

# Konfigurieren Sie RAVPN mit SAML-Authentifizierung unter Verwendung von Azure als IdP auf FTD, das von FDM 7.2 und niedriger verwaltet wird.

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Erstellen einer Zertifikatsanforderung \(Certificate Signing Request, CSR\) mit der Erweiterung "Basic Constraints: CA:TRUE"](#)

[Schritt 2: PKCS12-Datei erstellen](#)

[Schritt 3: Laden Sie das PKCS#12-Zertifikat in Azure und den FDM hoch.](#)

[Zertifikat in Azure hochladen](#)

[Zertifikat in FDM hochladen](#)

[Überprüfung](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie die SAML-Authentifizierung für Remote Access VPN mit Azure als IdP auf FTD konfigurieren, die mit FDM Version 7.2 oder niedriger verwaltet wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Secure Socket Layer (SSL)-Zertifikate
- OpenSSL
- Linux-Befehle
- Remote Access Virtual Private Network (RAVPN)
- Sicherer Firewall-Gerätanager (FDM)
- Security Assertion Markup Language (SAML)
- Microsoft Azure

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- OpenSSL-Version CiscoSSL 1.1.1j.7.2sp.230
- Secure Firewall Threat Defense (FTD) Version 7.2.0
- Secure Firewall Device Manager Version 7.2.0
- Interne Zertifizierungsstelle

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.


## Hintergrundinformationen

Die Verwendung der SAML-Authentifizierung für RAVPN-Verbindungen und viele andere Anwendungen ist in letzter Zeit aufgrund ihrer Vorteile beliebter geworden. SAML ist ein offener Standard für den Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen Parteien, insbesondere einem Identity Provider (IdP) und einem Service Provider (SP).

Es gibt eine Beschränkung in FTD, die von FDM Version 7.2.x oder niedriger verwaltet wird, wobei die einzige unterstützte IdP für die SAML-Authentifizierung Duo ist. In diesen Versionen müssen die für die SAML-Authentifizierung zu verwendenden Zertifikate beim Hochladen in den FDM die Erweiterung Basic Constraints: CA:TRUE aufweisen.

Aus diesem Grund werden Zertifikate, die von anderen IdPs (die nicht über die erforderliche Erweiterung verfügen) wie Microsoft Azure für die SAML-Authentifizierung bereitgestellt werden, in diesen Versionen nativ nicht unterstützt, sodass die SAML-Authentifizierung fehlschlägt.

---

 Hinweis: FDM-Versionen 7.3.x und höher ermöglichen die Aktivierung der Option "CA-Prüfung überspringen" beim Hochladen eines neuen Zertifikats. Damit wird die in diesem Dokument beschriebene Einschränkung behoben.

---

Wenn Sie RAVPN mit SAML-Authentifizierung konfigurieren und das von Azure bereitgestellte Zertifikat verwenden, das nicht über die Erweiterung Basic Constraints: CA:TRUE verfügt, wird beim Ausführen des Befehls `show saml metadata <trustpoint name>` zum Abrufen der Metadaten von der FTD Command Line Interface (CLI) eine leere Ausgabe angezeigt.

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

SP Metadata

-----

IdP Metadata

-----

## Konfigurieren

Es wird jedoch empfohlen, die Secure Firewall auf Version 7.3 oder höher zu aktualisieren. Wenn die Firewall aus irgendeinem Grund Version 7.2 oder niedriger ausführen muss, können Sie diese Einschränkung umgehen, indem Sie ein benutzerdefiniertes Zertifikat erstellen, das die Erweiterung Basic Constraints: CA:TRUE enthält. Nachdem das Zertifikat von einer benutzerdefinierten Zertifizierungsstelle signiert wurde, müssen Sie die Konfiguration im Azure SAML-Konfigurationsportal ändern, damit das Zertifikat stattdessen verwendet werden kann.

### Schritt 1: Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR) mit der Erweiterung "Basic Constraints: CA:TRUE"

In diesem Abschnitt wird beschrieben, wie Sie einen CSR mit OpenSSL erstellen, um die Basic Constraints: CA:TRUE Extension aufzunehmen.

1. Melden Sie sich bei einem Endpunkt an, auf dem die OpenSSL-Bibliothek installiert ist.
2. (Optional) Erstellen Sie ein Verzeichnis, in dem Sie die für dieses Zertifikat erforderlichen Dateien mit dem Befehl `mkdir <Ordnername>` finden.

```
<#root>
```

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

```
mkdir certificate
```

3. Wenn Sie ein neues Verzeichnis erstellt haben, wechseln Sie in dieses Verzeichnis, und generieren Sie einen neuen privaten Schlüssel, der mit dem Befehl `openssl genrsa -out <key_name>.key 4096` ausgeführt wird.

```
<#root>
```

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

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



Hinweis: 4096 Bit stellen die Schlüssellänge für dieses Konfigurationsbeispiel dar. Sie können bei Bedarf einen längeren Schlüssel angeben.

---

4. Erstellen Sie eine Konfigurationsdatei mit dem Befehl `touch <config_name>.conf`.
5. Bearbeiten Sie die Datei mit einem Texteditor. In diesem Beispiel wird Vim verwendet, und der Befehl `vim <config_name>.conf` wird ausgeführt. Sie können jeden anderen Texteditor verwenden.

<#root>

```
vim config.conf
```

6. Geben Sie die Informationen ein, die in die Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) aufgenommen werden sollen. Stellen Sie sicher, dass Sie die Erweiterung `basicConstraints = CA:true` in der Datei wie folgt angezeigt hinzufügen:

<#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
```

---

 Hinweis: `basicConstraints = CA:true` ist die Erweiterung, die das Zertifikat haben muss, damit das FTD das Zertifikat erfolgreich installieren kann.

---

7. Verwenden Sie den Schlüssel und die Konfigurationsdatei, die Sie in den vorherigen Schritten erstellt haben, und erstellen Sie den CSR mit dem Befehl `openssl req -new <key_name>.key -config <conf_name>.conf -out <CSR_Name>.csr`:

<#root>

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


8. Nach diesem Befehl wird die Datei `<CSR_name>.csr` im Ordner aufgelistet. Dabei handelt es sich um die CSR-Datei, die an den CA Server gesendet werden muss, um signiert zu werden.

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5  
MRQwEgYDVQQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqG  
SIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITCKD5VJa6KRssDJ8  
[...]
```

Output Omitted

```
[...]  
TRZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JspkvJmRpKSi1c7w  
3rKfTXe1ewT1IJdCmgpp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeG  
Wu6XM4o410LcRdaQZUhuFL/TPZSeLGB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKm  
RA==  
-----END CERTIFICATE REQUEST-----
```

---

 Hinweis: Aufgrund von Azure-Anforderungen ist es erforderlich, den CSR mit einer CA zu signieren, für die SHA-256 oder SHA-1 konfiguriert ist. Andernfalls lehnt die Azure-IDP das Zertifikat ab, wenn Sie es hochladen. Weitere Informationen finden Sie unter dem folgenden Link: [Erweiterte Optionen für die Zertifikatssignierung in einem SAML-Token](#)

---

9. Senden Sie diese CSR-Datei mit Ihrer Zertifizierungsstelle, um das signierte Zertifikat zu erhalten.

## Schritt 2: PKCS12-Datei erstellen

Nachdem Sie das Identitätszertifikat signiert haben, müssen Sie die Public-Key Cryptography Standards (PKCS#12)-Datei mit den nächsten drei Dateien erstellen:

- Signiertes Identitätszertifikat
- Privater Schlüssel (in den vorherigen Schritten definiert)
- Zertifizierungsstellen-Zertifikatkette

Sie können das Identitätszertifikat und die Zertifikatskette der Zertifizierungsstelle auf dasselbe Gerät kopieren, auf dem Sie den privaten Schlüssel und die CSR-Datei erstellt haben. Sobald die 3 Dateien ausgeführt wurden, führen Sie den Befehl `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_chain>.cer -inkey <private_key_name>.key -out <pkcs12_name>.pfx` aus, um das Zertifikat in PKCS#12 zu konvertieren.

<#root>

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

Nachdem Sie den Befehl ausgeführt haben, werden Sie aufgefordert, ein Kennwort einzugeben. Dieses Kennwort wird bei der Installation des Zertifikats benötigt.

Wenn der Befehl erfolgreich ausgeführt wurde, wird im aktuellen Verzeichnis eine neue Datei mit dem Namen "<pkcs12\_name>.pfx" erstellt. Dies ist Ihr neues PKCS#12-Zertifikat.

## Schritt 3: Laden Sie das PKCS#12-Zertifikat in Azure und den FDM hoch.

Sobald Sie die PKCS#12-Datei haben, müssen Sie sie in Azure und den FDM hochladen.

### Zertifikat in Azure hochladen

1. Melden Sie sich bei Ihrem Azure-Portal an, navigieren Sie zu der Enterprise-Anwendung, die Sie mit der SAML-Authentifizierung schützen möchten, und wählen Sie Single Sign-On aus.
2. Blättern Sie nach unten zum Abschnitt "SAML-Zertifikate" und wählen Sie das Symbol Weitere Optionen > Bearbeiten.

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> ...
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. Wählen Sie nun die Option Zertifikat importieren.

## 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. Suchen Sie die zuvor erstellte PKCS12-Datei, und verwenden Sie das Kennwort, das Sie beim Erstellen der PKCS#12-Datei eingegeben haben.




## 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. Wählen Sie abschließend die Option Zertifikat aktivieren.

## 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

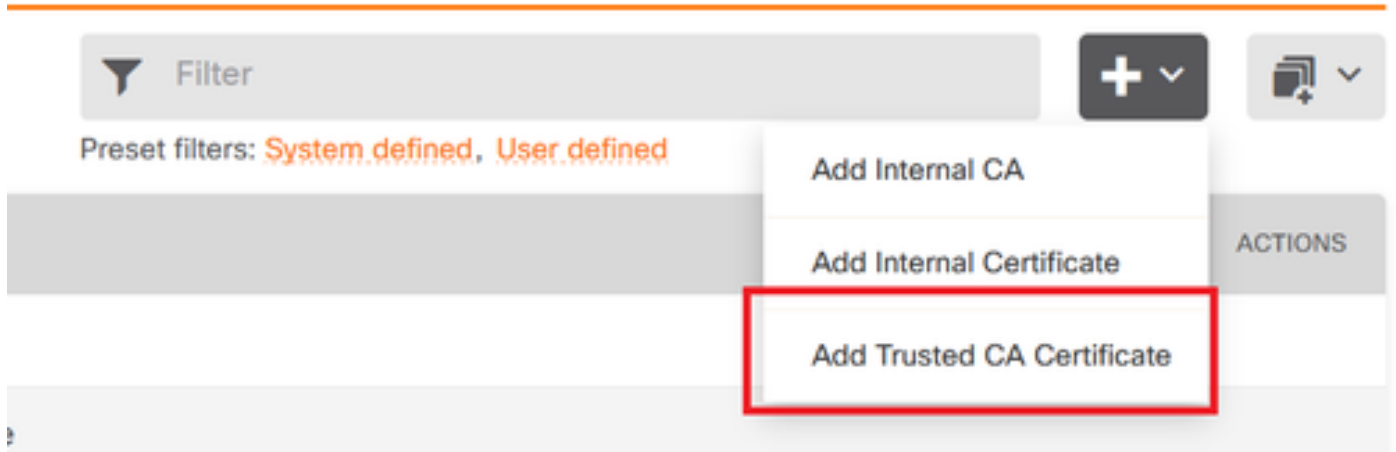
 Raw certificate download

 Download federated certificate XML

 Delete Certificate

Zertifikat in FDM hochladen

1. Navigieren Sie zu Objekte > Zertifikate > klicken Sie auf Vertrauenswürdiges Zertifizierungsstellenzertifikat hinzufügen.



2. Geben Sie den gewünschten Namen des Vertrauenspunkts ein, und laden Sie nur das Identitätszertifikat aus der IdP hoch (nicht die PKCS#12-Datei).

## Add Trusted CA Certificate

Name

azureIDP

Certificate No file uploaded yet

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

```
-----BEGIN CERTIFICATE-----
MIIEcjCCA1ggAwIBAgIBFzANBgkqhkiG9w0BAQsFADBBMQwwCgYDVQQLEwN2cG4x
DjAMBgNVBAoTBWVpc2NvMQwwCgYDVQQHEwNtZXZpdDAKBgNVBAGTA21leDELMAK
G
```

Validation Usage for Special Services

Please select

CANCEL OK

3. Legen Sie das neue Zertifikat im SAML-Objekt fest, und stellen Sie die Änderungen bereit.

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

## Überprüfung

Führen Sie den Befehl `show saml metadata <trustpoint name>` aus, um sicherzustellen, dass die Metadaten über die FTD-CLI verfügbar sind:

```
<#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...]/saml2" />
```



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.