

Configurar Provisionamento de Certificado Umbrella com o MS Intune

Contents

[Introdução](#)

[Overview](#)

[Pré-requisitos](#)

[Painel do Umbrella](#)

[Console do MS Intune](#)

Introdução

Este documento descreve a configuração do provisionamento de certificado Umbrella com o MS Intune.

Overview

Este guia de configuração cobre os elementos necessários para provisionar a CA raiz do guarda-chuva através do MS Intune.

Pré-requisitos

- Acesso ao painel do Umbrella
- CA raiz Umbrella
- Acesso ao Console do MS Intune

Painel do Umbrella

1. Acesse seu Umbrella Dashboard em Implantações > Configuração > Certificado Raiz e baixe a CA Raiz do Umbrella:



Settings

- Enable DOM Storage
- Enable Enhanced Protected Mode*
- Enable Integrated Windows Authentication*
- Enable native XMLHTTP support
- Enable Windows Defender SmartScreen
- Send Do Not Track requests to sites you visit in Internet E
- Use SSL 3.0
- Use TLS 1.0
- Use TLS 1.1
- Use TLS 1.2
- Warn about certificate address mismatch*
- Warn if changing between secure and not secure mode
- Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Restore advanced settings

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

Reset...

You should only use this if your browser is in an unusable state.

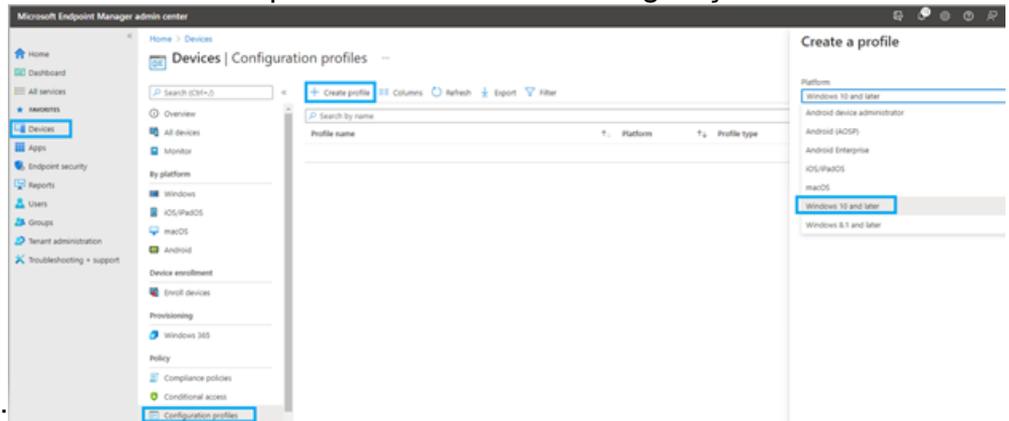
OK

Cancel

Apply

Console do MS Intune

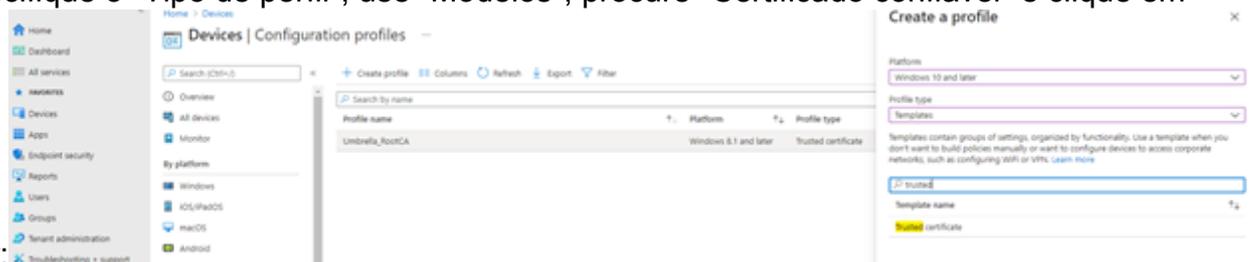
1. Acesse seu MS Intune MDM e vá em Dispositivos > Perfis de Configuração > Criar Perfil >



Selecionar Plataforma:

86b492a7fb03fb72fa2c255ed5f34309fc7427aee918937b6990a66f956dc9ac.png

2. Especifique o "Tipo de perfil", use "Modelos", procure "Certificado confiável" e clique em



Criar:

ca00d2c34ecac4f6fe2584d61b9c8a9832c458d7c083e0aabb532b8c8ebcd7aa.png

3. Insira um nome significativo para o perfil de Certificado de Confiabilidade e clique em Avançar.

Trusted certificate ...

Windows 10 and later

- 1 Basics
- 2 Configuration settings
- 3 Assignments
- 4 Applicability Rules
- 5 Review + create

Name *

Umbrella_RootCA

Description

Platform

Windows 10 and later

Profile type

Trusted certificate

Previous

Next

dfd78f03070787c9ffc4c6c968929d7a12be36429590740ed27641144cf143cf.png

4. Carregue a CA raiz do guarda-chuva, especifique o armazenamento de destino e clique em

Trusted certificate ...

Windows 10 and later

- 1 Basics
- 2 Configuration settings
- 3 Assignments
- 4 Applicability Rules
- 5 Review + create

Certificate file *

"Cisco_Umbrella_Root_CA.cer"

"Cisco_Umbrella_Root_CA.cer"

Destination store ⓘ

Computer certificate store - Root

Previous

Next

Avançar:

a318563a22a600910b206f01cdfb483ccc04cb0e15a1757c48e663cfe234ec0.png

Trusted certificate ...

Windows 10 and later

✓ Basics ✓ Configuration settings 1 Assignments 4 Applicability Rules 5 Review + create

Included groups

 Add groups  Add all users  Add all devices

Groups

All devices

Remove

Excluded groups

 When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

 Add groups

Groups

No groups selected

Previous

Next

93effe94c92c3b063c406e89c4b6d0f759cb8c5d606302e3701b702b1a8cb213.png

5. Especifique o grupo de usuários/dispositivos ao qual você deseja atribuir a CA raiz do

Trusted certificate ...

Windows 10 and later

✓ Basics ✓ Configuration settings ✓ Assignments 4 Applicability Rules 5 Review + create

Specify how to apply this profile within an assigned group. Intune will only apply the profile to devices that meet the combined criteria of these rules.

Rule Property Value

| | | |
|----------------------|----------------------|---|
| <input type="text"/> | <input type="text"/> |  |
|----------------------|----------------------|---|

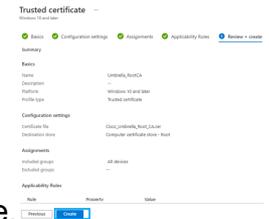
Previous

Next

guarda-chuva.

c436635d3e0dce29ec76802ffb26e604964abe08862c00ec25866dbf4a9d5b95.png

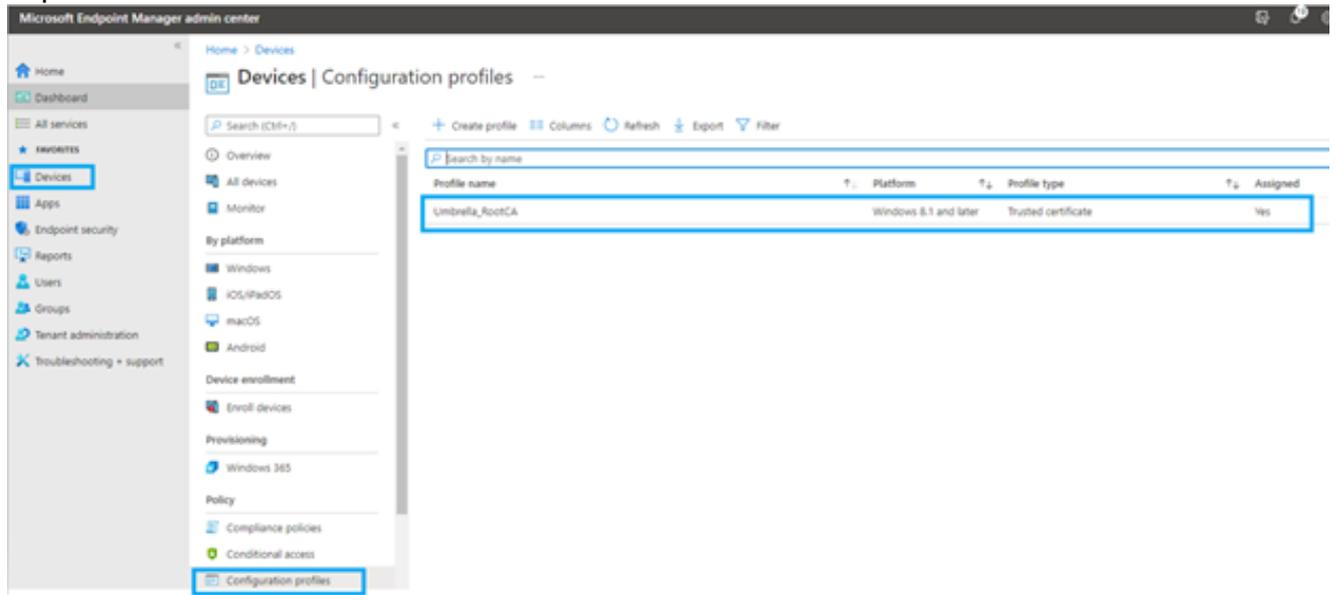
6. Opcionalmente, especifique "Regras de Aplicabilidade" e clique em Próximo.



7. Verifique se a configuração foi executada corretamente e clique em Create.

6329621f732c63ec97b6ef656b78dc1c392fe976105a0c3dbb7a779b945ba7e8.png

8. O perfil é criado.

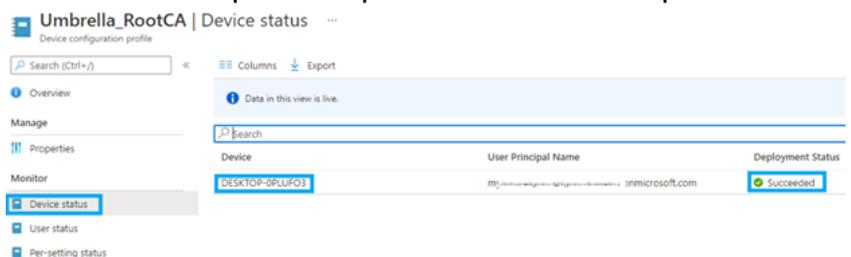


40c213cc1de22637d88e671a7074d58426573aed1f2fb7ebfda4bc338a691d84.png

9. Clique no perfil para navegar até a "página Visão geral", onde você pode verificar o status da atribuição e o número de dispositivos que têm a CA raiz do Umbrella implementada.

24b011d4b760c8245d7a4363e885857dea9881cb4ef0a683b83024e4e618ac9c.png

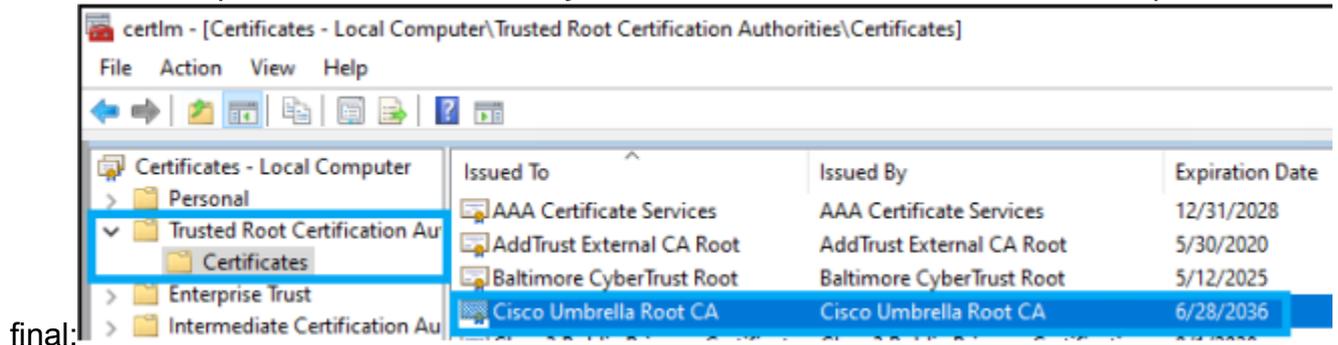
10. Você também pode clicar na seção "Status do dispositivo" para confirmar os dispositivos



que foram implantados com êxito.

cadac2eb3017c37d68f0f8aa8230508ea33777afb93250291384962555a4de2b.png

11. Você também pode confirmar a instalação no armazenamento da CA raiz do dispositivo



final:

a9e8eaebad6df501ad7627dbc87f5ea6cf9488b273925c5277fbf8a396ae1a49.png

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.