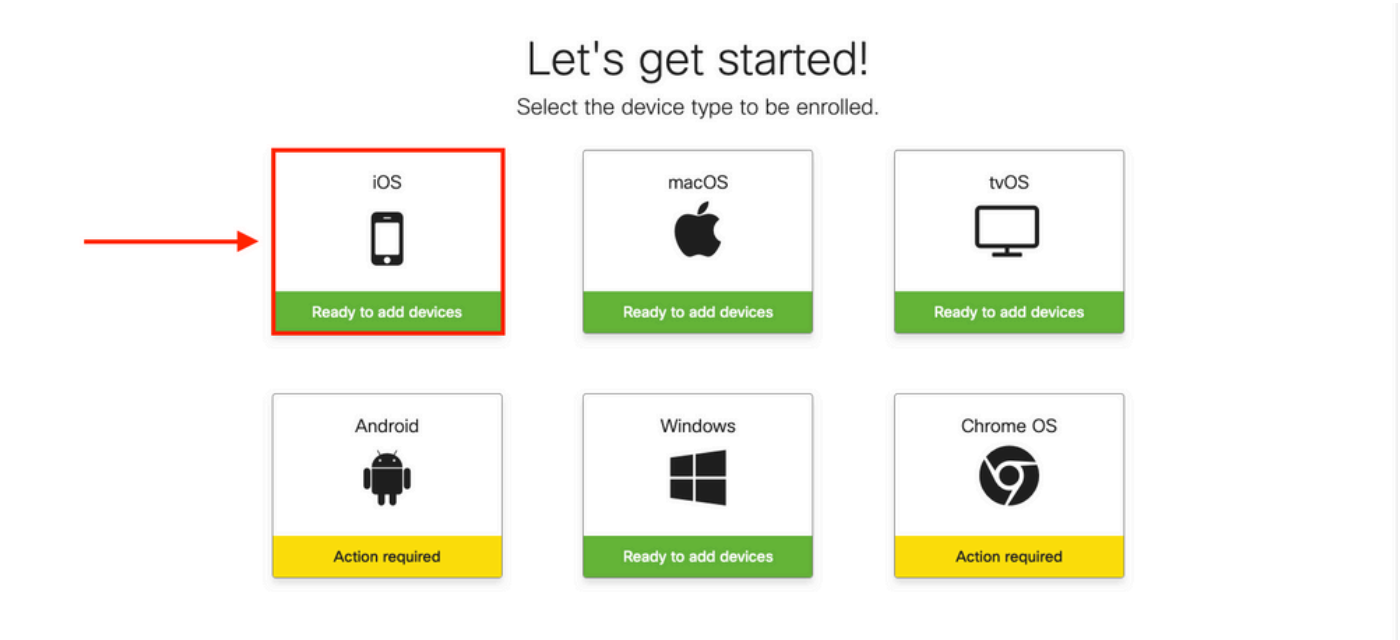
Configurar

Paso 1. Registro de dispositivos iOS en Meraki Systems Manager

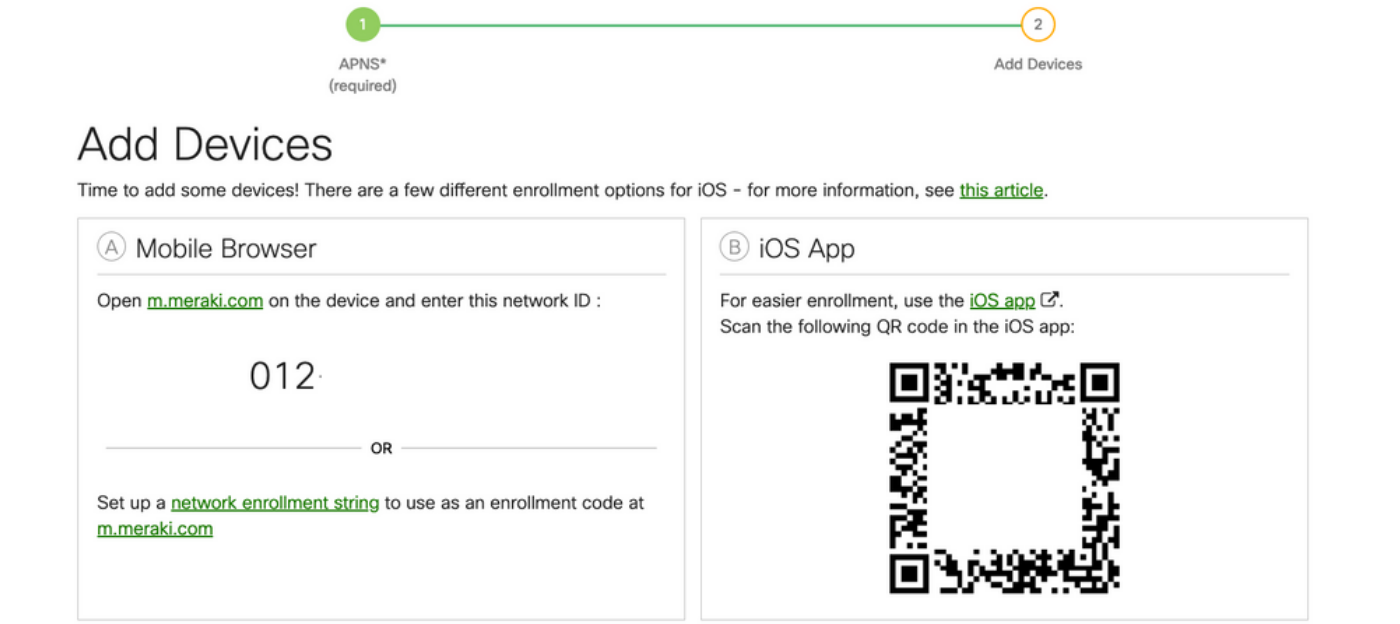
1.1. Vaya a **Systems Manager > Add Devices** .



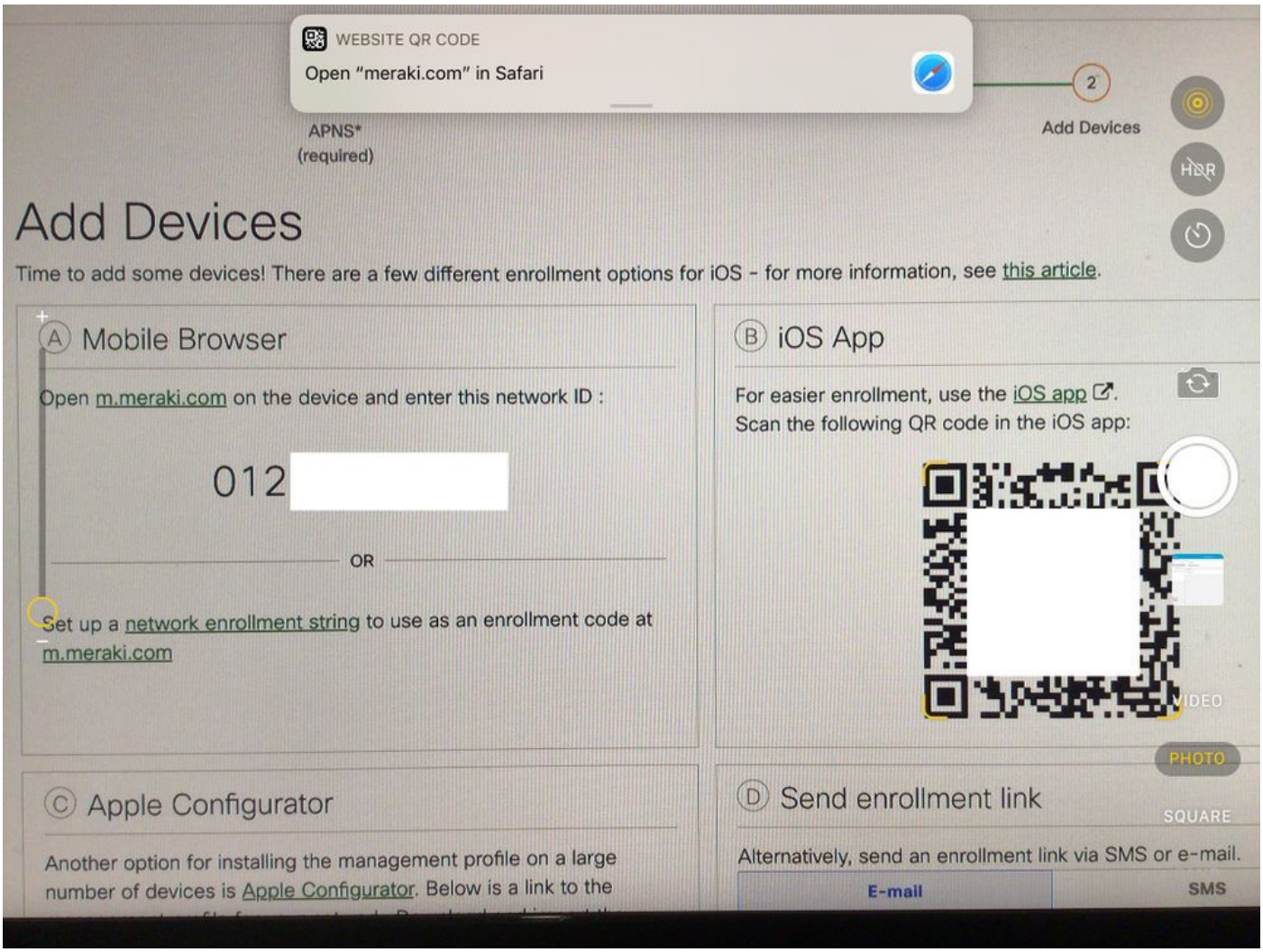
1.2. Haga clic en la opción **iOS** para iniciar la inscripción.



1.3. Inscriba el dispositivo a través del navegador de Internet o escanee el código QR con la cámara. En este documento, la cámara se utilizó para el proceso de inscripción.

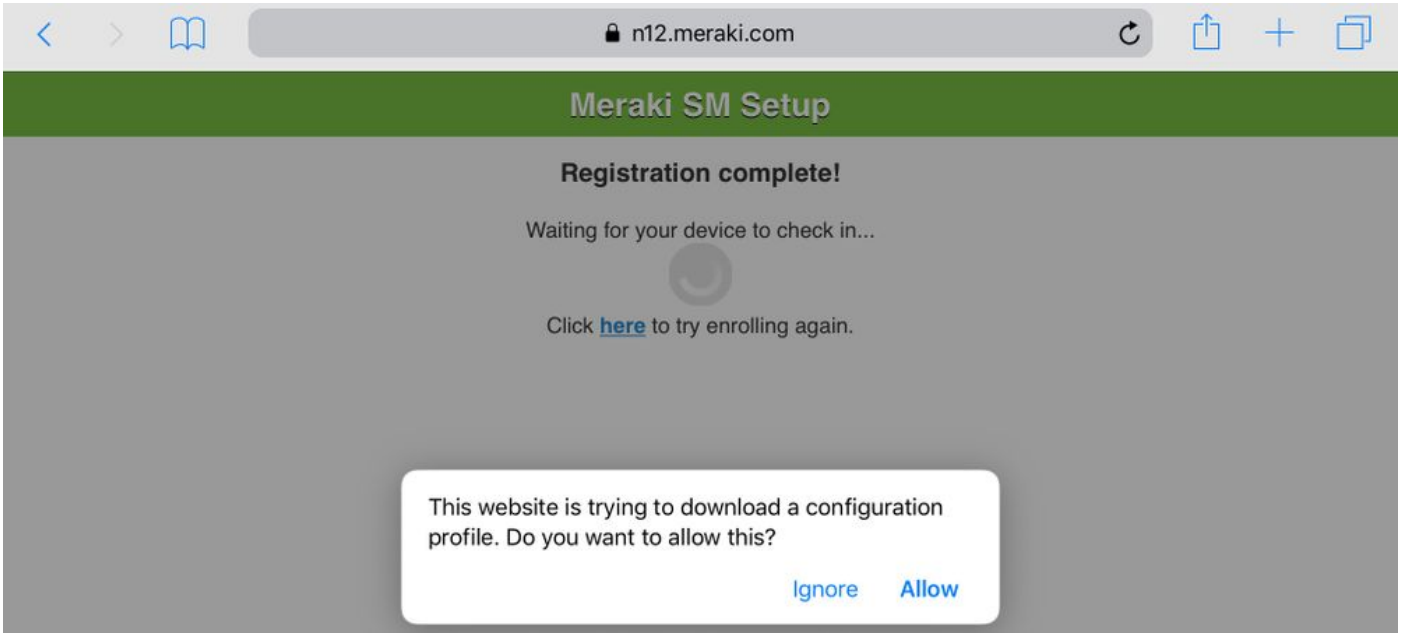


1.4. Cuando la cámara reconozca el código QR, seleccione la opción **Abrir "meraki.com" en la** notificación de **Safari** que aparece.

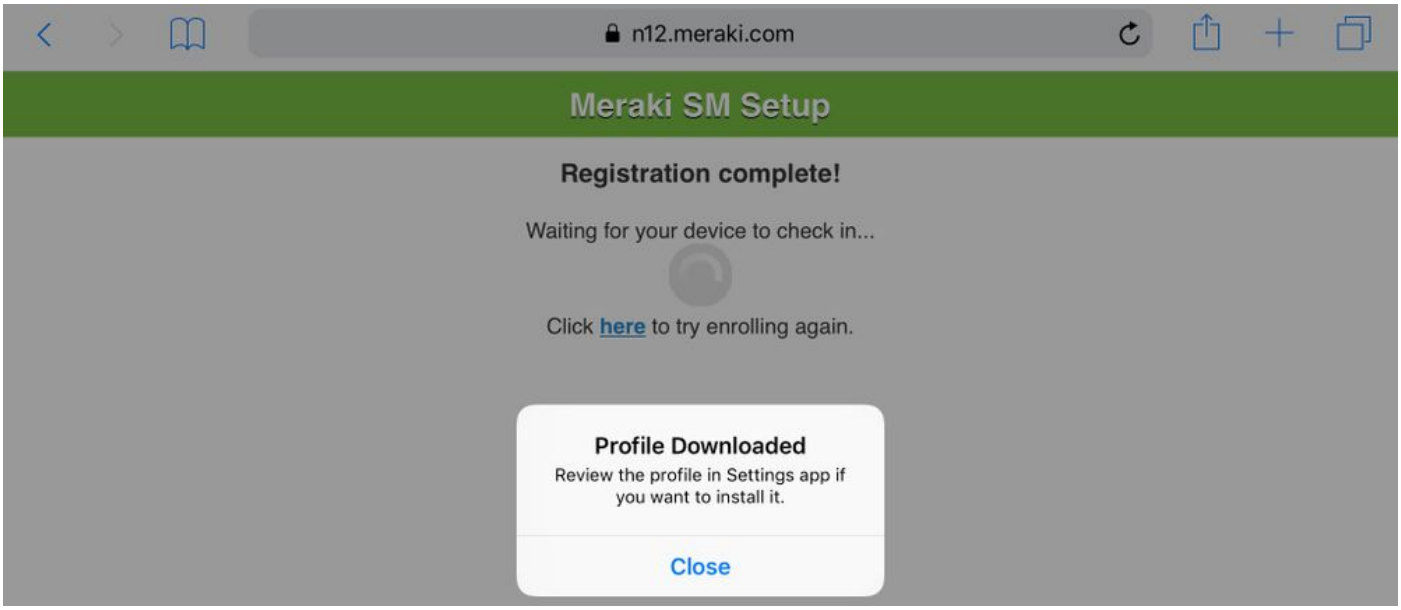


1.5. Cuando se le solicite, seleccione **Register**.

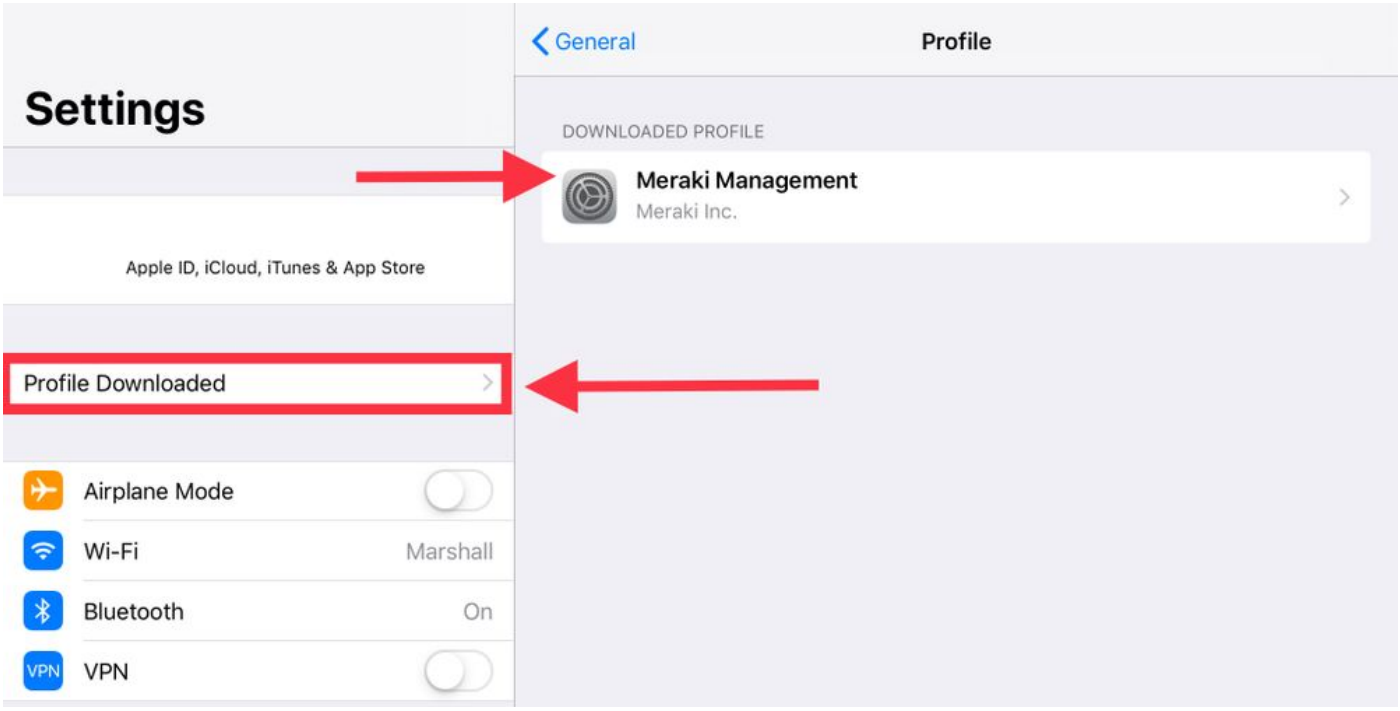
1.6. Seleccione **Allow** para permitir que el dispositivo descargue el perfil MDM.



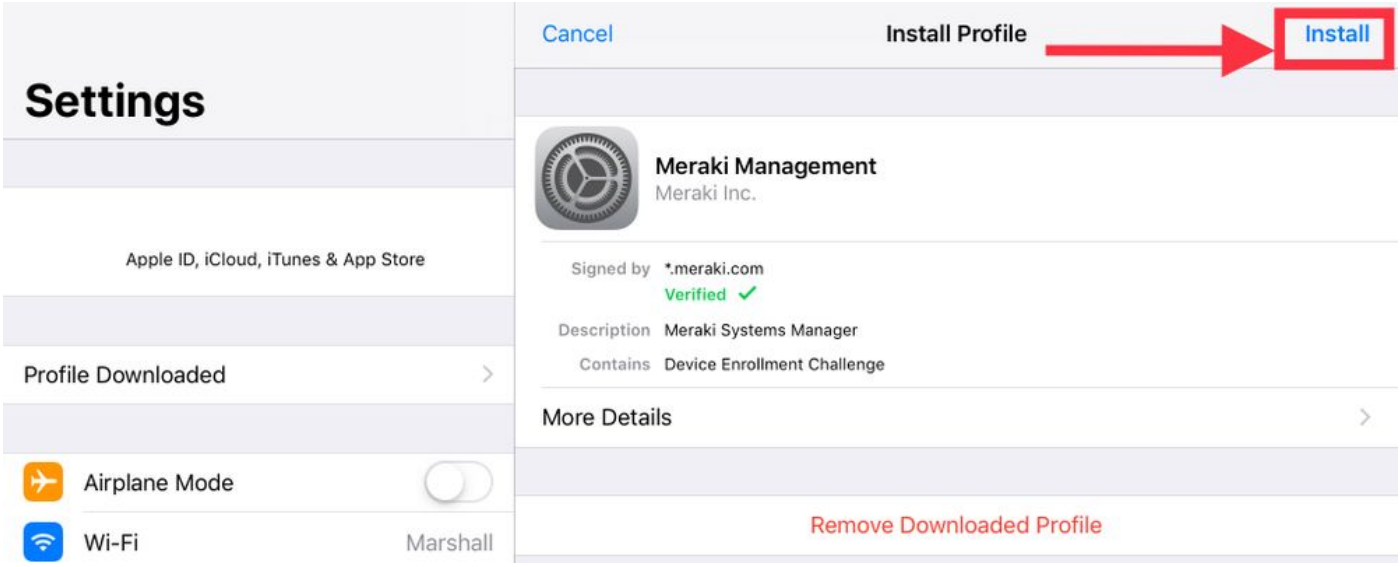
1.7. Seleccione **Cerrar** para completar la descarga.



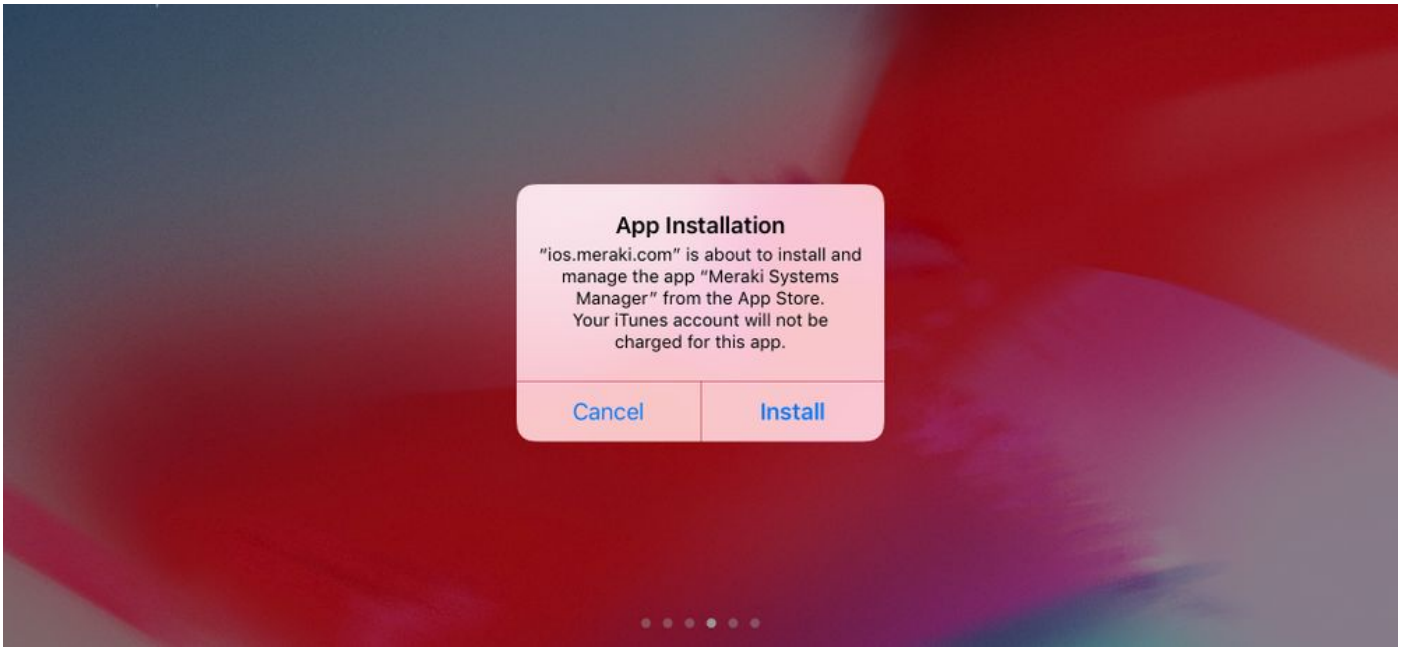
1.8. Navegue hasta la aplicación de configuración de iOS, busque la opción **Profile Downloaded** en el panel izquierdo y seleccione la sección **Meraki Management**.



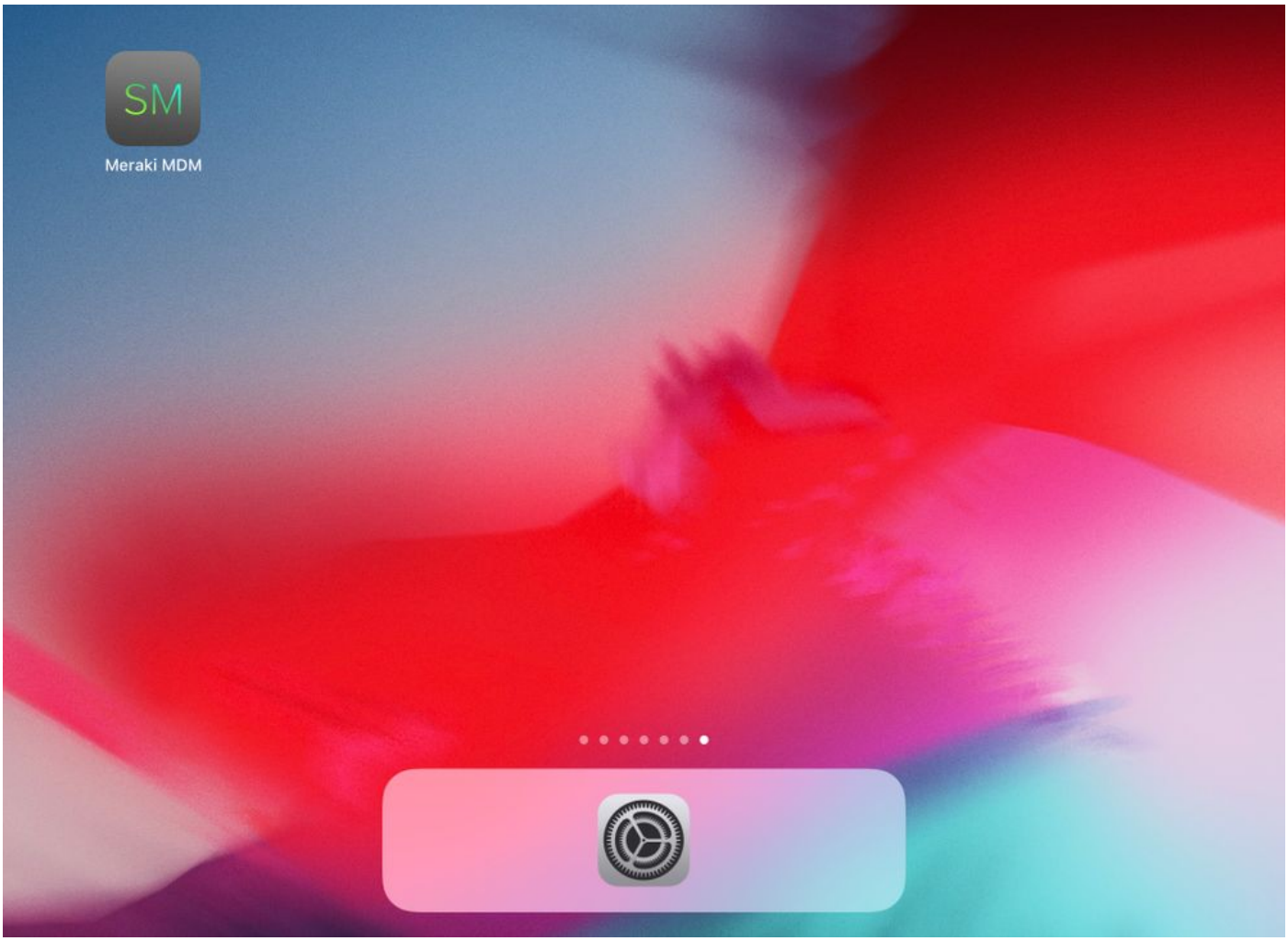
1.9. Seleccione la opción **Install** para instalar el perfil MDM.



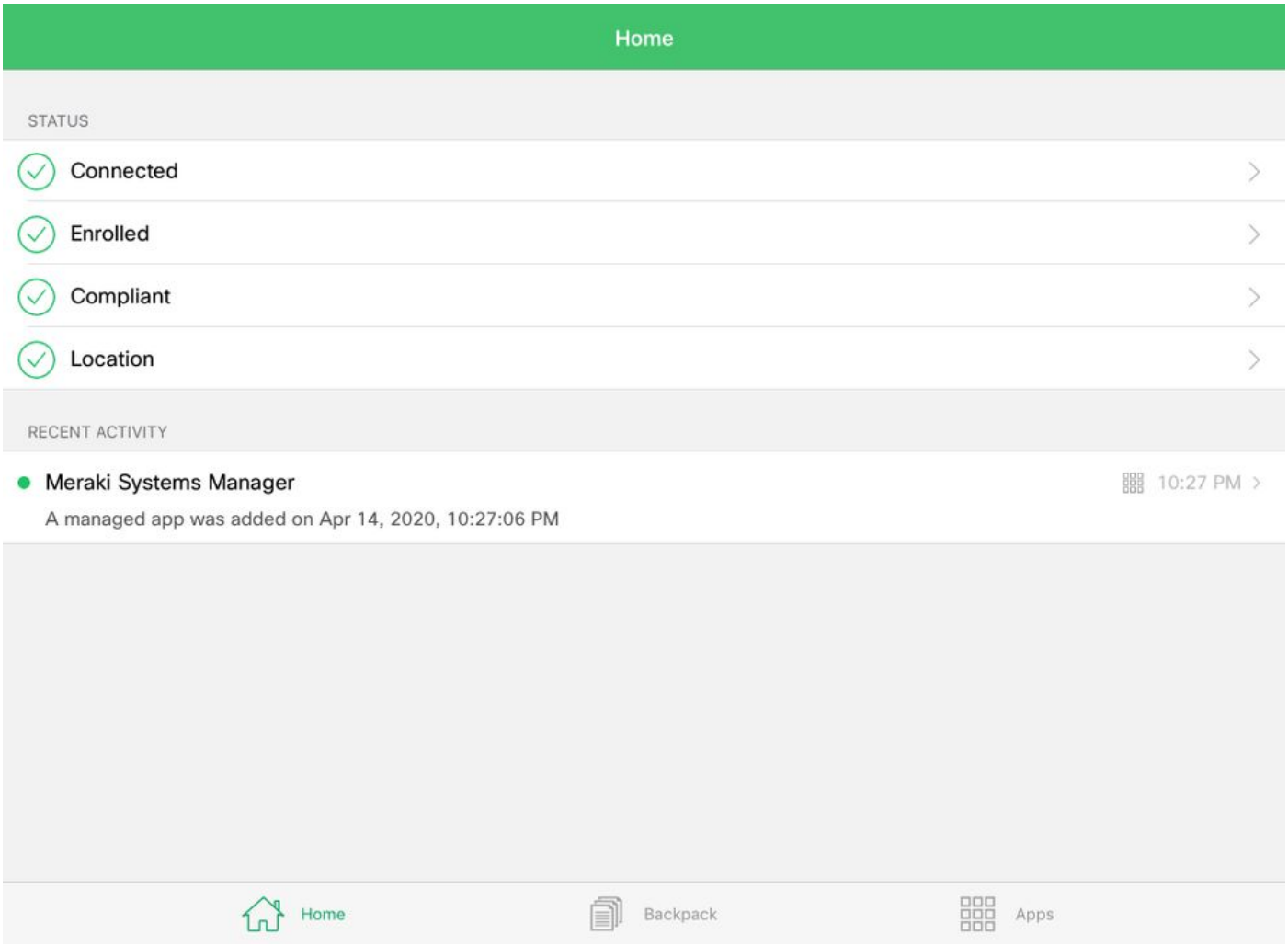
1.10. Debe conceder acceso a **Install** (**Instalar**) la aplicación SM.



1.11. Abra la aplicación descargada recientemente llamada **Meraki MDM** que se encuentra en la pantalla de inicio.



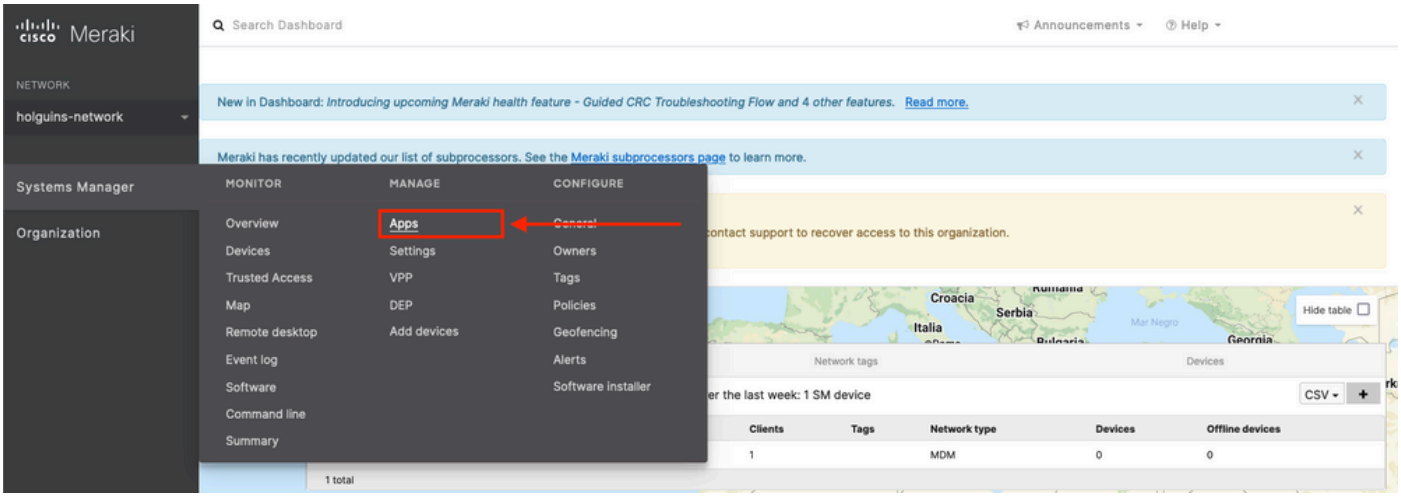
1.12. Verifique que todos los estados tengan una marca verde que confirme que la inscripción está completa.



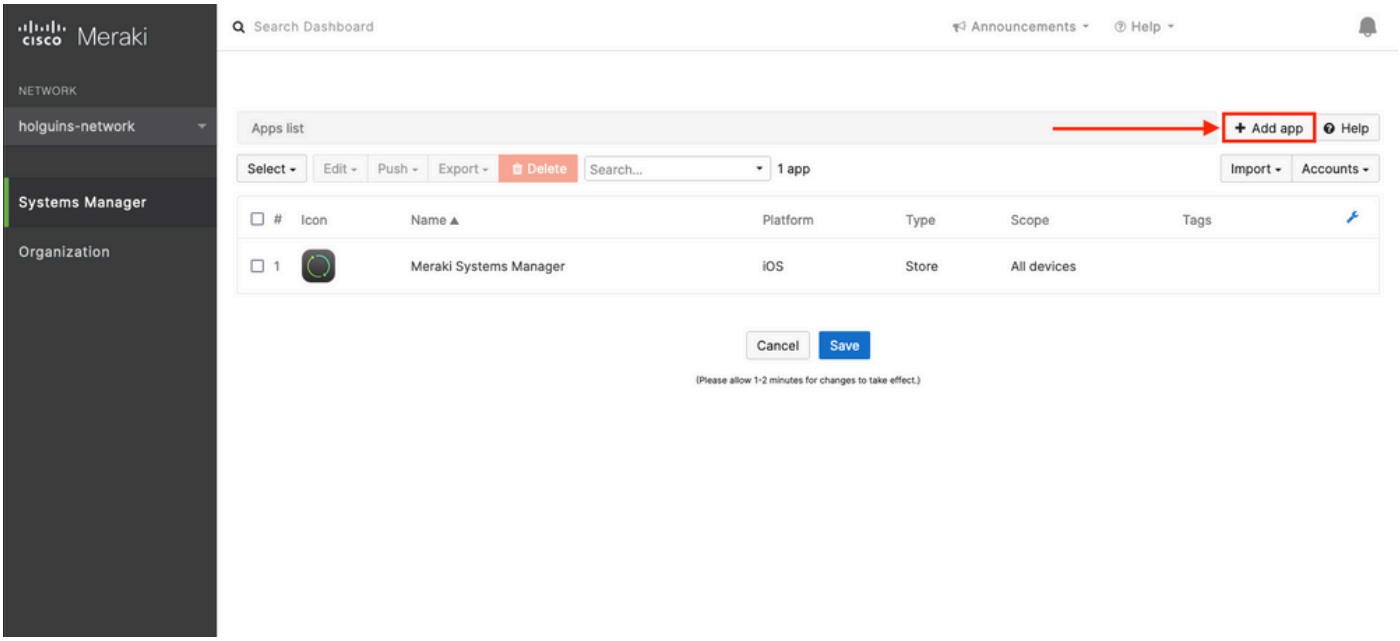
Paso 2. Configuración de aplicaciones gestionadas

Para configurar las aplicaciones tunelizadas para PerApp más adelante en este documento, necesita administrar esas mismas aplicaciones a través de SM. En este ejemplo de configuración, Firefox está diseñado para ser tunelizado a través de Per App, por lo tanto, se agrega a las aplicaciones administradas.

2.1. Navegue hasta **Systems Manager > Manage > Apps** para agregar las aplicaciones administradas.

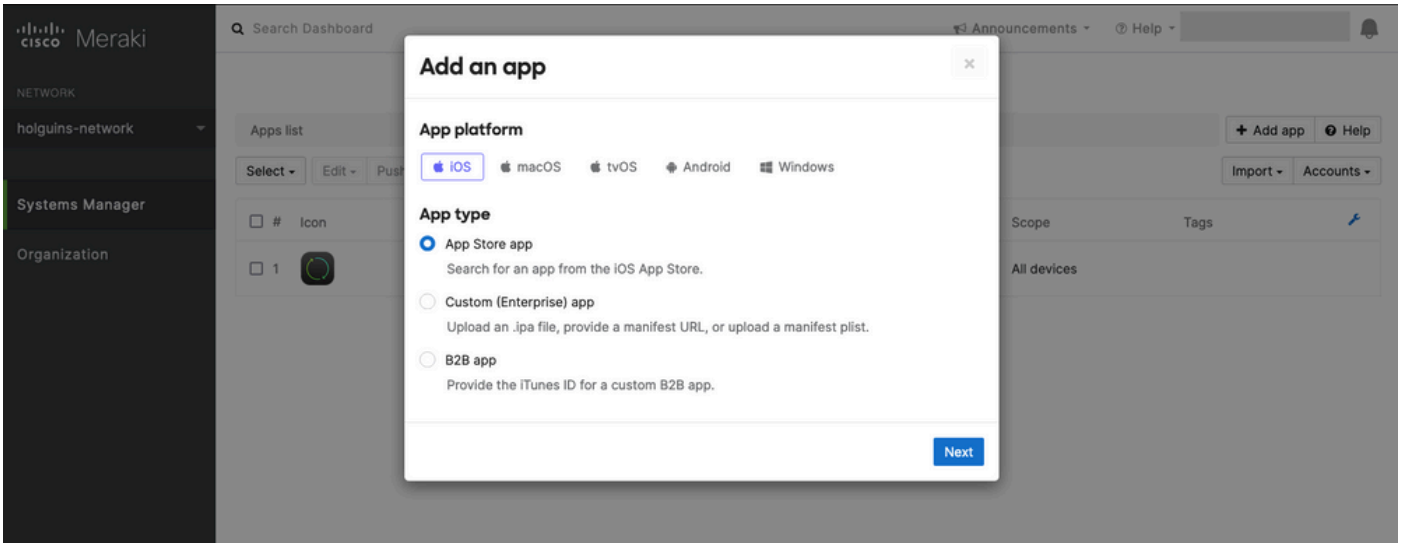


2.2. Seleccione la opción **Add app**.



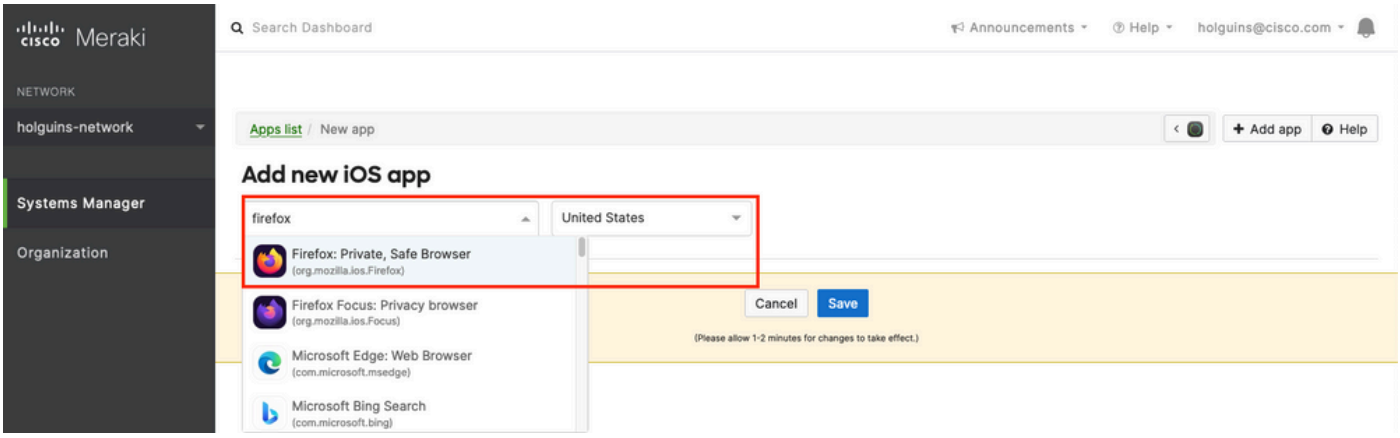
2.3. Seleccione el tipo de aplicación (App Store, aplicación personalizada, B2B) en función de dónde se almacene la aplicación. Seleccione **Next** una vez seleccionado.

En este ejemplo, la aplicación se almacena públicamente en la App Store.



2.4. Cuando se le solicite, busque la aplicación deseada y seleccione la región desde la que se descarga la aplicación. Seleccione **Guardar** una vez que se haya seleccionado la aplicación.

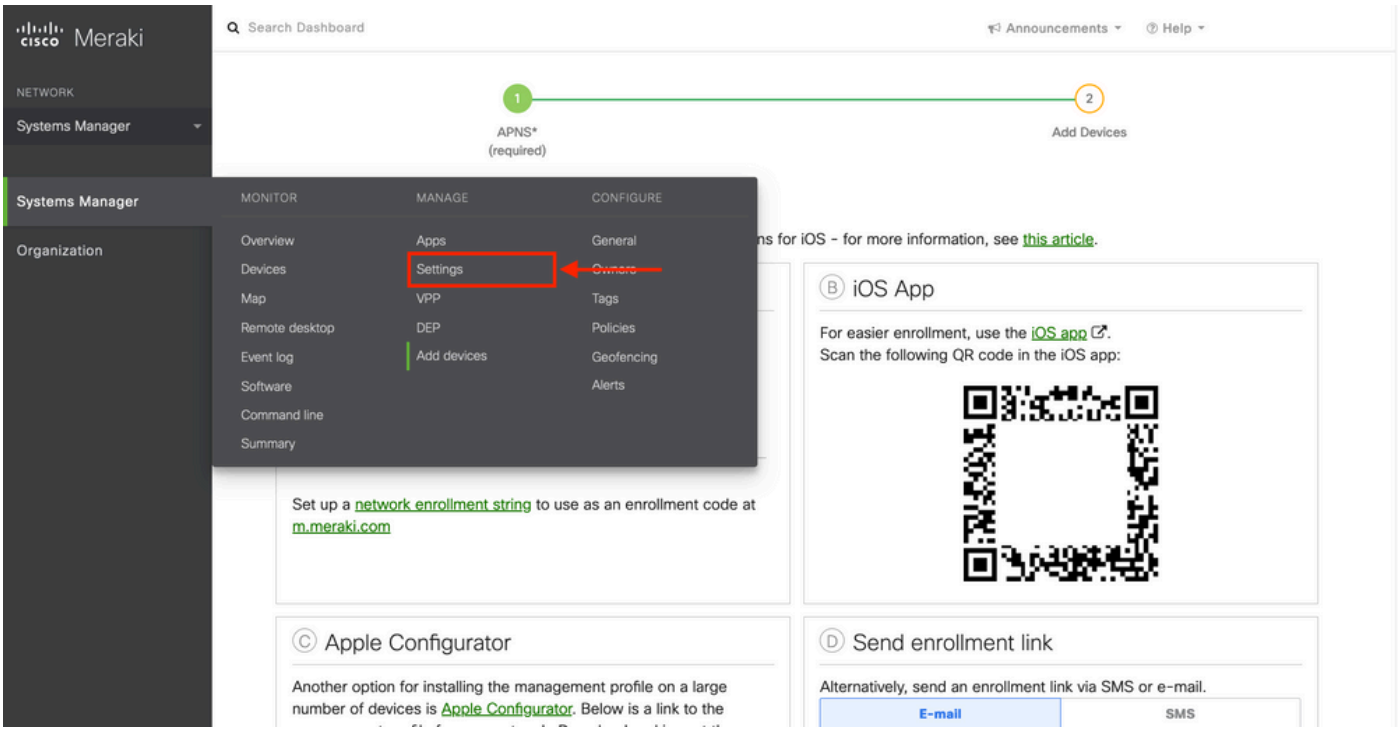
> **Nota**: si el país no coincide con la región de la cuenta de Apple, el usuario puede experimentar problemas con la aplicación.



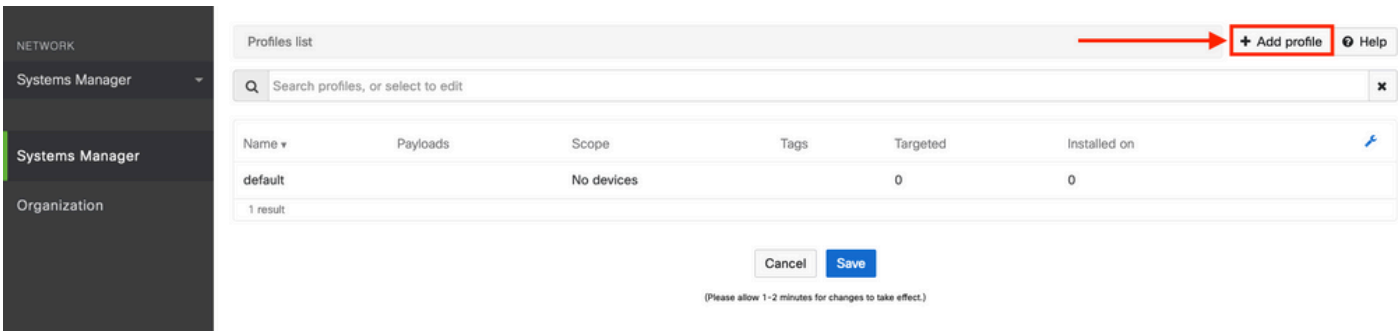
2.5. Haga clic en **Guardar** una vez que seleccione todas las aplicaciones deseadas.

Paso 3. Configurar perfil VPN por aplicación

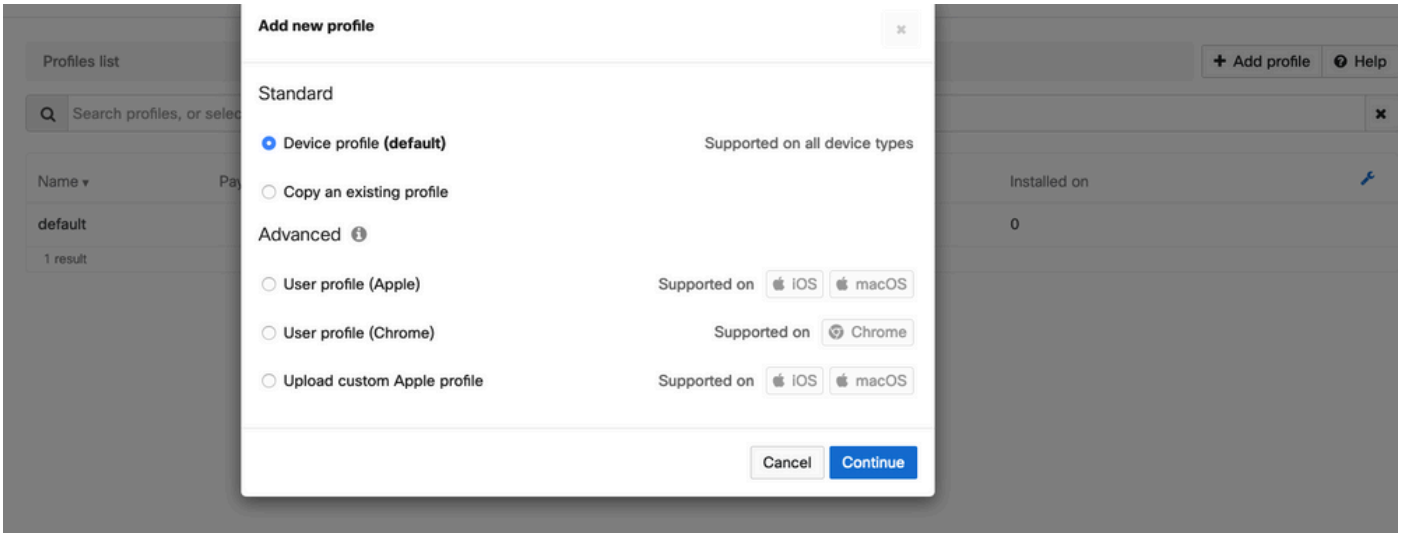
3.1. Vaya a **Systems Manager > Manage > Settings**



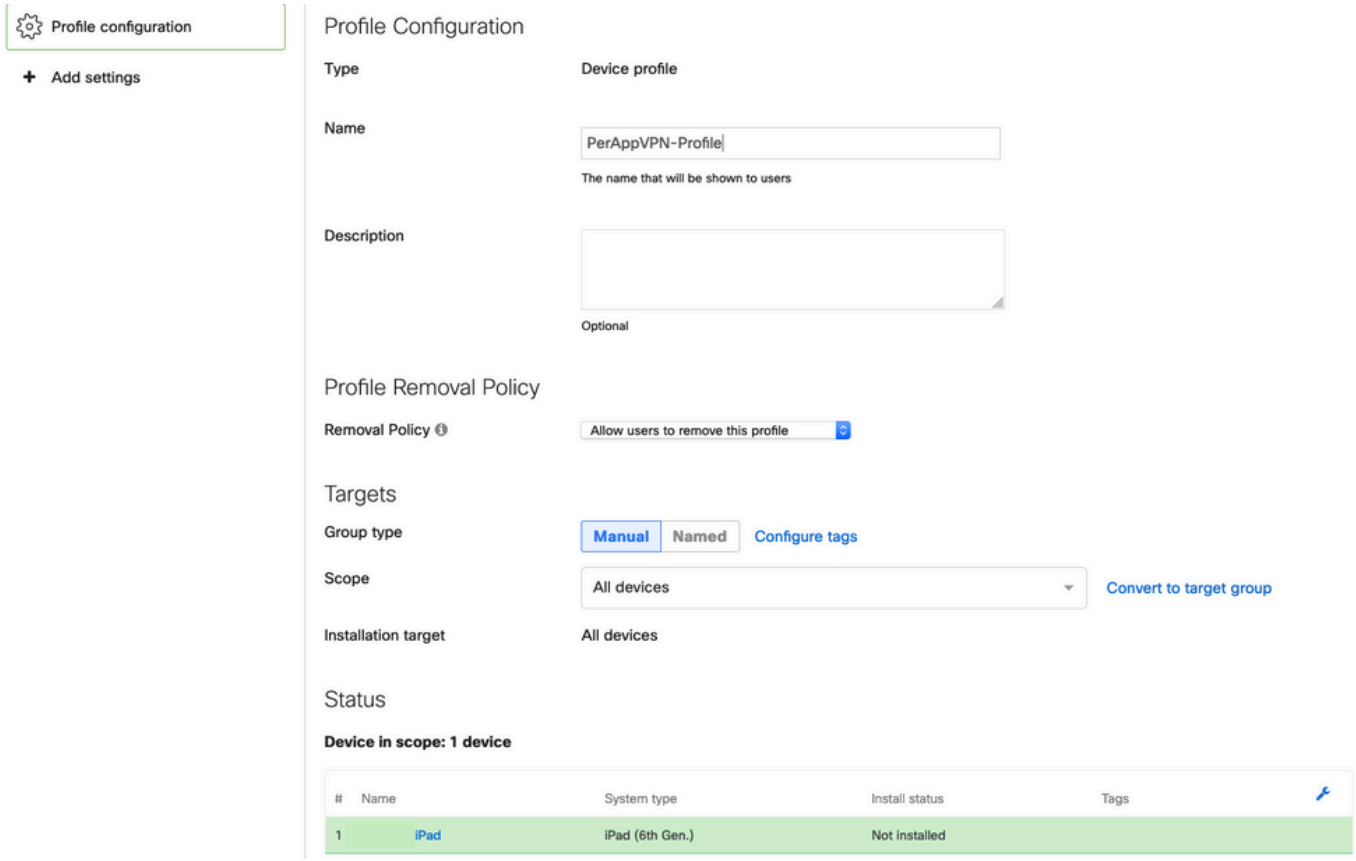
3.2. Seleccione la opción **Agregar perfil**.



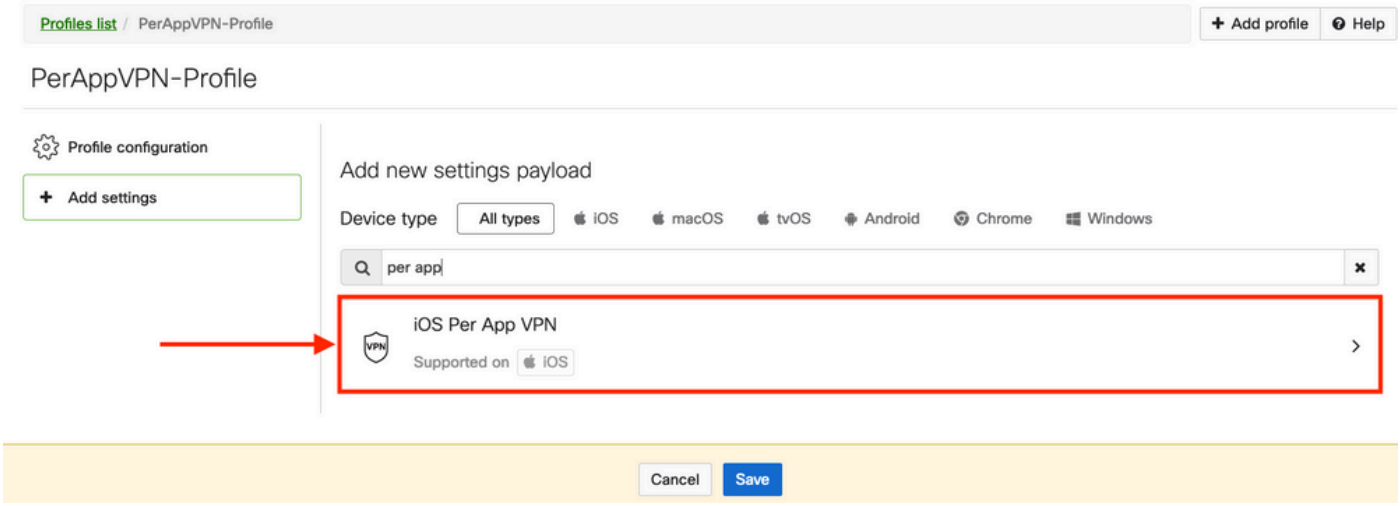
3.3. Seleccione **Perfil del dispositivo (predeterminado)** y haga clic en **Continuar.**



3.4. Una vez que se muestre el menú **Profile Configuration**, escriba el **Name** y seleccione los dispositivos de destino en **Scope**.



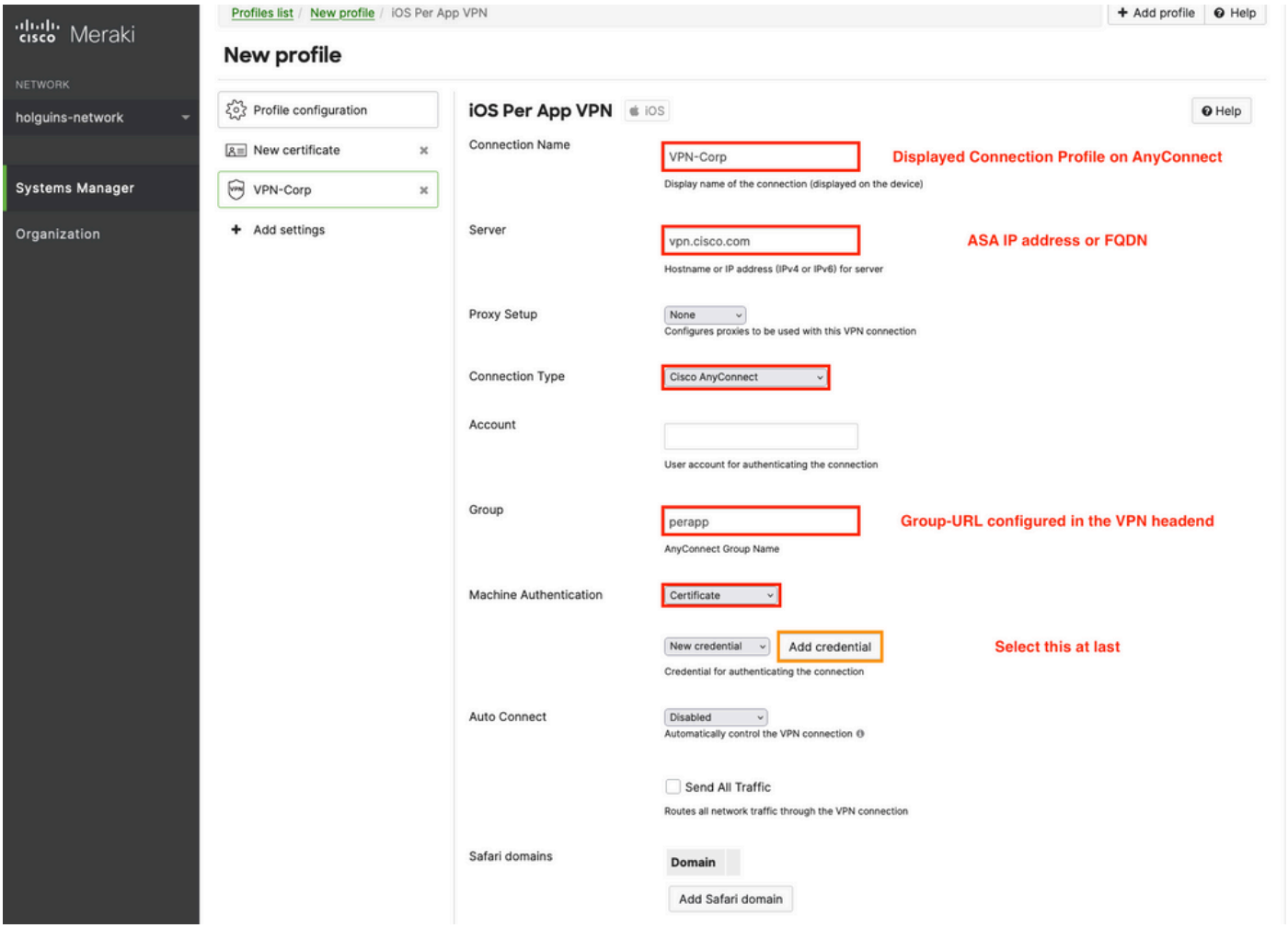
3.5. Seleccione **Add settings** y filtre los tipos de perfil por **iOS Per App VPN**, seleccione la opción que se muestra a continuación.



3.6. Una vez que se muestre el menú, escriba la información de conexión basada en el siguiente ejemplo.

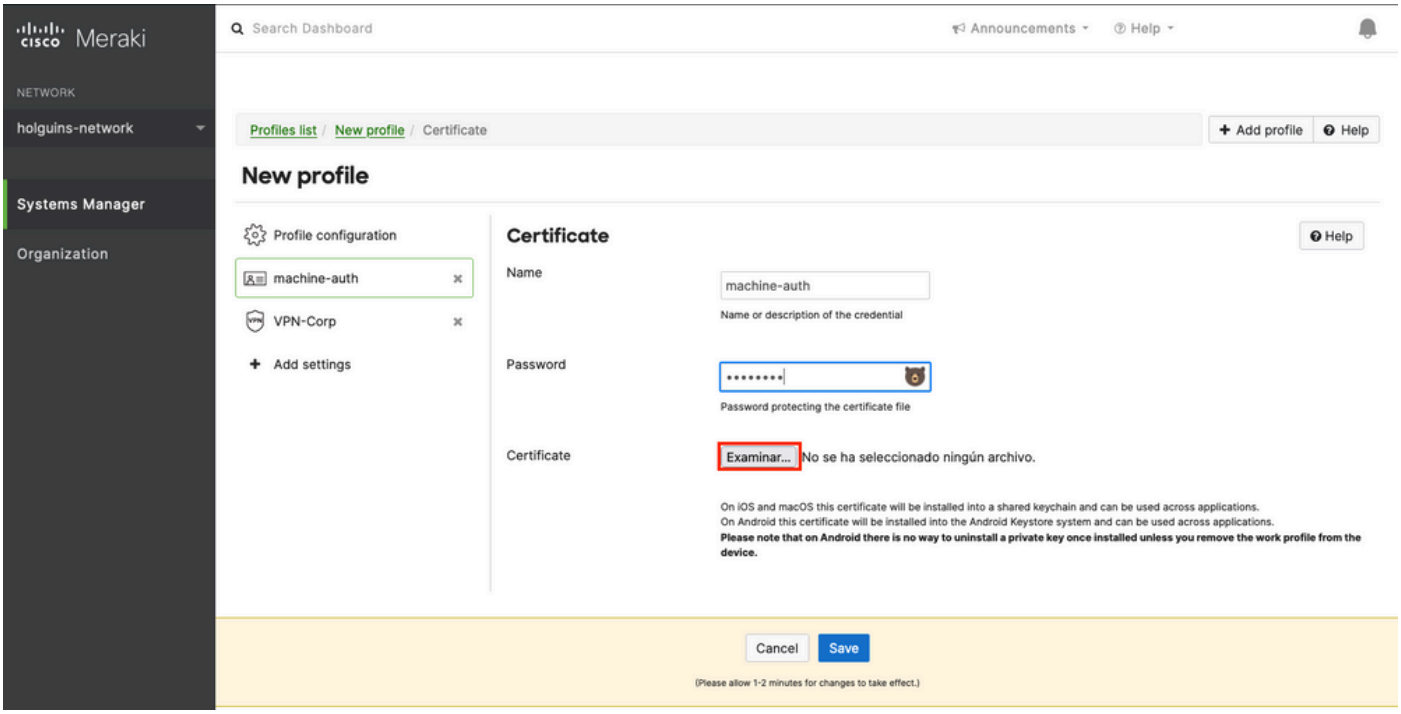
Systems Manager admite dos inscripciones de certificados para estas conexiones, SCEP e inscripción manual. En este ejemplo se utilizó la inscripción manual.

> **Nota**: Seleccione **Agregar credencial** una vez que haya rellenado los cuadros de texto, ya que esta opción le lleva a un nuevo menú para agregar un archivo de certificado.

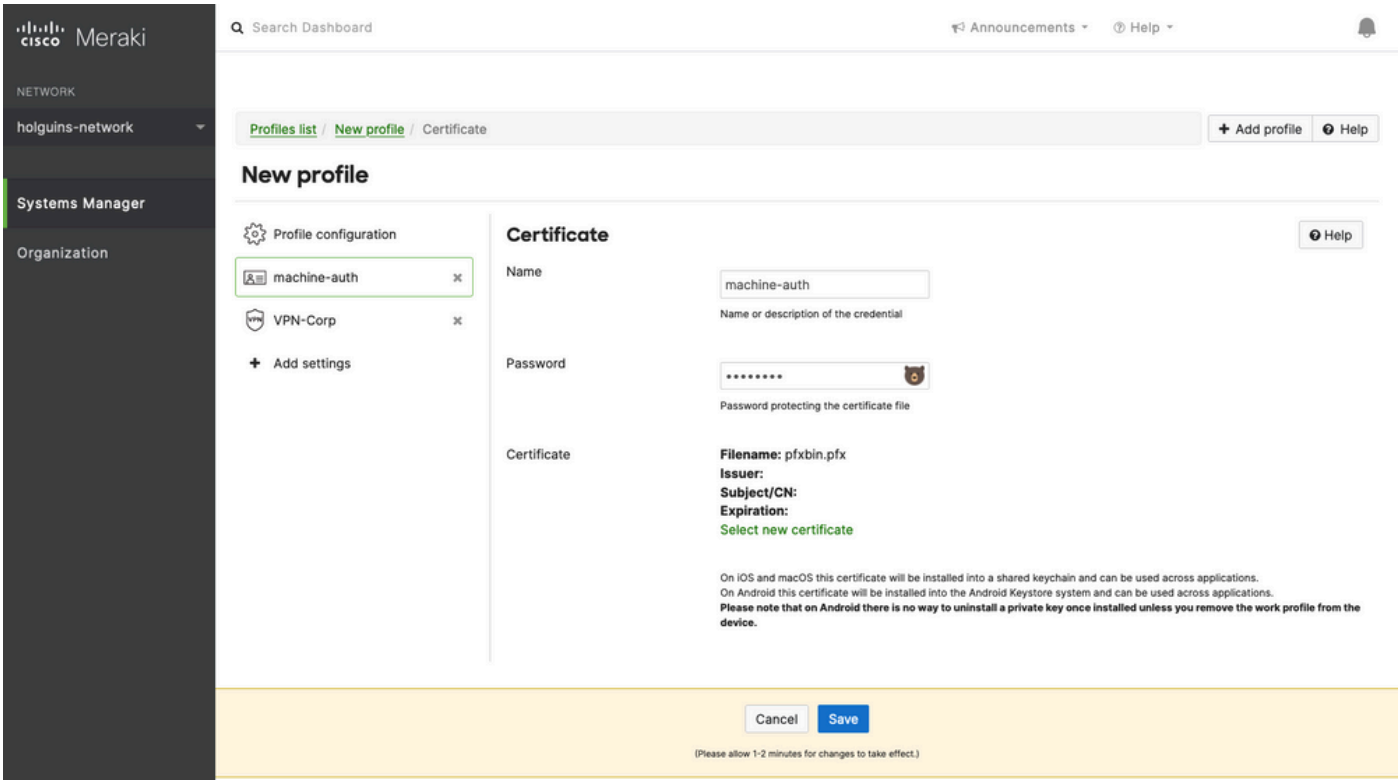


3.7. Una vez que hizo clic en **Agregar credencial** y fue redirigido al menú Certificado, escriba el **Nombre** del Certificado, navegue en su computadora y busque la **Contraseña** que protege el

archivo .pfx (archivo de certificado cifrado).

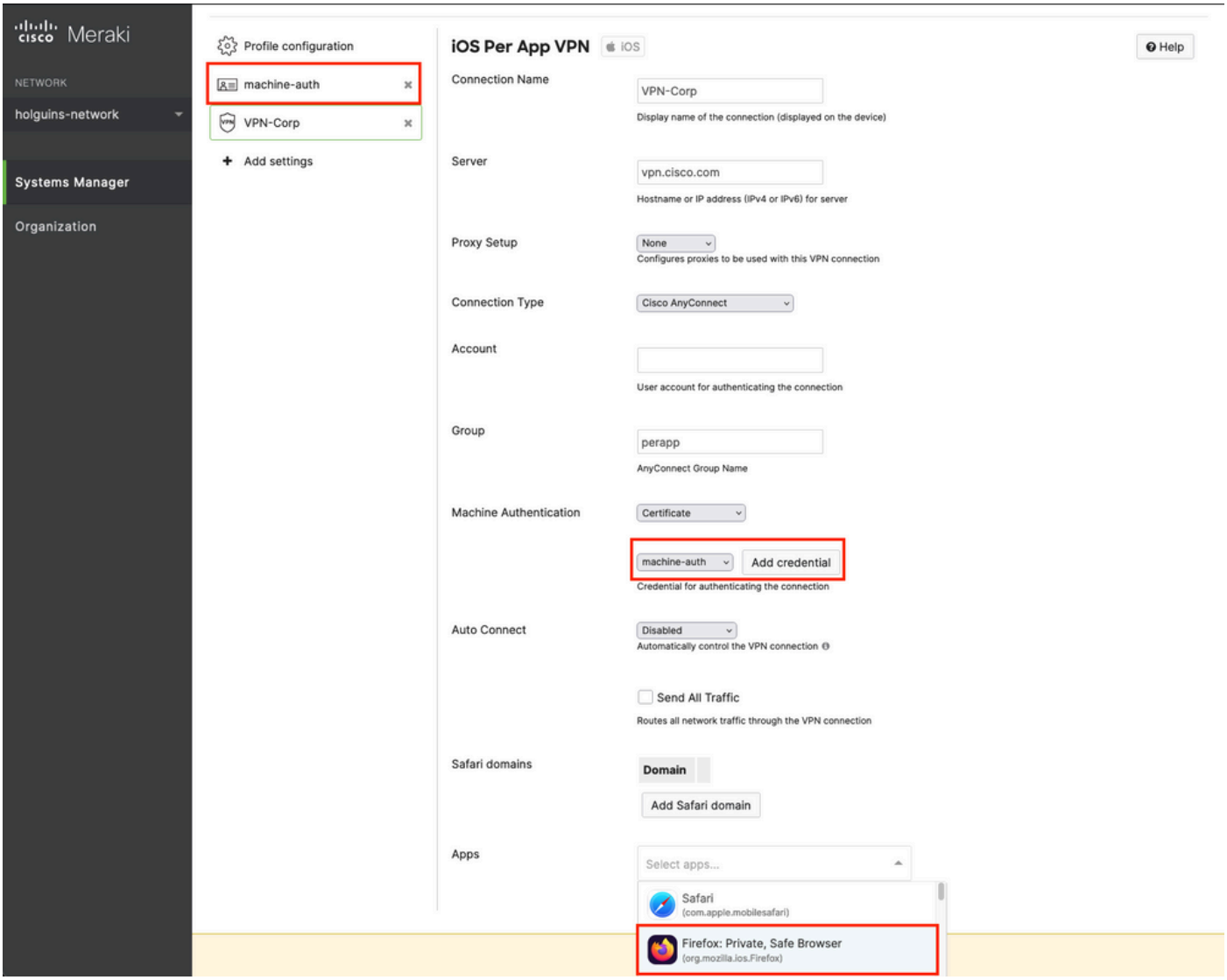


3.8. Una vez seleccionado el certificado, se muestra el nombre de archivo del certificado.

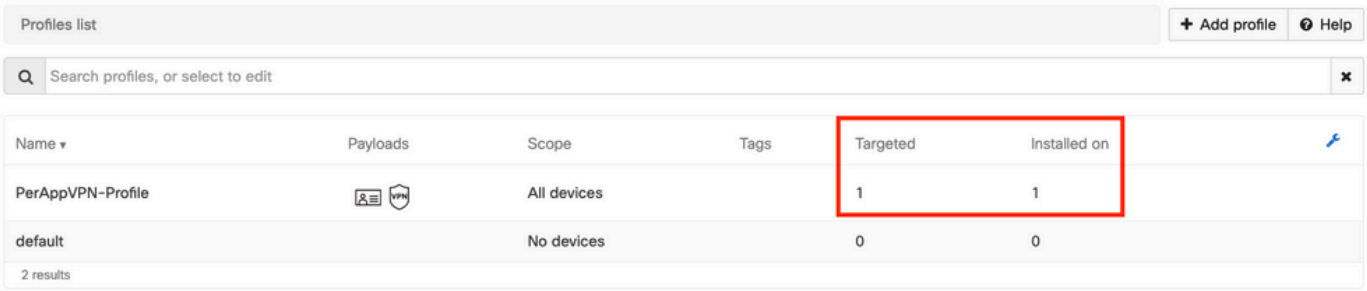


3.9. Una vez seleccionado el certificado, navegue hasta el perfil VPN en el que estaba anteriormente y seleccione la credencial importada recientemente y Seleccione la aplicación tunelizada (Firefox en este caso).

Haga clic en **Guardar** una vez que se haya completado.



3.10. Compruebe que el perfil está instalado en los dispositivos de destino.

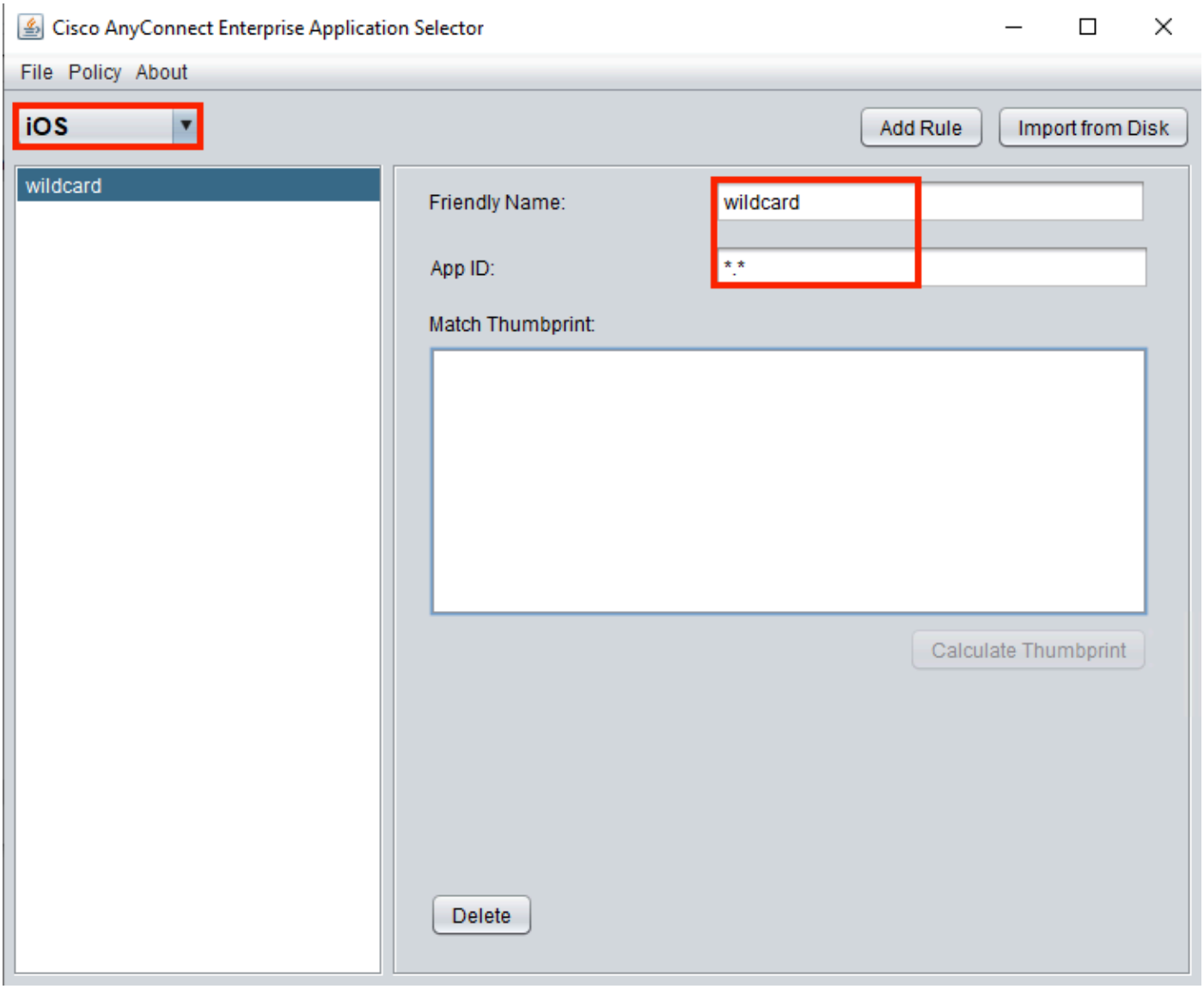


Paso 4. Configuración del selector de aplicaciones

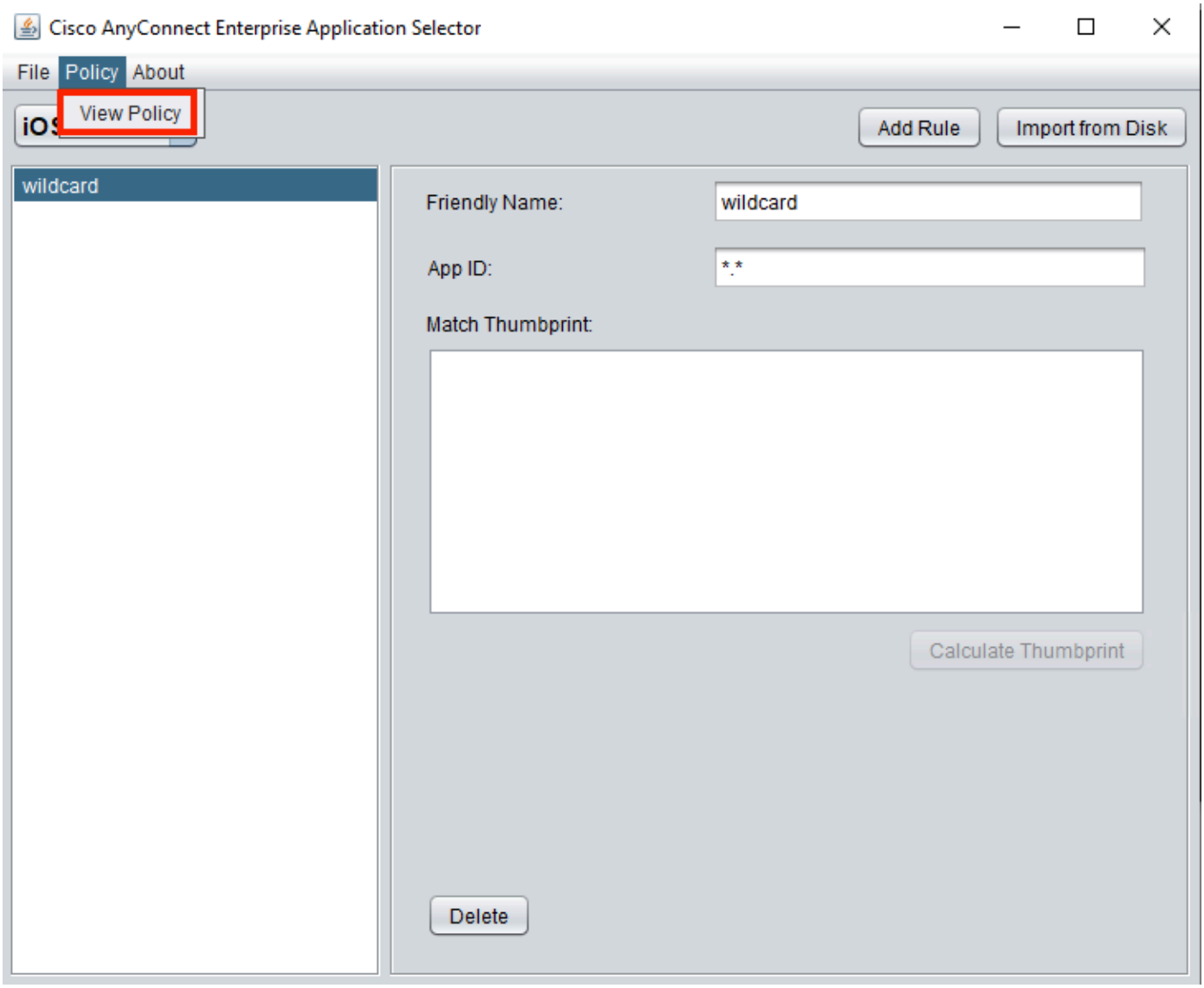
4.1. Descargue el selector de aplicaciones del sitio web de cisco https://software.cisco.com/download/home/286281283/type/282364313/release/AppSelector-2.0

> **Precaución**: ejecute la aplicación en un equipo con Windows. Los resultados mostrados no son los esperados cuando la herramienta se utiliza en dispositivos MacOS.

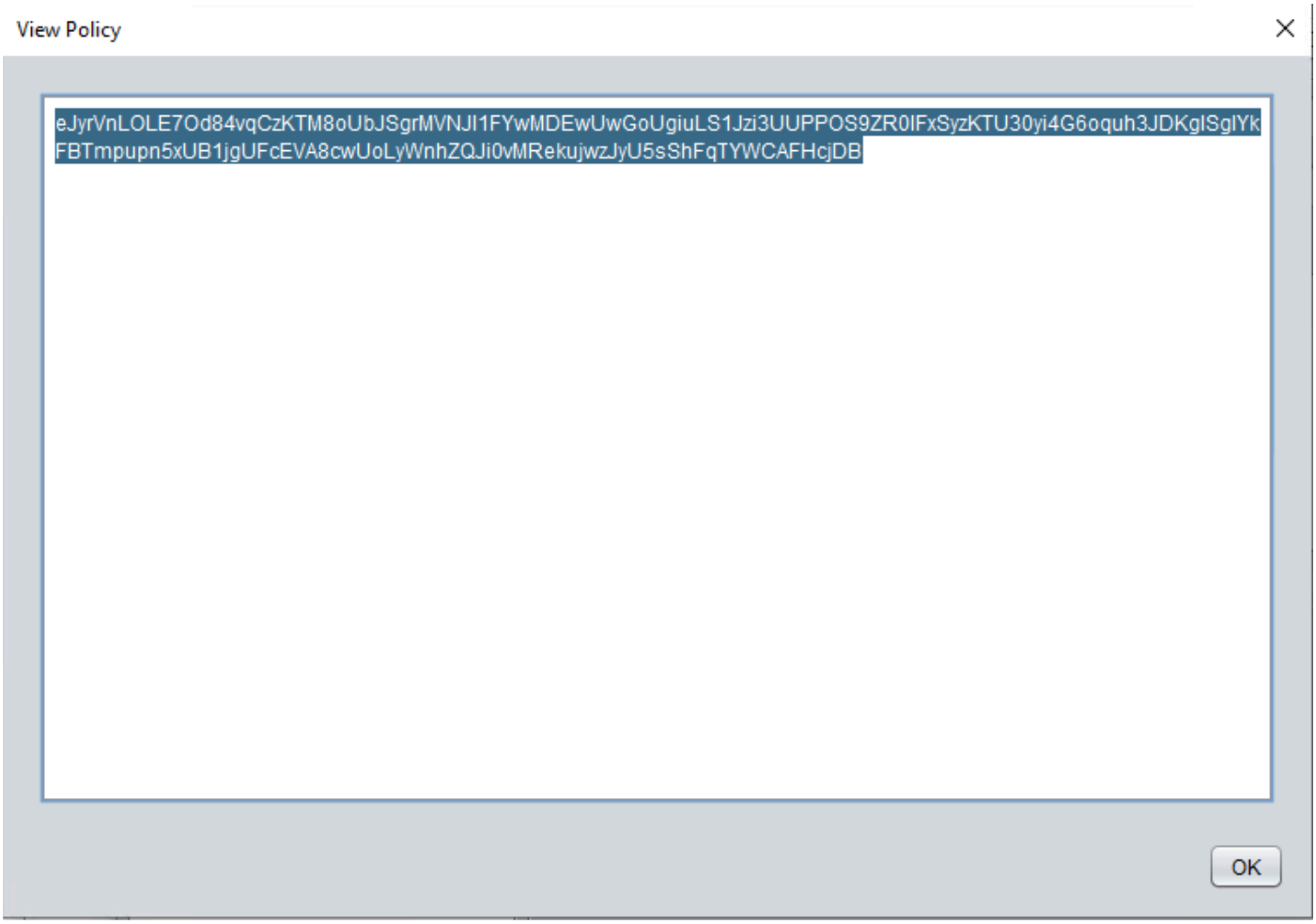
4.2. Abra la aplicación Java. Seleccione **iOS** en el menú desplegable, agregue un nombre descriptivo y asegúrese de escribir ***.*** en el **App ID**.



4.3. Navegue hasta **Política** y seleccione **Ver Política**



4.4. Copie la cadena mostrada. (Se utiliza más adelante en la configuración de cabecera de VPN).



Paso 5. Ejemplo de configuración VPN por aplicación de ASA

```
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
```

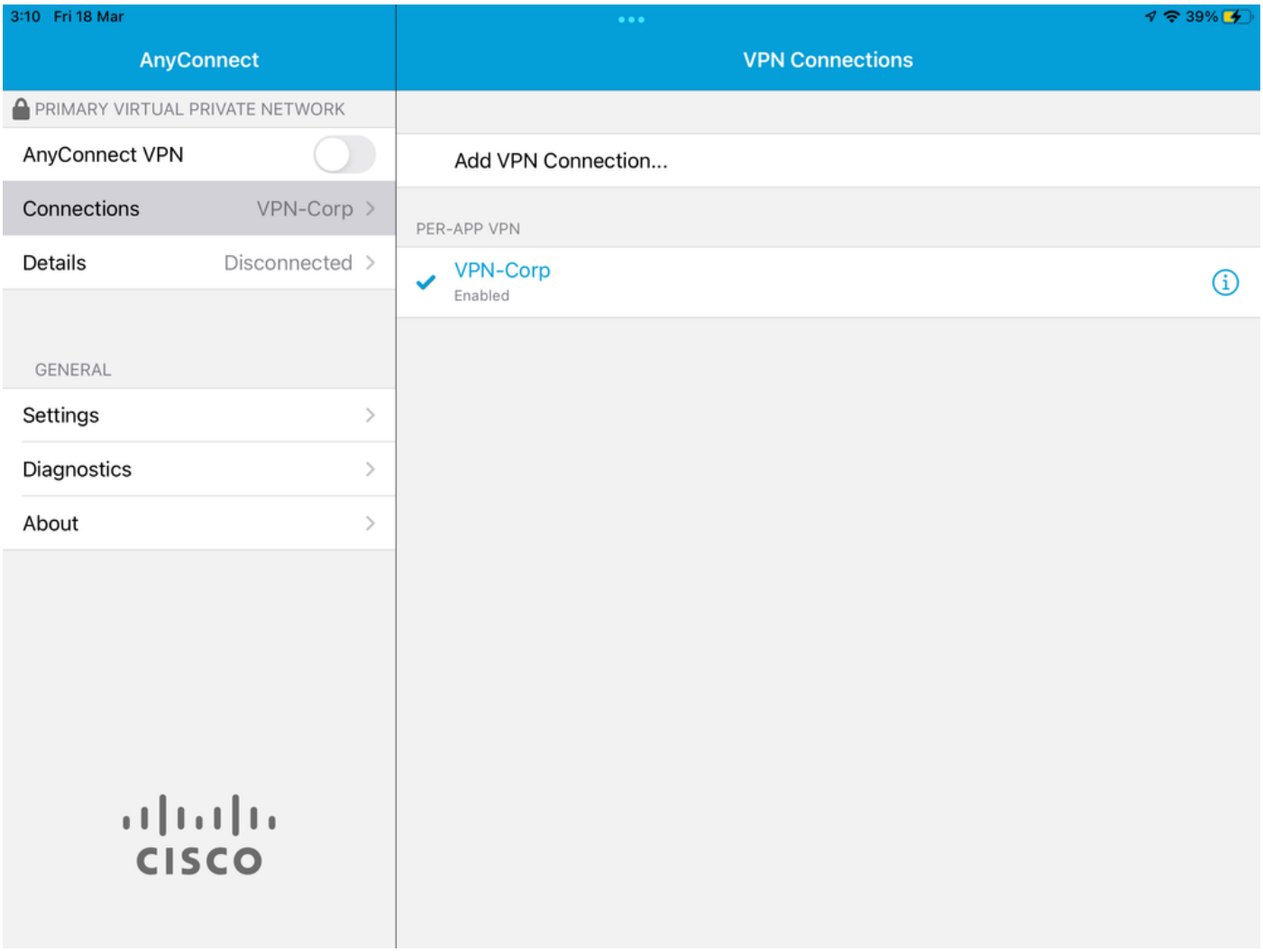
```
group-url https://vpn.cisco.com/perapp enable
```

Verificación

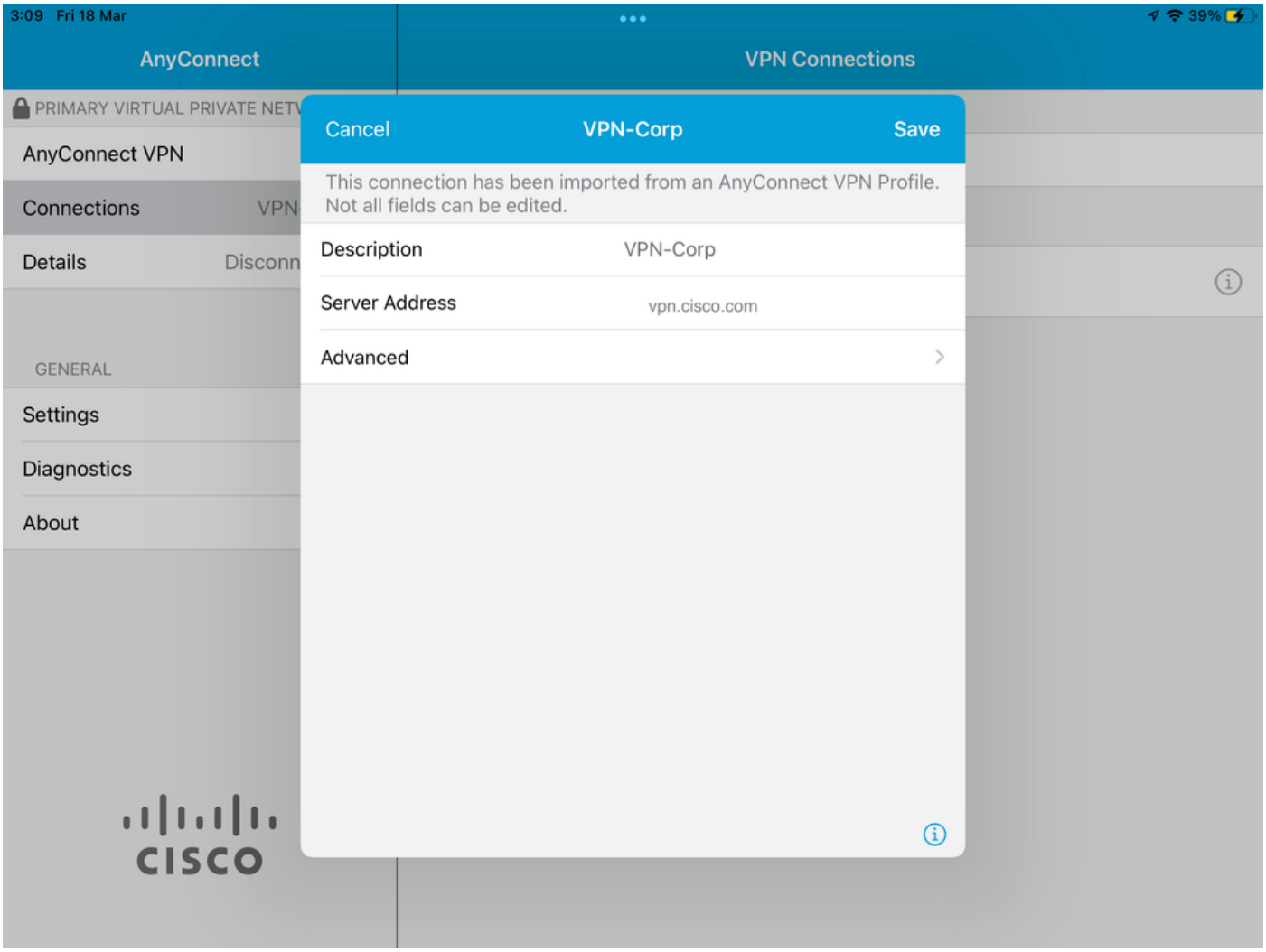
6. Verificar la instalación del perfil en la aplicación AnyConnect

6.1. Abra la aplicación AnyConnect y seleccione **Connections** en el panel izquierdo. El perfil VPN por aplicación debe mostrarse en una nueva sección denominada **VPN por aplicación**.

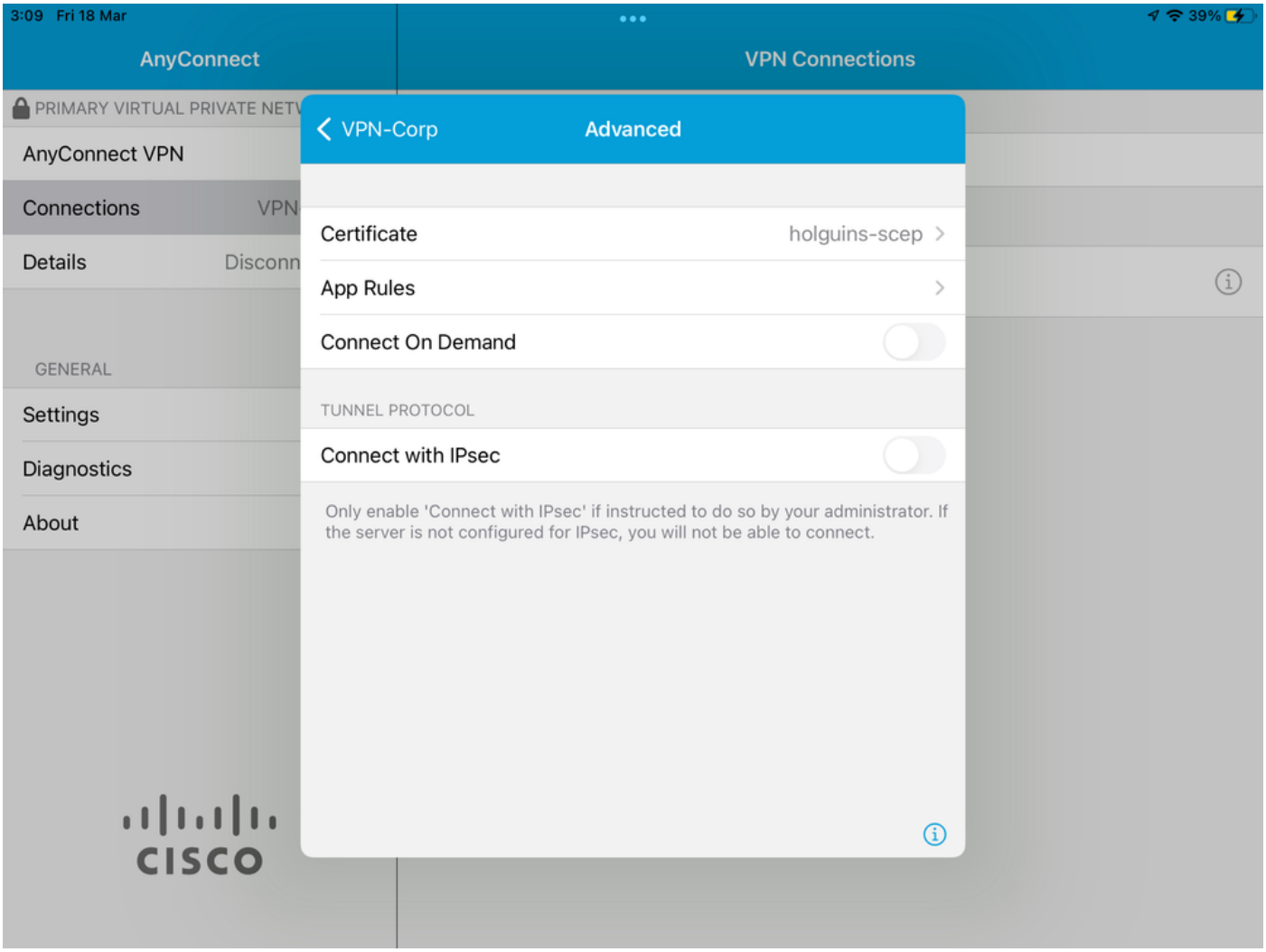
Seleccione **i** para mostrar los parámetros avanzados.



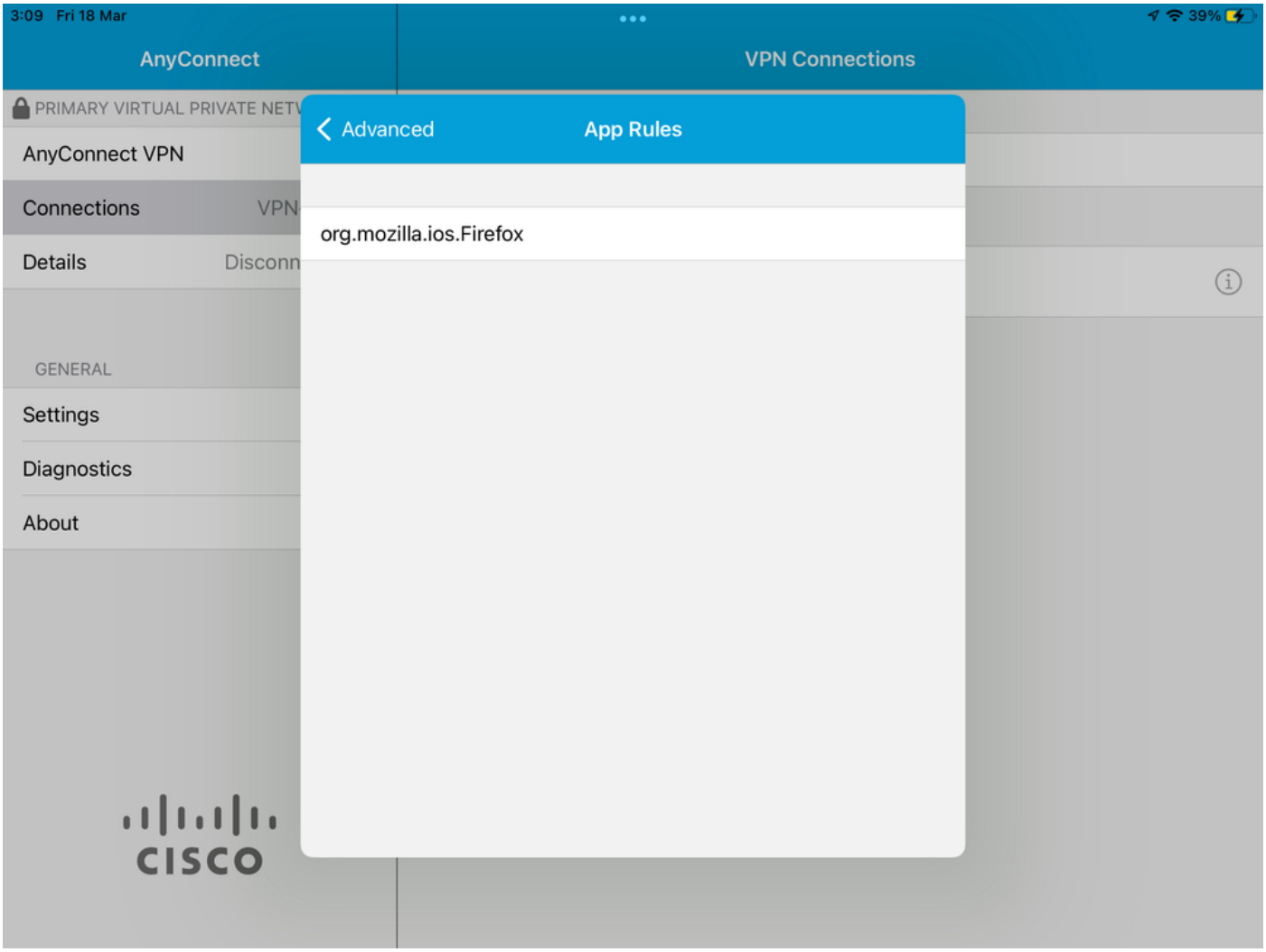
6.2. Seleccione la opción **Advanced**.



6.3. Seleccione la opción **App Rules**.



6.4. Por último, confirme que la regla de aplicación está instalada. (Mozilla es la aplicación tunelizada deseada en este documento, por lo que la instalación de la aplicación fue exitosa).



Troubleshoot

Actualmente no hay pasos específicos para solucionar problemas de este documento.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).