Configure FMC SSO with Azure as Identity Provider

Contents

Introduction

This document describes how to configure the Firepower Management Center (FMC) Single Sign-On (SSO) with Azure as Identity Provider (idP).

Security Assertion Markup Language (SAML) is most frequently the underlying protocol that makes SSO possible. A company maintains a single login page, behind it is an identity store and various authentication rules. It can easily configure any web app that supports SAML, which allows you to log in to all web applications. It also has the security benefit of neither forcing users to maintain (and potentially reuse) passwords for every web app they need access to, nor exposing passwords to those web apps.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Understanding of Firepower Management Center
- Basic understanding of Single Sign-On

Components Used

The information in this document is based on these software versions:

- Cisco Firepower Management Center (FMC) version 6.7.0
- Azure - IdP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SAML Terminologies

Configuration for SAML must be done in two places: at the IdP and at the SP. The IdP needs to be configured so it knows where and how to send users when they want to log in to a specific SP. The SP needs to be configured so it knows it can trust SAML assertions signed by the IdP.

Definition of a few terms that are core to SAML:

- Identity Provider (IdP) - The software tool or service (often visualized by a login page and/or dashboard) that performs the authentication; checks username and passwords, verify the account status, invokes two-factor, etc.

- Service Provider (SP) - The web application where the user tries to gain access.

- SAML Assertion - A message asserting a user's identity and often other attributes, sent over HTTP via browser redirects

IdP Configuration

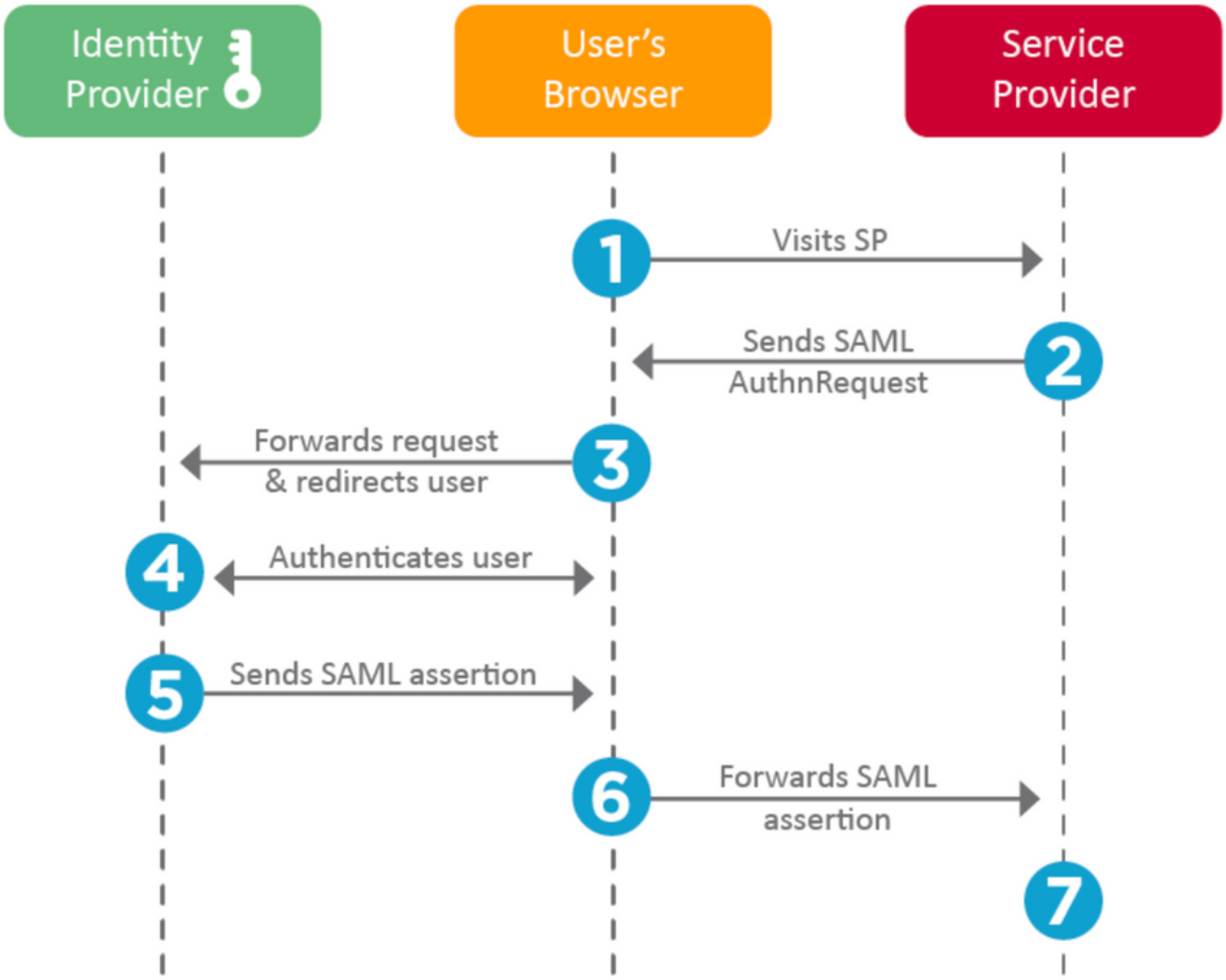
Specifications for a SAML assertion, what it should contain, and how it should be formatted, are provided by the SP and set at the IdP.

- EntityID - A globally unique name for the SP. Formats vary, but it's increasingly common to see this value formatted as a URL.
  Example: <https://<FQDN-or-IPaddress>/saml/metadata>

- Assertion Consumer Service (ACS) Validator - A security measure in the form of a regular expression (regex) that ensures the SAML assertion is sent to the correct ACS. This only comes into play during SP-initiated logins where the SAML request contains an ACS location, so this ACS validator would ensure that the SAML request-provided ACS location is legitimate.
  Example: **https://<FQDN-or-IPaddress>/saml/acs**

- Attributes - The number of and format of attributes can vary greatly. There's usually at least one attribute, the nameID, which is typically the username of the user trying to log in.

- SAML Signature Algorithm - SHA-1 or SHA-256. Less commonly SHA-384 or SHA-512. This algorithm is used in conjunction with the X.509 certificate is mentioned here.



SP Configuration

The reverse of the section above, this section speaks to information provided by the IdP and set at the SP.

- Issuer URL - Unique identifier of the IdP. Formatted as a URL containing information about the IdP so the SP can validate that the SAML assertions it receives are issued from the correct IdP.
  Example: <saml:Issuer https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/ >

- SAML SSO Endpoint / Service Provider Login URL - An IdP endpoint that initiates authentication when redirected here by the SP with a SAML request.
  Example: https://login.microsoftonline.com/023480840129412-824812/saml2

- SAML SLO (Single Log-out) Endpoint - An IdP endpoint that closes your IdP session when redirected here by the SP, typically after **log out** is clicked.
  Example: `https://access.wristbandtent.com/logout`

SAML on FMC

The SSO feature in FMC is introduced from 6.7. The new feature simplifies FMC Authorization (RBAC), as it maps the information that exists to FMC Roles. It applies to all FMC UI users and FMC roles. For now, it supports SAML 2.0 Specification, and these supported IDPs

- OKTA
- OneLogin
- PingID
- Azure AD
- Others (Any IDP that conforms to SAML 2.0)

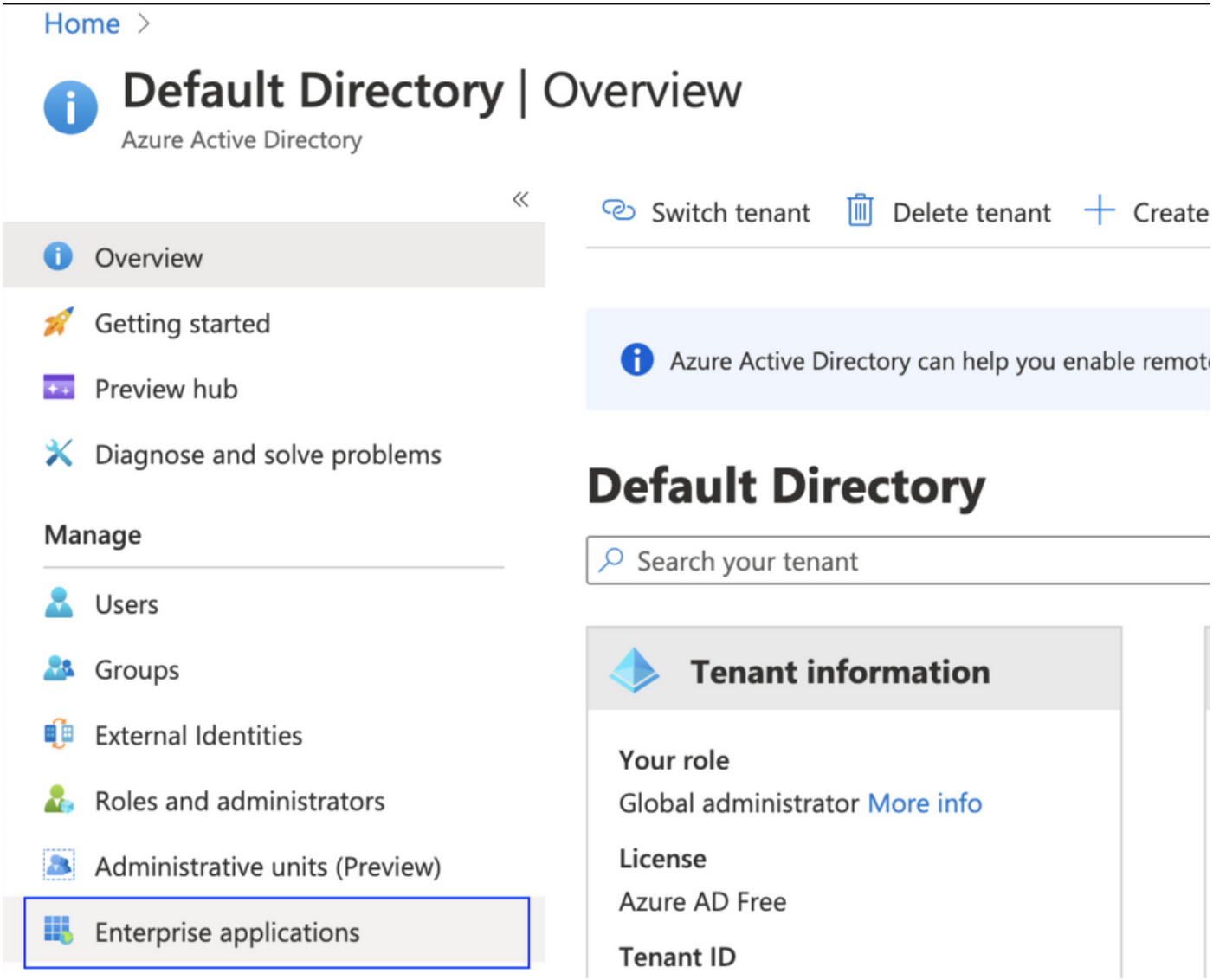
Limitations and Caveats

- SSO can be configured only for the Global Domain.
- FMCs in HA Pair need individual configuration.
- Only Local/AD admins can configure Single Sign-on.
- SSO initiated from Idp is not supported.

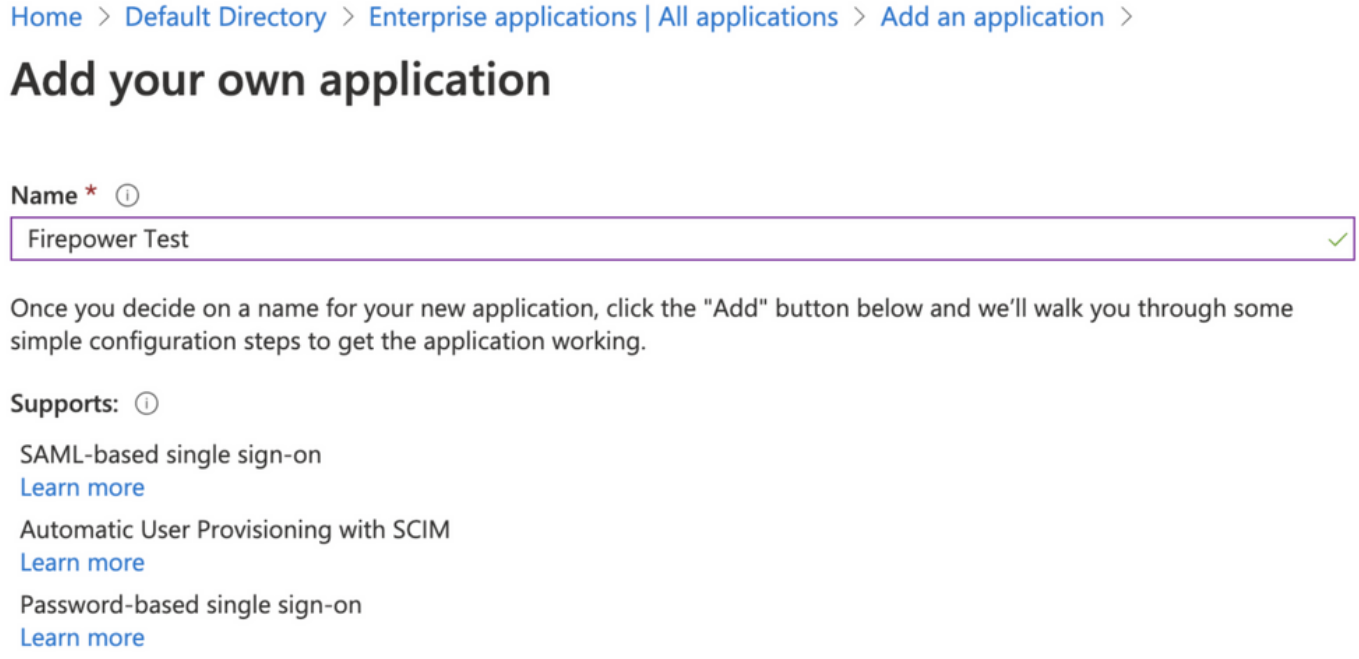
Configure

Configuration on Identity Provider

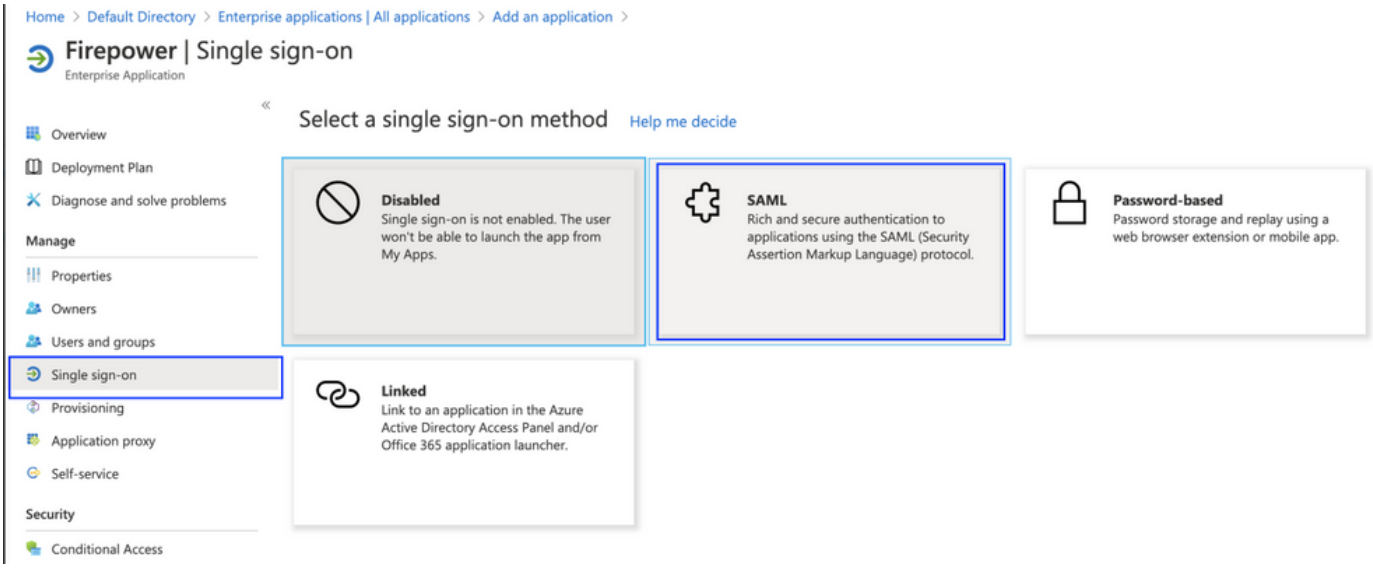
Step 1. Log in to Microsoft Azure. Navigate to **Azure Active Directory > Enterprise Application**.



- Step 2. Create **New Application** under Non-Gallery Application, as shown in this image.

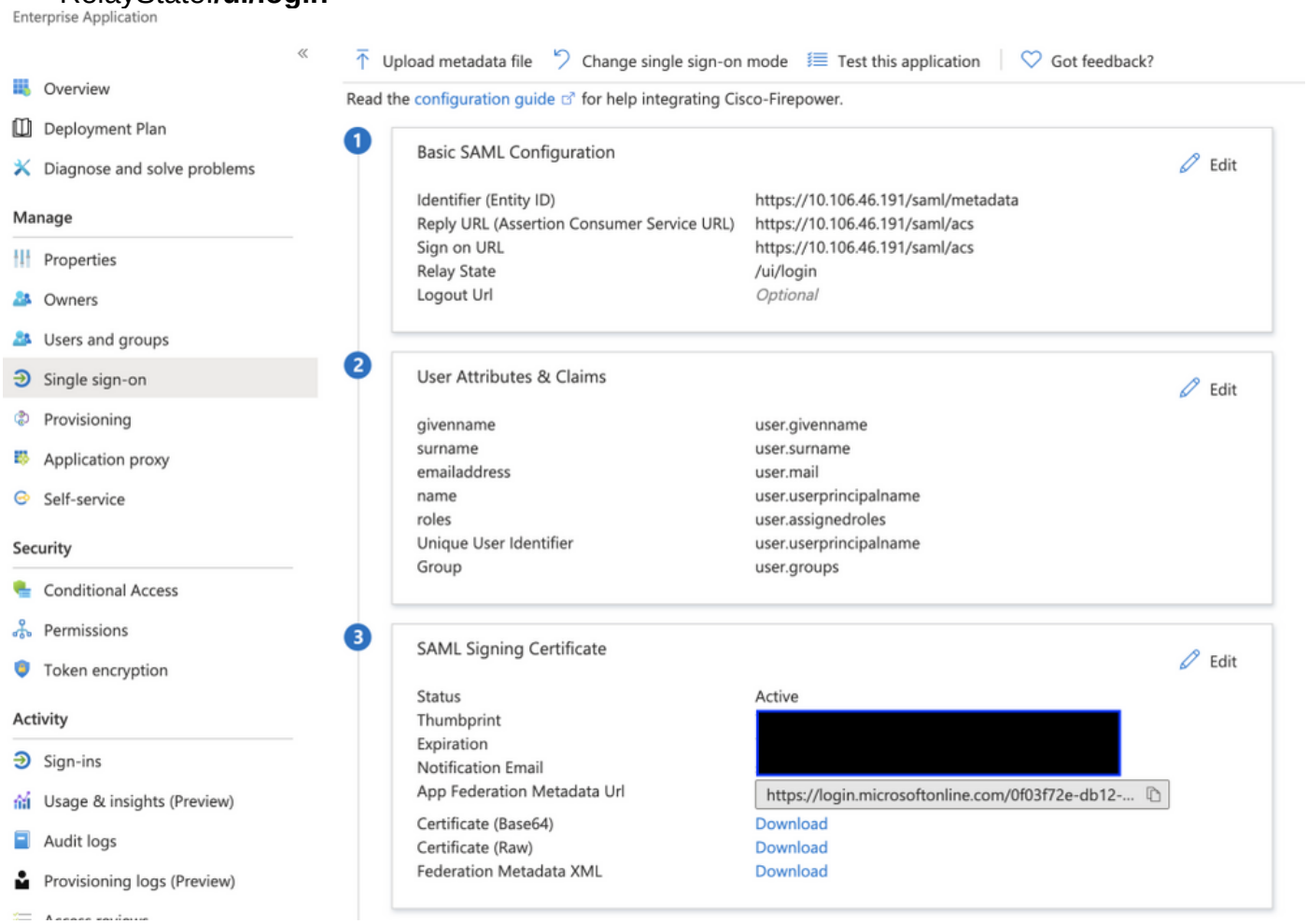


Step 3. Edit the Application that was created and navigate to **Set up single sign on > SAML**, as shown in this image.



Step 4. Edit the Basic SAML Configuration and provide the FMC Details :

- FMC URL: **https://<FMC-FQDN-or-IPaddress>**
- Identifier (Entity ID): **https://<FMC-FQDN-or-IPaddress>/saml/metadata**
- Reply URL: **https://<FMC-FQDN-or-IPaddress>/saml/acs**
- Sign on URL: **/https://<FMC-QDN-or-IPaddress>/saml/acs**
- RelayState:**/ui/login**

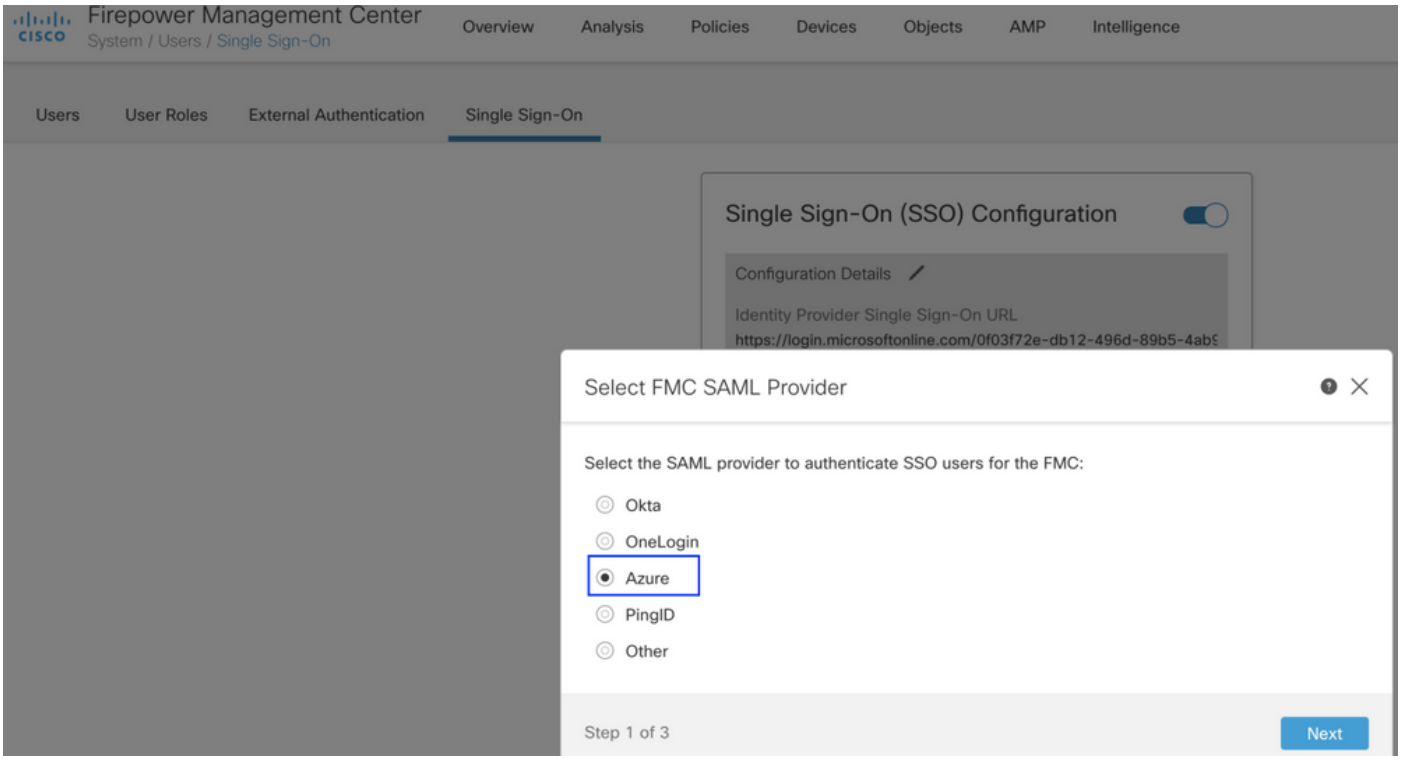


Keep the rest as default - this is further discussed for Role-based access.

This marks the end of the Identity provider configuration. Download the Federation Metadata XML which will be used for FMC Configuration.

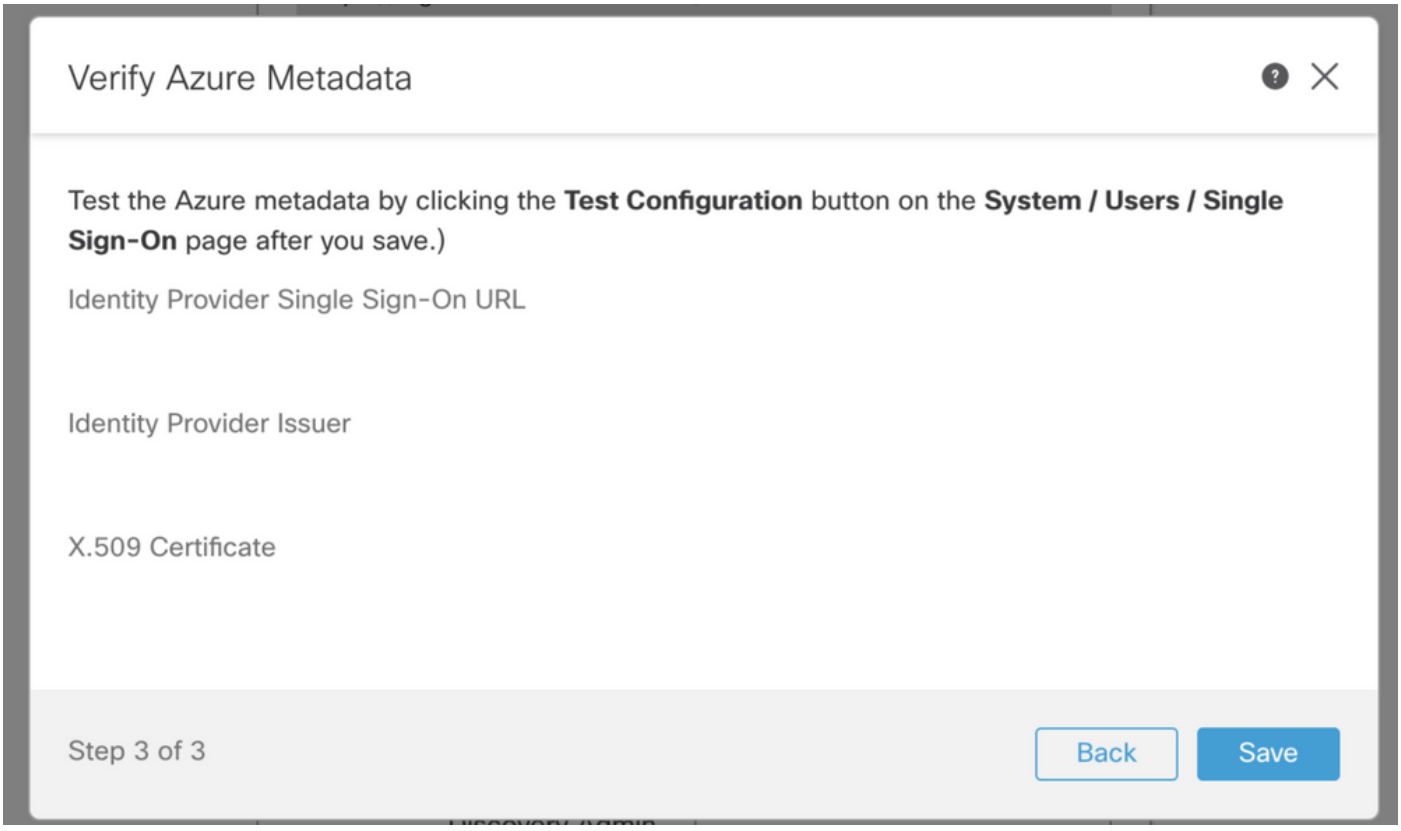
Configuration on Firepower Management Center

Step 1. Log in to FMC, navigate to **Settings > Users > Single Sign-On** and Enable SSO. Select **Azure** as Provider.



Step 2. Upload the XML file downloaded from Azure here. It auto-populates all the details needed.

Step 3. Verify the configuration and click **Save**, as shown in this image.

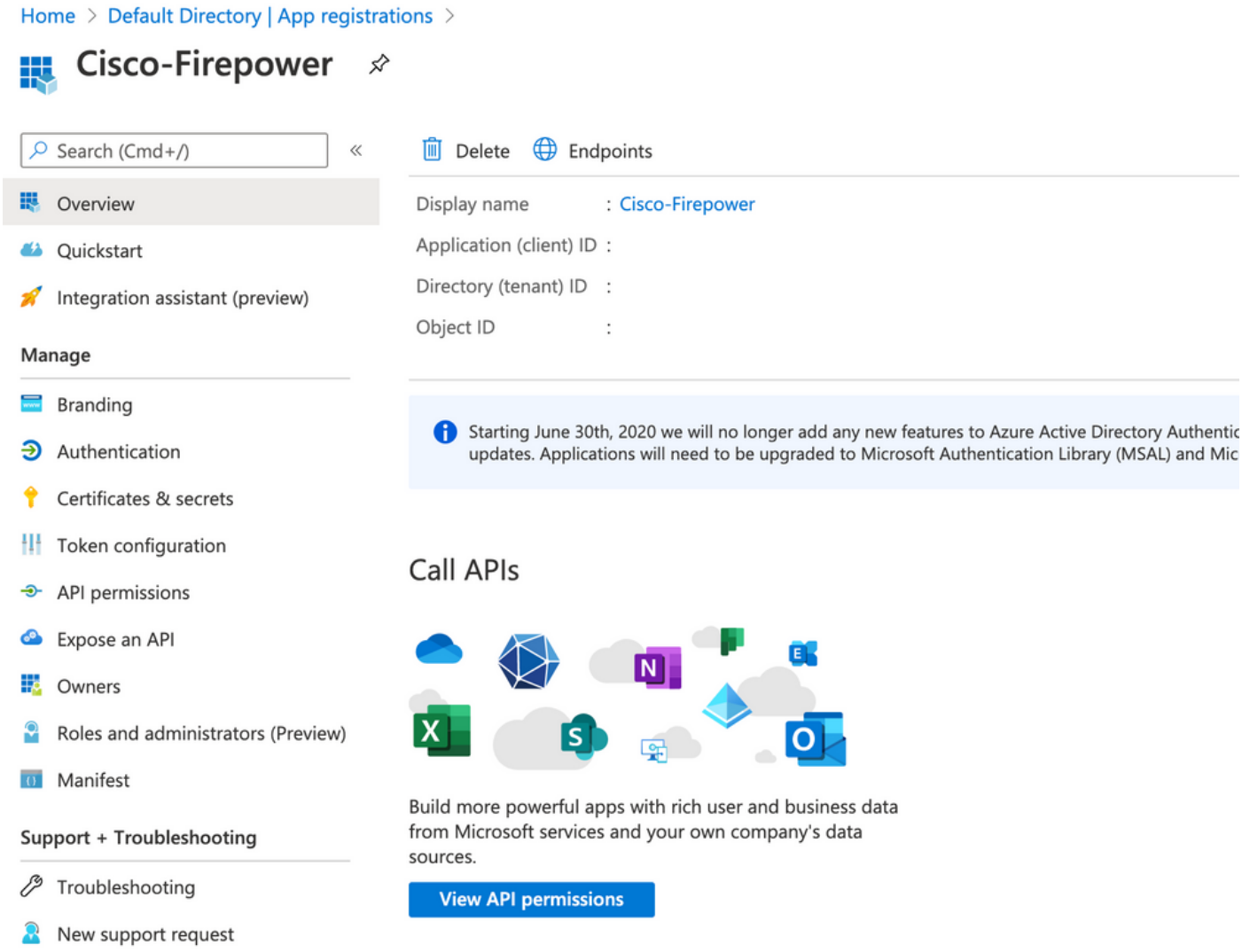


Advanced Configuration - RBAC with Azure

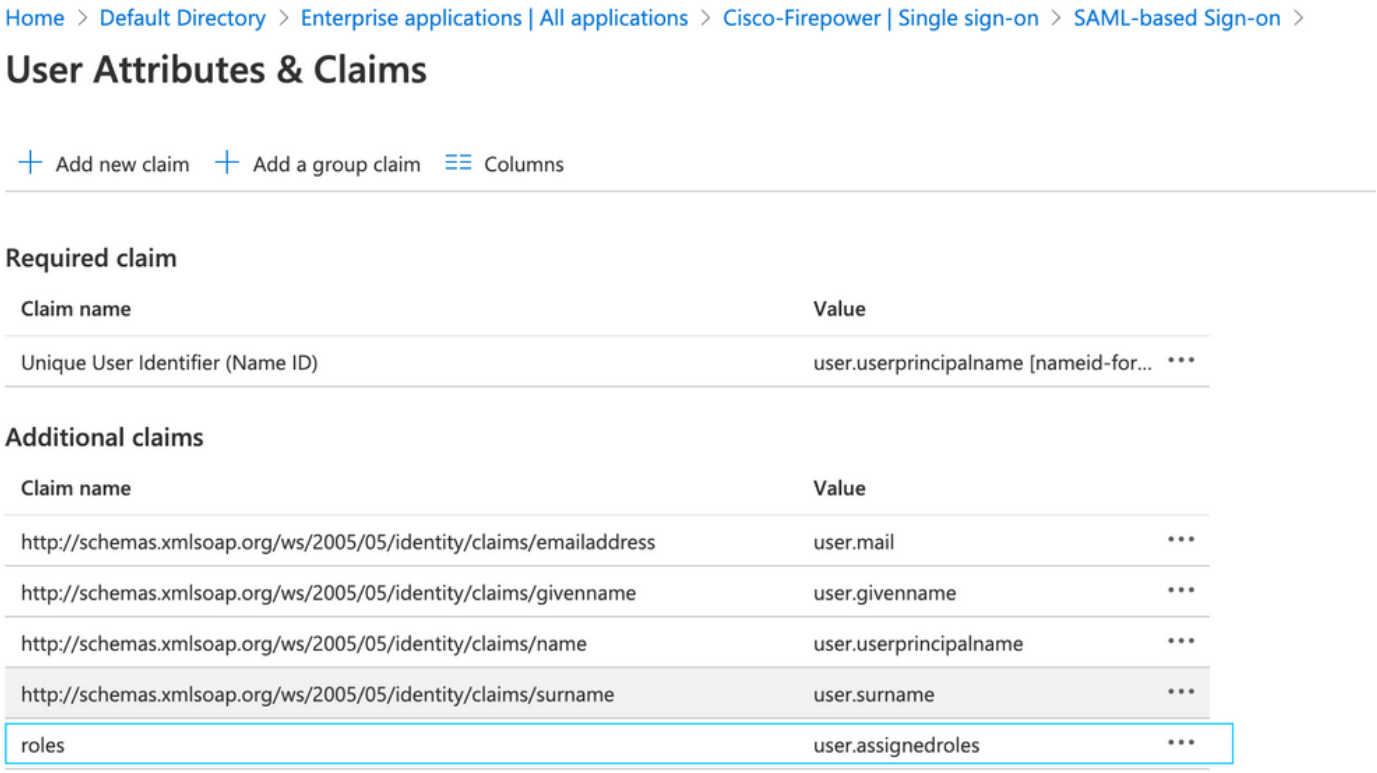
In order to use various role types to map to Roles of FMC - You need to edit the manifest of

Application on Azure to assign values to roles. By default, the roles have value as Null.

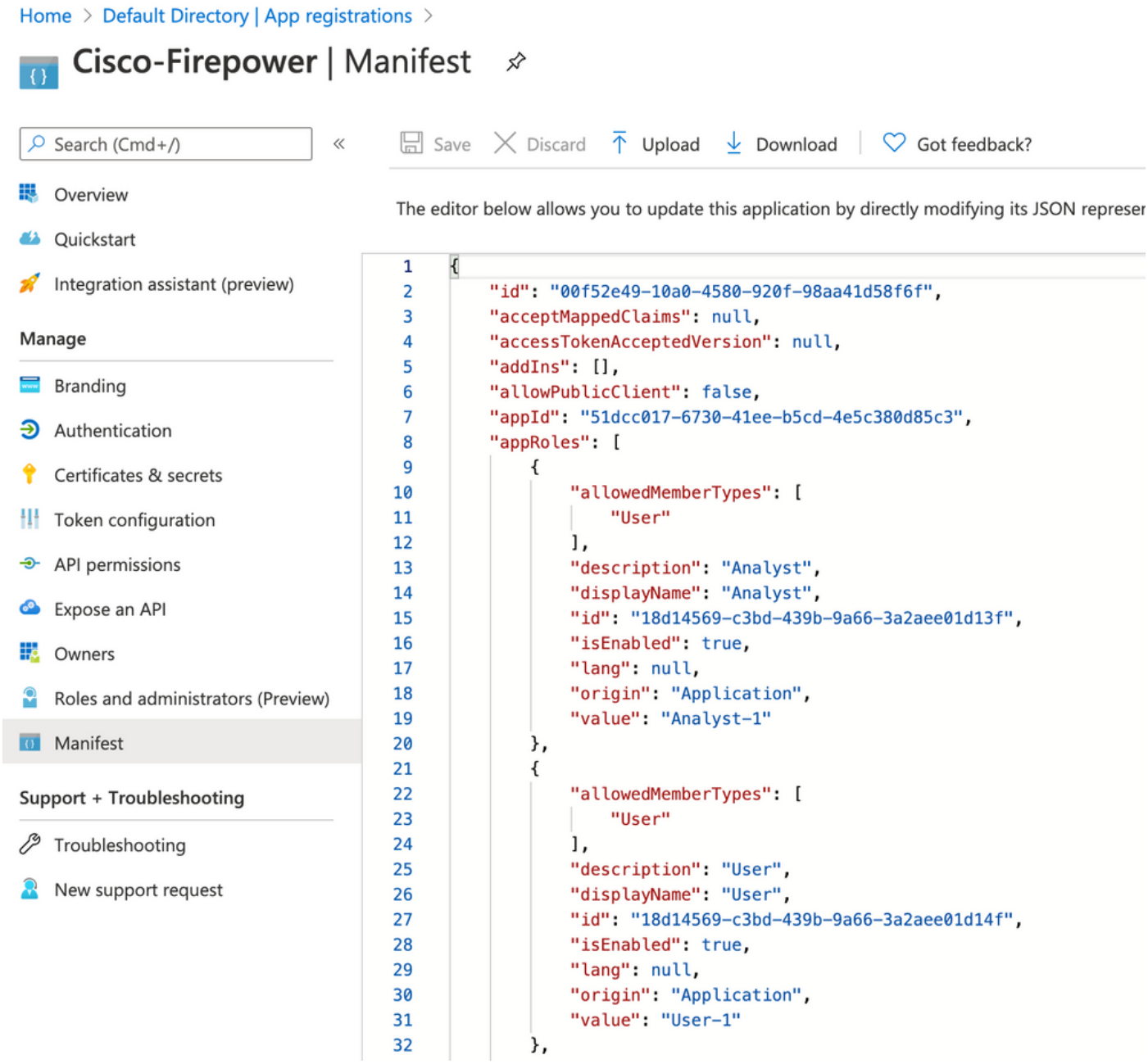
Step 1. Navigate to the **Application** that is created and click on **Single sign-on**.



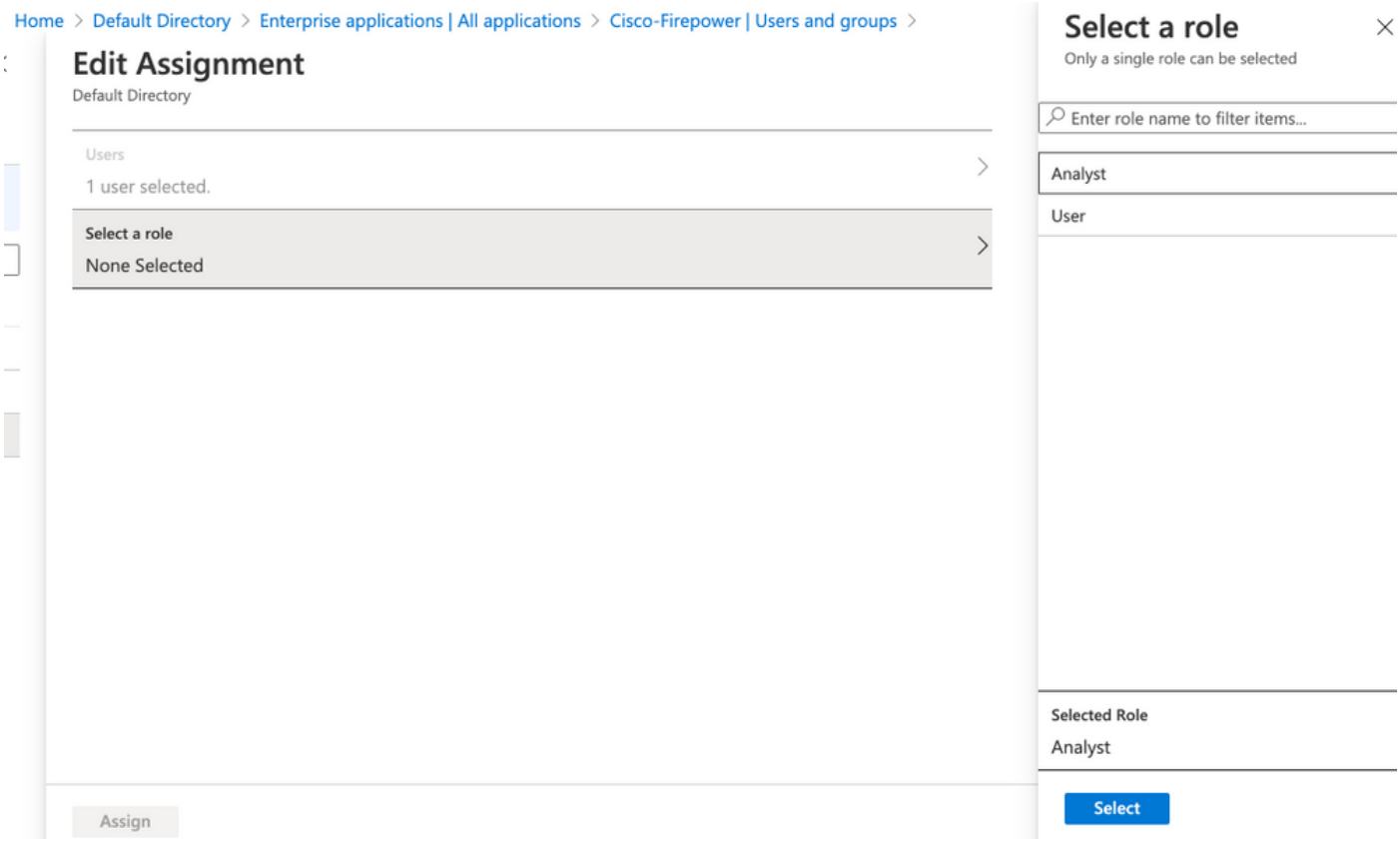
Step 2. Edit the User Attributes and Claims. Add a New claim with Name: **roles** and select the value as **user.assignedroles**.



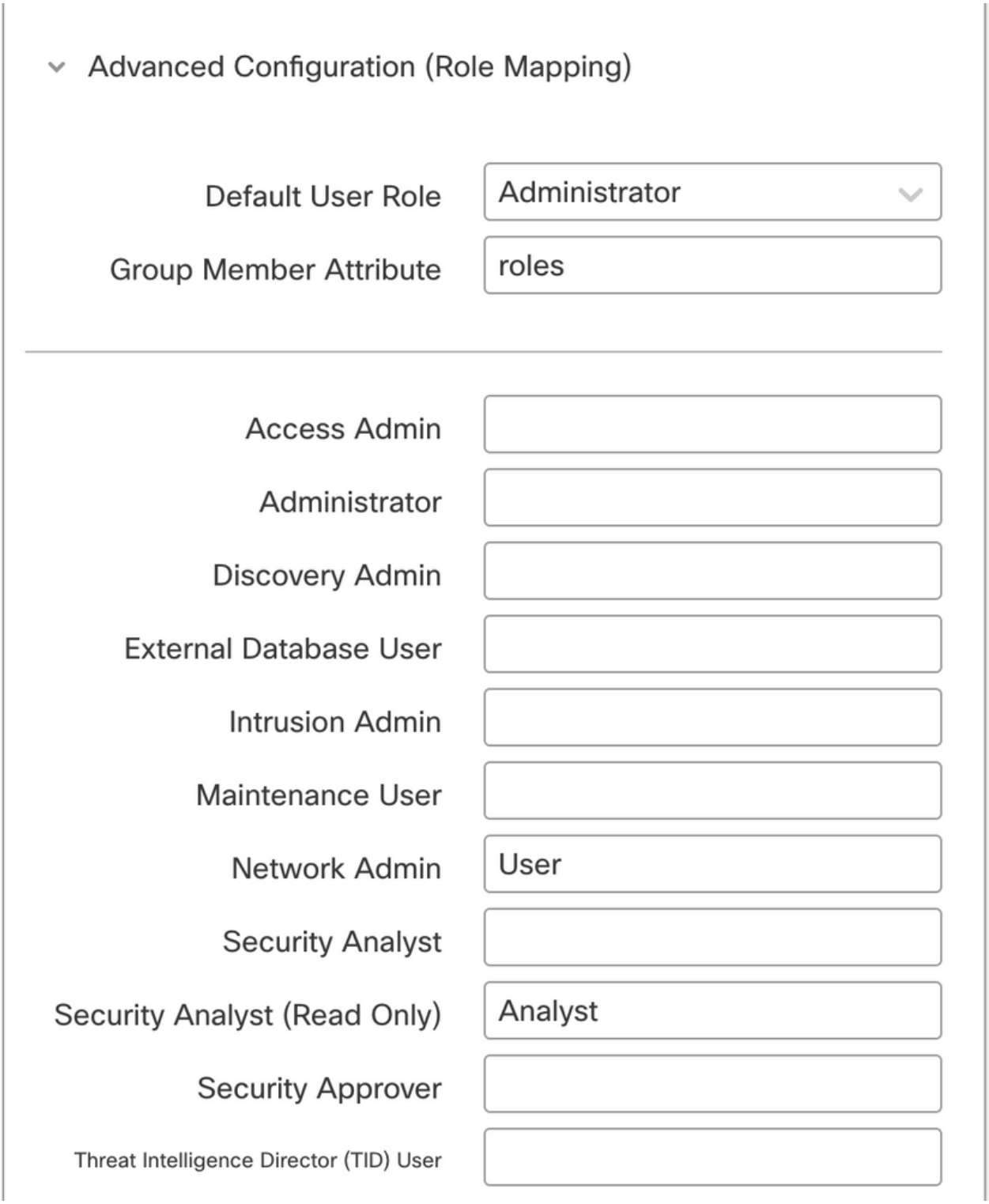
Step 3. Navigate to **<Application-Name> > Manifest**. Edit the Manifest. The file is in JSON format and a default User is available to copy. For example- here 2 roles are created: User and Analyst.



Step 4. Navigate to **<Application-Name> > Users and Groups**. Edit the user and assign the newly created roles, as shown in this image.



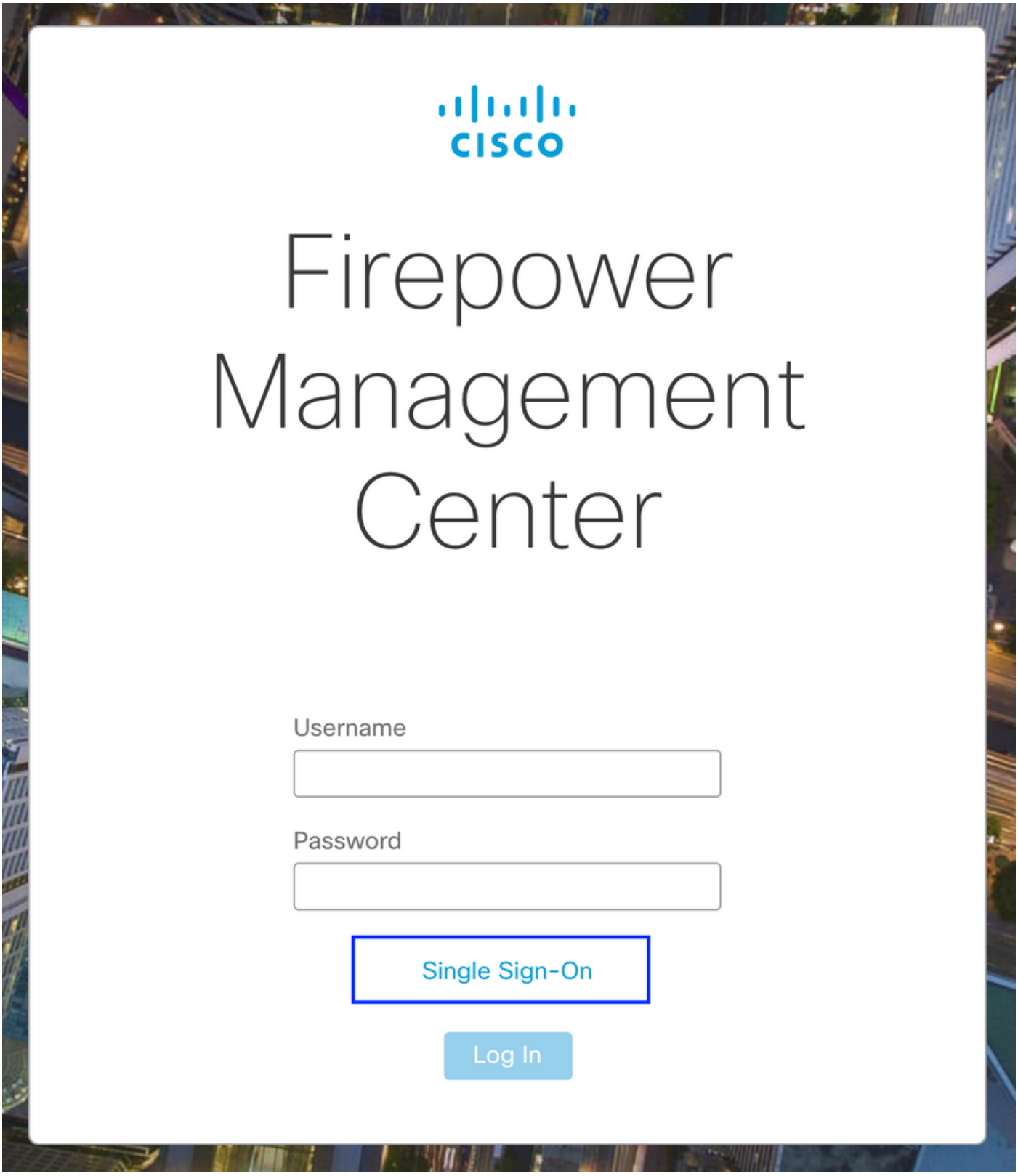
Step 4. Log in to FMC and edit the Advanced Configuration in SSO. For, Group Member Attribute: assign the **Display name** that you have provided in Application Manifest to the roles.



Once that is done, you should be able to log in to their designated role.

Verify

Step 1. Navigate to the FMC URL from your browser: https://<FMC URL>. Click on **Single Sign-On**, as shown in this image.



You are redirected to the Microsoft login page and successful login would return the FMC default page.

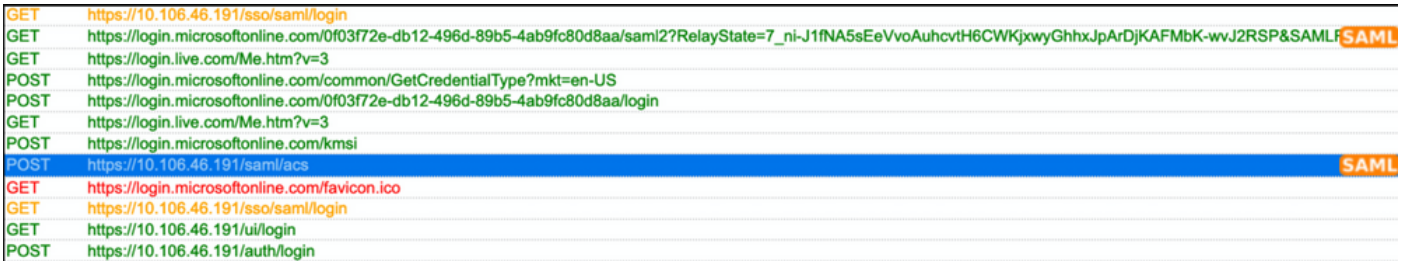
Step 2. On FMC, navigate to **System > Users** to see the SSO user added to the database.

test1@shbharticisco.onmicrosoft.com	Security Analyst	External (SSO)
test2guy@shbharticisco.onmicrosoft.com	Administrator	External (SSO)

Troubleshoot

Verify the SAML Authentication and this is the workflow you achieve for successful authorization (This image is of a lab environment) :

Browser SAML Logs



FMC SAML Logs

Verify the SAML Logs on FMC at**/var/log/auth-daemon.log**