

# 在FDM上使用SAML身份验证配置多个RAVPN配置文件

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

### [配置](#)

#### [第1步：使用OpenSSL创建自签名证书和PKCS#12文件](#)

#### [第2步：上传Azure和FDM上的PKCS#12文件](#)

##### [步骤 2.1将证书上传到Azure](#)

##### [步骤 2.2将证书上传到FDM](#)

### [验证](#)

---

## 简介

本文档介绍如何通过FDM在CSF上使用Azure作为IdP为远程访问VPN的多个连接配置文件配置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
- 远程访问虚拟专用网络(RAVPN)
- 思科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
- 思科安全防火墙(CSF)版本7.4.1
- 思科安全防火墙设备管理器版本7.4.1

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（或安全断言标记语言）是在各方（特别是身份提供程序(IdP)和服务提供程序(SP))之间交换身份验证和授权信息的开放标准。SAML身份验证用于远程访问VPN（RAVPN）连接和其他各种应用因其众多优势而日益流行。在Firepower管理中心(FMC)上，由于Connection Profile配置菜单中的Override Identity Provider Certificate选项可用，因此可以将多个连接配置文件配置为使用不同的IdP保护应用。此功能允许管理员使用每个连接配置文件的特定IdP证书覆盖单点登录(SSO)服务器对象中的主IdP证书。但是，此功能在Firepower设备管理器(FDM)上受到限制，因为它不提供类似选项。如果配置了第二个SAML对象，则尝试连接到第一个连接配置文件会导致身份验证失败，并显示错误消息：“由于检索单一登录cookie时出现问题，身份验证失败”。要解决此限制，可以创建自定义自签名证书并将其导入Azure以供所有应用程序使用。这样，只需在FDM中安装一个证书，即可对多个应用程序进行无缝SAML身份验证。

## 配置

### 第1步：使用OpenSSL创建自签名证书和PKCS#12文件

本节介绍如何使用OpenSSL创建自签名证书

1. 登录已安装OpenSSL库的终端。



注意：在本文档中，所使用的是Linux计算机，因此某些命令是特定于Linux环境的。但是，OpenSSL命令是相同的。

---

#### b.使用touch

`touch config.conf`  
命令创建一个配置文件。

<#root>

root@host#

```
touch config.conf
```

#### c.使用文本编辑器编辑文件。在本例中，使用Vim并运行vim

`.conf`

命令。您可以使用任何其他文本编辑器。

```
<#root>
```

```
root@host#
```

```
vim config.conf
```

d.输入要包括在自签名中的信息。

确保使用组织信息替换< >之间的值。

```
[req]
```

```
distinguished_name = req_distinguished_name
```

```
prompt = no
```

```
[req_distinguished_name]
```

```
C =
```

```
ST =
```

```
L =
```

```
O =
```

```
OU =
```

```
CN =
```

e.使用此命令基于

.conf

文件中指定的配置，使用SHA-256算法生成新的2048位RSA私钥和自签名证书，有效期为3650天。  
私钥保存到

.pem

，自签名证书保存到

.crt

o

<#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.在创建私钥和自签名证书后，它会将其导出到PKCS#12文件中，该文件是一种可以同时包含私钥和证书的格式。

<#root>

root@host#

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

.pem -in

.crt -name

-out

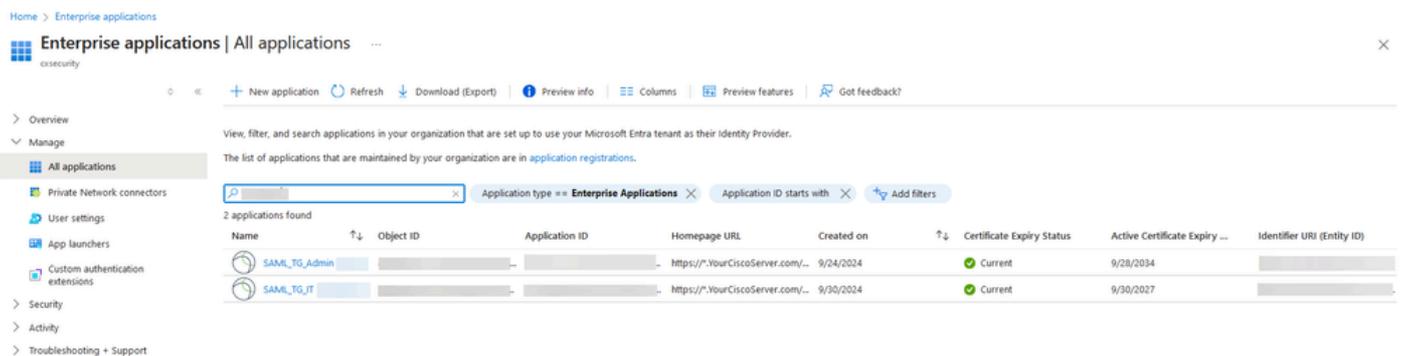
.pfx

```
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
```

注意密码。

## 第2步：上传Azure和FDM上的PKCS#12文件

确保在Azure上为在FDM上使用SAML身份验证的每个连接配置文件创建一个应用程序。



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, 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:

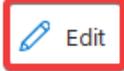
Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry	Identifier URI (Entity ID)
SAML_TG_Admin			https://YourCiscoServer.com/...	9/24/2024	Current	9/28/2034	
SAML_TG_IT			https://YourCiscoServer.com/...	9/30/2024	Current	9/30/2027	

当您具有步骤1：使用OpenSSL创建自签名证书和PKCS#12文件的PKCS#12文件后，必须针对多个应用程序将其上传到Azure，并在FDM SSO配置中进行配置。

### 步骤 2.1 将证书上传到Azure

- 登录您的Azure门户，导航到要使用SAML身份验证保护的企业应用程序，然后选择单一登录。
- 向下滚动到SAML Certificates 部分，然后选择More Options > Edit。

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:  

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

---

**Verification certificates (optional)**  Edit

Required: No

Active: 0

Expired: 0

c.现在请选择Import certificate选项。

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

### 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.最后，选择激活证书选项。

# 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?](#)

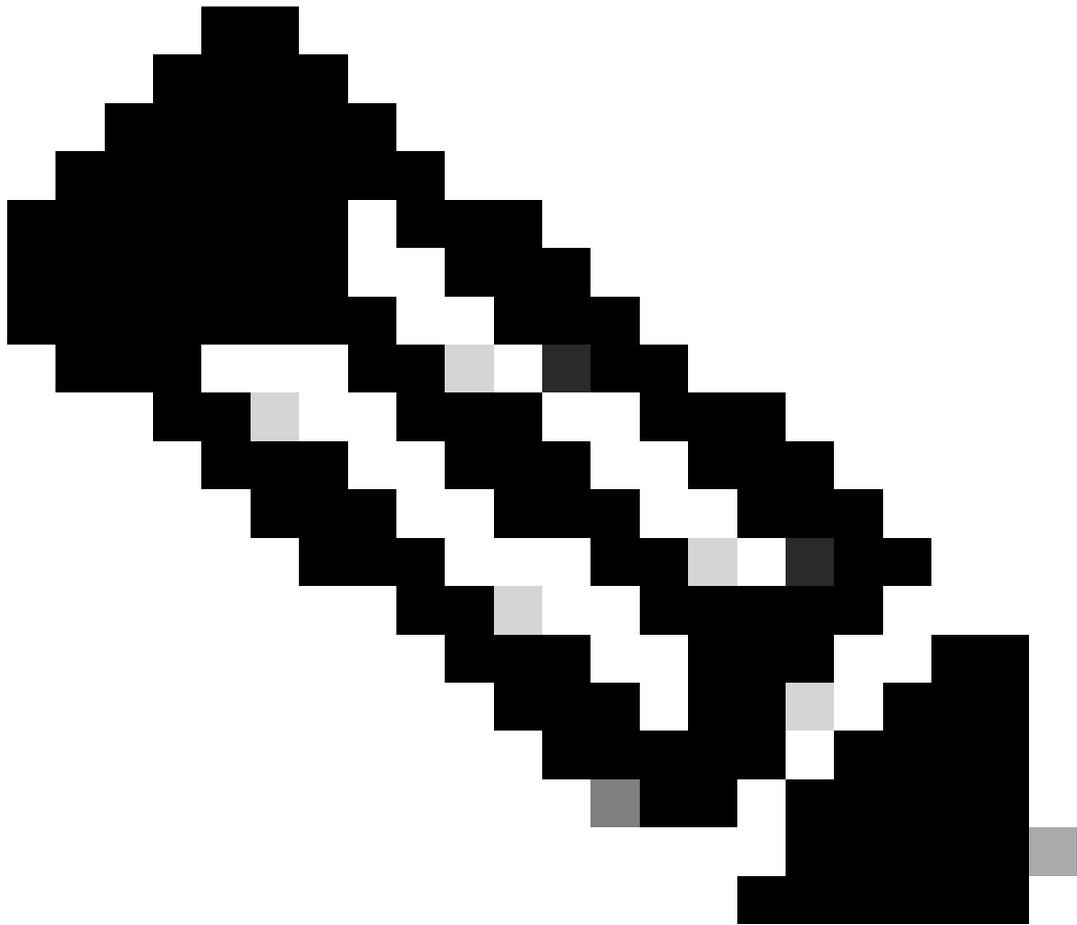
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	⋮
Active	9/27/2027, 5:51:21 PM	[Redacted]	⋮

Signing Option:

Signing Algorithm:

Notification Email Addresses:

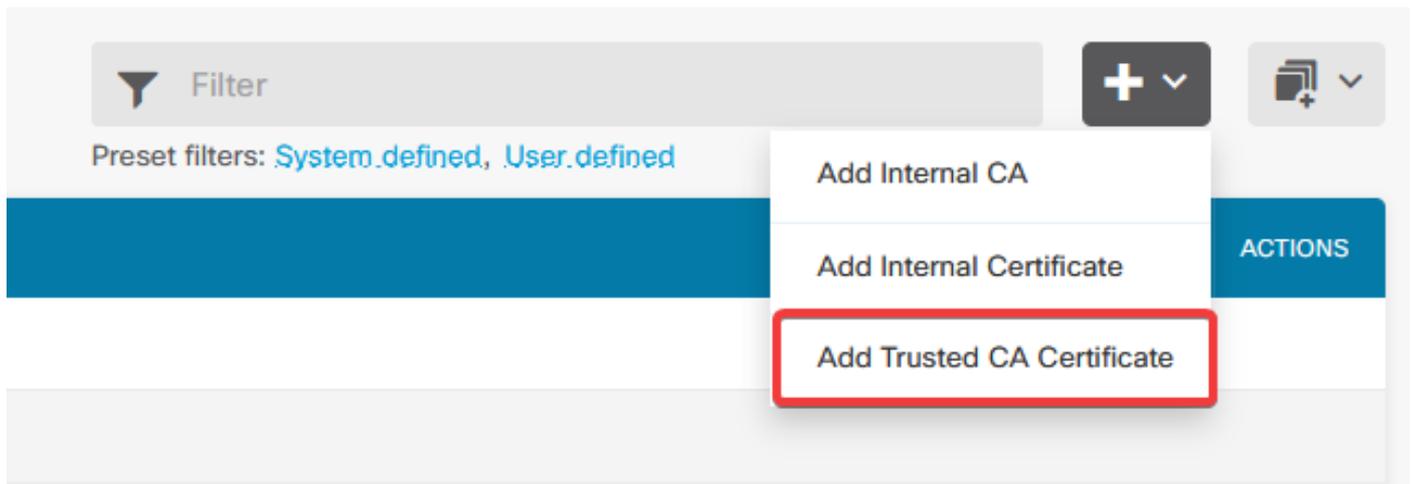
- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate



注意：请确保执行步骤2.1：将每个应用程序的证书上传到Azure。

## 步骤 2.2将证书上传到FDM

a. 导航至 **Objects > Certificates > Click Add Trusted CA certificate.**



b. 输入您喜欢的信任点名称，并仅从IdP（而非PKCS#12文件）上传身份证书，然后选中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  
MTIwMAYDVQQDEy1NaW5yb3NvZnQgQXp1cmUgRmVkdXJhdGVkIFNTTyBDZXJ0aWZp  
Y2E9ZTA0EwYwMDAEMzAwMTA0MTBzEwYwMDAEMzAwMTA0MTBzMDQyMjA0PzANBgkqhkiG9w0BAQsFAMAM
```

Skip CA Certificate Check

Validation Usage for Special Services

Please select

CANCEL

OK

c.在SAML对象中设置新证书。

# 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 Usage: ...)

Identity Provider Certificate

Azure\_SSO (Validation Usage: ...)

Request Signature

None

Request Timeout

*Range: 1 - 7200 (sec)*

d. 在使用SAML作为身份验证方法并在Azure中创建应用程序的不同连接配置文件上设置SAML对象。部署更改

## 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



## 验证

运行 `show running-config webvpn` 和 `show running-config tunnel-group` 命令以查看配置并验证在不同连接配置文件中配置了相同的IDP URL。

```
<#root>
```

```
firepower#
```

```
show running-confuting 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#
```

## 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）。