Configurar o SSO do FMC com o Azure como provedor de identidade

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Configuração do IdP](#)
[Configuração do SP](#)
[SAML no FMC](#)
[Limitações e caveats](#)
[Configurar](#)
[Configuração no provedor de identidade](#)
[Configuração do Firepower Management Center](#)
[Configuração avançada - RBAC com Azure](#)
[Verificar](#)
[Troubleshoot](#)
[Logs SAML do navegador](#)
[Logs SAML do FMC](#)

Introduction

Este documento descreve como configurar o SSO (Single Sign-On, logon único) do Firepower Management Center (FMC) com o Azure como provedor de identidade (idP).

O Security Assertion Markup Language (SAML) é com mais frequência o protocolo subjacente que torna o SSO possível. Uma empresa mantém uma única página de login, atrás dela está um repositório de identidade e várias regras de autenticação. Ele pode facilmente configurar qualquer aplicativo da Web que suporte SAML, o que permite que você faça login em todos os aplicativos da Web. Ele também tem o benefício de segurança de não forçar os usuários a manter (e potencialmente reutilizar) senhas para cada aplicativo da Web ao qual eles precisam acessar, nem expor senhas a esses aplicativos da Web.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica do Firepower Management Center
- Compreensão básica do login único

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Management Center (FMC) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Terminologias SAML

A configuração do SAML deve ser feita em dois locais: no IdP e no SP. O IdP precisa ser configurado para que ele saiba para onde e como enviar usuários quando desejam fazer logon em uma controladora específica. O SP precisa ser configurado para que ele saiba que pode confiar em asserções SAML assinadas pelo IdP.

Definição de alguns termos centrais para o SAML:

- Provedor de identidade (IdP) - A ferramenta ou serviço de software (geralmente visualizado por uma página de login e/ou painel) que executa a autenticação; verifica o nome de usuário e as senhas, verifica o status da conta, invoca dois fatores, etc.

- Provedor de serviços (SP) - O aplicativo da Web no qual o usuário tenta obter acesso.

- SAML Assertion - Uma mensagem que afirma a identidade de um usuário e, muitas vezes, outros atributos, enviada por HTTP via redirecionamentos do navegador

Configuração do IdP

As especificações de uma asserção SAML, o que ela deve conter e como deve ser formatada são fornecidas pelo SP e definidas no IdP.

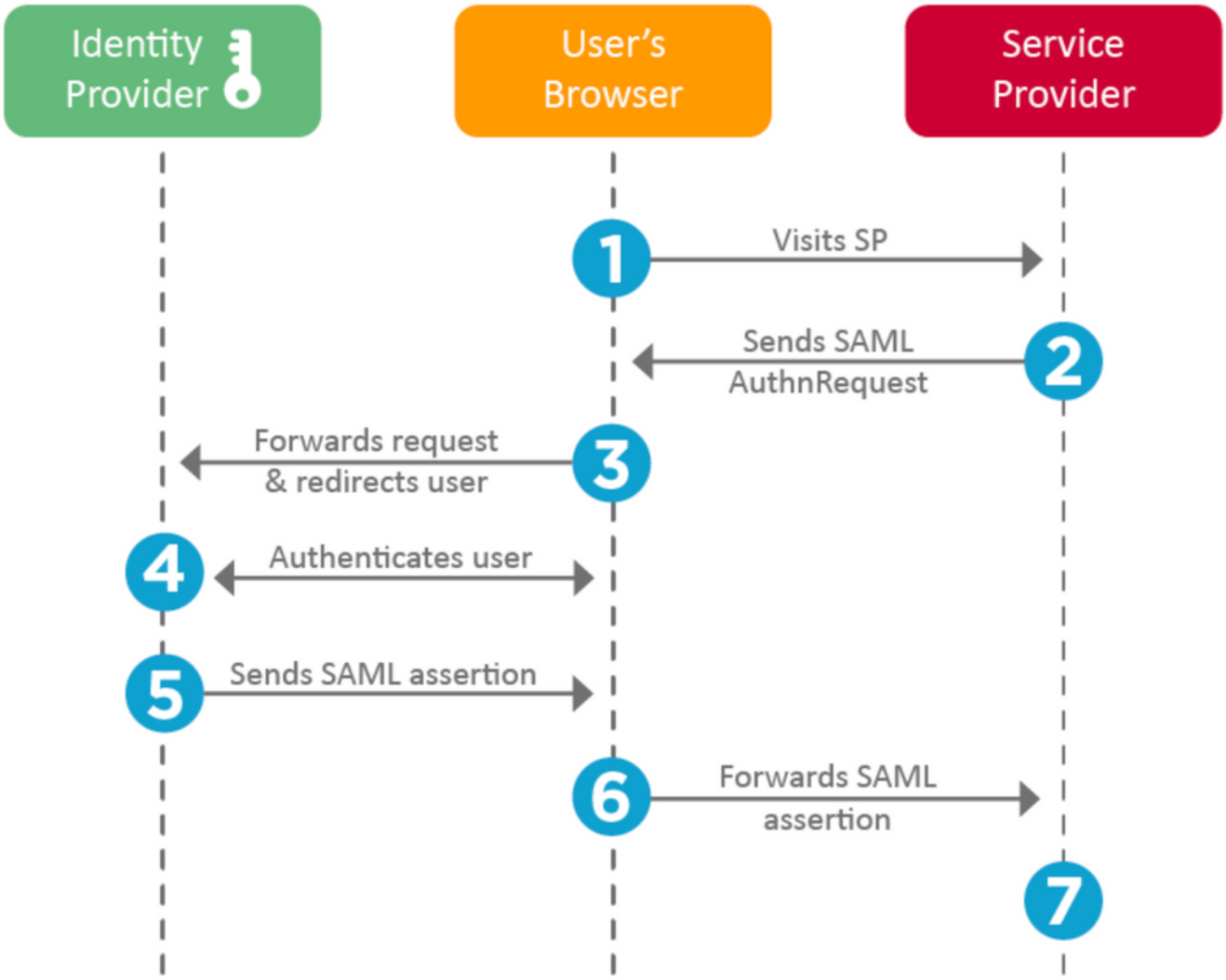
- EntityID - um nome globalmente exclusivo para o SP. Os formatos variam, mas é cada vez mais comum ver esse valor formatado como um URL.
  Exemplo: <https://<FQDN-or-IPaddress>/saml/metadados>

- Validador do Serviço de Consumidor de Asserção (ACS) - Uma medida de segurança na forma de uma expressão regular (regex) que garante que a asserção SAML seja enviada para o ACS correto. Isso só é executado durante os logins iniciados por SP em que a solicitação SAML contém um local ACS, portanto, esse validador ACS garante que o local ACS fornecido pela solicitação SAML é legítimo.
  Exemplo: **https://<FQDN-or-IPaddress>/saml/acs**

- Atributos - O número e o formato dos atributos podem variar muito. Geralmente, há pelo menos um atributo, o nameID, que normalmente é o nome de usuário do usuário que está

tentando fazer logon.

- Algoritmo de assinatura SAML - SHA-1 ou SHA-256. Menos comumente SHA-384 ou SHA-512. Este algoritmo é usado em conjunto com o certificado X.509 é mencionado aqui.



Configuração do SP

No verso da seção acima, esta seção fala sobre as informações fornecidas pelo IdP e definidas na controladora de armazenamento.

- URL do emissor - Identificador exclusivo do IdP. Formatado como um URL que contém informações sobre o IdP para que a controladora possa validar se as asserções SAML que recebe são emitidas do IdP correto.
  Exemplo: <saml:Issuer https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/ >

- Ponto de Extremidade SSO SAML / URL de Login do Provedor de Serviços - Um ponto de extremidade IdP que inicia a autenticação quando redirecionado aqui pelo SP com uma solicitação SAML.
  Exemplo: https://login.microsoftonline.com/023480840129412-824812/saml2

- Ponto de Extremidade SAML SLO (Logoff Único) - Um ponto de extremidade IdP que fecha sua sessão IdP quando redirecionada aqui pela controladora de armazenamento, geralmente após o **logoff** ser clicado.

Exemplo: `https://access.wristbandtent.com/logout`

SAML no FMC

O recurso SSO no FMC é apresentado a partir da versão 6.7. O novo recurso simplifica a RBAC (Autorização de FMC), pois mapeia as informações existentes para as funções de FMC. Ele se aplica a todos os usuários de IU do FMC e às funções do FMC. Por enquanto, ele suporta a especificação SAML 2.0 e esses IDPs suportados

- OKTA
- OneLogin
- PingID
- Azure AD
- Outros (qualquer IDP compatível com SAML 2.0)

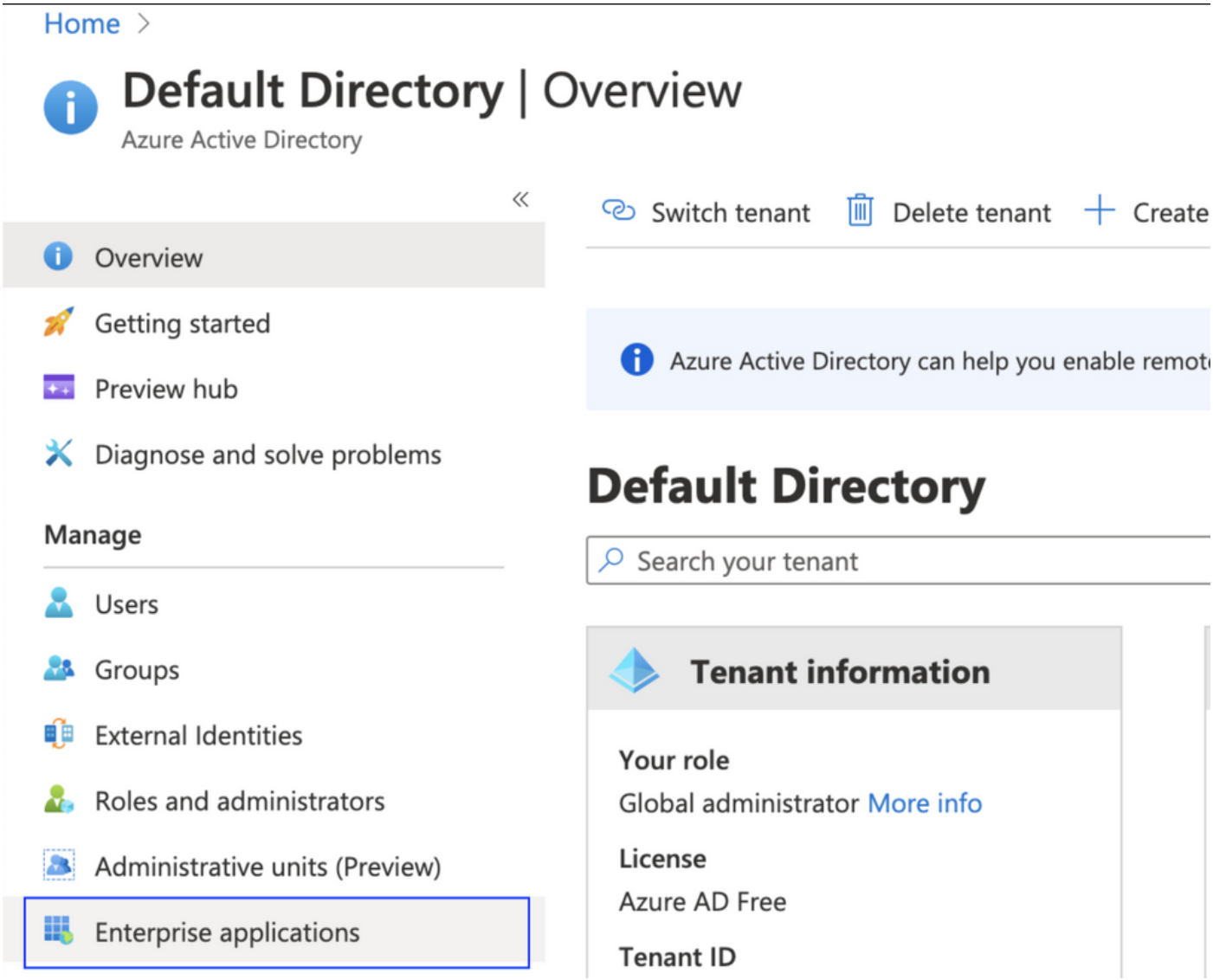
Limitações e caveats

- O SSO pode ser configurado somente para o domínio global.
- Os FMCs no par HA precisam de configuração individual.
- Somente administradores locais/AD podem configurar o Logon único.
- SSO iniciado a partir de Idp não é suportado.

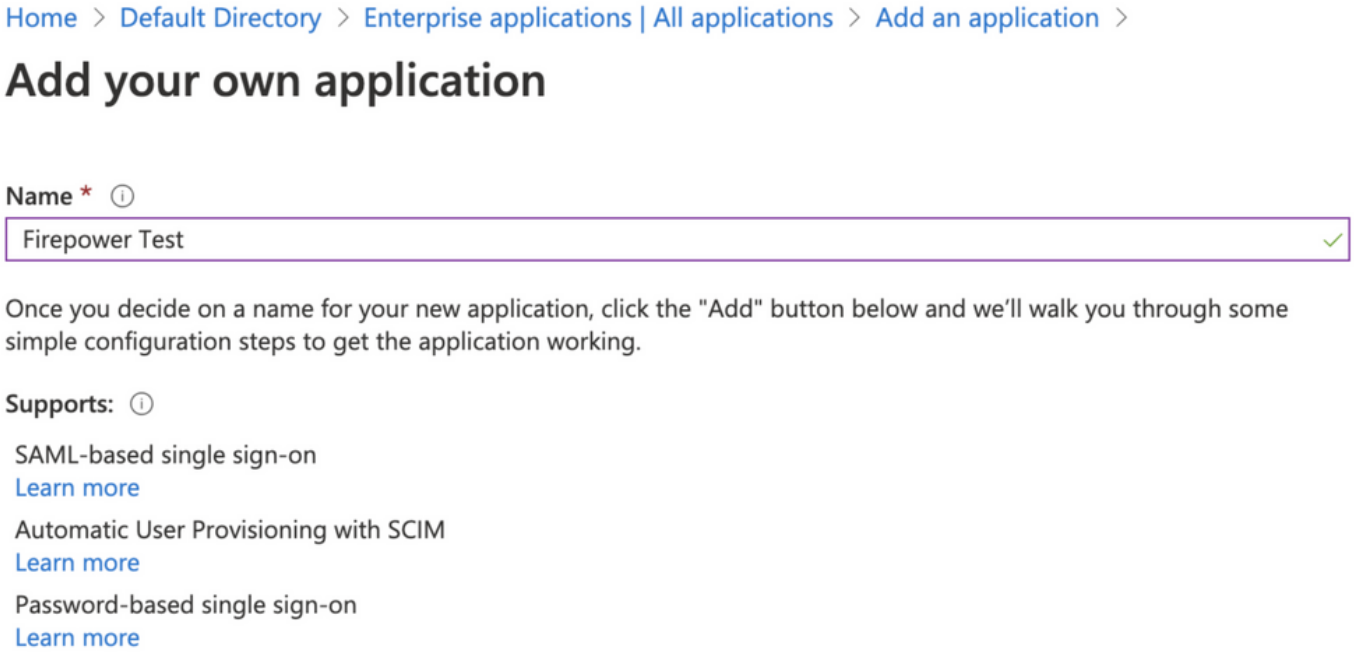
Configurar

Configuração no provedor de identidade

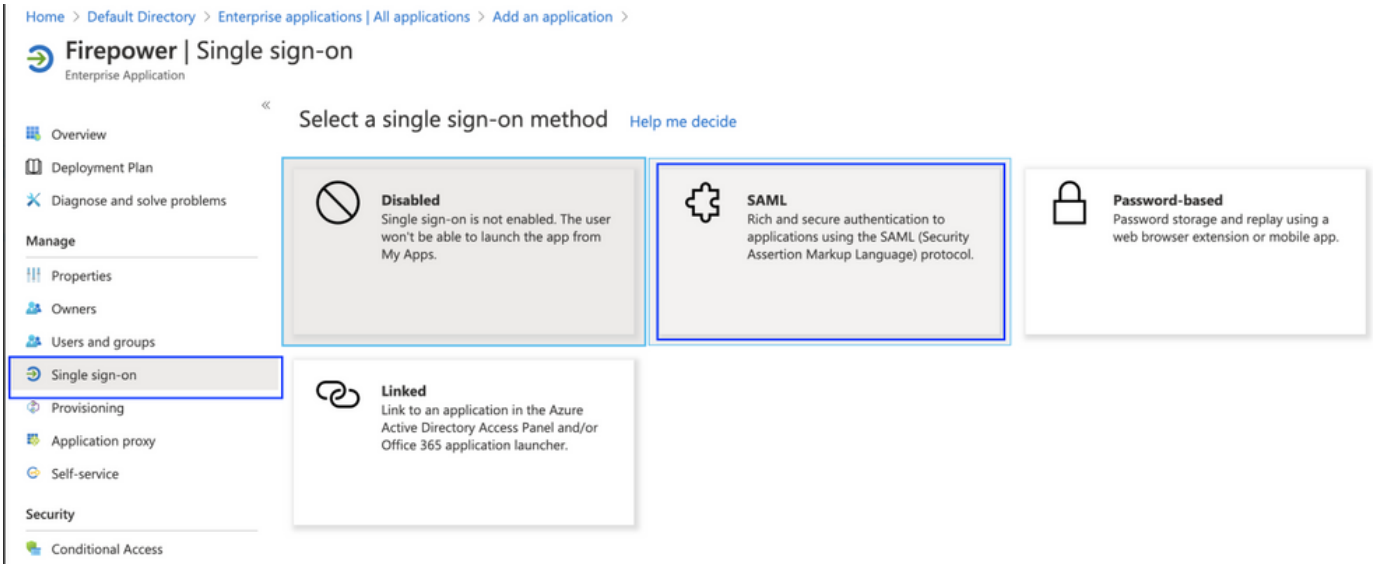
Etapa 1. Faça login no Microsoft Azure. Navegue para **Azure Ative Diretory > Enterprise Application**.



- Etapa 2. Criar **Novo Aplicativo** em Aplicativo Não Galeria, como mostrado nesta imagem.

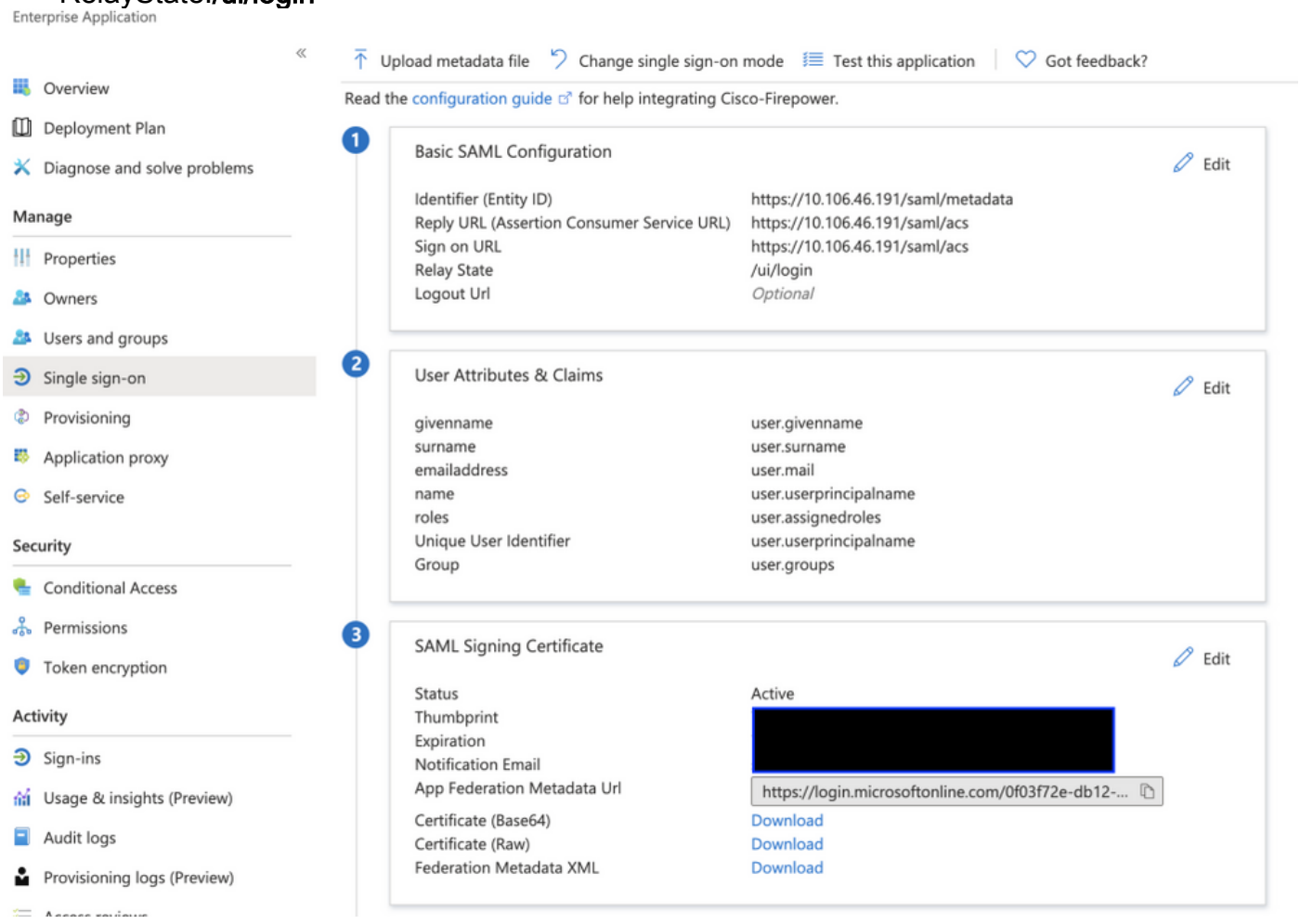


Etapa 3. Edite o Aplicativo que foi criado e navegue para **Configurar logon único > SAML**, como mostrado nesta imagem.



Etapa 4. Edite a Configuração SAML básica e forneça os detalhes do FMC:

- URL do FMC: https://<FMC-FQDN-or-IPaddress>
- Identificador (ID da entidade): https://<FMC-FQDN-or-IPaddress>/saml/metadados
- URL de resposta: https://<FMC-FQDN-or-IPaddress>/saml/acs
- URL de início de sessão: **/https://<FMC-QDN-or-IPaddress>/saml/acs**
- RelayState:**/ui/login**

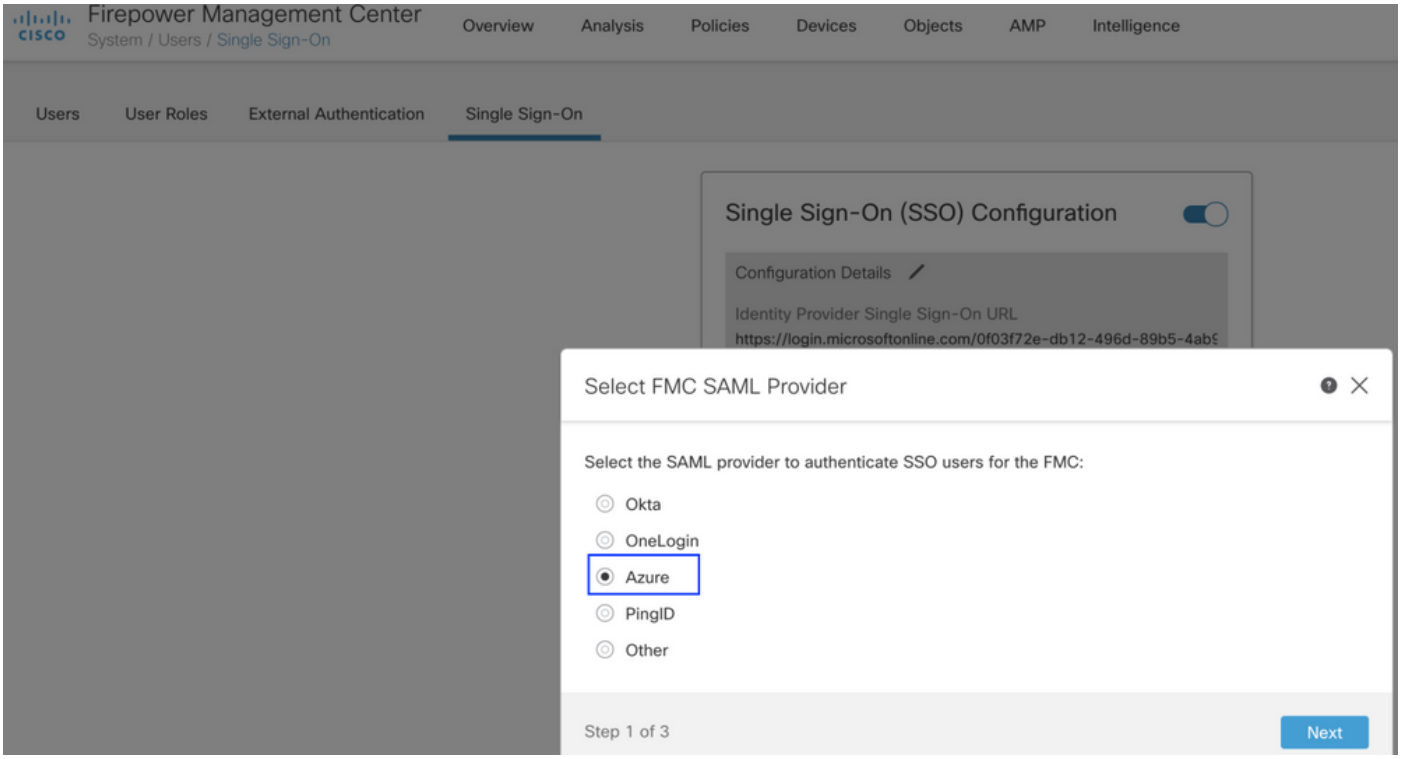


Mantenha o restante como padrão - isso é discutido com mais detalhes sobre o acesso baseado em função.

Isso marca o fim da configuração do provedor de identidade. Faça o download do XML de metadados de federação que será usado para a configuração do FMC.

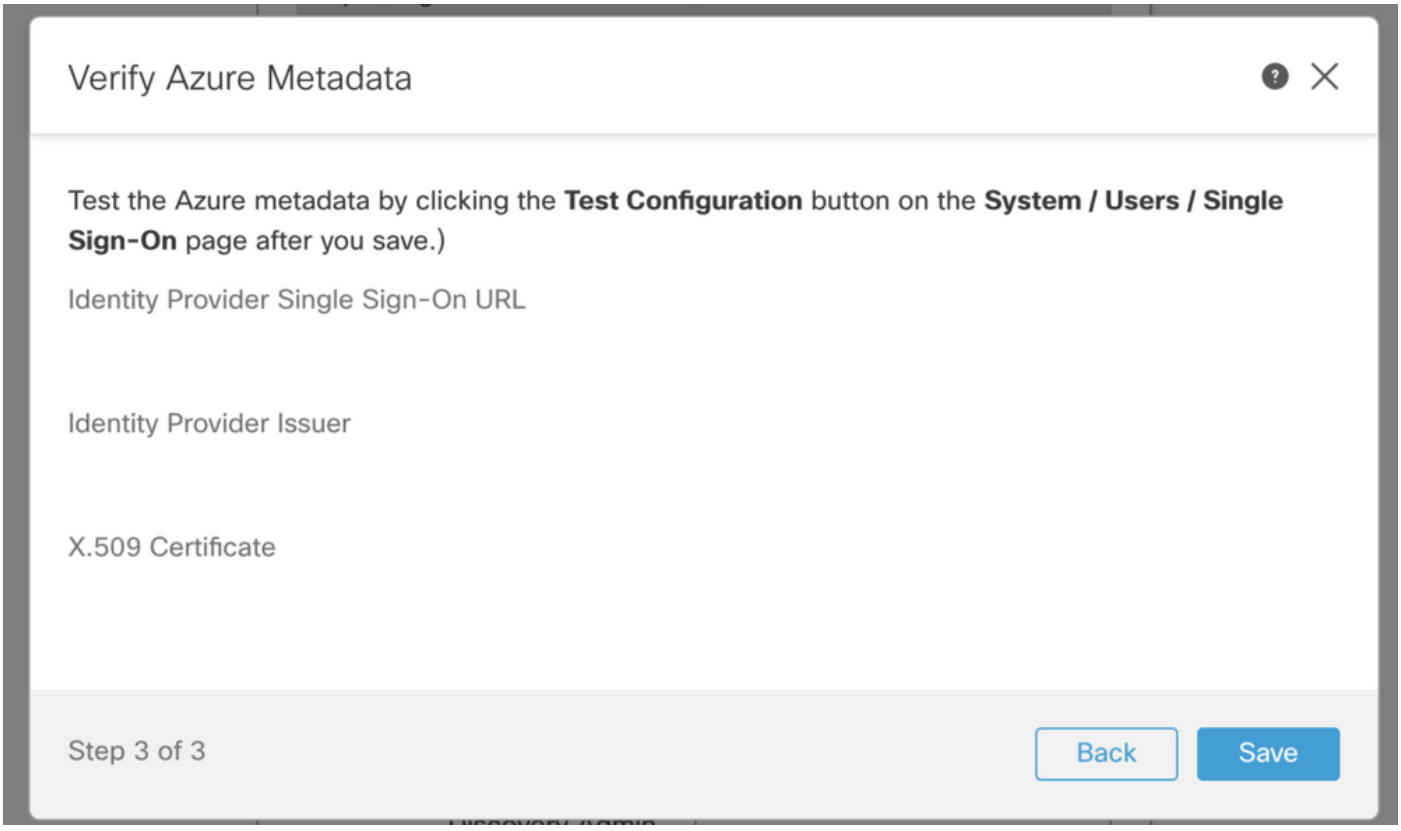
Configuração do Firepower Management Center

Etapa 1. Faça login no FMC, navegue para **Settings > Users > Single Sign-On** e Enable SSO. Selecione **Azure** como Provedor.



Etapa 2. Carregue o arquivo XML baixado do Azure aqui. Ele preenche automaticamente todos os detalhes necessários.

Etapa 3. Verifique a configuração e clique em **Salvar**, como mostrado nesta imagem.

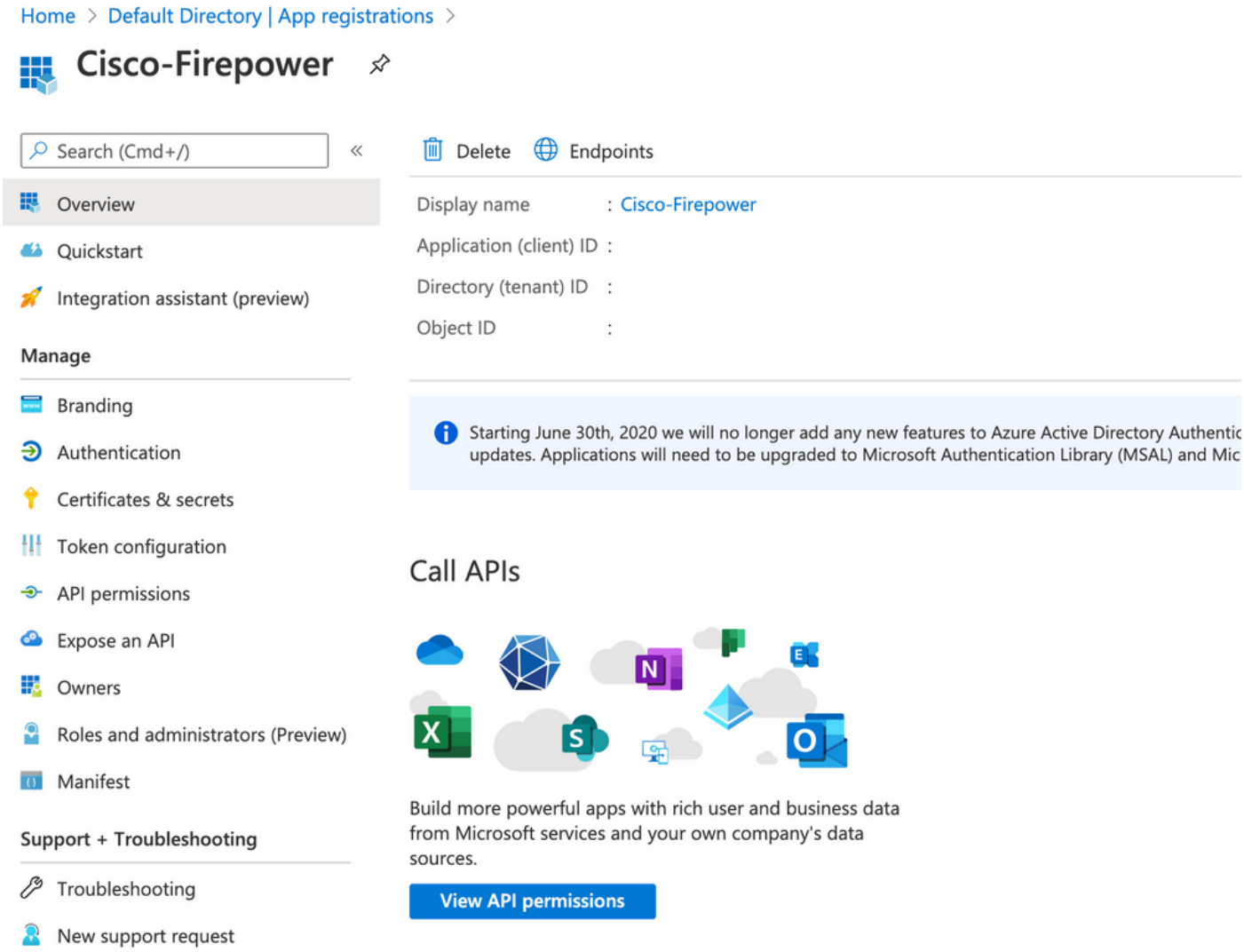


Configuração avançada - RBAC com Azure

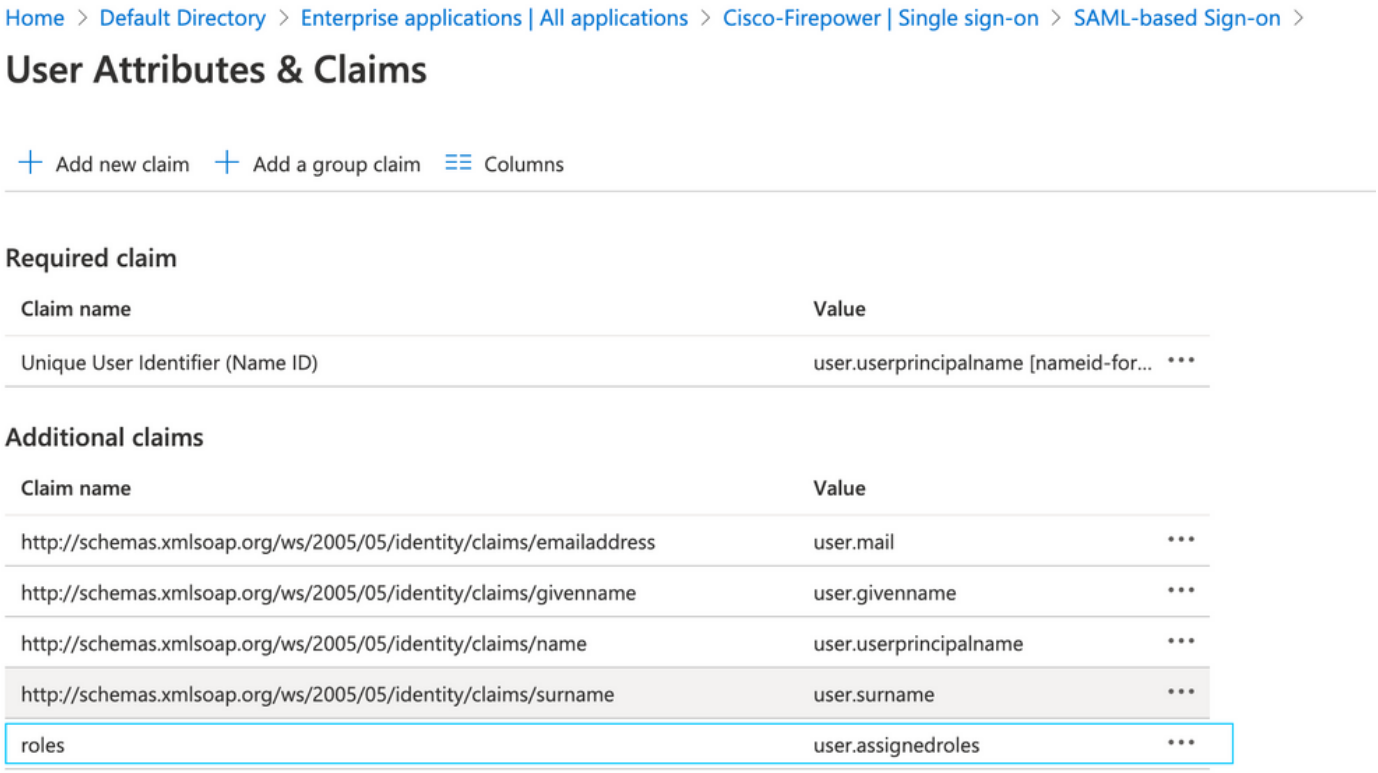
Para usar vários tipos de função para mapear para Funções do FMC - Você precisa editar o

manifesto do Aplicativo no Azure para atribuir valores a funções. Por padrão, as funções têm valor como Nulo.

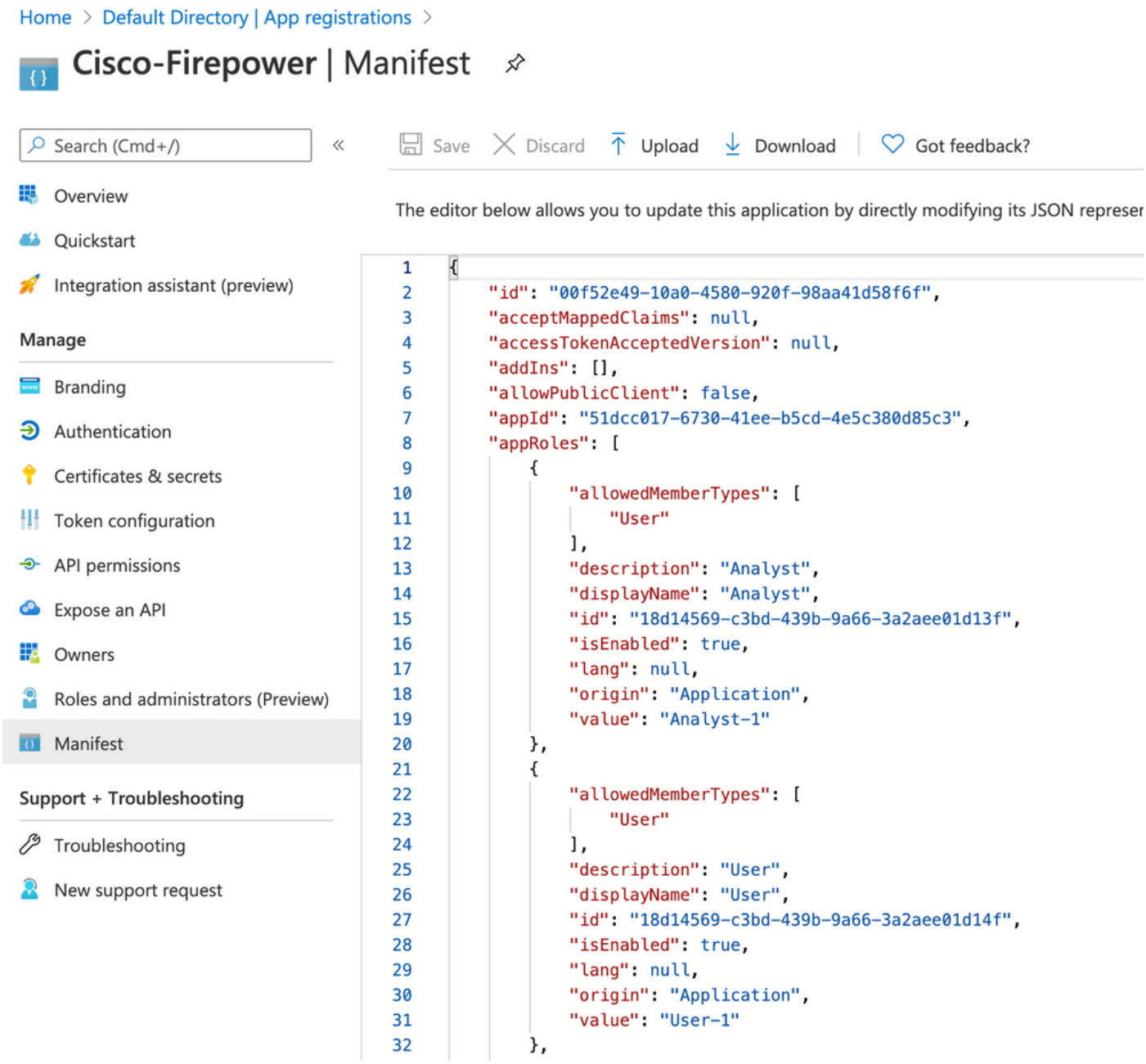
Etapa 1. Navegue até o **Aplicativo** criado e clique em **Logon único**.



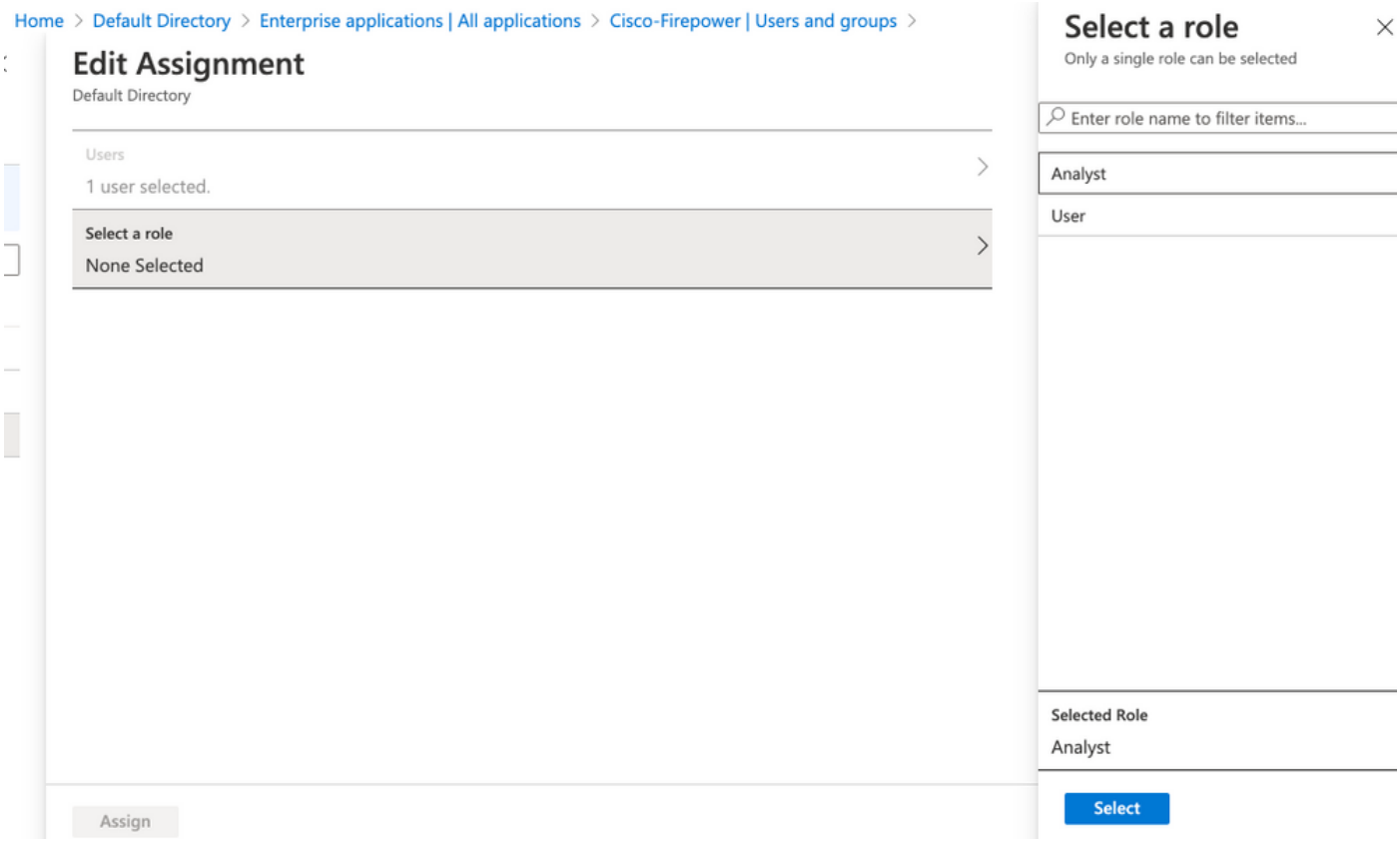
Etapa 2. Edite os atributos do usuário e as reivindicações. Adicionar uma nova reivindicação com o nome: **funções** e selecione o valor como **user.assignedroles**.



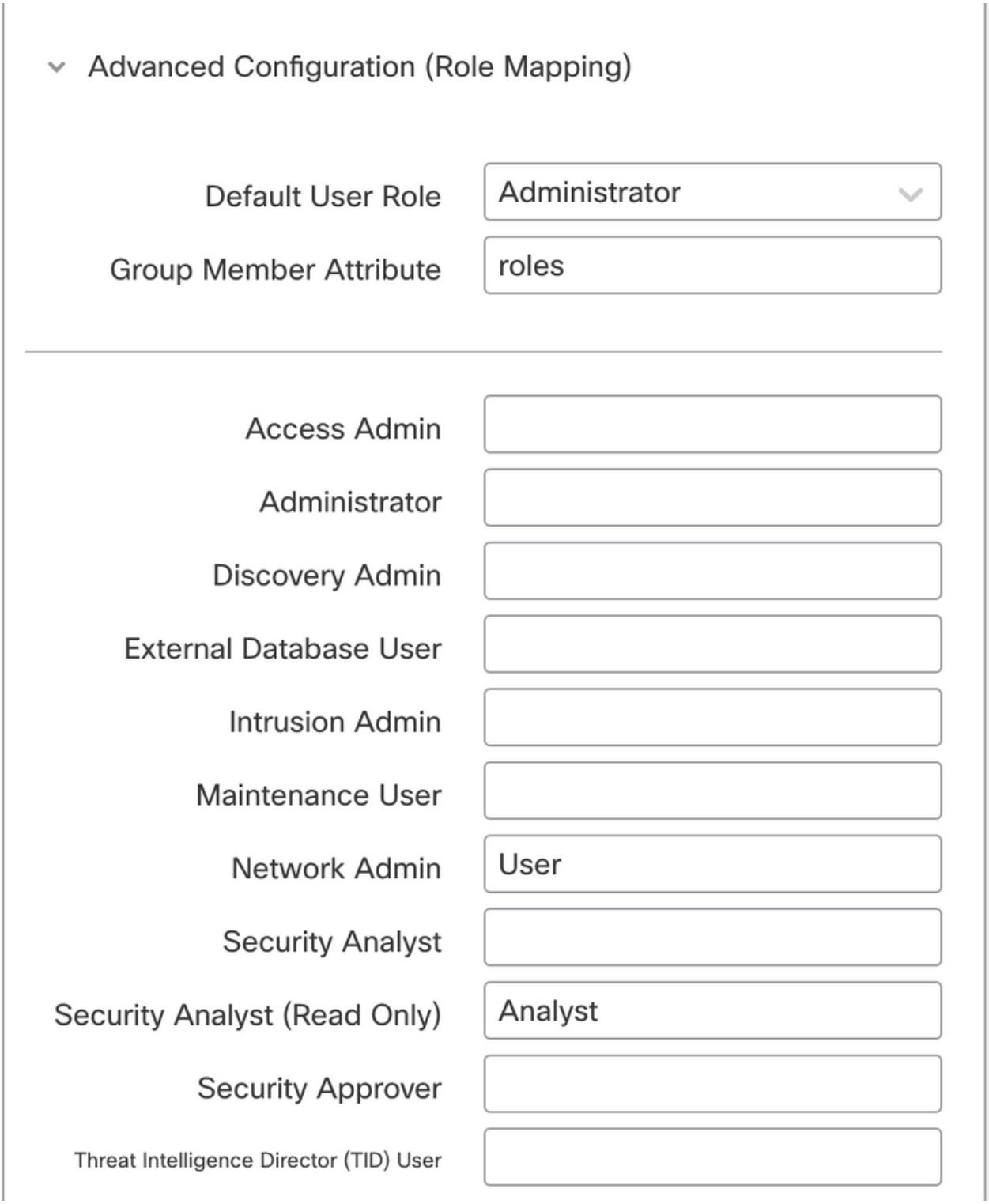
Etapa 3. Navegue até **<Application-Name> > Manifest**. Edite o Manifesto. O arquivo está no formato JSON e um usuário padrão está disponível para cópia. Por exemplo - aqui 2 funções são criadas: Usuário e analista.



Etapa 4. Navegue até **<Application-Name> > Users and Groups (Usuários e grupos)**. Edite o usuário e atribua as funções recém-criadas, como mostrado nesta imagem.



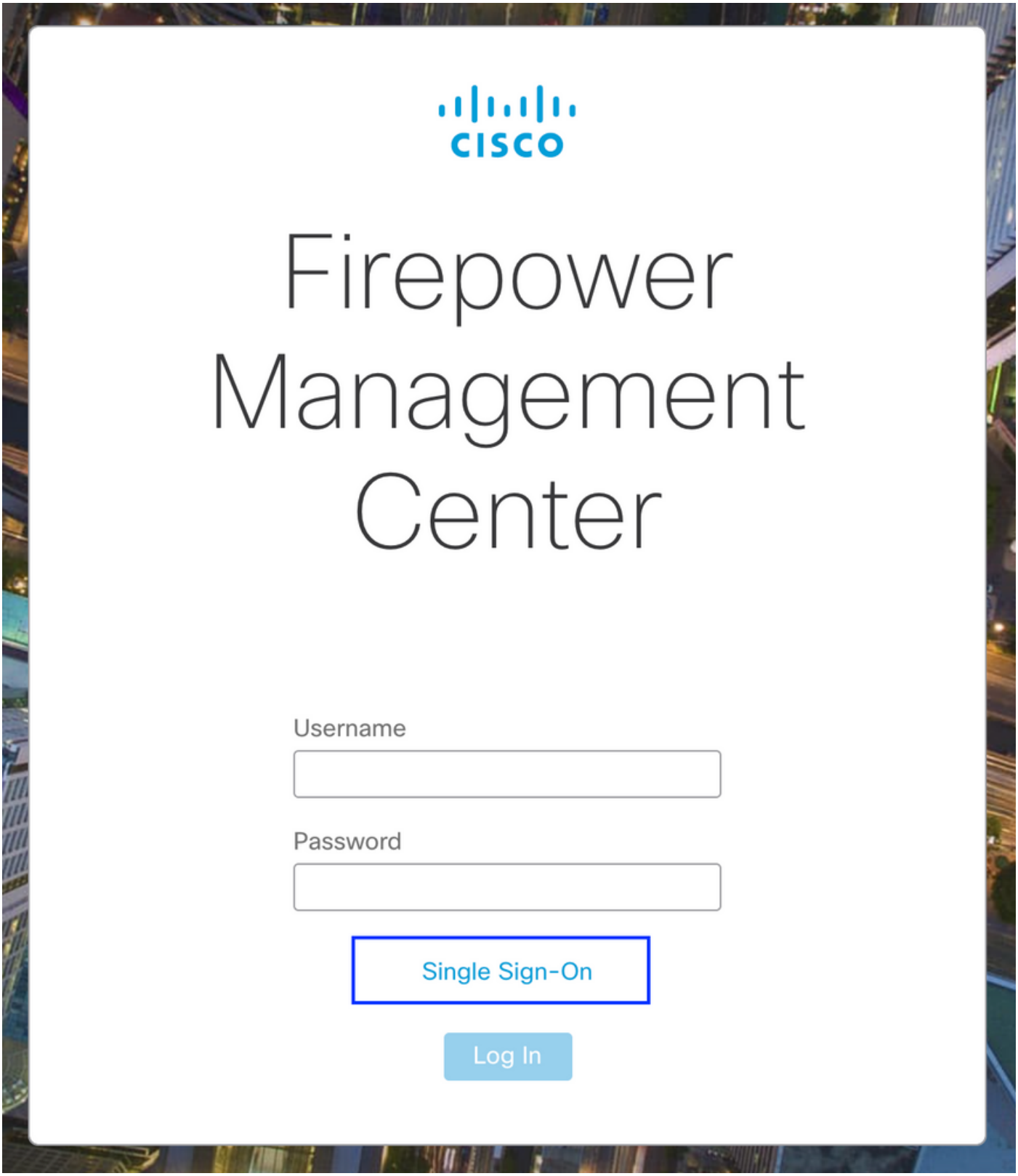
Etapa 4. Faça login no FMC e edite a Configuração avançada no SSO. Para, Atributo do membro do grupo: aatribua o **nome de exibição** que você forneceu no Manifesto do aplicativo às funções.



Depois que isso for feito, você poderá fazer login na função designada.

Verificar

Etapa 1. Navegue até a URL do FMC no seu navegador: https://<URL do FMC>. Clique em **Logon único**, como mostrado nesta imagem.



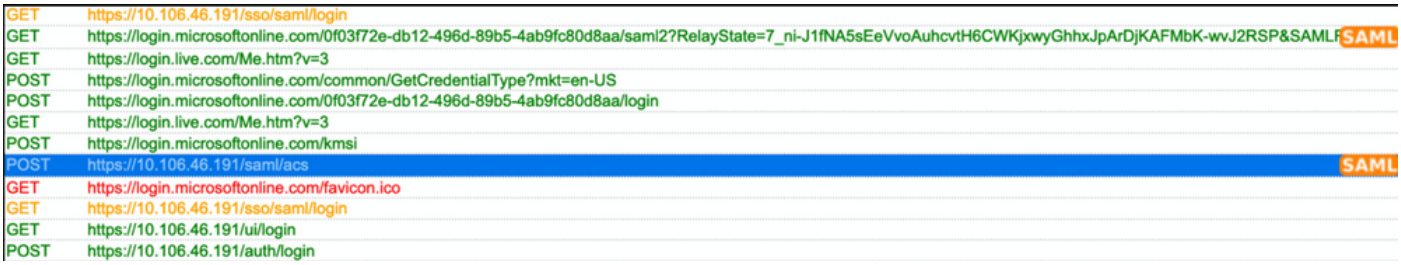
Você é redirecionado para a página de login da Microsoft e o login bem-sucedido retornará a página padrão do FMC.

Etapa 2. No FMC, navegue até **System > Users** para ver o usuário SSO adicionado ao banco de dados.

Troubleshoot

Verifique a autenticação SAML e este é o fluxo de trabalho que você obtém para uma autorização bem-sucedida (esta imagem é de um ambiente de laboratório):

Logs SAML do navegador



Logs SAML do FMC

Verifique os registros SAML no FMC em **/var/log/auth-daemon.log**