FMC SSO configureren als identiteitsprovider

Inhoud

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

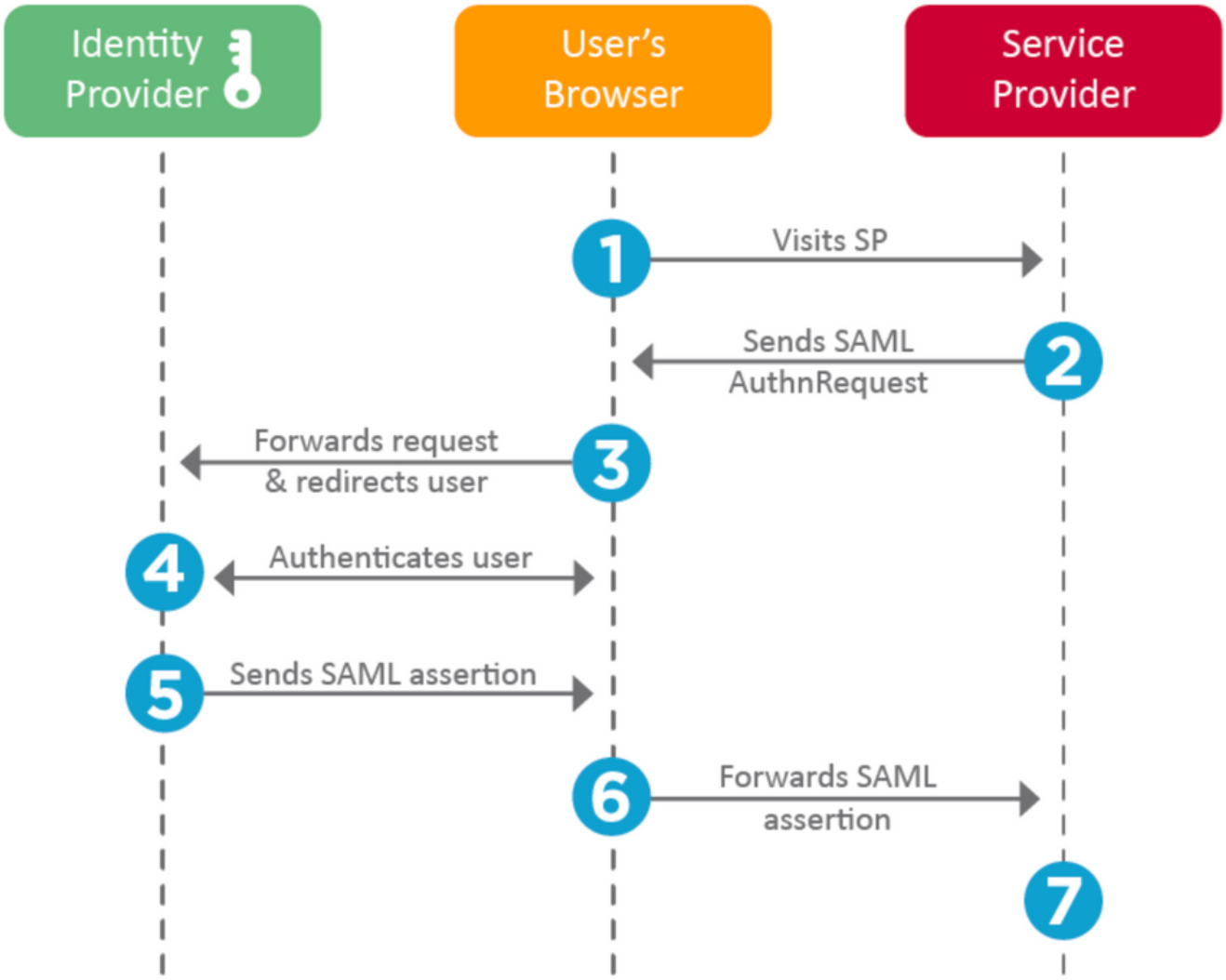
Specificaties voor een SAML bewering, wat het moet bevatten en hoe het moet worden geformatteerd, worden verstrekt door de SP en ingesteld op de IDP.

- 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 beweringen 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 geregisseerd 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)

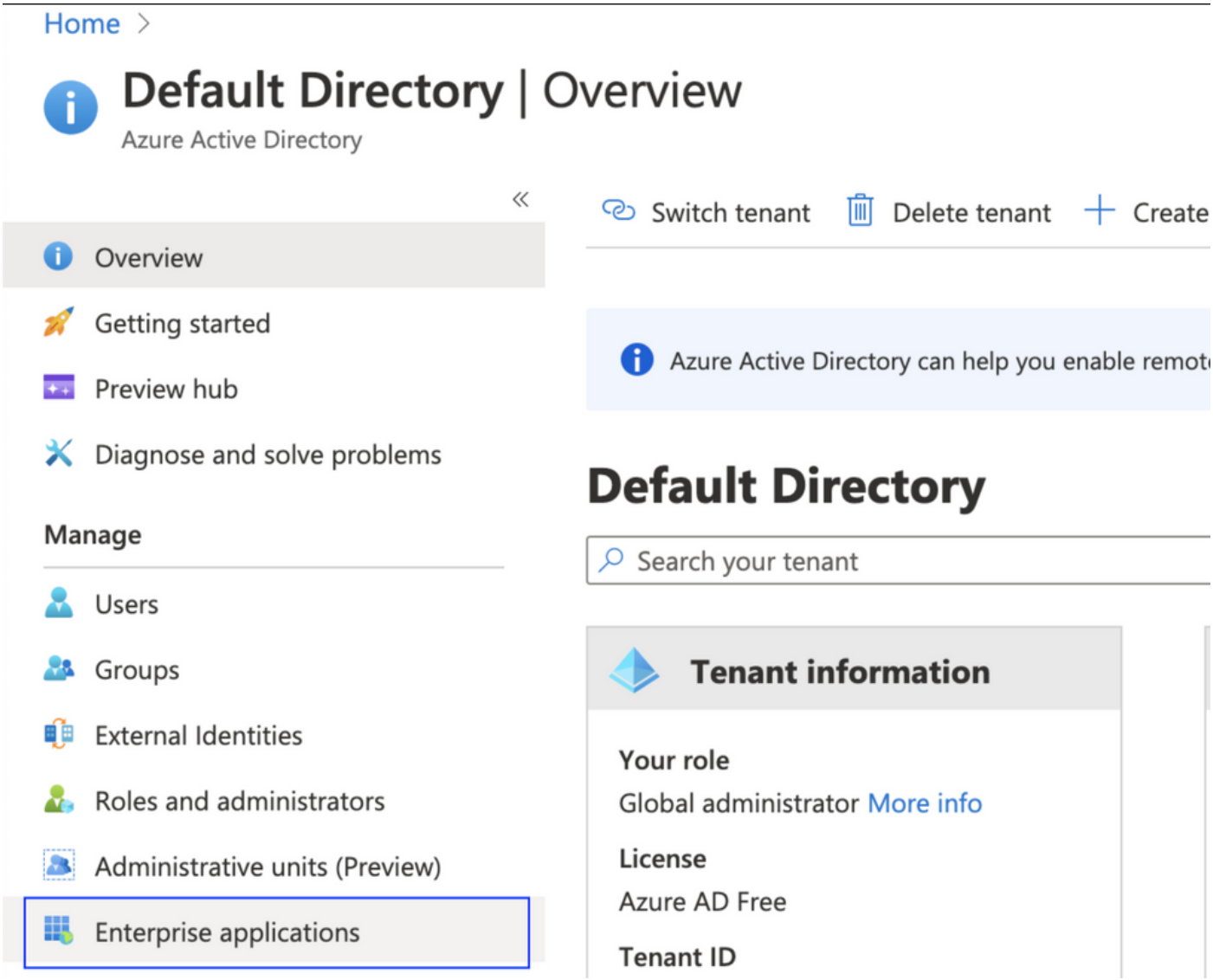
Beperkingen en beperkingen

- 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.

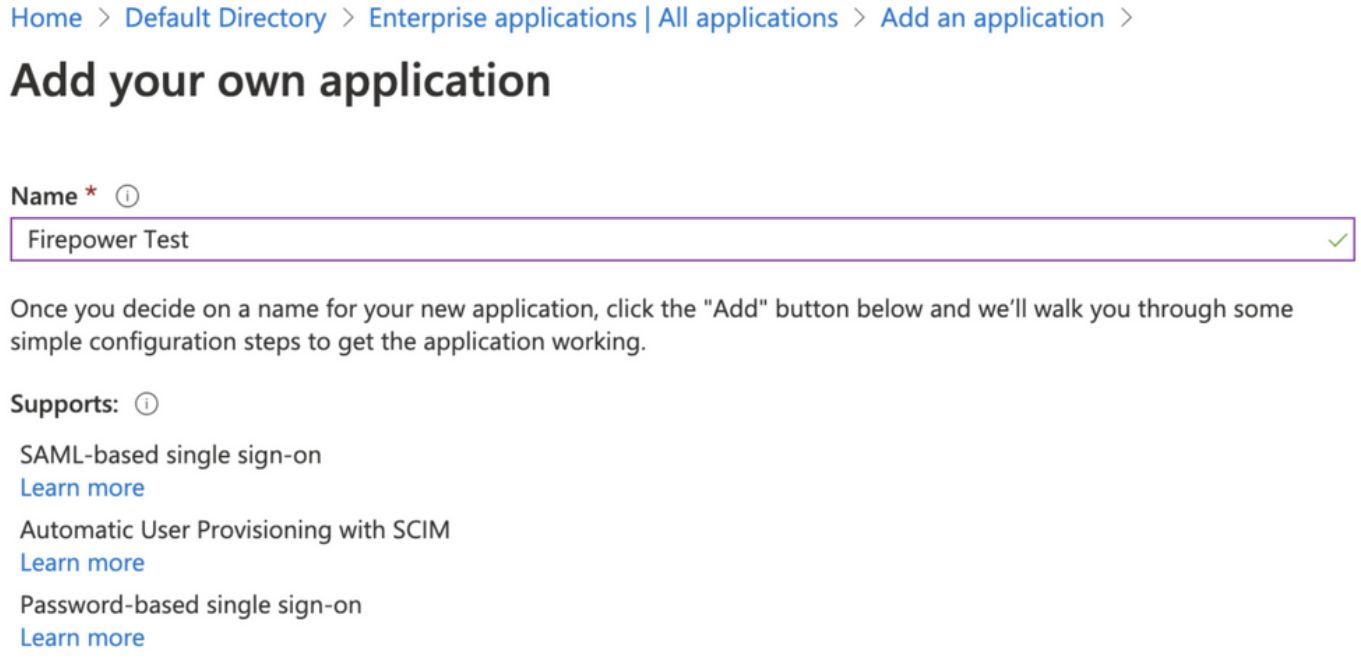
Configureren

Configuratie van identiteitsproviders

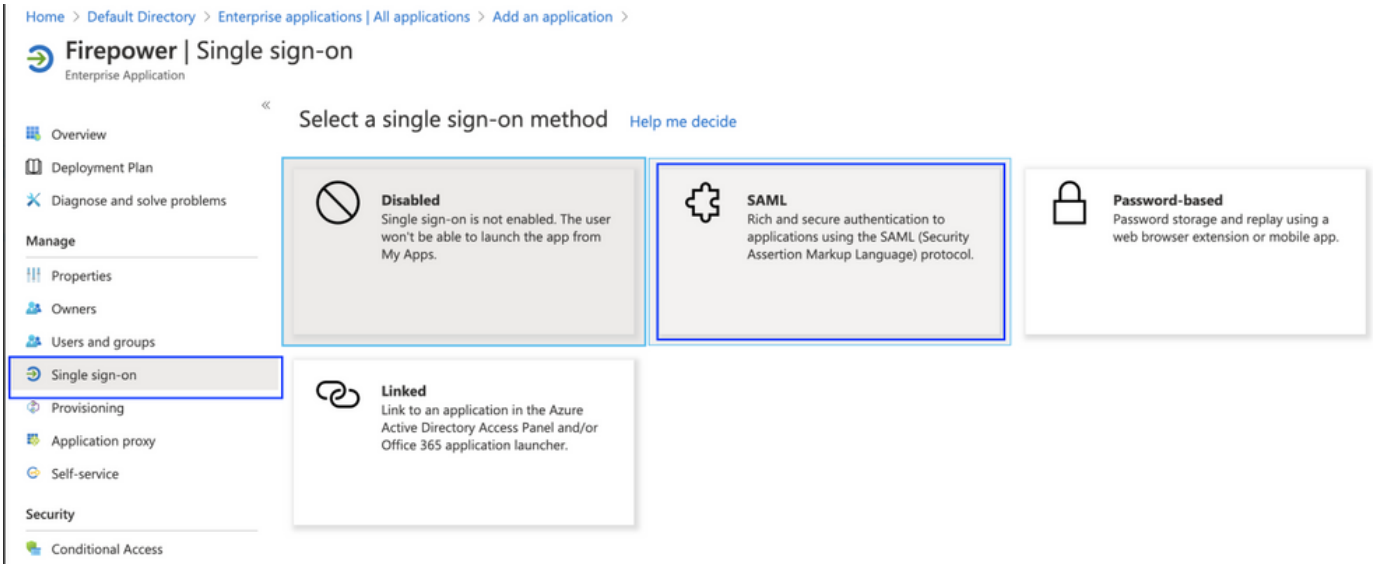
Stap 1. Meld u aan bij Microsoft Outlook. Navigeer naar **actieve map > Enterprise Application**.



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

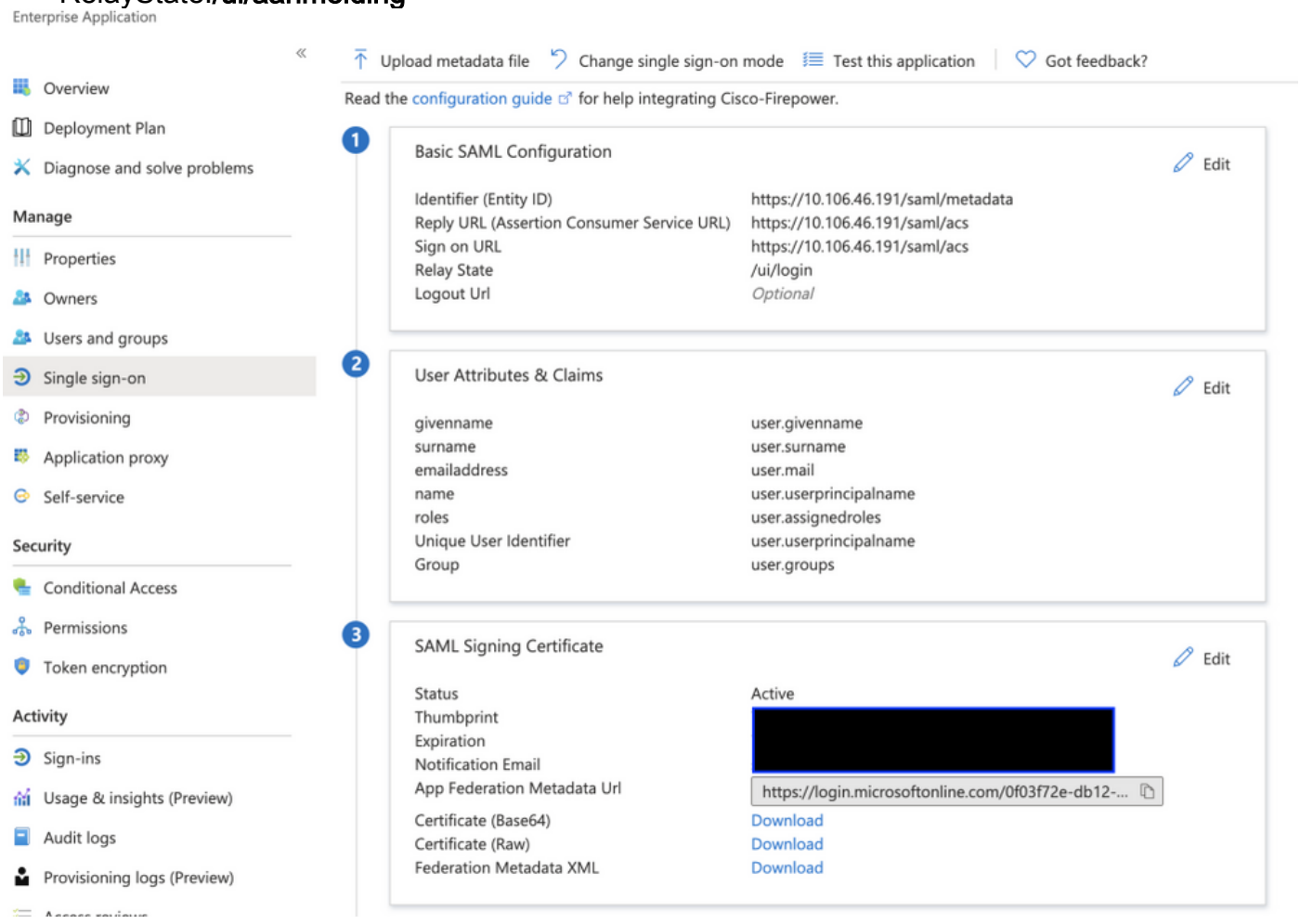


Stap 3. Bewerk de toepassing die is gemaakt en navigeer om **één teken in te stellen op > SAML**, zoals in deze afbeelding.



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**

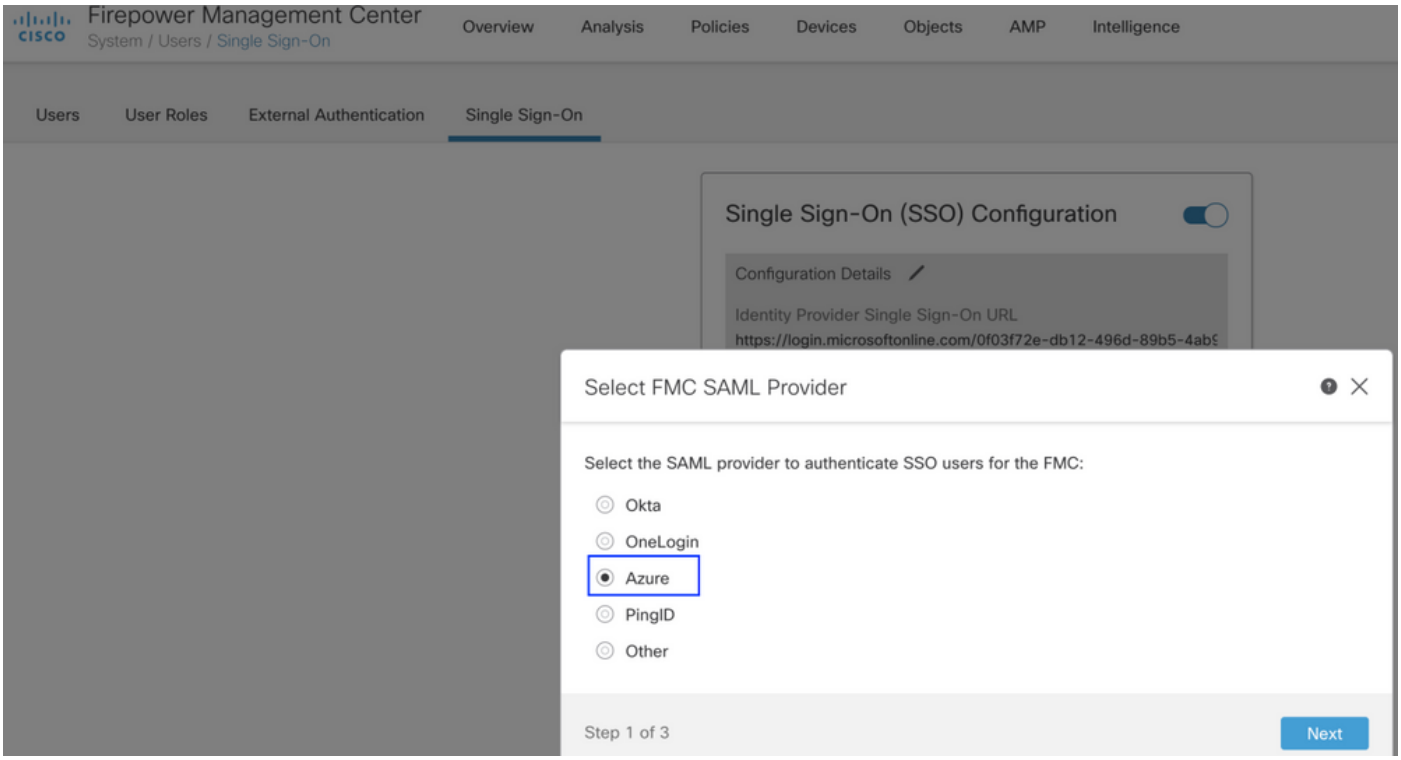


Houd de rest standaard - dit wordt verder besproken voor Rol-gebaseerde toegang.

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

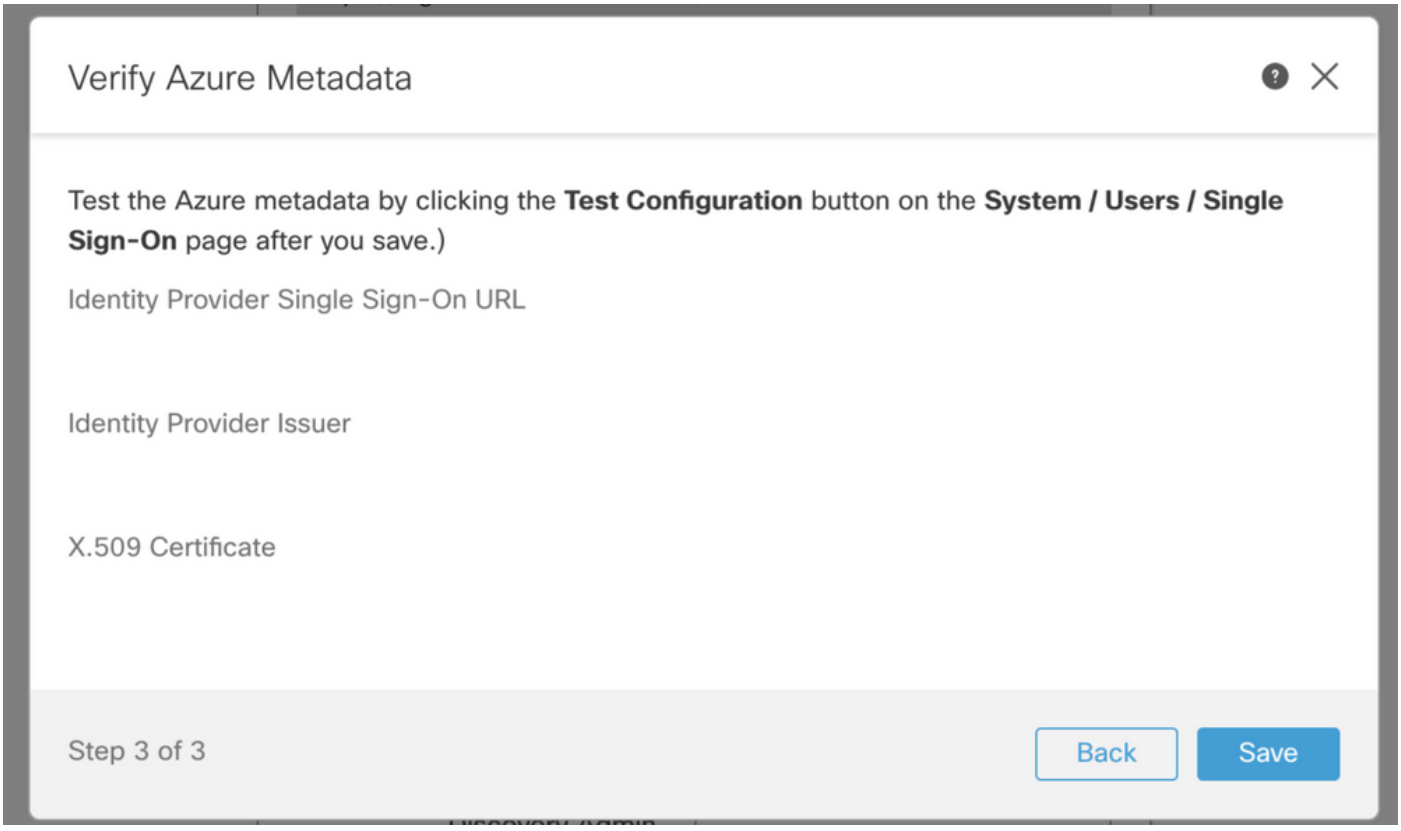
Configuratie van FireSIGHT Management Center

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.

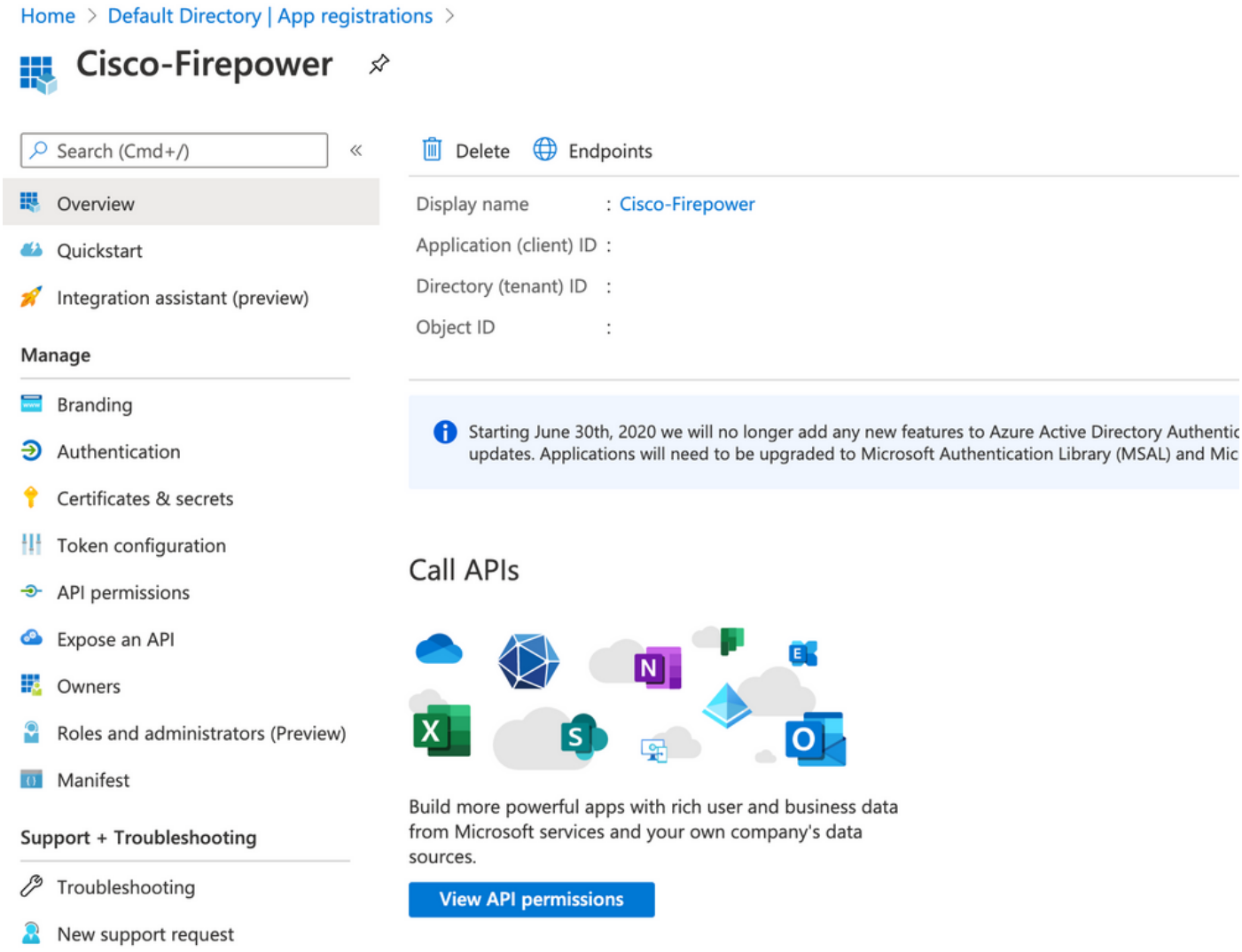


Geavanceerde configuratie - RBAC met KRK

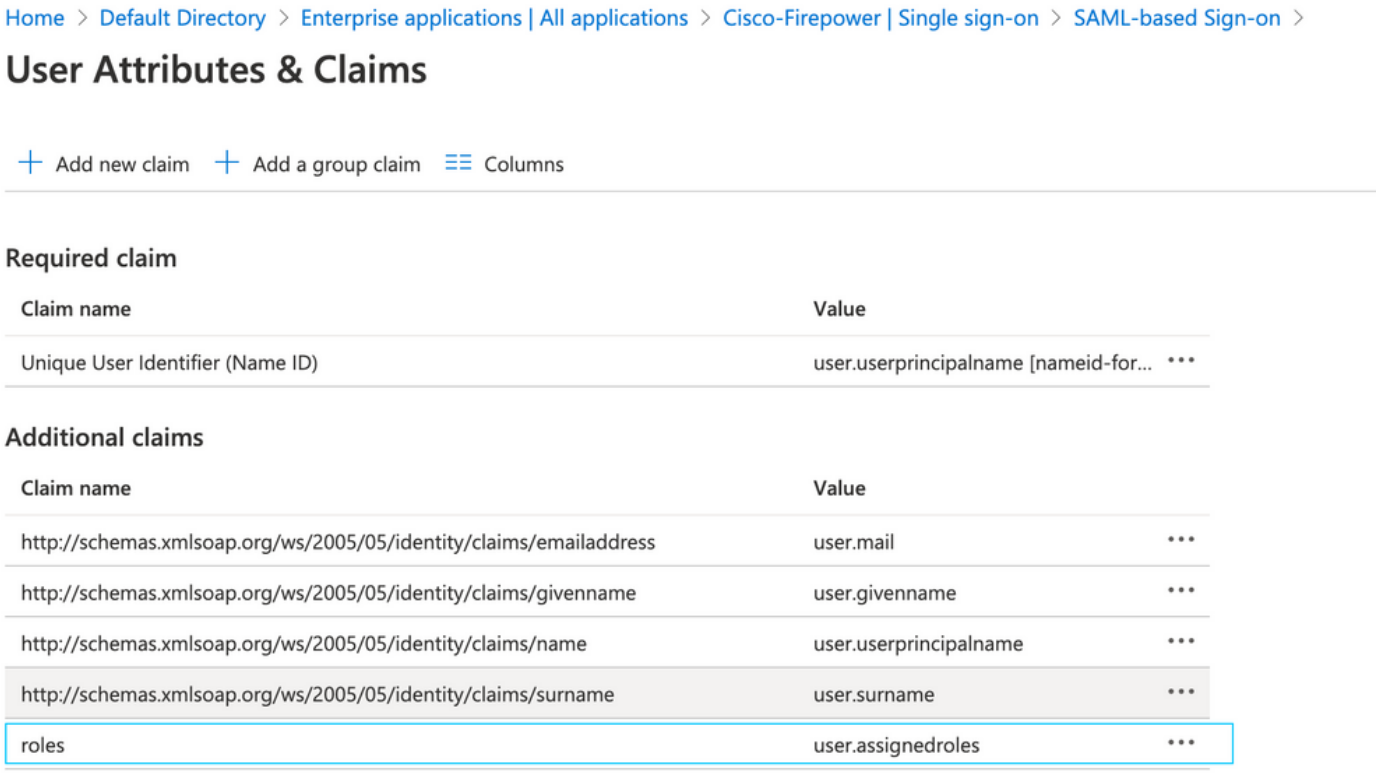
Om verschillende roltypes te gebruiken om aan Roles of FMC in kaart te brengen - moet je het

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

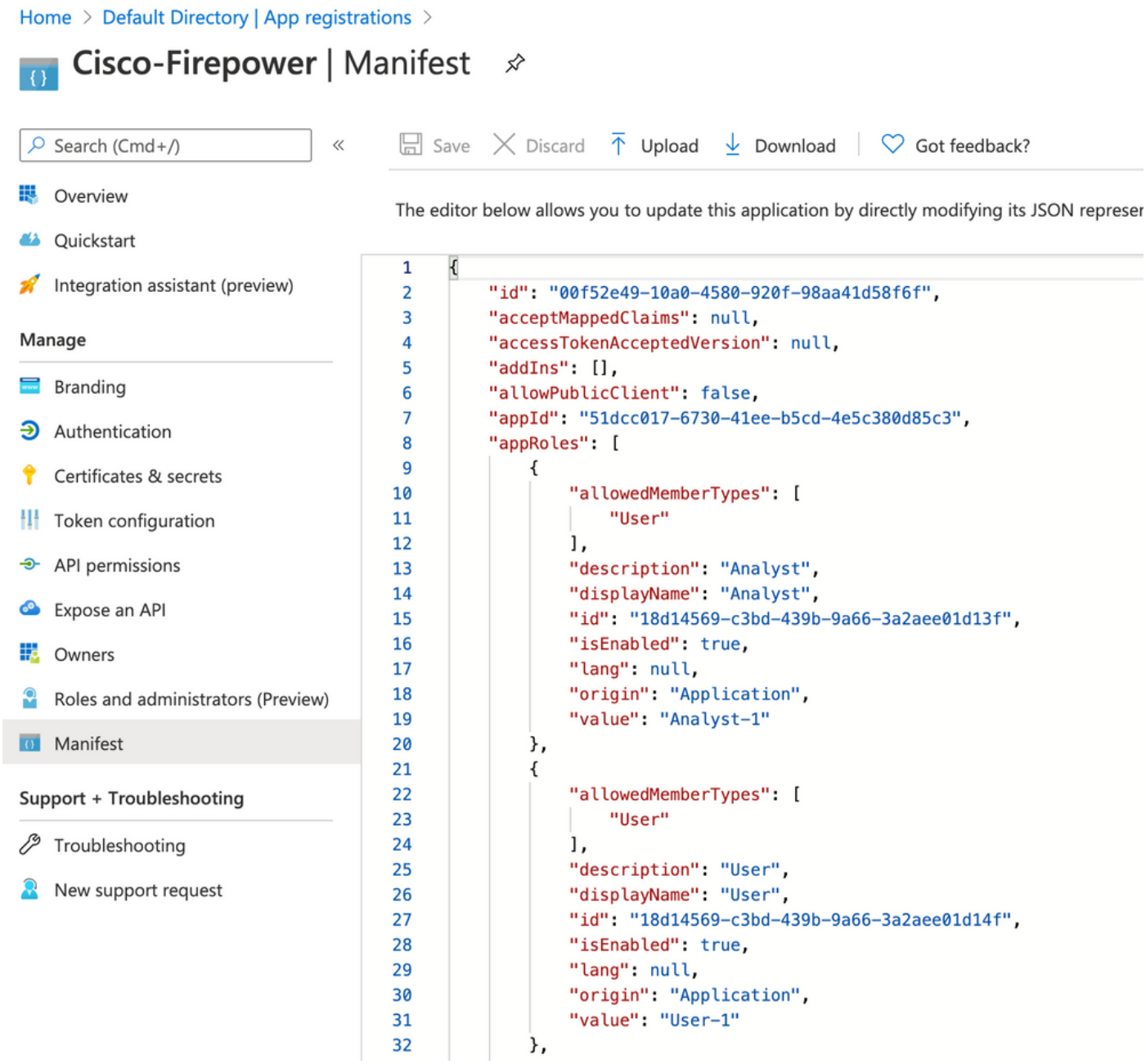
Stap 1. Navigeer naar de **toepassing** die wordt gemaakt en klik op **Enkelvoudig aanmelding**.



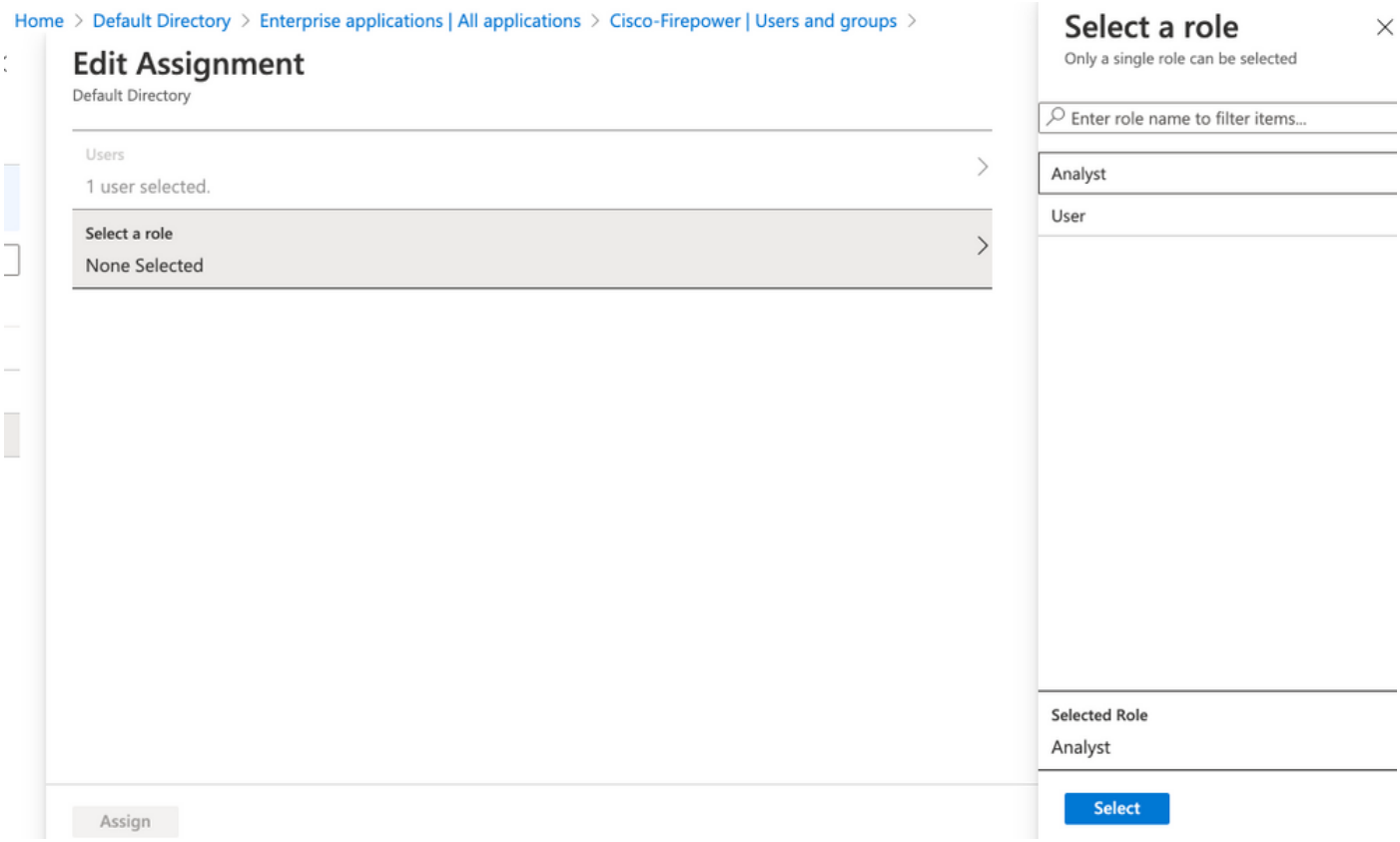
Stap 2. Bewerk de gebruikerskenmerken en -claims. Voeg een Nieuwe claim met Naam toe: **rollen** en selecteer de waarde als **door gebruiker.Toewijzende rollen**.



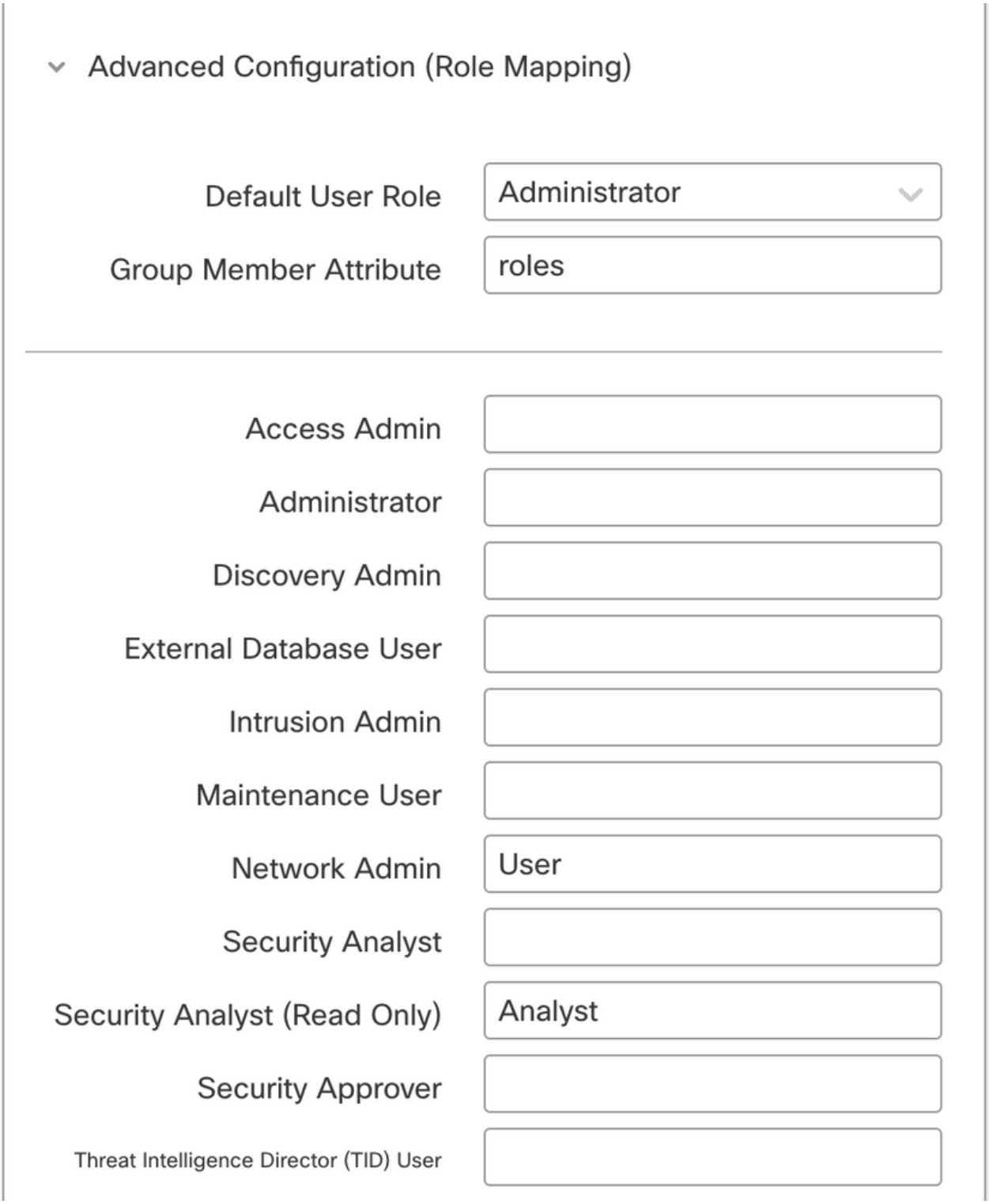
Stap 3. Navigeer naar **<Application-name> > manifest**. Bewerk het manifest. Het bestand is in JSON-indeling en er is een standaardgebruiker beschikbaar om te kopiëren. Bijvoorbeeld - hier worden 2 rollen gecreëerd: Gebruiker en Analyst.



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



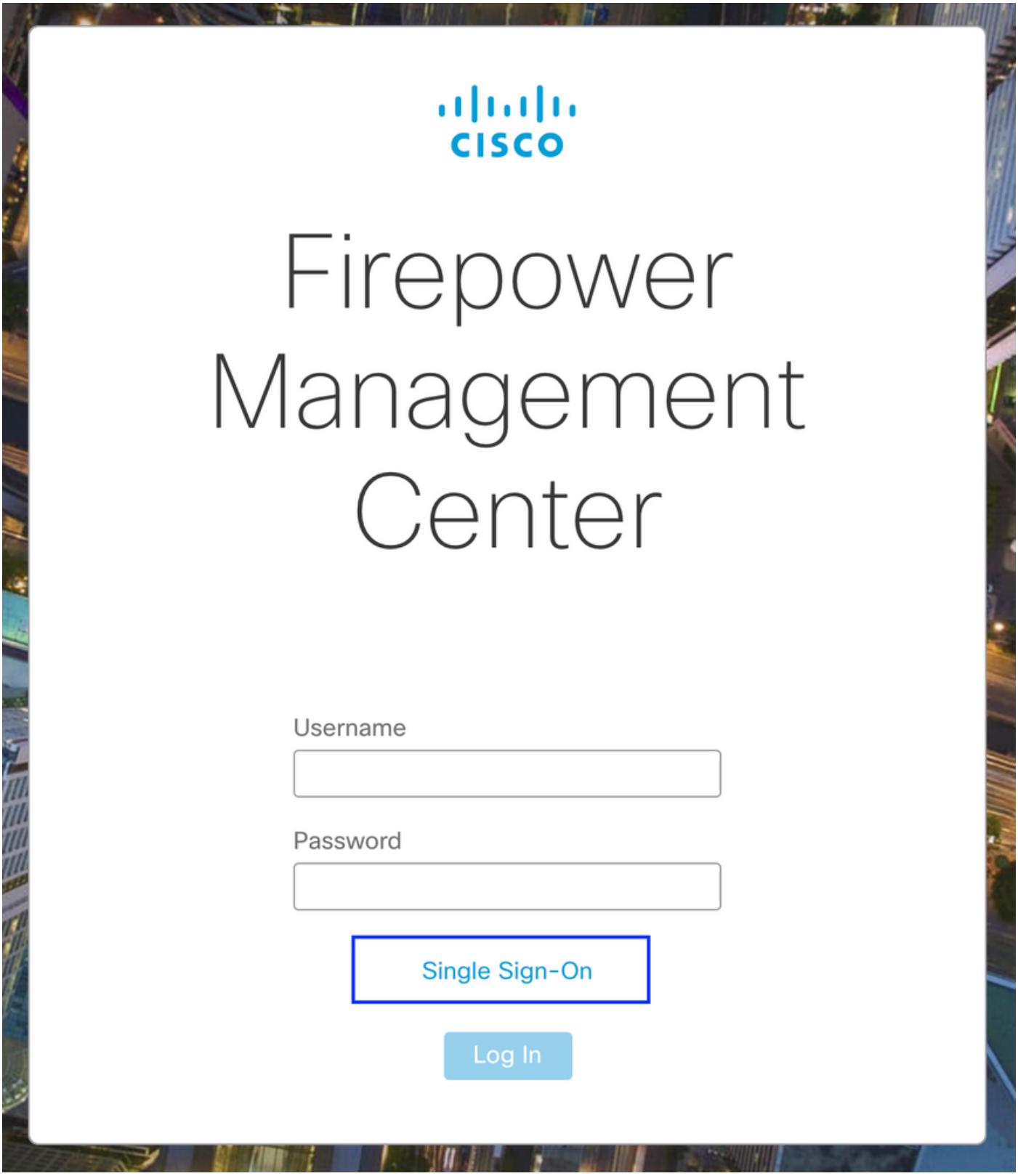
Stap 4. Meld u aan bij FMC en bevestig de geavanceerde configuratie in de BZB. voor, Kenmerk groepslid: awijs de **naam van het display** die u in Toepassingsmanifest hebt opgegeven, aan de rollen toe.



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.



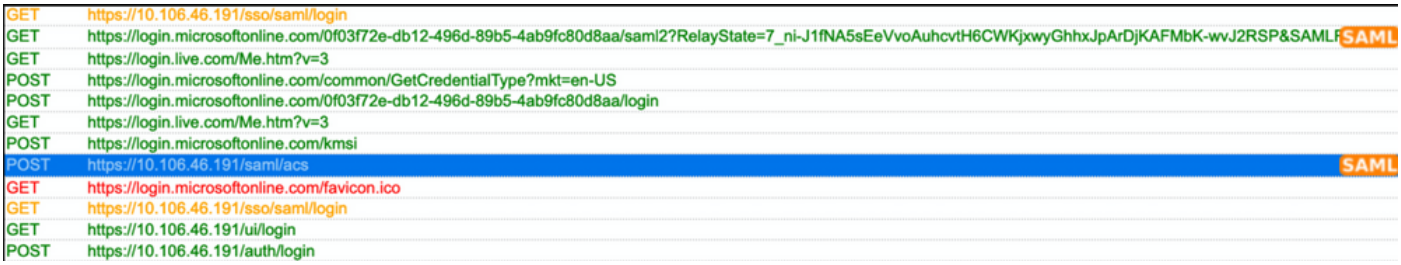
U wordt teruggestuurd naar de Microsoft inlogpagina en als u met succes inlogt, wordt de standaardpagina van FMC hersteld.

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

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



FMC SAML-vastlegging

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