

# Configuración de varios perfiles RAVPN con autenticación SAML en FDM

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Paso 1: Crear un certificado autofirmado y un archivo PKCS#12 mediante OpenSSL](#)

[Paso 2: Cargue el archivo PKCS#12 en Azure y FDM](#)

[Paso 2.1. Cargar el certificado en Azure](#)

[Paso 2.2. Cargar el certificado en FDM](#)

[Verificación](#)

---

## Introducción

Este documento describe cómo configurar la autenticación SAML para múltiples perfiles de conexión de VPN de acceso remoto usando Azure como IdP en CSF a través de FDM.

## Prerequisites

### Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Certificados de capa de socket seguro (SSL)
- OpenSSL
- Red privada virtual de acceso remoto (RAVPN)
- Cisco Secure Firewall Device Manager (FDM)
- Lenguaje de marcado de aserción de seguridad (SAML)
- Microsoft Azure

### Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- OpenSSL
- Cisco Secure Firewall (CSF) versión 7.4.1
- Cisco Secure Firewall Device Manager versión 7.4.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

SAML, o Lenguaje de marcado de aserción de seguridad, es un estándar abierto para el intercambio de información de autenticación y autorización entre partes, específicamente un Proveedor de identidad (IdP) y un Proveedor de servicios (SP). El uso de la autenticación SAML para conexiones VPN de acceso remoto (RAVPN) y varias otras aplicaciones se ha vuelto cada vez más popular debido a sus numerosas ventajas. En Firepower Management Center (FMC), se pueden configurar varios perfiles de conexión para utilizar diferentes aplicaciones protegidas por IdP gracias a la opción Omitir certificado de proveedor de identidad disponible en el menú de configuración Perfil de conexión. Esta función permite a los administradores anular el certificado IdP principal en el objeto de servidor de inicio de sesión único (SSO) con un certificado IdP específico para cada perfil de conexión. Sin embargo, esta funcionalidad está limitada en Firepower Device Manager (FDM), ya que no proporciona una opción similar. Si se configura un segundo objeto SAML, al intentar conectarse al primer perfil de conexión se produce un error de autenticación, que muestra el mensaje de error: "Error de autenticación debido a un problema al recuperar la cookie de inicio de sesión único". Para solucionar esta limitación, se puede crear e importar un certificado autofirmado personalizado en Azure para su uso en todas las aplicaciones. De este modo, solo es necesario instalar un certificado en FDM, lo que permite una autenticación SAML perfecta para varias aplicaciones.

## Configurar

### Paso 1: Crear un certificado autofirmado y un archivo PKCS#12 mediante OpenSSL

Esta sección describe cómo crear el certificado de firma automática mediante OpenSSL

1. Inicie sesión en un terminal que tenga instalada la biblioteca OpenSSL.



Nota: En este documento, se utiliza una máquina Linux, por lo que algunos comandos son específicos de un entorno Linux. Sin embargo, los comandos de OpenSSL son los mismos.

---

b. Cree un archivo de configuración mediante el `touch`

```
.conf  
comando.
```

```
<#root>
```

```
root@host#
```

```
touch config.conf
```

c. Edite el archivo con un editor de texto. En este ejemplo, se utiliza Vim y se ejecuta el `vim`

`.conf`  
comando. Puede utilizar cualquier otro editor de texto.

`<#root>`

`root@host#`

`vim config.conf`

d. Introduzca la información que se incluirá en la autofirma.

Asegúrese de reemplazar los valores entre `< >` por la información de su organización.

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

```
[req_distinguished_name]
C =
```

ST =

L =

O =

OU =

CN =

e. El uso de este comando genera una nueva clave privada RSA de 2048 bits y un certificado autofirmado usando el algoritmo SHA-256, válido durante 3650 días, basado en la configuración especificada en el

`.conf`

archivo. La clave privada se guarda en

`.pem`

y el certificado de firma automática se guarda en

`.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. Después de crear la clave privada y el certificado de firma automática, los exporta a un archivo PKCS#12, que es un formato que puede incluir tanto la clave privada como el certificado.

<#root>

root@host#

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

.pem -in

.crt -name

-out

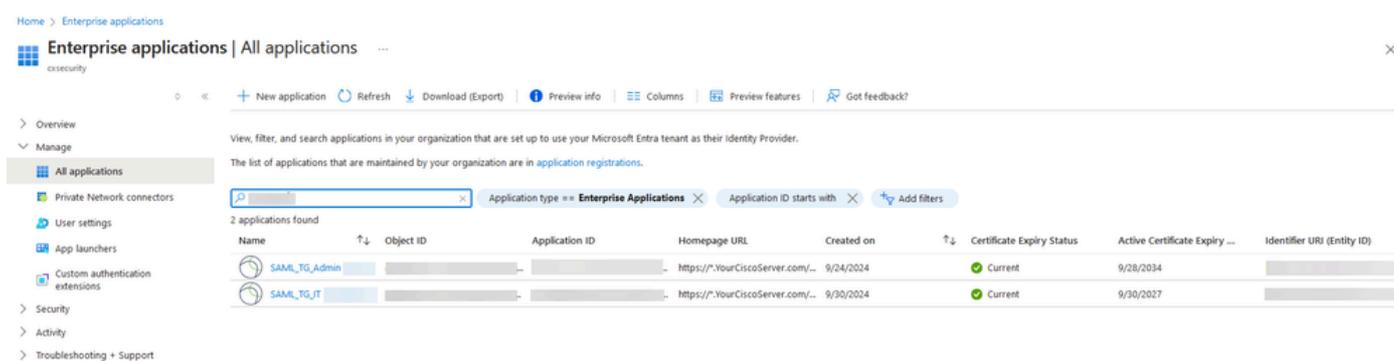
.pfx

```
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
```

Tome nota de la contraseña.

## Paso 2: Cargue el archivo PKCS#12 en Azure y FDM

Asegúrese de crear una aplicación en Azure para cada perfil de conexión que utilice la autenticación SAML en FDM.



The screenshot shows the Azure Enterprise Applications management console. The page title is "Enterprise applications | All applications". The left sidebar contains navigation options: Overview, Manage, All applications (selected), Private Network connectors, User settings, App launchers, Custom authentication extensions, Security, Activity, and Troubleshooting + Support. The main content area displays a table 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	

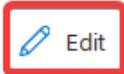
Una vez que tenga el archivo PKCS#12 del Paso 1: Crear un certificado autofirmado y un archivo PKCS#12 mediante OpenSSL, se debe cargar en Azure para varias aplicaciones y configurarse en la configuración de SSO de FDM.

### Paso 2.1. Cargar el certificado en Azure

a. Inicie sesión en el portal de Azure, navegue hasta la aplicación Enterprise que desea proteger con autenticación SAML y seleccione Single Sign-On.

b. Desplácese hacia abajo hasta la sección Certificados SAML y seleccione Más opciones > Editar.

### SAML Certificates

**Token signing certificate**  Edit

Status	Active
Thumbprint	[Redacted]
Expiration	9/28/2034, 1:05:19 PM
Notification Email	[Redacted]
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/"/> 
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

---

**Verification certificates (optional)**  Edit

Required	No
Active	0
Expired	0

c. Ahora, seleccione la opción 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. Busque el archivo PKCS#12 creado anteriormente y utilice la contraseña que introdujo al crear el archivo 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:  

e. Finalmente, seleccione la opción Make Certificate Active.

## 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



Nota: asegúrese de realizar el paso 2.1: Cargue el certificado en Azure para cada aplicación.

---

## Paso 2.2. Cargar el certificado en FDM

a. Desplácese hasta **Objects > Certificates > Click Add Trusted CA certificate.**



# 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. Establezca el objeto SAML en los diferentes perfiles de conexión que utilizan SAML como método de autenticación y para los que se creó la aplicación en Azure. Implementar los cambios

## 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



## Verificación

Ejecute los comandos `show running-config webvpn` y `show running-config tunnel-group` para revisar la configuración y verificar que la misma URL IDP esté configurada en los diferentes perfiles de conexión.

```
<#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#
```

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).