

在FDM 7.2及更低版本管理的FTD上使用Azure作为IdP配置SAML身份验证的RAVPN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[步骤1:创建扩展名为“Basic Constraints: CA:TRUE”的证书签名请求\(CSR\)](#)

[第二步：创建PKCS12文件](#)

[第三步：将PKCS#12证书上传到Azure和FDM](#)

[将证书上传到Azure](#)

[将证书上传到FDM](#)

[验证](#)

简介

本文档介绍如何在FDM 7.2版或更低版本管理的FTD上使用Azure作为IdP为远程访问VPN配置SAML身份验证。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 安全套接字层(SSL)证书
- OpenSSL
- Linux命令
- 远程访问虚拟专用网络(RAVPN)
- 安全防火墙设备管理器(FDM)
- 安全断言标记语言(SAML)
- Microsoft Azure

使用的组件

本文档中的信息基于以下软件版本：

- OpenSSL版本CiscoSSL 1.1.1j.7.2sp.230
- 安全防火墙威胁防御(FTD)版本7.2.0

- 安全防火墙设备管理器7.2.0版
- 内部证书颁发机构(CA)


本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SAML身份验证用于RAVPN连接和其他许多应用近来因其优势而越来越流行。SAML是在各方之间交换身份验证和授权信息的开放标准，特别是身份提供程序(IdP)和服务提供程序(SP)。

在FDM版本7.2.x或更低版本管理的FTD中有一个限制，其中唯一支持SAML身份验证的IdP是Duo。在这些版本中，将用于SAML身份验证的证书上传到FDM时，必须具有基本约束：CA:TRUE扩展名。

因此，由其他IdP（没有所需扩展名）提供的证书（例如Microsoft Azure for SAML身份验证）在这些版本中本机不受支持，导致SAML身份验证失败。

 **注意：** FDM版本7.3.x和更高版本允许在上传新证书时启用“跳过CA检查”选项。这解决了本文中介绍的限制。

如果使用Azure提供的证书配置RAVPN的SAML身份验证，并且该证书没有基本限制：CA:TRUE扩展，则当您运行`show saml metadata <trustpoint name>`命令从FTD命令行界面(CLI)检索元数据时，输出为空，如下所示：

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

```
IdP Metadata
```

```
-----
```

配置

解决此限制的建议计划是将安全防火墙升级到7.3版或更高版本，但是，如果出于任何原因需要防火墙运行7.2版或更低版本，您可以通过创建包含Basic Constraints: CA:TRUE扩展的自定义证书来解决此限制。证书由自定义CA签名后，您需要在Azure SAML配置门户中更改配置，使其改用此自定

义证书。

步骤1:创建扩展名为“Basic Constraints: CA:TRUE”的证书签名请求(CSR)

本节介绍如何使用OpenSSL创建CSR，使其包含基本限制：CA:TRUE扩展。

1.登录已安装OpenSSL库的终端。

2. (可选) 使用mkdir <folder name> 命令创建一个目录，您可以在其中找到此证书所需的文件。

```
<#root>
```

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

```
mkdir certificate
```

3.如果创建了新目录，请更改该目录并生成运行openssl genrsa -out <key_name>.key 4096命令的新私钥。

```
<#root>
```

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

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



注意:4096位代表此配置示例的密钥长度。如果需要，可以指定更长的密钥。

4.使用touch <config_name>.conf命令创建配置文件。

5.使用文本编辑器编辑文件。在本示例中，使用Vim并运行vim <config_name>.conf命令。您可以使用任何其他文本编辑器。

```
<#root>
```

```
vim config.conf
```

6.输入要包括在证书签名请求(CSR)中的信息。确保在文件中添加basicConstraints = CA:true扩展名，如下所示：

```
<#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
```



注:basicConstraints = CA:true是证书需要具有的扩展名，FTD才能成功安装证书。

7.使用在以上步骤中创建的密钥和配置文件，您可以使用openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr命令创建CSR:

```
<#root>
```

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

8.此命令后，您可以看到文件夹中列出的<CSR_name>.csr文件，该文件是必须发送到CA服务器进行签名的CSR文件。


```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIErTCCApuCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5
```

```
MRQwEgYDVQQHDAtnZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITCkD5VJa6KRssDJ8
[...]
```

Output Omitted

```
[...]
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JsPkvJmRpKSi1c7w
3rKfTXe1ewT1IJDcmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

 **注意：**由于Azure要求，必须使用配置了SHA-256或SHA-1的CA对CSR进行签名，否则，Azure IdP将在您上传证书时拒绝该证书。有关详细信息，请参阅以下链接：[SAML令牌中的高级证书签名选项](#)

9.将此CSR文件与您的CA一起发送以获取签名证书。

第二步：创建PKCS12文件

签署身份证书后，您需要使用以下3个文件创建公钥加密标准(PKCS#12)文件：

- 签名的身份证书
- 私钥（在前面的步骤中定义）
- CA证书链

您可以将身份证书和CA证书链复制到创建私钥和CSR文件的同一设备。一旦您有3个文件，请运行 `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` 命令，将证书转换为PKCS#12。

<#root>

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

运行命令后，系统将要求您输入密码。安装证书时需要此密码。

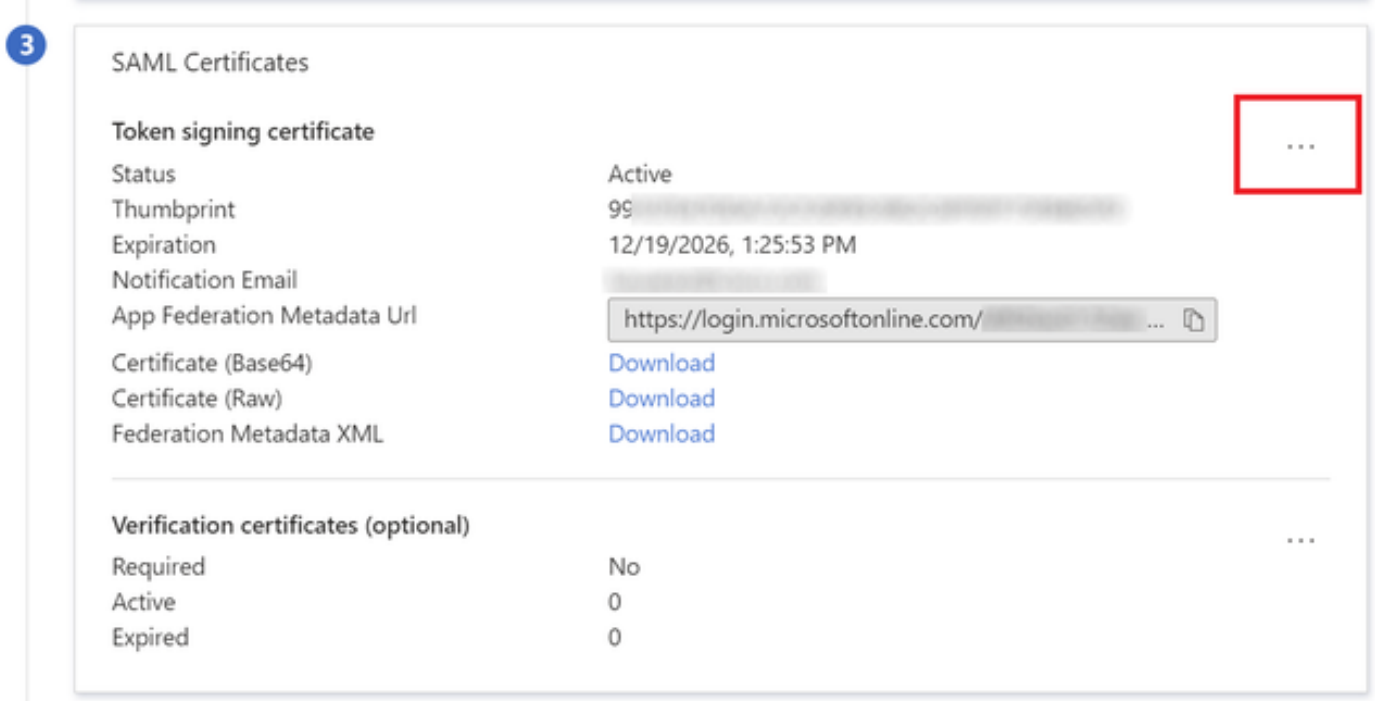
如果命令成功，将在当前目录中创建名为“<pkcs12_name>.pfx”的新文件。这是您的新PKCS#12证书。

第三步：将PKCS#12证书上传到Azure和FDM

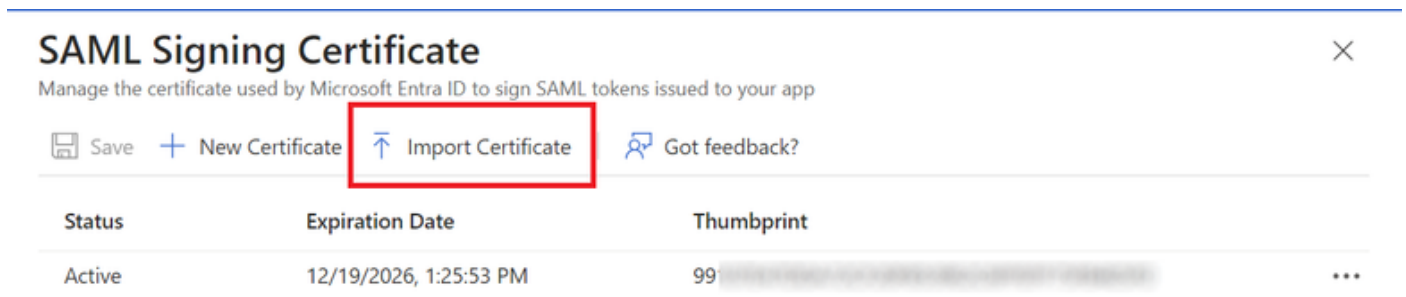
拥有PKCS#12文件后，需要将其上传到Azure和FDM。

将证书上传到Azure

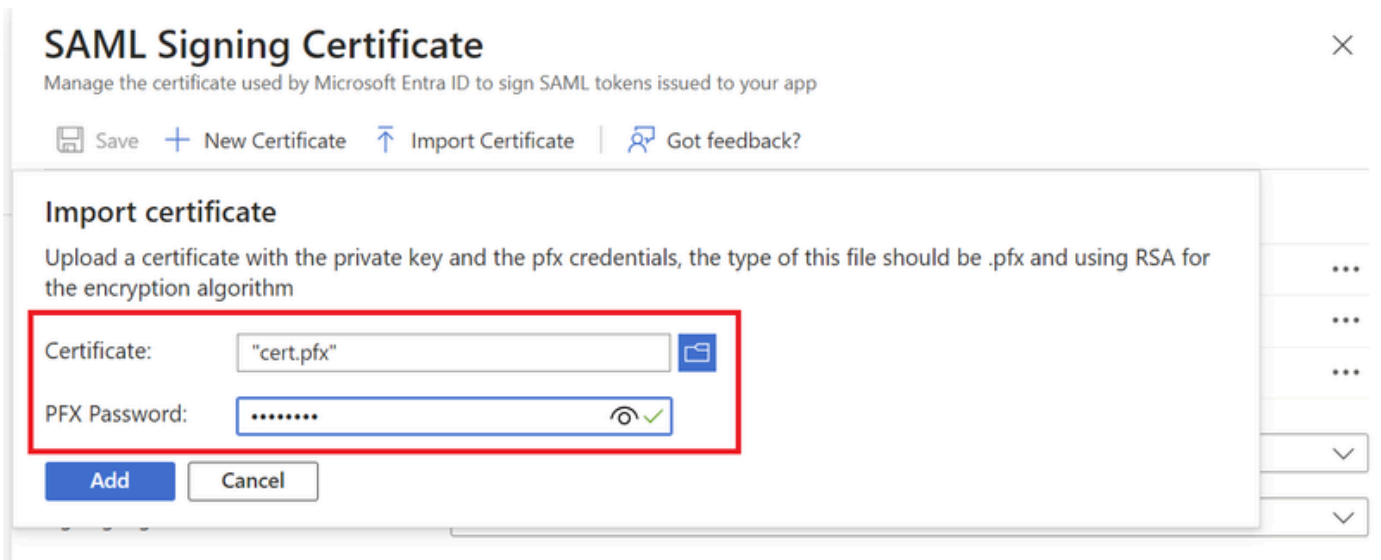
1. 登录到您的Azure门户，导航到要使用SAML身份验证保护的企业应用程序，然后选择单点登录。
2. 向下滚动到"SAML Certificates"部分，然后选择更多选项图标>编辑。



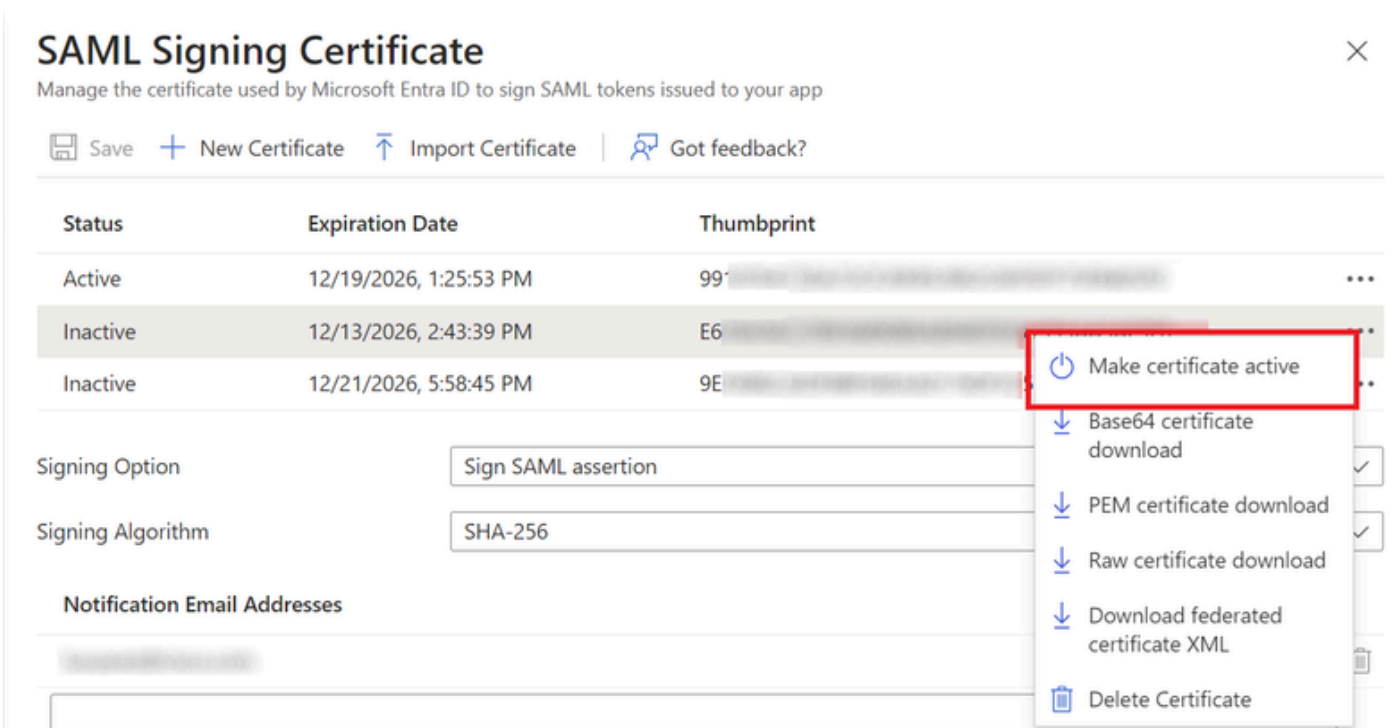
3. 现在选择Import certificate选项。



4. 查找以前创建的PKCS12文件，并使用您在创建PKCS#12文件时输入的密码。

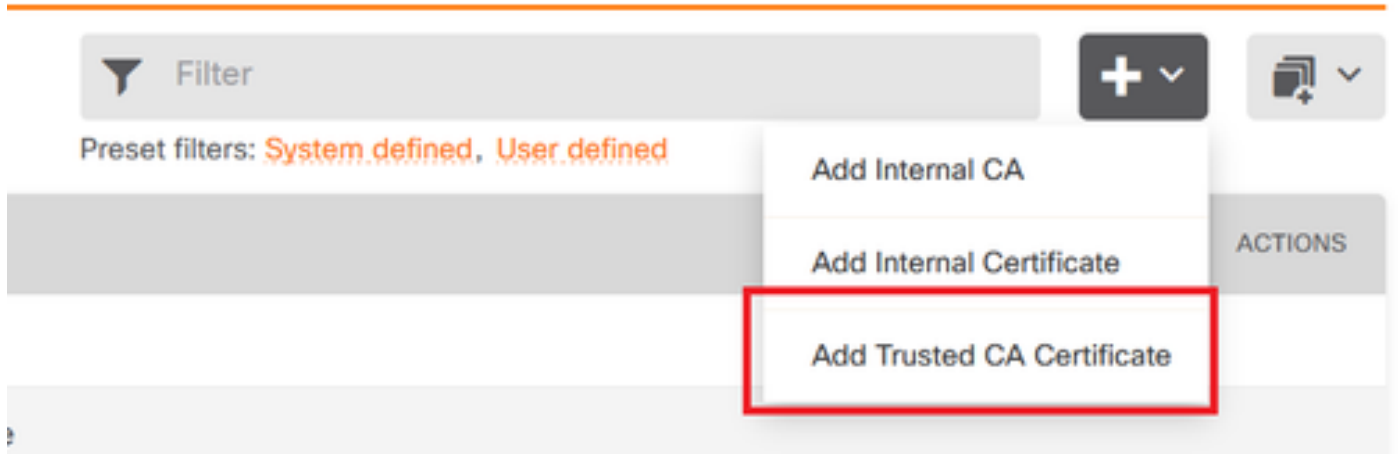


5.最后，选择激活证书选项。



将证书上传到FDM

1.导航到对象 > 证书 >单击添加受信任CA证书。



2. 输入您喜欢的信任点名称，并仅从IdP（不是PKCS#12文件）上传身份证书

Add Trusted CA Certificate ? ×

Name

Certificate No file uploaded yet

Paste certificate, or choose a file (DER, PEM, CRT, CER) [Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----
MIIEcjCCAlqgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBBMQwwCgYDVQQLEwN2cG4x
DjAMBgNVBAQoTBWtpc2NvMQwwCgYDVQQHEwNT.ZXpxDDAKBgNVBAgTA21leDELMAK
G
```

Validation Usage for Special Services

Please select ▼

CANCEL OK

3. 在SAML对象中设置新证书并部署更改。

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

验证

运行show saml metadata <trustpoint name>命令以确保元数据可从FTD CLI获得：

```
<#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...

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...]

3Zmzsc5faZ8dMX0+1ofQVvMaPifcZZFoM7oB09RK2PaMwIAV+Mw=

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

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

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。