Bereitstellung von Security Connector mit Intune

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Security Connector mithilfe von Intune bereitstellen.

Überblick

Dies ist eine schrittweise Anleitung, wie Sie Ihr iOS/iPadOS-Gerät über Intune MDM-verwalten und das Profil über den Apple Configurator übertragen können.

Weitere Informationen finden Sie hier in der Intune Registration-Dokumentation und im PDF-Leitfaden.

Anmerkung: Diese Methode zeigt Ihnen, wie Sie Ihre Geräte über Intune und Apple Configurator mit MDM konfigurieren.

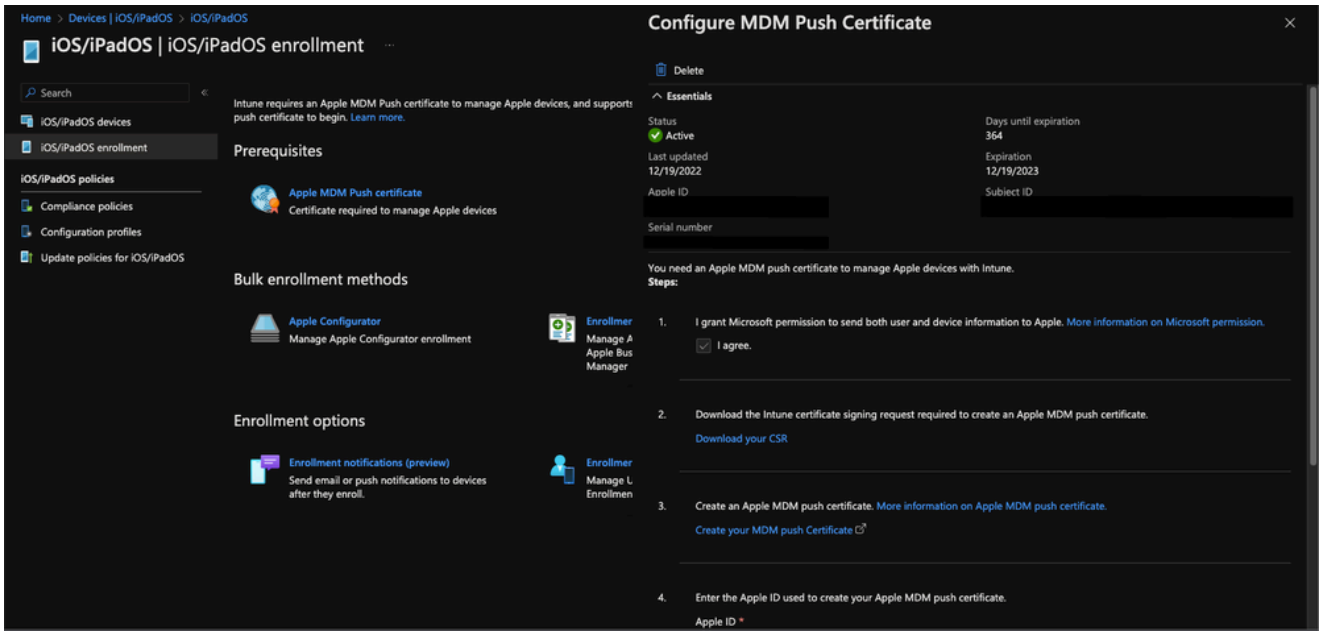
Wichtige Hinweise:

Wenn Sie Ihre betreuten Geräte über die Company Portal App MDM betreiben, können Sie mit Schritt 14 beginnen.

Dieser Artikel wird in der vorliegenden Form vom 12.04.2023 zur Verfügung gestellt. Umbrella Support garantiert nicht, dass diese Anleitung nach diesem Datum gültig bleibt und kann aufgrund von Updates von Microsoft Intune und Apple iOS geändert werden.

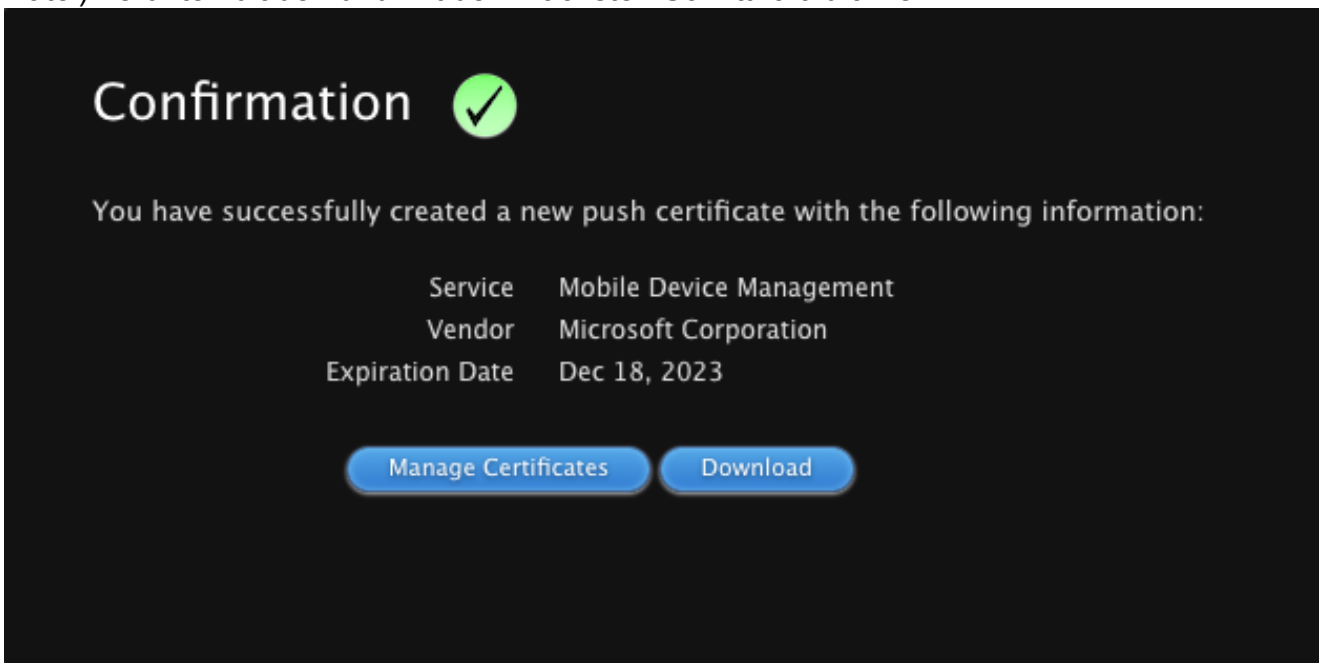
Vorgehensweise

1. Melden Sie sich beim Azure-Portal an, und suchen Sie nach "Intune". Oder gehen Sie zu https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/, und melden Sie sich an.
2. Wenn Sie sich auf der Intune-Homepage befinden, gehen Sie zu Devices —> iOS/iPadOS —> iOS/iPadOS-Anmeldung —> Apple MDM Push-Zertifikat, und klicken Sie auf "Download your CSR".



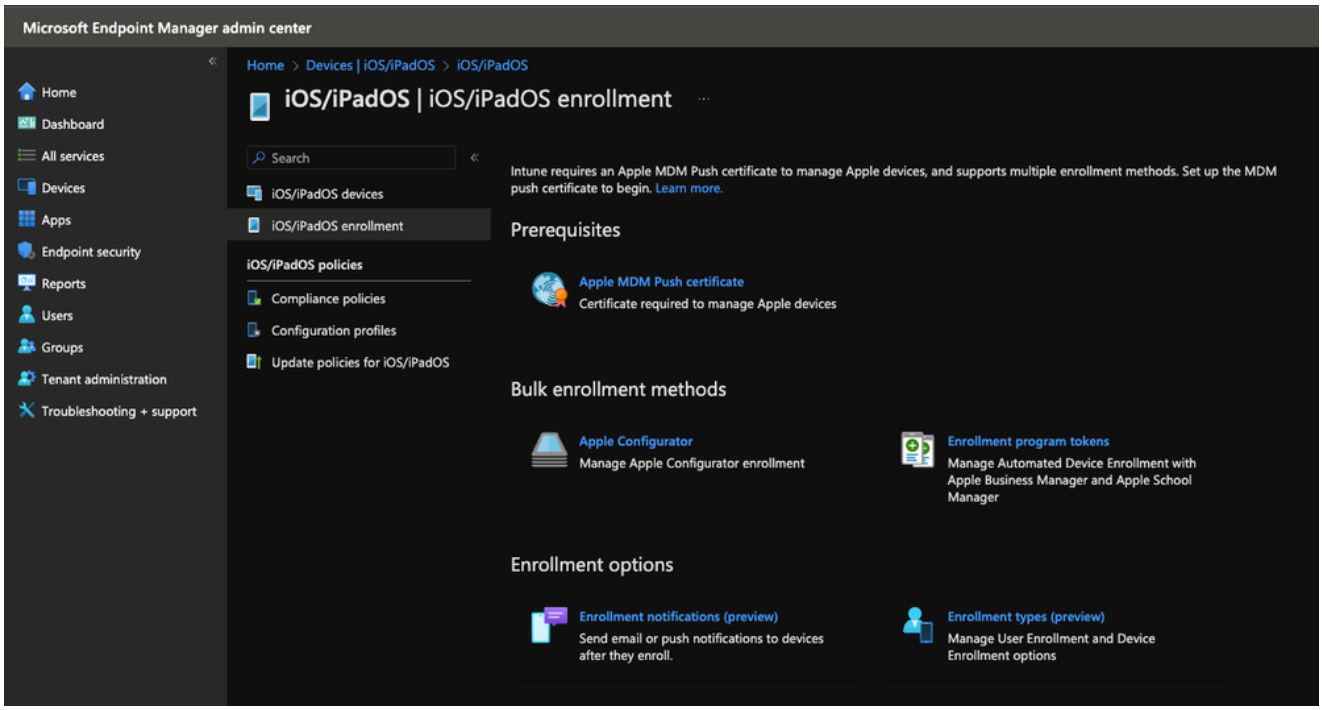
11752925317012

3. Klicken Sie dann auf "Create your MDM push Certificate" (MDM-Push-Zertifikat erstellen), das Sie zu https://identity.apple.com/pushcert/ umleitet.
4. Gehen Sie im Apple Push Certificates Portal zu "Create a Certificate" und laden Sie die gerade heruntergeladene Datei IntuneCSR.csr hoch. Nachdem die CSR-Datei erfolgreich hochgeladen wurde, klicken Sie auf "Herunterladen", um die Privacy Enhanced Mail (.pem-Datei) herunterzuladen und mit dem nächsten Schritt fortzufahren.

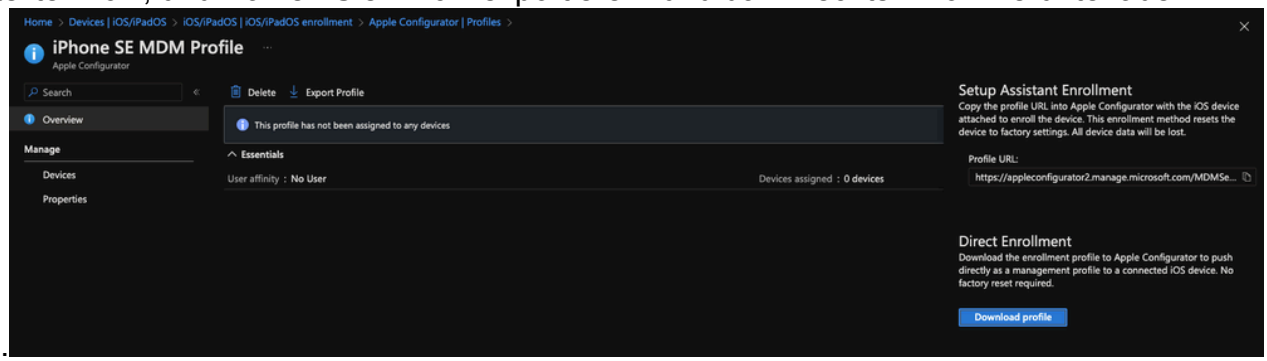


11752968667924

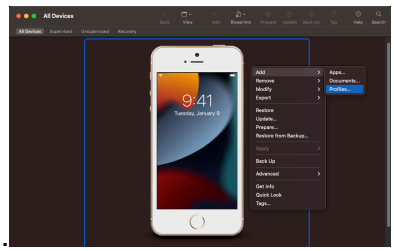
5. Geben Sie die E-Mail-Adresse Ihres Apple ID-Kontos ein, mit dem Sie sich beim Apple Push-Zertifizierungsportal angemeldet haben, laden Sie die .pem-Datei unter "Apple MDM Push Certificate" hoch, und drücken Sie "Upload". Wenn das Hochladen erfolgreich ist, sehen Sie die anderen Optionen für die "Masseneinschreibung Methoden" entsperren.



11752971407380

6. Gehen Sie zu Apple Configurator —> Profiles —> Create and create a new profile. Geben Sie ihm einen aussagekräftigen Namen, und wählen Sie für die Benutzeraffinität "Ohne Benutzeraffinität anmelden" aus. Klicken Sie nach dem Erstellen des Profils auf das neu erstellte Profil, und wählen Sie "Profil exportieren" und dann rechts "Profil herunterladen" aus. 

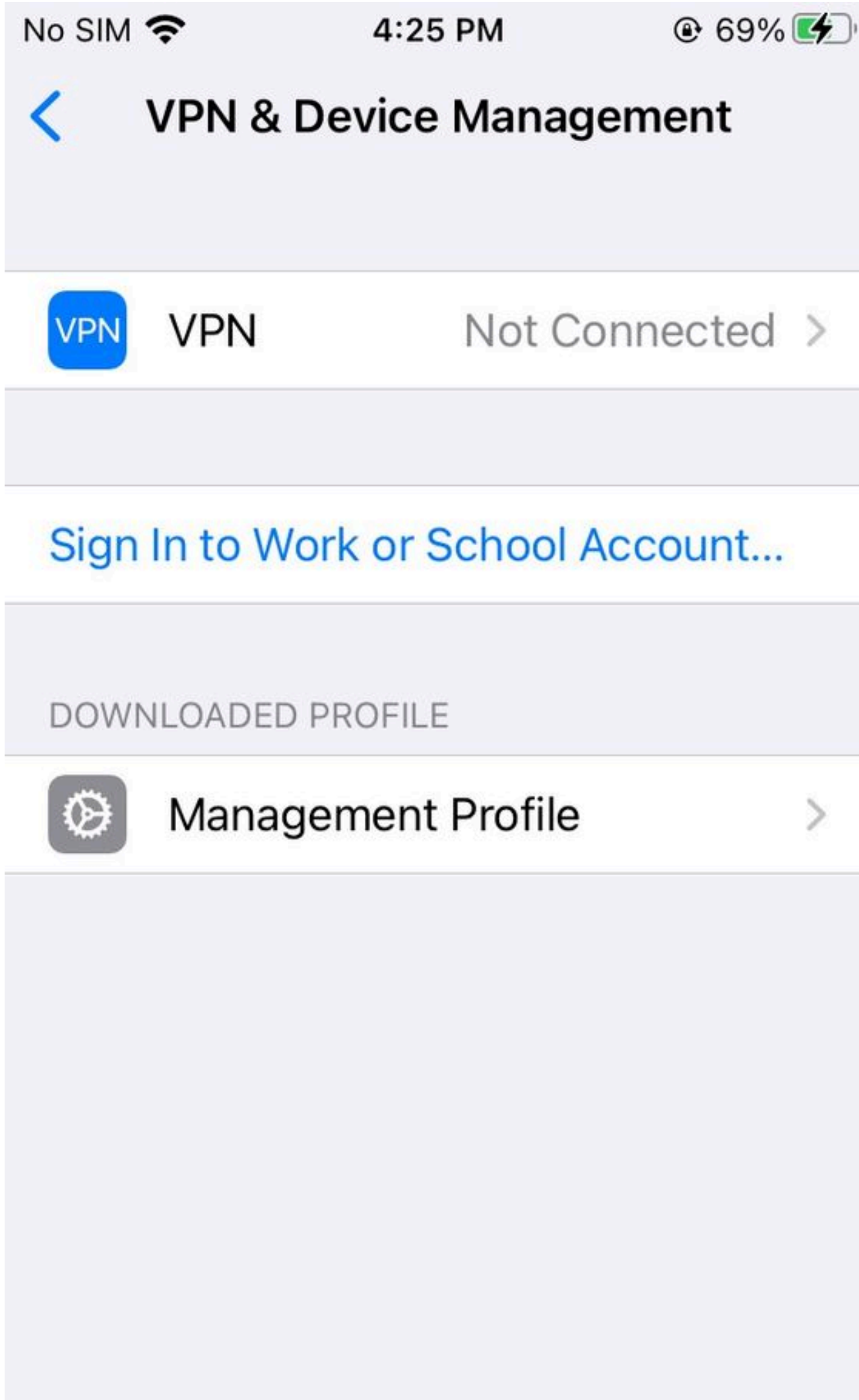
11753020728596

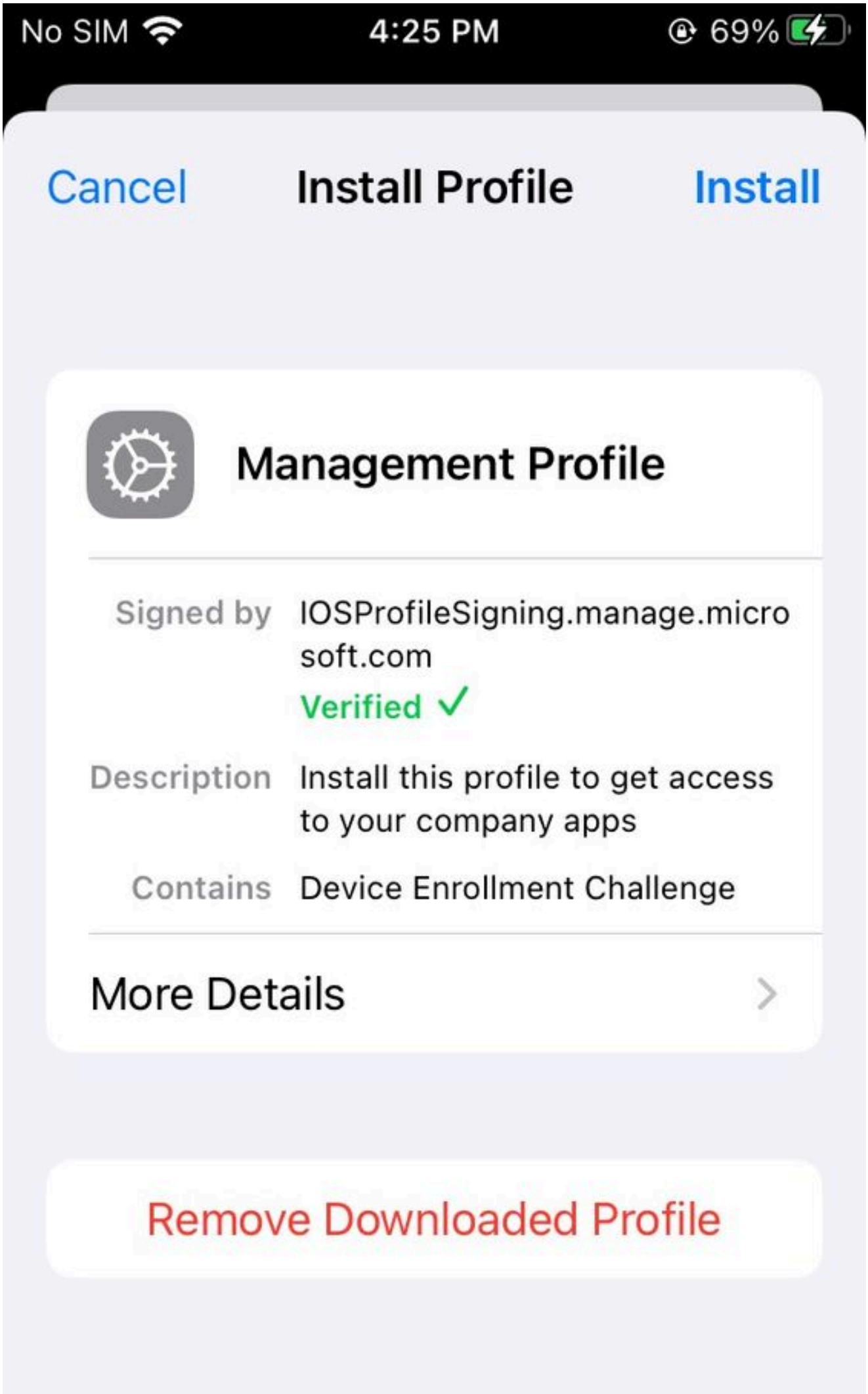
7. Laden Sie "Apple Configurator" aus dem App Store auf Ihr macOS herunter und starten Sie es. Schließen Sie Ihr Telefon über Lightning Cable an. Klicken Sie mit der rechten Maustaste auf Ihr Gerät in Apple Configurator und wählen Sie Hinzufügen —> Profile und dann die profile.mobileconfig-Datei, die Sie gerade heruntergeladen haben. 

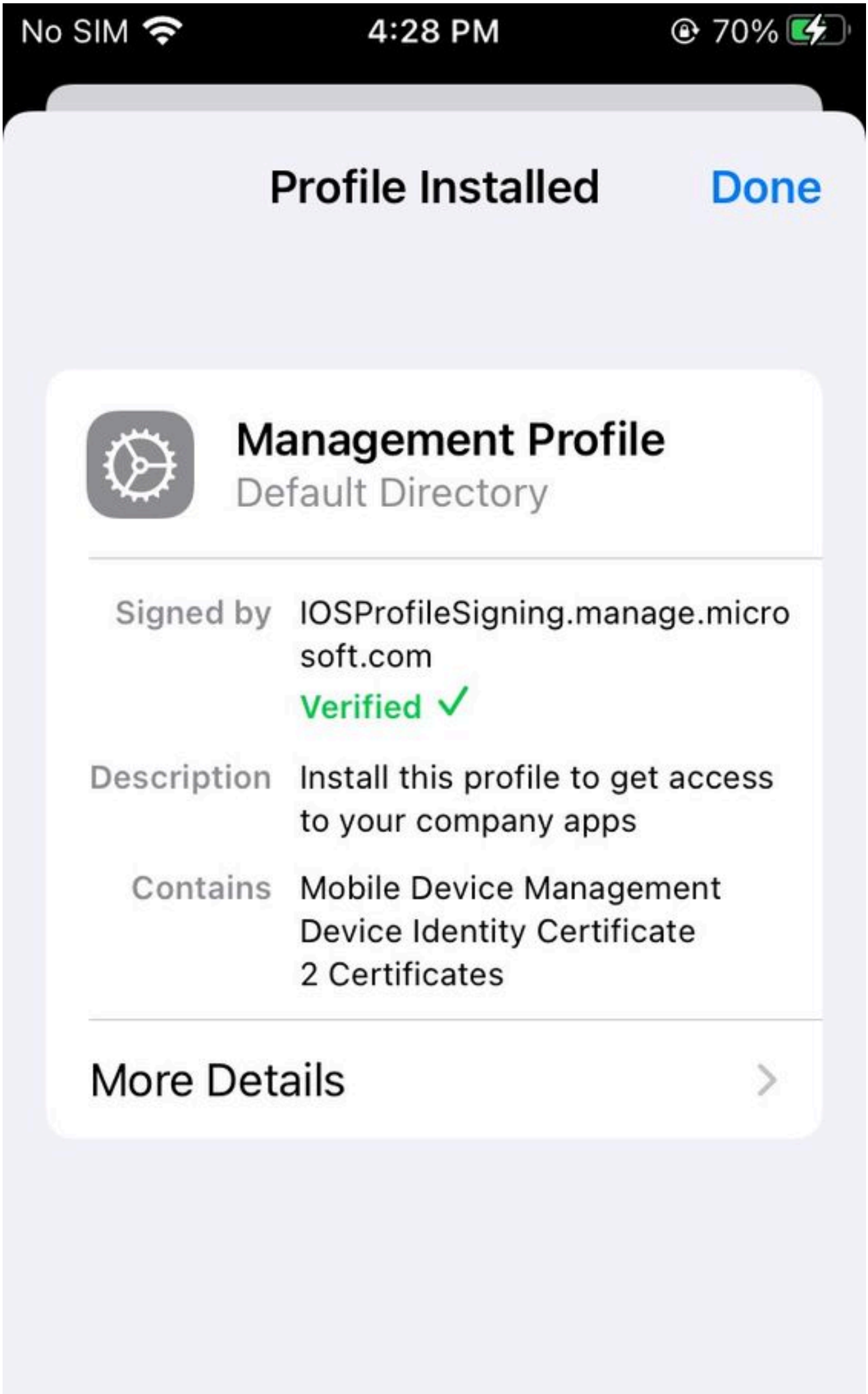
11753024446100

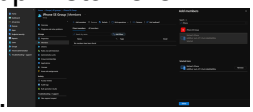
Windows-Alternative: iPhone-Konfigurationsprogramm

8. Sobald die Synchronisierung abgeschlossen ist, wechseln Sie auf Ihrem iOS/iPadOS-Gerät zur Einstellungs-App und zu Allgemein —> VPN & Gerätemanagement —> Managementprofil


No SIM
4:25 PM
69%
VPN & Device Management
VPN
VPN
Not Connected
Sign In to Work or School Account...
DOWNLOADED PROFILE
Management Profile

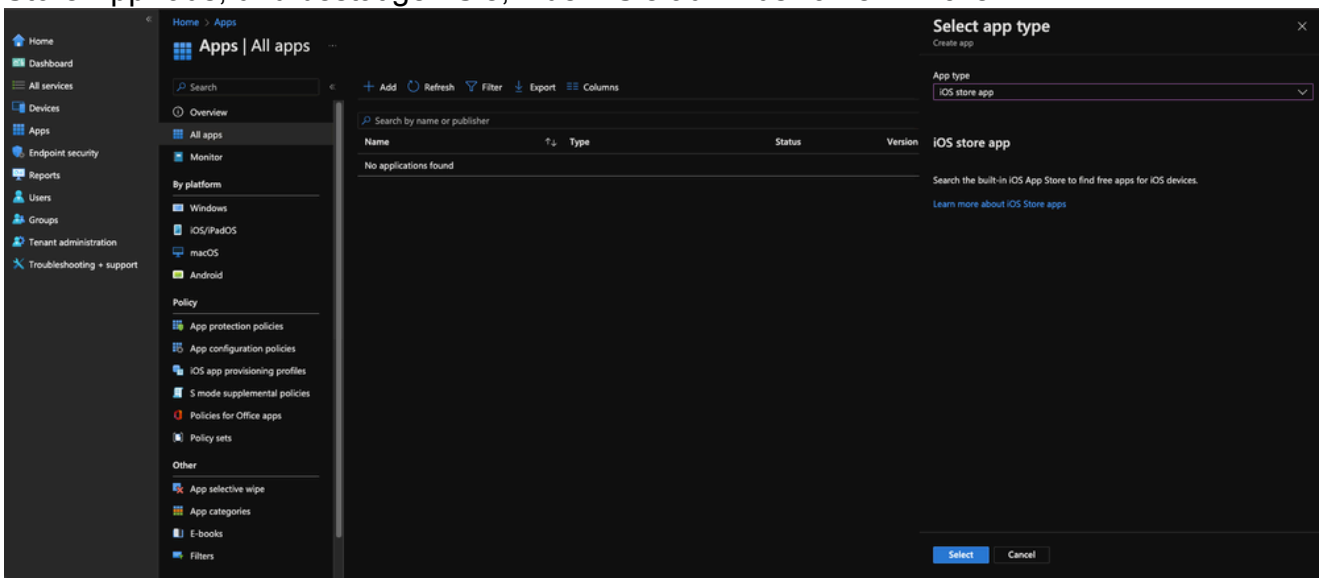

No SIM
4:25 PM
69%
Cancel
Install Profile
Install
Management Profile
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Device Enrollment Challenge
More Details
Remove Downloaded Profile


No SIM
4:28 PM
70%
Profile Installed
Done
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
More Details

. Suchen Sie das MDM-Gerät, auf dem Sie die Cisco Security Connector-App installieren möchten, in der Liste, und fügen Sie es der soeben erstellten Gruppe hinzu. 

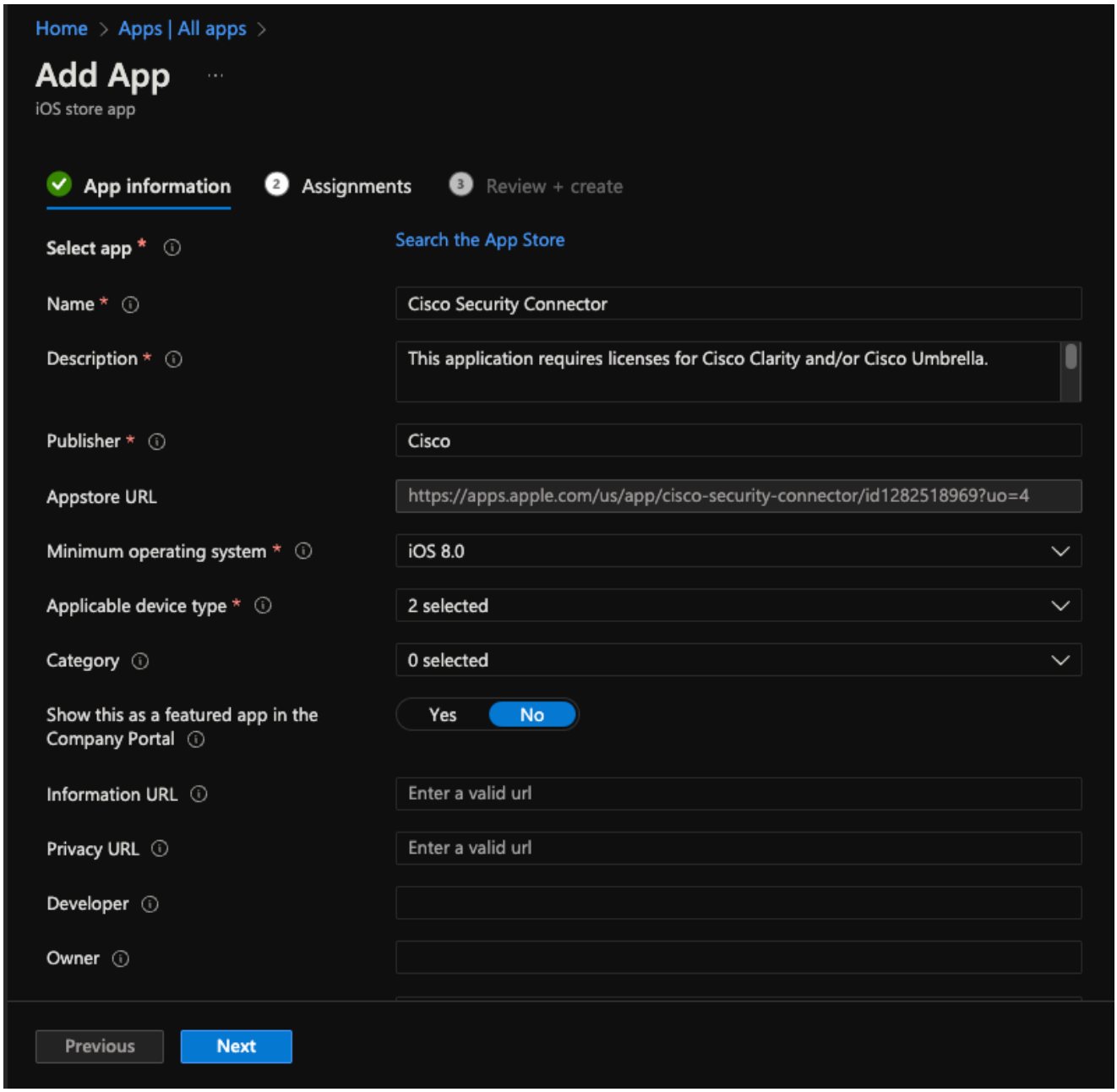
11753692550036

14. Gehen Sie zu Apps —> Alle Apps —> Hinzufügen. Wählen Sie dann für den App-Typ "iOS Store App" aus, und bestätigen Sie, indem Sie auf "Auswählen" klicken.



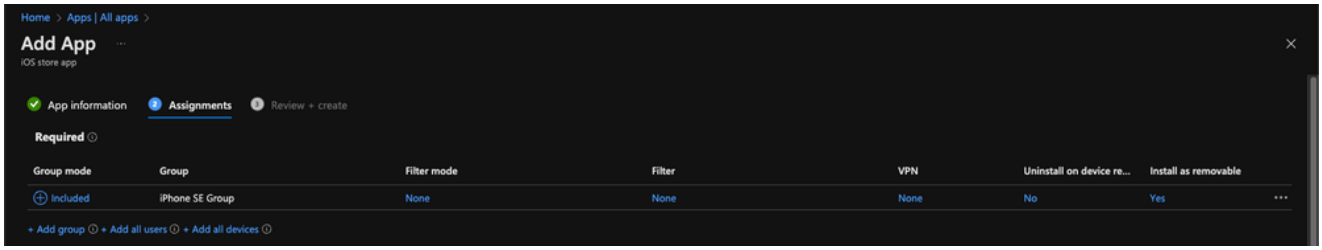
11753797372436

15. Wählen Sie "Nach App Store suchen", geben Sie "Cisco Security Connector" in die Suchleiste ein, und wählen Sie die App "Cisco Security Connector" aus, indem Sie auf "Auswählen" klicken.



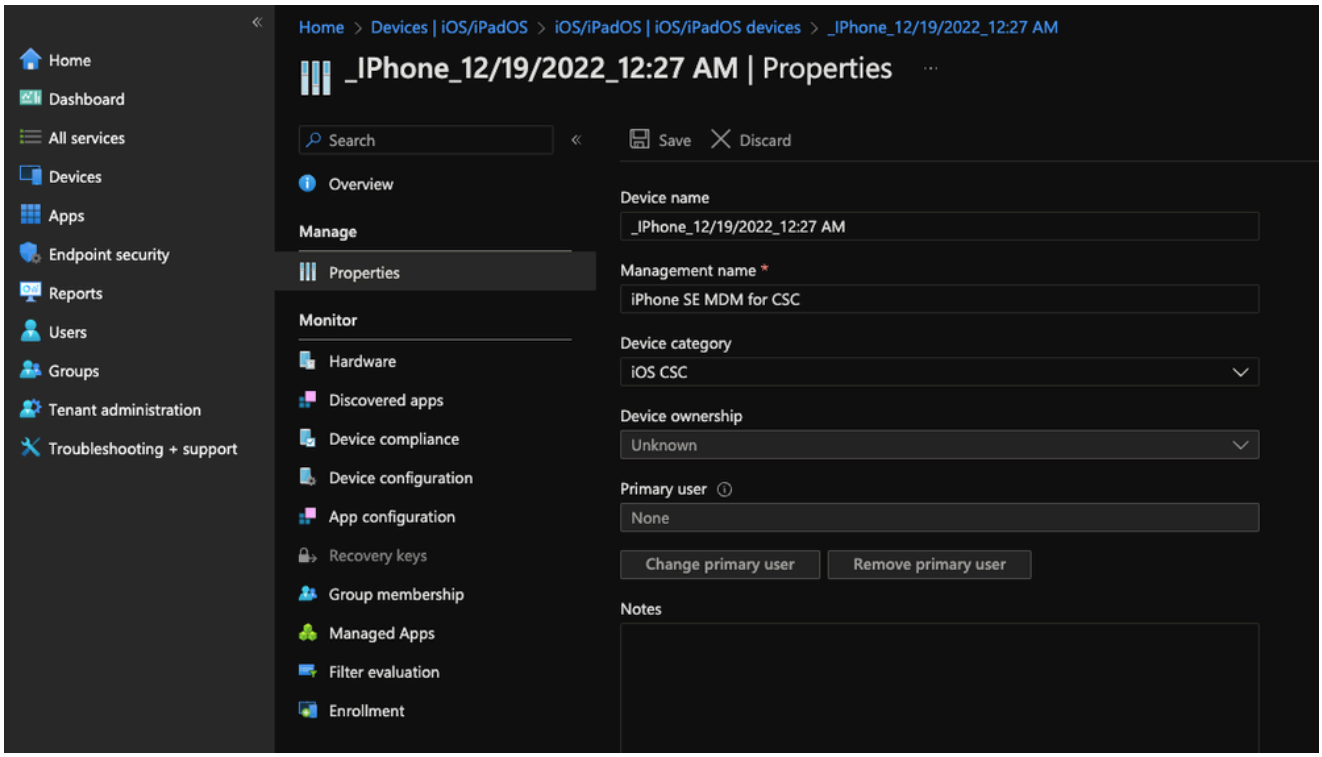
11753844054420

16. Fügen Sie unter Assignments (Zuweisungen) die Gruppe hinzu, die Sie in den vorherigen Schritten erstellt haben und die Ihr MDM-Gerät enthält, und fahren Sie dann mit Prüfen und erstellen



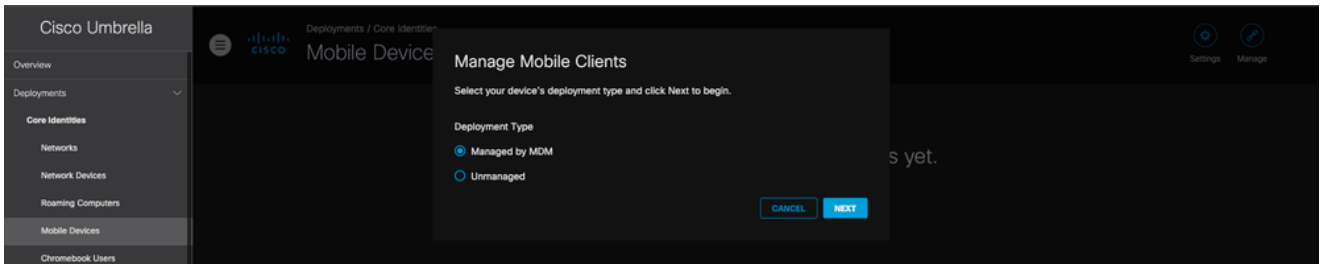
11753839516692

17. [Optionaler Schritt] Gehen Sie zu Geräte —> iOS/iPadOS —> iOS/iPadOS-Geräte —> Eigenschaften —> Gerätekategorie, erstellen Sie ein Profil, und weisen Sie es dem Gerät zu.



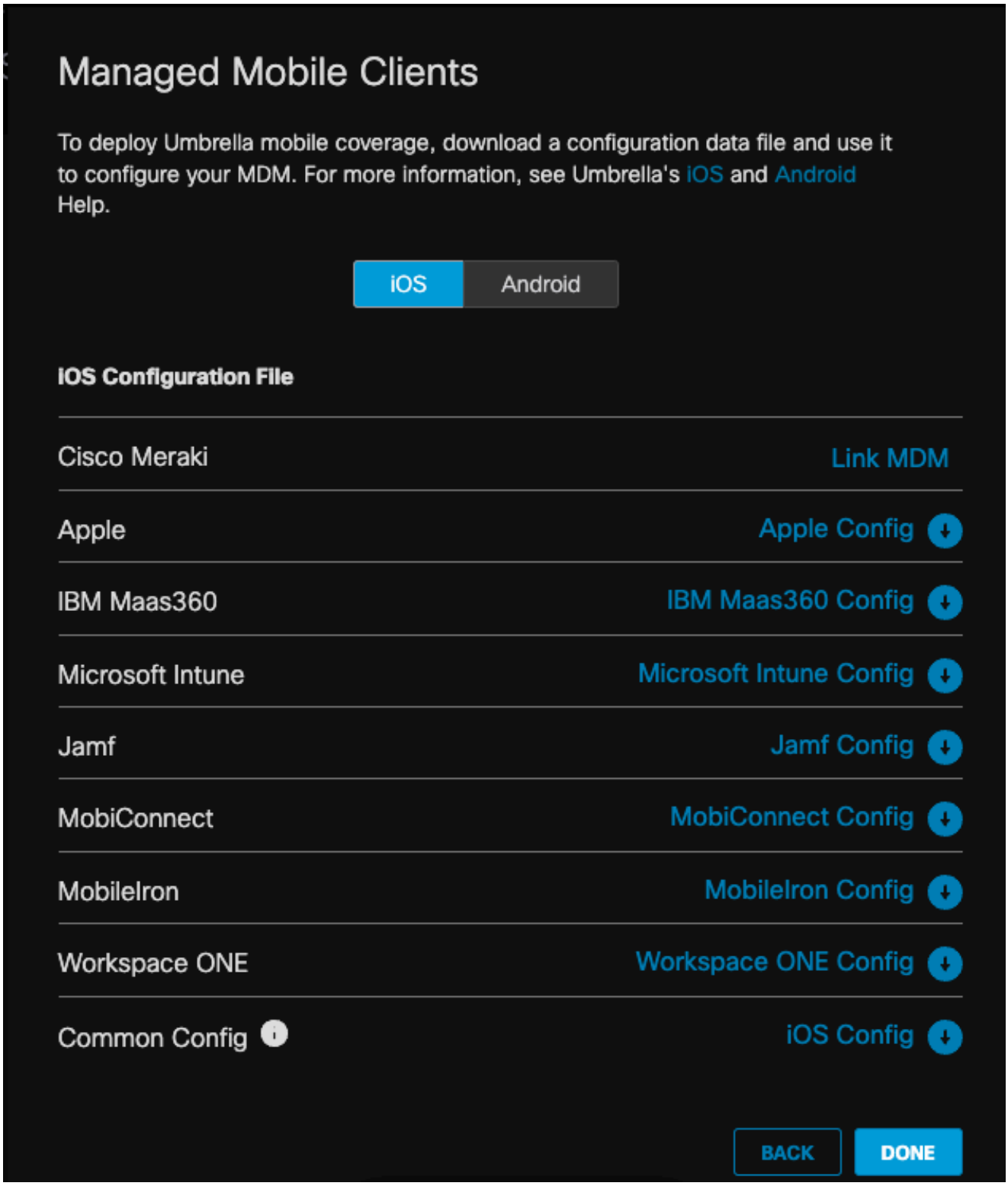
11753916236820

18. Melden Sie sich bei Ihrem Cisco Umbrella Dashboard unter Deployments —> Core Identities —> Mobile Devices —> oben rechts an: Verwalten —> Verwaltet von MDM



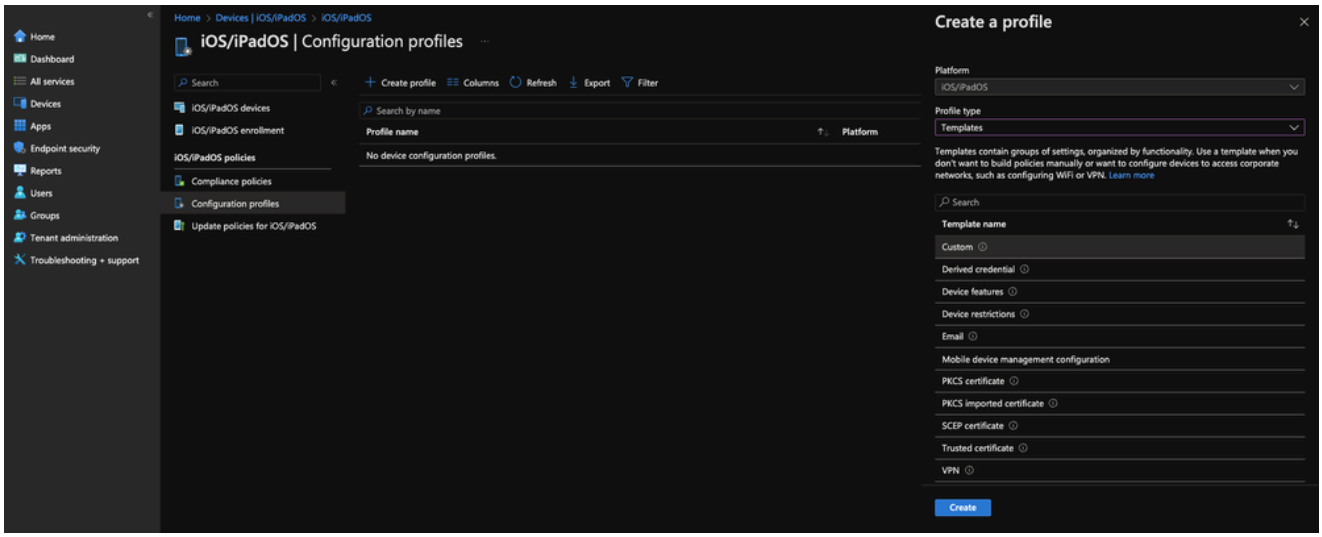
11753923081492

19. Gehen Sie dann zu iOS —> Microsoft Intune Config herunterladen. Geben Sie Ihre E-Mail-Adresse ein, an die E-Mails gesendet werden sollen, wenn Benutzer in der Cisco Security Connector-App die Option "Problem melden" auswählen.



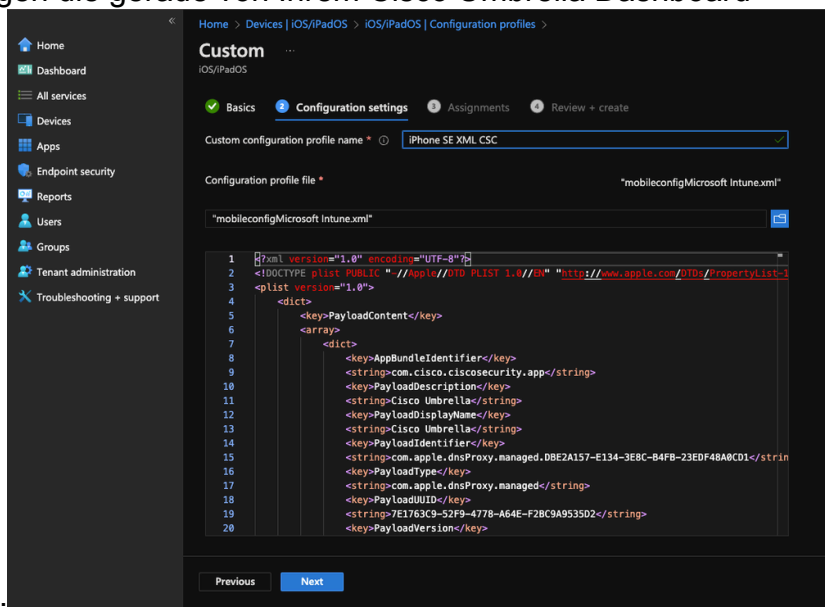
11753924523540

20. Gehen Sie zurück zu Ihrem Intune-Portal, unter Geräte —> iOS/iPadOS —> Konfigurationsprofile —> Profil erstellen —> Vorlagen —> Benutzerdefiniert



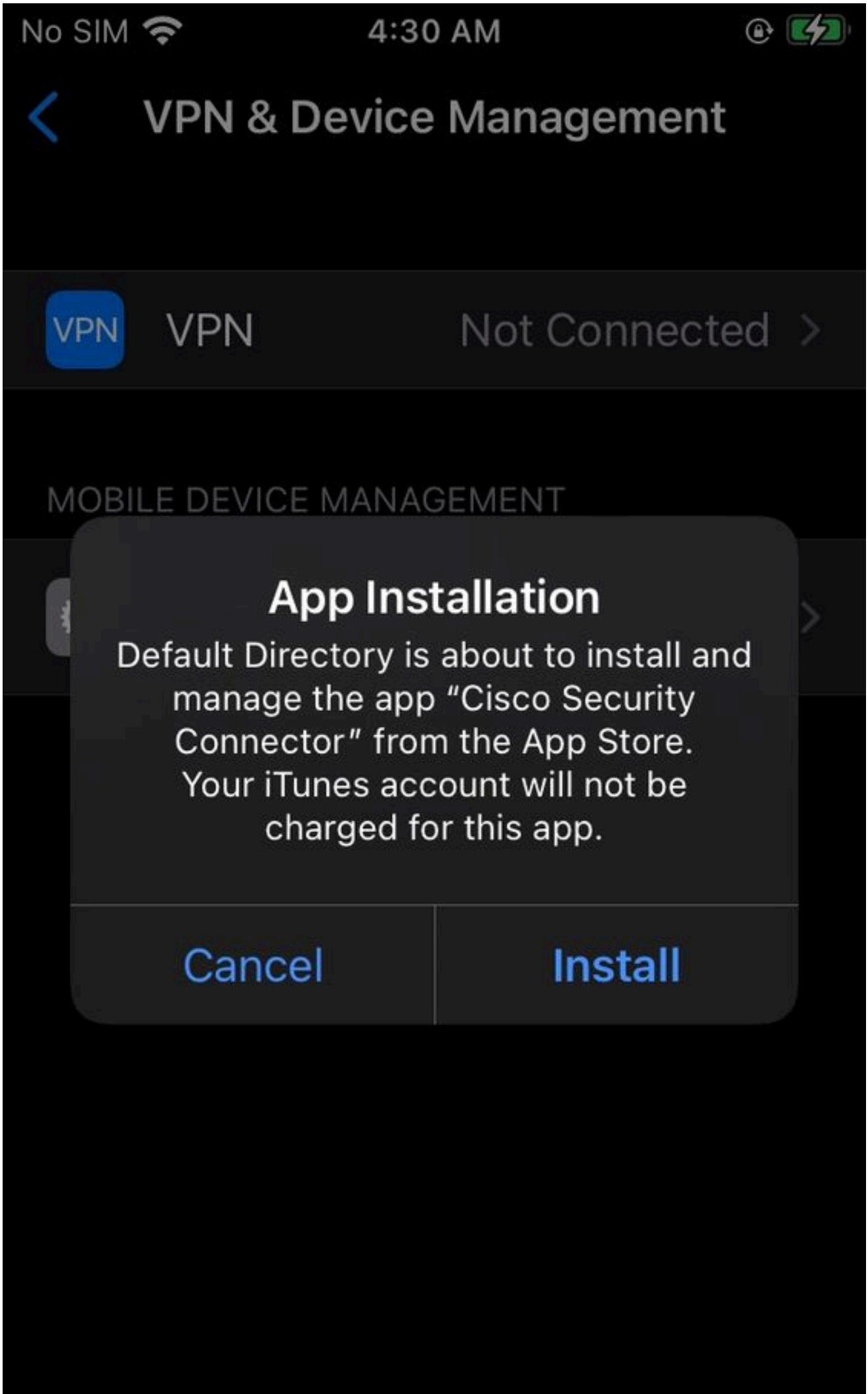
11753988354964

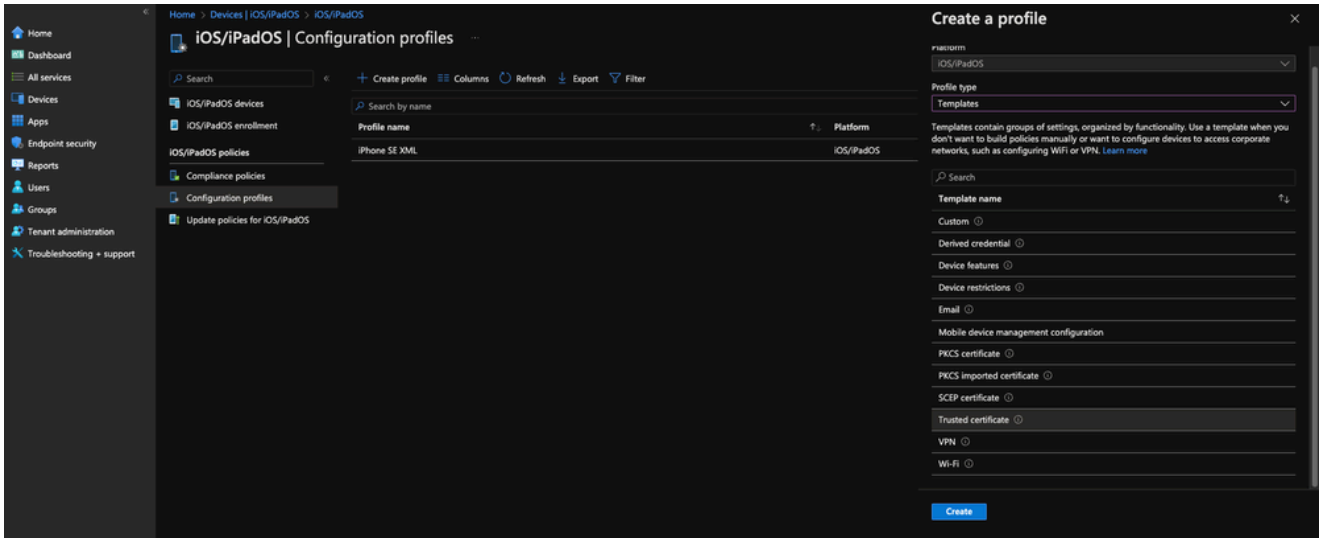
21. Geben Sie ihm einen aussagekräftigen Namen für Ihr Konfigurationsprofil. Laden Sie in Schritt 2 - Konfigurationseinstellungen die gerade von Ihrem Cisco Umbrella Dashboard heruntergeladene XML-Datei hoch.



11754000962196

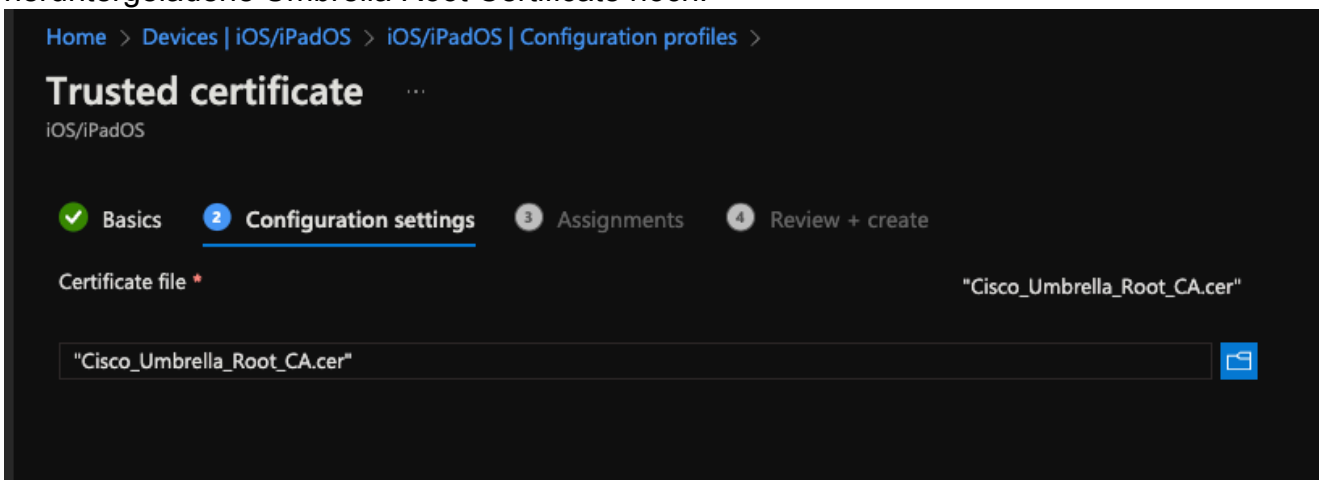
22. Weisen Sie unter Zuweisungen die Gruppe zu, die Sie zuvor erstellt haben und die Ihr MDM-Gerät enthält, und wählen Sie "Prüfen und erstellen".
23. Wechseln Sie zurück zu iOS/iPadOS-Geräten, wählen Sie Ihr MDM-Gerät aus, und klicken Sie oben auf "Sync". Auf Ihrem MDM-iOS/iPadOS-Gerät wird ein Popup-Fenster angezeigt, in dem Sie die Cisco Security Connector-App installieren können.


No SIM
4:30 AM
VPN & Device Management
VPN
VPN
Not Connected
MOBILE DEVICE MANAGEMENT
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.
Cancel
Install



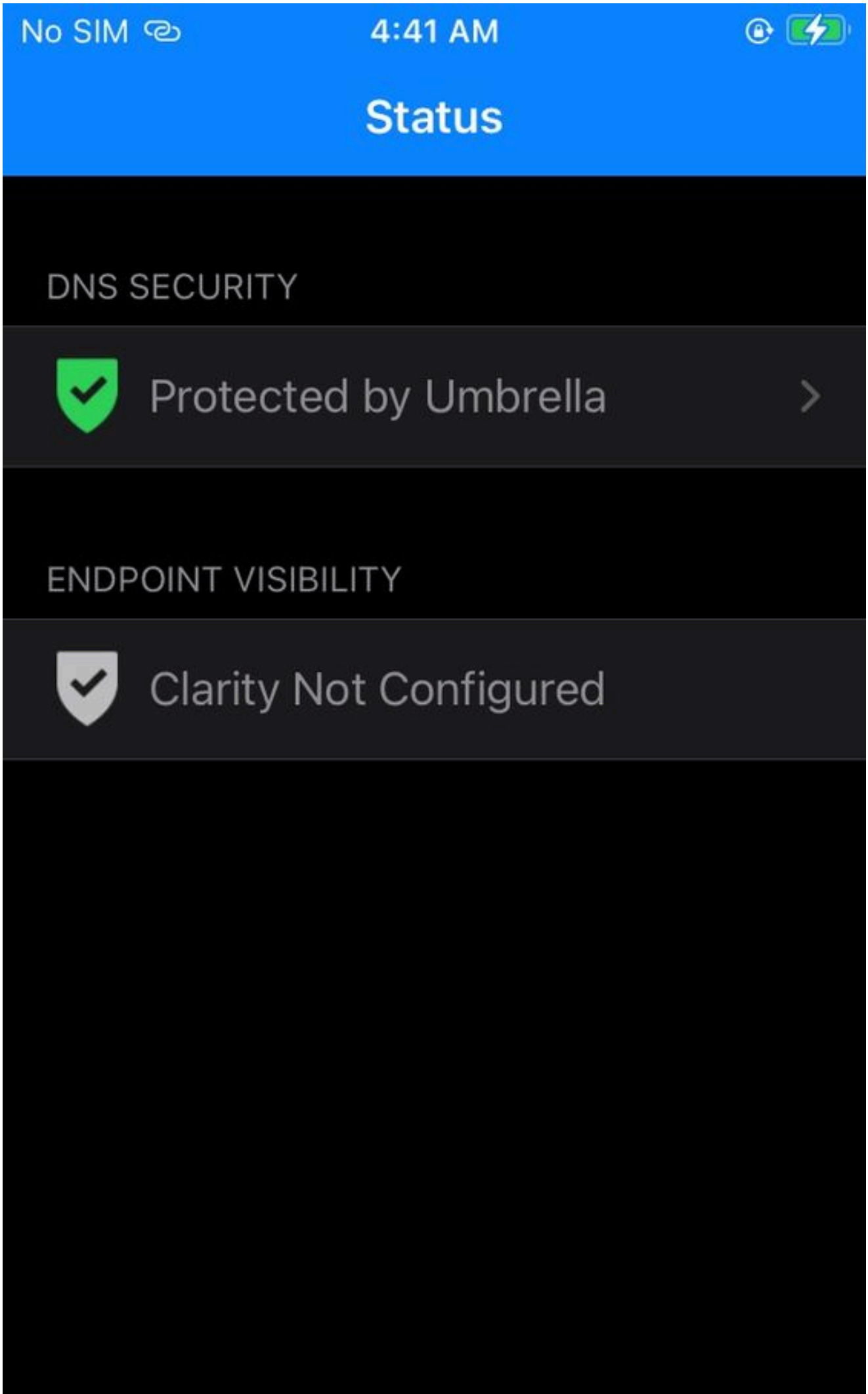
11754159037460

29. Laden Sie in Schritt 2 - Konfigurationseinstellungen das soeben von Schritt 27 heruntergeladene Umbrella Root Certificate hoch.



11754204605460

30. Wählen Sie für Schritt 3 - Aufgaben die Gruppe aus, die Ihr MDM iOS/iPadOS-Gerät enthält, und klicken Sie auf "Weiter" und "Erstellen".
31. Gehen Sie zurück zu iOS/iPadOS-Geräten und wählen Sie Ihr MDM-Gerät aus und klicken Sie erneut oben auf Sync (wie Schritt 24)
32. Schließen Sie die Cisco Security Connector-App, und starten Sie sie erneut. Jetzt wird der Status "Protected by Umbrella" angezeigt.


No SIM
4:41 AM
Status
DNS SECURITY
Protected by Umbrella
ENDPOINT VISIBILITY
Clarity Not Configured

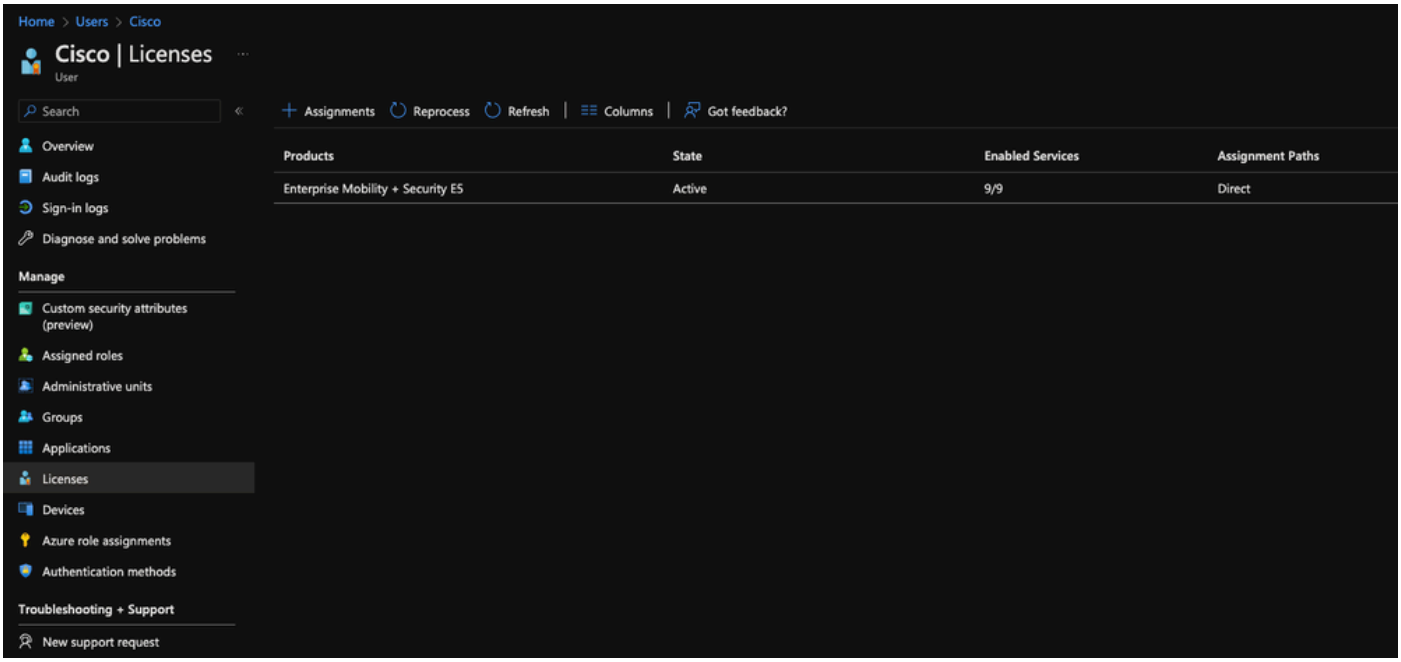

No SIM
4:48 AM
Cisco Umbrella
Welcome to Umbrella!
Your internet is faster, more reliable and better protected because you're using Cisco Umbrella.

- Sie können keine Einstellung "Eingeschränkte Apps" festlegen, die die Umbrella-App einschränkt, und/oder eine Einstellung "Ein- oder ausblenden", um die Umbrella-App auszublenden, die in Ihrem Gerätekonfigurationsprofil angewendet wird. (Wählen Sie unter Ihrem Intune-Admin-Center > Geräte > iOS/iPadOS > Konfiguration)

Fehlerbehebung

- Erfassen von Cisco Security Connector-Diagnoseprotokollen
- Fehler bei CSC-Protokoll "Problem melden", Funktion "Keine Admin-E-Mail"
- CSC: Ungeschützter Status in mobilen Netzwerken

Wenn Sie einen Fehler erhalten: "Der Benutzername wurde nicht erkannt. Dieser Benutzer ist nicht autorisiert, Microsoft Intune zu verwenden." gehen Sie zum Azure-Portal, wählen Sie unter "Users" den Benutzernamen oder das Konto aus, mit dem Sie Intune konfigurieren, gehen Sie zu "Licenses", und stellen Sie sicher, dass dem Benutzer eine aktive Intune-Lizenz zugewiesen ist.



11754557401748

Protokolle

Standardmäßig lautet das Kennwort für das Protokoll bypass_email_filters . Diese finden Sie auch unter UmbrellaProblemReport.txt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.