

FMC SSO configureren als identiteitsprovider

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[IDp-configuratie](#)

[SP-configuratie](#)

[SAML op FMC](#)

[Beperkingen en beperkingen](#)

[Configureren](#)

[Configuratie van identiteitsproviders](#)

[Configuratie van FireSIGHT Management Center](#)

[Geavanceerde configuratie - RBAC met KRK](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Logbestanden van browser SAML](#)

[FMC SAML-vastlegging](#)

Inleiding

In dit document wordt beschreven hoe u het FireSIGHT Management Center (FMC) Single Sign-On (SSO) kunt configureren met AVC als Identity Provider (IDP).

Security Association Markup Language (SAML) is meestal het onderliggende protocol dat SSO mogelijk maakt. Een bedrijf behoudt één inlogpagina, achter deze pagina staat een identiteitswinkel en verschillende verificatieregels. U kunt eenvoudig elke webapp configureren die SAML ondersteunt, zodat u kunt inloggen in alle webtoepassingen. Het heeft ook het veiligheidsvoordeel dat het gebruikers niet dwingt om wachtwoorden te onderhouden (en mogelijk te hergebruiken) voor elke webapp waar ze toegang toe hebben, of om wachtwoorden aan die webapps bloot te stellen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisbegrip van FireSIGHT Management Center
- Basisbegrip van één enkele aanmelding

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Firepower Management Center (FMC) versie 6.7.0
- karwei - IDP

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

SAML-afsluitingen

De configuratie voor SAML moet op twee plaatsen worden uitgevoerd: bij de IDP en bij de SP. De IDP moet zo worden geconfigureerd dat deze weet waar en hoe u gebruikers kunt verzenden als ze willen inloggen in een specifiek SP. SP moet worden geconfigureerd zodat hij weet dat hij SAML-beweringen kan vertrouwen die door de IDP zijn ondertekend.

Definitie van enkele termen die de kern van SAML vormen:

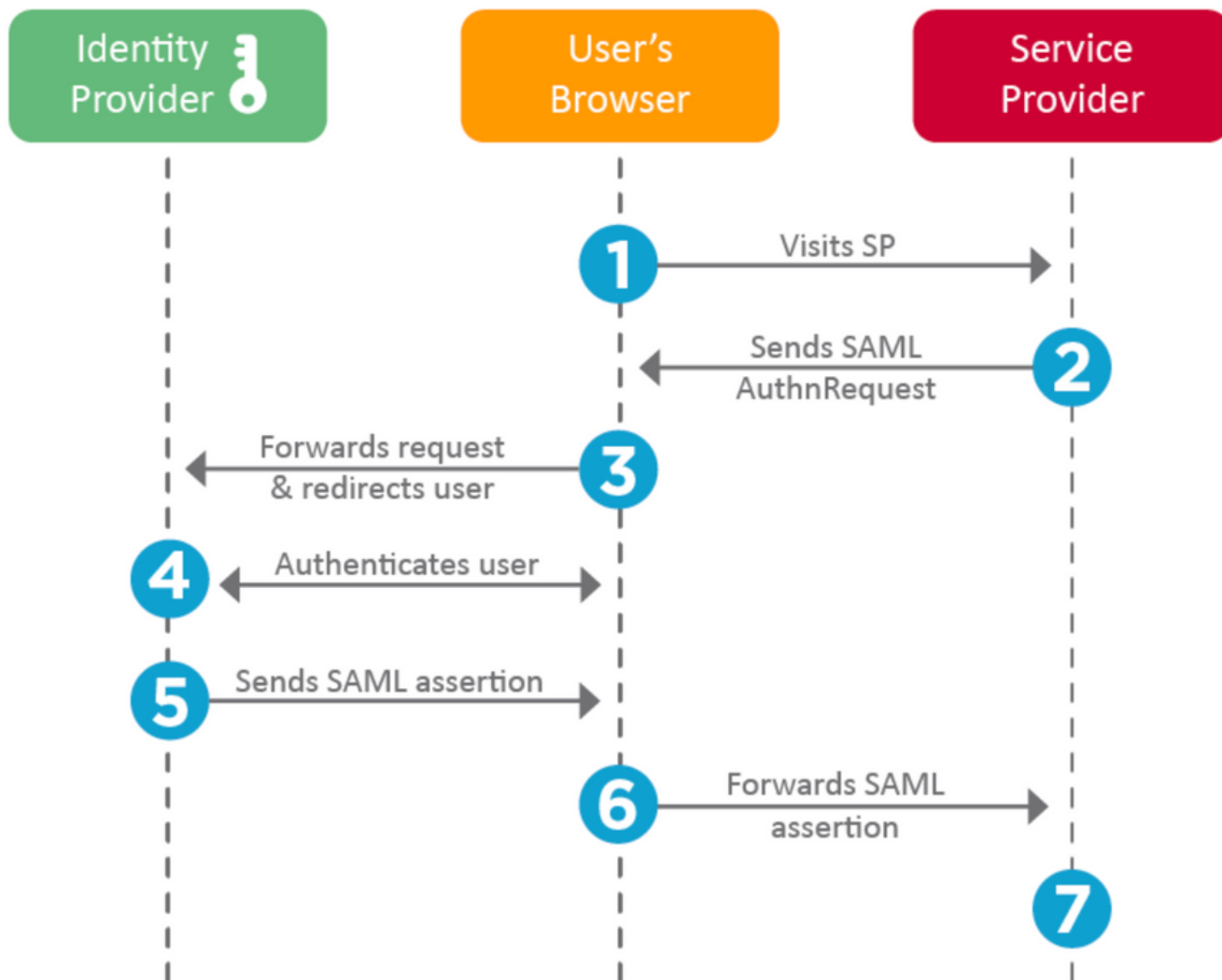
- Identity Provider (IDP) - Het software-gereedschap of de service (vaak gevisualiseerd door een inlogpagina en/of dashboard) die de verificatie uitvoert; controleert de gebruikersnaam en de wachtwoorden, controleert de status van de rekening, beroept zich op twee factoren, enz.
- Service Provider (SP) - De webtoepassing waar de gebruiker toegang probeert te verkrijgen.
- SAML Assering - Een bericht waarin de identiteit van een gebruiker en vaak andere eigenschappen wordt bevestigd, verzonden over HTTP via browser-omleidingen

IDp-configuratie

Specificaties voor een SAML bewering, wat het moet bevatten en hoe het moet worden geformatteerd, worden verstrekt door de SP en ingesteld op de IDP.

- EntiteitID - Een globaal unieke naam voor de SP. De formaten variëren, maar het is steeds gebruikelijker om deze waarde te zien die als een URL wordt geformatteerd.
Voorbeeld: <https://<FQD-or-IP-adres>/saml/metadata>
- Betrouwbaarheidsdienst (ACS) Geldigheidsinstelling - Een veiligheidsmaatregel in de vorm van een reguliere expressie (regex) die garandeert dat de SAML-bewering naar de juiste ACS wordt verzonden. Dit komt alleen in werking tijdens SP-geïnitieerde logins waar het SAML-verzoek een ACS-locatie bevat, zodat deze ACS-validator ervoor zou zorgen dat de door SAML opgegeven ACS-locatie legitiem is.
Bijvoorbeeld: <https://<FQDN-or-IPadres>/saml/acs>
- Eigenschappen - Het aantal en het formaat van eigenschappen kan sterk verschillen. Er is gewoonlijk ten minste één eigenschap, de naamID, die gewoonlijk de gebruikersnaam is van de gebruiker die probeert in te loggen.

- Algoritme van SAML - SHA-1 of SHA-256. Minder gebruikelijk SHA-384 of SHA-512. Dit algoritme wordt gebruikt in combinatie met het X.509-certificaat, wordt hier vermeld.



SP-configuratie

De achterkant van de bovenstaande sectie verwijst naar informatie die door de IDP is verstrekt en op de SP is ingesteld.

- URL van de uitgevende instelling - Uniek identificatienummer van de IDP. Opgemaakt als een URL met informatie over IDP zodat SP kan valideren dat de SAML bewerkingen die het ontvangt van de juiste IDP worden uitgegeven.
Bijvoorbeeld: <saml:emittent <https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/> >
- SAML SSO Endpoint / Login URL van serviceproviders - Een IDP-eindpunt dat verificatie initieert wanneer u deze door de SP-modus herleid hebt met een SAML-verzoek.
Bijvoorbeeld: <https://login.microsoftonline.com/023480840129412-824812/saml2>
- SAML SLO (Single Log-out) Endpoint - Een IDP-eindpunt dat uw IDP-sessie sluit wanneer u hier door de SP opnieuw geregistreerd wordt, doorgaans nadat op **log out** is gedrukt.
Bijvoorbeeld: <https://access.wristbandtent.com/logout>

SAML op FMC

De SSO-functie in het VCC is ingevoerd vanaf 6.7. De nieuwe functie vereenvoudigt de VMC- autorisatie (RBAC), omdat de informatie die bestaat op de FMC Roles in kaart wordt gebracht. Het is van toepassing op alle FMC UI-gebruikers en FMC-rollen. Op dit moment ondersteunt het SAML 2.0 Specificatie en deze ondersteunde IDP's

- OKTA
- OneLogin
- PingID
- AD
- Overige (elke IDP die voldoet aan SAML 2.0)

Beperkingen en beperkingen

- SSO kan alleen worden ingesteld voor het Global Domain.
- FMC's in HA-air moeten individueel worden geconfigureren.
- Alleen lokale/AD-managers kunnen één aanmelding configureren.
- SSO gestart vanaf Idp wordt niet ondersteund.

Configureren

Configuratie van identiteitsproviders

Stap 1. Meld u aan bij Microsoft Outlook. Navigeer naar **actieve map > Enterprise Application**.

Default Directory | Overview

Azure Active Directory

Overview

Getting started

Preview hub

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units (Preview)

Enterprise applications

Switch tenant Delete tenant Create

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

- Step 2. Maak **een nieuwe toepassing** onder deze afbeelding.

[Home](#) > [Default Directory](#) > [Enterprise applications | All applications](#) > [Add an application](#) >

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](#)

Step 3. Bewerk de toepassing die is gemaakt en navigeer om **één teken in te stellen op > SAML**, zoals in deze afbeelding.

Home > Default Directory > Enterprise applications | All applications > Add an application >

Firepower | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access

Select a single sign-on method [Help me decide](#)

Disabled

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based

Password storage and replay using a web browser extension or mobile app.

Linked

Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Stap 4. Bewerk de basisconfiguratie van SAML en specificeer de FMC-details:

- FMC-URL: <https://<FMC-FQDN-of-IP-adres>>
- Identificatiecode (entiteit-ID): <https://<FMC-FQDN-of-IP-adres>/saml/metadata>
- URL: <https://<FMC-FQDN-of-IP-adres>/saml/AC's>
- Aanmelden URL: <https://<FMC-QDN-of-IP-adres>/saml/acs>
- RelayState:/ui/aanmelding

Enterprise Application

- 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.

- 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
- 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
- SAML Signing Certificate** [Edit](#)

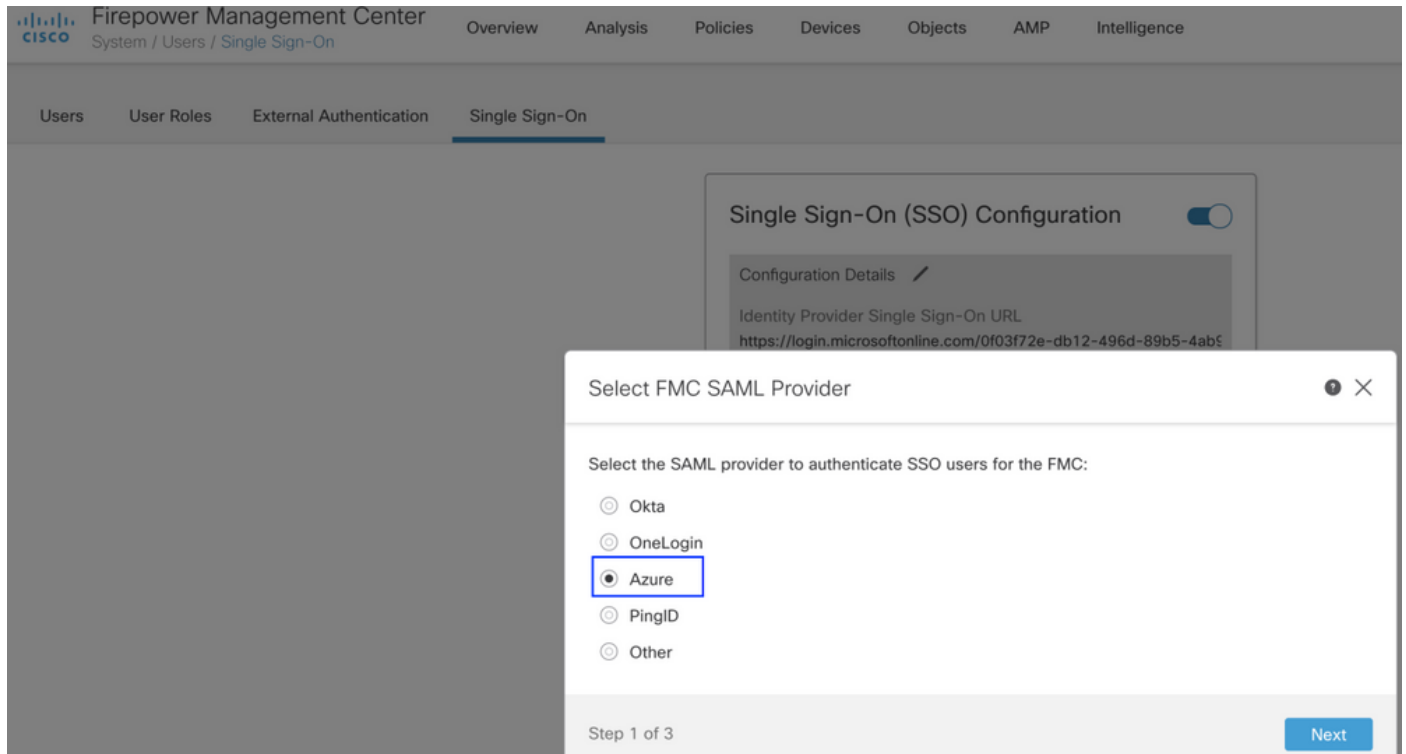
Status	Active
Thumbprint	[REDACTED]
Expiration	[REDACTED]
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Houd de rest standaard - dit wordt verder besproken voor Rol-gebaseerde toegang.

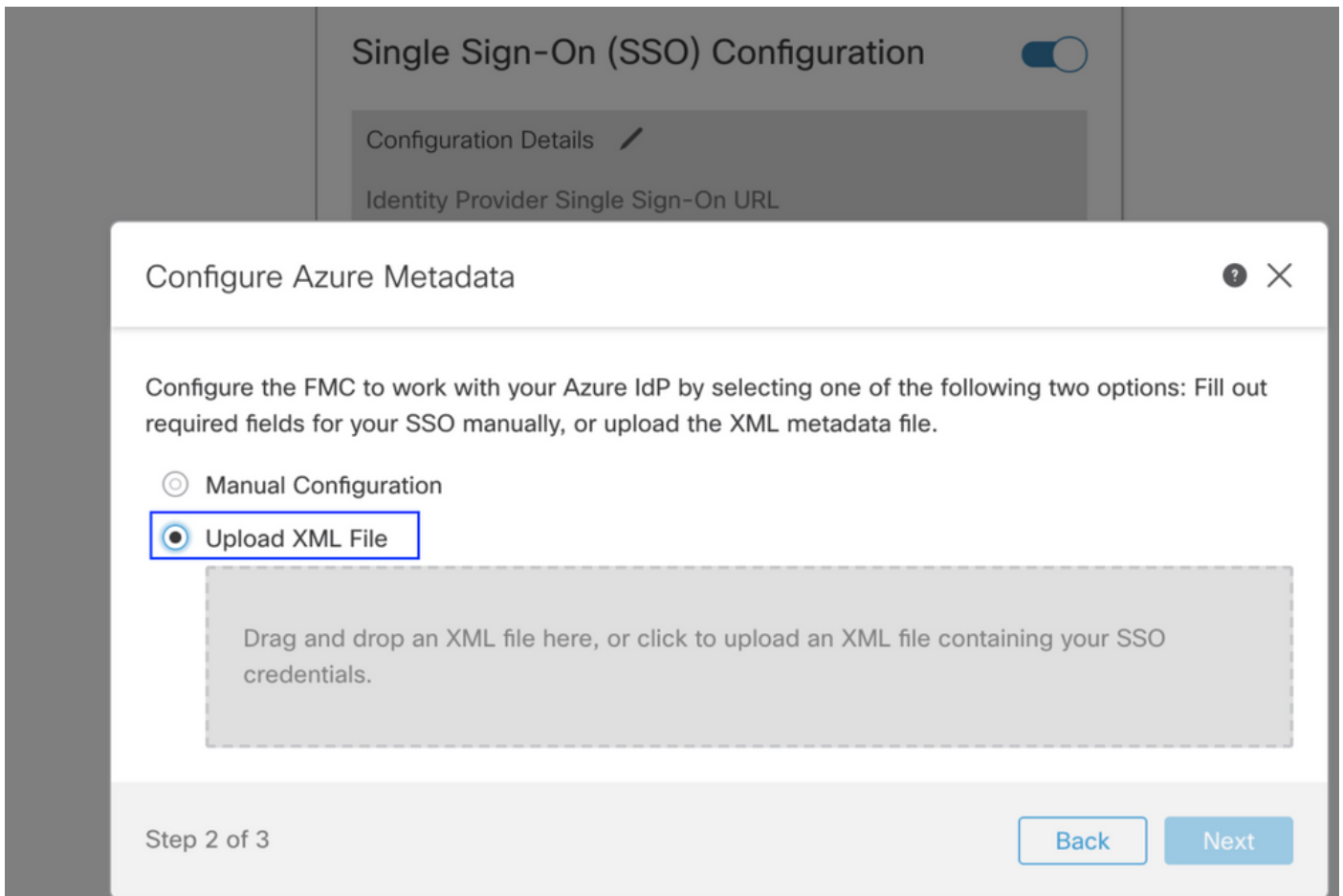
Dit markeert het einde van de configuratie van de Identity Provider. Downloadt de Federatie Metagegevens XML die voor FMC-configuratie zullen worden gebruikt.

Configuratie van FireSIGHT Management Center

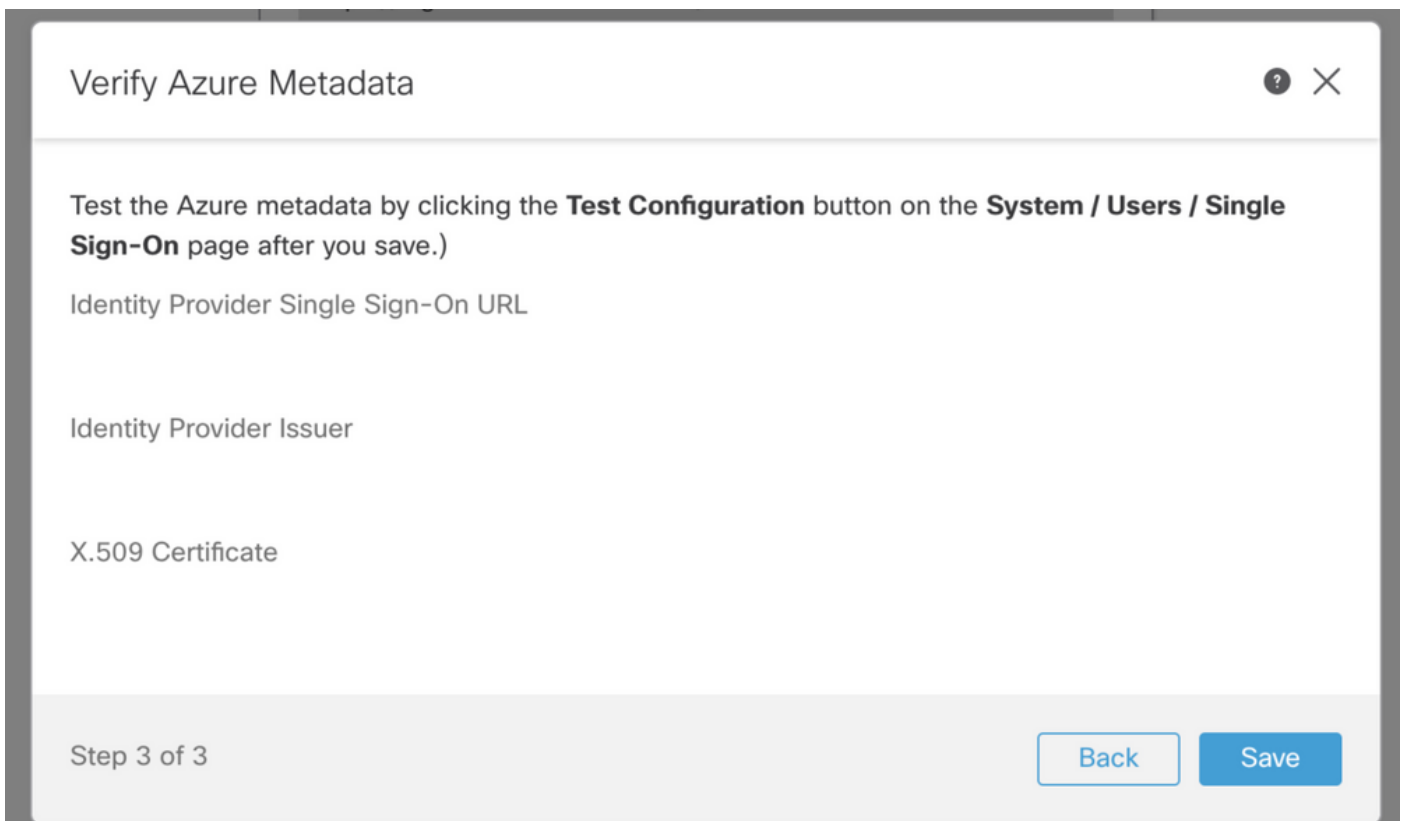
Stap 1. Meld u aan bij FMC, navigeer naar **Instellingen > Gebruikers > Enkelvoudig aanmelding en SSO inschakelen**. Selecteer **RKI** als Provider.



Stap 2. Upload het XML-bestand dat hier wordt gedownload van de KRKI. Het vult alle benodigde details automatisch.



Stap 3. Controleer de configuratie en klik op **Opslaan**, zoals in deze afbeelding.



Geavanceerde configuratie - RBAC met KRK



Om verschillende roltypes te gebruiken om aan Roles of FMC in kaart te brengen - moet je het

manifest van de Toepassing op de KRI bewerken om waarden aan rollen toe te wijzen. Standaard hebben de rollen waarde als leeg.

Stap 1. Navigeer naar de **toepassing** die wordt gemaakt en klik op **Enkelvoudig aanmelding**.

Home > Default Directory | App registrations >

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 Authentic 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](#)

Stap 2. Bewerk de gebruikerskenmerken en -claims. Voeg een Nieuwe claim met Naam toe: **rollen** en selecteer de waarde als **door gebruiker.Toewijzende rollen**.

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 ***

Stap 3. Navigeer naar **<Application-name> > manifest**. Bewerk het manifest. Het bestand is in JSON-indeling en er is een standaardgebruiker beschikbaar om te kopiëren. Bijvoorbeeld - hier worden 2 rollen gecreëerd: Gebruiker en Analyst.

Cisco-Firepower | Manifest



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 represe

```
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     {
23       "allowedMemberTypes": [
24         "User"
25       ],
26       "description": "User",
27       "displayName": "User",
28       "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",
29       "isEnabled": true,
30       "lang": null,
31       "origin": "Application",
32       "value": "User-1"
33     },
34   ]
35 }
```

Stap 4. Navigeer naar **<Application-naam> gebruikers en groepen**. Bewerk de gebruiker en deel de nieuwe rollen toe, zoals in deze afbeelding.

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

Stap 4. Meld u aan bij FMC en bevestig de geavanceerde configuratie in de BZB. voor, Kenmerk groepsid: awijs de **naam van het display** die u in Toepassingsmanifest hebt opgegeven, aan de rollen toe.

▼ 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

User

Analyst

Als dat eenmaal is gebeurd, moet je in staat zijn in te loggen op hun specifieke rol.

Verifiëren

Stap 1. Navigeer naar de FMC URL van uw browser: <https://<FMC URL>>. Klik op **Enkelvoudige aanmelding**, zoals in deze afbeelding.



Firepower Management Center

Username

Password

Single Sign-On

Log In

U wordt teruggestuurd naar de Microsoft inlogpagina en als u met succes inlogt, wordt de standaardpagina van FMC hersteld.

Stap 2. Op FMC navigeer naar **Systeem > Gebruikers** om de SSO-gebruiker aan de database te zien toevoegen.

test1@shbhartiscisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbhartiscisco.onmicrosoft.com

Administrator

External (SSO)

Problemen oplossen

Controleer de SAML-verificatie en dit is de werkschema's die u met succes hanteert (Dit beeld is van een labomgeving):

Logbestanden van browser SAML

GET	https://10.106.46.191/sso/saml/login	
GET	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/saml2?RelayState=7_ni-J1fNA5eEeVvoAuhcviH6CwKjxwyGhnxJpArDjKAFMbK-wvJ2RSP&SAML	SAML
GET	https://login.live.com/Me.htm?v=3	
POST	https://login.microsoftonline.com/common/GetCredentialType?mkt=en-US	
POST	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/login	
GET	https://login.live.com/Me.htm?v=3	
POST	https://login.microsoftonline.com/kmsi	
POST	https://10.106.46.191/saml/acs	SAML
GET	https://login.microsoftonline.com/favicon.ico	
GET	https://10.106.46.191/sso/saml/login	
GET	https://10.106.46.191/ui/login	
POST	https://10.106.46.191/auth/login	

FMC SAML-vastlegging

Controleer de SAML-vastlegging op FMC op `/var/log/auth-daemon.log`

```
root@shbharti1ffncl1:/var/log# tail -f auth-daemon.log
auth-daemon 2020/08/09 04:59:11 I! Writing Audit Log to DB.
auth-daemon 2020/08/09 04:59:11 I! Parsing SAML ACS Response
auth-daemon 2020/08/09 04:59:11 I! SAML ACS Response Parsed, ID: id-56574e8a5f44bdd58102743d2cc9350b75f74d8c
auth-daemon 2020/08/09 04:59:11 I! Authorizing Response, ID : id-56574e8a5f44bdd58102743d2cc9350b75f74d8c
auth-daemon 2020/08/09 04:59:11 I! No member value in Data. Using Default Role.
auth-daemon 2020/08/09 04:59:11 I! Attribute Map in the token : map[http://schemas.microsoft.com/claims/authmethodsreferences:[http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password]
http://schemas.microsoft.com/identity/claims/objectid:[b5-4ab9fc80d8aa/] http://schemas.microsoft.com/identity/claims/objectid:[a] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname:[Test 1] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[test@shbhartiCisco.onmicrosoft.com] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:[Guy]
mapped_role_uid:[bee2eb18-e129-11df-a04a-42c66f0a3b36]]
auth-daemon 2020/08/09 04:59:11 I! Redirecting ID : id-56574e8a5f44bdd58102743d2cc9350b75f74d8c, URI : /sso/saml/login
```