

Configuración de RAVPN con autenticación SAML mediante Azure como IdP en FTD administrado por FDM 7.2 y versiones posteriores

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Paso 1. Cree una solicitud de firma de certificado \(CSR\) con la extensión "Restricciones básicas: CA:TRUE"](#)

[Paso 2. Crear archivo PKCS12](#)

[Paso 3. Cargue el certificado PKCS#12 en Azure y FDM](#)

[Cargar el certificado en Azure](#)

[Cargar el certificado en FDM](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar la autenticación SAML para VPN de acceso remoto usando Azure como IdP en FTD administrado por FDM versión 7.2 o inferior.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Certificados de capa de socket seguro (SSL)
- OpenSSL
- Comandos de Linux
- Red privada virtual de acceso remoto (RAVPN)
- Administrador de dispositivos de firewall seguro (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 Versión CiscoSSL 1.1.1j.7.2sp.230
- Secure Firewall Threat Defence (FTD) versión 7.2.0
- Secure Firewall Device Manager versión 7.2.0
- Autoridad de certificación interna (CA)


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

El uso de autenticación SAML para conexiones RAVPN y muchas otras aplicaciones se ha vuelto más popular últimamente debido a sus ventajas. SAML 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).

Hay una limitación en FTD administrado por las versiones de FDM 7.2.x o inferiores donde el único IdP soportado para la autenticación SAML es Duo. En estas versiones, los certificados que se utilizarán para la autenticación SAML deben tener la extensión Restricciones básicas: CA:TRUE al cargarlos en FDM.

Por esta razón, los certificados proporcionados por otros IdPs (que no tienen la extensión requerida) como Microsoft Azure para la autenticación SAML no son compatibles de forma nativa en estas versiones, lo que hace que falle la autenticación SAML.

 Nota: las versiones de FDM 7.3.x y posteriores permiten que la opción Omitir comprobación de CA se active al cargar un nuevo certificado. Esto resuelve la limitación descrita en este documento.

En caso de que configure RAVPN con autenticación SAML mediante el certificado proporcionado por Azure y que no tenga la extensión Basic Constraints: CA:TRUE, cuando ejecute el comando `show saml metadata <trustpoint name>` para recuperar los metadatos de la Interfaz de línea de comandos (CLI) de FTD, el resultado se mostrará en blanco como se muestra a continuación:

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

SP Metadata

IdP Metadata

Configurar

El plan sugerido para resolver esta limitación es actualizar Secure Firewall a la versión 7.3 o superior; sin embargo, si por cualquier motivo necesita que el firewall ejecute la versión 7.2 o inferior, puede solucionar esta limitación creando un certificado personalizado que incluya la extensión Restricciones básicas: CA:TRUE. Una vez que el certificado está firmado por una CA personalizada, debe cambiar la configuración en el portal de configuración SAML de Azure para que utilice este certificado personalizado en su lugar.

Paso 1. Cree una solicitud de firma de certificado (CSR) con la extensión "Restricciones básicas: CA:TRUE"

En esta sección se describe cómo crear un CSR mediante OpenSSL para que incluya la extensión Restricciones básicas: CA:TRUE.

1. Inicie sesión en un terminal que tenga instalada la biblioteca OpenSSL.
2. (Opcional) Cree un directorio donde pueda localizar los archivos necesarios para este certificado mediante el comando `mkdir <nombre de carpeta>` .

```
<#root>
```

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


```
mkdir certificate
```

3. Si ha creado un nuevo directorio, cámbielo y genere una nueva clave privada ejecutando el comando `openssl genrsa -out <key_name>.key 4096`.

```
<#root>
```

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

```
openssl genrsa -out privatekey.key 4096
```

 Nota: 4096 bits representa la longitud de clave para este ejemplo de configuración. Si es necesario, puede especificar una clave más larga.

4. Cree un archivo de configuración mediante el comando touch <config_name>.conf.

5. Edite el archivo con un editor de texto. En este ejemplo, se utiliza Vim y se ejecuta el comando vim <config_name>.conf. Puede utilizar cualquier otro editor de texto.

```
<#root>
```

```
vim config.conf
```

6. Introduzca la información que se incluirá en la solicitud de firma de certificado (CSR).

Asegúrese de agregar la extensión basicConstraints = CA:true en el archivo como se muestra a continuación:

```
<#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
```

 Nota: basicConstraints = CA:true es la extensión que el certificado debe tener para que el FTD instale correctamente el certificado.

7. Utilizando la clave y el archivo de configuración creados en los pasos anteriores, puede crear el CSR con el comando openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr:

```
<#root>
```


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

8. Después de este comando, puede ver su archivo <CSR_name>.csr listado en la carpeta, que es el archivo CSR que debe ser enviado al servidor de la CA para ser firmado.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITCkD5VJa6KRssDJ8
[...]
```

Output Omitted

```
[...]
TRZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JSPkvJmRpKSi1c7w
3rKfTXe1ewT1IJDcmgpp6qrrwEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLgJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

 Nota: debido a los requisitos de Azure, es necesario firmar el CSR con una CA que tenga SHA-256 o SHA-1 configurado; de lo contrario, el IdP de Azure rechaza el certificado cuando lo carga. Puede encontrar más información en el siguiente enlace: [Opciones avanzadas de firma de certificados en un token SAML](#)

9. Envíe este archivo CSR con su CA para obtener el certificado firmado.

Paso 2. Crear archivo PKCS12

Una vez firmado el certificado de identidad, debe crear el archivo Public-Key Cryptography Standards (PKCS#12) con los tres archivos siguientes:

- Certificado de identidad firmado
- Clave privada (definida en los pasos anteriores)
- Cadena de certificados de CA

Puede copiar el certificado de identidad y la cadena de certificados de CA en el mismo dispositivo en el que creó la clave privada y el archivo CSR. Una vez que tenga los 3 archivos ejecute el comando `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` para convertir el certificado en PKCS#12.

<#root>

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

Después de ejecutar el comando, se le pedirá que introduzca una contraseña. Esta contraseña es necesaria al instalar el certificado.

Si el comando se ejecuta correctamente, se crea un nuevo archivo denominado "`<pkcs12_name>.pfx`" en el directorio actual. Este es su nuevo certificado PKCS#12.

Paso 3. Cargue el certificado PKCS#12 en Azure y FDM

Una vez que tenga el archivo PKCS#12, debe cargarlo en Azure y en FDM.

Cargar el certificado en Azure

1. Inicie sesión en el portal de Azure, navegue hasta la aplicación Enterprise que desea proteger con autenticación SAML y seleccione Inicio de sesión único.
2. Desplácese hasta la sección "Certificados SAML" y seleccione el icono Más opciones > Editar.

3

SAML Certificates

Token signing certificate ...

Status	Active
Thumbprint	99 [redacted]
Expiration	12/19/2026, 1:25:53 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) ...

Required	No
Active	0
Expired	0

3. 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	12/19/2026, 1:25:53 PM	99 [redacted]	...

4. Busque el archivo PKCS12 creado anteriormente y utilice la contraseña introducida al crear el archivo PKCS#12.

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?

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

5. 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	
Active	12/19/2026, 1:25:53 PM	99:.....	...
Inactive	12/13/2026, 2:43:39 PM	E6:.....	...
Inactive	12/21/2026, 5:58:45 PM	9E:.....	...

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

Cargar el certificado en FDM

1. Navegue hasta Objetos > Certificados > Haga clic en Agregar certificado de CA de confianza.

https://login.microsoftonline.com/

Supported protocols: https, http

Sign Out URL

https://login.microsoftonline.com/

Supported protocols: https, http

Service Provider Certificate

ftdSAML

Identity Provider Certificate

azureIDP

Request Signature

None

Request Timeout ⓘ

Range: 1 - 7200 (sec)

This SAML identity provider (IDP) is on an internal network

Request IDP re-authentication at login ⓘ

CANCEL

OK

Verificación

Ejecute el comando `show saml metadata <trustpoint name>` para asegurarse de que los metadatos estén disponibles desde la CLI de 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">

MIIDbzCCA1egAwIBAgIBDDANBgkqhkiG9w0BAQwFADBbMQwwCgYDVQQLEwN2cG4x

...omitted...

HGa+/IfNKKqkhgT6q4egqMHiA==

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

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

IdP Metadata

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

MIIEcjCCA1qgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBbMQwwCgYDVQQLEwN2cG4x

[...omitted...]

3Zmzsc5faZ8dMX0+1ofQVvMaPifcZZFoM7oB09RK2PaMwIAV+Mw=

Location="https://login.microsoftonline.com/[...omitted...]/sam12" />

Location="https://login.microsoftonline.com/[...omitted...]/sam12" />

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


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).