

Implantar Conector de Segurança com o Intune

Contents

[Introdução](#)

[Overview](#)

[Procedimento](#)

[Limitações](#)

[Troubleshooting](#)

[Logs](#)

Introdução

Este documento descreve como implantar o Conector de Segurança usando o Intune.

Overview

Este é um guia passo a passo sobre como obter o gerenciamento MDM do dispositivo iOS/iPadOS via Intune e enviar o perfil via Apple Configurator

Você também pode consultar nossa documentação de [Registro do Intune](#) e o [guia em PDF](#) aqui

Note: este método mostra como MDM seus dispositivos via Intune e Apple Configurator

Notas Importantes:

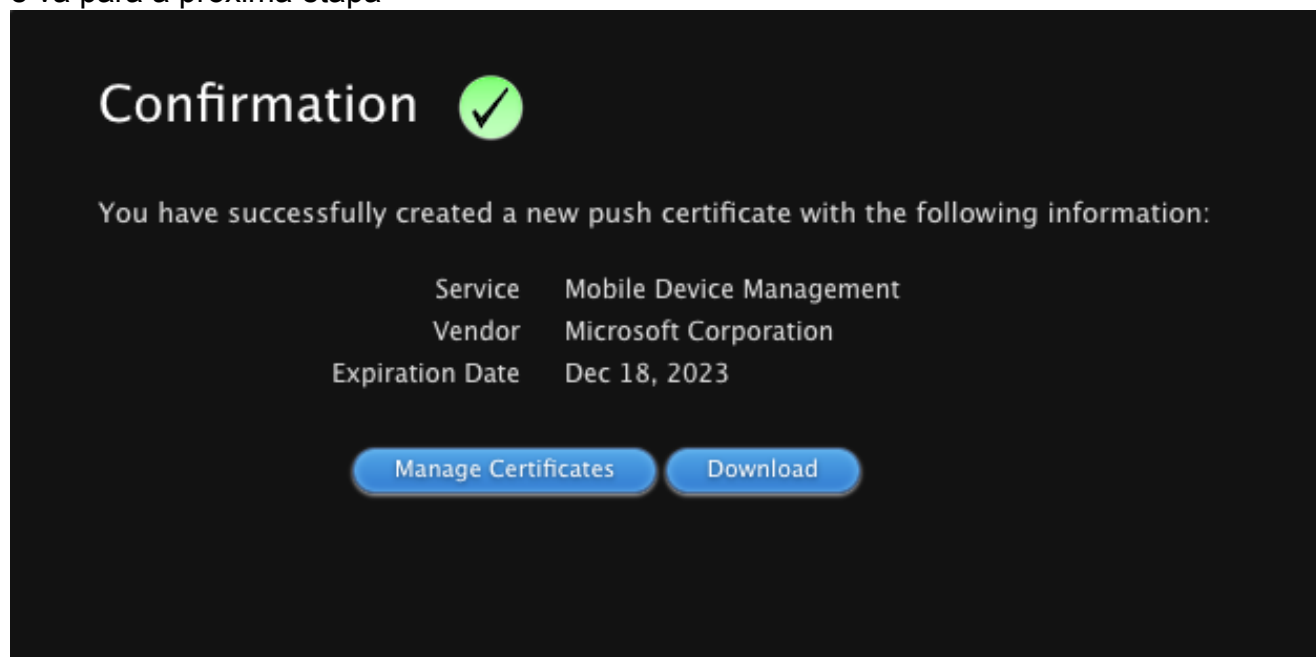
Se você estiver fazendo o MDM de seus dispositivos supervisionados por meio do aplicativo Portal da empresa, poderá começar na Etapa 14.

Este artigo é fornecido como está a partir de 12/04/2023, o suporte Umbrella não garante que essas instruções permanecerão válidas após esta data e está sujeito a alterações com base em atualizações do Microsoft Intune e Apple iOS.

Procedimento

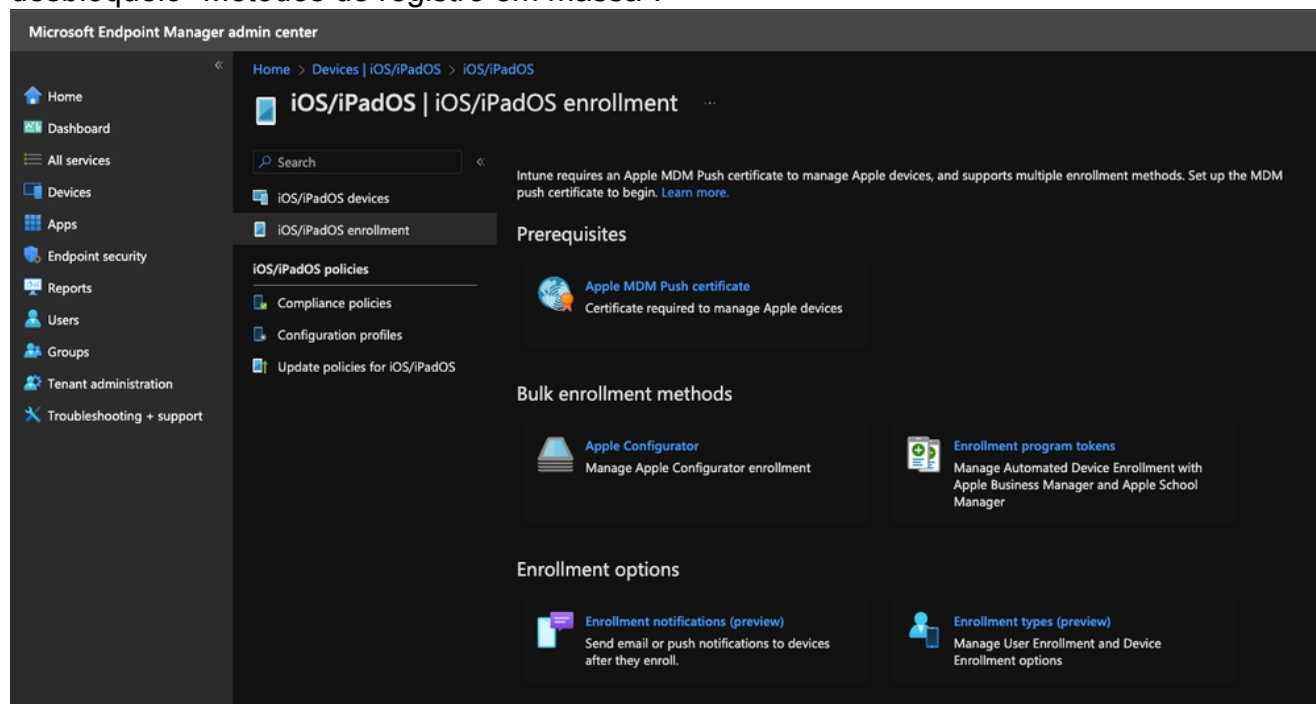
1. Faça login no Portal do Azure e procure por "Intune". Como alternativa, acesse https://intune.microsoft.com/Error/UE_404.aspxerrorpath=/ e faça login
2. Quando estiver na página inicial do Intune, vá para Dispositivos —> iOS/iPadOS —> inscrição no iOS/iPadOS —> Certificado Apple MDM Push e clique em "Baixar seu CSR" 
- 11752925317012
3. Em seguida, clique em "Create your MDM push Certificate" (Criar seu certificado MDM push), que o redireciona para <https://identity.apple.com/pushcert/>
4. No Portal de Certificados por Push da Apple, vá para "Criar um Certificado" e carregue o

arquivo IntuneCSR.csr que você acabou de baixar. Depois que o arquivo CSR tiver sido carregado com êxito, clique em "Download" para baixar o Privacy Enhanced Mail (.pem file) e vá para a próxima etapa



11752968667924

5. Insira o endereço de e-mail da sua conta Apple ID que você usou para entrar no Apple Push Certificates Portal e carregar o arquivo .pem em "Apple MDM push certificate" e pressione "Upload". Se o carregamento for bem-sucedido, você verá as outras opções para o desbloqueio "Métodos de registro em massa".



11752971407380

6. Vá para Apple Configurator —> Profiles —> Create e crie um novo perfil. Dê a ele um nome significativo e, para Afinidade do usuário, selecione "Inscrever-se sem afinidade do usuário". Depois de criar o perfil, clique no perfil recém-criado e selecione "Export Profile" (Exportar

perfil) e "Download Profile" (Baixar perfil) no lado direito

11753020728596

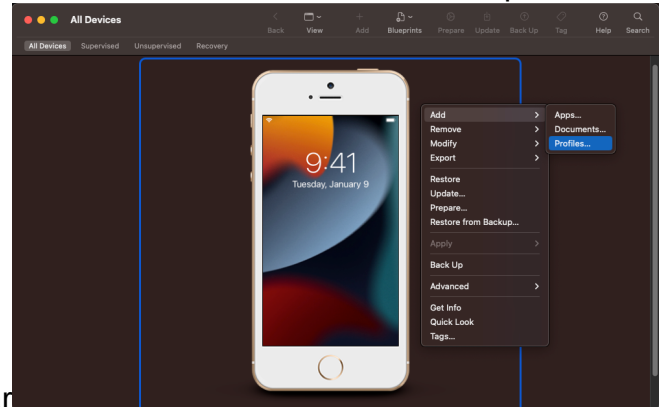
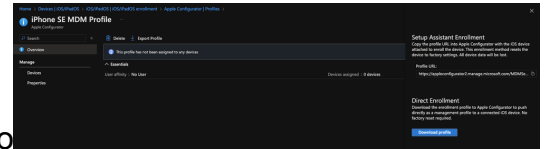
7. Faça o download e inicie o "Apple Configurator" no seu MacOS a partir da App Store e conecte o seu telefone através do Lightning Cable. Clique com o botão direito do mouse em seu dispositivo no Apple Configurator selecione Add —> Profiles e selecione o arquivo

profile.mobileconfig que você acabou de baixar

11753024446100

Alternativa do Windows: Utilitário de configuração do iPhone

8. Quando a sincronização terminar, no dispositivo iOS/iPadOS, vá para o aplicativo Configurações e vá para Geral —> VPN e Gerenciamento de Dispositivos —> Perfil de gerenciamento



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 ✓

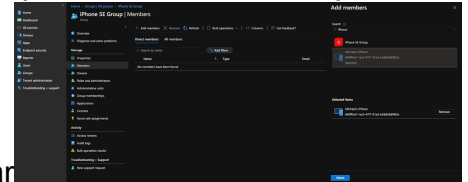
Description Install this profile to get access to your company apps

Contains Mobile Device Management
Device Identity Certificate
2 Certificates

More Details



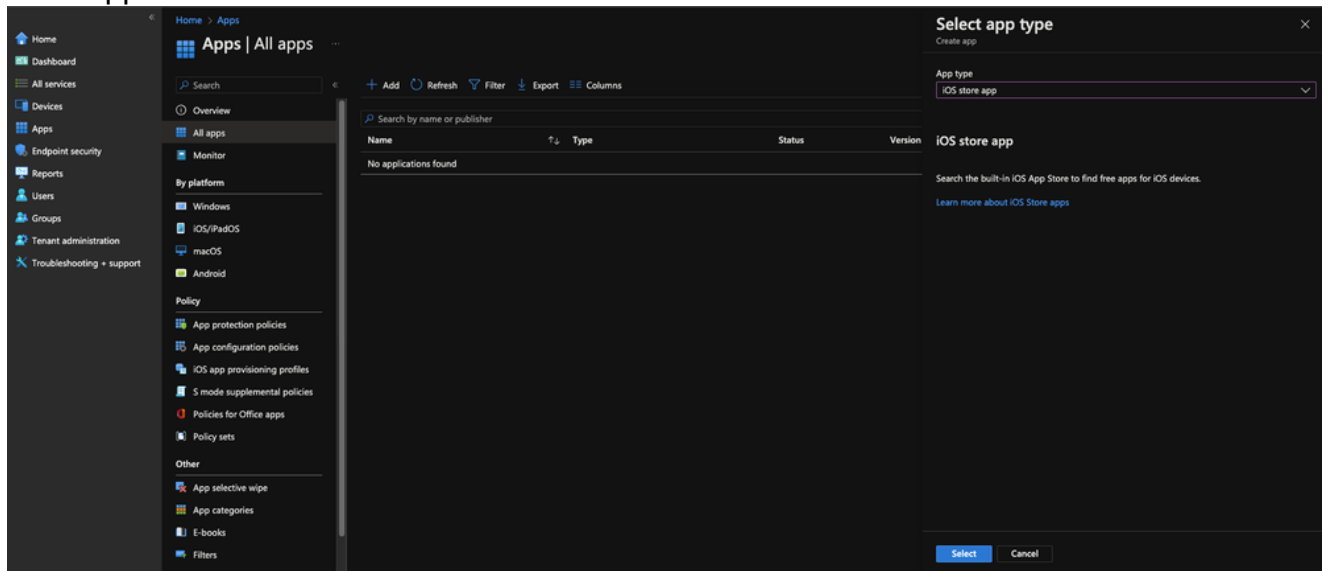
. Encontre o dispositivo MDM no qual você deseja instalar o aplicativo Cisco Security



Connector na lista e adicione-o ao grupo que acabou de criar

11753692550036

14. Vá para Apps —> All apps —> Add. Em seguida, para Tipo de aplicativo, selecione "iOS store app" e confirme clicando em "Selecionar"



11753797372436

15. Selecione "Search for App Store" e insira "Cisco Security Connector" na barra de pesquisa e selecione o aplicativo "Cisco Security Connector" clicando em "Select"

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. Em Assignments, adicione o grupo que você criou nas etapas anteriores que contêm seu dispositivo MDM, em seguida, continue com Revisar e criar

Home > Apps | All apps >

Add App

iOS store app

1 App information 2 Assignments 3 Review + create

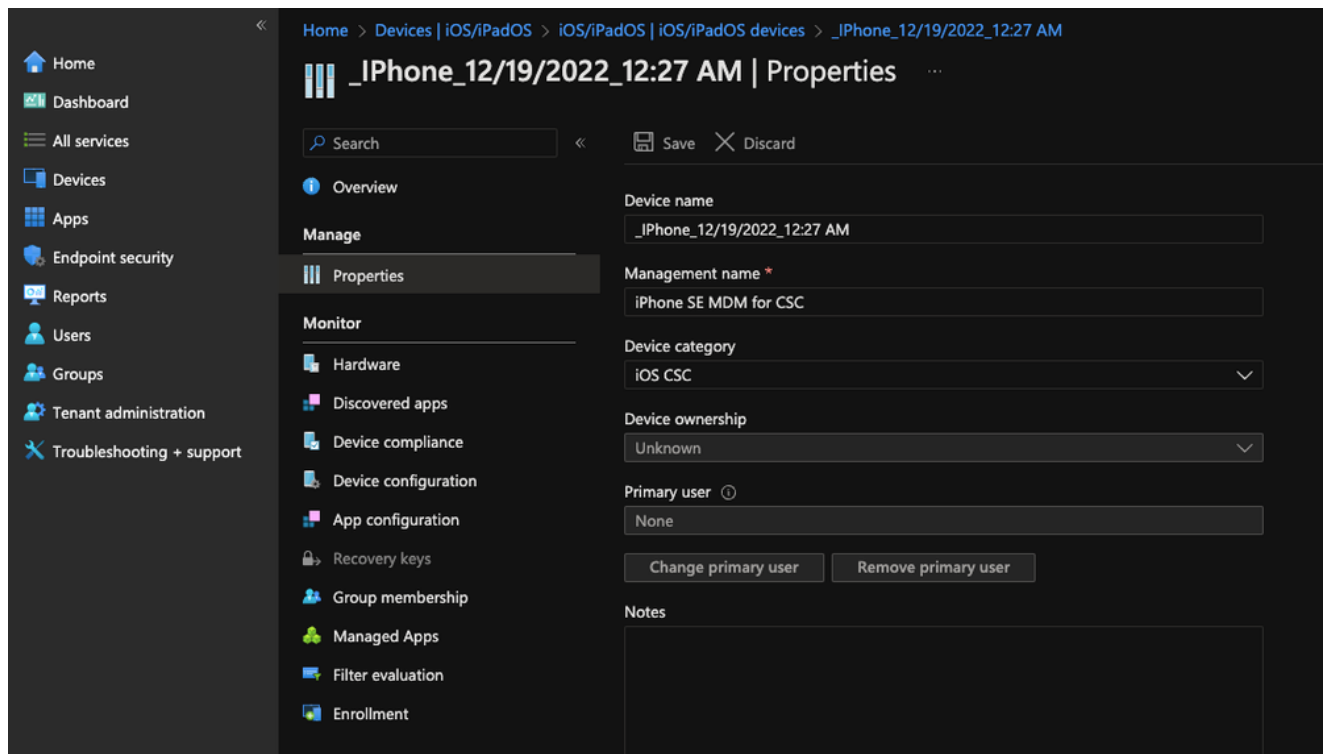
Required ⓘ

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 ⓘ

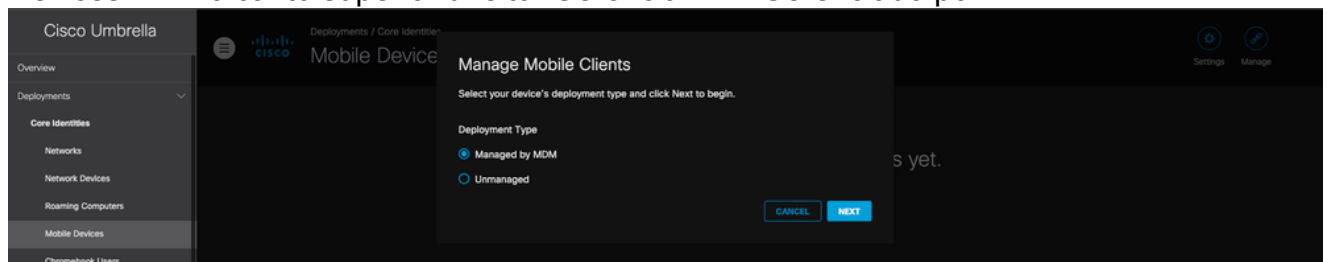
11753839516692

17. [Etapa opcional] Vá para Devices —> iOS/iPadOS —> iOS/iPadOS devices —> Properties —> Device Category, crie um perfil e atribua-o ao dispositivo



11753916236820

18. Faça login no painel do Cisco Umbrella, em Deployments —> Core Identities —> Mobile Devices —> no canto superior direito: Gerenciar —> Gerenciado por MDM



11753923081492

19. Em seguida, vá para iOS —> Download da Configuração do Microsoft Intune. Insira seu endereço de e-mail para o qual você deseja que os e-mails vão quando os usuários selecionarem "Relatar um problema" no aplicativo Cisco Security Connector

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 

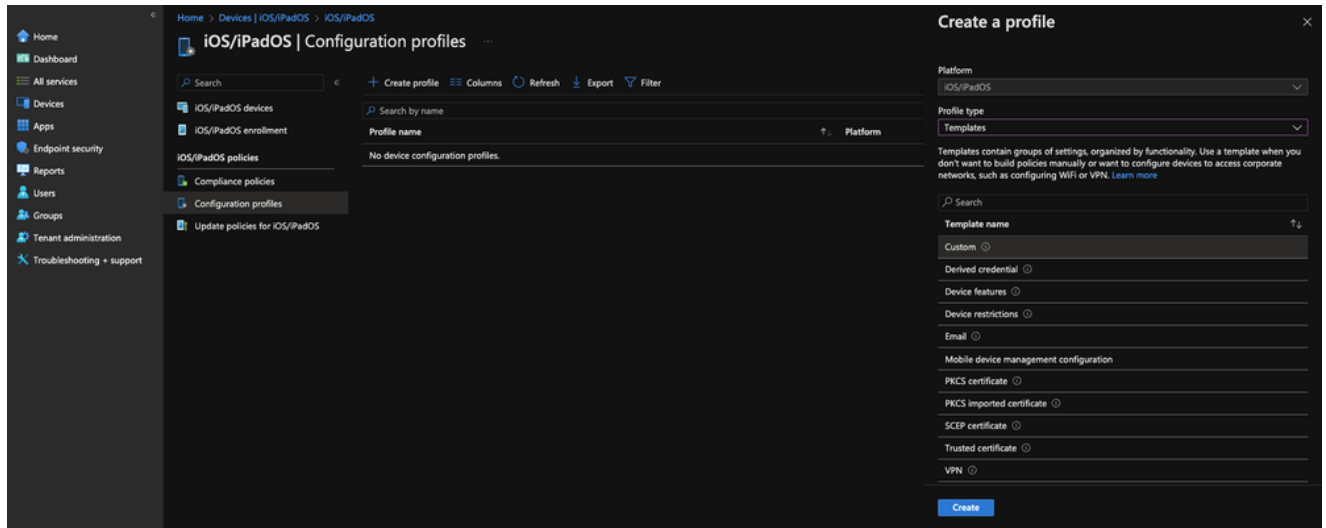
[iOS Config](#) 

BACK

DONE

11753924523540

20. Volte para o portal do Intune, em Dispositivos —> iOS/iPadOS —> Perfis de Configuração —> Criar Perfil —> Modelos —> Personalizado



11753988354964

21. Dê um nome significativo ao seu perfil de configuração. Na Etapa 2 - Definições de configuração, carregue o arquivo XML que acabou de baixar do painel do Cisco Umbrella 

11754000962196

22. Em Assignments, atribua o grupo que você criou anteriormente e que contém seu dispositivo MDM e selecione "Review and Create"
23. Volte para os dispositivos iOS/iPadOS e selecione seu dispositivo MDM, pressione sincronizar na parte superior e você obterá um pop-up em seu dispositivo MDM iOS/iPadOS para instalar o aplicativo Cisco Security Connector

No SIM



4:30 AM



VPN & Device Management

VPN

VPN

Not Connected



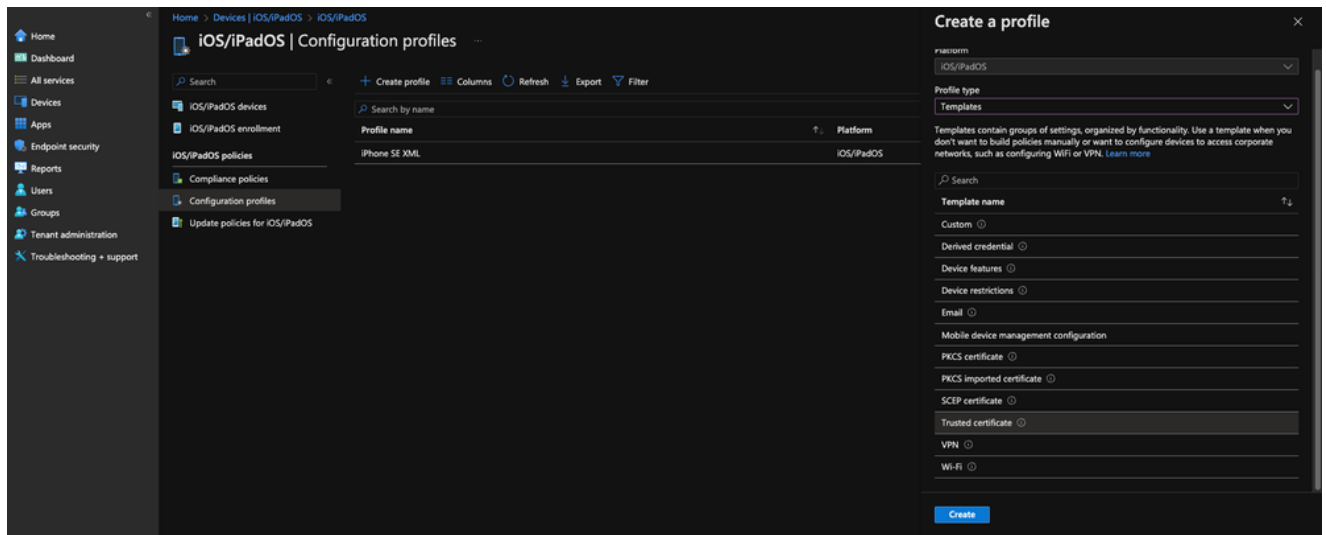
MOBILE DEVICE MANAGEMENT

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.

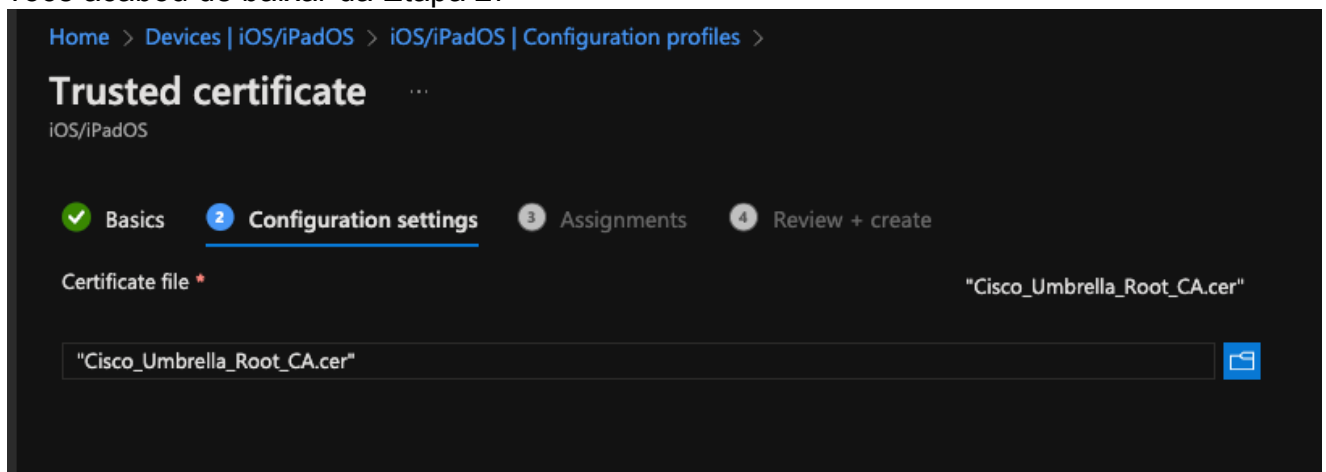
Cancel

Install



11754159037460

29. Na Etapa 2 - Definições de configuração, carregue o certificado raiz do guarda-chuva que você acabou de baixar da Etapa 27



11754204605460

30. Para a Etapa 3 - Atribuições, selecione o grupo que contém seu dispositivo MDM iOS/iPadOS e clique em "Avançar" e "Criar"
31. Volte para os dispositivos iOS/iPadOS, selecione seu dispositivo MDM e pressione sincronizar na parte superior novamente (como na etapa 24)
32. Feche e reinicie o aplicativo Cisco Security Connector novamente. Agora você vê o status como "Protegido pelo Umbrella"

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.

- Você não pode ter nenhuma configuração "Aplicativos Restritos" que restrinja o aplicativo Umbrella e/ou qualquer configuração "Mostrar ou Ocultar" para ocultar o aplicativo Umbrella aplicado ao seu perfil de configuração de dispositivo. (Em seu centro de administração do Intune > Dispositivos > iOS/iPadOS > Configuração)

Troubleshooting

- Como coletar logs de diagnóstico do Cisco Security Connector
- Erro "No Admin Email" na função "Report A Problem" do registro do CSC
- CSC: Status de "desprotegido" em redes móveis

Se você receber uma mensagem de erro: "Nome de usuário não reconhecido. Este usuário não está autorizado a usar o Microsoft Intune", vá para o Portal do Azure, em "Usuários", selecione o nome de usuário ou a conta que você está usando para configurar o Intune, vá para "Licenças" e verifique se você tem uma Licença do Intune ativa atribuída ao usuário

Home > Users > Cisco

Cisco | Licenses

User

Search

+ Assignments Reprocess Refresh Columns Got feedback?

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

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

11754557401748

Logs

Por padrão, a senha dos logs é `bypass_email_filters`. Também pode ser encontrado no `UmbrellaProblemReport.txt`

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.