

在FDM上設定多個具有SAML驗證的RAVPN設定檔

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[第1步：使用OpenSSL建立自簽名證書和PKCS#12檔案](#)

[第2步：上載Azure和FDM上的PKCS#12檔案](#)

[步驟 2.1. 將證書上傳到Azure](#)

[步驟 2.2. 將憑證上傳到FDM](#)

[驗證](#)

簡介

本文檔介紹如何透過FDM在CSF上使用Azure作為IdP為遠端訪問VPN的多個連線配置檔案配置SAML身份驗證。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 安全通訊端層(SSL)憑證
- OpenSSL
- 遠端存取虛擬私人網路(RAVPN)
- 思科安全防火牆裝置管理員(FDM)
- 安全宣告標籤語言(SAML)
- Microsoft Azure

採用元件

本檔案中的資訊是根據以下軟體版本：

- OpenSSL
- 思科安全防火牆(CSF)版本7.4.1
- 思科安全防火牆裝置管理員版本7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

SAML或安全斷言標籤語言是一種用於在各方之間交換身份驗證和授權資訊的開放標準，特別是身份提供程式(IdP)和服務提供程式(SP)。SAML身份驗證用於遠端訪問VPN (RAVPN)連線和多種其他應用程式因其眾多優勢而日益流行。在Firepower管理中心(FMC)上，由於連線配置檔案配置選單中的覆蓋身份提供程式證書選項，可以將多個連線配置檔案配置為使用不同受IdP保護的應用程式。此功能允許管理員使用每個連線設定檔的特定IdP憑證，覆寫單一登入(SSO)伺服器物件中的主要IdP憑證。但是，此功能在Firepower裝置管理器(FDM)上受到限制，因為它不提供類似的選項。如果配置了第二個SAML對象，則嘗試連線到第一個連線配置檔案會導致身份驗證失敗，並顯示錯誤消息：「由於檢索單一登入cookie時出現問題，身份驗證失敗」。為繞過此限制，可以建立自定義自簽名證書並將其導入到Azure中，以便在所有應用程式中使用。如此一來，FDM中只需要安裝一個憑證，即可針對多個應用程式進行緊密的SAML驗證。

設定

第1步：使用OpenSSL建立自簽名證書和PKCS#12檔案

本節介紹如何使用OpenSSL建立自簽名證書

1. 登入已安裝OpenSSL庫的終結點。



注意：在本文檔中，使用的是Linux電腦，因此某些命令是特定於Linux環境的。但是，OpenSSL指令是相同的。

b. 使用 `touch`

`touch config.conf`
命令建立配置檔案。

<#root>

root@host#

```
touch config.conf
```

c. 使用文本編輯器編輯檔案。在本例中，使用Vim並運行 `vim`

`.conf`

命令。您可以使用任何其他文字編輯器。

```
<#root>
```

```
root@host#
```

```
vim config.conf
```

d.輸入要包含在自簽中的資訊。

請務必以組織資訊取代< >之間的值。

```
[req]
```

```
distinguished_name = req_distinguished_name
```

```
prompt = no
```

```
[req_distinguished_name]
```

```
C =
```

```
ST =
```

```
L =
```

```
O =
```

```
OU =
```

```
CN =
```

e.使用此命令將生成一個新的2048位RSA私鑰和一個使用SHA-256演算法的自簽名證書，根據

`.conf`
檔案中指定的配置，有效期為3650天。私鑰儲存到

`.pem`
，並且自簽名證書儲存到

`.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.在建立私鑰和自簽名證書之後，它將它們導出到PKCS#12檔案中，這是可以包括私鑰和證書的格式。

<#root>

root@host#

openssl pkcs12 -export -inkey

.pem -in

.crt -name

-out

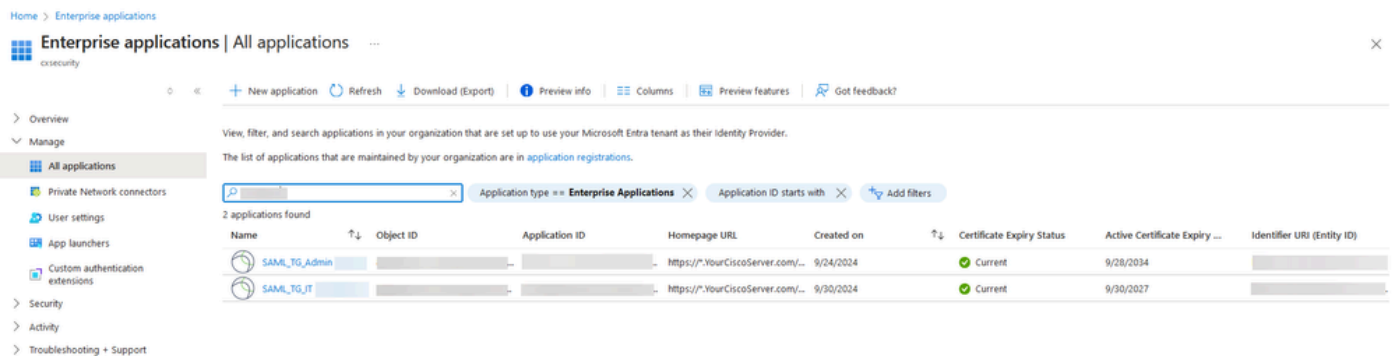
.pfx

```
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
```

記下密碼。

第2步：上載Azure和FDM上的PKCS#12檔案

確保在Azure上為在FDM上使用SAML身份驗證的每個連線配置檔案建立應用程式。



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:

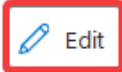
Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry	Identifier URI (Entity ID)
SAML_TG_Admin			https://*.YourCiscoServer.com/...	9/24/2024	Current	9/28/2034	
SAML_TG_IT			https://*.YourCiscoServer.com/...	9/30/2024	Current	9/30/2027	

當您具有步驟1：使用OpenSSL建立自簽名證書和PKCS#12檔案中的PKCS#12檔案後，必須針對多個應用程式將其上傳到Azure，並在FDM SSO配置中進行配置。

步驟 2.1.將證書上傳到Azure

- 登入您的Azure門戶，導航到要使用SAML身份驗證保護的企業應用程式，然後選擇單一登入。
- 向下滾動到SAML Certificates 部分，然後選擇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.現在，選擇導入證書選項。

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.尋找先前建立的PKCS#12檔案，並使用您在建立PKCS#12檔案時輸入的密碼。

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.最後，選擇啟用證書選項。

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?

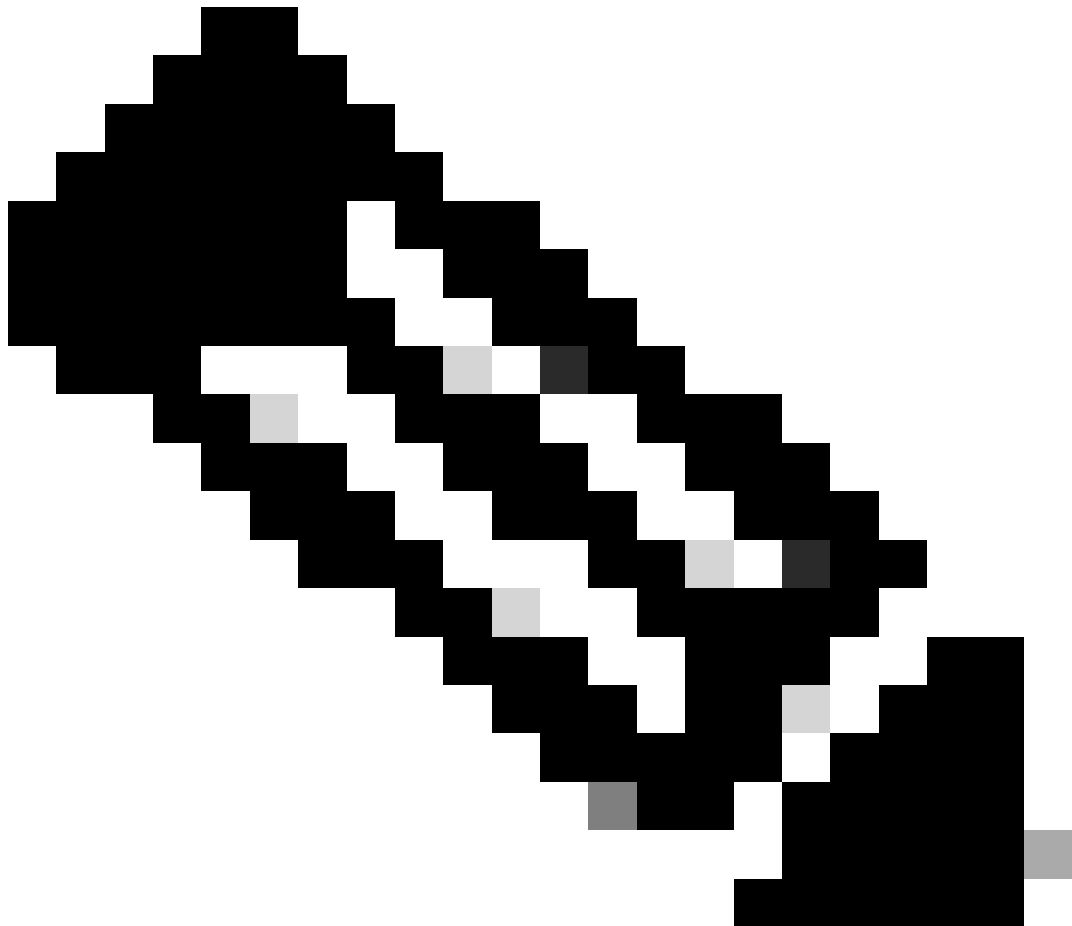
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	⋮
Active	9/27/2027, 5:51:21 PM	[Redacted]	⋮

Signing Option:

Signing Algorithm:

Notification Email Addresses:

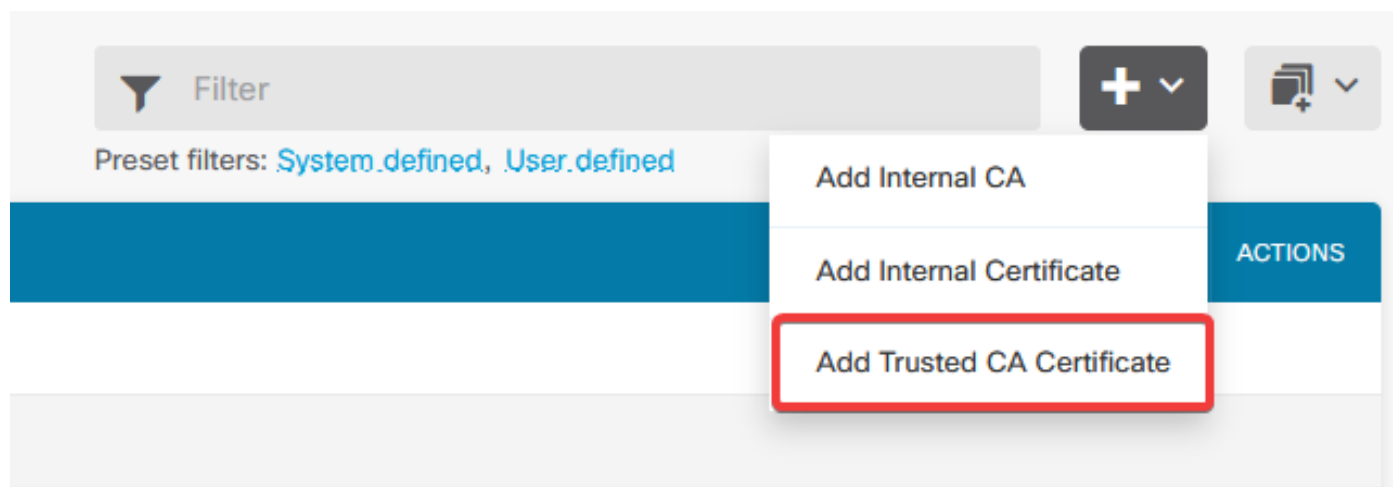
- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate



注意：請務必執行步驟2.1：將證書上傳到每個應用程式的Azure。

步驟 2.2.將憑證上傳到FDM

a. 導航至 Objects > Certificates > Click Add Trusted CA certificate。



b. 輸入您喜歡的信任點名稱，並僅從IdP（而非PKCS#12檔案）上傳身份證書，然後檢查Skip CA Certificate Check。

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.使用SAML作為身份驗證方法並在Azure中建立應用程式的不同連線配置檔案上設定SAML對象。
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



驗證

運行 `show running-config webvpn` 和 `show running-config tunnel-group` 命令以檢視配置，並驗證在不同連線配置檔案上配置了相同的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#
```


關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。