

# Configurare RAVPN con autenticazione SAML utilizzando Azure as IdP su FTD Gestito da FDM 7.2 e versioni precedenti

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Passaggio 1. Creare una richiesta di firma del certificato \(CSR\) con estensione "Basic Constraints: CA:TRUE"](#)

[Passaggio 2. Crea file PKCS12](#)

[Passaggio 3. Carica il certificato PKCS#12 in Azure e FDM](#)

[Carica il certificato in Azure](#)

[Carica il certificato in FDM](#)

[Verifica](#)

---

## Introduzione

In questo documento viene descritto come configurare l'autenticazione SAML per la VPN ad accesso remoto utilizzando Azure as IdP su FTD gestito da FDM versione 7.2 o successiva.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Certificati SSL (Secure Sockets Layer)
- OpenSSL
- Comandi Linux
- RAVPN (Virtual Private Network) di accesso remoto
- Secure Firewall Device Manager (FDM)
- SAML (Security Assertion Markup Language)
- Microsoft Azure

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- OpenSSL versione CiscoSSL 1.1.1j.7.2sp.230
- Secure Firewall Threat Defense (FTD) versione 7.2.0
- Secure Firewall Device Manager versione 7.2.0
- CA (Certification Authority) interna

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.


## Premesse

L'uso dell'autenticazione SAML per le connessioni RAVPN e molte altre applicazioni è diventato più popolare di recente a causa dei suoi vantaggi. SAML è uno standard aperto per lo scambio di informazioni di autenticazione e autorizzazione tra le parti, in particolare un provider di identità (IdP) e un provider di servizi (SP).

Esiste un limite nel FTD gestito da FDM versione 7.2.x o inferiore in cui l'unico IdP supportato per l'autenticazione SAML è Duo. In queste versioni, i certificati da utilizzare per l'autenticazione SAML devono avere l'estensione Basic Constraints: CA:TRUE quando vengono caricati in FDM.

Per questo motivo, i certificati forniti da altri IdP (che non dispongono dell'estensione necessaria) come Microsoft Azure per l'autenticazione SAML non sono supportati in modo nativo in queste versioni, con conseguente errore dell'autenticazione SAML.

---

 Nota: le versioni 7.3.x e successive di FDM consentono di abilitare l'opzione Ignora controllo CA durante il caricamento di un nuovo certificato. In questo modo viene eliminata la limitazione descritta nel presente documento.

---

Se si configura RAVPN con l'autenticazione SAML utilizzando il certificato fornito da Azure e che non dispone dell'estensione Basic Constraints: CA:TRUE, quando si esegue il comando `show saml metadata <trustpoint name>` per recuperare i metadati dall'interfaccia della riga di comando (CLI) FTD, l'output viene lasciato vuoto come mostrato di seguito:

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

```
IdP Metadata
```

# -----

## Configurazione

Per risolvere questo problema, si consiglia di aggiornare il firewall protetto alla versione 7.3 o successiva. Se tuttavia per qualsiasi motivo è necessario che il firewall esegua la versione 7.2 o precedente, è possibile aggirare questo limite creando un certificato personalizzato che includa l'estensione Basic Constraints: CA:TRUE. Dopo che il certificato è stato firmato da una CA personalizzata, è necessario modificare la configurazione nel portale di configurazione SAML di Azure per utilizzare questo certificato personalizzato.

### Passaggio 1. Creare una richiesta di firma del certificato (CSR) con estensione "Basic Constraints: CA:TRUE"

In questa sezione viene descritto come creare un CSR utilizzando OpenSSL in modo da includere l'estensione Basic Constraints: CA:TRUE.

1. Accedere a un endpoint in cui è installata la libreria OpenSSL.
2. (Facoltativo) Creare una directory in cui è possibile individuare i file necessari per il certificato utilizzando il comando `mkdir <nome cartella>`.

<#root>

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

```
mkdir certificate
```


3. Se è stata creata una nuova directory, passare a tale directory e generare una nuova chiave privata eseguendo il comando `openssl genrsa -out <nome_chiave>.key 4096`.

<#root>

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

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

---

 Nota: 4096 bit rappresenta la lunghezza della chiave per questo esempio di configurazione. Se necessario, è possibile specificare una chiave più lunga.

---

4. Creare un file di configurazione utilizzando il comando `touch <config_name>.conf`.
5. Modificare il file con un editor di testo. Nell'esempio viene utilizzato Vim e viene eseguito il

comando vim <config\_name>.conf. È possibile utilizzare qualsiasi altro editor di testo.

```
<#root>
```

```
vim config.conf
```

6. Inserire le informazioni da includere nella richiesta di firma del certificato (CSR). Assicurarsi di aggiungere l'estensione basicConstraints = CA:true nel file, come mostrato di seguito:

```
<#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 è l'estensione che il certificato deve avere affinché l'FTD possa installare correttamente il certificato.

---

7. Utilizzando la chiave e il file di configurazione creati nei passaggi precedenti, è possibile creare il CSR con il comando `openssl req -new <nome_chiave>.key -config <nome_conf>.conf -out <nome_CSR>.csr`:

<#root>

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


8. Dopo questo comando, è possibile visualizzare il file <CSR\_name>.csr elencato nella cartella, ovvero il file CSR che deve essere inviato al server CA per essere firmato.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDbXR5
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITckD5VJa6KRssDJ8
[...]
```

Output Omitted

```
[...]
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JsPkvJmRpKSi1c7w
3rKfTXe1ewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm
RA==
-----END CERTIFICATE REQUEST-----
```

---

 Nota: a causa dei requisiti di Azure, è necessario firmare il CSR con una CA con SHA-256 o SHA-1 configurata. In caso contrario, il provider di servizi Internet Azure rifiuta il certificato quando viene caricato. Per ulteriori informazioni, fare clic sul collegamento seguente: [Opzioni avanzate di firma dei certificati in un token SAML](#)

---

9. Inviare il file CSR alla CA per ottenere il certificato firmato.

## Passaggio 2. Crea file PKCS12

Dopo aver firmato il certificato di identità, è necessario creare il file PKCS#12 (Public-Key Cryptography Standards) con i tre file successivi:

- Certificato di identità firmato
- Chiave privata (definita nei passaggi precedenti)

- Catena certificati CA

È possibile copiare il certificato di identità e la catena di certificati CA nello stesso dispositivo in cui sono stati creati la chiave privata e il file CSR. Dopo aver eseguito i 3 file, eseguire il comando `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <nome_chiave_privata>.key -out <nome_pkcs12>.pfx` per convertire il certificato in PKCS#12.

<#root>

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

Dopo aver eseguito il comando, verrà richiesto di immettere una password. La password è necessaria per l'installazione del certificato.

Se il comando ha esito positivo, nella directory corrente viene creato un nuovo file denominato "<pkcs12\_name>.pfx". Questo è il nuovo certificato PKCS#12.

### Passaggio 3. Carica il certificato PKCS#12 in Azure e FDM

Dopo aver ottenuto il file PKCS#12, è necessario caricarlo in Azure e in FDM.

Carica il certificato in Azure

1. Accedere al portale di Azure, passare all'applicazione Enterprise da proteggere con l'autenticazione SAML e selezionare Single Sign-On.
2. Scorrere fino alla sezione Certificati SAML" e selezionare l'icona Altre opzioni > Modifica.

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	<a href="https://login.microsoftonline.com/[redacted]">https://login.microsoftonline.com/[redacted]</a> <span>...</span>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

---

**Verification certificates (optional)** ...

Required	No
Active	0
Expired	0

3. Selezionare l'opzione Importa certificato.

## 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. Individuare il file PKCS12 creato in precedenza e utilizzare la password immessa al momento della creazione del file 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. Infine, selezionare l'opzione Rendi certificato attivo.

## 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

Carica il certificato in FDM

1. Passare a Oggetti > Certificati > Fare clic su Aggiungi certificato CA attendibile.



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

## Verifica

Eseguire il comando `show saml metadata <trustpoint name>` per verificare che i metadati siano disponibili dalla CLI 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...

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...]/sam12" />

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

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



## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).