Déployer le connecteur de sécurité avec Intune

Table des matières

Introduction

Ce document décrit comment déployer le connecteur de sécurité à l'aide d'Intune.

Aperçu

Il s'agit d'un guide étape par étape sur la façon d'obtenir votre appareil iOS/iPadOS MDM-gérer via Intune, et pousser le profil via Apple Configurator

Vous pouvez également consulter notre documentation d'enregistrement Intune et notre guide PDF ici

Remarque : cette méthode vous montre comment gérer vos appareils MDM via Intune et Apple Configurator

Remarques importantes :

Si vous utilisez MDM pour vos périphériques supervisés via l'application Company Portal, vous pouvez commencer à l'étape 14.

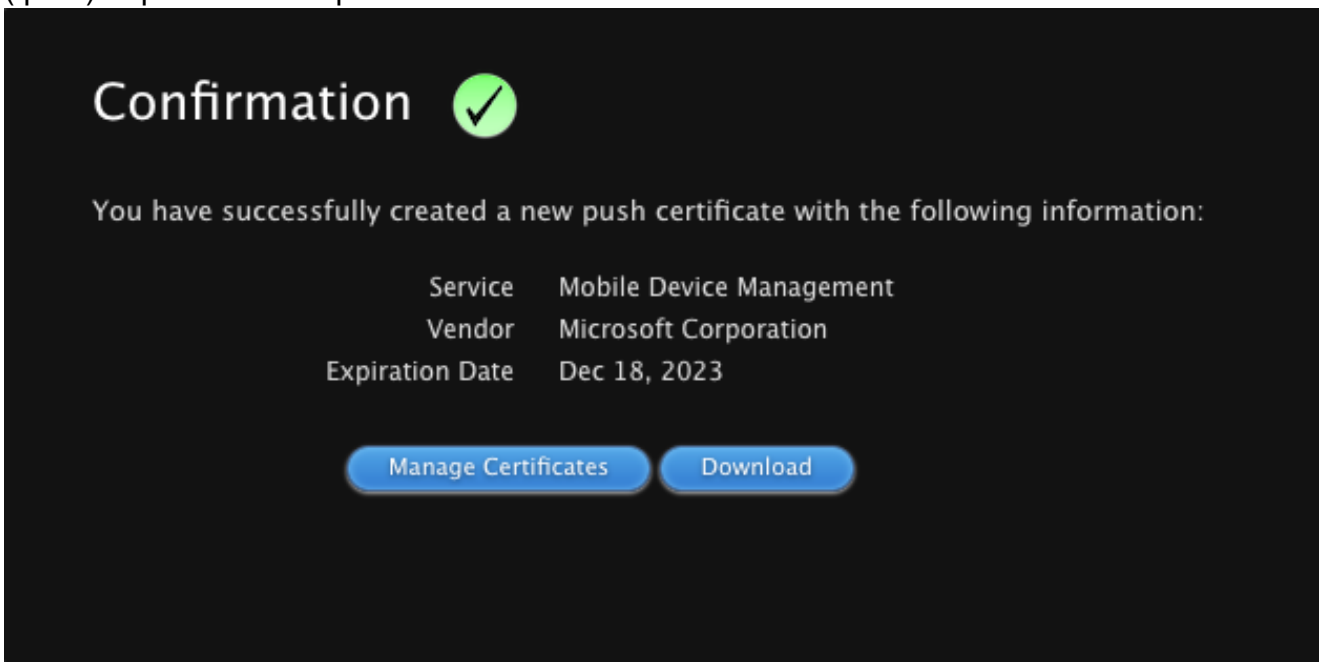
Cet article est fourni en l'état à partir du 12/04/2023, le support Umbrella ne garantit pas que ces instructions resteront valides après cette date et sont sujettes à modification en fonction des mises à jour de Microsoft Intune et Apple iOS.

Procédure

1. Connectez-vous au portail Azure et recherchez « Intune ». Vous pouvez également vous connecter à l'adresse https://intune.microsoft.com/Error/UE_404?aspxerrorpath=/ et vous connecter
2. Une fois sur la page d'accueil d'Intune, allez à Devices —> iOS/iPadOS —> iOS/iPadOS enrollment —> Apple MDM Push certificate et cliquez sur "Download your CSR" 

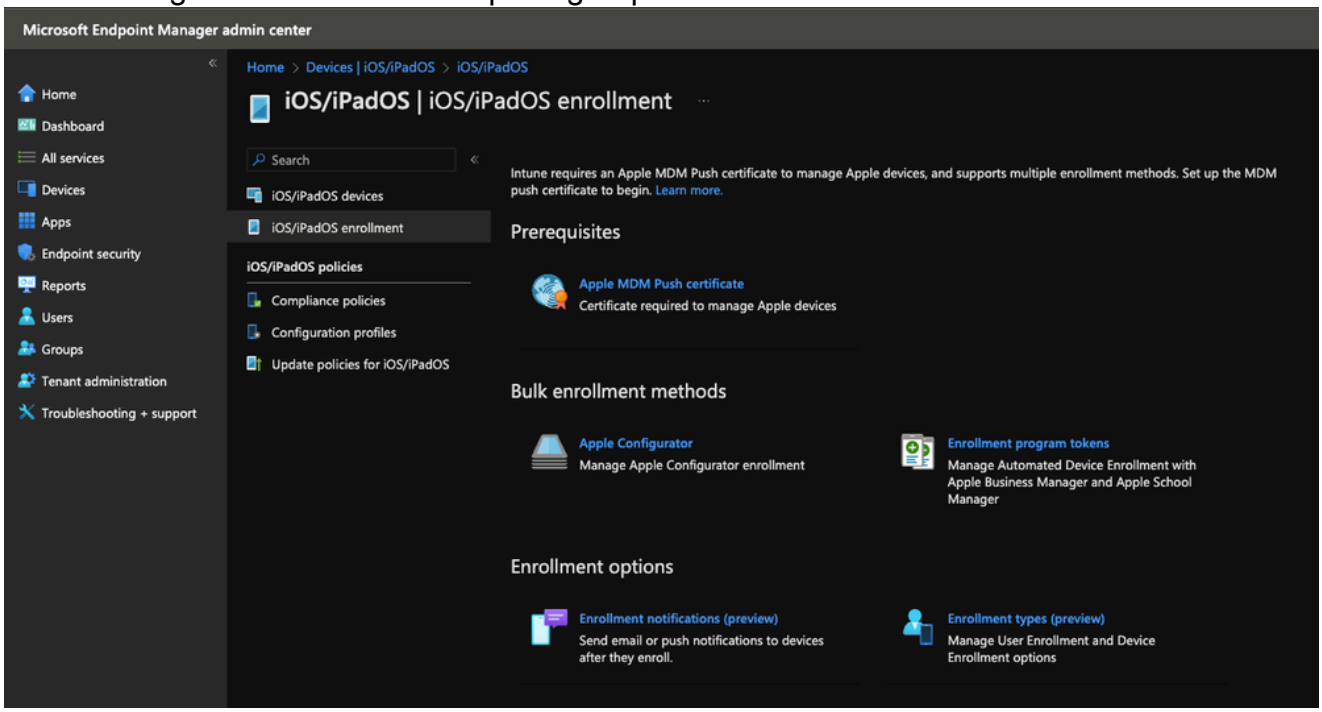
11752925317012

3. Cliquez ensuite sur « Create your MDM push Certificate » (Créer votre certificat de diffusion MDM), qui vous redirige vers https://identity.apple.com/pushcert/
4. Sur le portail Apple Push Certificates, accédez à « Créer un certificat » et téléchargez le fichier IntuneCSR.csr que vous venez de télécharger. Une fois le fichier CSR téléchargé avec succès, cliquez sur « Télécharger » pour télécharger le fichier Privacy Enhanced Mail (.pem) et passez à l'étape suivante



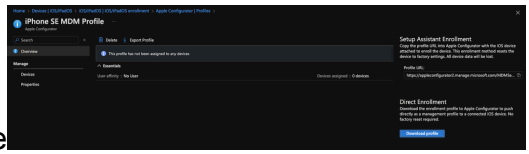
11752968667924

5. Entrez l'adresse e-mail de votre compte Apple ID que vous avez utilisé pour vous connecter au portail Apple Push Certificates et télécharger le fichier .pem sous "Apple MDM push certificate" et appuyez sur "Upload". Si le téléchargement a réussi, les autres options du déverrouillage « Méthodes d'inscription groupée » s'affichent.



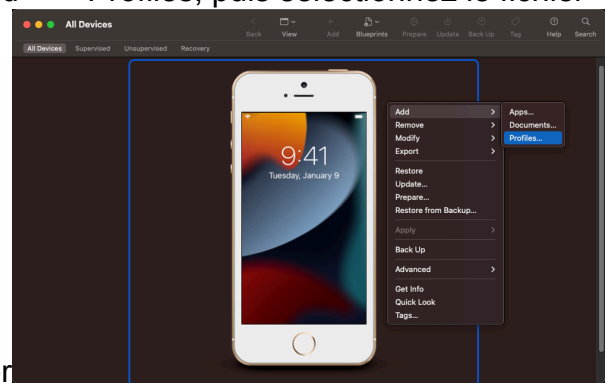
11752971407380

6. Accédez à Apple Configurator —> Profiles —> Create et créez un nouveau profil. Donnez-lui un nom significatif et pour Affinité utilisateur sélectionnez "S'inscrire sans affinité utilisateur". Une fois que ce profil a été créé, cliquez sur votre profil nouvellement créé et sélectionnez « Exporter le profil », puis « Télécharger le profil » à droite



11753020728596

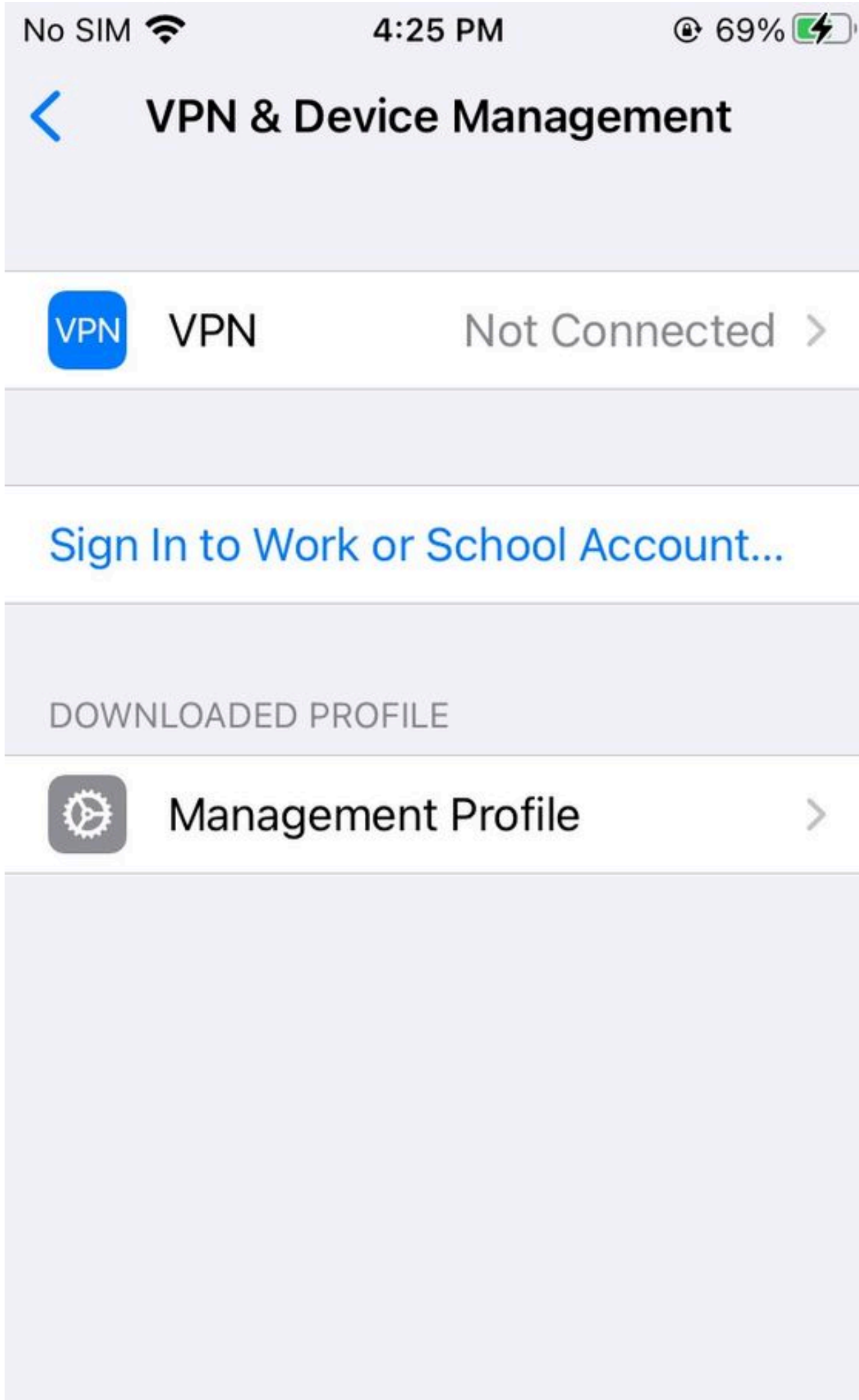
7. Téléchargez et lancez « Apple Configurator » sur votre macOS depuis l'App Store et connectez votre téléphone via Lightning Cable. Cliquez avec le bouton droit sur votre appareil dans Apple Configurator, sélectionnez Add —> Profiles, puis sélectionnez le fichier profile.mobileconfig que vous venez de télécharger

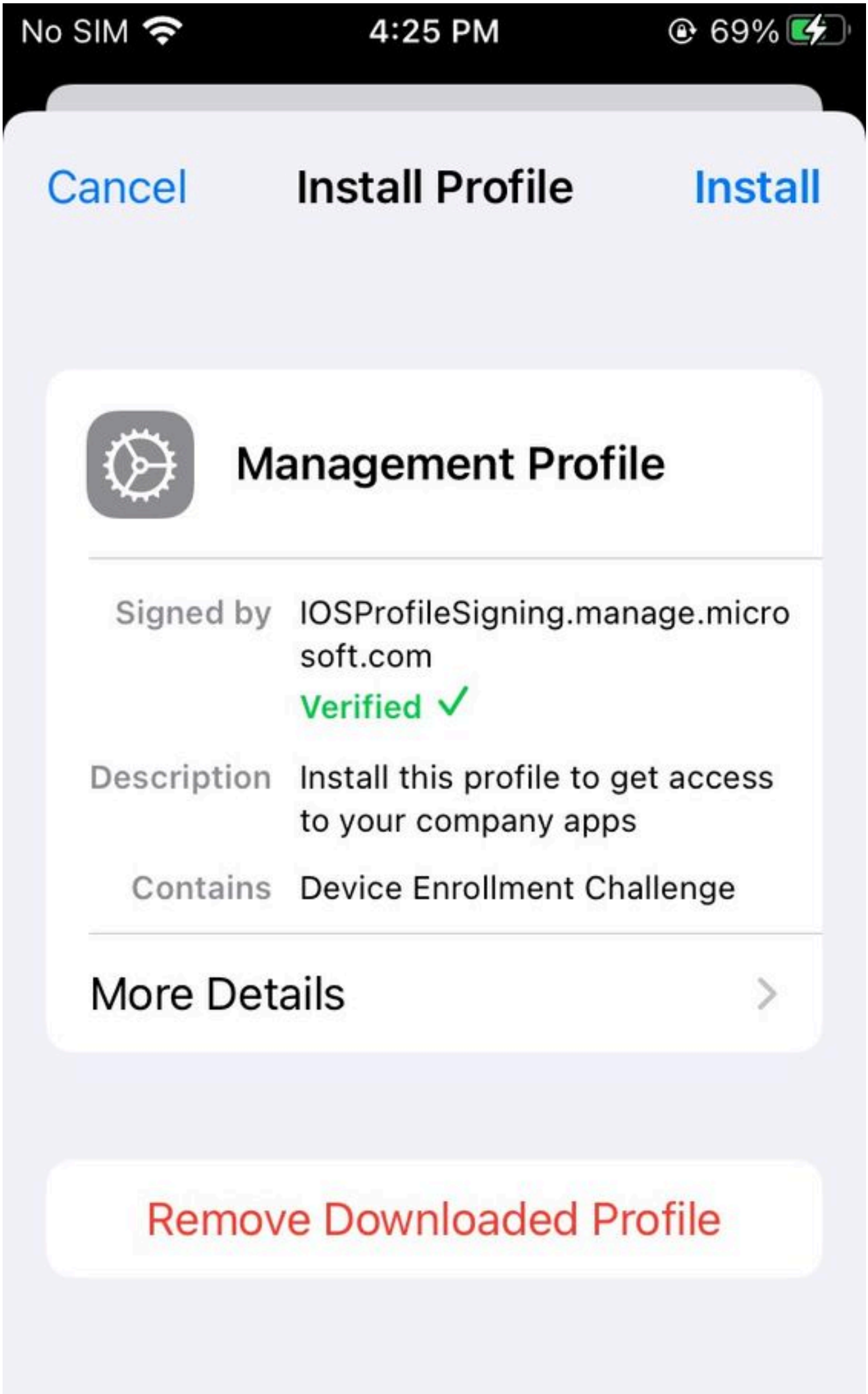


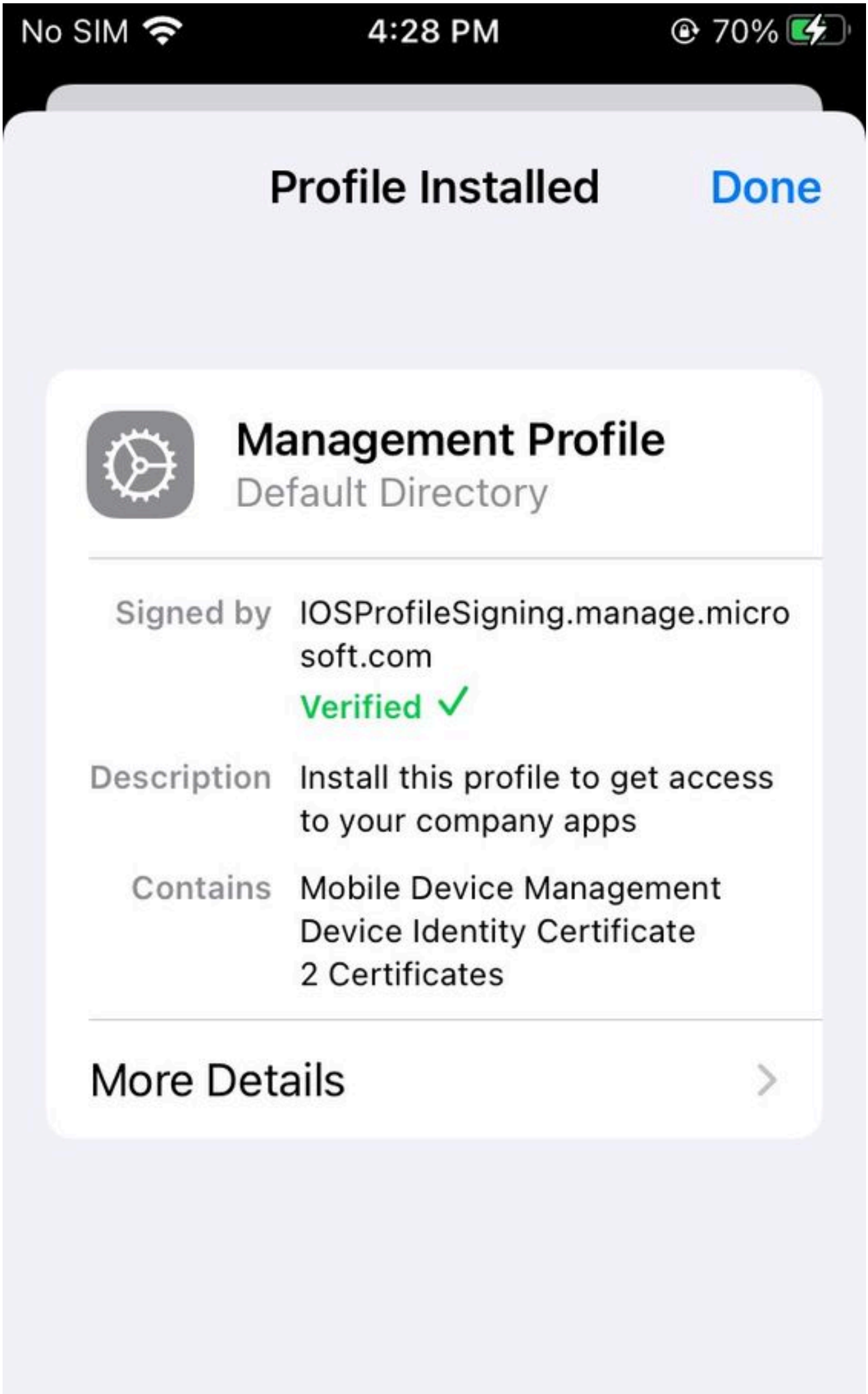
11753024446100

Alternatif Windows : Utilitaire de configuration iPhone

8. Une fois la synchronisation terminée, sur votre appareil iOS/iPadOS, accédez à l'application Paramètres et accédez à Général —> Gestion des VPN et des appareils —> Profil de gestion


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

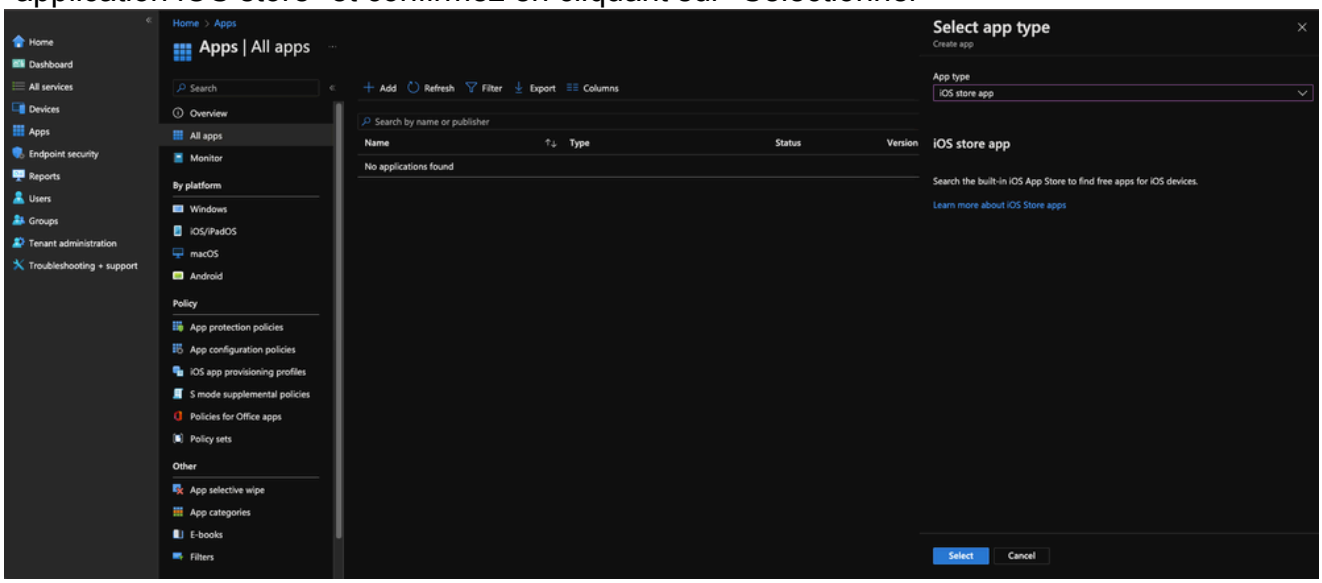

No SIM
4:25 PM
69%
Cancel
Install Profile
Install
Management Profile
Signed by
IOSProfileSigning.manage.microsoft.com
Verified
Description
Install this profile to get access to your company apps
Contains
Device Enrollment Challenge
More Details
Remove Downloaded Profile


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

. Recherchez votre périphérique MDM sur lequel vous souhaitez installer l'application Cisco Security Connector, dans la liste et ajoutez-le au groupe que vous venez de créer 

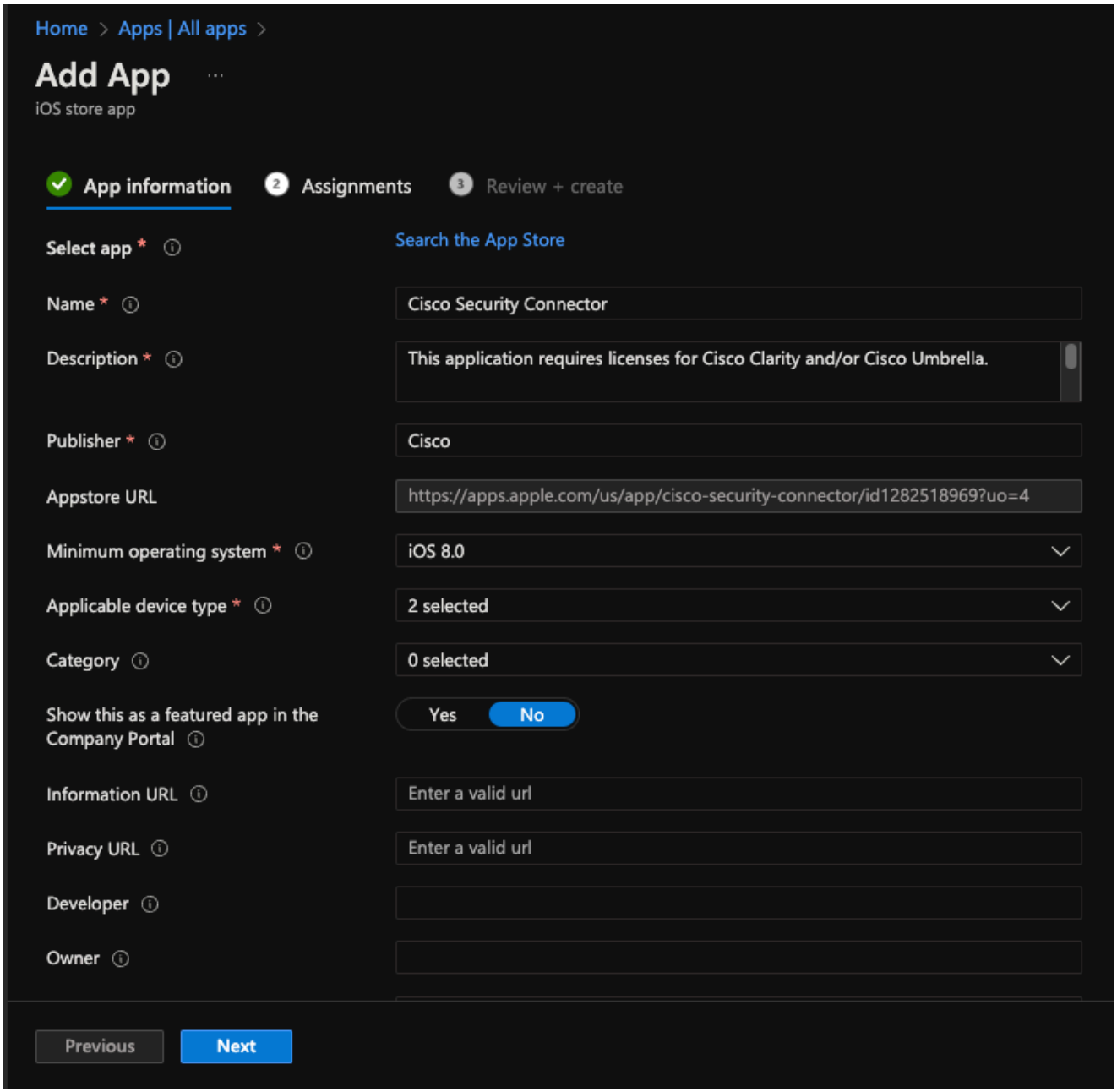
11753692550036

14. Accédez à Apps —> All apps —> Add. Ensuite, pour le type d'application, sélectionnez "application iOS store" et confirmez en cliquant sur "Sélectionner"



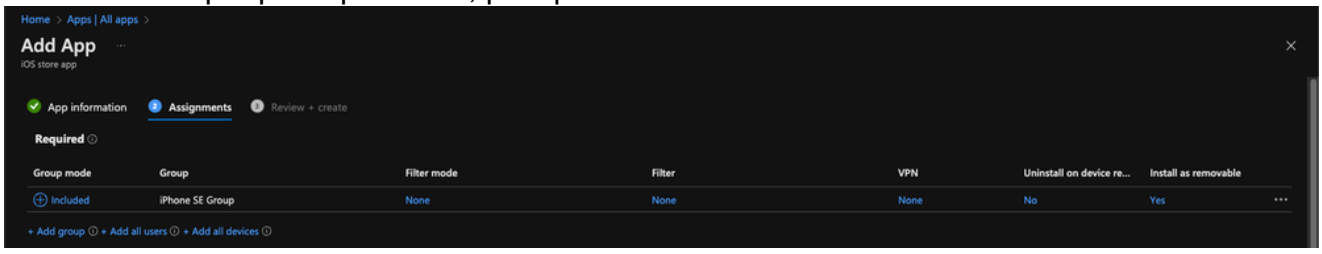
11753797372436

15. Sélectionnez « Rechercher dans l'App Store », saisissez « Cisco Security Connector » dans la barre de recherche et sélectionnez l'application « Cisco Security Connector » en cliquant sur « Sélectionner »



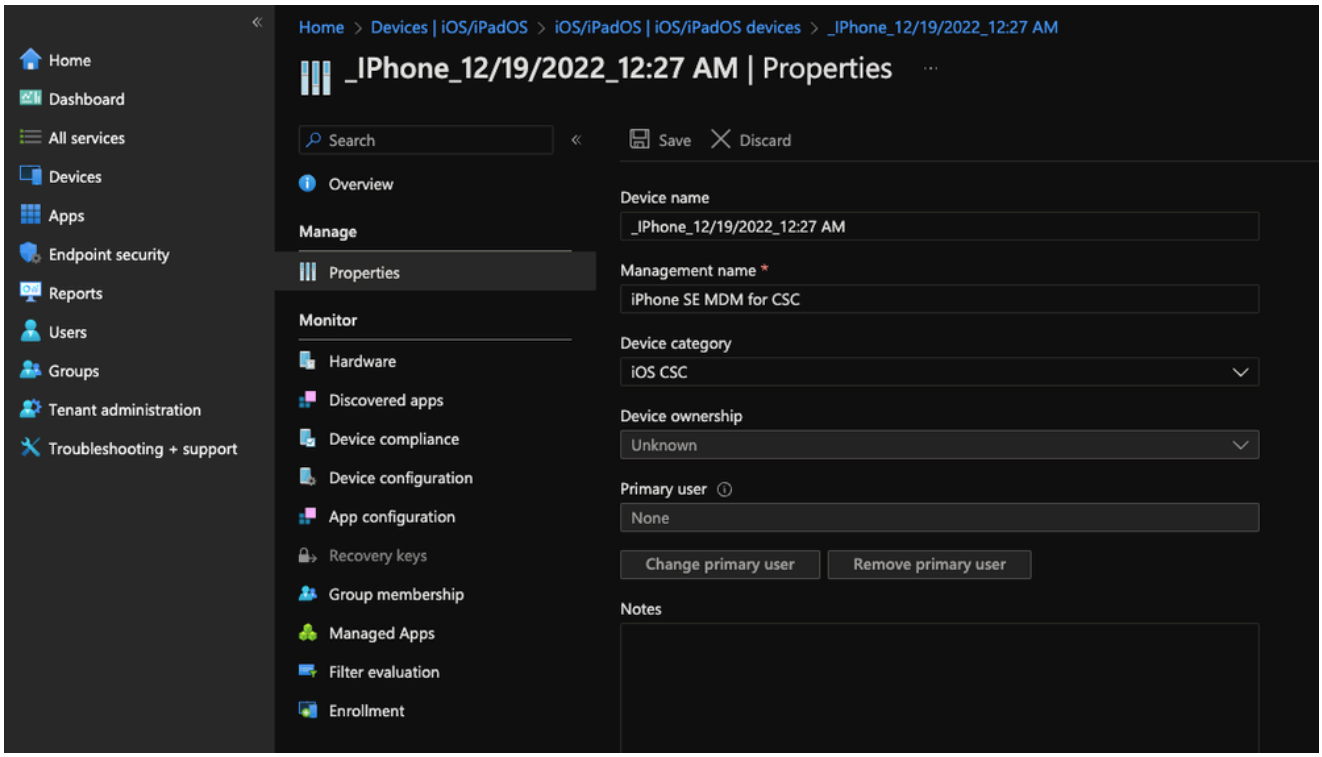
11753844054420

16. Sous Assignments, ajoutez le groupe que vous avez créé dans les étapes précédentes qui contient votre périphérique MDM, puis passez à l' Vérifier et créer



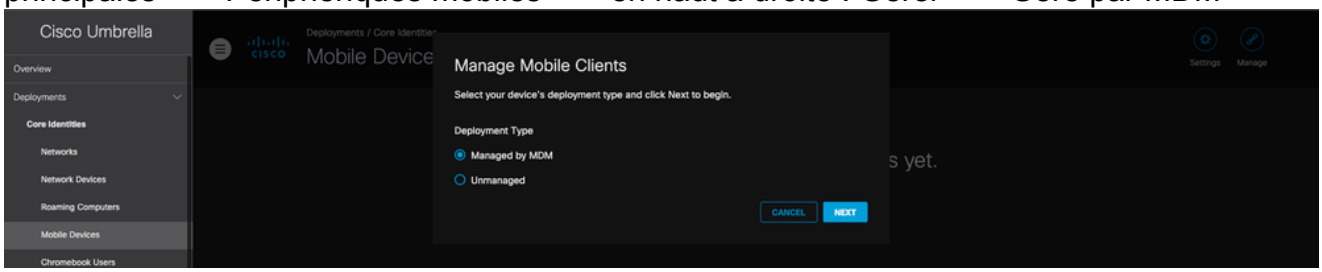
11753839516692

17. [Étape facultative] Accédez à Périphériques —> iOS/iPadOS —> Périphériques iOS/iPadOS —> Propriétés —> Catégorie de périphérique, créez un profil et attribuez-le au périphérique



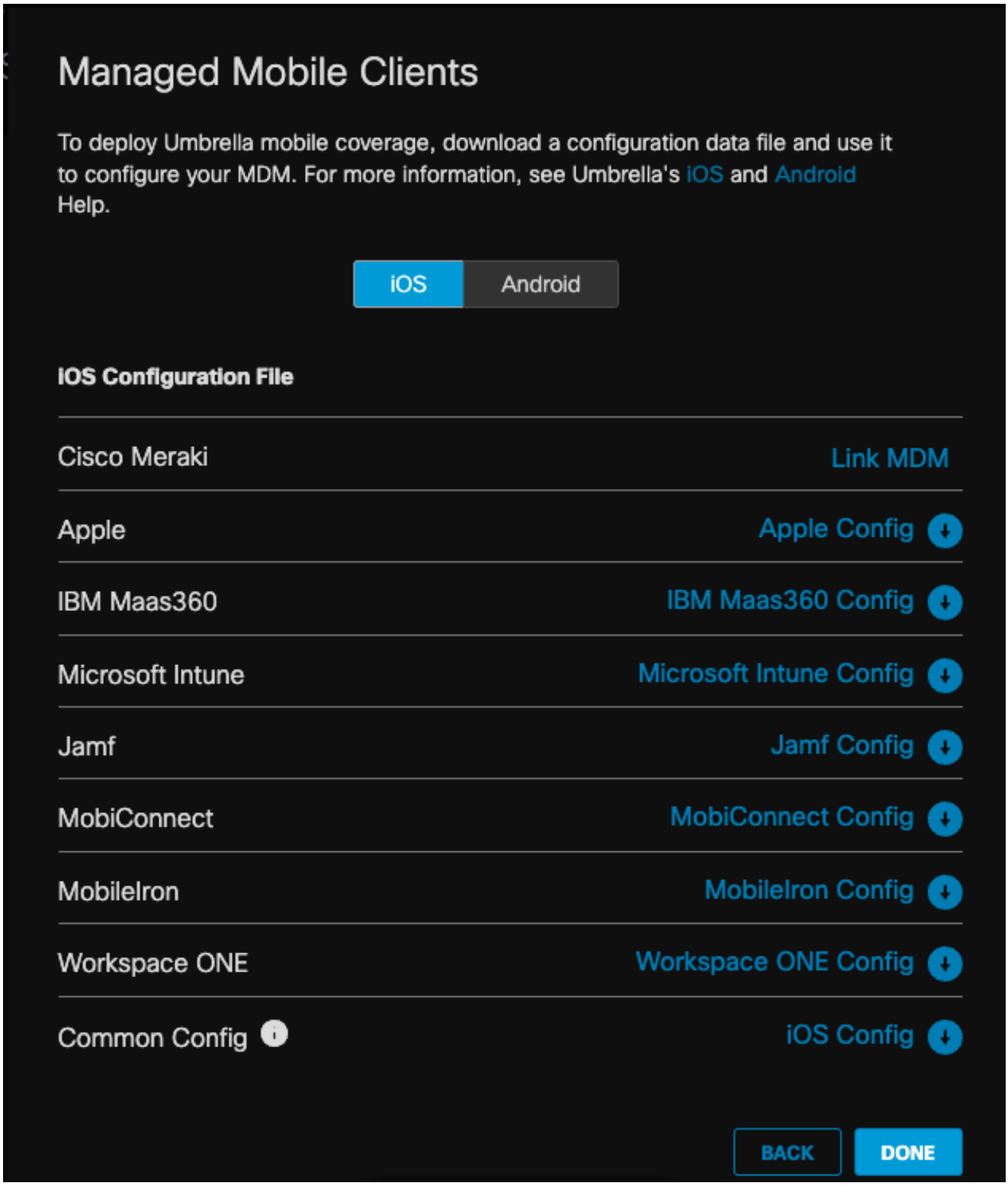
11753916236820

18. Connectez-vous à votre tableau de bord Cisco Umbrella, sous Déploiements —> Identités principales —> Périphériques mobiles —> en haut à droite : Gérer —> Géré par MDM



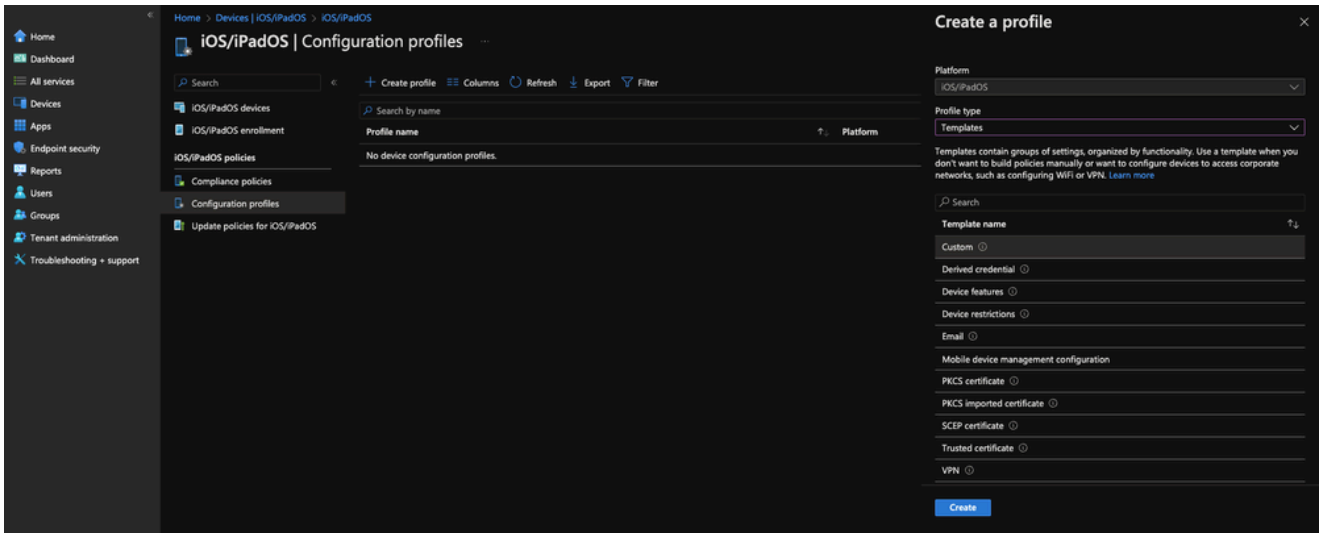
11753923081492

19. Accédez ensuite à iOS —> Téléchargement de la configuration Microsoft Intune. Saisissez l'adresse e-mail à laquelle vous souhaitez que les e-mails soient envoyés lorsque les utilisateurs sélectionnent Signaler un problème dans l'application Cisco Security Connector



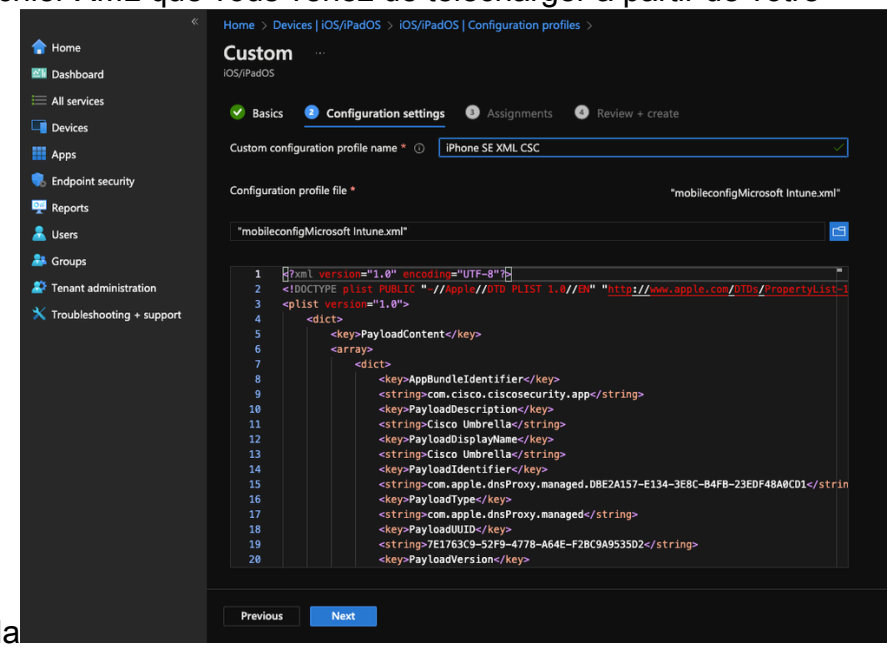
11753924523540

20. Revenez à votre portail Intune, sous Périphériques —> iOS/iPadOS —> Profils de configuration —> Créer un profil —> Modèles —> Personnalisé



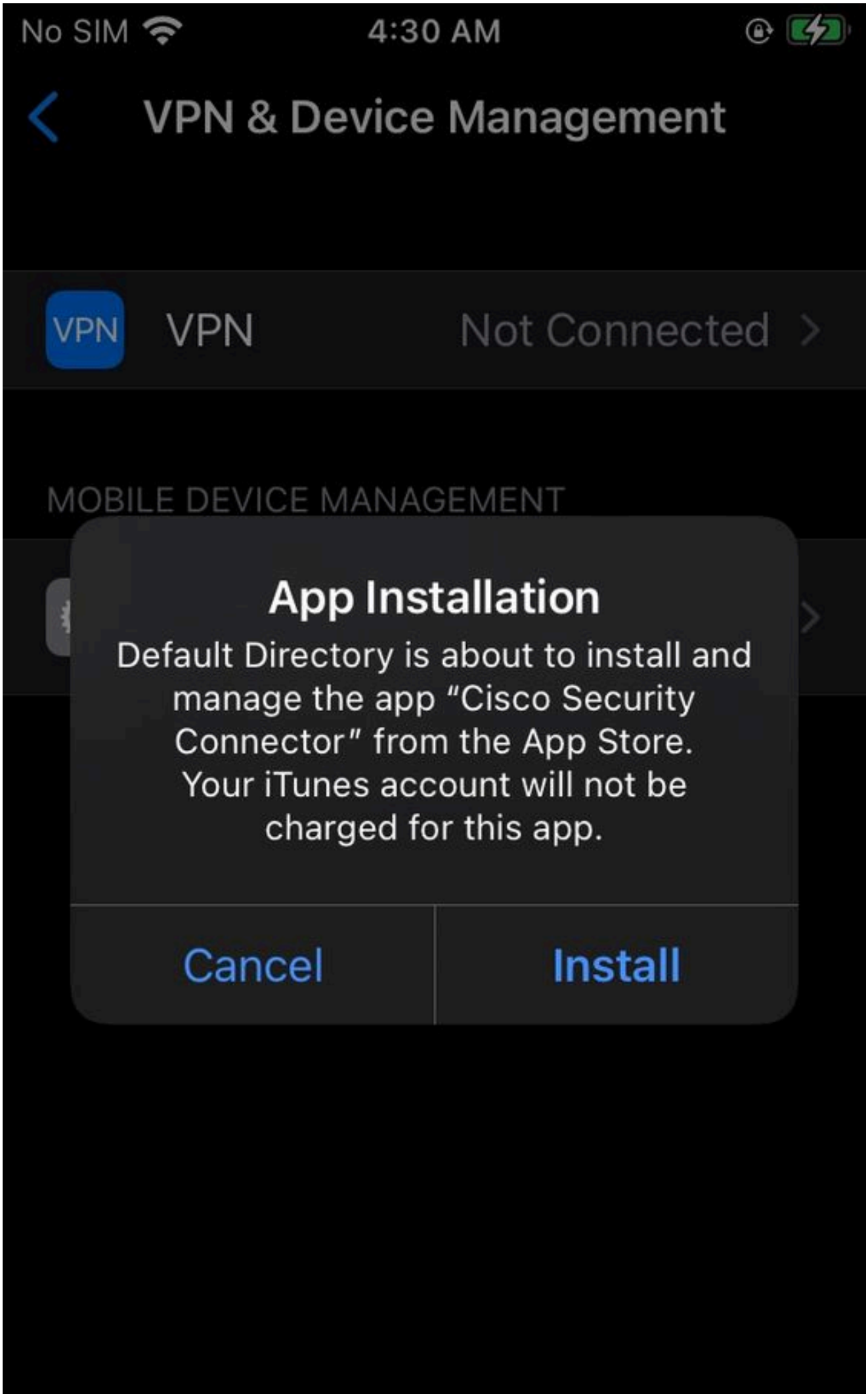
11753988354964

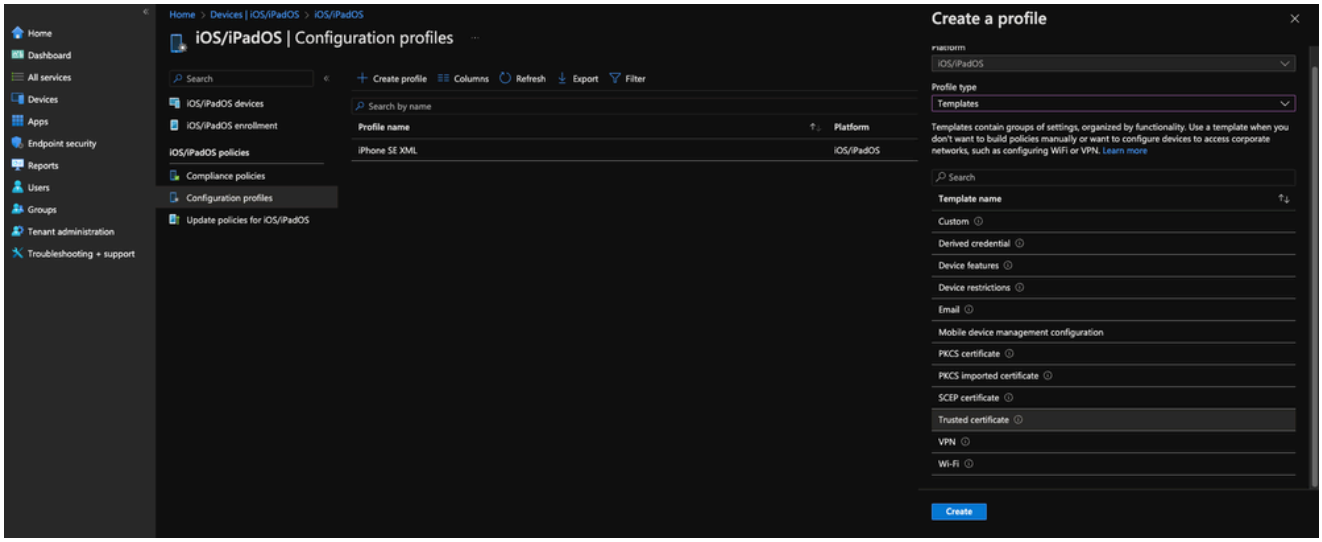
21. Donnez-lui un nom significatif pour votre profil de configuration. À l'étape 2 - Paramètres de configuration, téléchargez le fichier XML que vous venez de télécharger à partir de votre tableau de bord Cisco Umbrella



11754000962196

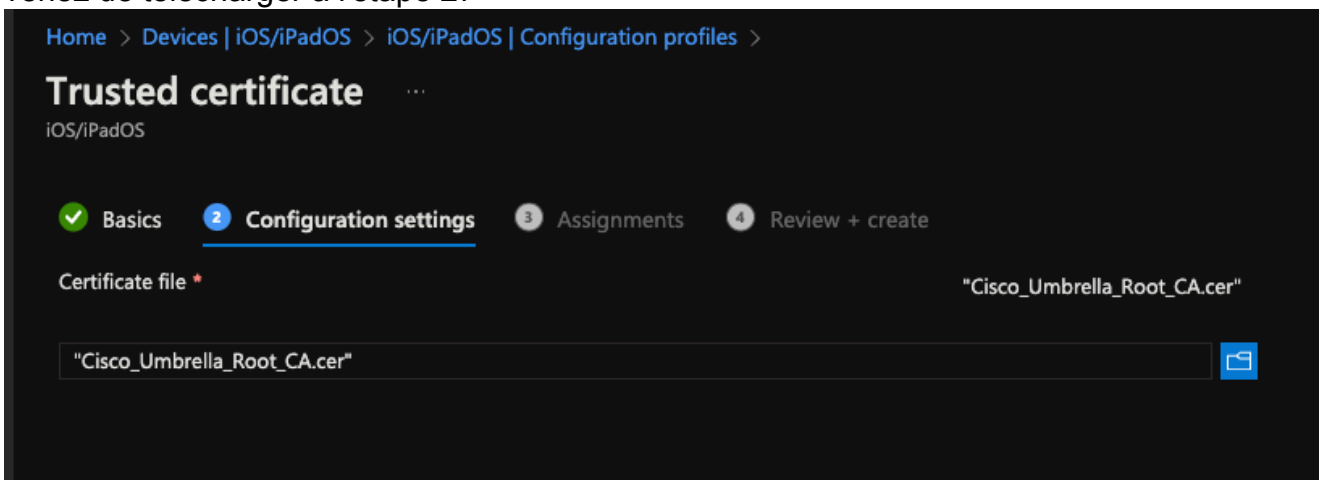
22. Sous Assignments, attribuez le groupe que vous avez créé précédemment et qui contient votre périphérique MDM et sélectionnez « Review and Create »
23. Retournez aux appareils iOS/iPadOS et sélectionnez votre appareil MDM et cliquez sur sync en haut et vous obtenez une fenêtre contextuelle sur votre appareil MDM iOS/iPadOS pour installer l'application Cisco Security Connector


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



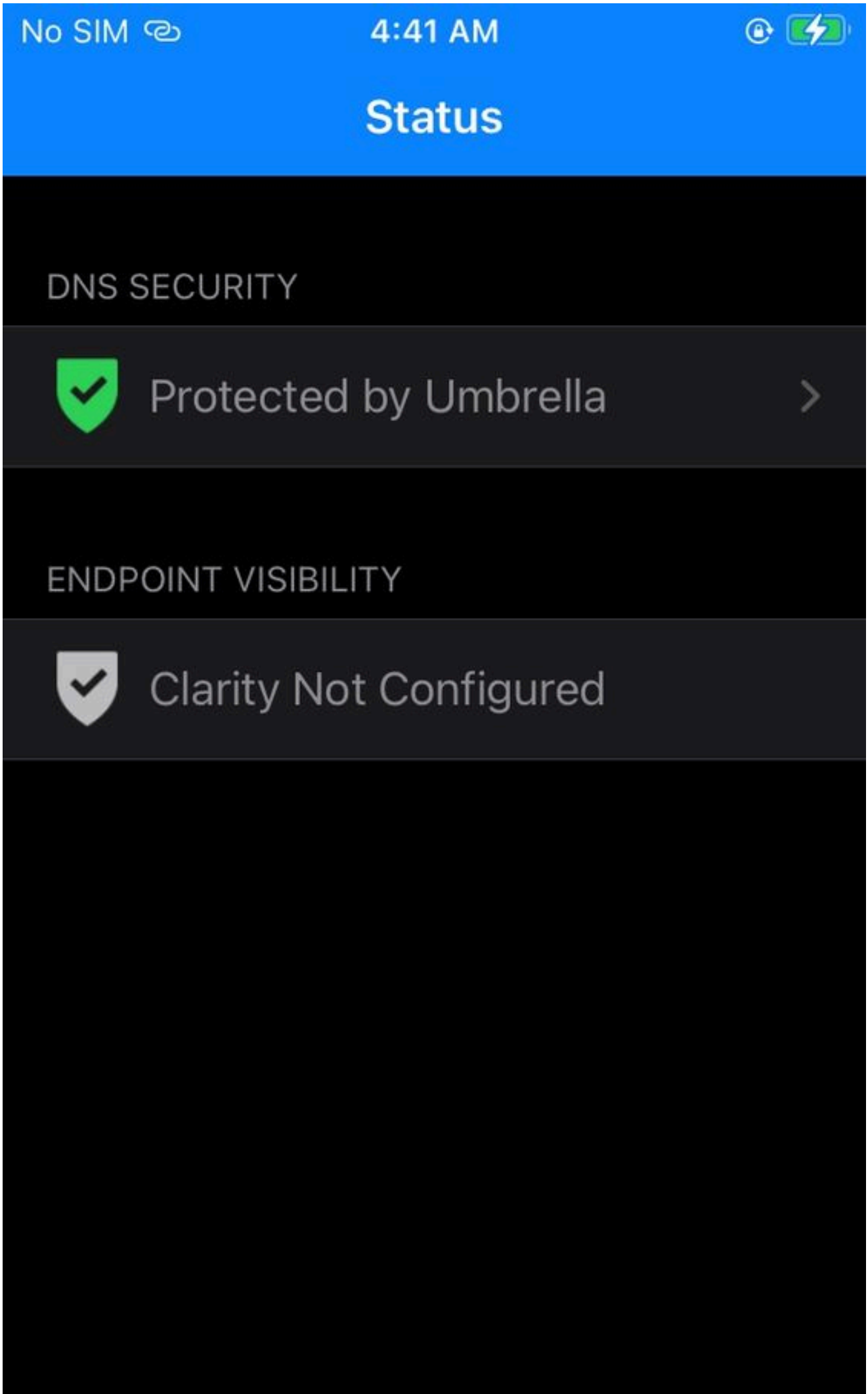
11754159037460

29. À l'étape 2 - Paramètres de configuration, téléchargez le certificat racine Umbrella que vous venez de télécharger à l'étape 27



11754204605460

30. Pour l'étape 3 - Affectations, sélectionnez le groupe qui contient votre appareil MDM iOS/iPadOS et cliquez sur "Next" et "Create"
31. Retournez aux appareils iOS/iPadOS et sélectionnez votre appareil MDM et appuyez à nouveau sur sync en haut (comme étape 24)
32. Fermez et relancez l'application Cisco Security Connector. Vous voyez maintenant l'état "Protégé par un parapluie"


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

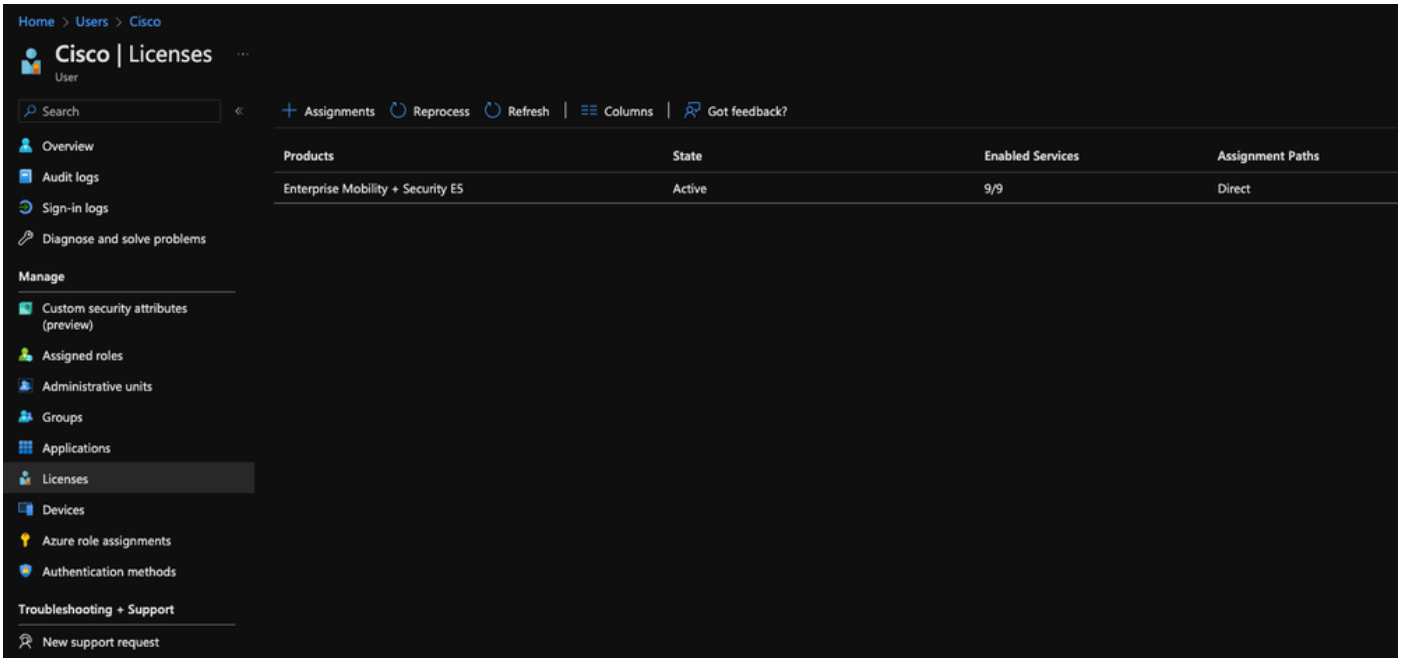

No SIM
4:48 AM
Cisco Umbrella
Welcome to Umbrella!
Your internet is faster, more reliable and better protected because you're using Cisco Umbrella.

- Vous ne pouvez pas avoir de paramètre « Applications restreintes » limitant l'application Umbrella, et/ou de paramètre « Afficher ou masquer » pour masquer l'application Umbrella appliquée dans votre profil de configuration d'appareil.(Sous votre Centre d'administration Intune > Appareils > iOS/iPadOS > Configuration)

Dépannage

- Comment collecter les journaux de diagnostic du connecteur de sécurité Cisco
- Erreur du journal CSC « Signaler un problème » Fonction « Aucun e-mail d'administrateur »
- CSC : État « Non protégé » sur les réseaux mobiles

Si vous obtenez une erreur : "Nom d'utilisateur non reconnu. Cet utilisateur n'est pas autorisé à utiliser Microsoft Intune", accédez au portail Azure, sous « Utilisateurs » et sélectionnez le nom d'utilisateur ou le compte que vous utilisez pour configurer Intune, accédez à « Licences » et assurez-vous qu'une licence Intune active est attribuée à l'utilisateur



11754557401748

Journaux

Par défaut, le mot de passe des journaux est bypass_email_filters . Vous pouvez également le trouver dans UmbrellaProblemReport.txt

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.