

使用Azure作为身份提供程序配置FMC SSO

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[IdP配置](#)

[SP配置](#)

[FMC上的SAML](#)

[限制与问题说明](#)

[配置](#)

[身份提供程序上的配置](#)

[在Firepower管理中心上配置](#)

[高级配置 — RBAC与Azure](#)

[验证](#)

[故障排除](#)

[浏览器SAML日志](#)

[FMC SAML日志](#)

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。

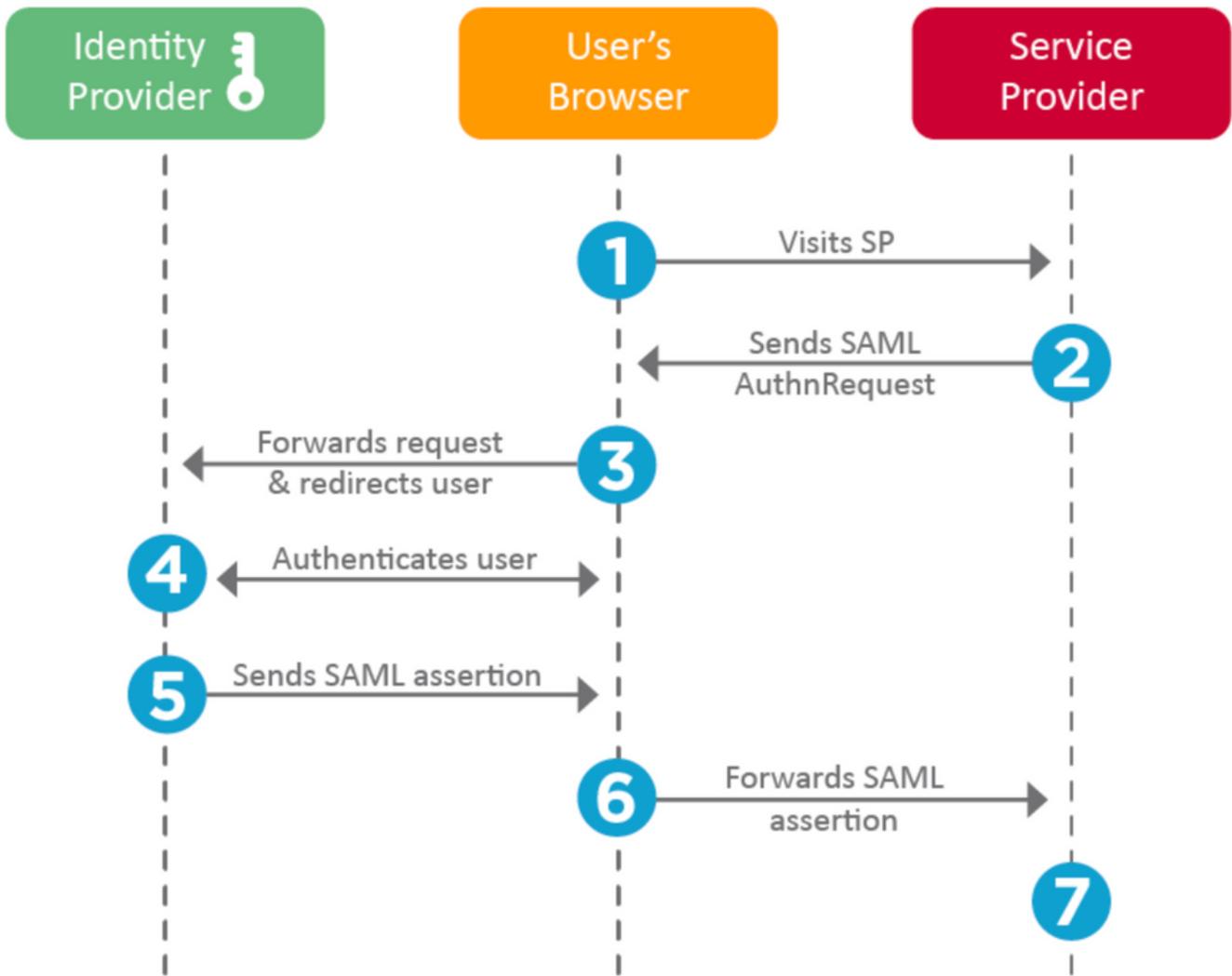
对SAML核心的几个术语的定义：

- 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**。

The screenshot shows the Azure Active Directory 'Default Directory | Overview' page. The page has a navigation menu on the left with the following items: Overview (selected), Getting started, Preview hub, Diagnose and solve problems, Manage (Users, Groups, External Identities, Roles and administrators, Administrative units (Preview), and Enterprise applications (highlighted with a blue box)). The main content area includes a search bar labeled 'Search your tenant', a 'Tenant information' section with details like 'Your role: Global administrator', 'License: Azure AD Free', and 'Tenant ID'. At the top right, there are actions: 'Switch tenant', 'Delete tenant', and 'Create'. A notification banner at the top right states: 'Azure Active Directory can help you enable remot...'

- 步骤2.在“**非库应用程序**”下创建新应用程序，如下图所示。

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](#)

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。

The screenshot shows the 'Single sign-on' configuration page for an application named 'Firepower'. The page title is 'Firepower | Single sign-on' and it is categorized as an 'Enterprise Application'. The left-hand navigation pane includes sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Users and groups), Single sign-on (highlighted), Provisioning, Application proxy, Self-service, Security, and Conditional Access. The main content area is titled 'Select a single sign-on method' and offers four options: 'Disabled' (not enabled), 'SAML' (rich and secure authentication), 'Password-based' (password storage and replay), and 'Linked' (link to an application in the Azure Active Directory Access Panel). The 'SAML' option is highlighted with a blue border.

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](https://<FMC-QDN-or-IPaddress>/saml/acs)
- RelayState:/ui/login

Manage

Security

Activity

Read the [configuration guide](#) for help integrating Cisco-Firepower.

1 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	<i>Optional</i>

2 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

3 SAML Signing Certificate [Edit](#)

Status	Active
Thumbprint	<div style="background-color: black; width: 100%; height: 1.2em;"></div>
Expiration	
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

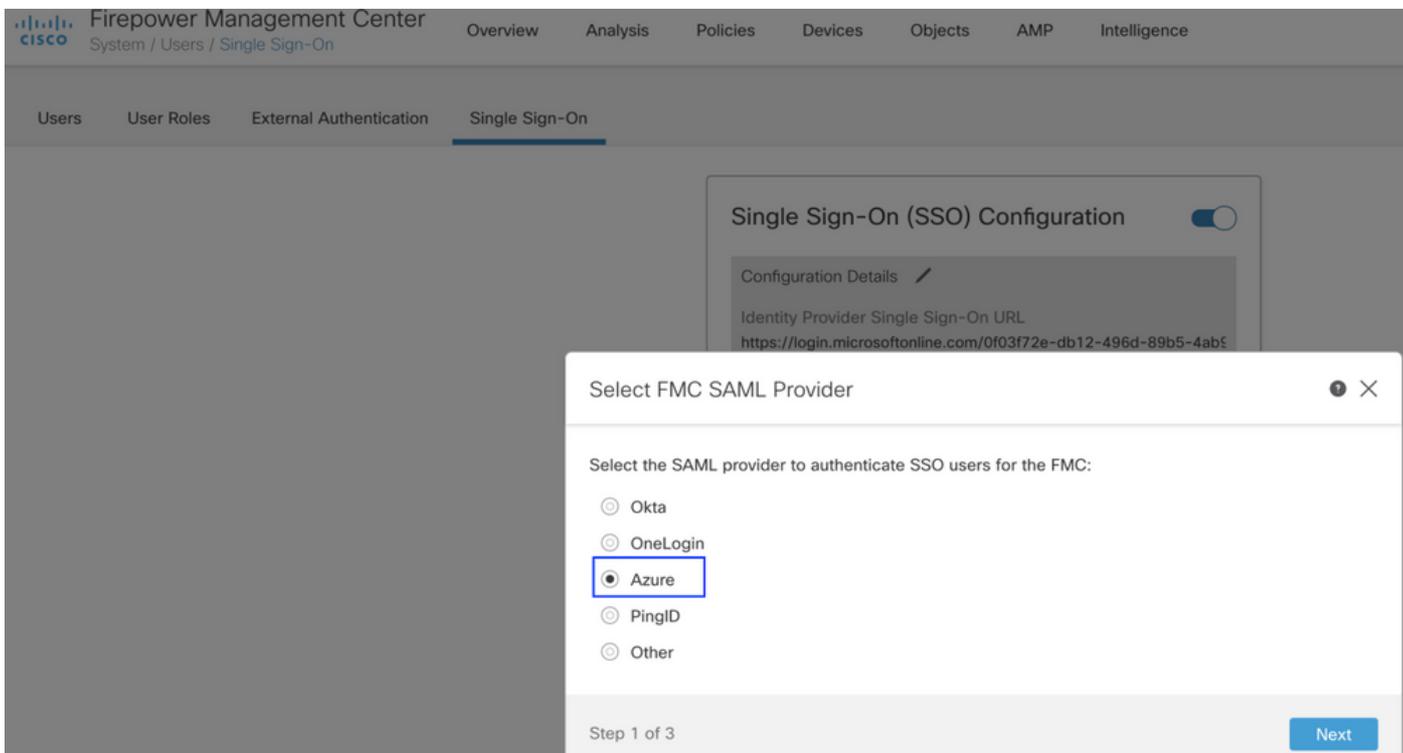
将其余内容保留为默认值 — 基于角色的访问将进一步讨论。

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。

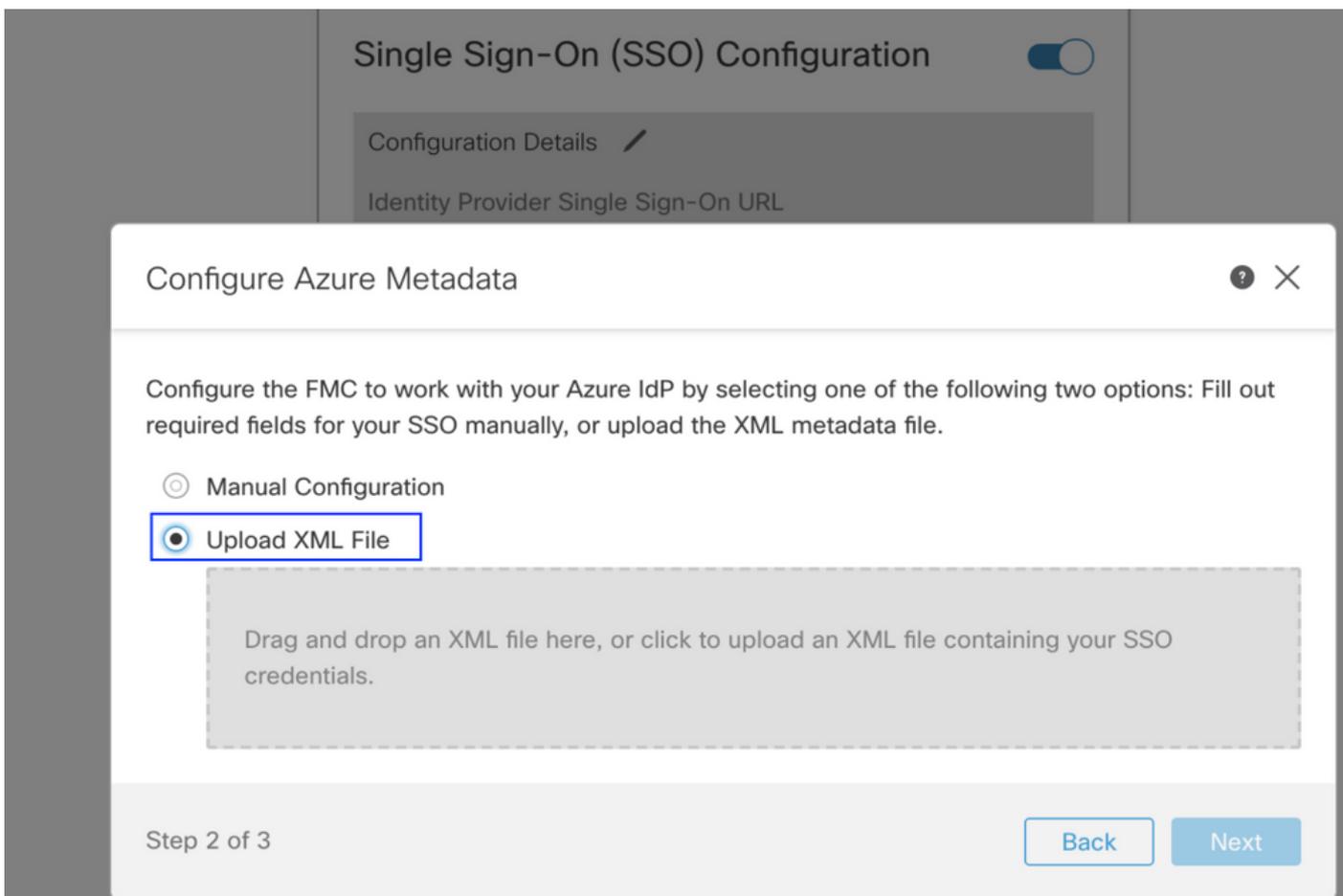
在Firepower管理中心上配置

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

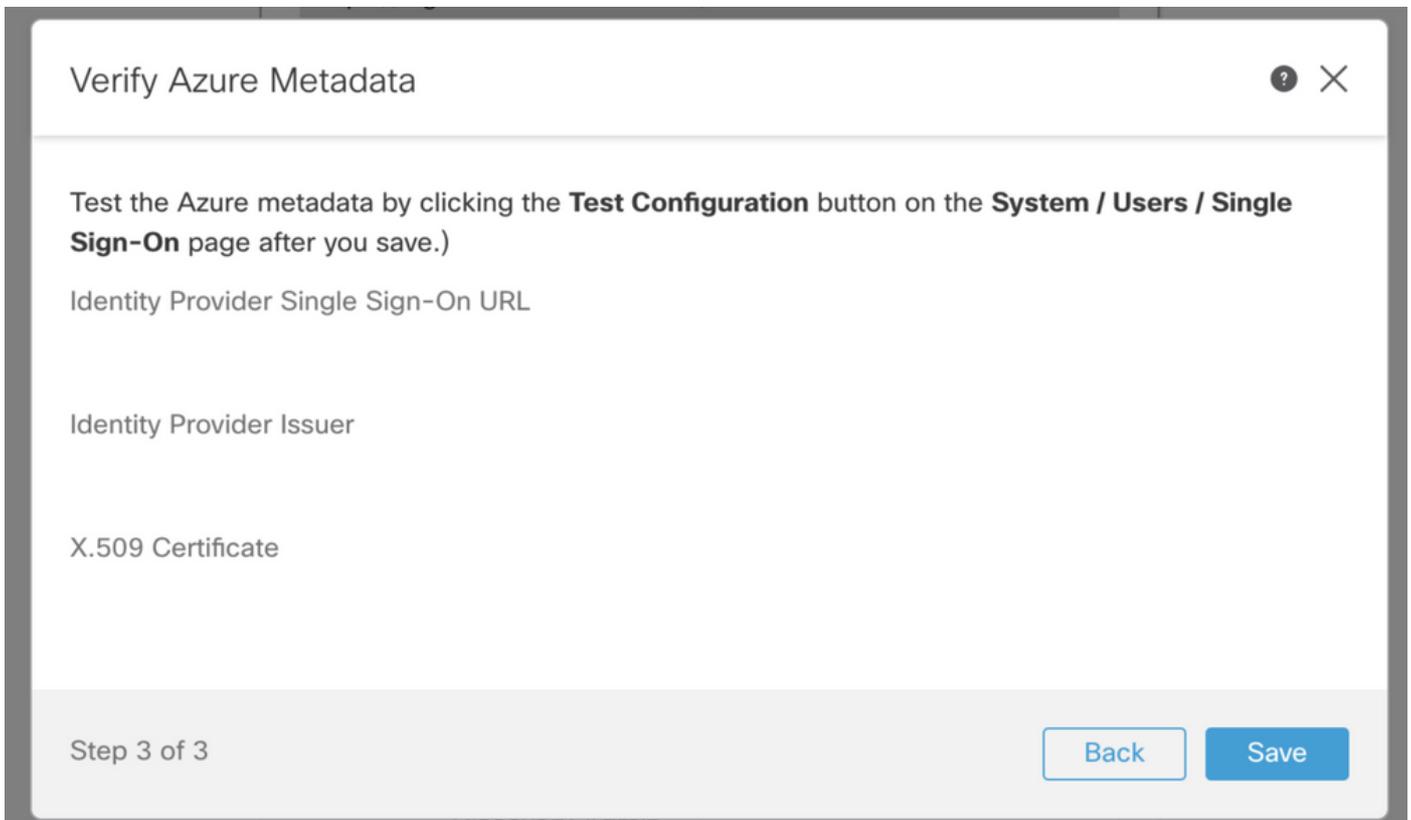
。



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。

Cisco-Firepower

<<

 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 Authentication 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](#)

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。

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 ***

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。

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

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。

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

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。

▼ 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	User
Security Analyst	
Security Analyst (Read Only)	Analyst
Security Approver	
Threat Intelligence Director (TID) User	

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。



Firepower Management Center

Username

Password

Single Sign-On

Log In

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@shbhartisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbhartisco.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

GET	https://10.106.46.191/sso/saml/login
GET	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/saml2?RelayState=7_ni-J1fNA5eEeVvoAuhcvtH6CWKjxwyGhnxJpArDjKAFMbK-wvJ2RSP&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
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日志

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

```
root@shbharti11ffncl1:/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-56574e8a5f44bdd50102743d2cc9350b75f74d8c
auth-daemon 2020/08/09 04:59:11 I! Authorizing Response, ID : id-56574e8a5f44bdd50102743d2cc9350b75f74d8c
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] h
http://schemas.microsoft.com/identity/claims/objectid [b5-4ab9fc80d8aa/] http://schemas
.microsoft.com/identity/claims/objectid [a] http://schemas.xmlsoap.org/w
/2005/05/identity/claims/givenname:[Test 1] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[test@shbhartiisco.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-56574e8a5f44bdd50102743d2cc9350b75f74d8c, URI : /sso/saml/login
```