

ةقداصمب ةددعتم WAPN تافي صوت ليكشت SAML ىل فDM

تايوت حمل

[ةمدقم](#)

[ةيساس الابلطت](#)

[تابلطت](#)

[ةمدختسم الابلطت](#)

[ةيساس الابلطت](#)

[نيوك](#)

[OpenSSL مادختساب PKCS#12 فلم و ايتاذ ةعقوم ةداهش عاشنا: 1 ةوطخل](#)

[FDM و Azure ىل ةكس#12 فلم لي محت: 2 ةوطخل](#)

[Azure ىل ةداهش ل لي محت: 2.1 ةوطخل](#)

[FDM ىل ةداهش ل لي محت: 2.2 ةوطخل](#)

[ةحصلا نم ققحت](#)

ةمدقم

ل ةددعتم لي صوت فيرعت تافل ل SAML ةقداصم نيوك ةي فيك دن تسم ال اذه في
FDM ر ب ةكس CSF ىل Azure AS IDp مادختساب Remote Access VPN.

ةيساس الابلطت

تابلطت

ةيلات ال عيضاوم الابل ةيساس ةفرعم كي دل نوك نابل Cisco في صوت:

- SSL) ةنم ال لي صوت ال ذخأم ةقبط تاداهش
- OpenSSL
- RAVPN) ةيره اظلال ةصاخ ال د ب نع لوصول ةك ب ش
- Cisco نم (FDM) نم ال ةي امحل راج زاه ري دم
- SAML) نام ال دي كأت زي مرت ةغل
- Microsoft Azure

ةمدختسم الابلطت

ةيلات ال جم ارب ال تارادص ال دن تسم ال اذه في ةراول تامول عمل دن تست:

- OpenSSL
- Cisco Secure Firewall (CSF)، رادص ال 7.4.1
- Cisco Secure Firewall Device Manager، رادص ال 7.4.1

صاخ ةي لمعم ةئيب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ م تناك اذا .(يضا رتفا) حوسم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي قكتك بش

ةيساسأ تامولعم

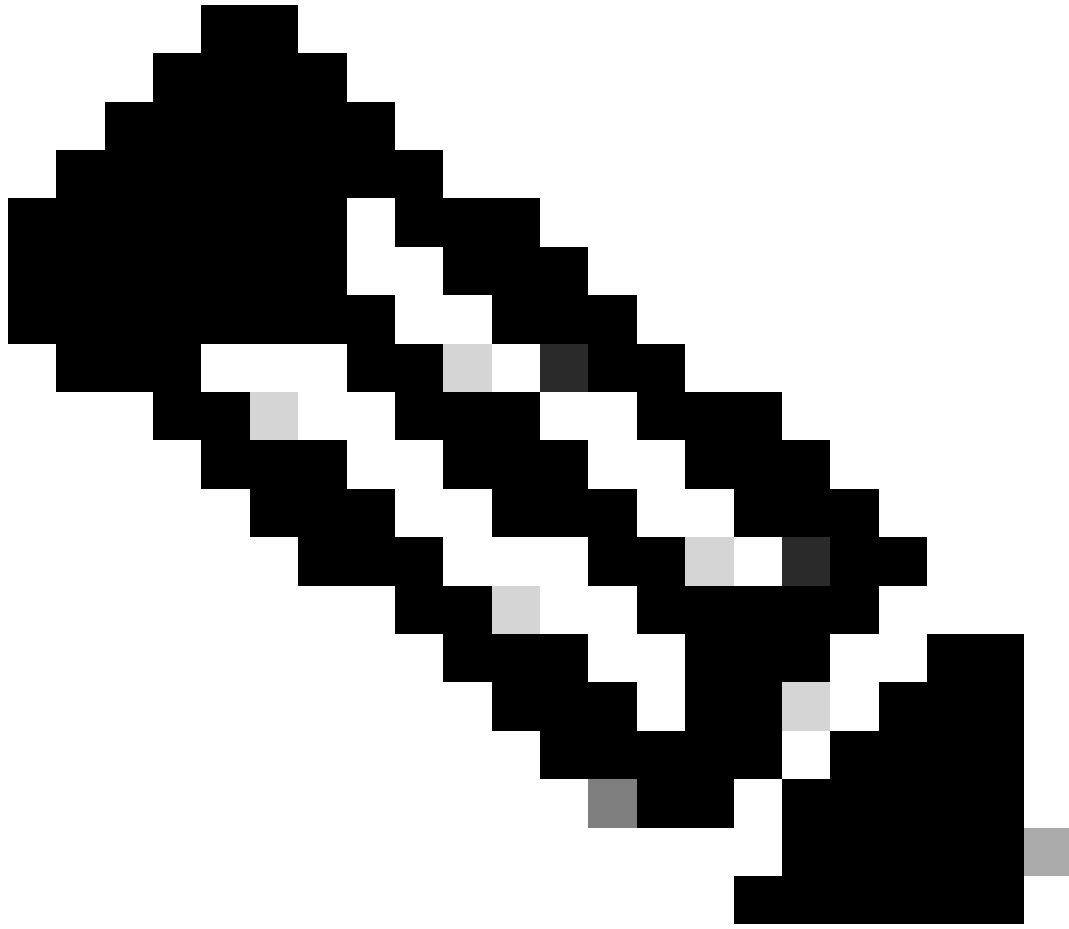
ضيوفتلاو ةقداصملا تامولعم لدابتل حوتفم راي عم يه نامأل دي كأت زييمت ةغل وأ SAML مادختسا حبصأ .(SP) ةمدخلل دوزمو (IDP) ةيوهلا رفوم دي دحتلا هجو يلعو ،فارطألا ني ب ةفلتخملل رخألا تاقيبطتلاو Remote Access VPN (RAVPN) تالاصتال SAML ةقداصم نكمي ،(FMC) ةرادا زكرم ي ف .ةددعتملا اهيازم ببسب ديازتم لكشب ةعئاش ببسب ةفلتخم P فرعمب ةيمحم تاقيبطت مادختسال ةددعتم ليصوت تافيصوت نيوكت هذه حمست .لاصتالا فيرعت فلم نيوكت ةمئاق ي ف رفوتملا ةيوهلا دوزم زواجت ةداهش راخ يداحألا لوخدلا ليحست مداخ نئاك ي ف ةيساسألا IdP ةداهش زواجت ني لوؤسملل ةزيملا يلع ةدودحم ةفي طولل هذه نإف ،كلذ عمو .لاصتالا فيرعت فلم لكل ةني عم IdP ةداهشب (SSO) ،ناث SAML نئاك نيوكت ةلاح ي ف .الاثامم اراخ رفوت ال اهأل "FirePOWER (FDM) ةزهجأ ري دم" ضرعيو ،ةقداصملا ي ف لشف لوألا ليصوتلا فيرعت فلمب لاصتالا ةلواحم نع جتنني طابترالا فيرعت فلم دادرتسا ي ف ةلكشم ببسب ةقداصملا تلشف" :أطخالا ةلاسر ةيتاذ ةصصخم ةداهش عاشنإ نكمي ،ديقلا اذه يلع لمعلل "يداحألا لوخدلا ليحستل ،كلذب مايقلا لالخنمو .تاقيبطتلا لك ربع مادختسال Azure ي ف اهداريتساو عيقوتلا ةينامأ حيتي امم ،(FDM) لوحملا تانايب ةدعاق ةرادا ي ف طقف ةدحاو ةداهش تي بثت مزلي ةددعتملا تاقيبطتلا ةمات ةسالسب SAML ةقداصم

نيوكتلا

OpenSSL مادختساب PKCS#12 فلمو ايتاذ ةعقوم ةداهش عاشنإ :1 ةوطخل

OpenSSL مادختساب ايتاذ ةعقوملا ةداهشلا عاشنإ ةيفي ك مسقلا اذه حضوي

1. اهيلع OpenSSL ةبتم تي بثت مت ةيانهن ةطقن يلى لوخدلا لاجس .



ةصاخ رم اوألا ضعب نإف كلذل ،Linux زاهج مادختسا متي ،دنتسملا اذه يف :ةظحالم
اهسفن يه OpenSSL رماوأنإف ،كلذعمو .Linux ةئيب

ب. touch مادختساب نيوكت فلم عاشنإ.

```
.conf  
رمألا
```

```
<#root>
```

```
root@host#
```

```
touch config.conf
```

ليغشت متي و VIM مادختسا متي ،لاثلما اذه يف .يصرن ررحم مادختساب فلملا ريرحت ج.
vim رماألا

.conf

رأ صوصن ررحم يأ مادختسإ كنكمي .

<#root>

root@host#

vim config.conf

يتاذلا عيقوتلا يف اهني ماضتل تامولعمل لخدأ د.

كب ةصاخلا ةسسؤملا تامولعمل ب < > نيب ميقلال لادبتسإ نم دكأت

[req]

distinguished_name = req_distinguished_name

prompt = no

[req_distinguished_name]

C =

ST =

L =

O =

OU =

CN =

ايتا ذة ع ق و م ة داه ش و ت ب 2048 راد ص | د ي د ج ص ا خ R S A ح ا ت ف م ء ا ش ن | م ت ي ، ر م أ ل ا ا ذ ه م ا د خ ت س ا ب . ه
ي ف د د ح م ل ا ن ي و ك ت ل ا ل ا ا د ا ن ت س ا ، ا م و ي 3650 ة د م ل ة ح ل ا ص ، S H A - 256 ة ي م ز ر ا و خ م ا د خ ت س ا ب

.conf

ه ي ل ع ص ا خ ل ا ح ا ت ف م ل ا ظ ف ح م ت ي . ف ل م ل ا

.pem

ه ي ل ع ا ي ت ا ذ ة ع ق و م ل ا ة د ا ه ش ل ا ظ ف ح م ت ي و

.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_ss0.crt
Generating a RSA private key
.....+++++
writing new private key to 'Azure_key.pem'
-----
root@host:~#
```

PKCS#12 فلم إلى مهري دصت ب موق ي ، اي تا ذة ع ق و م ل ا ة د ا ه ش ل ا و ص ا خ ل ا ح ا ت ف م ل ا ء ا ش ن ا د ع ب . و
ة د ا ه ش ل ا و ص ا خ ل ا ح ا ت ف م ل ا ن م ل ك ن م ض ت ي ن ا ن ك م ي ق ي س ن ت و ه و .

<#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
```

رورملا ةم لك ىلإ هبتنا

Azure و FDM ىل ع PKCS#12 فلم لىمحت: 2 ةوطخ ل

ىل ع SAML ةقداصم مدختسي لى صوت لى صوت لى ع Azure قىببطت عاشنإ نم دكأت FDM.

The screenshot shows the Microsoft Entra 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 columns for Name, Object ID, Application ID, Homepage URL, Created on, Certificate Expiry Status, Active Certificate Expiry, and Identifier URI (Entity ID). Two applications are listed: SAML_TG_Admin and SAML_TG_IT, both with a status of "Current".

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	

PKCS#12 فلم و ايتاذ ةعقوم ةداهش عاشنإ: 1 ةوطخ ل نم PKCS#12 فلم ىل ع ك لوصح درجم نىوكت ي ف هنىوكت و تاقيببطل نم دىدلل Azure ىلإ هلىمحت بجى، OpenSSL مادختساب FDM SSO.

Azure ىلإ ةداهش لىمحت. 2.1 ةوطخ ل

هتيامح دىرت يذلا ةسسؤملا قىببطت ىلإ لقتناو، ك ب صاخال Azure لخدم ىلإ لوخدلا لىس أ. يداخال لوخدلا لىمحت ددحو، SAML ةقداصم ب

ريحت > تارايلخ لا نم دي زملا ددحو SAML تاداهش مسق ىلا لفسأل ري رمتلاب مق ب.

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: <https://login.microsoftonline.com/>

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional) Edit

Required	No
Active	0
Expired	0

ةداهش داري تسلا رايخ ددح، نآلا ج.

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: [Sign SAML assertion](#)

Signing Algorithm: [SHA-256](#)

د. PKCS#12 ل تفلخ ام دنع تلخد ةم لكلا مدختسا و اقباس تفلخ دربم PKCS#12 ل نع شحبا .
دربم .

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: [File](#)

PFX Password: [Check](#)

[Add](#) [Cancel](#)

ةطشن ةداهشلا لعج رايخ ددح، اريخا ه.

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?](#)

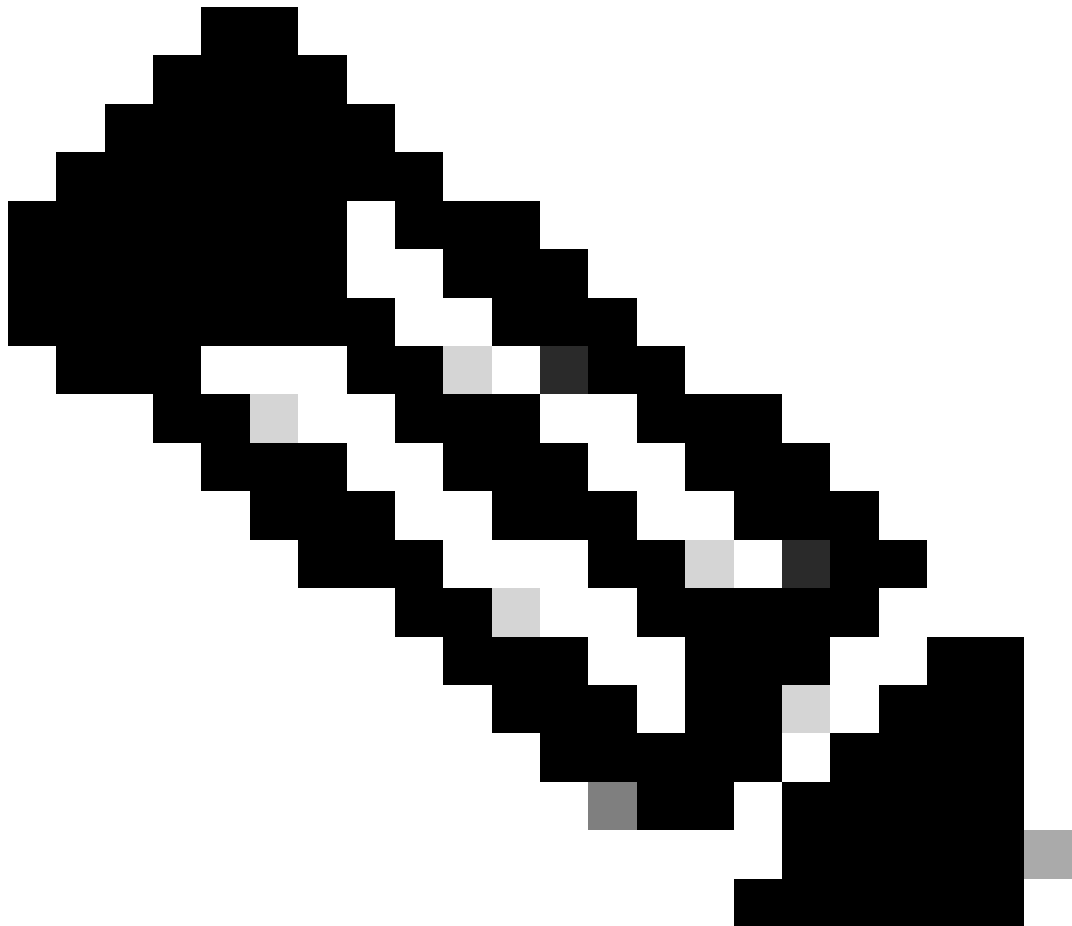
Status	Expiration Date	Thumbprint	
Inactive	9/28/2034, 1:05:19 PM	[Redacted]	⋮
Active	9/27/2027, 5:51:21 PM	[Redacted]	⋮

Signing Option:

Signing Algorithm:

Notification Email Addresses:

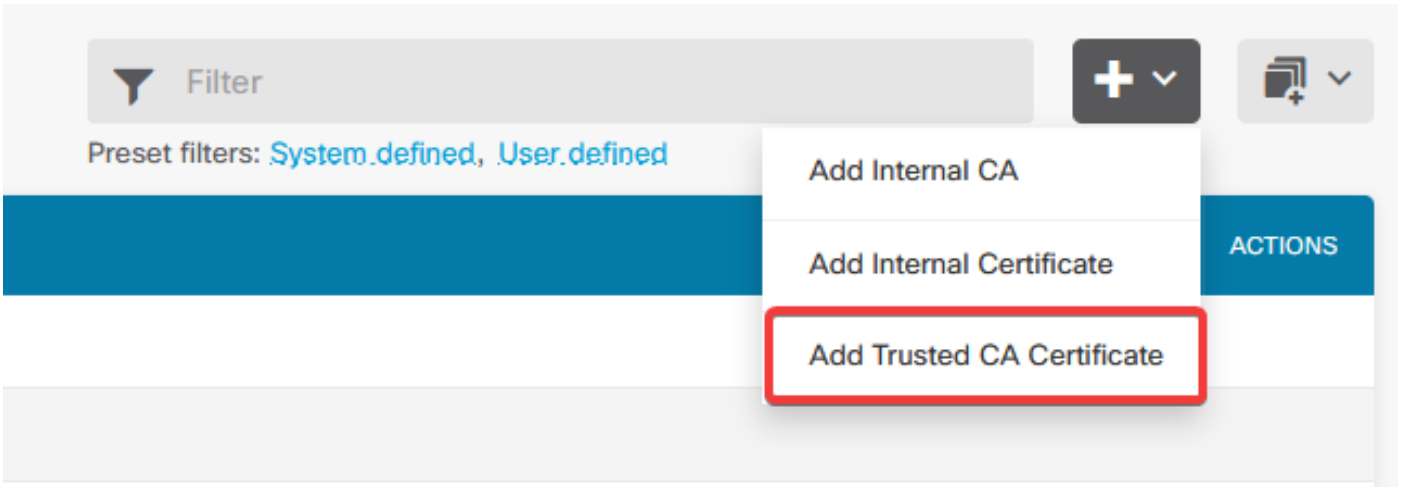
- Make certificate active
- Base64 certificate download
- PEM certificate download
- Raw certificate download
- Download federated certificate XML
- Delete Certificate



قېبىت لىك Azure ىلى ەدەش لى لىمىت: 2.1 ە وۇخ لى ذىفنت نىم دىكأت: ەظىال م

FDM إلى ةداهش ل ليمحت 2.2 ةوطخ ل

أ. إلى لقتنا أ. Objects > Certificates > Click Add Trusted CA certificate.



ب. فلم سي ل) IdP نم طقف ةيوله ل ةداهش ل ليمحت ب مقو هلضفت يذلا TrustPoint مس لخدأ. ب. Skip CA Certificate Check نم ققحتو، (PKCS#12).

Add Trusted CA Certificate



Name

Azure_SSO

Certificate

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

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----  
MIIC8DCCAdigAwIBAgIQGDZUgz1YHI5PirWojole+zANBgkqhkiG9w0BAQsFADA0  
MTIwMAYDVQQDEy1NaWNYb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZp  
Y2E9ZTA0EwYwMDAEMzAwMTA0MTBzEwYwMDAEMzAwMTA0MTBzMDQyMjA0PQ==
```

Skip CA Certificate Check

Validation Usage for Special Services

Please select

CANCEL

OK

SAML نئاك في ةديدجال ةداهشلا نييعت ج.

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)

SAML مَدْخَسْت يَتَلَا فَلَخْم لَ لَصَوْت لَ فَيَرَع تَافَلَم يَلَع SAML نَئَاكَ نَيَع تَب مَق د. تَارِيغْت لَ رَشَن. Azure فَيَا هَل قَيَبَطْت لَ عَاشَنَا مَت يَتَلَاو قَوَاصِم قَيَرَطَك

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

AzureAD



تحصيل نم ققحتلا

ققحتلا او نيوكتلا ةعجارم رمأل show running-config tunnel-group WebVPN و show running-config لئغشتب مق ةفلا تخملا لاصتالا فيرعت تافل ملى ع نيحزانلاب صاخلا URL سفن نيوكت نم.

<#root>

firepower#

show running-config 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#
```


ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا