

在由FDM 7.2及更低版本管理的FTD上使用Azure作為IdP配置SAML身份驗證的RAVPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟 1. 建立副檔名為「基本約束：CA:TRUE」的證書簽名請求\(CSR\)](#)

[步驟 2. 建立PKCS12檔案](#)

[步驟 3. 將PKCS#12證書上傳到Azure和FDM](#)

[將證書上傳到Azure](#)

[將證書上傳到FDM](#)

[驗證](#)

簡介

本文檔介紹如何在FDM版本7.2或更低版本管理的FTD上使用Azure作為IdP為遠端訪問VPN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
- Linux命令
- 遠端存取虛擬私人網路(RAVPN)
- 安全防火牆裝置管理員(FDM)
- 安全斷言標籤語言(SAML)
- Microsoft Azure

採用元件

本檔案中的資訊是根據以下軟體版本：

- OpenSSL版本CiscoSSL 1.1.1j.7.2sp.230
- 安全防火牆威脅防禦(FTD)版本7.2.0

- 安全防火牆裝置管理員版本7.2.0
- 內部憑證授權單位(CA)


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身份驗證用於RAVPN連線和其他許多應用程式近來因其優勢而越來越流行。SAML是在各方之間交換身份驗證和授權資訊的開放標準，具體來說是指身份提供程式(IdP)和服務提供程式(SP)。

在FDM 7.2.x或更低版本管理的FTD中存在一個限制，其中SAML身份驗證的唯一支援的IdP是Duo。在這些版本中，將用於SAML身份驗證的證書上載到FDM時，必須具有基本約束：CA:TRUE副檔名。

因此，由其他IdP (沒有所需的副檔名) 提供的證書 (例如Microsoft Azure for SAML身份驗證) 在這些版本中原生不受支援，導致SAML身份驗證失敗。

 注意：FDM版本7.3.x和更高版本允許在上載新證書時啟用「跳過CA檢查」選項。這解決了本文檔中所述的限制。

如果使用Azure提供的證書配置SAML身份驗證的RAVPN，並且該證書沒有基本約束：CA:TRUE擴展，則在運行show saml metadata <trustpoint name> 命令從FTD命令列介面(CLI)檢索後設資料時，輸出為空，如下所示：

```
<#root>
firepower#
show saml metadata
```

```
SP Metadata
-----
IdP Metadata
-----
```

設定

解決此限制的建議計畫是將Secure Firewall升級到7.3版或更高版本，但是，如果出於任何原因需要防火牆運行7.2版或更低版本，您可以通過建立包含Basic Constraints: CA:TRUE擴展的自定義證書來解決此限制。證書由自定義CA簽名後，您需要在Azure SAML配置門戶中更改配置，以便改用此

自定義證書。

步驟 1. 建立副檔名為「基本約束：CA:TRUE」的證書簽名請求(CSR)

本節介紹如何使用OpenSSL為包含基本約束：CA:TRUE擴展建立CSR。

1. 登入到已安裝OpenSSL庫的終結點。
2. (可選) 使用`mkdir <folder name>` 命令建立一個目錄，您可以在其中找到此證書所需的檔案。

```
<#root>
```

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

```
mkdir certificate
```

3. 如果建立了新目錄，請更改該目錄的目錄，並生成運行`openssl genrsa -out <key_name>.key 4096`命令的新私鑰。

```
<#root>
```

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

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



註:4096位表示此配置示例的金鑰長度。如果需要，可以指定一個較長的金鑰。

4. 使用`touch <config_name>.conf`命令建立組態檔。
5. 使用文本編輯器編輯檔案。在本範例中，使用Vim，並執行`vim <config_name>.conf`命令。您可以使用任何其他文本編輯器。

```
<#root>
```

```
vim config.conf
```

6. 輸入要包括在證書簽名請求(CSR)中的資訊。確保在檔案中新增`basicConstraints = CA:true`副檔名，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
```



註: basicConstraints = CA:true是憑證需要具有的擴充模組，FTD才能成功安裝憑證。

7.使用在前面的步驟中建立的金鑰和組態檔，可以使用openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr指令建立CSR:

```
<#root>
```

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

8.執行此命令後，您可以看到資料夾中列出的<CSR_name>.csr檔案，該檔案是必須傳送到CA伺服器進行簽署的CSR檔案。


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

```
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5
```

```
MRQwEgYDVQHQHDAtnZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITCkD5VJa6KRssDJ8
[...]
```

Output Omitted

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

 注意：由於 Azure 要求，必須使用配置了 SHA-256 或 SHA-1 的 CA 對 CSR 進行簽名，否則，Azure IdP 將在你上載證書時拒絕該證書。可在以下連結中找到更多資訊：[SAML 令牌中的高級證書簽名選項](#)

9. 將此 CSR 檔案與您的 CA 一起傳送以獲取已簽名的證書。

步驟 2. 建立 PKCS#12 檔案

簽署身份證書後，您需要使用以下 3 個檔案建立公鑰加密標準 (PKCS#12) 檔案：

- 簽名的身份證書
- 私鑰 (在前面的步驟中定義)
- CA 憑證鏈結

您可以將身份證書和 CA 證書鏈複製到建立私鑰和 CSR 檔案的同一裝置。收到 3 個檔案後，執行 `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` 命令將憑證轉換為 PKCS#12。

```
<#root>
```

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

執行命令後，系統會要求您輸入密碼。安裝證書時需要此密碼。

如果命令成功，將在當前目錄中建立名為「<pkcs12_name>.pfx」的新檔案。這是您的新 PKCS#12 證書。

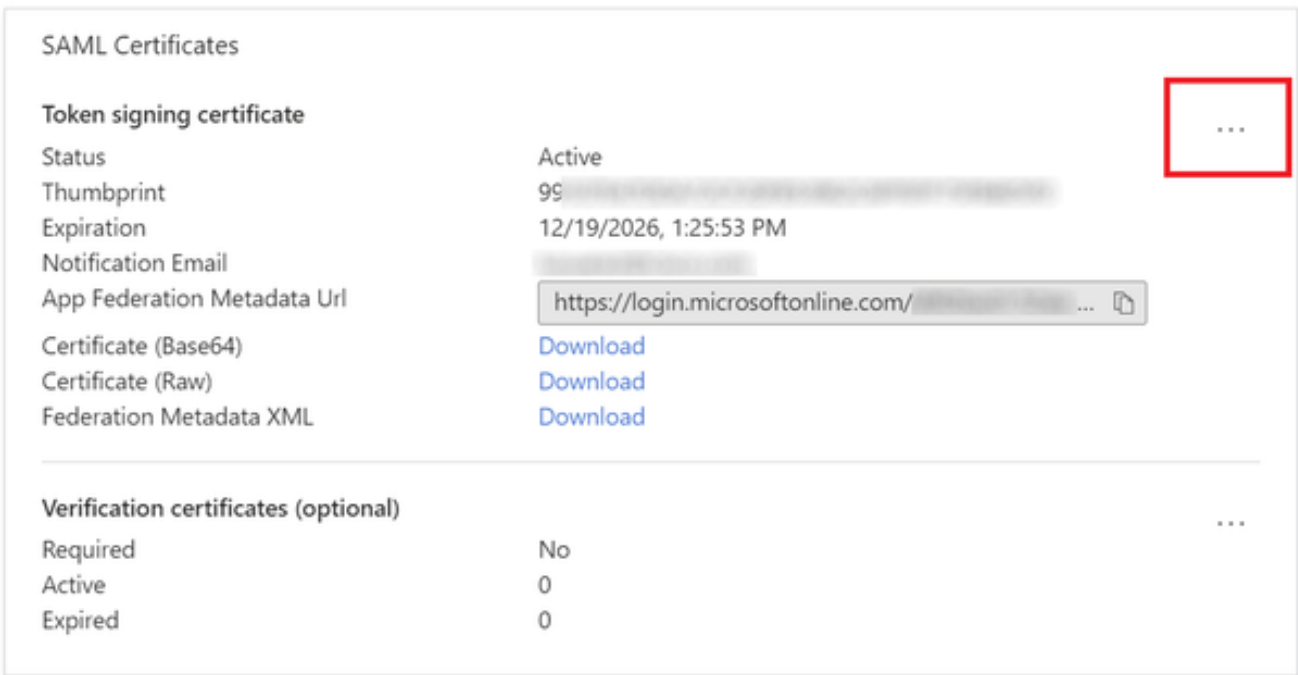
步驟 3. 將 PKCS#12 證書上載到 Azure 和 FDM

收到 PKCS#12 檔案後，需要將其上傳到 Azure 和 FDM。

將證書上傳到Azure

1. 登入到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」。
2. 向下滾動至SAML Certificates部分，然後選擇More Options圖示 > Edit。

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/...>

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional) ...

Required No

Active 0

Expired 0

3. 現在選擇匯入證書選項。

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

4. 查詢以前建立的PKCS12檔案，並使用您在建立PKCS#12檔案時輸入的密碼。


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.最後，選擇Make Certificate Active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	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

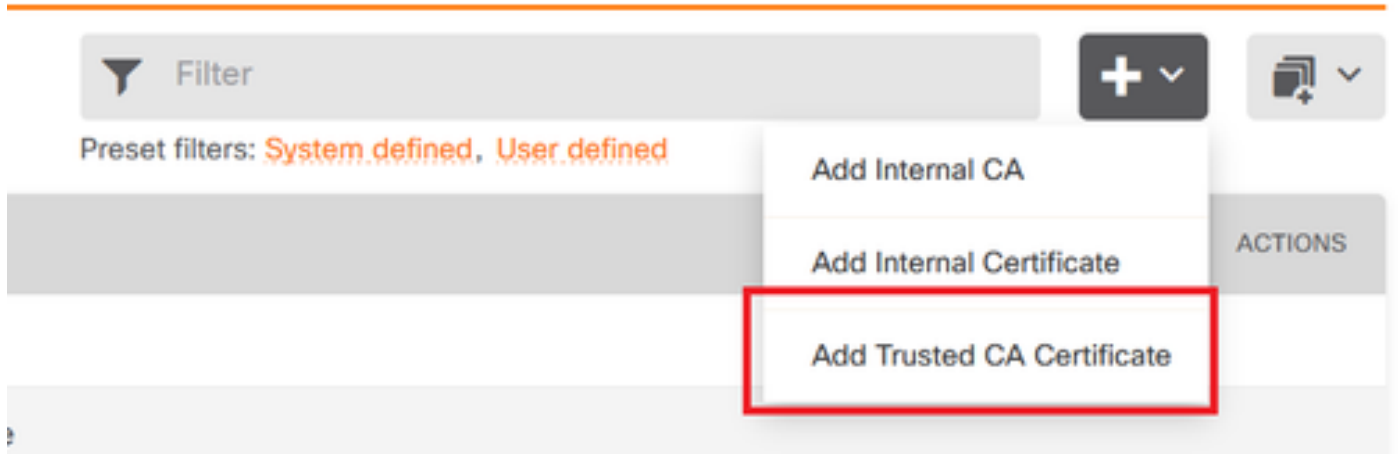
 Raw certificate download

 Download federated certificate XML

 Delete Certificate

將證書上傳到FDM

1.導航到對象 > 證書 >按一下新增受信任CA證書。



2. 輸入您喜歡的信任點名稱，僅從IdP（而不是PKCS#12檔案）上傳身份證書

Add Trusted CA Certificate ? ×

Name

Certificate No file uploaded yet

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

```
-----BEGIN CERTIFICATE-----
MIIEcjCCAlqgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBBMQswCgYDVQQLEwN2cG4x
DjAMBglVBAoTBWtpc2NvMQswCgYDVQQHEwNT.ZXpxDDAKBgNVBAgTA21leDELMAK
G
```

Validation Usage for Special Services

Please select ▼

CANCEL OK

3. 在SAML對象中設定新證書並部署更改。

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

驗證

運行show saml metadata <trustpoint name>命令以確保後設資料可從FTD CLI獲得：

```
<#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">

MIIDbzCCA1egAwIBAgIBDDANBgkqhkiG9w0BAQwFADBbMQwwCgYDVQQLEWV2cG4x

...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" />

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）。