

Intuneと共にセキュリティコネクタを展開する

内容

[はじめに](#)

[概要](#)

[手順](#)

[制限事項](#)

[トラブルシューティング](#)

[ログ](#)

はじめに

このドキュメントでは、Intuneを使用してセキュリティコネクタを展開する方法について説明します。

概要

これは、iOS/iPadOSデバイスをIntune経由でMDM管理し、Apple Configurator経由でプロファイルをプッシュする方法のステップバイステップガイドです

また、こちらから[Intune登録](#)ドキュメントと[PDFガイド](#)を参照することもできます

注：この方法では、IntuneおよびApple Configuratorを使用してデバイスをMDMする方法を示します

特記事項：

会社のポータルアプリケーションを使用して、監視対象デバイスのMDMを行う場合は、ステップ14から開始できます。

この記事は2023年4月12日現在のまま提供されています。Umbrellaサポートでは、これらの手順がこの日付以降も有効であることを保証せず、Microsoft IntuneおよびApple iOSからの更新に基づいて変更されることがあります。

手順

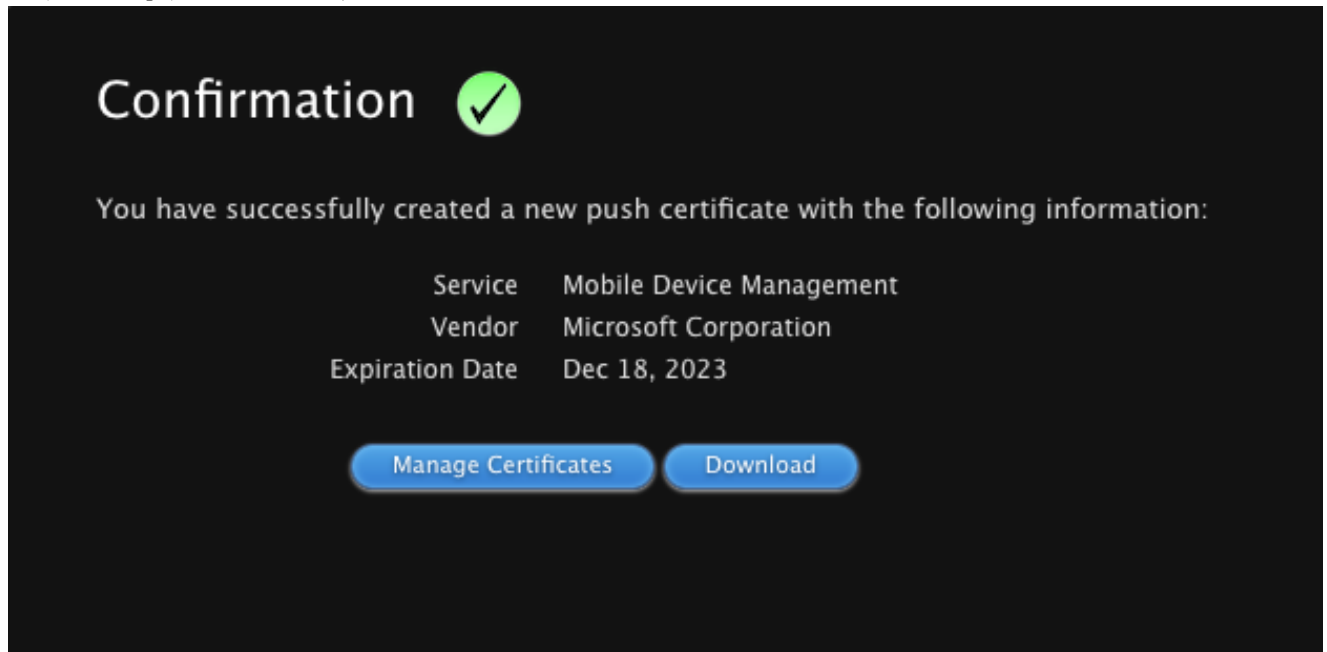
1. Azureポータルにログインして、「Intune」を検索します。または、https://intune.microsoft.com/Error/UE_404.aspxerrorpath=/にアクセスしてログインします
2. Intuneホームページが表示されたら、Devices → iOS/iPadOS → iOS/iPadOS enrollment → Apple MDM Push certificateの順に選択し、[Download your CSR]をクリックします。■

11752925317012

3. 次に、「Create your MDM push Certificate (MDMプッシュ証明書の作成)」をクリックし

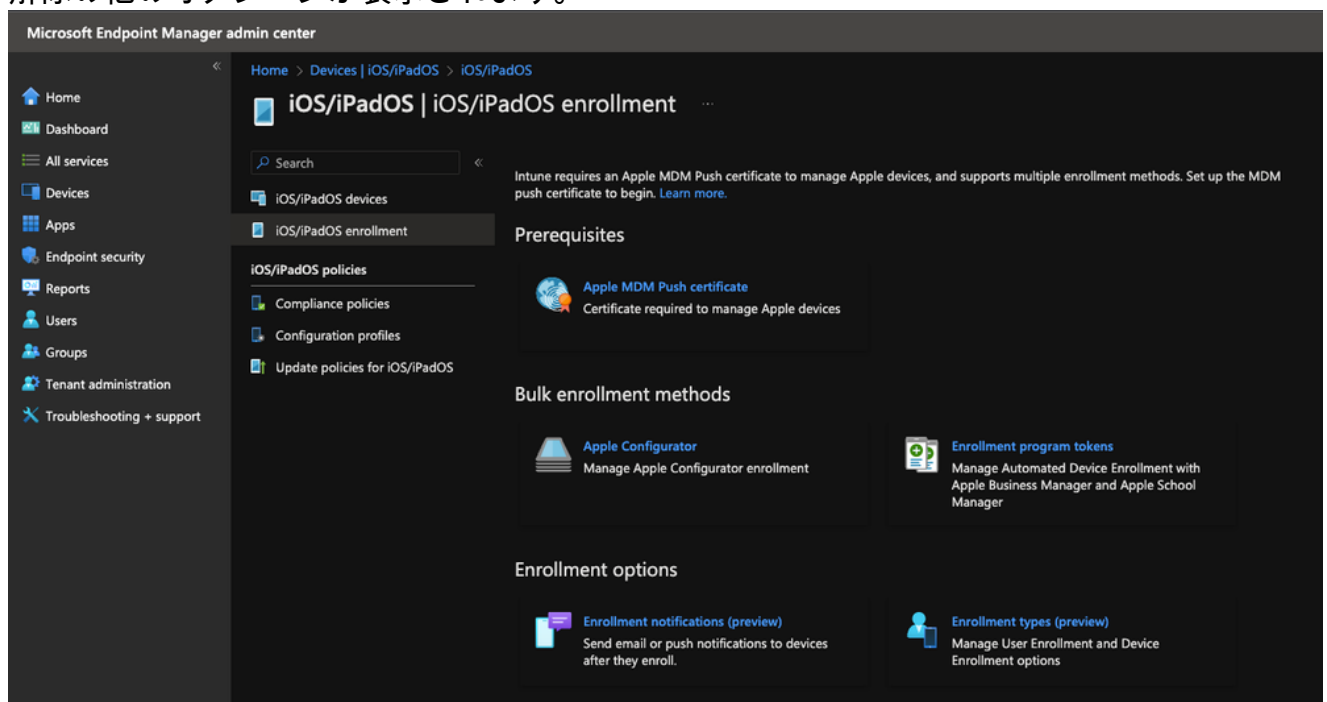
ます。<https://identity.apple.com/pushcert/>にリダイレクトされます。

- Apple Push Certificates Portalで、[証明書の作成]に移動し、ダウンロードしたIntuneCSR.csrファイルをアップロードします。CSRファイルが正常にアップロードされたら、「Download」をクリックしてプライバシー強化メール(.pemファイル)をダウンロードし、次の手順に進みます



11752968667924

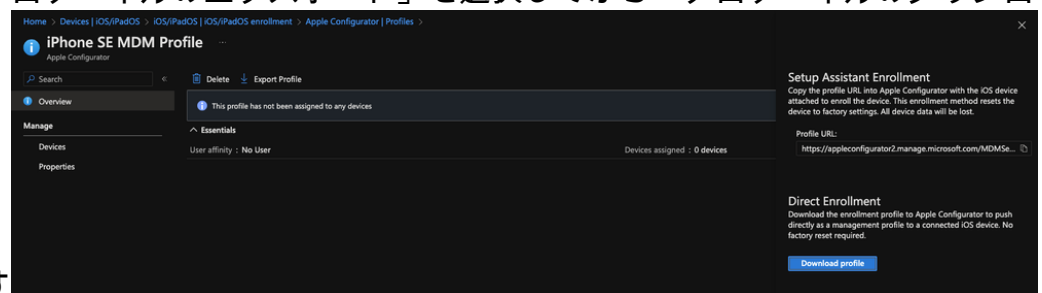
- Apple Push Certificates Portalへのサインインに使用したApple IDアカウントの電子メールアドレスを入力し、「Apple MDM push certificate」の下に.pemファイルをアップロードして、「アップロード」を押します。アップロードが成功すると、「一括登録方法」ロック解除の他のオプションが表示されます。



11752971407380

- Apple Configurator → Profiles → Createの順に選択し、新しいプロファイルを作成します

。わかりやすい名前を付け、「ユーザアフィニティ」で「ユーザアフィニティなしで登録」を選択します。そのプロファイルを作成したら、新しく作成したプロファイルをクリックし、右側にある「プロファイルのエクスポート」を選択してから「プロファイルのダウンロード」



ード」を選択します

11753020728596

7. App StoreからMacOSに「Apple Configurator」をダウンロードして起動し、Lightning Cable経由で電話を接続します。Apple Configuratorでデバイスを右クリックし、Add → Profilesを選択してから、ダウンロードしたprofile.mobileconfigファイルを選択します



11753024446100

Windows代替：iPhone構成ユーティリティ

8. 同期が完了したら、iOS/iPadOSデバイスでSettings appに移動し、General → VPN & Device Management → に移動します 管理プロファイル

No SIM 

4:25 PM

@ 69% 



VPN & Device Management



VPN

Not Connected >

[Sign In to Work or School Account...](#)

DOWNLOADED PROFILE



Management Profile



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

Profile Installed

[Done](#)



Management Profile

Default Directory

Signed by IOSProfileSigning.manage.microsoft.com

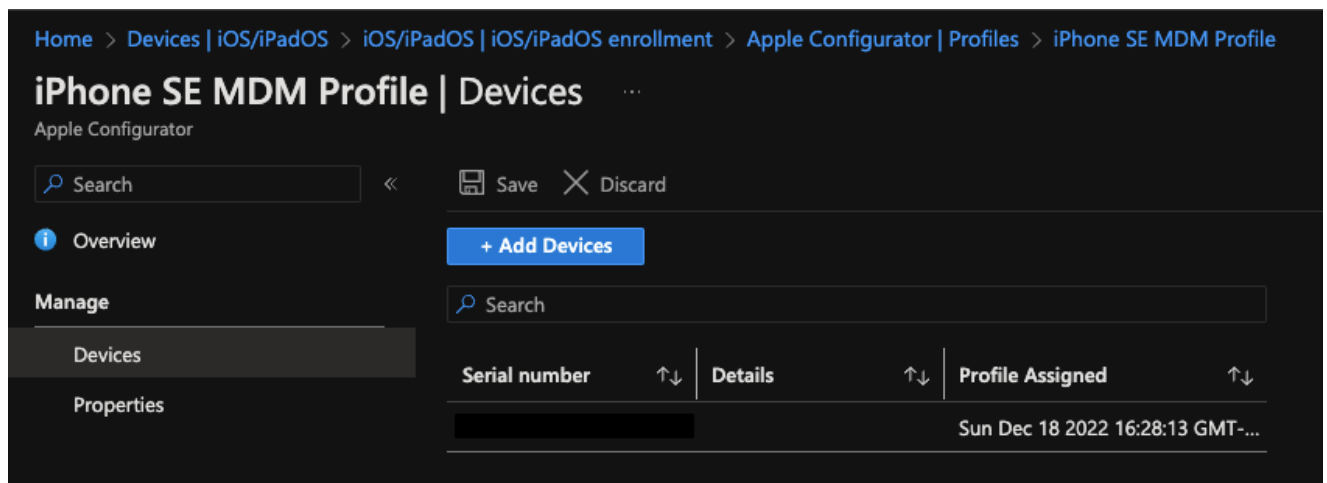
Verified ✓

Description Install this profile to get access to your company apps

Contains Mobile Device Management
Device Identity Certificate
2 Certificates

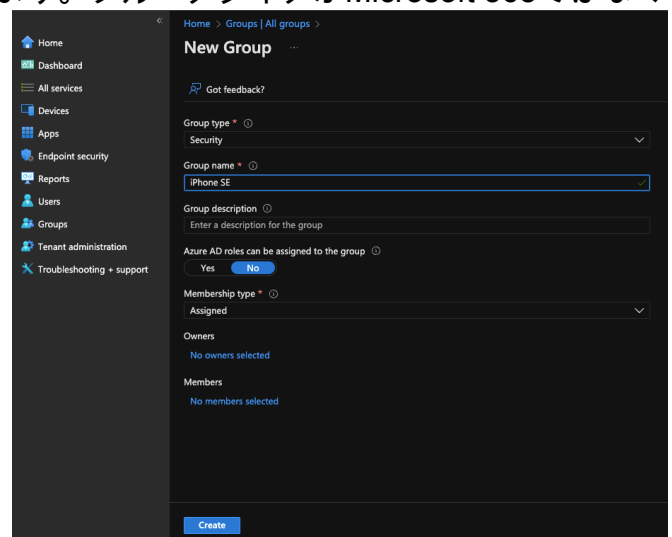
More Details





11753595983892

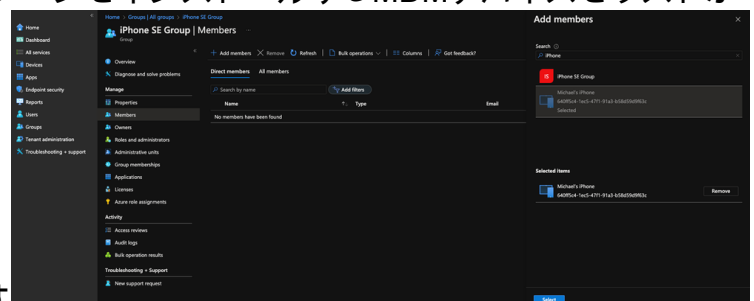
12. デバイスをMDMに登録したので、Groups → All Groups → New Groupの順に選択し、新しいグループを作成してデバイスを割り当てます。グループタイプがMicrosoft 365ではなく



「Security」であることを確認してください。

11753690347284

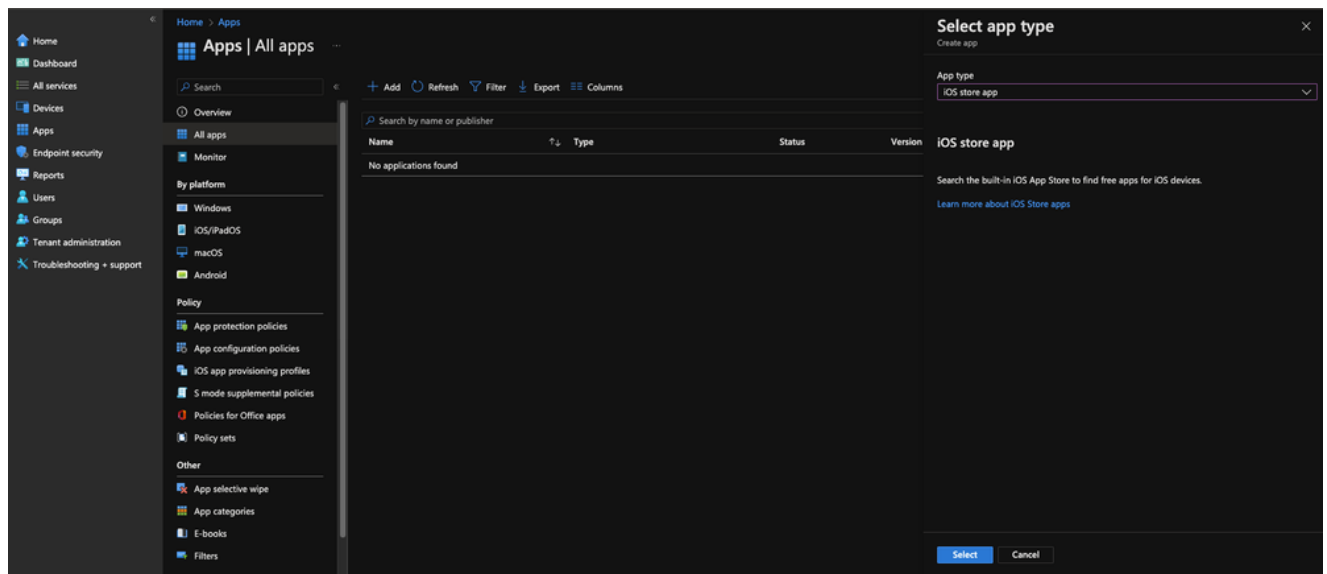
13. 作成したばかりのグループをクリックして、Members → Add Membersの順に選択します。Cisco Security ConnectorアプリケーションをインストールするMDMデバイスをリストか



ら探し、作成したグループに追加します

11753692550036

14. Apps → All apps → Addの順に選択します。アプリの種類は「iOSストアアプリ」を選択し、「選択」をクリックして確認します



11753797372436

15. 「Search for App Store」を選択し、検索バーに「Cisco Security Connector」と入力し、「Select」をクリックして「Cisco Security Connector」アプリを選択します

Home > Apps | All apps >

Add App

iOS store app

1 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 ⓘ

Previous Next

11753844054420

16. Assignmentsの下に、前の手順で作成した、MDMデバイスを含むグループを追加してから、次に進みます レビューと作成

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

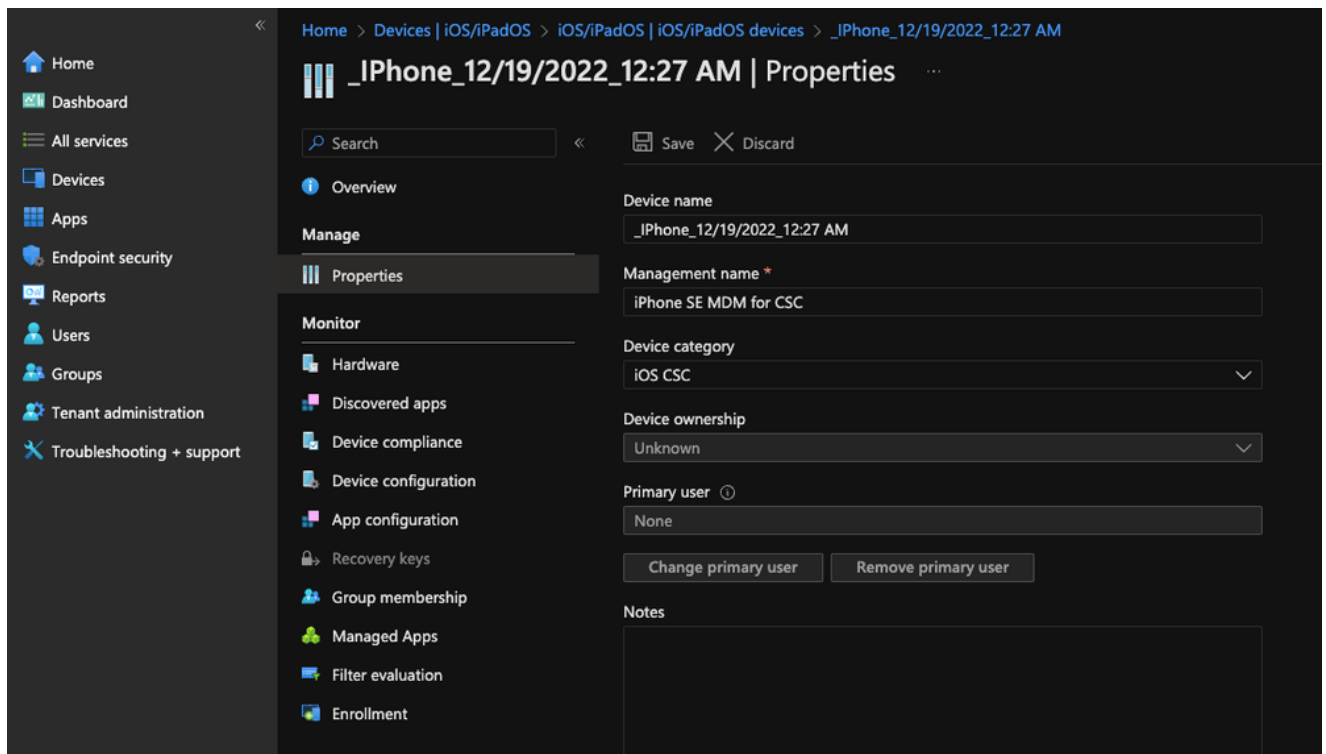
Required ⓘ

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

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

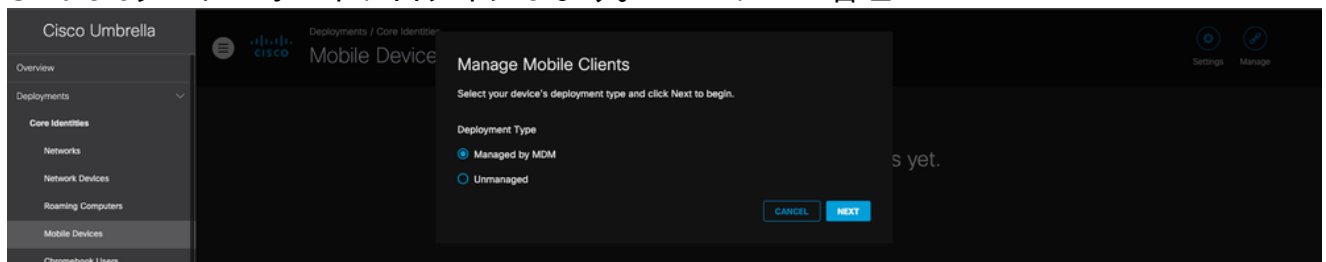
11753839516692

17. [オプションのステップ] Devices → iOS/iPadOS → iOS/iPadOS devices → Properties → Device Categoryの順に選択し、プロファイルを作成してデバイスに割り当てます



11753916236820

18. Deployments → Core Identities → Mobile Devices → 右上のManage → で、Cisco Umbrellaダッシュボードにログインします。MDMによる管理



11753923081492

19. 次に、iOS → Microsoft Intune構成のダウンロードに移動します。ユーザがCisco Security Connectorアプリケーションで「問題の報告」を選択したときに電子メールを送信する電子メールアドレスを入力します

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

Android

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 

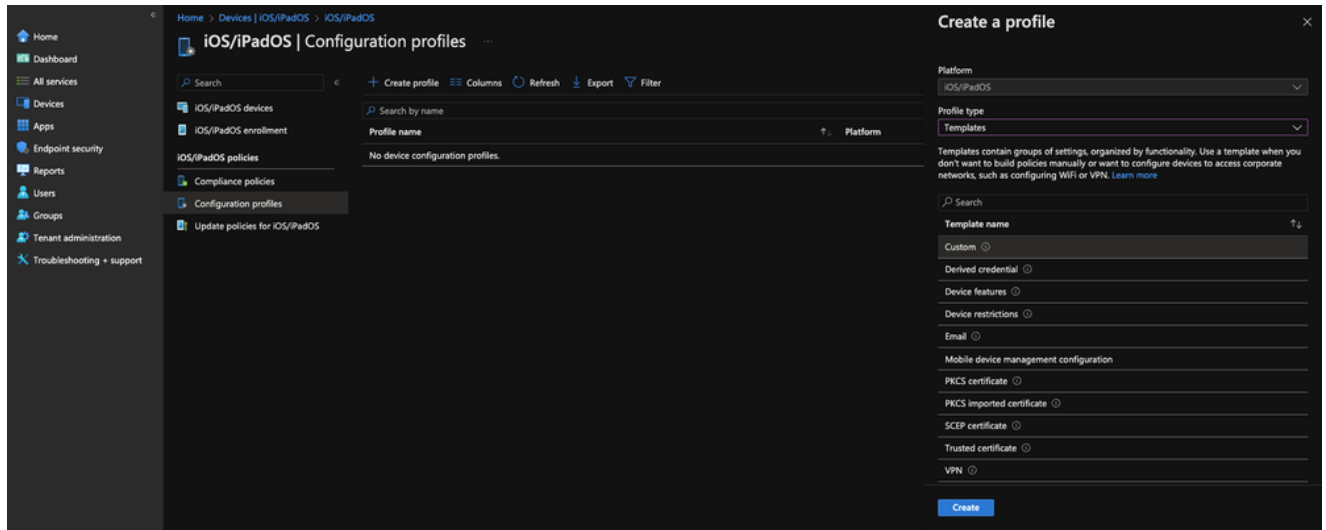
[iOS Config](#) 

BACK

DONE

11753924523540

20. Intuneポータルに戻り、Devices → iOS/iPadOS → Configuration Profiles → Create Profile → Templates → Custom



11753988354964

21. 設定プロファイルにわかりやすい名前を付けます。「ステップ2：設定」で、Cisco UmbrellaダッシュボードからダウンロードしたばかりのXMLファイルをアップロードします

11754000962196

22. Assignmentsの下で、MDMデバイスを含む、以前作成したグループを割り当て、「Review and Create」を選択します
23. iOS/iPadOSデバイスに戻り、MDMデバイスを選択して上部のsyncをクリックすると、MDM iOS/iPadOSデバイスにCisco Security Connectorアプリをインストールするためのポップアップが表示されます

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

No SIM 

4:31 AM



Status

DNS SECURITY



Not Protected by Umbrella



ENDPOINT VISIBILITY



Clarity Not Configured

No SIM



4:32 AM



< Status

Umbrella

PROTECTION STATUS

IPv4 Status

Limited

IPv6 Status

Limited

DIAGNOSTICS

Generate Diagnostics

Generate additional diagnostics for problem repo...

DETAILS

Org ID

[REDACTED]

Device ID

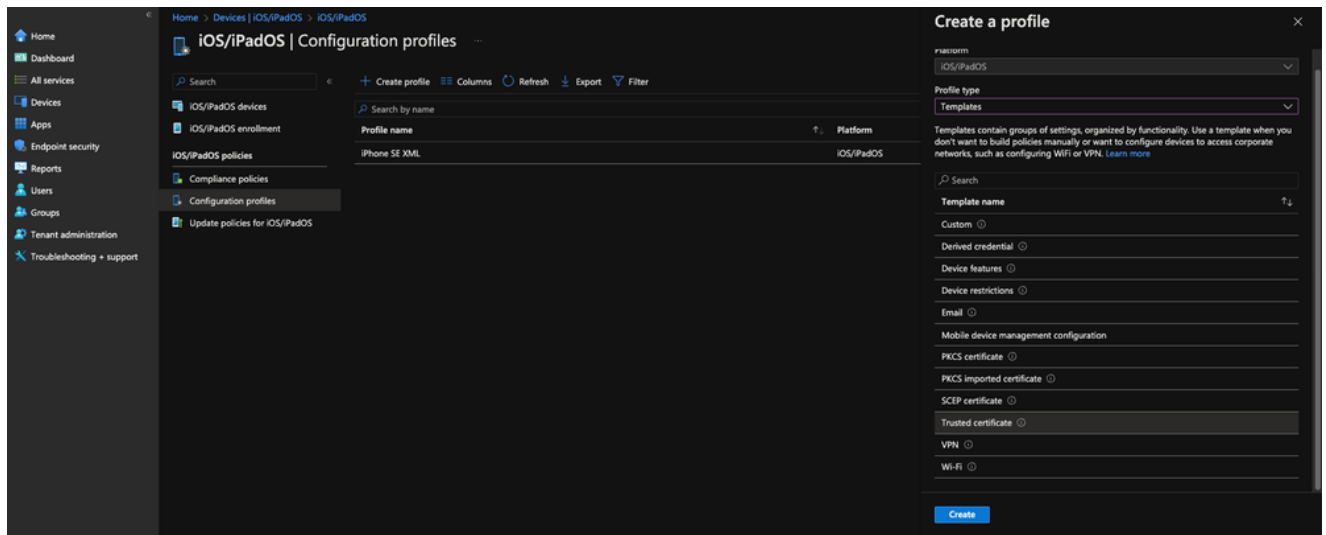
[REDACTED]

Device Label

[REDACTED]

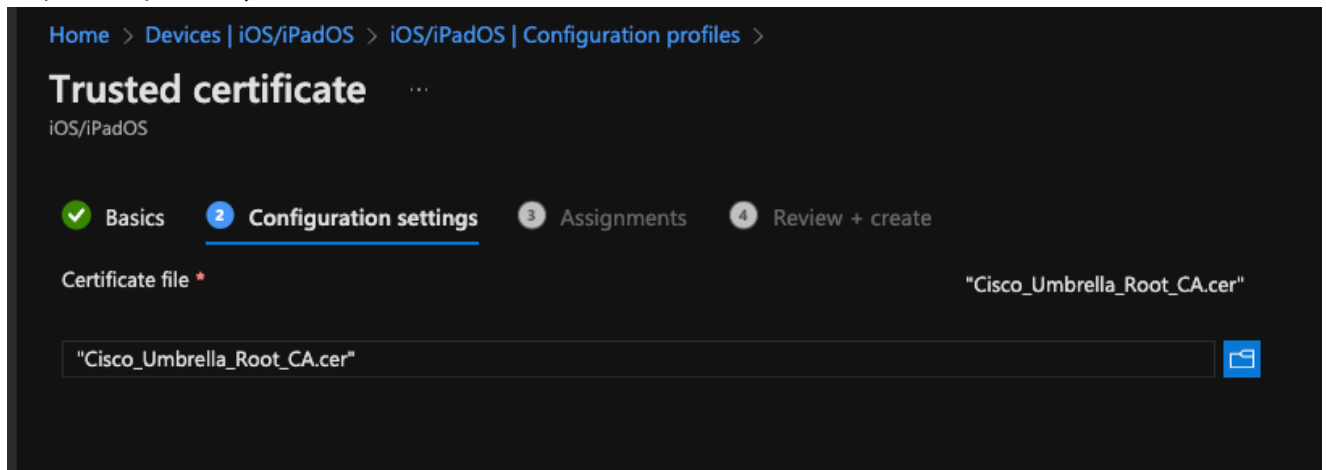
Notifications

Disabled



11754159037460

29. 「ステップ2：構成設定」で、ステップ27からダウンロードしたUmbrellaルート証明書をアップロードします



11754204605460

30. 「ステップ3 – 割り当て」で、MDM iOS/iPadOSデバイスを含むグループを選択し、「次へ」および「作成」をクリックします。
31. iOS/iPadOSデバイスに戻り、MDMデバイスを選択して、もう一度上部のsyncをクリックします (ステップ24と同様)
32. Cisco Security Connectorアプリを一度閉じてから再起動します。ステータスが「Protected by Umbrella」と表示されます。

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.

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。