使用Azure作为身份提供程序配置FMC SSO

目录

简介

本文档介绍如何配置Firepower管理中心(FMC)单点登录(SSO)，将Azure作为身份提供程序(idP)。

安全断言标记语言(SAML)是使SSO成为可能的基础协议。公司维护一个登录页，后面是身份库和各种身份验证规则。它可以轻松配置支持SAML的任何Web应用，这允许您登录到所有Web应用。它还具有安全优势，既不强制用户维护（并可能重复使用）他们需要访问的每个Web应用的密码，也不向这些Web应用泄露密码。

先决条件

要求

Cisco 建议您了解以下主题：

- 对Firepower管理中心的基本了解
- 对单点登录的基本了解

使用的组件

本文档中的信息基于以下软件版本：

- 思科Firepower管理中心(FMC)版本6.7.0

- Azure - IdP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SAML术语

SAML的配置必须在两个位置完成：在IDP和SP。需要配置IdP，以便它知道用户要登录特定SP时向何处以及如何发送。 SP需要进行配置，以便它知道它可以信任由IdP签名的SAML断言。

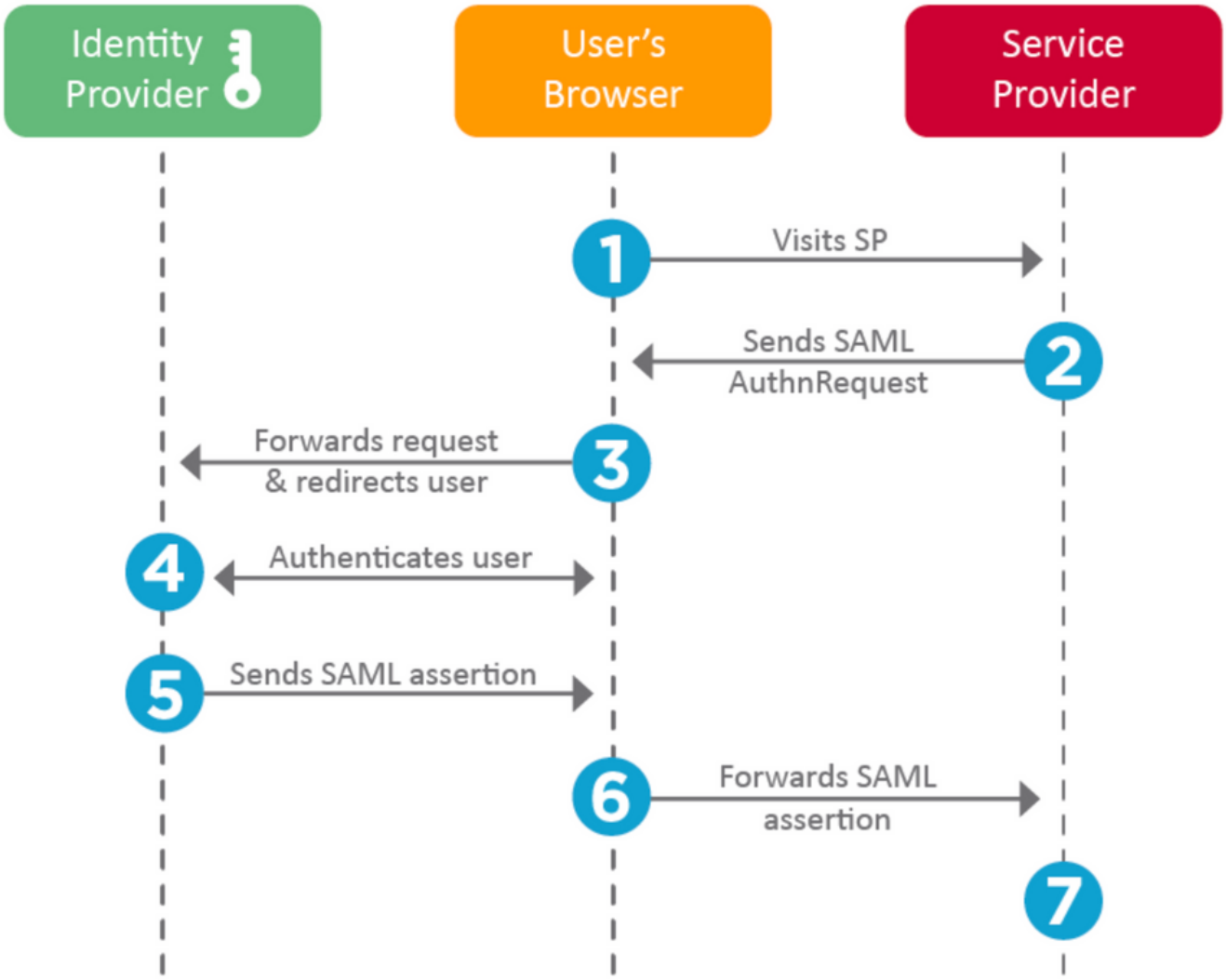
对SAML核心的几个术语的定义：

- 身份提供程序(IdP) — 执行身份验证的软件工具或服务（通常由登录页和/或控制面板可视化）；检查用户名和密码、验证帐户状态、调用双因素等。
- 服务提供商(SP) — 用户尝试访问的Web应用。
- SAML断言 — 通过浏览器重定向通过HTTP发送的断言用户身份和通常是其他属性的消息

IdP配置

SP提供SAML断言的规范、其应包含的内容以及其格式设置，并在IdP处设置。

- 实体ID - SP的全局唯一名称。格式不同，但越来越常见的情况是将此值设置为URL。
  示例： <https://<FQDN或IPaddress>/saml/metadata>
- 断言使用者服务(ACS)验证器 — 以正则表达式(regex)形式的安全措施，可确保SAML断言发送到正确的ACS。这仅在SP启动的登录期间发生，其中SAML请求包含ACS位置，因此此ACS验证器将确保SAML请求提供的ACS位置是合法的。
  示例：**https://<FQDN — 或 — IPaddress>/saml/acs**
- 属性 — 属性的数量和格式可能会有很大差异。通常至少有一个属性，名称ID，通常是尝试登录的用户的用户名。
- SAML签名算法 — SHA-1或SHA-256。SHA-384或SHA-512较少。此处提到此算法与X.509证书结合使用。



SP配置

与上述部分相反，本部分介绍IdP提供的信息，并在SP设置。

- 颁发者URL - IdP的唯一标识符。格式化为包含有关IdP信息的URL，以便SP可以验证其接收的SAML断言是否从正确的IdP发出。
  示例： <saml:Issuer https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/ >
- SAML SSO终端/服务提供商登录URL — 当SP通过SAML请求重定向到此时启动身份验证的IdP终端。
  示例：https://login.microsoftonline.com/023480840129412-824812/saml2
- SAML SLO（单次注销）终端 — SP重定向到此处时关闭IdP会话的IdP终端，通常在单击注销后。
  示例：`https://access.wristbandtent.com/logout`

FMC上的SAML

FMC中的SSO功能从6.7开始引入。新功能简化了FMC授权(RBAC)，因为它将现有信息映射到FMC角色。它适用于所有FMC UI用户和FMC角色。目前，它支持SAML 2.0规范，并且这些支持的IDP

- 奥克塔
- OneLogin
- PingID
- Azure AD
- 其他（任何符合SAML 2.0的IDP）

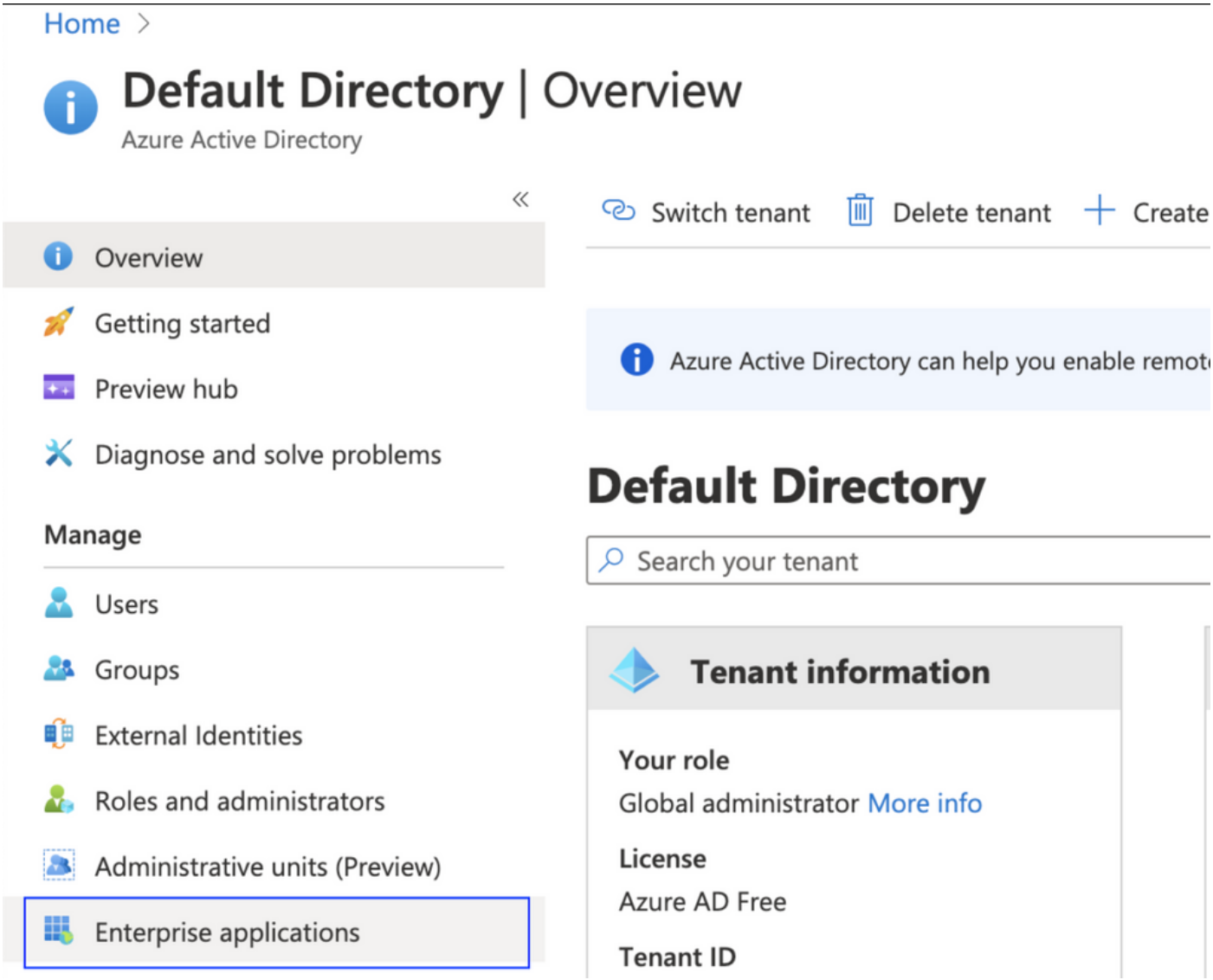
限制与问题说明

- SSO只能配置为全局域。
- HA对中的FMC需要单独配置。
- 只有本地/AD管理员可以配置单点登录。
- 不支持从Idp启动的SSO。

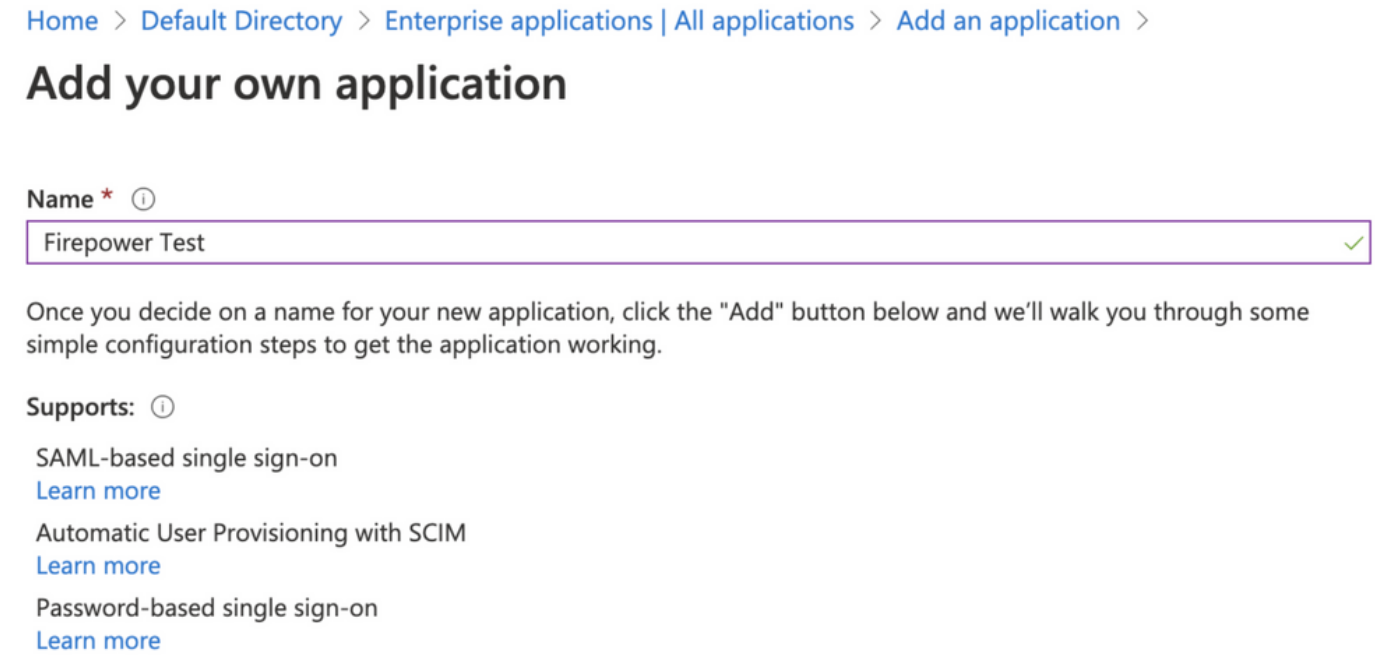
配置

身份提供程序上的配置

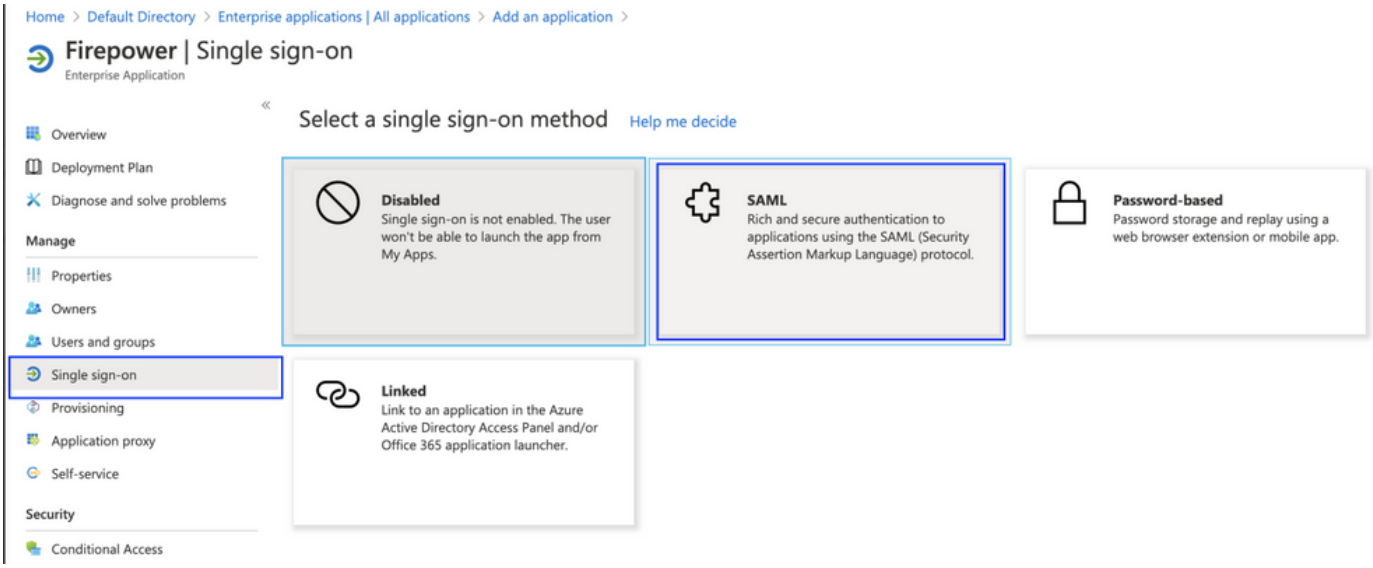
步骤1.登录Microsoft Azure。导航至**Azure Active Directory >企业应用程序**。



- 步骤2.在“**非库应**用程序”下创建新应用程序，如下图所示。

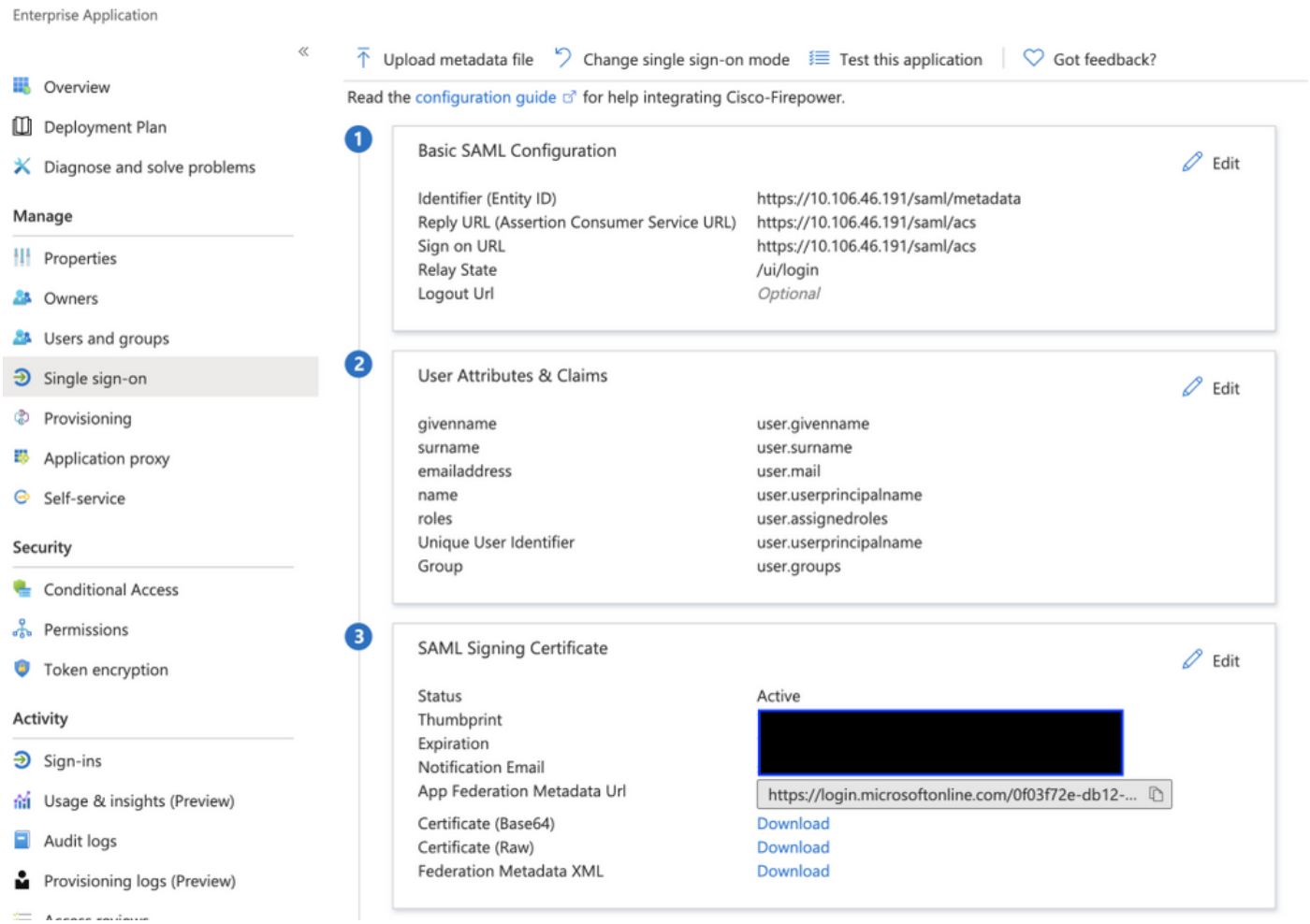


步骤3.编辑已创建的应用并导航至**Set up single sign on > SAML**，如下图所示。



步骤4.编辑基本SAML配置并提供FMC详细信息：

- FMC URL: **https://<FMC-FQDN — 或 — IPaddress>**
- 标识符（实体ID）： **https://<FMC-FQDN — 或 — IPaddress>/saml/metadata**
- 回复URL: **https://<FMC-FQDN — 或 — IPaddress>/saml/acs**
- 登录URL: **/https://<FMC-QDN-or-IPaddress>/saml/acs**
- RelayState:**/ui/login**

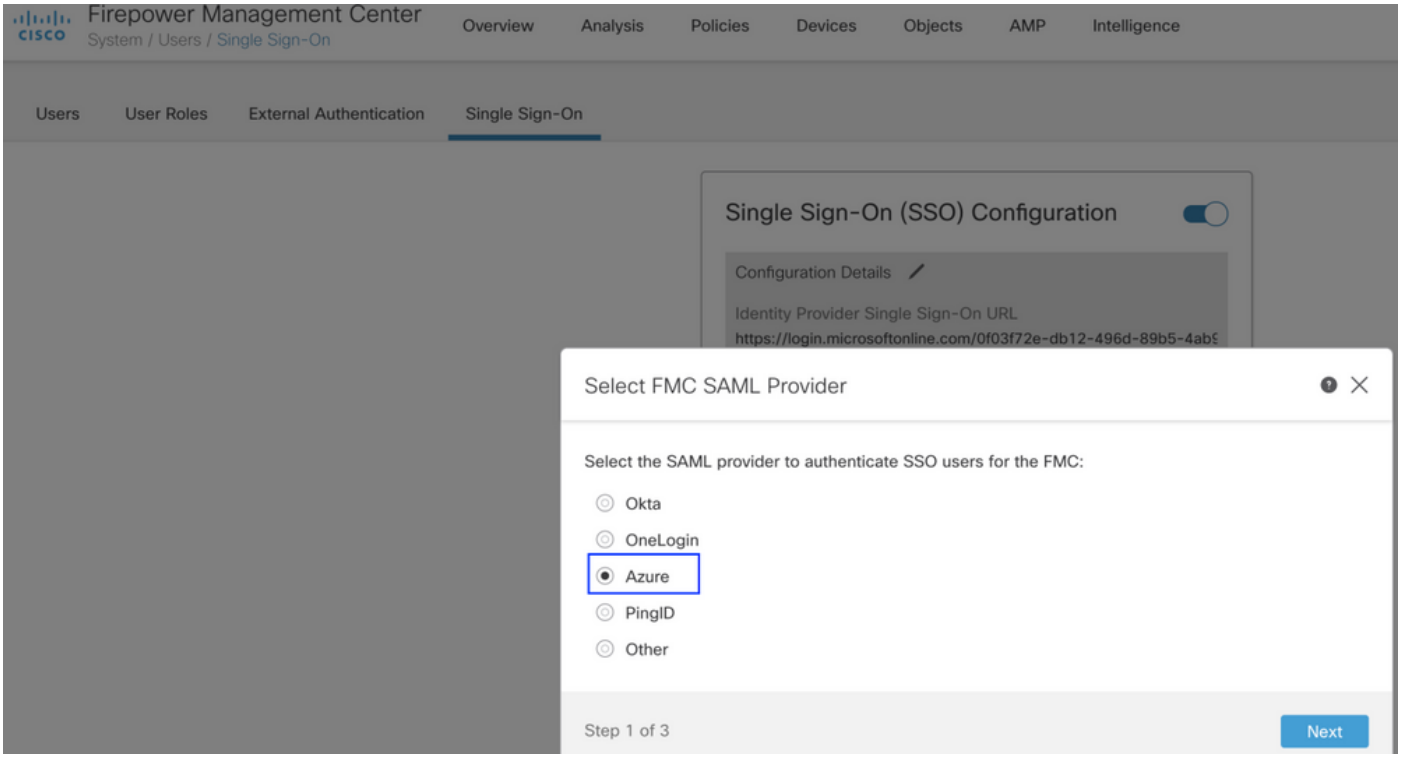


将其余内容保留为默认值 — 基于角色的访问将进一步讨论。

这将标记身份提供程序配置的结束。下载将用于FMC配置的联合元数据XML。

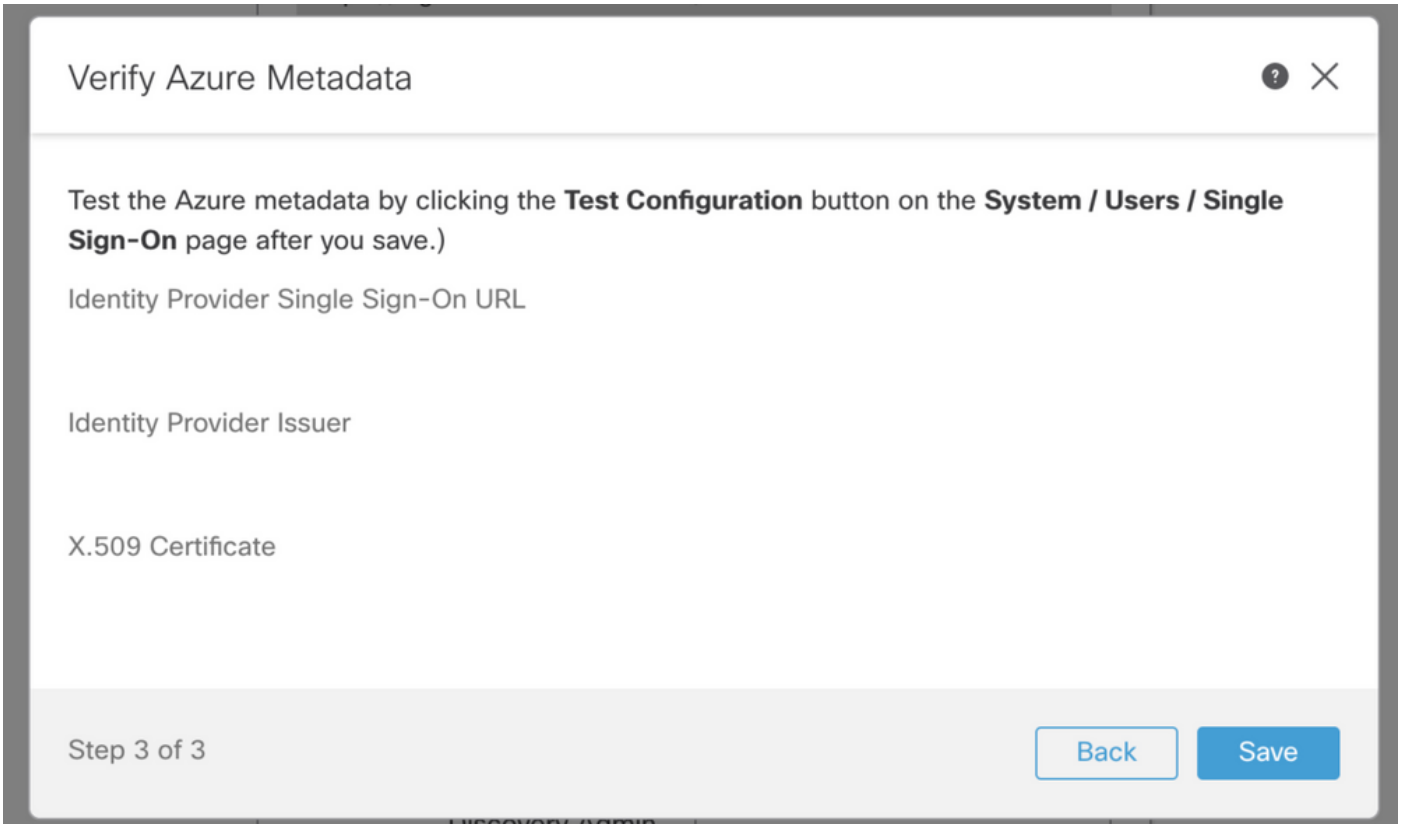
在Firepower管理中心上配置

步骤1.登录FMC，导航至**Settings > Users > Single Sign-On**并启用SSO。选择**Azure**作为提供程序。



步骤2.上传从Azure下载的XML文件。自动填充所需的所有详细信息。

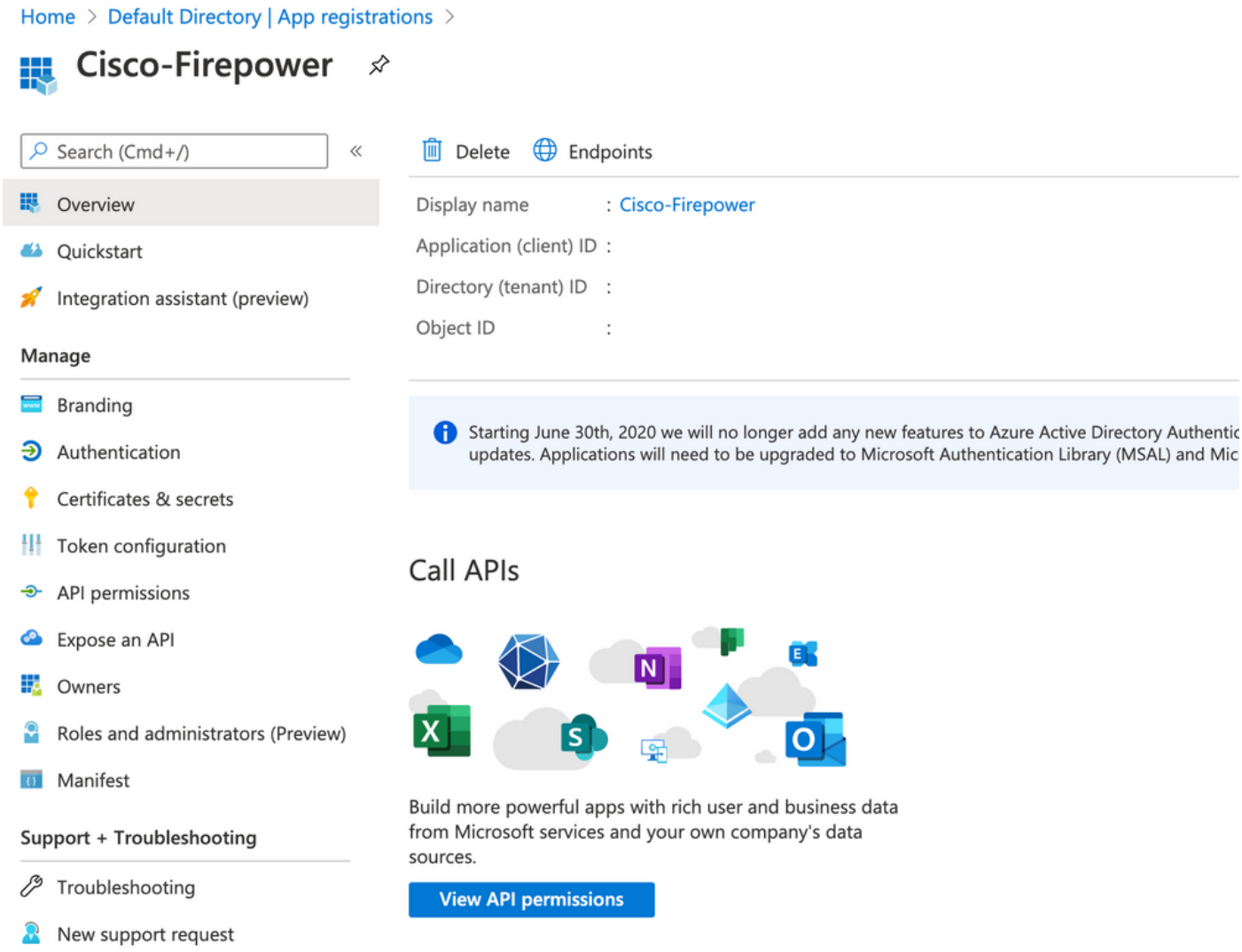
步骤3.检验配置并单击**Save**，如下图所示。



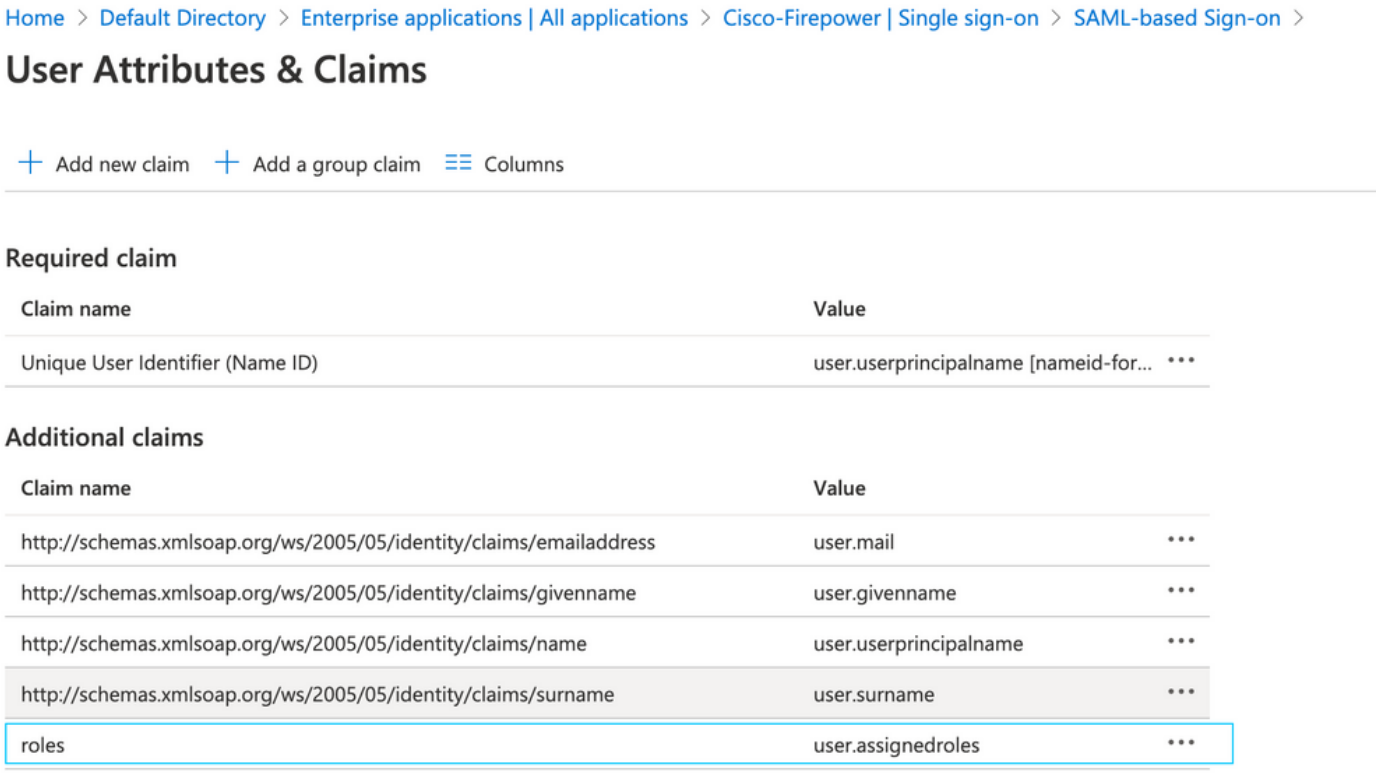
高级配置 — RBAC与Azure

要使用各种角色类型映射到FMC的角色 — 您需要编辑Azure上应用程序的清单，以向角色分配值。默认情况下，角色的值为Null。

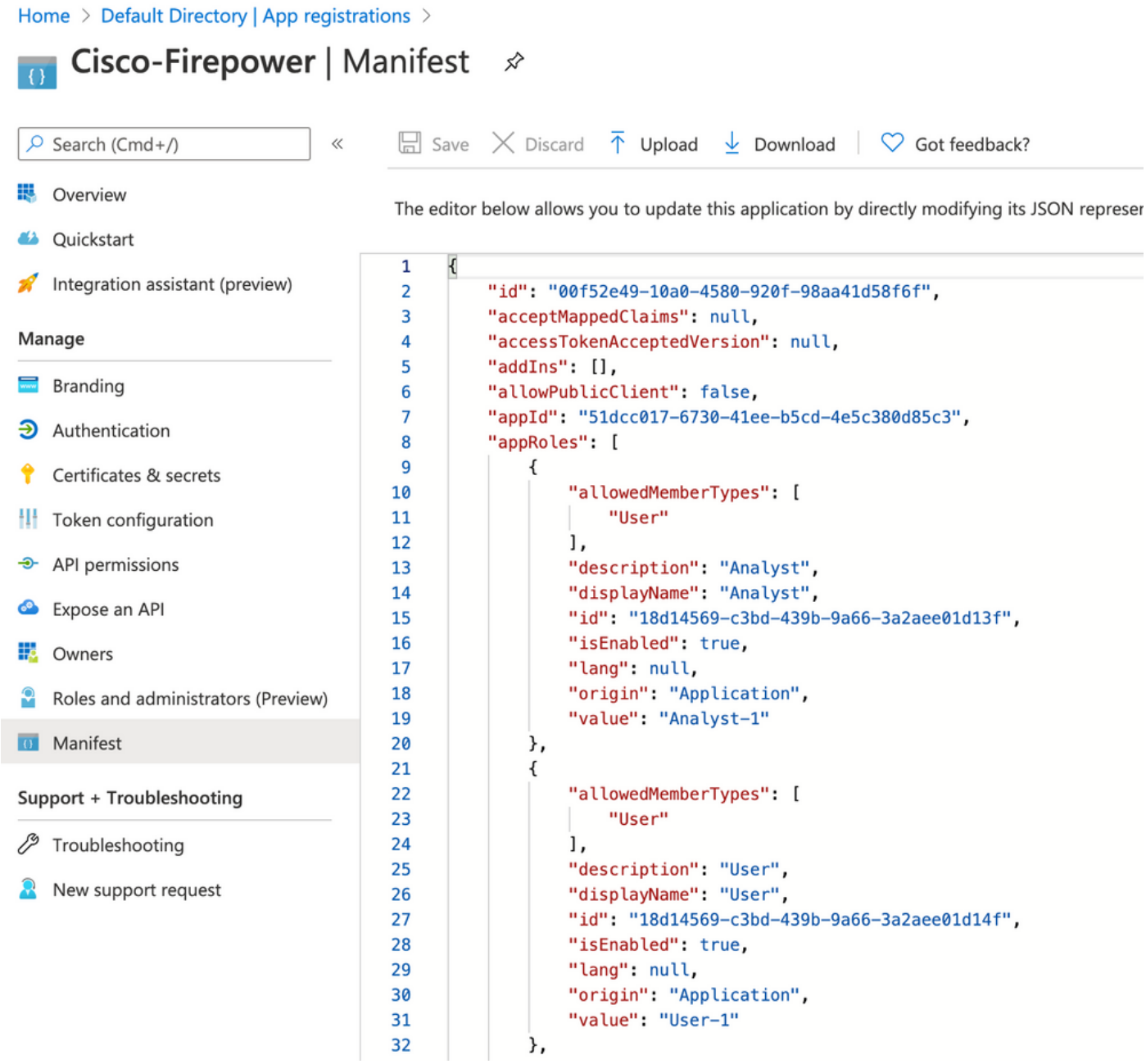
步骤1.导航至已创**建的**应用程序，然后单**击单点登录**。



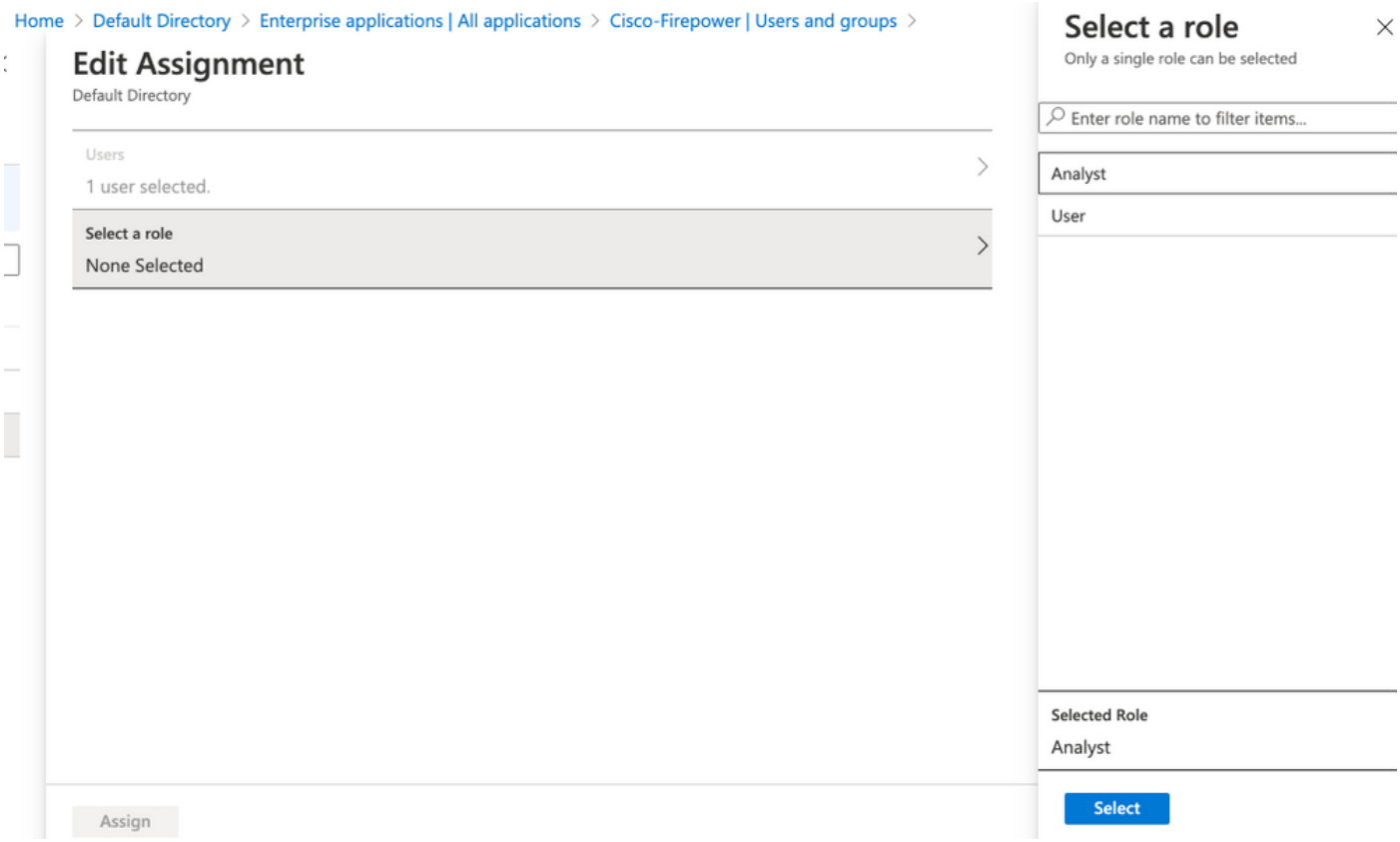
步骤2.编辑用户属性和声明。添加名称为：**角色**，并选择值**user.assignedroles**。



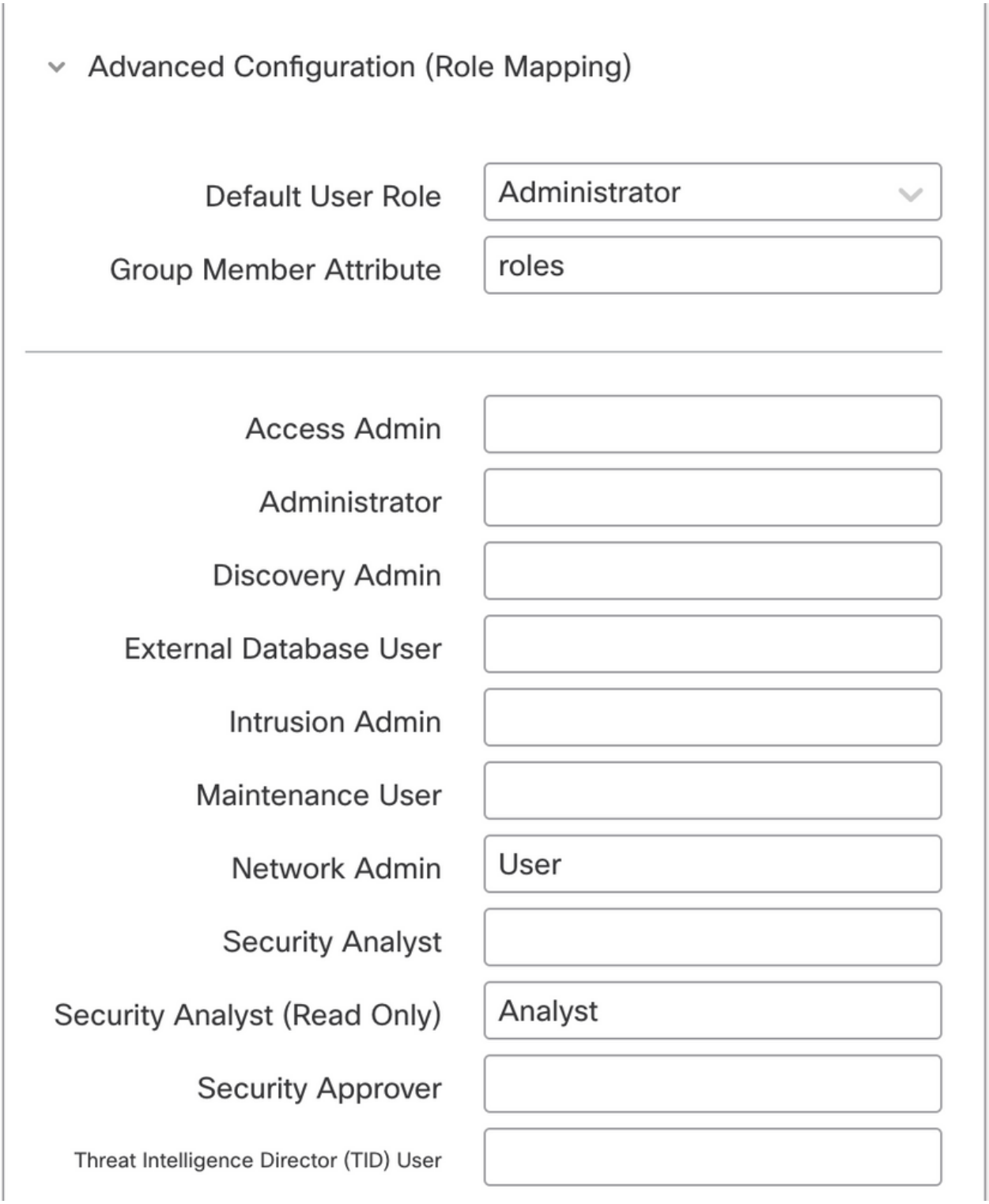
步骤3.导航至**<Application-Name> > Manifest**。 编辑清单。文件为JSON格式，默认用户可供复制。例如，此处创建了2个角色：用户和分析师。



步骤4.导航至<Application-Name> > Users and Groups。编辑用户并分配新创建的角色，如下图所示。



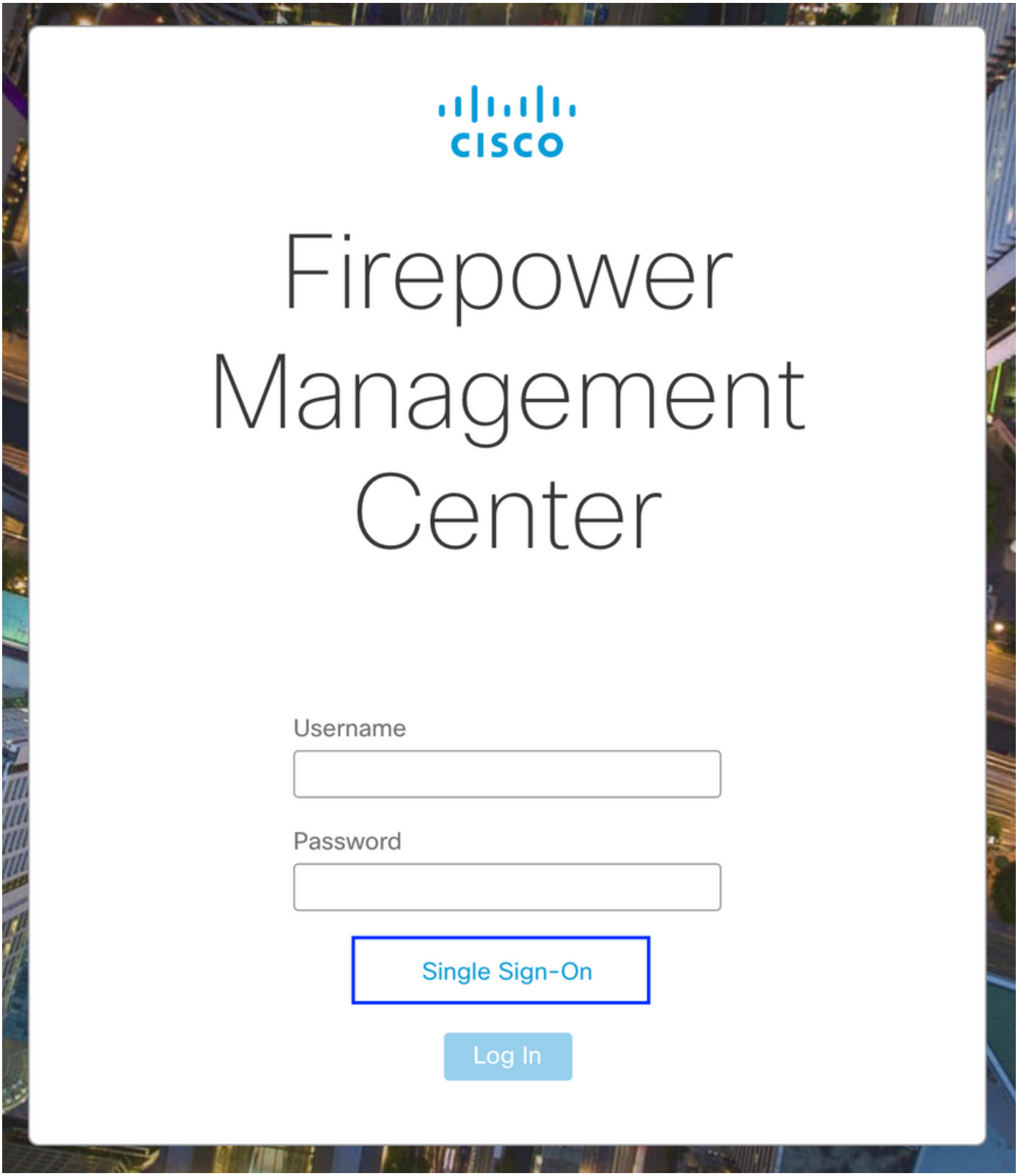
步骤4.登录FMC并编辑SSO中的高级配置。对于， 组成员属性：a将您在Application Manifest中提供的“显示名称”(Display name)指定给角色。



完成后，您应能登录到其指定角色。

验证

步骤1.从浏览器导航至FMC URL:https://<FMC URL>。单击**Single Sign-On**，如此图所示。



您被重定向到Microsoft登录页面，成功登录将返回FMC默认页面。

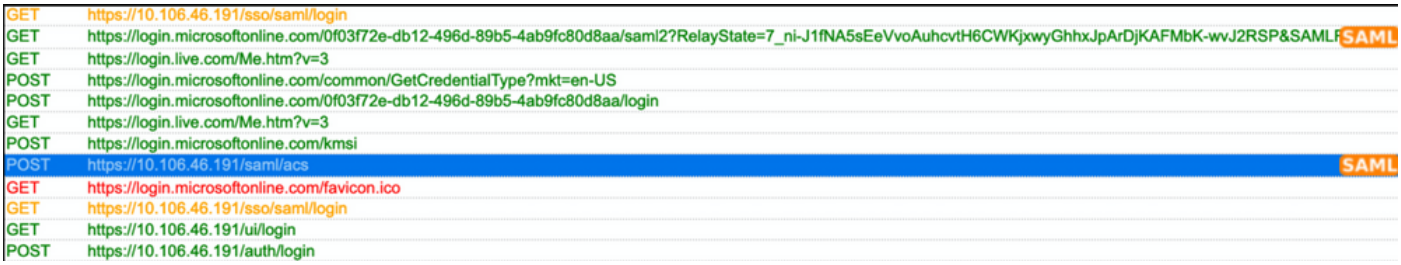
步骤2.在FMC上，导航至**System > Users**，查看已添加到数据库的SSO用户。

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

故障排除

验证SAML身份验证，这是您为成功授权而实现的工作流程（此映像属于实验环境）：

浏览器SAML日志



FMC SAML日志

在/var/log/auth-daemon.log上验证FMC上的SAML日志