

アイデンティティプロバイダーとしてAzureを使用したFMC SSOの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[IdPの設定](#)

[SPの設定](#)

[FMCのSAML](#)

[制限および警告](#)

[設定](#)

[アイデンティティプロバイダーの設定](#)

[Firepower Management Centerの設定](#)

[高度な構成 – AzureによるRBAC](#)

[確認](#)

[トラブルシューティング](#)

[ブラウザのSAMLログ](#)

[FMC SAMLログ](#)

概要

このドキュメントでは、アイデンティティプロバイダー(idP)としてAzureを使用してFirepower Management Center(FMC)シングルサインオン(SSO)を設定する方法について説明します。

Security Assertion Markup Language(SAML)は、SSOを可能にする基盤プロトコルとして最も頻繁に使用されます。ある企業が単一のログインページを維持し、その背後にアイデンティティストアとさまざまな認証ルールがあります。SAMLをサポートする任意のWebアプリケーションを簡単に設定でき、すべてのWebアプリケーションにログインできます。また、アクセスが必要なすべてのWebアプリのパスワードをユーザーに強制的に保持(および再利用の可能性のある)させたり、それらのWebアプリにパスワードを公開したりしないことによるセキュリティ上の利点もあります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center(FMC)の基礎知識
- シングルサインオンに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Firepower Management Center(FMC)バージョン6.7.0
- Azure - IdP

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SAML用語

SAMLの設定は、次の2つの場所で行う必要があります。IdPとSPで確認できますIdPを設定して、特定のSPにログインする際にユーザを送信する場所と方法を把握する必要があります。SPは、IdPによって署名されたSAMLアサーションを信頼できるように設定する必要があります。

SAMLの中核となる用語の定義：

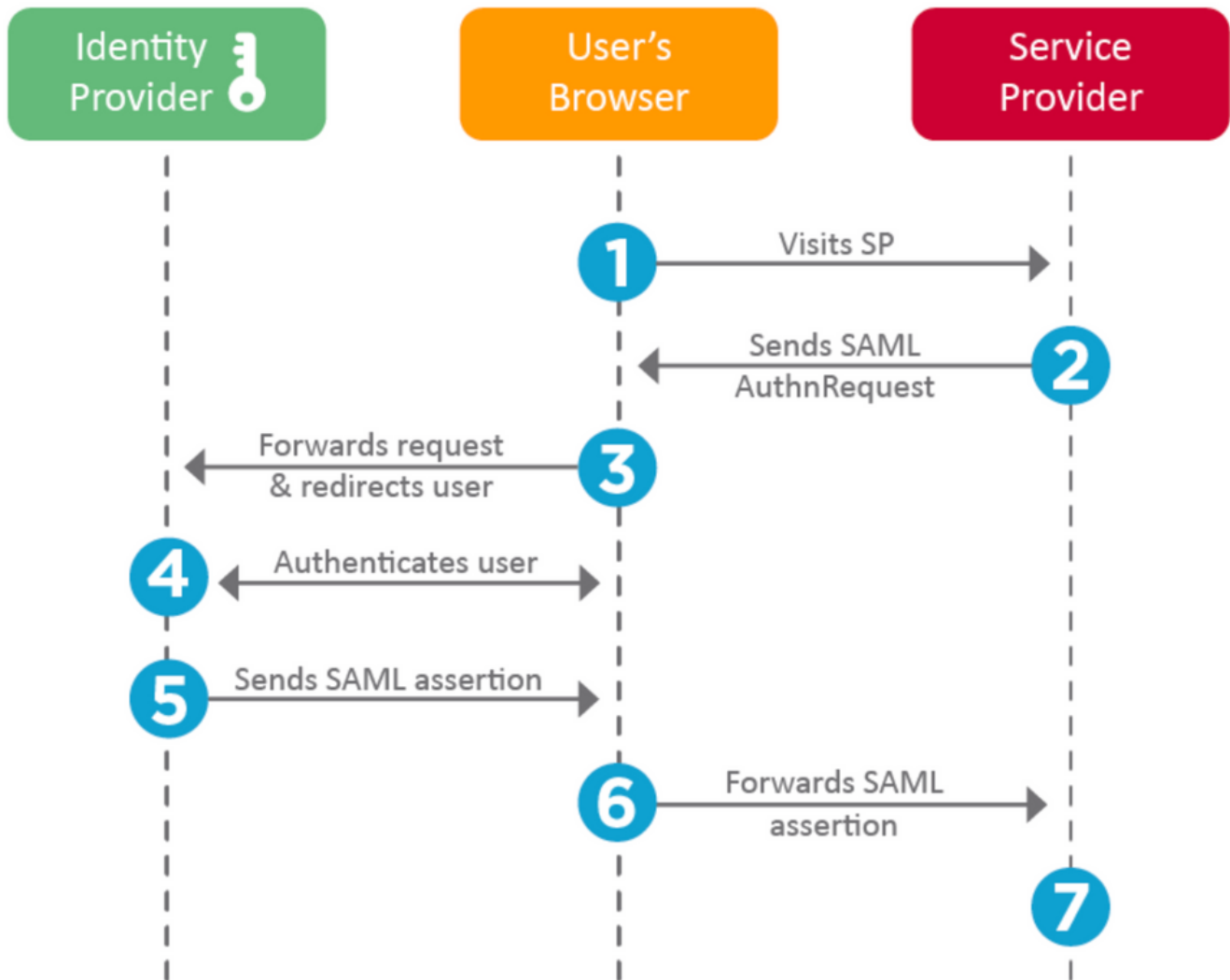
- Identity Provider(IdP)：認証を実行するソフトウェアツールまたはサービス（通常はログインページやダッシュボードで視覚化）。ユーザ名とパスワードの確認、アカウントのステータスの確認、2ファクタの呼び出しなど
- サービスプロバイダー(SP)：ユーザがアクセスを試行するWebアプリケーション。
- SAMLアサーション：ユーザのIDおよびその他の属性をアサーションするメッセージ。ブラウザリダイレクトを介してHTTPで送信されます。

IdPの設定

SAMLアサーションの仕様、内容、フォーマット方法は、SPによって提供され、IdPで設定されません。

- EntityID:SPのグローバルに一意的な名前。形式は異なりますが、この値をURL形式で表示することは一般的になってきています。
例：<https://<FQDNまたはIPアドレス>/saml/metadata>
- Assertion Consumer Service(ACS)Validator - SAMLアサーションが正しいACSに送信されることを保証する、正規表現(regex)形式のセキュリティ測定値。これは、SAML要求にACSの場所が含まれるSP開始ログイン時にのみ実行されるため、このACS検証ツールは、SAML要求が提供するACSの場所が正当であることを確認します。
例：<https://<FQDN-or-IPaddress>/saml/acs>
- 属性：属性の数と形式は大きく異なります。通常、少なくとも1つの属性nameIDが存在します。これは通常、ログインを試みるユーザのユーザ名です。

- SAMLシグニチャアルゴリズム：SHA-1またはSHA-256。一般的ではないSHA-384またはSHA-512。このアルゴリズムは、X.509証明書と組み合わせて使用されます。



SPの設定

上記のセクションとは逆に、このセクションではIdPが提供する情報を説明し、SPで設定します。

- 発行者URL - IdPの一意の識別子。SPが受信したSAMLアサーションが正しいIdPから発行されていることを検証できるように、IdPに関する情報を含むURLとしてフォーマットされます。
例： <saml:Issuer <https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/> >
- SAML SSOエンドポイント/サービスプロバイダーのログインURL:SAML要求でSPによってリダイレクトされたときに認証を開始するIdPエンドポイント。
例： <https://login.microsoftonline.com/023480840129412-824812/saml2>
- SAML SLO (シングルログアウト) エンドポイント：SPからリダイレクトされたときにIdPセッションを閉じるIdPエンドポイントで、通常はログアウトをクリックした後は閉じます。
例： <https://access.wristbandtent.com/logout>

FMCのSAML

FMCのSSO機能は6.7から導入されました。新しい機能は、FMC権限に存在する情報をマッピングするため、FMC認可(RBAC)を簡素化します。これは、すべてのFMC UIユーザおよびFMCロールに適用されます。現時点では、SAML 2.0仕様およびサポートされるIDPをサポートしています

- OKTA
- OneLogin
- PingID
- Azure AD
- その他 (SAML 2.0に準拠する任意のIDP)

制限および警告

- SSOはグローバルドメインに対してのみ設定できます。
- HAペアのFMCには個別の設定が必要です。
- シングルサインオンを設定できるのは、ローカル/AD管理者のみです。
- Idpから開始されたSSOはサポートされていません。

設定

アイデンティティプロバイダーの設定

ステップ1:Microsoft Azureにログインします。[Azure Active Directory] > [エンタープライゼーションアプリケーション]に移動します。



Default Directory | Overview

Azure Active Directory



Switch tenant



Delete tenant



Create



Overview



Getting started



Preview hub



Diagnose and solve problems

Manage



Users



Groups



External Identities



Roles and administrators



Administrative units (Preview)



Enterprise applications



Azure Active Directory can help you enable remote

Default Directory



Search your tenant



Tenant information

Your role

Global administrator [More info](#)

License

Azure AD Free

Tenant ID

- ステップ2 : 次の図に示すように、非ギャラリーアプリケーションの下に新しいアプリケーションを作成します。

[Home](#) > [Default Directory](#) > [Enterprise applications | All applications](#) > [Add an application](#) >

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](#)

ステップ3 : 作成したアプリケーションを編集し、次の図に示すように、[Set up single sign on > SAML]に移動します。

Home > Default Directory > Enterprise applications | All applications > Add an application >

Firepower | Single sign-on

Enterprise Application

« Select a single sign-on method [Help me decide](#)

- Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Password-based**
Password storage and replay using a web browser extension or mobile app.
- Linked**
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Navigation menu:

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access

ステップ4：基本的なSAML設定を編集し、FMCの詳細を指定します（SAML設定の基本はSAML設定です）。

- FMC URL: <https://<FMC-FQDNまたはIPアドレス>>
- 識別子 (エンティティID) : <https://<FMC-FQDN-or-IPaddress>/saml/metadata>
- 返信URL: <https://<FMC-FQDN-or-IPaddress>/saml/acs>
- サインオンURL: [/https://<FMC-QDN-or-IPaddress>/saml/acs](https://<FMC-QDN-or-IPaddress>/saml/acs)
- RelayState: [/ui/login](#)

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

- [Overview](#)
- [Deployment Plan](#)
- [Diagnose and solve problems](#)

Manage

- [Properties](#)
- [Owners](#)
- [Users and groups](#)
- [Single sign-on](#)
- [Provisioning](#)
- [Application proxy](#)
- [Self-service](#)

Security

- [Conditional Access](#)
- [Permissions](#)
- [Token encryption](#)

Activity

- [Sign-ins](#)
- [Usage & insights \(Preview\)](#)
- [Audit logs](#)
- [Provisioning logs \(Preview\)](#)

1

[Edit](#)

Basic SAML Configuration

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

[Edit](#)

User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
roles	user.assignedroles
Unique User Identifier	user.userprincipalname
Group	user.groups

3

[Edit](#)

SAML Signing Certificate

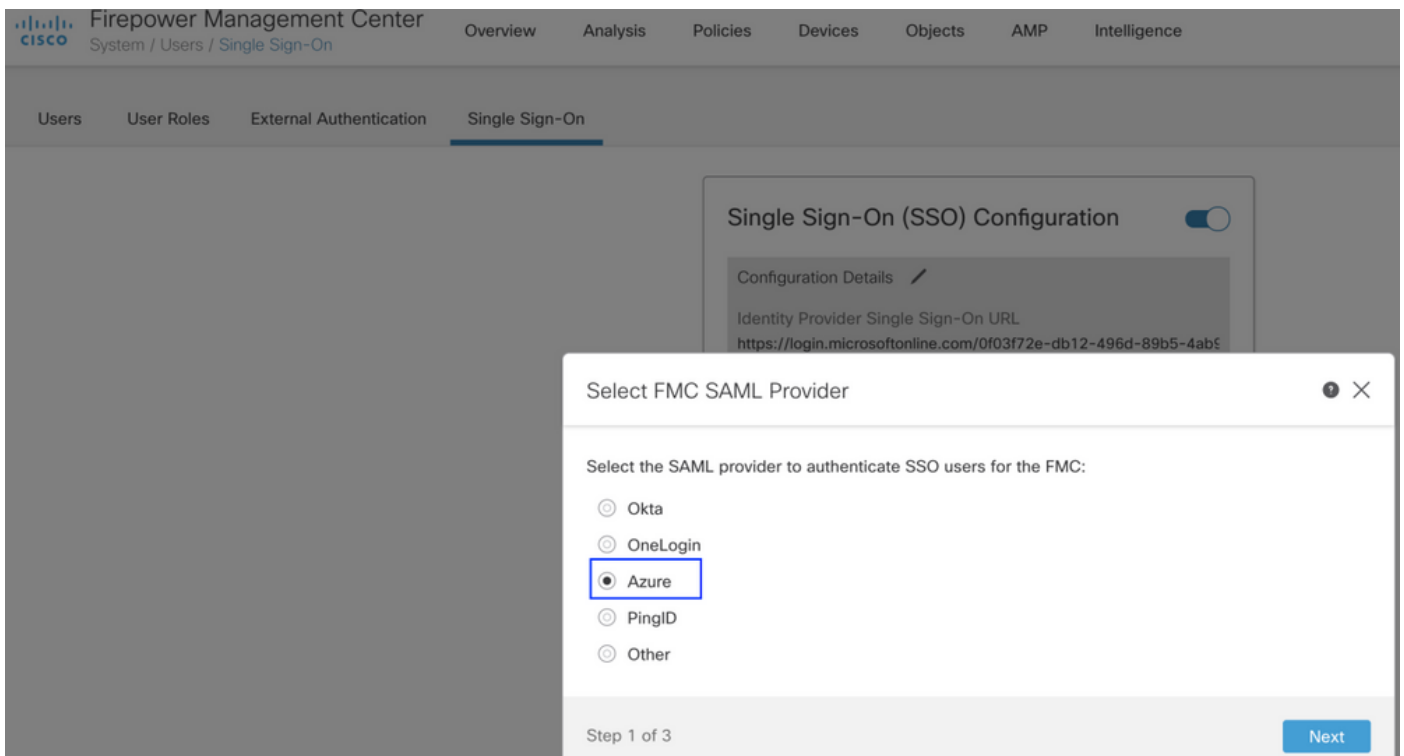
Status	Active
Thumbprint	[REDACTED]
Expiration	[REDACTED]
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

残りはデフォルトのままにします。これは、ロールベースのアクセスに関してさらに説明します。

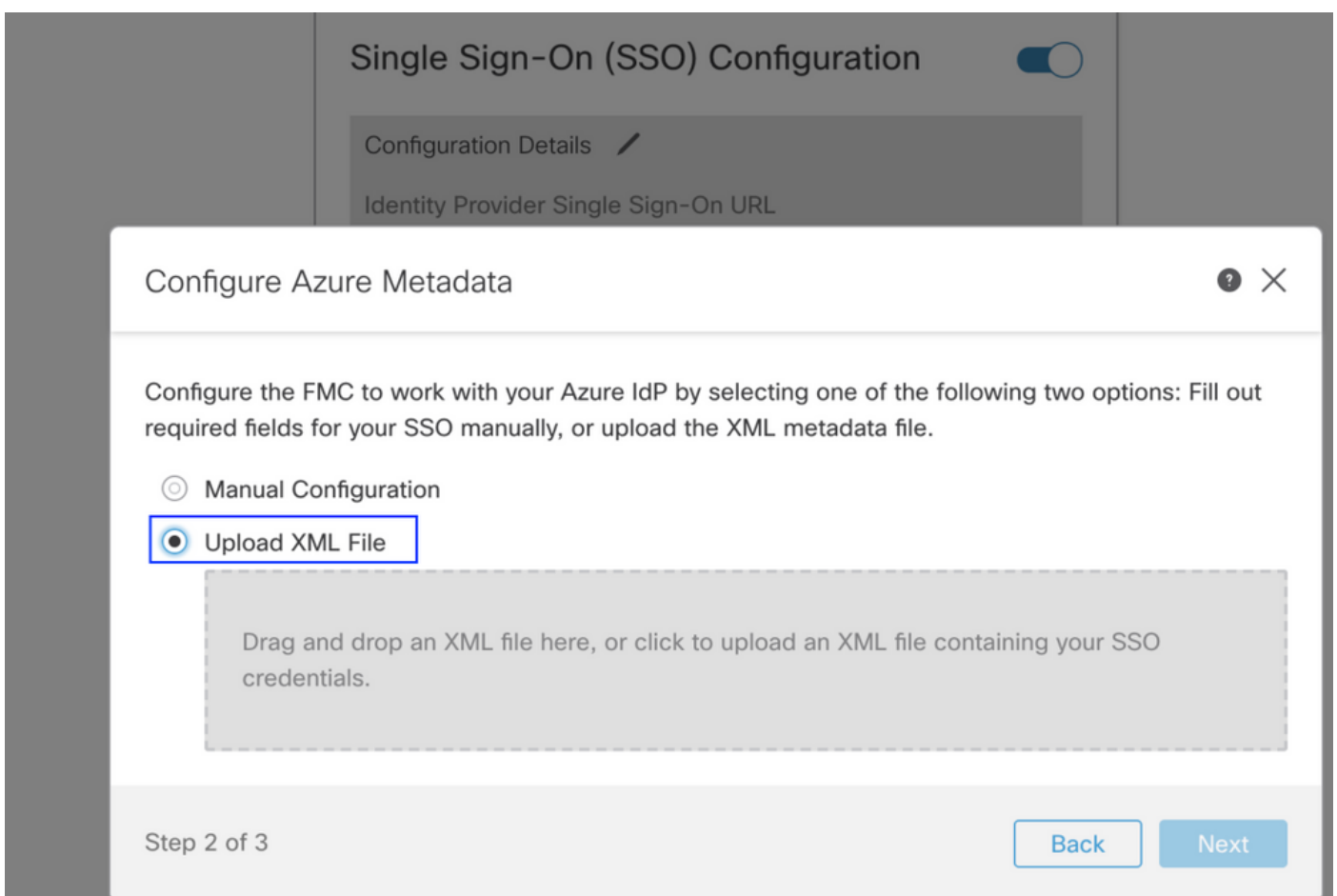
これにより、IDプロバイダーの設定が終了します。FMCの設定に使用するフェデレーションメタデータXMLをダウンロードします。

Firepower Management Centerの設定

ステップ1:FMCにログインし、[Settings] > [Users] > [Single Sign-On]に移動し、[SSO]を有効にします。プロバイダとしてAzureを選択します。



ステップ2: AzureからダウンロードしたXMLファイルをここにアップロードします。必要なすべての詳細が自動入力されます。



ステップ3: 設定を確認し、次の図に示すように[Save]をクリックします。

Verify Azure Metadata ? ×

Test the Azure metadata by clicking the **Test Configuration** button on the **System / Users / Single Sign-On** page after you save.)

Identity Provider Single Sign-On URL

Identity Provider Issuer

X.509 Certificate

Step 3 of 3

[Back](#) [Save](#)

高度な構成 – AzureによるRBAC

さまざまなロールタイプを使用してFMCのロールにマッピングするには – Azure上のアプリケーションのマニフェストを編集して、ロールに値を割り当てる必要があります。デフォルトでは、ロールの値はNullです。

ステップ1：作成したアプリケーションに移動し、[シングルサインオン]をクリックします。


Cisco-Firepower

Search (Cmd+*/*)

 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 Authentic 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](#)

ステップ2 : ユーザ属性と要求を編集します。[Name]に新しい要求を追加します。rolesとし、値としてuser.assignedrolesを選択します。

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 ***

ステップ3:[<アプリケーション名>] > [マニフェスト]に移動します。 マニフェストを編集します。ファイルはJSON形式で、デフォルトのユーザがコピーできます。たとえば、次の2つのロールが作成されます。ユーザおよびアナリスト。

Cisco-Firepower | Manifest

Search (Cmd+/) <<  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 }
```

ステップ4:[<アプリケーション名>] > [ユーザとグループ]に移動します。次の図に示すように、ユーザを編集し、新しく作成したロールを割り当てます。

Edit Assignment

Default Directory

Users

1 user selected. >

Select a role >

None Selected

Assign

Select a role

Only a single role can be selected

Analyst

User

Selected Role

Analyst

Select

ステップ4:FMCにログインし、SSOの詳細設定を編集します。を参照, グループメンバー属性 : aアプリケーションマニフェストでロールに指定した表示名に署名します。

▼ 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	

その後、指定されたロールにログインできます。

確認

ステップ1 : ブラウザからFMC URL(<https://<FMC URL>>)に移動します。次の図に示すように、[Single Sign-On]をクリックします。



Firepower Management Center

Username

Password

Single Sign-On

Log In

Microsoftログインページにリダイレクトされ、ログインに成功するとFMCのデフォルトページが返されます。

ステップ2:FMCで、[System] > [Users]に移動し、データベースに追加されたSSOユーザを確認します。

test1@shbhartiscisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbhartiscisco.onmicrosoft.com

Administrator

External (SSO)

トラブルシュート

SAML認証を確認します。これは、承認を成功させるために行うワークフローです (このイメージはラボ環境のもので) 。

ブラウザのSAMLログ

GET	https://10.106.46.191/sso/saml/login	
GET	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/saml2?RelayState=7_ni-J1fNA5eEeVvoAuhcviH6CwKjxwyGhxxJpArDjKAFMbK-wvJ2RSP&SAML	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	SAML
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ログ

/var/log/auth-daemon.logにあるFMCのSAMLログの確認

```
root@shbharti1ffncl:/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-56574e8a5f44bdd58102743d2cc9350b75f74d8c
auth-daemon 2020/08/09 04:59:11 I! Authorizing Response, ID : id-56574e8a5f44bdd58102743d2cc9350b75f74d8c
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:[redacted] b5-4ab9fc80d8aa/] http://schemas
.microsoft.com/identity/claims/objectid:[redacted] a] http://schemas.xmlsoap.org/w
/2005/05/identity/claims/givenname:[Test 1] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[test@shbhartiCisco.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-56574e8a5f44bdd58102743d2cc9350b75f74d8c, URI : /sso/saml/login
```