Configurar RAVPN com Autenticação SAML Usando o Azure como IdP no FTD Gerenciado pelo FDM 7.2 e Inferior

Contents

Introdução

Este documento descreve como configurar a autenticação SAML para VPN de Acesso Remoto usando o Azure como IdP no FTD gerenciado pelo FDM versão 7.2 ou anterior.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Certificados SSL
- OpenSSL
- Comandos do Linux
- Rede Virtual Privada de Acesso Remoto (RAVPN)
- Gerenciador de Dispositivos de Firewall Seguro (FDM)
- SAML (Security Assertion Markup Language, Linguagem de marcação de asserção de segurança)
- Microsoft Azure

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- OpenSSL Versão CiscoSSL 1.1.1j.7.2sp.230
- Secure Firewall Threat Defense (FTD) versão 7.2.0
- Secure Firewall Device Manager versão 7.2.0
- Autoridade de Certificação Interna (CA)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O uso da autenticação SAML para conexões RAVPN e muitos outros aplicativos tornou-se mais popular ultimamente devido às suas vantagens. O SAML é um padrão aberto para a troca de informações de autenticação e autorização entre as partes, especificamente um Provedor de Identidade (IdP) e um Provedor de Serviços (SP).

Há uma limitação no FTD gerenciado pelas versões do FDM 7.2.x ou anterior em que o único IdP suportado para autenticação SAML é Duo. Nessas versões, os certificados a serem usados para autenticação SAML devem ter a extensão Restrições Básicas: CA:TRUE ao serem carregados no FDM.

Por esse motivo, certificados fornecidos por outros IdPs (que não têm a extensão necessária) como o Microsoft Azure para autenticação SAML não têm suporte nativo nessas versões, fazendo com que a autenticação SAML falhe.

Observação: as versões do FDM 7.3.x e mais recentes permitem que a opção Ignorar Verificação da CA seja habilitada ao carregar um novo certificado. Isso resolve a limitação descrita neste documento.

Caso você configure o RAVPN com autenticação SAML usando o certificado fornecido pelo Azure e que não tenha a extensão Basic Constraints: CA:TRUE, quando você executar o comando show saml metadata <nome do ponto de confiança> para recuperar os metadados da Interface de Linha de Comando (CLI) do FTD, a saída ficará em branco como exibido a seguir:

<#root>

```
firepower#

show saml metadata
```

```
SP Metadata
-----------

IdP Metadata
-----------
```

Configurar

O plano sugerido para resolver essa limitação é atualizar o Firewall Seguro para a versão 7.3 ou superior; no entanto, se por algum motivo você precisar que o Firewall execute a versão 7.2 ou inferior, você poderá contornar essa limitação criando um certificado personalizado que inclua a extensão Basic Constraints: CA:TRUE. Quando o certificado for assinado por uma CA personalizada, você precisará alterar a configuração no portal de configuração SAML do Azure para que ele use esse certificado personalizado.

Etapa 1. Crie uma CSR (Certificate Signing Request, solicitação de assinatura de certificado) com a extensão "Basic Constraints: CA:TRUE"

Esta seção descreve como criar um CSR usando o OpenSSL para que ele inclua a Extensão Basic Constraints: CA:TRUE.

1. Faça login em um endpoint que tenha a biblioteca OpenSSL instalada.

2. (Opcional) Crie um diretório onde você possa localizar os arquivos necessários para este certificado usando o comando mkdir <nome da pasta>.

<#root>

```
root@host1:/home/admin#
```

mkdir certificate

3. Se você criou um novo diretório, altere-o e gere uma nova chave privada executando o comando openssl genrsa -out <nome_da_chave>.key 4096.

<#root>

```
root@host1:/home/admin/certificate#
```

openssl genrsa -out privatekey.key 4096

> Observação: 4096 bits representam o comprimento da chave para este exemplo de configuração. Você pode especificar uma chave mais longa, se necessário.

4. Crie um arquivo de configuração usando o comando touch <config_name>.conf.

5. Edite o arquivo com um editor de texto. Neste exemplo, o Vim é usado e o comando vim <config_name>.conf é executado. Você pode usar qualquer outro editor de texto.

<#root>

```
vim config.conf
```

6. Insira as informações a serem incluídas na CSR (Certificate Signing Request, Solicitação de assinatura de certificado). Certifique-se de adicionar a extensão basicConstraints = CA:true no arquivo como exibido a seguir:

<#root>

```
[ req ]

default_bits = 4096

default_md = sha256

prompt = no

encrypt_key = no

distinguished_name = req_distinguished_name

req_extensions = v3_req

[ req_distinguished_name ]

countryName =

stateOrProvinceName =
```

localityName =

organizationName =

organizationalUnitName =

commonName =

[v3_req]

```
basicConstraints = CA:true
```

Observação: basicConstraints = CA:true é a extensão que o certificado precisa ter para que o FTD instale com êxito o certificado.

7. Usando a chave e o arquivo de configuração criados nas etapas anteriores, você pode criar o CSR com o comando openssl req -new <nome_da_chave>.key -config <nome_da_conf>.conf -out <Nome_do_CSR>.csr:

<#root>

```
openssl req -new -key privatekey.key -config config.conf -out CSR.csr
```

8. Após esse comando, você poderá ver o arquivo <CSR_name>.csr listado na pasta, que é o arquivo CSR que deve ser enviado ao servidor CA para ser assinado.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC01laXhjbyBDaXR5
MRQwEgYDVQQHDAtNZW14Y28gQ2l0eTEOMAwGA1UECgwFQ2lzY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQDRWH+ij26HuF/Y6NvITCkD5VJa6KRssDJ8
[...]

Output Omitted

[...]
lRZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTw1Q5h23JsPkvJmRpKSilc7w
3rKfTXelewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

Observação: devido aos requisitos do Azure, é necessário assinar o CSR com uma CA que tenha SHA-256 ou SHA-1 configurado; caso contrário, o Azure IdP rejeitará o certificado quando você carregá-lo. Mais informações podem ser encontradas no seguinte link: Opções avançadas de assinatura de certificado em um token SAML

9. Envie este arquivo CSR com sua CA para obter o certificado assinado.

Etapa 2. Criar arquivo PKCS12

Depois de assinar o certificado de identidade, você precisa criar o arquivo de Padrões de Criptografia de Chave Pública (PKCS#12) com os próximos 3 arquivos:

- Certificado de identidade assinado
- Chave privada (definida nas etapas anteriores)
- Cadeia de certificados CA

Você pode copiar o certificado de identidade e a cadeia de certificados da autoridade de certificação para o mesmo dispositivo em que criou a chave privada e o arquivo CSR. Quando você tiver os 3 arquivos executados, execute o comando openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx para converter o certificado em PKCS#12.

<#root>

```
openssl pkcs12 -export -in id.cer -certfile ca_chain.cer -inkey privatekey.key -out cert.pfx
```

Depois de executar o comando, você é solicitado a inserir uma senha. Essa senha é necessária quando você instala o certificado.

Se o comando tiver sido bem-sucedido, um novo arquivo chamado "<pkcs12_name>.pfx" será criado no diretório atual. Este é seu novo certificado PKCS#12.

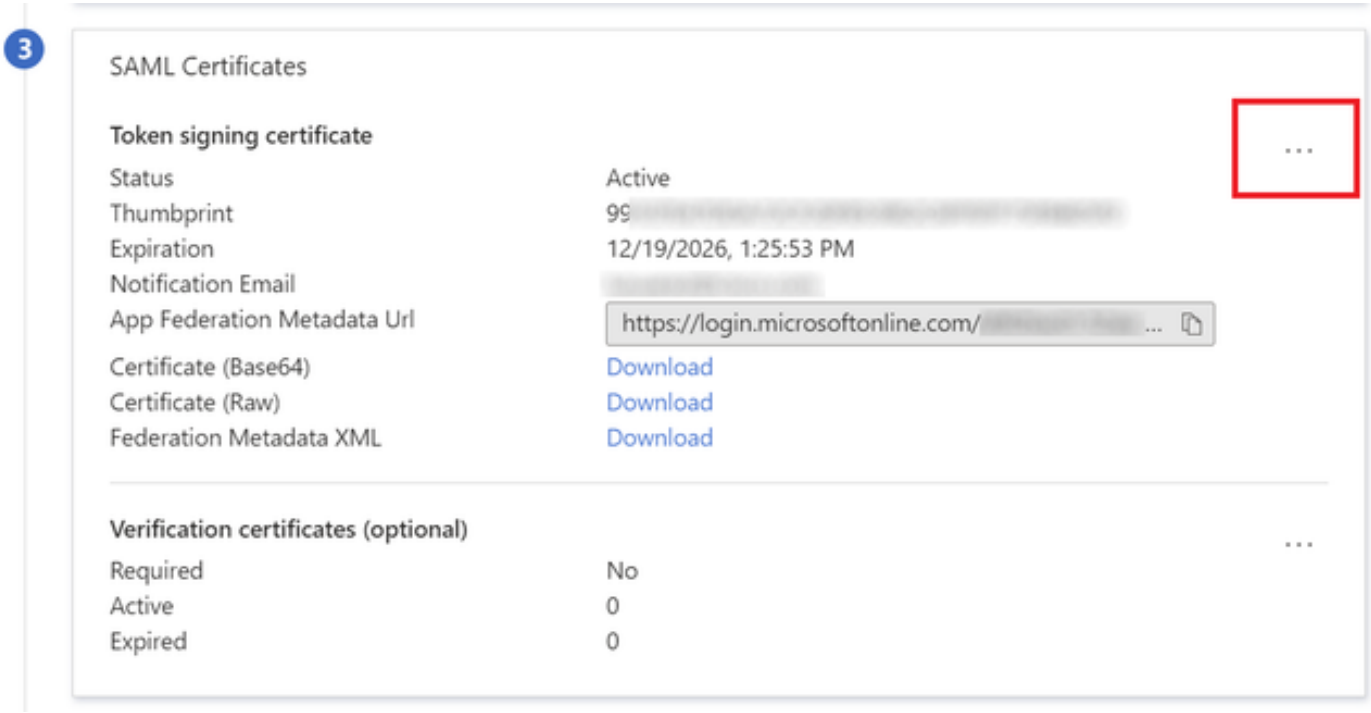
Etapa 3. Carregar o Certificado PKCS#12 para o Azure e o FDM

Quando tiver o arquivo PKCS#12, você precisará carregá-lo no Azure e no FDM.

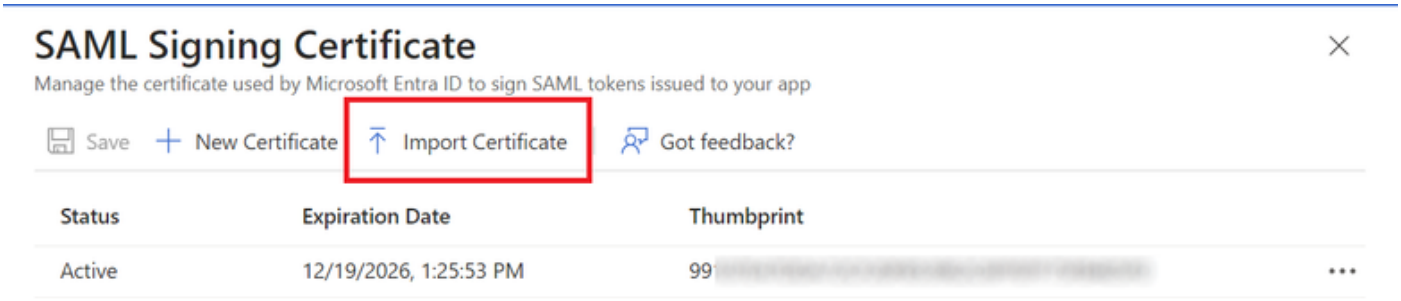
Carregar o Certificado no Azure

1. Faça logon no portal do Azure, navegue até o aplicativo empresarial que deseja proteger com a autenticação SAML e selecione Logon Único.

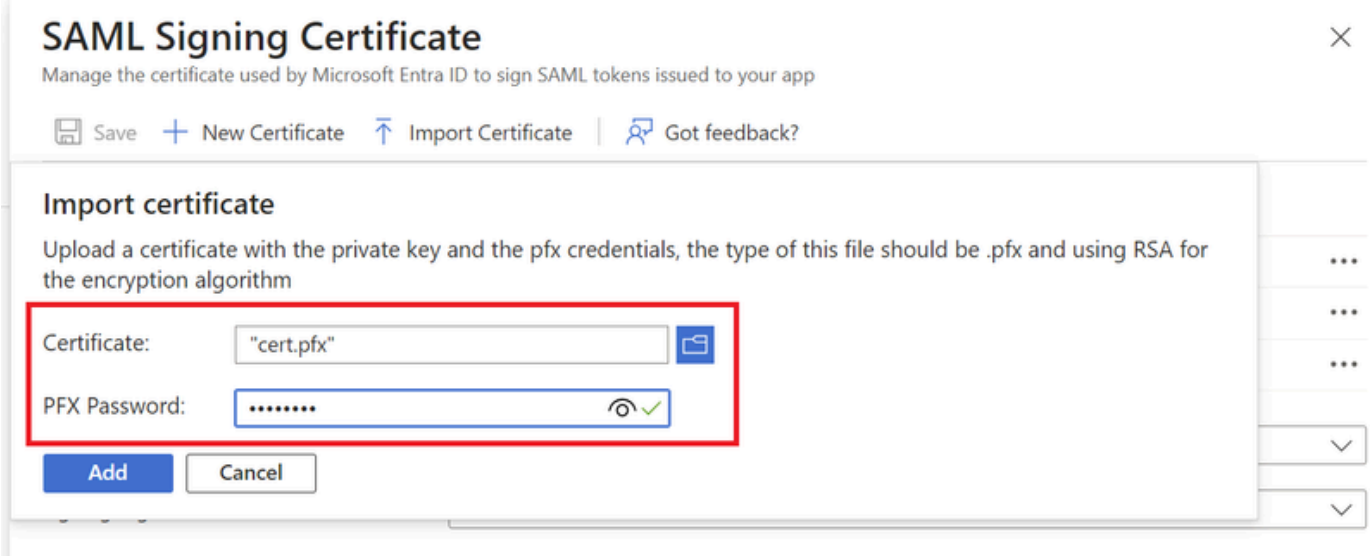
2. Role para baixo até a seção Certificados SAML" e selecione o ícone Mais Opções > Editar.



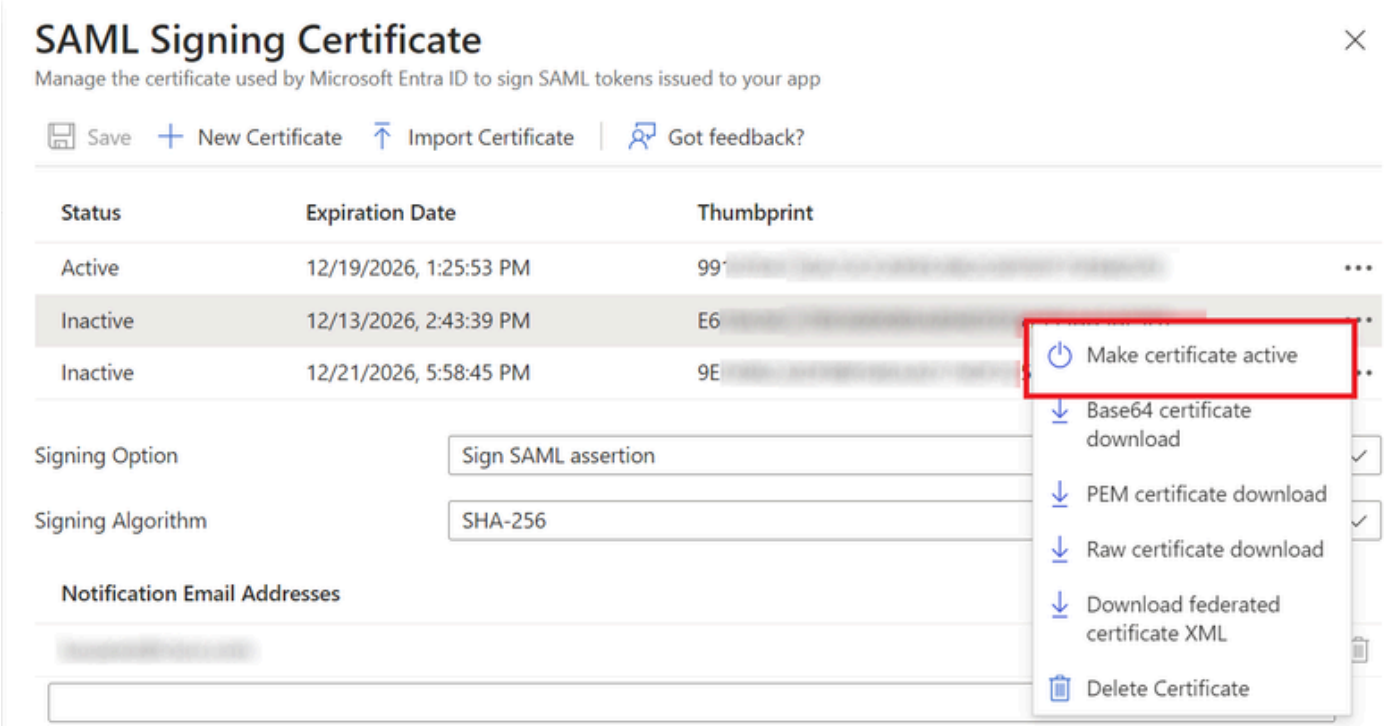
3. Agora selecione a opção Importar certificado.



4. Localize o arquivo PKCS12 criado anteriormente e use a senha que você digitou ao criar o arquivo PKCS#12.

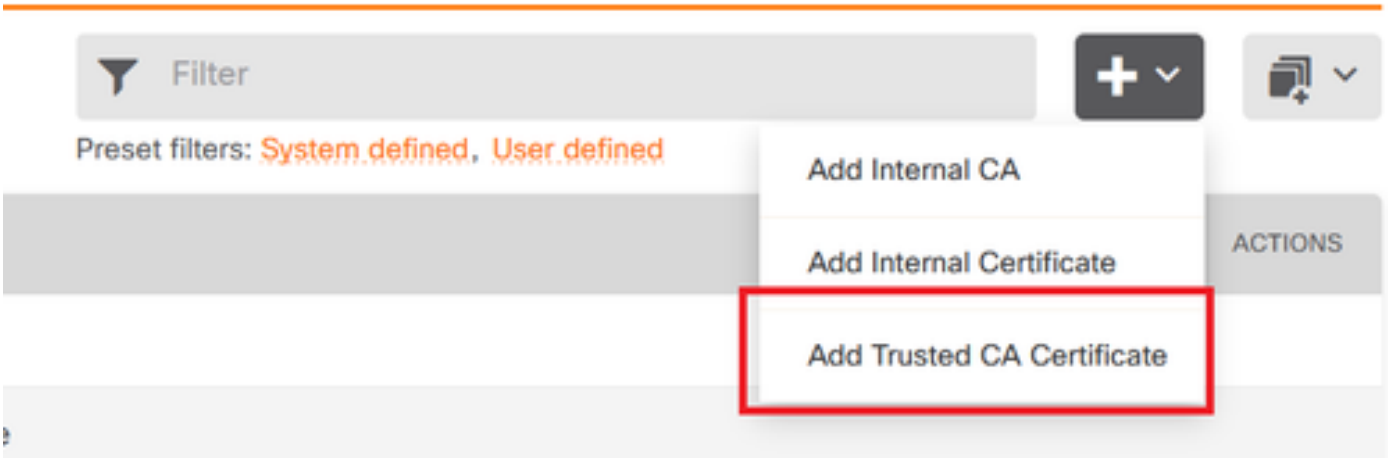


5. Finalmente, selecione a opção Tornar Certificado Ativo.

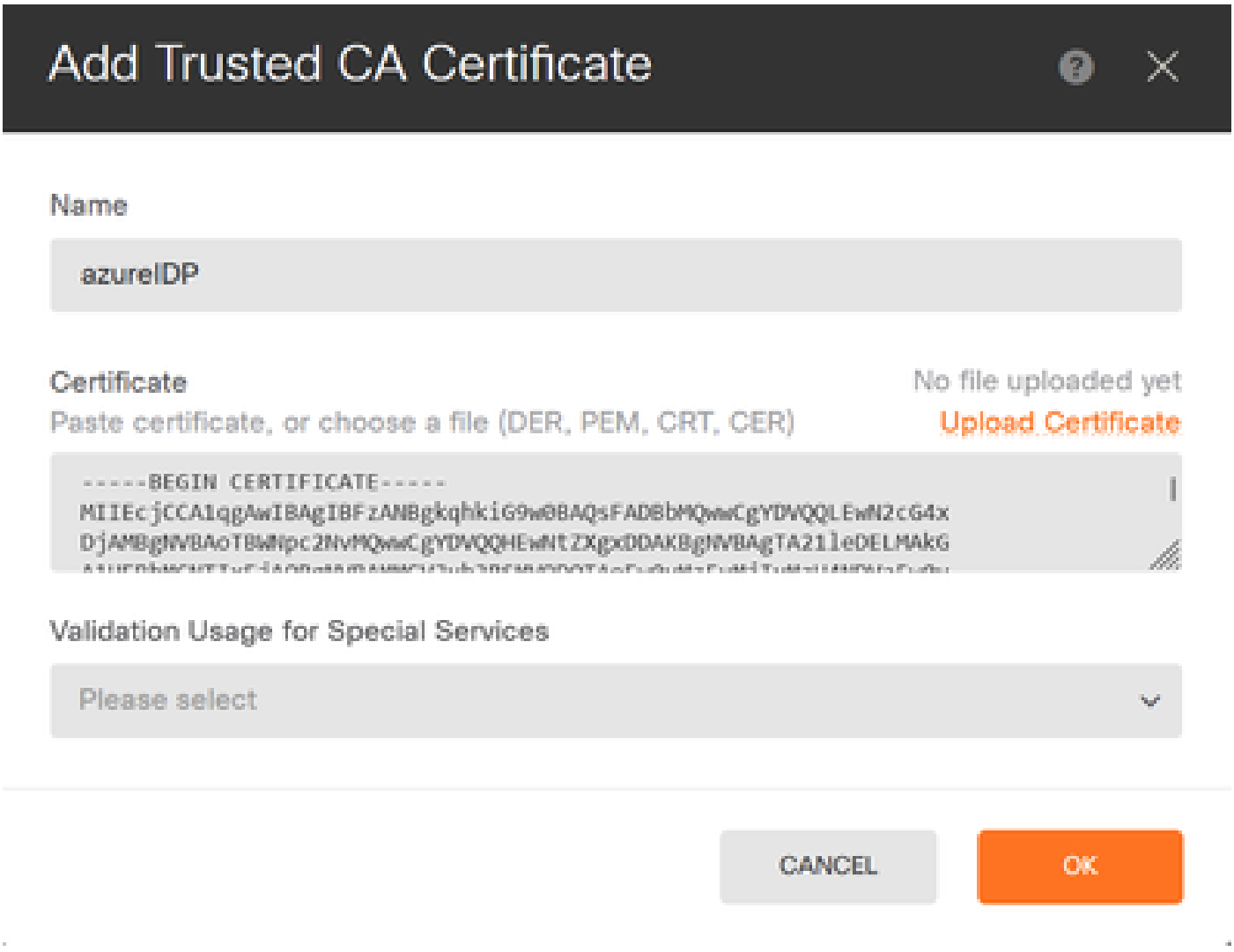


Carregar o Certificado no FDM

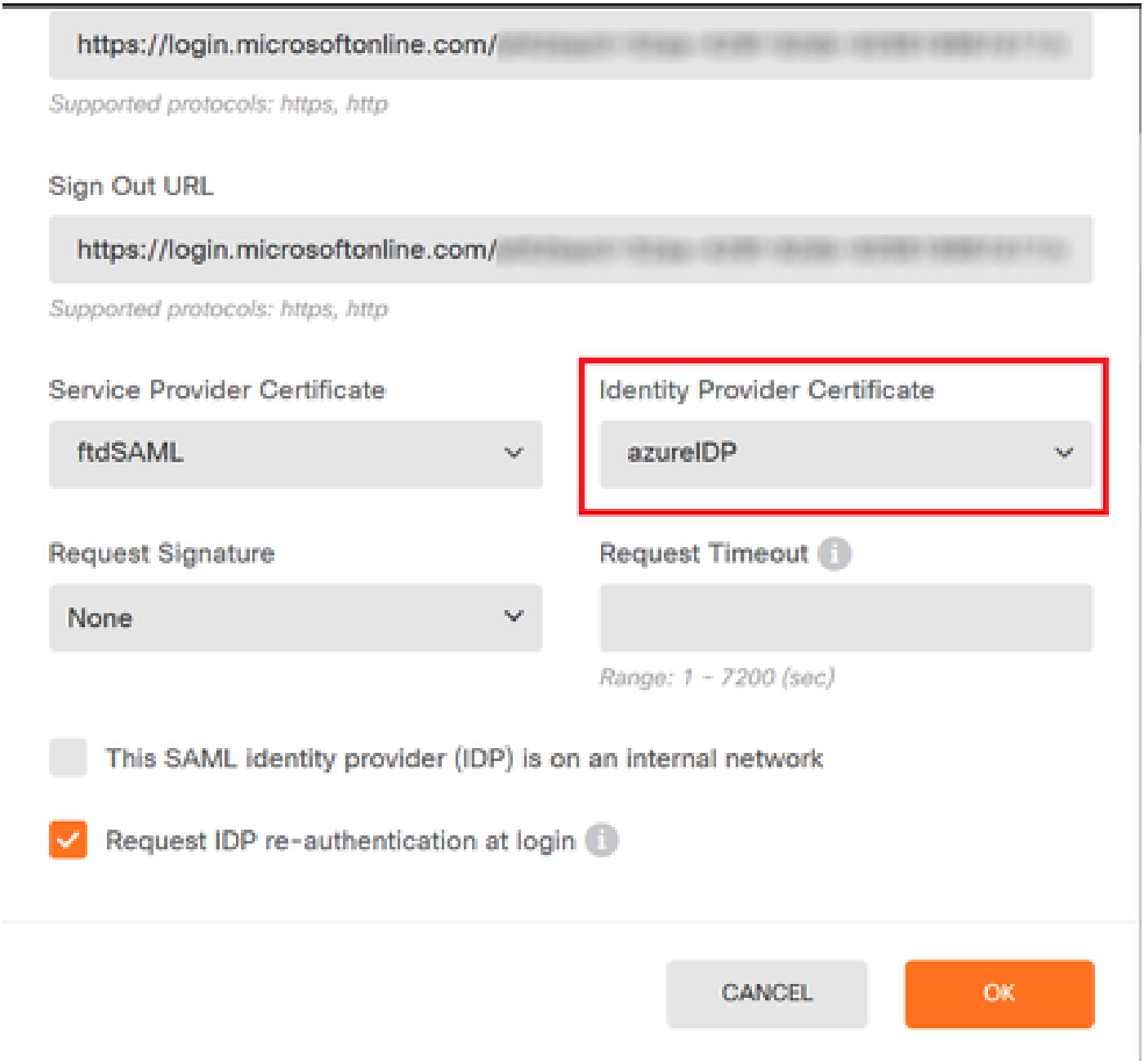
1. Navegue até Objetos > Certificados > Clique em Adicionar certificado CA confiável.



2. Digite o nome do ponto confiável que você preferir e carregue somente o certificado de Identidade do IdP (não o arquivo PKCS#12)



3. Defina o novo certificado no objeto SAML e implante as alterações.



Verificar

Execute o comando show saml metadata <nome do ponto de confiança> para garantir que os metadados estejam disponíveis na CLI do FTD:

<#root>

```
firepower#

show saml metadata azure


SP Metadata
-----------
```

xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

MIIDbzCCAlegAwIBAgIBDDANBgkqhkiG9w0BAQwFADBbMQwwCgYDVQQLEwN2cG4x

...omitted...

HGaq+/IfNKKqkhgT6q4egqMHiA==

Location="https://[...omitted...]/+CSCOE+/saml/sp/logout"/>

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://[...omitted...]/+CSCOE+/saml/sp/logout"/>

IdP Metadata
----

xmlns="urn:oasis:names:tc:SAML:2.0:metadata">

MIIEcjCCA1qgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBbMQwwCgYDVQQLEwN2cG4x

[...omitted...]

3Zmzsc5faZ8dMXO+1ofQVvMaPifcZZFoM7oBO9RK2PaMwIAV+Mw=

Location="https://login.microsoftonline.com/[...omitted...]/saml2" />

Location="https://login.microsoftonline.com/[...omitted...]/saml2" />

```
Location="https://login.microsoftonline.com/[...omitted...]/saml2" />
```

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.