

رفومك Azure مادختساب FMC SSO نيوكت ةيوه

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[SAML تاحلطصم](#)

[IDp نيوكت](#)

[SP نيوكت](#)

[FMC لعل SAML](#)

[تاريذختلا ودوخللا](#)

[نيوكتلا](#)

[ةيوهلا رفوم لعل نيوكتلا](#)

[Firepower ةرادا زكرم لعل نيوكتلا](#)

[Azure عم RBAC - مدقتم نيوكت](#)

[ةحصللا تمققوختلا](#)

[اهجالصا واطخألا فاشكتسا](#)

[ضرعتسملا SAML تالچس](#)

[FMC SAML تالچس](#)

ةمدقملا

Firepower (FMC) ةرادا زكرم ليداخل لوخدلا ليجست نيوكت ةيفيك دنتسملا اذه حضوي (IDp). ةيوه رفومك Azure مادختساب (SSO).

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتل عيضاوملاب ةفرعم كيذل نوكت ناب Cisco ي صوت:

- FirePOWER ةرادا زكرم ليجست يساسألا مهفلا
- يداخل لوخدلا ليجست يساسألا مهفلا

ةمدختسملا تانوكملا

ةيلاتل جماربل تارادصا لىا دنتسملا اذه في ةدراولا تامولعملا دنتست:

- Cisco Firepower (FMC) 6.7.0 رادصإلإ، ةرادإ زكرم
- Azure - IdP

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف، لئغشتلا ديق كتكبتش

ةيساسأ تامولعم

SAML تاحلطم

SSO لئعجي يذلا يساسألا لوكوتوربلا نايحألا مظعم يف ه (SAML) نامألا ديكأت زيميتم ةغل ةيوه نزخم دجوي ةحفصلا هذه فلخ، ةدحاو لوخد لئجست ةحفصب ةكرشلا ظفتحت. انكمم حمسي يذلاو، SAML معددي بيوقيبطت ي نيوكت ةلوهسب هنكمي. ةعونتم ةقداصم دعاوقو نامألا ةزيم يلع يوطني ال هنا امك. بيولا تاقيبطت عيمج يلا لوخدلا لئجستب كل لكل (اهمدختسإ ةداعإ امبرو) رورملا تاملكب ظافتحالا يلع نيمدختسمل رابجإ يف ةلثمتملا. بيولا يلع تاقيبطتلا هذهل رورملا تاملكب ضرع وأ، هيلإ لوصوللا يلا نوجاتحي بيوقيبطت

فرعي ثيحب ةمدخلال فرعم نيوكت بجي. SP يفو IDp يف: نيناكم يف SAML نيوكت عارجإ بجي (SP) ةمدخر فوم يلا لوخدلا لئجست يف نوبغري امدمع نيمدختسمل لاسرا ةيفيكيو ناكم لبق نم ةعقووملا SAML تاديكأت يف ةقتلا هنكمي هنا فرعي يحتح SP نيوكت مزلي. ددحم IdP.

SAML ل ةيساسألا تاحلطملا ضعب فيرعت:

- لئجست ةحفص ةطساوب اهروصت متي ام ابلاغ) جم انربلا ةمدخ وأ ةادأ - (IdP) ةيوهلا رفوم مدمختسمل مسا نم ققحتي؛ ةقداصملا ذيفنتب موقت يتلا (تامولعم ةحول وأو لوخد يرخأ ةقداصمو، نيلماع يعدتسيو، باسحلا ةلاح نم ققحتي، رورملا تاملكو
- لوصول قح باسكتك مدمختسمل لواح ي شيح بيوقيبطت - (SP) ةمدخلال دوزم.
- HTTP ربعا هلاسرلا متي، يرخأ تامس ابلاغو مدمختسمل ةيوه دكؤت ةلاسر - SAML ديكأتب ضرعتسمل هيجوت ةداعإ تايلمع لالخ نم

IDp نيوكت

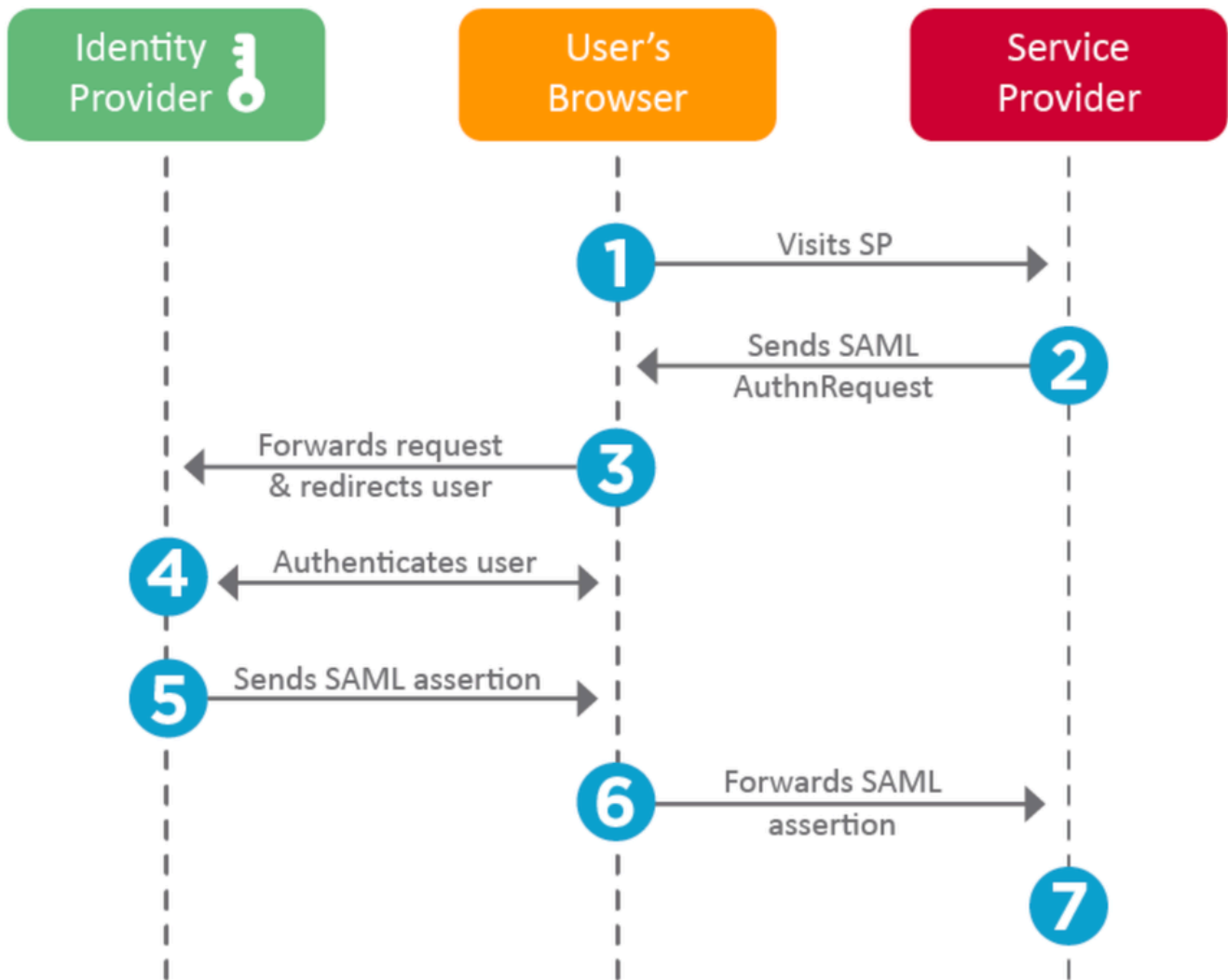
ممتي و SP ةطساوب هقيسننت ةيفيكيو هيلع يوتحي امو SAML ديكأتب تافصاوم ريفوت ممتي IdP يف هانبيعت

- EntityID - لئجست SP ل يومومع ديرف مسا - URL ناوئعك ةقسنم ةميقلا هذه ةيؤر ديازتم لئجست: <https://<FQDN-or-IPaddress>/saml/metadata>
- لئجست يف نامأ عارجإ ه - Confirmation Consumer Service (ACS) ةحص نم ققحتلا ةادأ

اذه لي غشت متي .حيحصل ACS لى SAML دي كأت لاسرا نمضي (regex) يداع ريبعت
 عقوم لىل SAML بلط يوتحي شيح SP اهأدب يتل لوخدلا ليحست تايلمع اناثا طقف
 SAML بلط عطساوب هري فوت مت يذل ACS عقوم نا اذه ACS ققدم نمضي س كلذل ACS،
 يعرش.

لاثم: <https://<FQDN-or-IPaddress>/saml/acs>

- ةمس كانه نوكي ام ةداع .ريبك دح لىل اه لكشو تامسلا ددع فلتخي نا نكمي - تامسلا
 لواحي يذل مدختس ملب صاخلا مدختس ملب مسا ةداع يهو، NameID يهو، لقألا لىل ةدحاو
 لوخدلا ليحست.
- متي . SHA-512 أو SHA-384 زارط اعويش لقأ . SHA-256 أو SAML - SHA-1 عي قوت ةيمزراوخ
 انه ةروكذملا X.509 ةداهش عم نارقتالاب ةيمزراوخلا هذه مادختسا



SP نيوكت

يف ةدح ملب تا فرعمل نم ةمدقملا تامولعمل نع مسقلا اذه ثدحتي ،هالعا مسقلا س كع لىل وعو
 تامدخلا ةمئاق.

- تامولعمل لىل يوتحي URL نا ونعك هقي سننت مت . فرعمل ل دي رفلال فرعملال - ردمصملا URL
 اهاردصا متي اهالقتي يتل SAML تا دي كأت نا نم ققحتلا نم SP نكم تي يتح IdP لوح

ح.حصل ال P فرعم نم

- ةياهن ةطقن - ةمدخلال دوزم / SAML ل SSO ةياهن ةطقن ىل ل لوخدلا ليجستل URL ناونع SAML ب ل ط عم SP ةطساوب انه هيجوتل ةداع ل دنع ةقداصلم اذبت يتل ال IdP لاثم: <https://login.microsoftonline.com/023480840129412-824812/saml2>
- ةسلج قلغت يتل ال IdP ةياهن ةطقن - (يداحأل جورخلال ليجست) SAML SLO ةياهن ةطقن IdP جورخلال ليجست قوف رقلال دعب ةداع ، SP ةطساوب انه اههيجوت ةداع ل دنع IdP لاثم: <https://access.wristbandtent.com/logout>

SAML ىل ع FMC

ثي ح ، FMC (RBAC) ضيوفت ةديجلال ةزيمال طسبت .6.7 نم FMC في SSO ةزيم ميديقت متي مدختسم ةهجاو يم دختسم ةفاك ىل ع قبطني وهو .FMC راودأل ةدوجومال تامولعملال ططخت امنأ ممدب ءالؤه موق ي ثي ح ، SAML 2.0 تافصاوم معدت ، يلالحال تقولال ي فو .FMC راودأ فو FMC نيحزانل

- اتكوا
- OneLogin
- PingID
- يد يدروزال
- (SAML 2.0 رايعم ال عم قفاوت ي حزان ي) ىرخأ

تاريذحتلال او دودحل

- ي مومع ال لاجم لل ال SSO نيوك نكمي ال
- ةيدرف ةئيهت ىل ل (HA) رفوتال جوزي في (FMC) لك يهل ةرادا في مكحتل تادحوجاتحت
- يداحأل لوخدلا ليجست نيوك ي ل حم ال/ال عال ال ي لوؤس مل طقف نكمي
- ايلخاد نيحزانل نم هؤاشن مت يذلا ةي ندمال ةمدخلال ماظن معد متي مل

نيوكتل

ةيوهل رفوم ىل ع نيوكتل

Microsoft Azure ىل ل قتنا . Azure Active Directory > Enterprise Application ىل ل لوخدلا ل جس .1 ةوطخلال Application.



Default Directory | Overview

Azure Active Directory



Switch tenant



Delete tenant



Create



Overview



Getting started



Preview hub



Diagnose and solve problems

Manage



Users



Groups



External Identities



Roles and administrators



Administrative units (Preview)



Enterprise applications



Azure Active Directory can help you enable remote

Default Directory



Search your tenant



Tenant information

Your role

Global administrator [More info](#)

License

Azure AD Free

Tenant ID

- هذه هي فحوصات و الامك، ضع م ريغ قيبطت نمض ديدج قيبطت عاشن اب مق 2. ةوطخال ةروصل:

Add your own application

Name * ⓘ

Firepower Test



Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: ⓘ

SAML-based single sign-on

[Learn more](#)

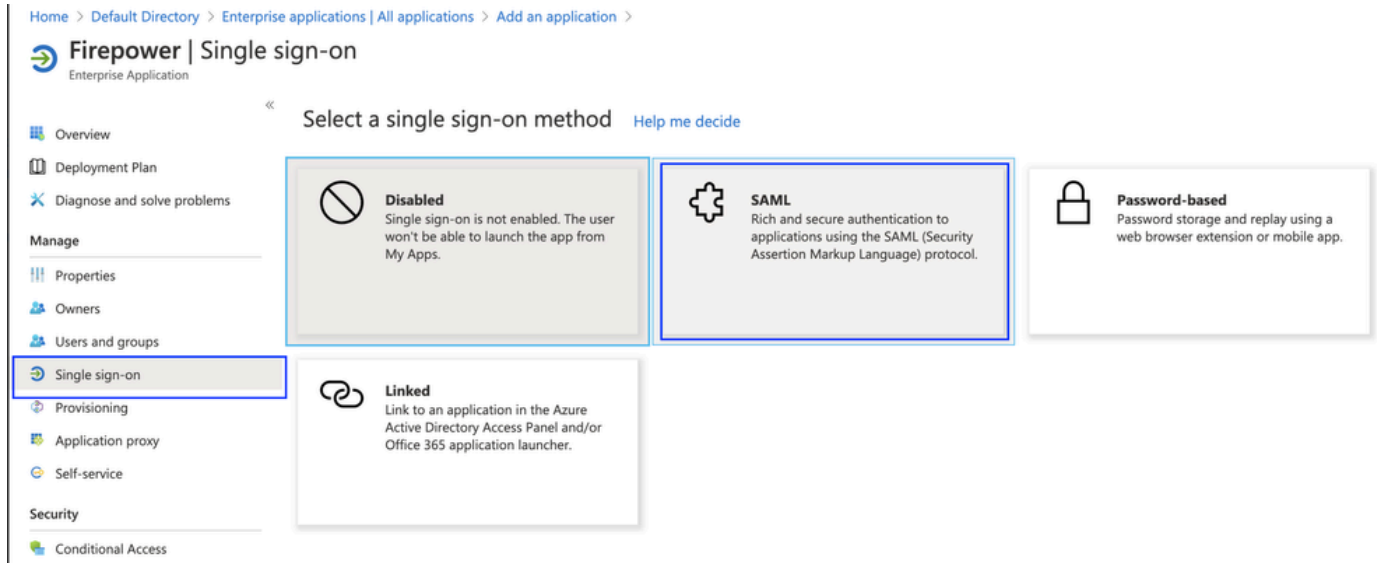
Automatic User Provisioning with SCIM

[Learn more](#)

Password-based single sign-on

[Learn more](#)

SAML، > دحاو لوخد ليجست دادعإل حفصتو هؤاشن| مت يذلا قيبتتال ريرحتب مق 3. ةوطخل ةروصلال هذه يف حضوم وه امك



FMC: ليصافت ريفوتو يساسأل SAML نيوكت ريرحت 4. ةوطخل

- فMC ل URL ناونع: <https://<FMC-FQDN-or-IPaddress>>
- (ةدحول فرعم) فرعمل: <https://<FMC-FQDN-or-IPaddress>/saml/metadata>
- درلاب صاخال URL ناونع: <https://<FMC-FQDN-or-IPaddress>/saml/acs>
- URL ل لوخدلا ليجست: <https://<FMC-QDN-or-IPaddress>/saml/acs>
- RelayState:/ui/login

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Provisioning logs (Preview)

« [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) | [Got feedback?](#)

Read the [configuration guide](#) for help integrating Cisco-Firepower.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	https://10.106.46.191/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://10.106.46.191/saml/acs
Sign on URL	https://10.106.46.191/saml/acs
Relay State	/ui/login
Logout Url	Optional

2 User Attributes & Claims [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
roles	user.assignedroles
Unique User Identifier	user.userprincipalname
Group	user.groups

3 SAML Signing Certificate [Edit](#)

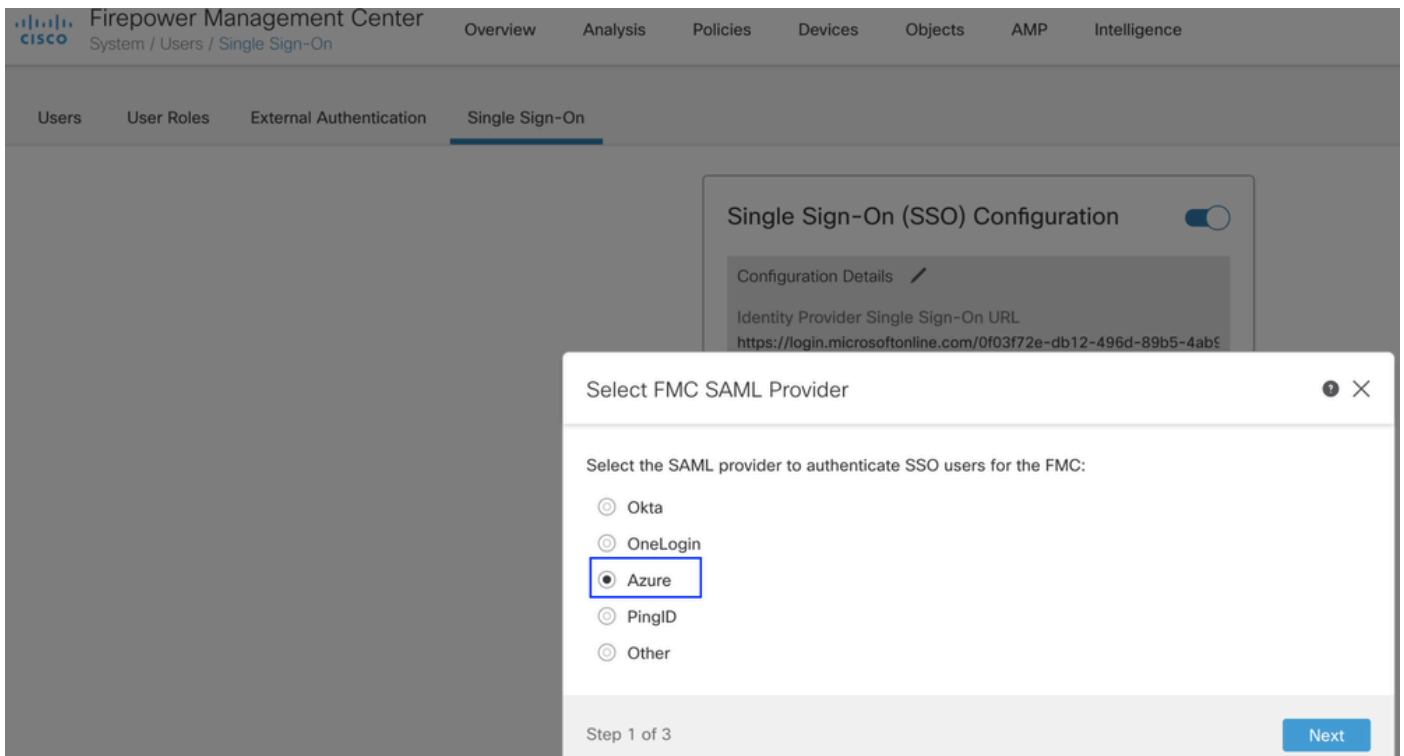
Status	Active
Thumbprint	<div style="background-color: black; width: 100px; height: 15px;"></div>
Expiration	
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

دنتسمل لوصولل يفاضل لكش ب رمأل اذه ةشقانم متت - يضارتفاك يقابلاب ظافتحال راودأل إلى.

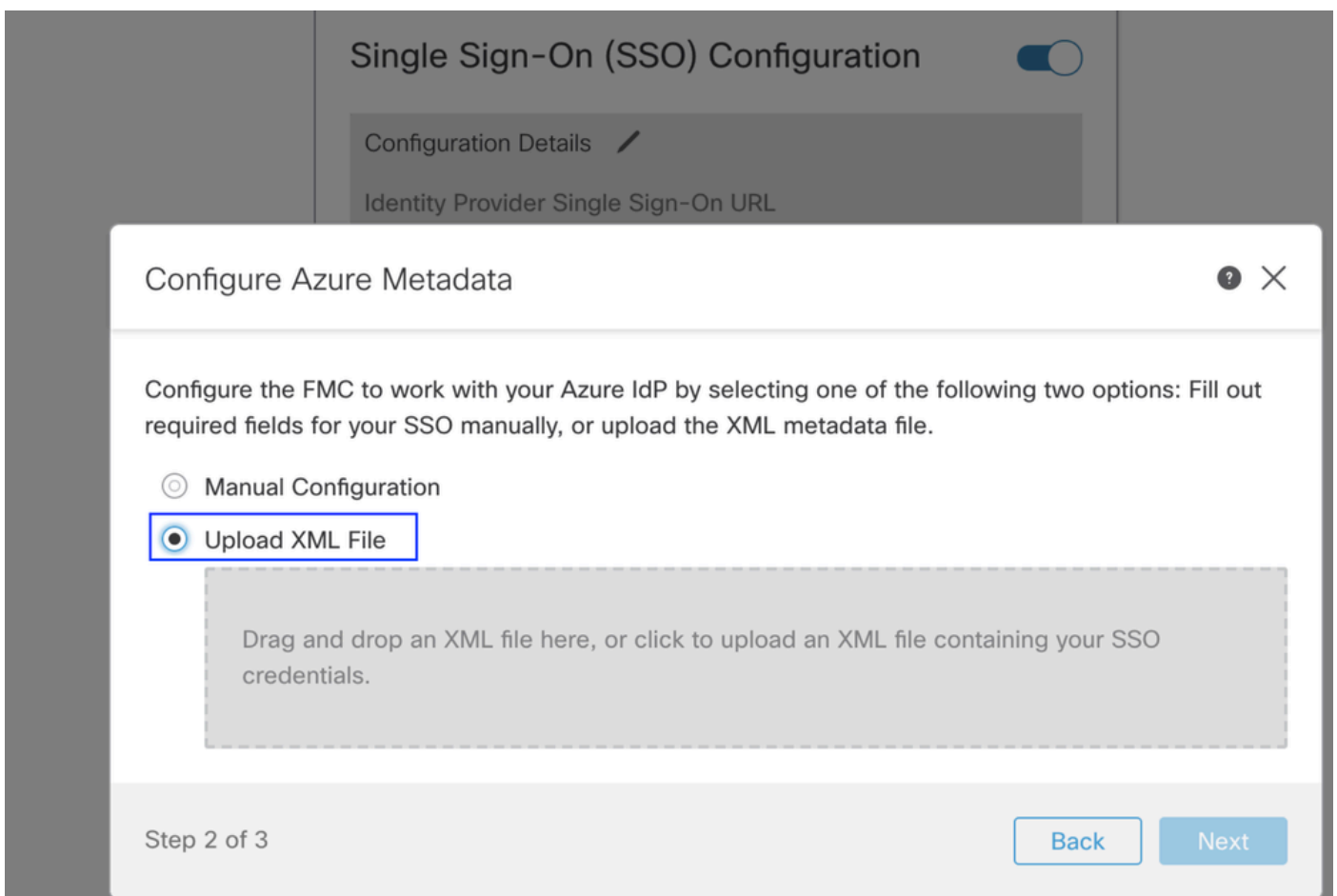
يذل داحتال فيرعت تانايلبل XML ليزنت. ةيوهال رفوم نيوكت ةياهن لىل ةمالع عضي اذهو FMC. نيوكتل همادختسا متي

Firepower ةرادل زكرم لىل ع نيوكتل

لوخدال ليجست > نيمدختسمل > تادادعال إلى لىل لقتنا، FMC إلى لوخدال لىل جس 1. ةوطخل رفومك Azure دح. SSO نيومتوي دخال



عيج ميمعتب ايئاقلت موقوي. انه Azure نم هل يزنن مت يذلا XML فلم لي محت. 2 ةوطخلال ةبولطم لال لي صافات لال.



ةروصلال هذه يف حضورم وه امك، ظفح قوف رقناو نيوكتال نم ققحت. 3 ةوطخلال

Verify Azure Metadata

Test the Azure metadata by clicking the **Test Configuration** button on the **System / Users / Single Sign-On** page after you save.)

Identity Provider Single Sign-On URL

Identity Provider Issuer

X.509 Certificate

Step 3 of 3

[Back](#) [Save](#)

Azure RBAC - مدمقتم نيوكت

Azure ىلع قيبتل نايب ريرحت بچي - FMC راودأ نييعتلة فلتم راودأ عاونأ مادختسال ةيلاخ ةميقي ىلع راودألا يوتحت، يضارتفا لكش ب. راودألل ميقي نييعتله.

يدألا لوخدلا ليچست قوف رقناو هؤاشنإ مت يذلا قيبتل ىلإ لقتنا 1. ةوطخلا

Cisco-Firepower

Search (Cmd+/) <<

 Delete  Endpoints

- Overview
- Quickstart
- Integration assistant (preview)


Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Display name : Cisco-Firepower
Application (client) ID :
Directory (tenant) ID :
Object ID :

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Mic

Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

ديحت و راودألا :مسالاب ةديج ةبلاطم ةفاضلا .تابلاطمل او مدختس مل تامس ريحت 2. ةوطخلا
user.Assignedroles. ةميقللا

User Attributes & Claims

+ Add new claim + Add a group claim ≡ Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***
roles	user.assignedroles ***

قېسىن تېب فل م ل . ن ا ي ب ل ا ر ي ر ح ت ب م ق . <Application-Name> > Manifest . ي ل ا ل ق ت ن ا . 3 . ة و ط خ ل ا ن ي ر و د ء ا ش ن ا م ت ي ا ن ه - ل ا ث م ل ا ل ي ب س ي ل ع . خ س ن ل ل ي ض ا ر ت ف ا م د خ ت س م ر ف و ت ي و JSON ل ل ح م ل ا و م د خ ت س م ل ا .

Cisco-Firepower | Manifest

Search (Cmd+)



Save



Discard



Upload



Download



Got feedback?

- Overview
- Quickstart
- Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)

Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

The editor below allows you to update this application by directly modifying its JSON representation.

```
1 {
2   "id": "00f52e49-10a0-4580-920f-98aa41d58f6f",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": false,
7   "appId": "51dcc017-6730-41ee-b5cd-4e5c380d85c3",
8   "appRoles": [
9     {
10      "allowedMemberTypes": [
11        "User"
12      ],
13      "description": "Analyst",
14      "displayName": "Analyst",
15      "id": "18d14569-c3bd-439b-9a66-3a2aee01d13f",
16      "isEnabled": true,
17      "lang": null,
18      "origin": "Application",
19      "value": "Analyst-1"
20    },
21    {
22      "allowedMemberTypes": [
23        "User"
24      ],
25      "description": "User",
26      "displayName": "User",
27      "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",
28      "isEnabled": true,
29      "lang": null,
30      "origin": "Application",
31      "value": "User-1"
32    }
33  ]
34 }
```

مذخست سمل ريرحتب مق .تاعومجمل او نومذخت سمل <application-name> يلى لقتنا . 4 ةوطخلا ةروصلا هذه يف حضوم وه امك ، اثيدح اهؤاشن مت يتلا راودال نييعتو .

Edit Assignment

Default Directory

Users

1 user selected.

Select a role

None Selected

Assign

Select a role

Only a single role can be selected

Enter role name to filter items...

Analyst

User

Selected Role

Analyst

Select

مق: ةومجملا وضع ةمس، ل SSO في مدقتملا نيوكتلا ررحو FMC ىلى لوخدلا ل جس. 4 ةوطخال راودألل قيبتاتلا نايب في هريفوتب تمق يذلا ضرعلا مسا نييعتب

Advanced Configuration (Role Mapping)

Default User Role

Administrator

Group Member Attribute

roles

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

نعم العمل مه رودى الى لود دلا لى جست ك نكمى ، ك لذب ما يقى ل درجم بو .

ة حصلا نم ققحتلا

نم (FMC) ةسسألا ةحوللا ةرادى فى مكحتلا ةدحوب صاخلا URL ناو نع لى لقتنا . 1 ةوطخلا حضورم وه امك ، يدألا لود دلا لى جست لى رقتنا . <https://<FMC URL>> :كب صاخلا ضرعتسملا ةروصلا هذه فى .



Firepower Management Center

Username

Password

Single Sign-On

Log In

ليجست يدؤيسو Microsoft لي لوخدلا ليحست ةحفص لي كهيجوت ةداع لك لذ دع ب متت FMC ل ةيضارتفال ةحفصل اعجارا لي احانلا لوخدلا

هتفاضل تمت يذلا SSO مدختسم ةيؤرل ني مدختسم > ماظن لي لقتنا ، FMC ي ف 2. ةوطخلل اتانايبل ةدعاق لي

test1@shbharticisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbharticisco.onmicrosoft.com

Administrator

External (SSO)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومجم مادختساب دن تسمل اذو Cisco تمچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم ميققتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاخلا مهتغب
Cisco يلخت. فرتم مچرت مامدقئ يتل ةيفارتحال ةمچرتل عم لالحل و
ىلإ أمئاد عوچرلاب يصوت و تامچرتل هذه ةقदन ةتئل وئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزئلچنل دن تسمل