

Configurar Vários Perfis RAVPN com Autenticação SAML no FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1: Crie um certificado autoassinado e um arquivo PKCS#12 usando o OpenSSL](#)

[Etapa 2: Carregue o arquivo PKCS#12 no Azure e no FDM](#)

[Etapa 2.1. Carregar o Certificado no Azure](#)

[Etapa 2.2. Carregar o Certificado no FDM](#)

[Verificar](#)

Introdução

Este documento descreve como configurar a autenticação SAML para Vários Perfis de Conexão de VPN de Acesso Remoto usando o Azure como IdP no CSF via FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Certificados SSL
- OpenSSL
- Rede Virtual Privada de Acesso Remoto (RAVPN)
- Gerenciador de dispositivos do Cisco Secure Firewall (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
- Cisco Secure Firewall (CSF) versão 7.4.1
- Cisco Secure Firewall Device Manager versão 7.4.1

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

SAML, ou Security Assertion Markup Language, é um padrão aberto para troca de informações de autenticação e autorização entre as partes, especificamente um Identity Provider (IdP) e um Service Provider (SP). O uso da autenticação SAML para conexões de VPN de Acesso Remoto (RAVPN) e vários outros aplicativos tornou-se cada vez mais popular devido às suas inúmeras vantagens. No Firepower Management Center (FMC), vários Perfis de conexão podem ser configurados para usar aplicativos protegidos por IdP diferentes devido à opção Substituir certificado do provedor de identidade disponível no menu de configuração Perfil de conexão. Este recurso permite que os administradores substituam o certificado IdP primário no objeto do Servidor de Signon Único (SSO) por um certificado IdP específico para cada perfil de conexão. No entanto, essa funcionalidade é limitada no Firepower Device Manager (FDM), pois não oferece uma opção semelhante. Se um segundo objeto SAML estiver configurado, tentar se conectar ao primeiro Perfil de Conexão resultará em uma falha de autenticação, exibindo a mensagem de erro: "Falha de autenticação devido a um problema na recuperação do cookie de logon único". Para contornar essa limitação, um certificado Autoassinado personalizado pode ser criado e importado para o Azure para uso em todos os aplicativos. Ao fazer isso, apenas um certificado precisa ser instalado no FDM, permitindo a autenticação SAML perfeita para vários aplicativos.

Configurar

Etapa 1: Crie um certificado autoassinado e um arquivo PKCS#12 usando o OpenSSL

Esta seção descreve como criar o certificado Autoassinado usando o OpenSSL

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



Observação: neste documento, uma máquina Linux é usada, portanto, alguns comandos são específicos de um ambiente Linux. No entanto, os comandos do OpenSSL são os mesmos.

b. Crie um arquivo de configuração usando o `touch`

```
.conf  
comando.
```

```
<#root>
```

```
root@host#
```

```
touch config.conf
```

c. Edite o arquivo com um editor de texto. Neste exemplo, o Vim é usado e o `vim`

.conf
comando é executado. Você pode usar qualquer outro editor de texto.

<#root>

root@host#

vim config.conf

d. Insira as informações a serem incluídas no campo Autoassinado.

Certifique-se de substituir os valores entre < > as informações de sua empresa.

```
[req]
distinguished_name = req_distinguished_name
prompt = no
```

```
[req_distinguished_name]
C =
```

ST =

L =

O =

OU =

CN =

e. O uso desse comando gera uma nova chave privada RSA de 2048 bits e um certificado autoassinado usando o algoritmo SHA-256, válido por 3650 dias, com base na configuração especificada no

`.conf`

arquivo. A chave privada é salva em

`.pem`

e o certificado Autoassinado é salvo em

`.cert`

.

<#root>

root@host#

```
openssl req -newkey rsa:2048 -nodes -keyout
```

```
.pem -x509 -sha256 -days 3650 -config
```

```
.conf -out
```

.crt

```
root@host:~# openssl req -newkey rsa:2048 -nodes -keyout Azure_key.pem -x509 -sha256 -days 3650 -config config.conf -out Azure_SSO.crt
Generating a RSA private key
.....+++++
writing new private key to 'Azure_key.pem'
-----
root@host:~#
```

f. Depois de criar a chave privada e o certificado Autoassinado, ele a exporta para um arquivo PKCS#12, que é um formato que pode incluir a chave privada e o certificado.

<#root>

root@host#

```
openssl pkcs12 -export -inkey
```

.pem -in

.crt -name

-out

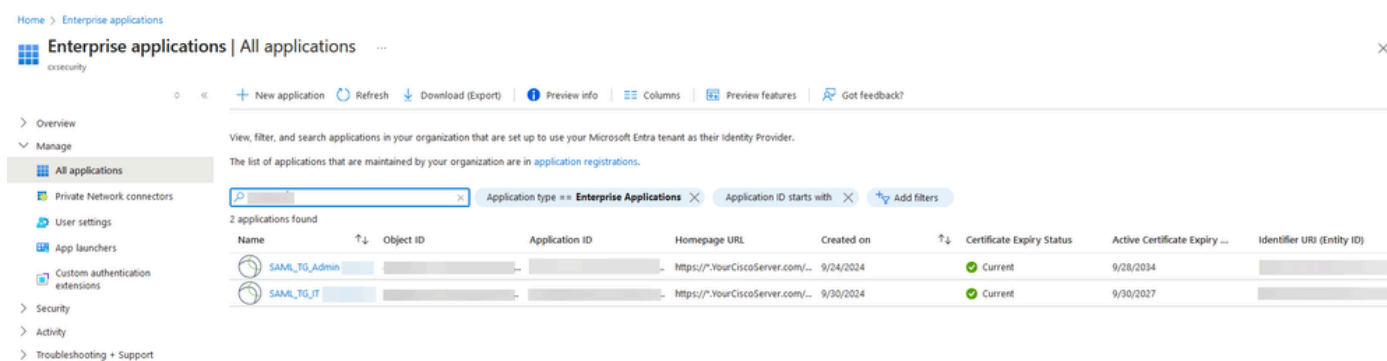
.pfx

```
root@host:~# openssl pkcs12 -export -inkey Azure_key.pem -in Azure_SSO.crt -out Azure_SSO.pfx
Enter Export Password:
Verifying - Enter Export Password:
root@host:~#
root@host:~# ls
Azure_SSO.crt Azure_SSO.pfx Azure_key.pem config.conf
```

Anote a senha.

Etapa 2: Carregue o arquivo PKCS#12 no Azure e no FDM

Certifique-se de criar um aplicativo no Azure para cada Perfil de Conexão que esteja usando a autenticação SAML no FDM.



The screenshot shows the Azure Enterprise Applications management console. The page title is "Enterprise applications | All applications". The main content area displays a list of applications with the following columns: Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiry Status, Active Certificate Expiry, and Identifier URI (Entity ID). Two applications are listed:

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry	Identifier URI (Entity ID)
SAML_TG_Admin			https://*.YourCiscoServer.com/...	9/24/2024	Current	9/28/2034	
SAML_TG_IT			https://*.YourCiscoServer.com/...	9/30/2024	Current	9/30/2027	

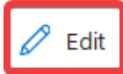
Depois que você tiver o arquivo PKCS#12 da Etapa 1: Criar um Certificado AutoAssinado e o arquivo PKCS#12 usando OpenSSL, ele deverá ser carregado para o Azure para vários aplicativos e configurado na configuração SSO do FDM.

Etapa 2.1. Carregar o Certificado no Azure

a. Faça login no portal do Azure, navegue para o aplicativo Enterprise que deseja proteger com a autenticação SAML e selecione Logon Único.

b. Role para baixo até a seção Certificados SAML e selecione Mais opções > Editar.

SAML Certificates


Token signing certificate 

Status: Active

Thumbprint: [Redacted]

Expiration: 9/28/2034, 1:05:19 PM


Notification Email: [Redacted]

App Federation Metadata Url: [https://login.microsoftonline.com/\[Redacted\]](https://login.microsoftonline.com/[Redacted]) 

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional) 

Required: No

Active: 0

Expired: 0

c. Agora, selecione a opção Importar certificado.

SAML Signing Certificate

Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

 Save  New Certificate  **Import Certificate**  Got feedback?

Status	Expiration Date	Thumbprint	
Active	8/25/2029, 7:03:32 PM	[Redacted]	...


Signing Option:

Signing Algorithm:

d. Localize o arquivo PKCS#12 criado anteriormente e use a senha digitada quando criou o arquivo PKCS#12.

Import certificate

Upload a certificate with the private key and the pfx credentials, the type of this file should be .pfx and using RSA for the encryption algorithm

Certificate: 

PFX Password: 

Add

Cancel

e. Por fim, selecione a opção Tornar Certificado Ativo.

SAML Signing Certificate



Manage the certificate used by Microsoft Entra ID to sign SAML tokens issued to your app

Save [+ New Certificate](#) [↑ Import Certificate](#) | [Got feedback?](#)

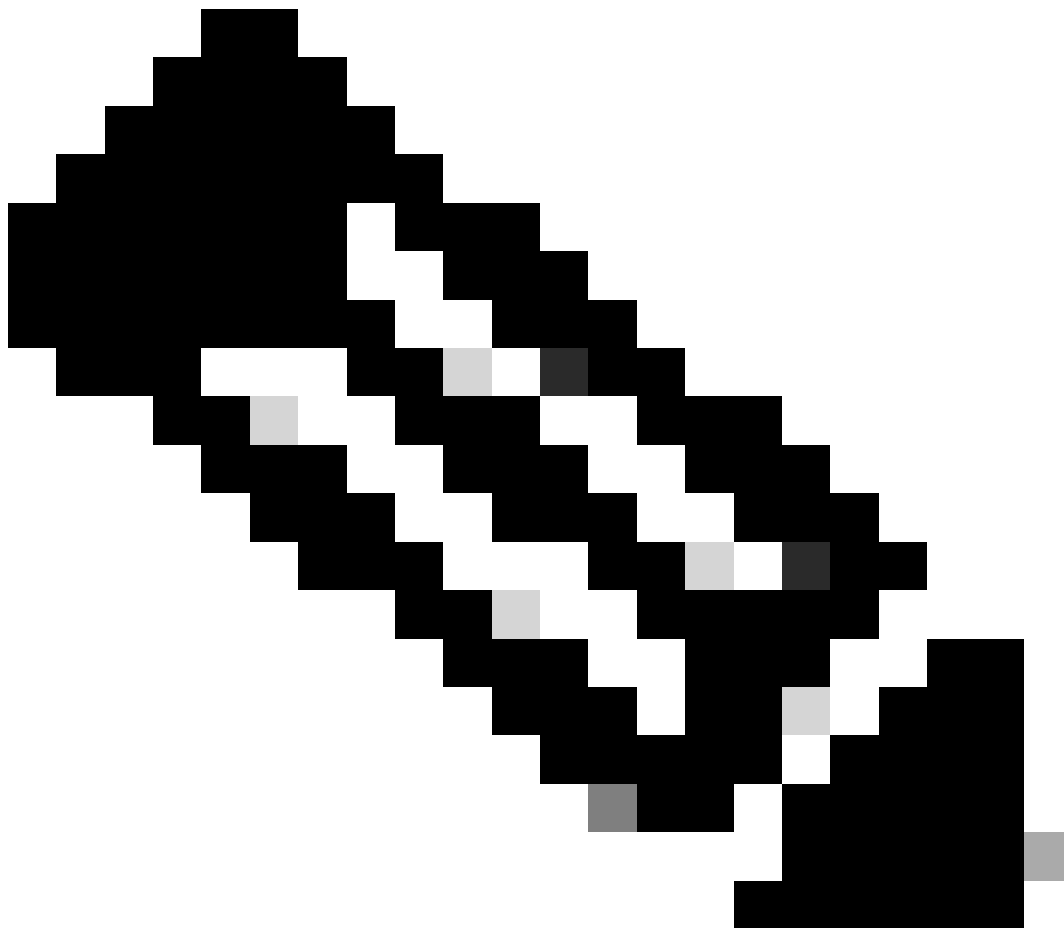
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	⋮
Active	9/27/2027, 5:51:21 PM	[Redacted]	⋮

Signing Option:

Signing Algorithm:

Notification Email Addresses:

- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate

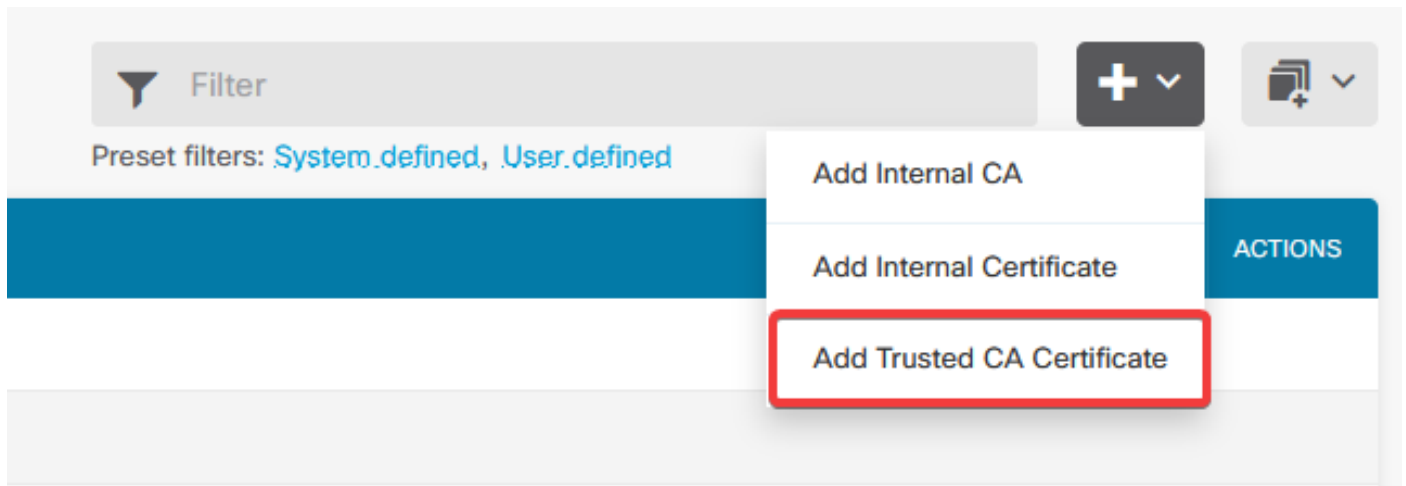


Observação: certifique-se de executar a Etapa 2.1: Carregar o Certificado para o Azure

para cada aplicativo.

Etapa 2.2. Carregar o Certificado no FDM

a. Navegue até **Objects > Certificates > Click Add Trusted CA certificate.**



b. Insira o nome do ponto de confiança que você prefere e carregue somente o certificado de identidade do IdP (não o arquivo PKCS#12) e marque a **Skip CA Certificate Check**.

Add Trusted CA Certificate



Name

Azure_SSO

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----  
MIIC8DCCAdigAwIBAgIQGDZUgz1YHI5PirWojole+zANBgkqhkiG9w0BAQsFADA0  
MTIwMAYDVQQDEy1NaWwNyb3NvZnQgQXp1cmUgRmVkdXJhdGVkIFNTTyBDZXJ0aWZp  
Y2E9ZTA0EwYwMDAEMzAwMTA0MTBzEwYwMDAEMzAwMTA0MTBzMDQyMjA0PzANBgkqhkiG9w0BAQsFAMAM
```

Skip CA Certificate Check

Validation Usage for Special Services

Please select

CANCEL

OK

c. Defina o novo certificado no objeto SAML.

Edit SAML Server



Name

AzureIDP

Description

Identity Provider (IDP) Entity ID URL

https://

Sign In URL

https://

Supported protocols: https, http

Sign Out URL

https://

Supported protocols: https, http

Service Provider Certificate

(Validation Us...

Identity Provider Certificate

Azure_SSO (Validation Usage: ...

Request Signature

None

Request Timeout

Range: 1 - 7200 (sec)

d. Defina o objeto SAML nos diferentes Perfis de Conexão que estão usando SAML como o método de autenticação e para o qual o aplicativo foi criado no Azure. Implantar as alterações

Device Summary

Remote Access VPN Connection Profiles

2 connection profiles

Filter



#	NAME	AAA	GROUP POLICY	ACTIONS
1	SAML_TG_Admin	Authentication: SAML Authorization: None Accounting: None	SAML_GP_Admin	
2	SAML_TG_IT	Authentication: SAML Authorization: None Accounting: None	SAML_GP_IT	

Primary Identity Source

Authentication Type

SAML



SAML Login Experience

VPN client embedded browser

Default OS browser

Primary Identity Source for User Authentication

AzureIDP



Verificar

Execute os comandos `show running-config webvpn` e `show running-config tunnel-group` para revisar a configuração e verificar se a mesma URL do IDP está configurada nos diferentes Perfis de Conexão.

```
<#root>
```

```
firepower#
```

```
show running-config webvpn
```

```
webvpn
```

```
enable outside
```

```
http-headers
```

```
hsts-server
```

```
enable
```

```
max-age 31536000
```

```
include-sub-domains
```

```
no preload
```

```
hsts-client
```

```
enable
```

```
x-content-type-options
```

```
x-xss-protection
```

```
content-security-policy
```

```
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.10.08029-webdeploy-k9.pkg 2
```

anyconnect profiles defaultClientProfile disk0:/anyconncprofs/defaultClientProfile.xml
anyconnect enable

saml idp https://saml.lab.local/af42bac0

/

url sign-in https://login.saml.lab.local/af42bac0

/saml2

url sign-out https://login.saml.lab.local/af42bac0

/saml2

base-url https://Server.cisco.com

trustpoint idp

Azure_SSO

```
trustpoint sp FWCertificate
```

```
no signature
```

```
force re-authentication
```

```
tunnel-group-list enable
```

```
cache
```

```
disable
```

```
error-recovery disable
```

```
firepower#
```

```
<#root>
```

```
firepower#
```

```
show running-config tunnel-group
```

```
tunnel-group SAML_TG_Admin type remote-access
```

```
tunnel-group SAML_TG_Admin general-attributes
```

```
address-pool Admin_Pool
```

```
default-group-policy SAML_GP_Admin
```

```
tunnel-group SAML_TG_Admin webvpn-attributes
```

```
authentication saml
```

```
group-alias SAML_TG_Admin enable
```

```
saml identity-provider https://saml.lab.local/af42bac0
```

/

```
tunnel-group SAML_TG_IT type remote-access
tunnel-group SAML_TG_IT general-attributes
  address-pool IT_Pool
  default-group-policy SAML_GP_IT
tunnel-group SAML_TG_IT webvpn-attributes
```

```
  authentication saml
```

```
group-alias SAML_TG_IT enable
```

```
saml identity-provider https://saml.lab.local/af42bac0
```

/

```
firepower#
```


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.