

# SAML ةقداصم مادختساب RAPN نيوكت ممت يذلا FTD ىلع IDp ك Azure مادختساب لقاؤ 7.2 FDM ةطساوب هترادإ

## تايوت حمل

[ةمدقم](#)

[ةيساس ألاتابلطت](#)

[تابلطت](#)

[ةمدختسملاتانوك](#)

[ةيساس أتامولعم](#)

[نيوكت](#)

["CA:TRUE": ةيساس ألدوي قلا" دادتماب \(CSR\) ةداهش عي قوت بلط عاشنا. 1 ةوطخلا](#)

[PKCS12 فلم عاشنا. 2 ةوطخلا](#)

[FDM و Azure ىل. PKCS#12 ةداهش لىمحت. 3 ةوطخلا](#)

[Azure ىل. ةداهش لىمحت](#)

[FDM ىل. ةداهش لىمحت](#)

[ةحصلا نم ققحت](#)

## ةمدقم

مادختساب VPN ىل دعب نع لوصول SAML ةقداصم نيوكت ةيفي دنتمسمل اذه حضوي  
لقاؤ 7.2 فدم وأ رادصال ةطساوب هترادإ ممت يذلا FTD ىلع IDp ك Azure.

## ةيساس ألاتابلطت

### تابلطت

ةيلاتل عيضاوملاب ةيساس أةفرعم كي دل نوكت ناب Cisco ىصوت:

- SSL) ةنم آلا لىصوتلا ذخأم ةقبط تاداهش
- OpenSSL
- Linux رم أو
- (RAVPN) ةيره اظلال ةصاخلا دعب نع لوصول ةكبش
- (FDM) نم آلا ةيامحل رادج ةزهجأ ريدم
- (SAML) نام آلا دي كأت زيمرت ةغل
- Microsoft Azure

### ةمدختسملاتانوك

ةيلاتل جماربال تارادصا ىل دنتمسمل اذه يف ةدراول تامولعملا دنتمست

- OpenSSL رادصإل Cisco SSL 1.1.1j.7.2sp.230
- 7.2.0 رادصإل (FTD)، نمألآة إمامحل رادج ديهت دض عافدلأ
- Secure Firewall Device Manager، رادصإل 7.2.0
- (CA) ةيلخادلأ ةداهشلل حنم ةهج


ةصاخ ةيلممعم ةئيب يف ةدوجوملأ ةزهجالأ نم دنتسملأ اذه يف ةدراولأ تامولعملأ عاشنإ م تناك اذإ. (يضارتفا) حوسمم نيوكتب دنتسملأ اذه يف ةمدختسملأ ةزهجالأ عيمج تادب رملأ يأل لمحتحملأ ريثأتلل كمهف نم دكأتف، ليغشتلأ ديق كتكبش

## ةيساسأ تامولعمل

اعويش رثكأ رخألأ تاقيببطلل نم ديدعلأ RAPN تالاصتال SAML ةقداصم مادختسإ حبصأ ةقداصملا تامولعمل لدابتل حوتفم رايعم وه SAML. اهايازم ببسب ةريخألأ ةنوالأ يف (SP). ةمدخلل دوزمو (IDp) ةيوهال رفوم اديحتو، فارطألأ ني بضيوفتلأو

P فرعم نوكي شيح لقلأ وأ FDM 7.2.x تارادصإ ةطساوب هترادا ممت FTD يف دييقت دجوي يتلأ تاداهشلل يوتحت نأ بجي، تارادصإلأ هذه يف Duo. وه SAML ةقداصملا دمتمعملأ ديحولل إلأ اهليمحت دنم ca:TRUE: ةيساسألأ قحللملأ دويق يلع SAML ةقداصملا اهمادختسإ ممتيس FDM.

قحللملأ يلع يوتحت ال يتلأ) رخأ تافرعم نم ةمدقملا تاداهشلل دامتعا متي ال، ببسلأ اذهلو امم، تارادصإلأ هذه يف يعيبط لكشب SAML ةقداصملا Microsoft Azure لثم (بولطملا) SAML ةقداصم لشف يف ببستتي

 عجرملأ صحف يطخت رايخ نيكم ت شحلألأ تارادصإلأ او FDM 7.3.x تارادصإلأ حيتت: ةظحالم دنتسملأ اذه يف حضورملأ دييقتلأ لحي اذه. ةديج ةداهش لي ممت دنم قداصملا

Azure نم ةمدقملا ةداهشلل مادختسإب SAML ةقداصم مادختسإب RAPN نيوكت ةلاح يف show saml metadata رملألأ ليغشت دنم، CA:TRUE extension: ةيساسألأ دويقلأ يلع يوتحت ال يتلأو FTD، يف (CLI) رملأوالأ رطس ةهجاو نم فيرعتلأ تانايب دادرئسال <trustPoint name> metadata <trustPoint name> يلاتلأ ضرعم وه امك اغراف جارخإلأ نوكي:

```
<#root>
```

```
firepower#
```

```
show saml metadata
```

```
SP Metadata
```

```
-----
```

```
IdP Metadata
```

```
-----
```

# نيوكتل

وأ 7.3 رادصلإلى نمآلةامحل رادج ةيقرت يف دويقل هذه لعل ةحرتقملة طخلال لثمتت ليغشلة ةياملال رادج إلى بابسأل نم ببس يأل جاتحت تنك إذا، كلذ نم مغرلا يلع، يلع نمضتت ةصصخم ةداهش عاشنإ لالخنم ديدحتلال اذه لوح لمعلال كنكميف، لقا وأ 7.2 رادصلإلى جاتحت، صصخم قدصم عجرم نم ةداهشلال عيقوت درجمب. CA:TRUE: يساسأل دادتمالال نم ال دب ةصصخملة ةداهشلال هذه مادختسال Azure SAML نيوكت لخدم يف نيوكتلال ريغت كلذ.

ةيساسأل دويقلال قحلم مادختساب (CSR) ةداهش عيقوت بلط عاشنإ 1. ةوطخلال CA:TRUE

ةيساسأل دويقلال نيوضتل هل OpenSSL مادختساب CSR عاشنإ ةيفيك مسقلا اذه فصيفي CA:TRUE Extension.

1. اهيفي OpenSSL ةبتكم تيبتت مت ةياهن ةطقن إلى لوخدلال لفس.

2. ةداهشلال هذهل ةبولطملال تافللملال عقوم ديدحت كنكمي شيح ليلد عاشنإب مق (يفرايخإ).  
mkdir <folder name> رملال مادختساب

<#root>

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

```
mkdir certificate
```


3. لغشي ديدج صاخ جاتفم عاشنإو هيفي إلى ليلدلال ريغتت مقف، ديدج ليلد عاشنإب تمق إذا.  
openssl genrsa -out <key\_name>.key 4096 رملال

<#root>

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

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

---

 جاتفم ديدحت كنكمي. اذه نيوكتلال لاثمل جاتفملا لوطتت ةدحو 4096 لثمت: ةظالم رملال مزلا إذا لوطأ

---

4. رملال مادختساب نيوكت فلم عاشنإب مق. touch <config\_name>.conf

5. ليغشت متيفي Vim مادختسإ متيفي، لاثملا اذه يف. يصرن ررحم مادختساب فلملال ريحبت مق. رصوصن ررحم ي مادختسإ كنكمي. vim <config\_name>.conf رملال

<#root>

```
vim config.conf
```

6. إضافة نم دكأت (CSR) ةداهشلا عيقوت بلط يف اهنيمضت متيس يتلا تامولعمل لخدأ.  
basicConstraints = ca:true extension يف فلملل يف  
كلكلذ دعب ضرعم وه امك فلملل يف:

```
<#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

---

 يكل ةداهشلا هيلع يوتحت نأ بجي يذلا قحللملا وه BasicConstraints = CA:True ةظحالم  
حاجنب ةداهشلا تيبتت نم FTD نكمتي.

---

ءاشنإ كنكمي ،ةقباسلا تاوطخلا يف هؤاشنإ مت يذلا حاتفملاو نيوكتلا فلم مادختساب 7.

CSR مَادخْتَسَابِ رْمَأَلَا مَادخْتَسَابِ  
`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. فلم وهو، دلجمل ايف جردملا كب صاخلا <CSR\_name>.csr فلم ىرت نأ كنكمي، رمال اذه دعب. عي قوتل لل CA مداخل لىل هلاسرا بجي يذال CSR.

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

```
MIIErTCCApUCAQAwSTELMAkGA1UEBhMCTVgxFDASBgNVBAgMC011aXhjbyBDaXR5MRQwEgYDVQHDAtNZW14Y28gQ210eTEOMAwGA1UECgwFQ21zY28wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQRWH+ij26HuF/Y6NvITckD5VJa6KRssDJ8 [...]
```


Output Omitted

[...]

```
1RZ3ac3uV0y0kG6FamW3BhceYcDEQN+V0SInZZZQTW1Q5h23JsPkvJmRpKSi1c7w3rKfTXe1ewT1IJdCmgrp6qrwmEAPyrj/XnYyM/2nc3E3yJLxbGyT++yiVrr2RJeGwu6XM4o410LcRdaQZUhuFL/TPZSeLGJB2KU6XuqPMtGAvdmCgqdPSkwWc9mdnzKmRA==
```

-----END CERTIFICATE REQUEST-----

---

 نم ةنوكم CA لوصو ةطقنب CSR عي قوت يروضلا نم، Azure تابلطتمل ارظن: ةظحالم روثعل انكمي. اهللمحت دنع ةداهشلا ضفري Azure فرعم نإف، ال، او، SHA-1 أو SHA-256 [يف ةمدقتملا تاداهشلا عي قوت تاراخي](#): لىل طابترالا لىل تامولعمل نم ديزم لىل [زي مملل SAML زمر](#)

---

9. ةعقوملا ةداهشلا لىل لوصلل قوصملا عجرملا عم اذه CSR فلم لسرا.

## PKCS12 فلم عاشنإ 2. ةوطخلا

حاتفملا ريفشت ريعام فلم عاشنإل جاتحت كنإف، ةيوهلا ةداهش عي قوتب موقت نأ درجمب: ةيلاتل ةثالثل تافللملا عم (PKCS#12) ماعلا:

- ةعقوم ةيوه ةداهش
- (ةقباسلا توطخلا يفرعم) صاخحاتفم
- CA تاداهش ةلسلس

تمق شيح زاهجال سفن لىل قوصملا عجرملا ةداهش ةلسلسو ةيوهلا ةداهش خسن كنكمي موقت يثلل ةثالثل تافللملا كيدل نوكي نأ درجمب. CSR فلمو صاخلا حاتفملا عاشنإب `openssl pkcs12 -export -in <id_certificate>.cer -certfile <ca_cert_series>.cer -`

inkey <private\_key\_name>.key -out <pkcs12\_name>.pfx إلى PKCS#12. لإعدادها ليعمل رمها

<#root>

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

تثبيت دقة بولطم هذه رورم الةم لك. رورم الةم لك لإخذ كنم بلطي، رمال ليعشت دعب الةم لك.

يه هذه الةم لك ليعلدل في "pkcs12\_name.pfx" م ساب ديدج فلم عاشنإ متي، رمال حجن إذا الةم لك PKCS#12 ديدج الةم لك.

### FDM و Azure إلى PKCS#12 الةم لك ليعمحت. 3. ةوطخال

FDM و Azure إلى الةم لك ليعمحت إلى جاتحت، PKCS#12 فلم لكي دل نوكي نأ درجم ب

Azure إلى الةم لك ليعمحت

1. ةقداصمب هتياحم ديرت الةم لك Enterprise قيبطت إلى لقتنا، Azure لخدم إلى لوخدل لچس. SAML ددحو ليعمحت.

2. ريرحت > تاراخال نم ديزم الةم لك نوقيا ددحو "SAML تاداهش مسق إلى لفسال ريرمتلاب مق.

3

#### SAML Certificates

|                                  |   |     |
|----------------------------------|---|-----|
| <b>Token signing certificate</b> |   | ... |
| Status                           | Active  |     |
| Thumbprint                       | 95  |     |
| Expiration                       | 12/19/2026, 1:25:53 PM  |     |
| Notification Email               |   |     |
| App Federation Metadata Url      | <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> |     |
| Certificate (Base64)             | <a href="#">Download</a>  |     |
| Certificate (Raw)                | <a href="#">Download</a>  |     |
| Federation Metadata XML          | <a href="#">Download</a>  |     |

---

|   |    |     |
|---|----|-----|
| <b>Verification certificates (optional)</b> |    | ... |
| Required                                    | No |     |
| Active                                      | 0  |     |
| Expired                                     | 0  |     |

3. ةداهش داري تسإ رايخ نألآ ددح.

## 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. امدن ع اهتلخدأ ي تال رورملا ةم لك مدختساواق بس م هؤاشنإ مت يذلا PKCS12 فلم نع ثحبا .  
PKCS#12 فلم ءاشنإب تمق


## 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: "cert.pfx" 

PFX Password: .....  

Add

Cancel

5. ةطاشن ةداهشلا ل عج رايخ ددح، اريخأ.



## 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: Sign SAML assertion

Signing Algorithm: SHA-256

Notification Email Addresses: [Redacted]

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

FDM إلى عداش لى لي محت

1. عقت قوصم عجرم عداش ةفاضا إلى ع رقنا > تاداهش > تانئاك إلى لقتنا.

Filter

Preset filters: System defined, User defined

- Add Internal CA
- Add Internal Certificate
- Add Trusted CA Certificate

ACTIONS

2. فلم سىل (IdP) نم طقف ةيوهال عداش لى لي محت وه لصف ت يذال TrustPoint مسا لخدأ (PKCS#12)

## 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-----
MIIECjCCAlqgAwIBAgIBFzANBgkqhkiG9w0BAQsFAAD6bMQwwCgYDVOQLEwN2cG4x
DjAMBgNVBAoTBWVpc2NvMQwwCgYDVOQHEwNtZXpxDDAKBgNVBAgTA21leDELMAkG
A4UUAQoDARUwDQYJKoZIhvcNAQEBBQADggGPAD6bMQwwCgYDVOQLEwN2cG4x
-----
```

Validation Usage for Special Services

Please select

CANCEL

OK

3. تاريخي غتال رشنو SAML نئاك في ةدي دجل ةداهشلا نبي عتب مق.

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

## ةحصل لا نم ققحتلا

نم فيرعتلا تانايب رفوت نامضل <trustPoint name> show saml metadata رمالا ليغشتب مق  
ب FTD: ب ةصاخلا (CLI) رمالا رطس ةهجاو

```
<#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" />
```



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل