Deploy Security Connector with Intune

Contents

Introduction

This document describes how to deploy the Security Connector using Intune.

Overview

This is a step-by-step guide on how to get your iOS/iPadOS device MDM-manage via Intune, and push the profile via Apple Configurator

You can also reference our Intune Registration documentation and PDF guide here

Note: this method shows you how to MDM your devices via Intune and Apple Configurator

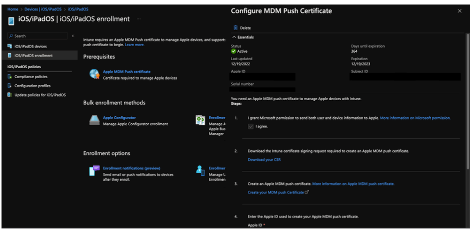
Important Notes:

If you are MDM-ing your **supervised** devices via the Company Portal App, then you can start at Step 14.

This article is provided as-is as of 04/12/2023, Umbrella support does not guarantee these instructions will remain valid after this date and is subject to change based on updates from Microsoft Intune and Apple iOS.

Procedure

1. Log into the Azure Portal and search for "Intune". Alternatively, go to https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/ and login
2. Once you are on the Intune homepage, go to **Devices** --> **iOS/iPadOS** --> **iOS/iPadOS enrollment** --> **Apple MDM Push certificate** and click "Download your CSR"


Home > Devices | iOS/iPadOS > iOS/iPadOS
iOS/iPadOS | iOS/iPadOS enrollment
Search
iOS/iPadOS devices
iOS/iPadOS enrollment
iOS/iPadOS policies
Compliance policies
Configuration profiles
Update policies for iOS/iPadOS
Prerequisites
Apple MDM Push certificate
Certificate required to manage Apple devices
Bulk enrollment methods
Apple Configurator
Manage Apple Configurator enrollment
Enrollmer
Manage A
Apple Bus
Manager
Enrollment options
Enrollment notifications (preview)
Send email or push notifications to devices after they enroll.
Enrollmer
Manage U
Enrollmen
Configure MDM Push Certificate
Delete
Essentials

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports push certificate to begin. Learn more.

Status: Active

Days until expiration: 364

Last updated: 12/19/2022

Expiration: 12/19/2023

Apple ID: [redacted]

Subject ID: [redacted]

Serial number: [redacted]

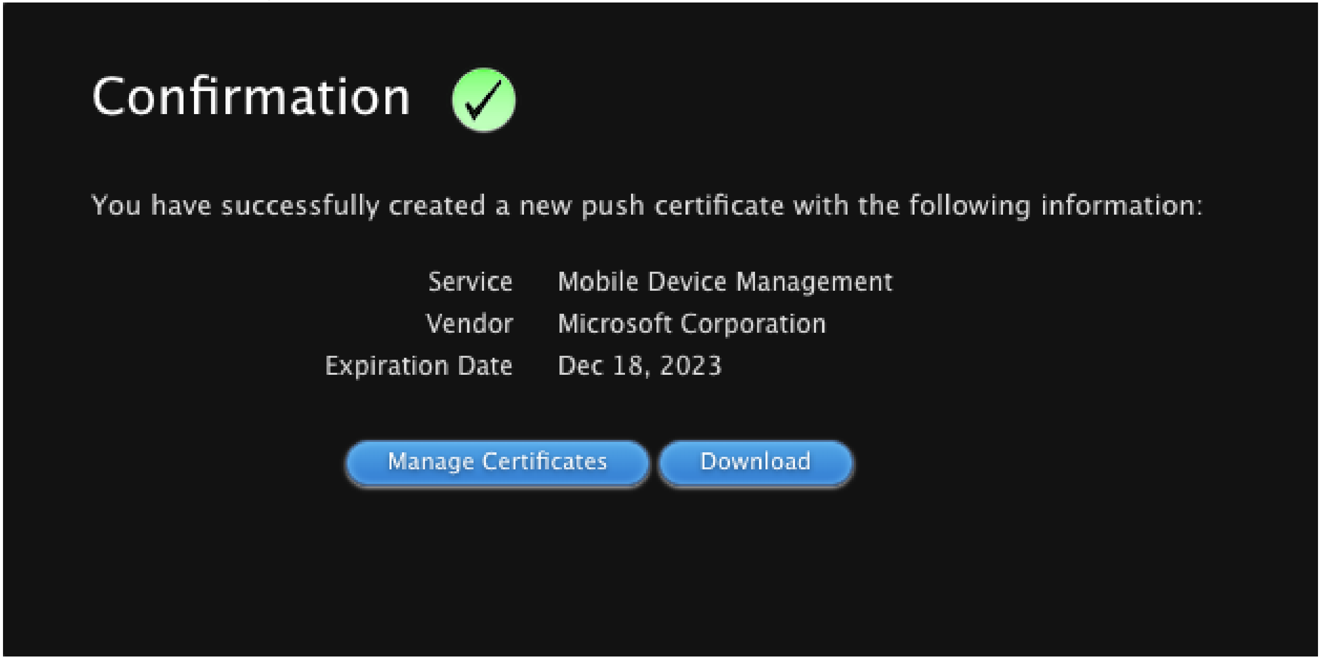
You need an Apple MDM push certificate to manage Apple devices with Intune.
Steps:

1. I grant Microsoft permission to send both user and device information to Apple. More information on Microsoft permission.
   ☑ I agree.
2. Download the Intune certificate signing request required to create an Apple MDM push certificate.
   Download your CSR
3. Create an Apple MDM push certificate. More information on Apple MDM push certificate.
   Create your MDM push Certificate
4. Enter the Apple ID used to create your Apple MDM push certificate.
   Apple ID *

11752925317012

3. Then, click on "Create your MDM push Certificate", which redirects you to https://identity.apple.com/pushcert/
4. On the Apple Push Certificates Portal, go to "Create a Certificate" and upload the **IntuneCSR.csr** file

you just downloaded. Once the CSR file has been uploaded successfully, click "Download" to download the Privacy Enhanced Mail (*.pem* file) and proceed to the next step



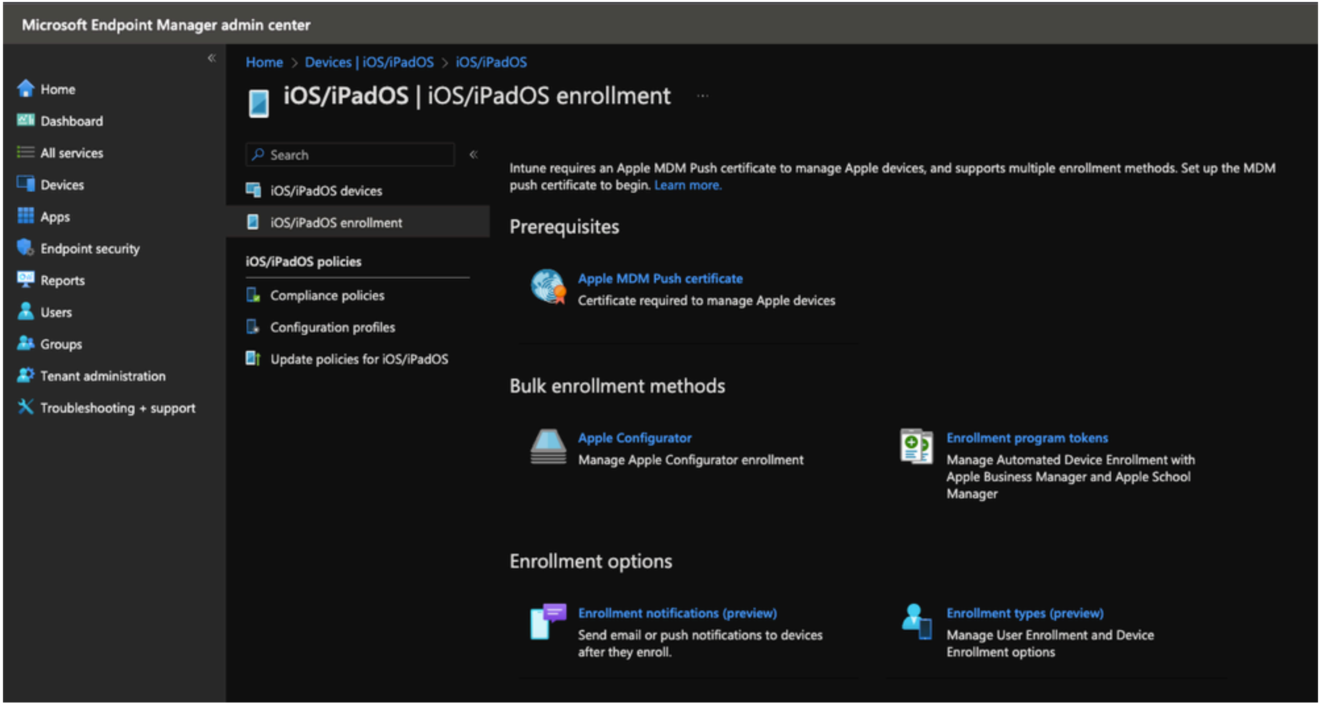
Confirmation ✓

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Microsoft Corporation
Expiration Date	Dec 18, 2023

11752968667924

5. Enter the email address of your Apple ID account that you used to sign into the Apple Push Certificates Portal and upload the *.pem* file under "Apple MDM push certificate" and press "Upload". If the upload is successful, you see the other options for the "Bulk enrollment methods" unlock.



iOS/iPadOS | iOS/iPadOS enrollment

Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more.

Prerequisites

Apple MDM Push certificate
Certificate required to manage Apple devices

Bulk enrollment methods

Apple Configurator
Manage Apple Configurator enrollment

Enrollment program tokens
Manage Automated Device Enrollment with Apple Business Manager and Apple School Manager

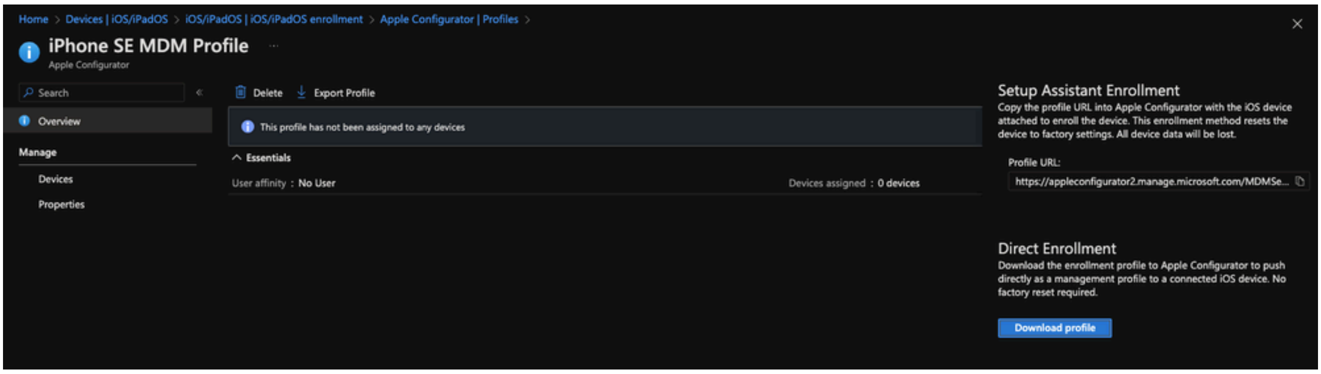
Enrollment options

Enrollment notifications (preview)
Send email or push notifications to devices after they enroll.

Enrollment types (preview)
Manage User Enrollment and Device Enrollment options

11752971407380

6. Go to **Apple Configurator** --> **Profiles** --> **Create** and create a new profile. Give it a meaningful name and for **User affinity** select "Enroll without user affinity". Once that profile has been created, click into your newly created profile and select "Export Profile" and then "Download Profile" on the right hand side


Home > Devices | iOS/iPadOS > iOS/iPadOS | iOS/iPadOS enrollment > Apple Configurator | Profiles >

iPhone SE MDM Profile

Apple Configurator

This profile has not been assigned to any devices

Essentials

User affinity : No User

Devices assigned : 0 devices

Setup Assistant Enrollment

Copy the profile URL into Apple Configurator with the iOS device attached to enroll the device. This enrollment method resets the device to factory settings. All device data will be lost.

Profile URL:

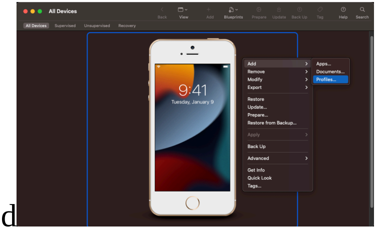
https://appleconfigurator2.manage.microsoft.com/MDMSe...

Direct Enrollment

Download the enrollment profile to Apple Configurator to push directly as a management profile to a connected iOS device. No factory reset required.

11753020728596

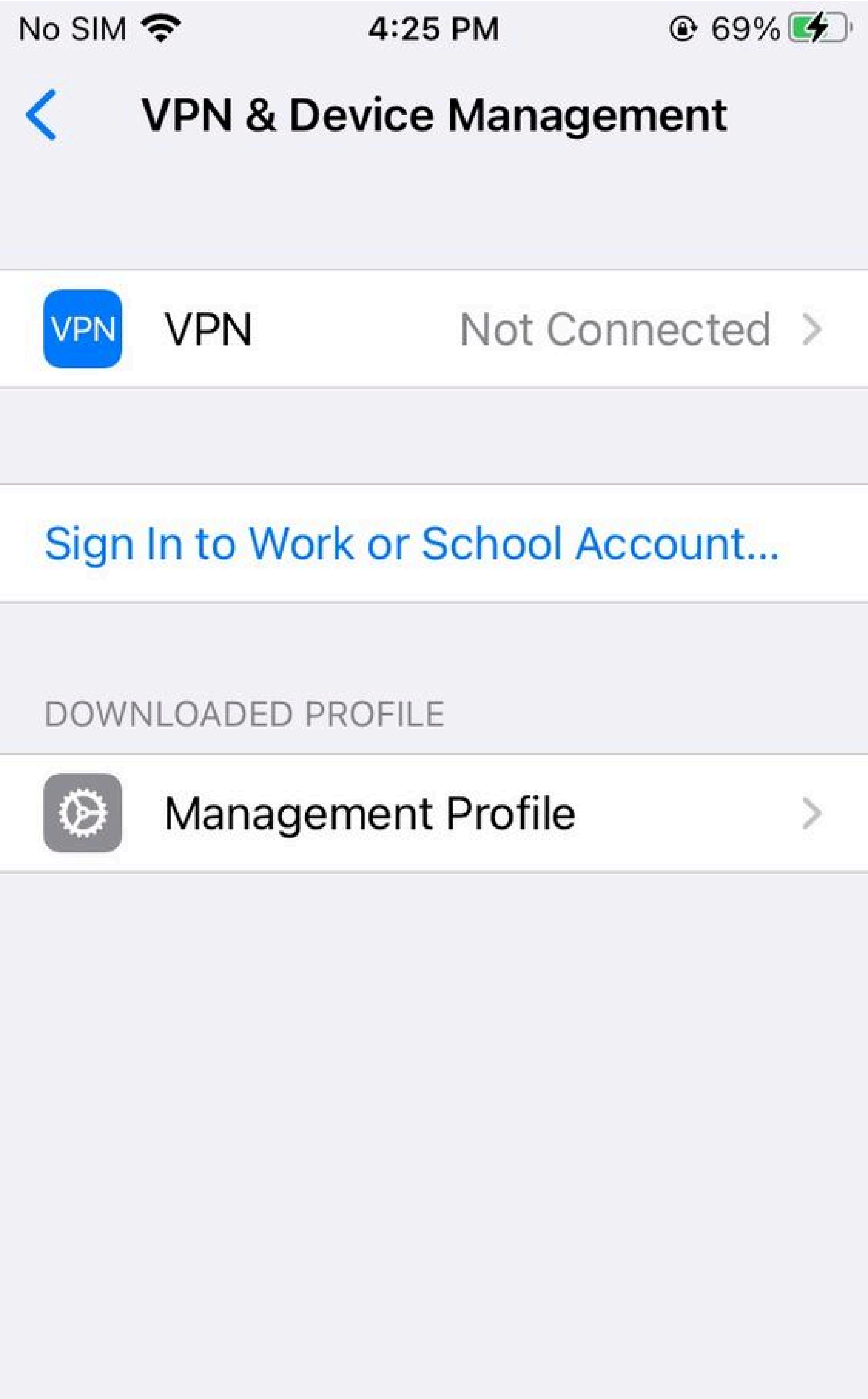
7. Download and launch "Apple Configurator" on your macOS from the App Store and connect your phone via Lightning Cable. Right click on your device within Apple Configurator select **Add** --> **Profiles** and then select the **profile.mobileconfig** file you just downloaded



11753024446100

Windows alternate: iPhone Configuration Utility

8. Once the sync has finished, on your iOS/iPadOS device go to **Settings app** and go to **General** --> **VPN & Device Management** --> **Management Profile**



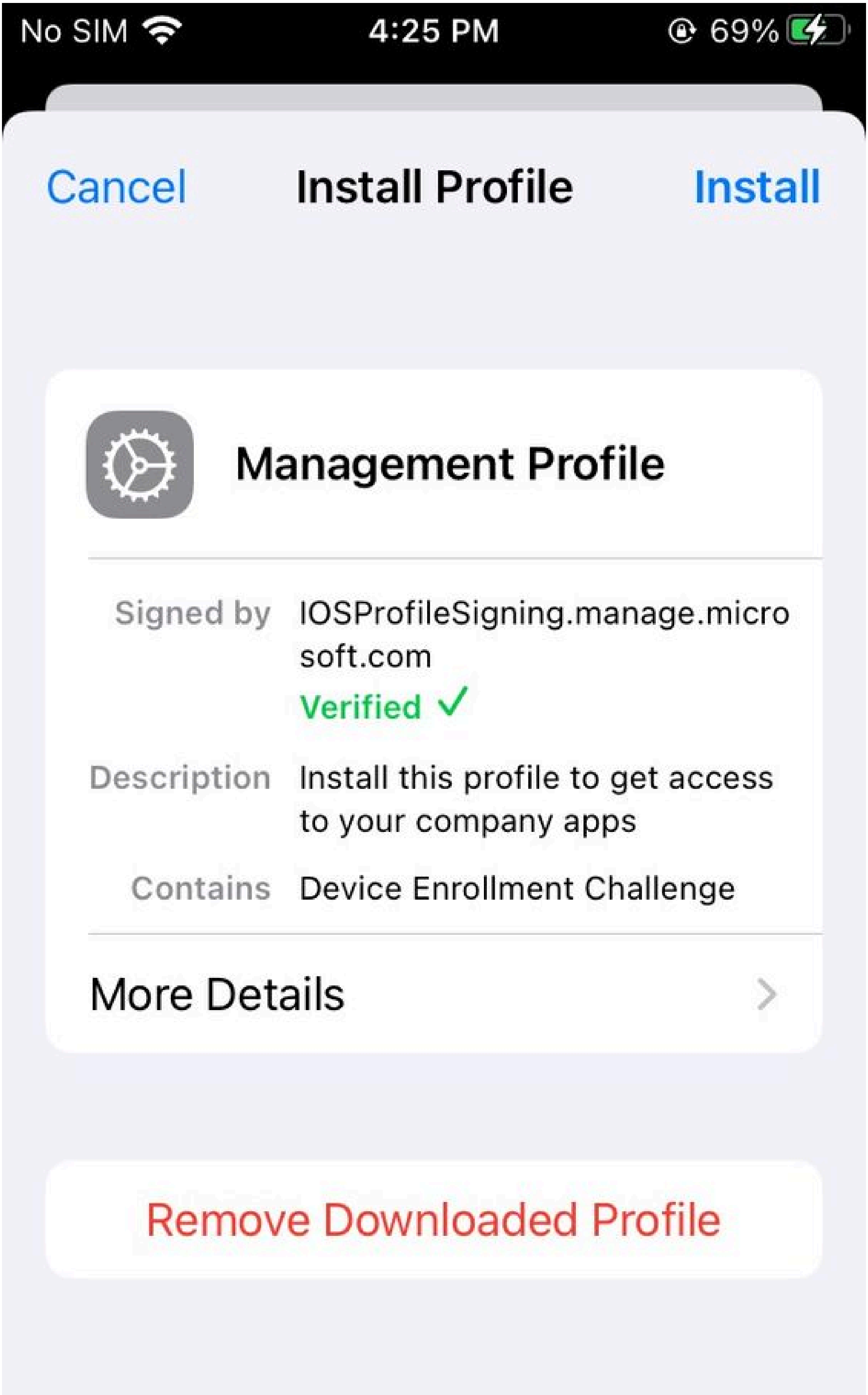
VPN & Device Management

VPN Not Connected

Sign In to Work or School Account...

DOWNLOADED PROFILE

Management Profile



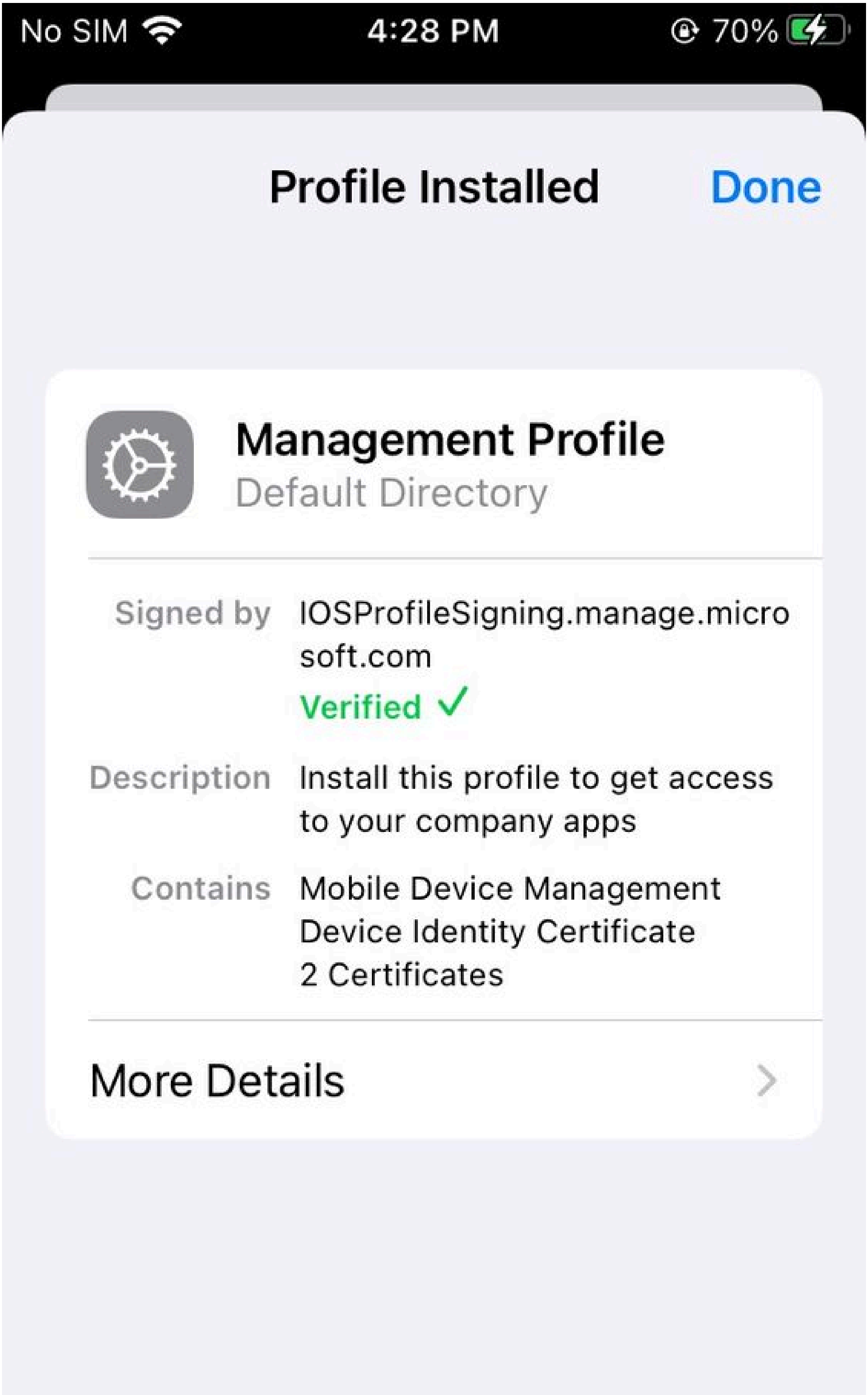
Management Profile

Signed by IOSProfileSigning.manage.microsoft.com

Verified ✓

Description Install this profile to get access to your company apps

Contains Device Enrollment Challenge



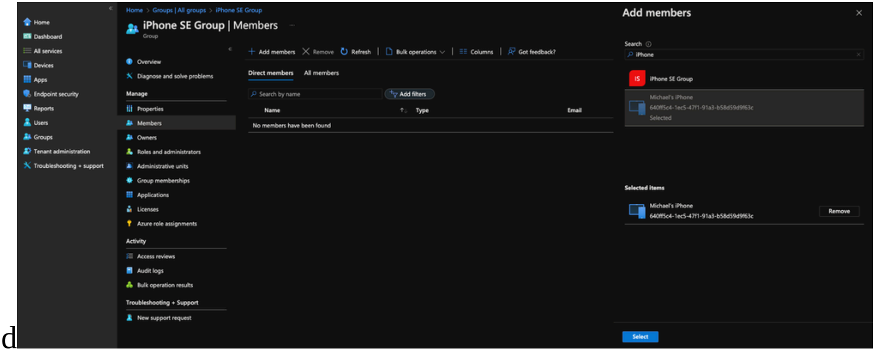
Profile Installed

Management Profile

Default Directory

Signed by	IOSProfileSigning.manage.microsoft.com Verified ✓
Description	Install this profile to get access to your company apps
Contains	Mobile Device Management Device Identity Certificate 2 Certificates

. Find your MDM-device you want to install the Cisco Security Connector app on, on the list and add it to the group you have just created



No members have been found

Search: iPhone

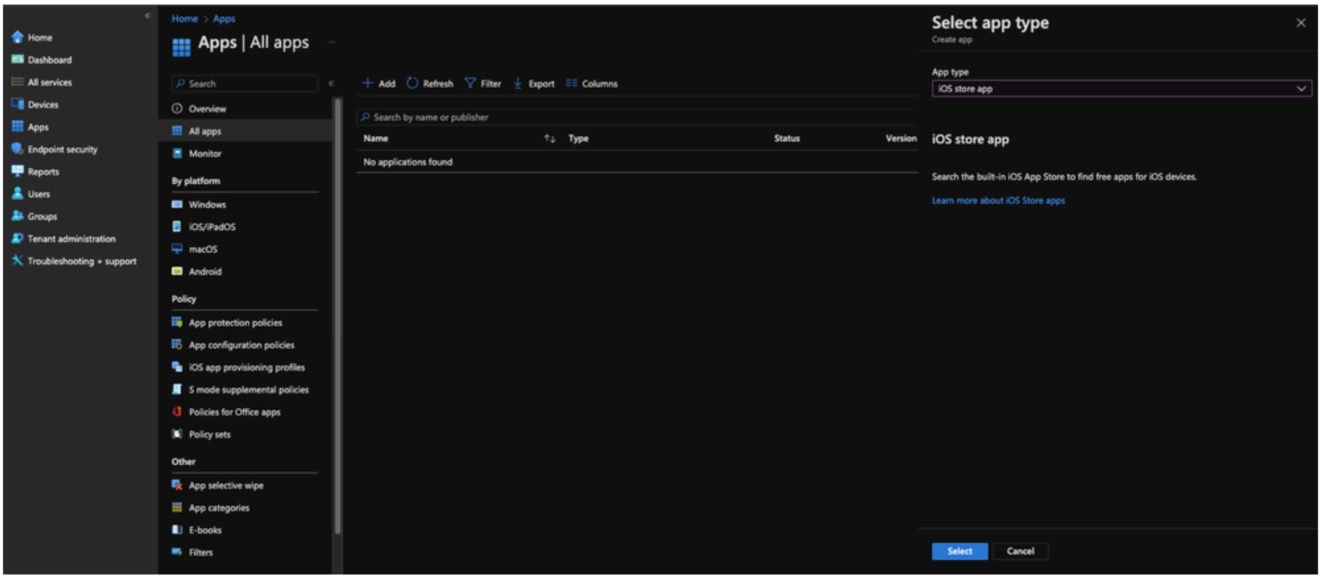
IS iPhone SE Group

Michael's iPhone
640ff5c4-1ec5-47f1-91a3-b58d59d9f63c
Selected

Selected items: Michael's iPhone 640ff5c4-1ec5-47f1-91a3-b58d59d9f63c

11753692550036

14. Go to **Apps** --> **All apps** --> **Add**. Then for App type, select "iOS store app" and confirm by clicking "Select"



No applications found

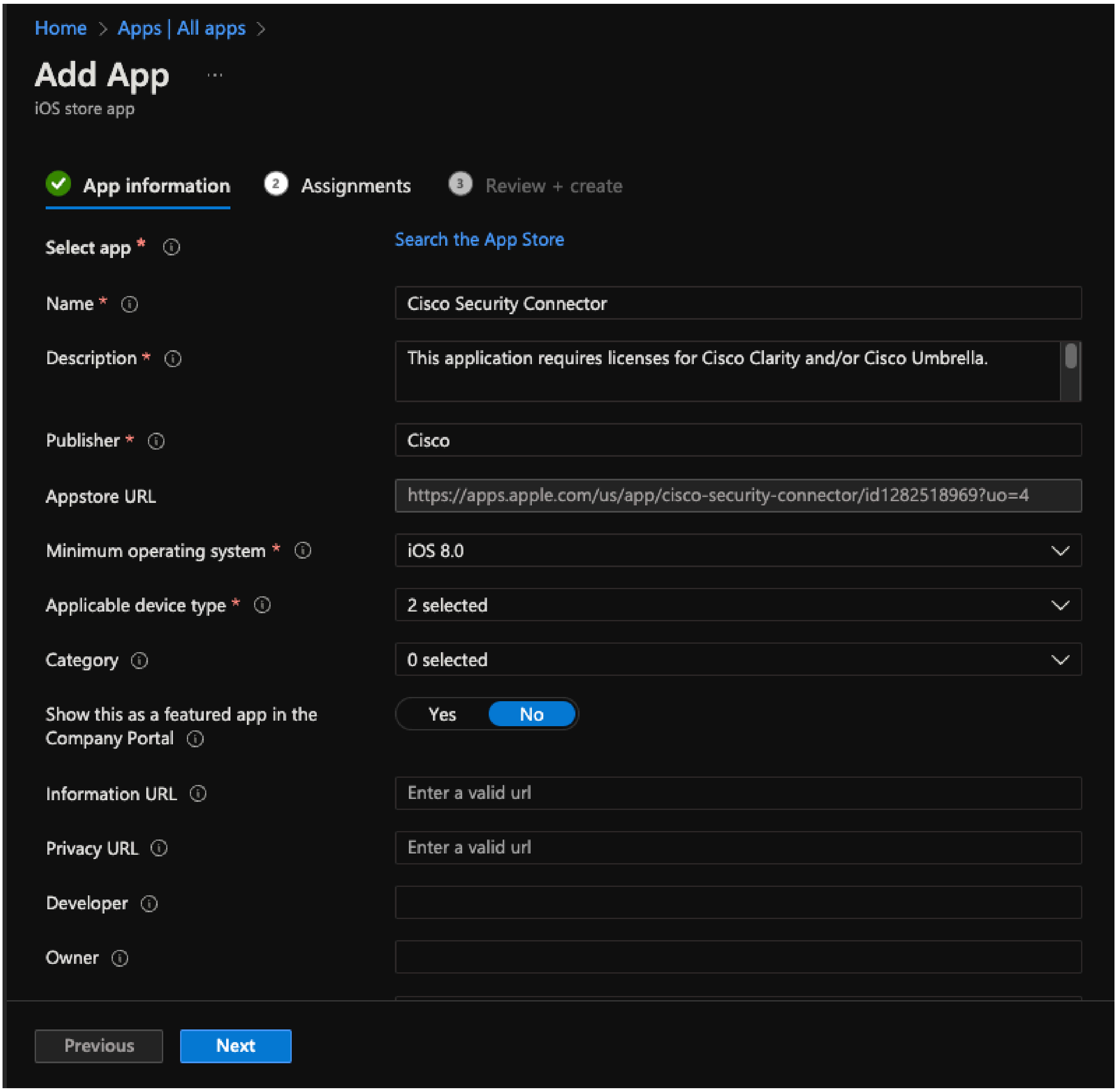
App type: iOS store app

iOS store app

Search the built-in iOS App Store to find free apps for iOS devices.

11753797372436

15. Select "Search for App Store" and enter "Cisco Security Connector" in the search bar and select the "Cisco Security Connector" app by clicking "Select"



Home > Apps | All apps >

Add App

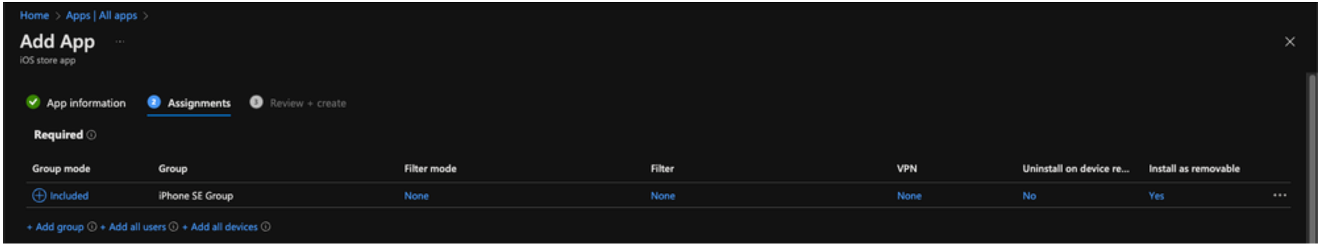
iOS store app

✓ App information 2 Assignments 3 Review + create

Select app *	Search the App Store
Name *	Cisco Security Connector
Description *	This application requires licenses for Cisco Clarity and/or Cisco Umbrella.
Publisher *	Cisco
Appstore URL	https://apps.apple.com/us/app/cisco-security-connector/id1282518969?uo=4
Minimum operating system *	iOS 8.0
Applicable device type *	2 selected
Category	0 selected
Show this as a featured app in the Company Portal	Yes [✓ No]
Information URL	Enter a valid url
Privacy URL	Enter a valid url
Developer	
Owner	

11753844054420

16. Under **Assignments**, add the group you have created in the earlier steps which contains your MDM-device then proceed with **Review and Create**



Home > Apps | All apps >

Add App

iOS store app

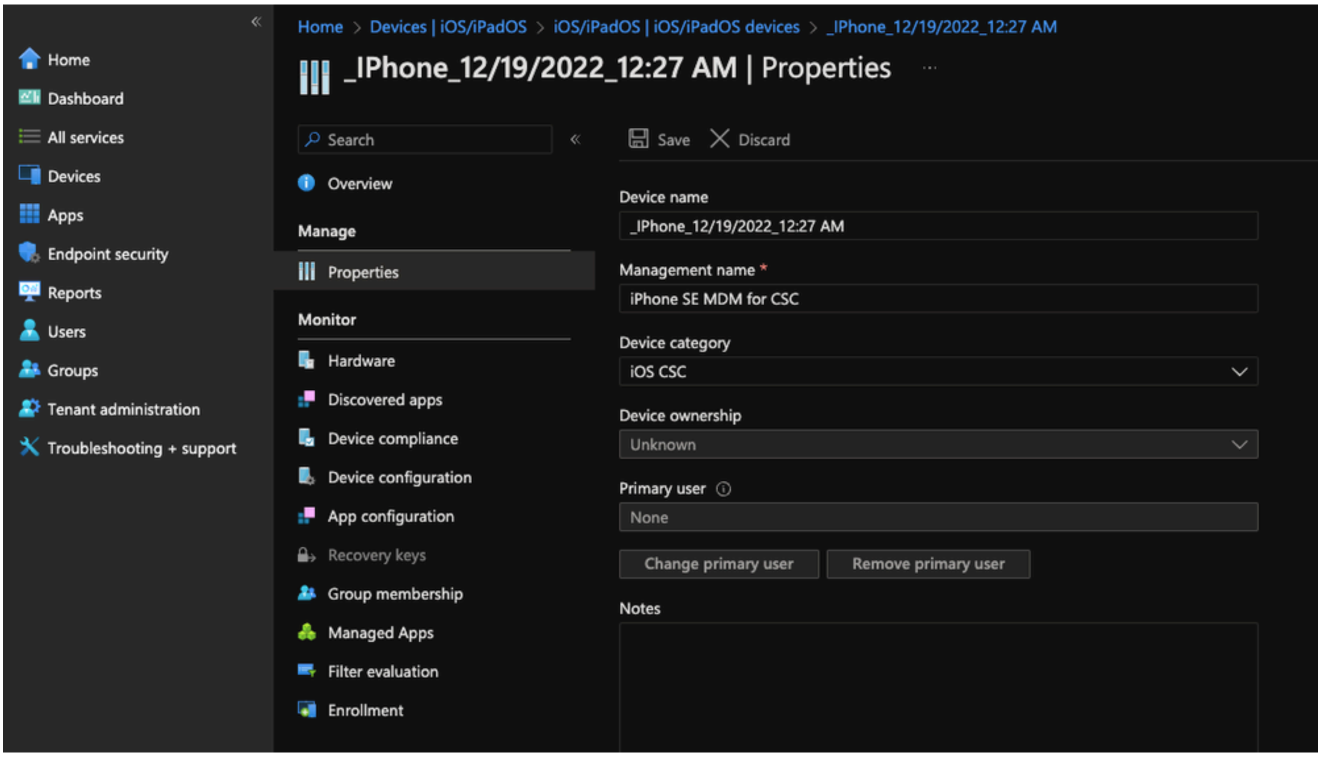
✓ App information 2 Assignments 3 Review + create

Required

Group mode	Group	Filter mode	Filter	VPN	Uninstall on device re...	Install as removable
Included	iPhone SE Group	None	None	None	No	Yes

11753839516692

17. **[Optional step]** Go to **Devices** --> **iOS/iPadOS** --> **iOS/iPadOS devices** --> **Properties** --> **Device Category,** create a profile and assign it to the device



_IPhone_12/19/2022_12:27 AM | Properties

Device name
_IPhone_12/19/2022_12:27 AM

Management name *
iPhone SE MDM for CSC

Device category
iOS CSC

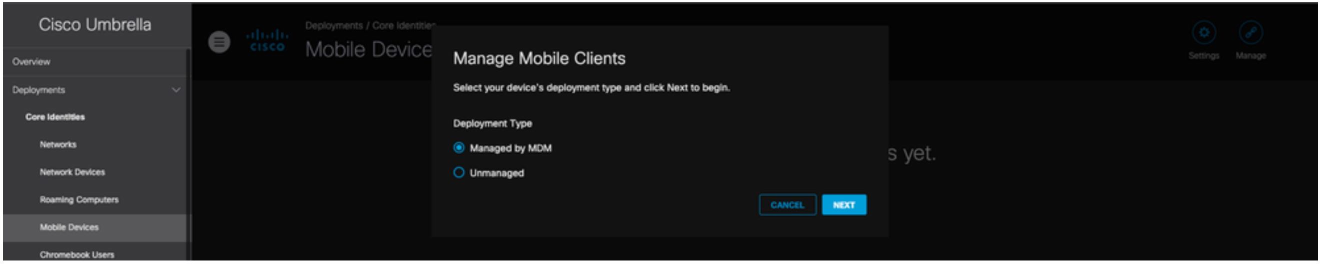
Device ownership
Unknown

Primary user
None

Notes

11753916236820

18. Log into your Cisco Umbrella dashboard, under **Deployments** --> **Core Identities** --> **Mobile Devices** --> top right: **Manage** --> **Managed by MDM**



Manage Mobile Clients

Select your device's deployment type and click Next to begin.

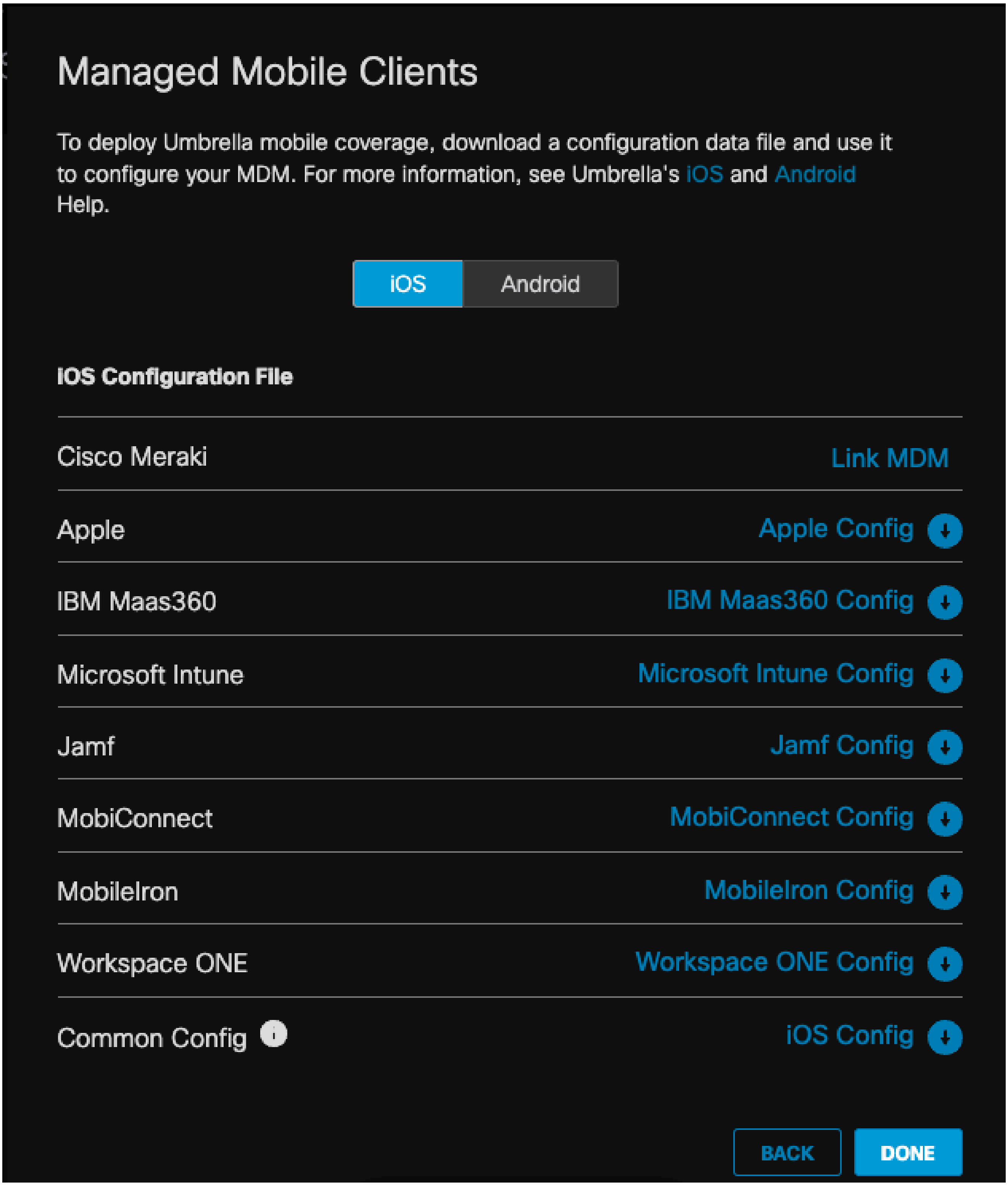
Deployment Type

● Managed by MDM

○ Unmanaged

11753923081492

19. Then go to **iOS** --> **Microsoft Intune Config download**. Enter your email address that you want emails to go to when users select "Report a problem" within the Cisco Security Connector app



Managed Mobile Clients

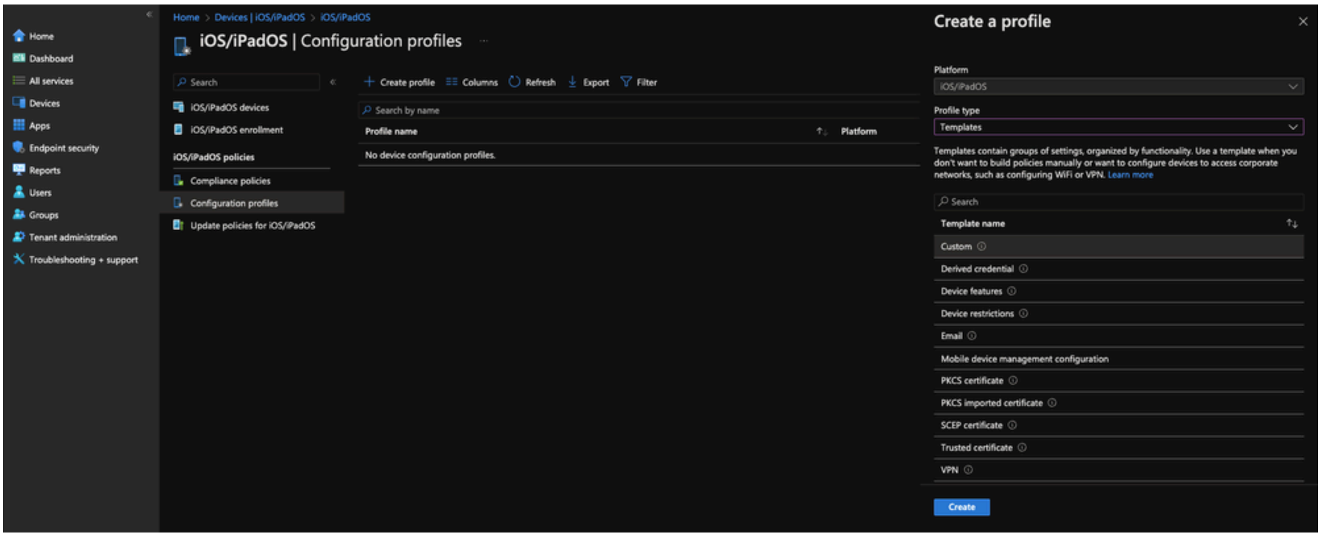
To deploy Umbrella mobile coverage, download a configuration data file and use it to configure your MDM. For more information, see Umbrella's iOS and Android Help.

iOS Configuration File

Cisco Meraki	Link MDM
Apple	Apple Config
IBM Maas360	IBM Maas360 Config
Microsoft Intune	Microsoft Intune Config
Jamf	Jamf Config
MobiConnect	MobiConnect Config
MobileIron	MobileIron Config
Workspace ONE	Workspace ONE Config
Common Config	iOS Config

11753924523540

20. Go back to your Intune portal, under **Devices** --> **iOS/iPadOS** --> **Configuration Profiles** --> **Create Profile** --> **Templates** --> **Custom**



Profile name	Platform
No device configuration profiles.	

Create a profile

Platform: iOS/iPadOS

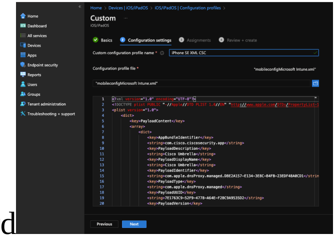
Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

Template name
Custom
Derived credential
Device features
Device restrictions
Email
Mobile device management configuration
PKCS certificate
PKCS imported certificate
SCEP certificate
Trusted certificate
VPN

11753988354964

21. Give it a meaningful name for your configuration profile. In **Step 2 - Configuration settings**, upload the XML file you have just downloaded from your Cisco Umbrella dashboard



Custom configuration profile name *: iPhone SE XML CSC

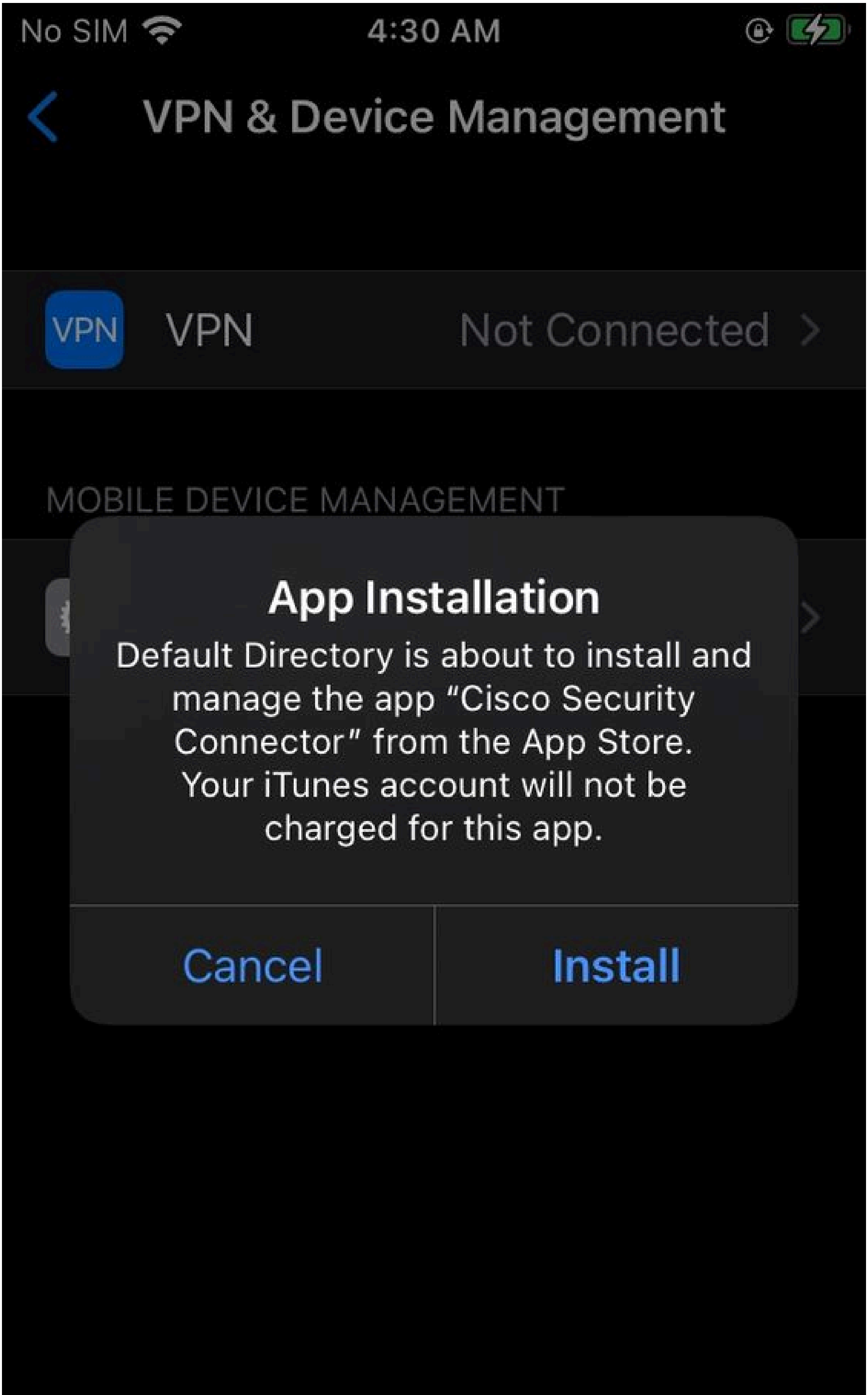
Configuration profile file *: "mobileconfigMicrosoft Intune.xml"

"mobileconfigMicrosoft Intune.xml"

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>AppBundleIdentifier</key>
                <string>com.cisco.ciscosecurity.app</string>
                <key>PayloadDescription</key>
                <string>Cisco Umbrella</string>
                <key>PayloadDisplayName</key>
                <string>Cisco Umbrella</string>
                <key>PayloadIdentifier</key>
                <string>com.apple.dnsProxy.managed.DBE2A157-E134-3E8C-B4FB-23EDF48A0CD1</strin
                <key>PayloadType</key>
                <string>com.apple.dnsProxy.managed</string>
                <key>PayloadUUID</key>
                <string>7E1763C9-52F9-4778-A64E-F2BC9A9535D2</string>
                <key>PayloadVersion</key>
```

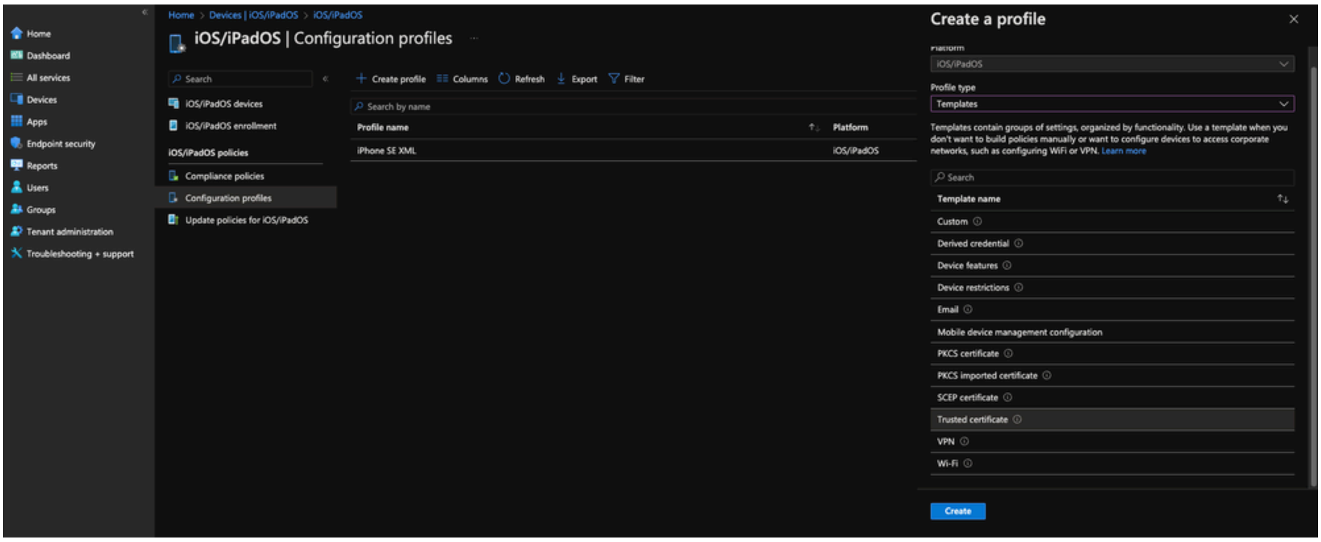
11754000962196

22. Under **Assignments**, assign the group you have created earlier that contains your MDM-device and select "Review and Create"
23. Go back to **iOS/iPadOS devices** and select your MDM-device and hit sync at the top and you get a pop-up on your MDM iOS/iPadOS device to install the Cisco Security Connector app



App Installation

Default Directory is about to install and manage the app "Cisco Security Connector" from the App Store. Your iTunes account will not be charged for this app.



iOS/iPadOS | Configuration profiles

Profile name	Platform
iPhone SE XML	iOS/iPadOS

Create a profile

Platform: iOS/iPadOS

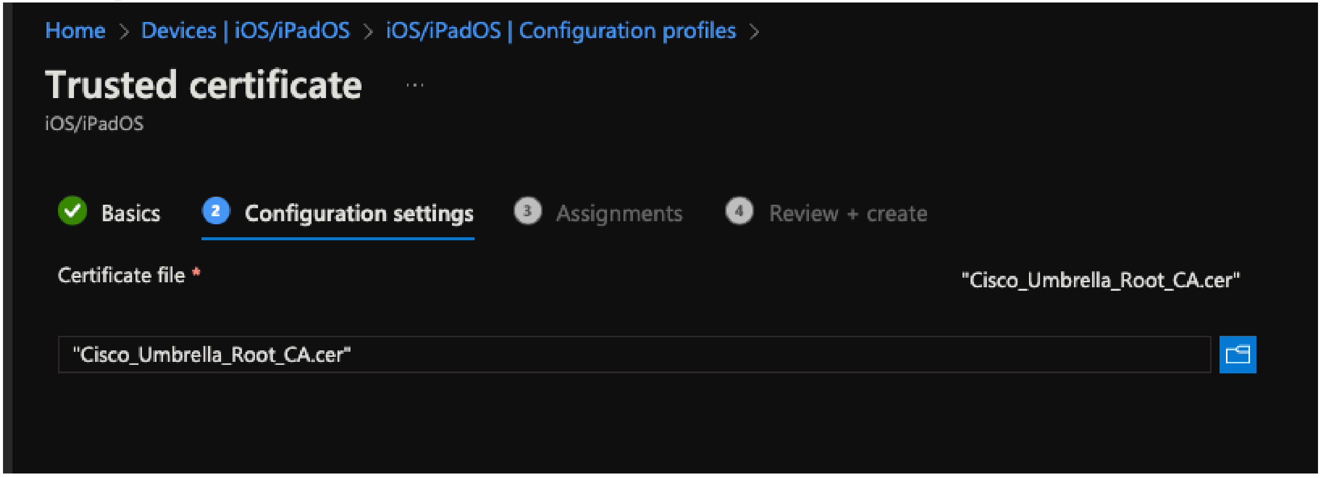
Profile type: Templates

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

Template name
Custom
Derived credential
Device features
Device restrictions
Email
Mobile device management configuration
PKCS certificate
PKCS imported certificate
SCEP certificate
Trusted certificate
VPN
Wi-Fi

11754159037460

29. In **Step 2 - Configuration settings**, upload the Umbrella Root Certificate you have just downloaded from Step 27


Home > Devices | iOS/iPadOS > iOS/iPadOS | Configuration profiles >
Basics
2 Configuration settings
3 Assignments
4 Review + create

Trusted certificate

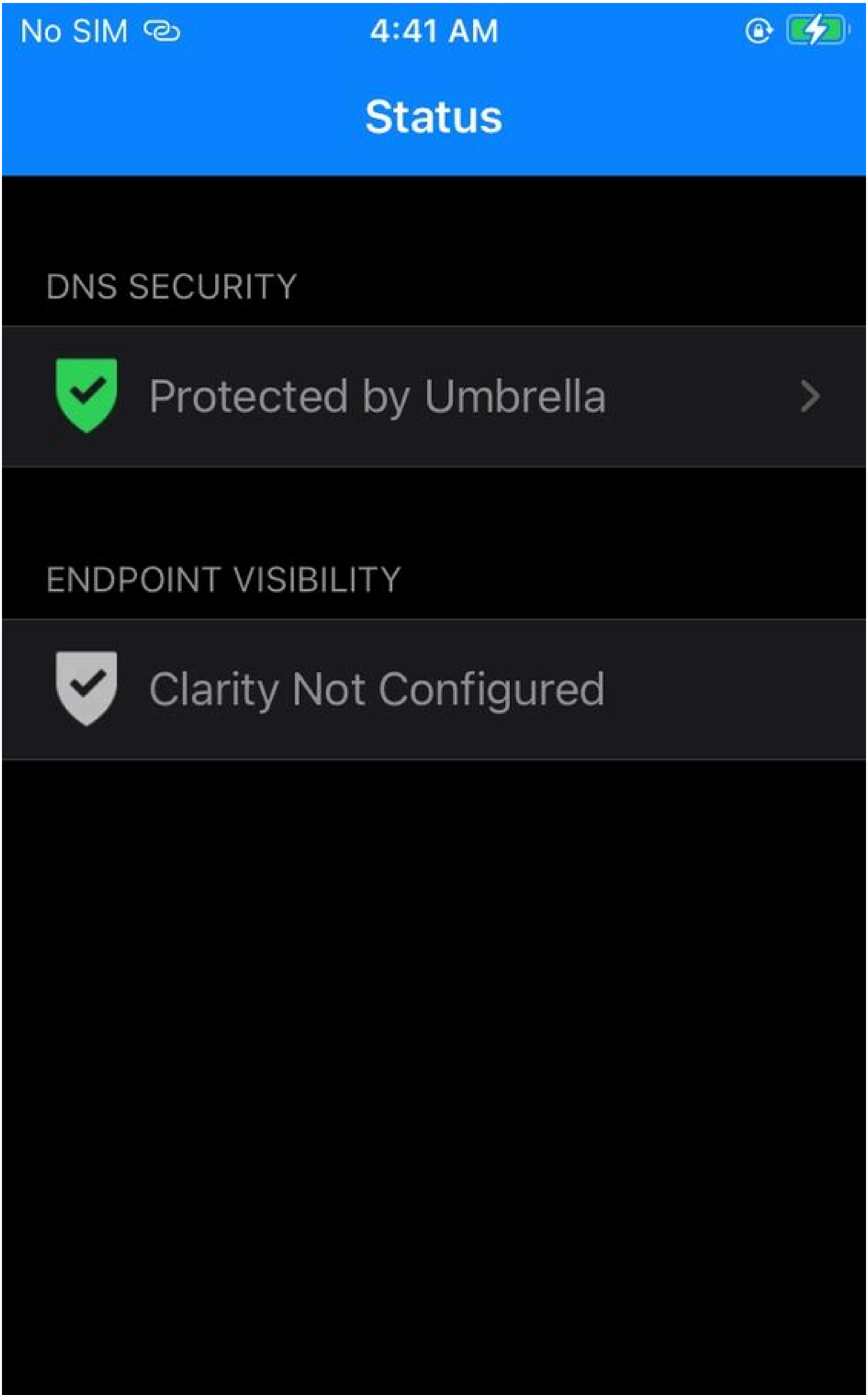
iOS/iPadOS

Certificate file * "Cisco_Umbrella_Root_CA.cer"

"Cisco_Umbrella_Root_CA.cer"

11754204605460

30. For **Step 3 - Assignments**, select the group that contains your MDM iOS/iPadOS device and click "Next" and "Create"
31. Go back to iOS/iPadOS devices and select your MDM-device and hit sync at the top once again (like step 24)
32. Close and relaunch the Cisco Security Connector app again. You now see the status as "Protected by Umbrella"



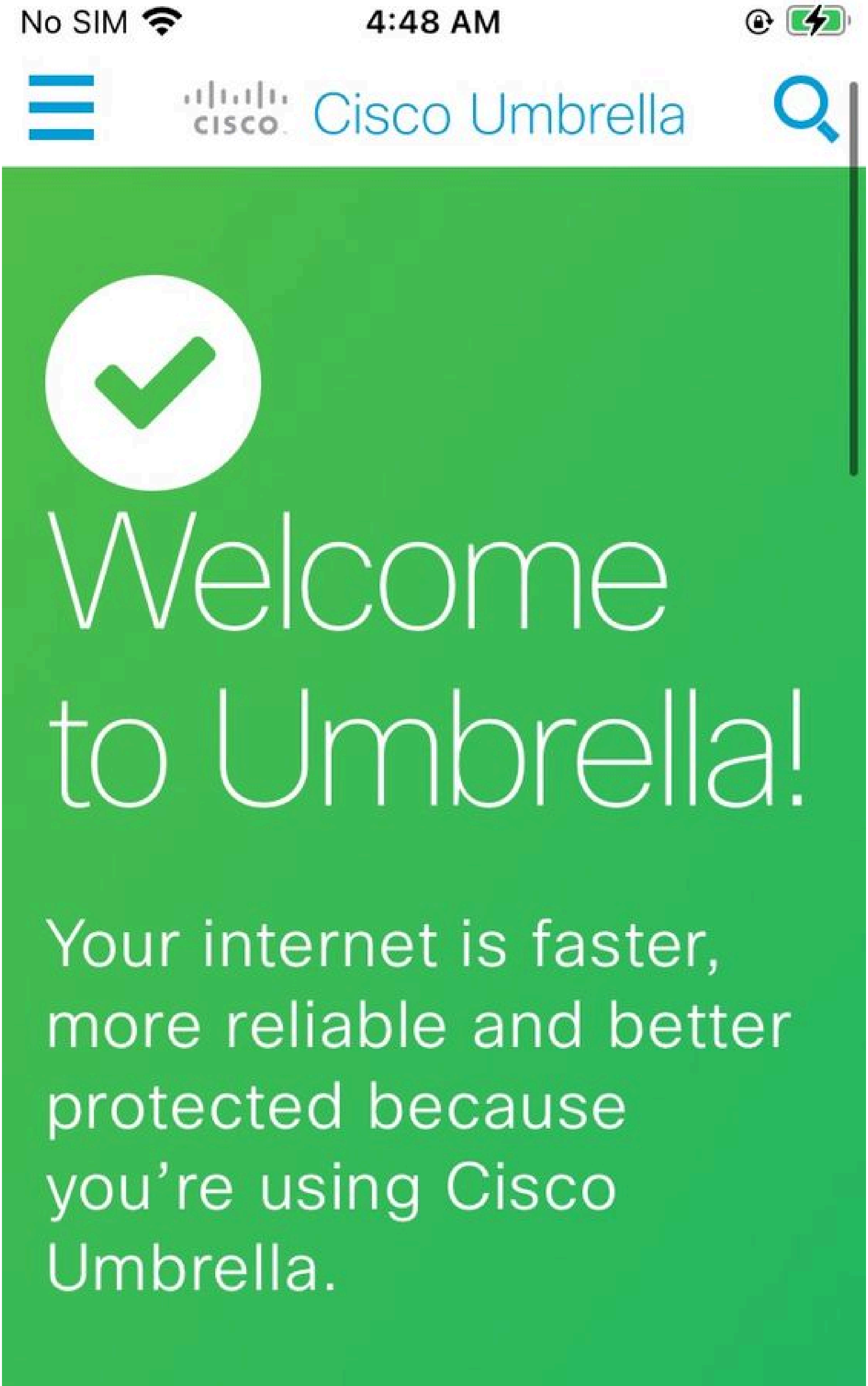
Status

DNS SECURITY

✓ Protected by Umbrella

ENDPOINT VISIBILITY

✓ Clarity Not Configured



Welcome to Umbrella!

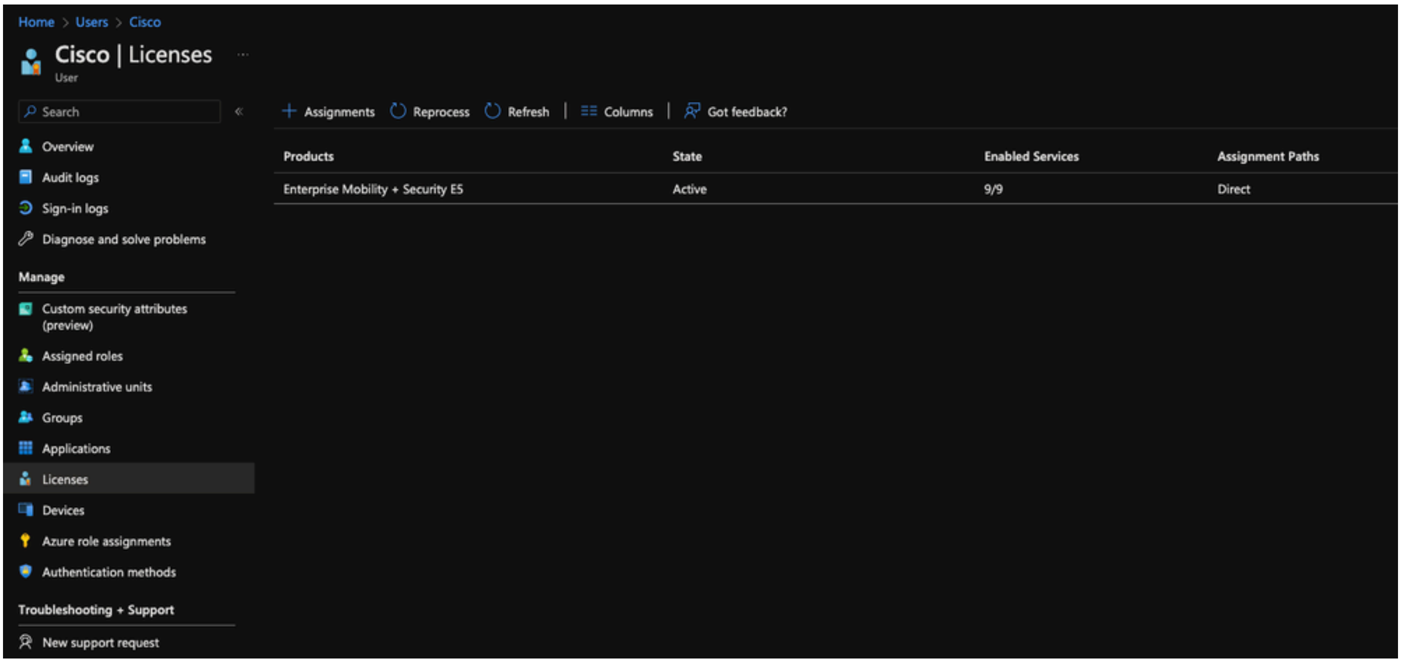
Your internet is faster, more reliable and better protected because you’re using Cisco Umbrella.

- You cannot have any "Restricted Apps" setting restricting the Umbrella app, and/or any "Show or Hide" setting to hide the Umbrella app applied in your device configuration profile.(Under your Intune admin center > Devices > iOS/iPadOS > Configuration)

Troubleshooting

- How to Collect Cisco Security Connector Diagnostics Logs
- CSC Log "Report A Problem" Function "No Admin Email" Error
- CSC: "Unprotected" status on mobile networks

If you are getting an **Error: "User Name not recognized. This user is not authorized to use Microsoft Intune"**, go to the Azure Portal, under "Users" and select the username or account you are using to configure Intune, go to "Licenses" and make sure you have an active Intune License assigned to the user



Products	State	Enabled Services	Assignment Paths
Enterprise Mobility + Security E5	Active	9/9	Direct

117545557401748

Logs

By default, the logs password is **bypass_email_filters** . This can also be located in the UmbrellaProblemReport.txt