

Konfigurieren von FMC SSO mit Azure als Identity Provider

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[IDP-Konfiguration](#)

[SP-Konfiguration](#)

[SAML auf FMC](#)

[Einschränkungen und Bedenken](#)

[Konfiguration](#)

[Konfiguration für Identitätsanbieter](#)

[Konfiguration des FirePOWER Management Center](#)

[Erweiterte Konfiguration - RBAC mit Azure](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[SAML-Browserprotokolle](#)

[FMC SAML-Protokolle](#)

Einführung

In diesem Dokument wird beschrieben, wie das FirePOWER Management Center (FMC) Single Sign-On (SSO) mit Azure als Identity Provider (IdP) konfiguriert wird.

Security Assertion Markup Language (SAML) ist häufig das zugrunde liegende Protokoll, das SSO ermöglicht. Ein Unternehmen unterhält eine einzige Anmeldeseite, hinter der sich ein Identitätsspeicher und verschiedene Authentifizierungsregeln befinden. Es kann problemlos jede Web-App konfigurieren, die SAML unterstützt, sodass Sie sich bei allen Webanwendungen anmelden können. Sie hat außerdem den Sicherheitsvorteil, dass Benutzer weder gezwungen werden, Kennwörter für jede Webanwendung, auf die sie zugreifen müssen, zu verwalten (und diese möglicherweise wiederverwenden), noch Kennwörter für diese Web-Apps freigeben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis von FirePOWER Management Center
- Grundlegende Kenntnisse der Single Sign-On

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco FirePOWER Management Center (FMC) Version 6.7.0
- Azure - IDP

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

SAML-Terminologie

Die Konfiguration für SAML muss an zwei Stellen erfolgen: am IdP und am SP. Die IDs müssen so konfiguriert werden, dass sie wissen, wo und wie Benutzer gesendet werden, wenn sie sich bei einem bestimmten Service Provider anmelden möchten. Der SP muss konfiguriert werden, damit er weiß, dass er SAML-Assertionen vertrauen kann, die von der IdP signiert wurden.

Definition einiger Begriffe, die für SAML von grundlegender Bedeutung sind:

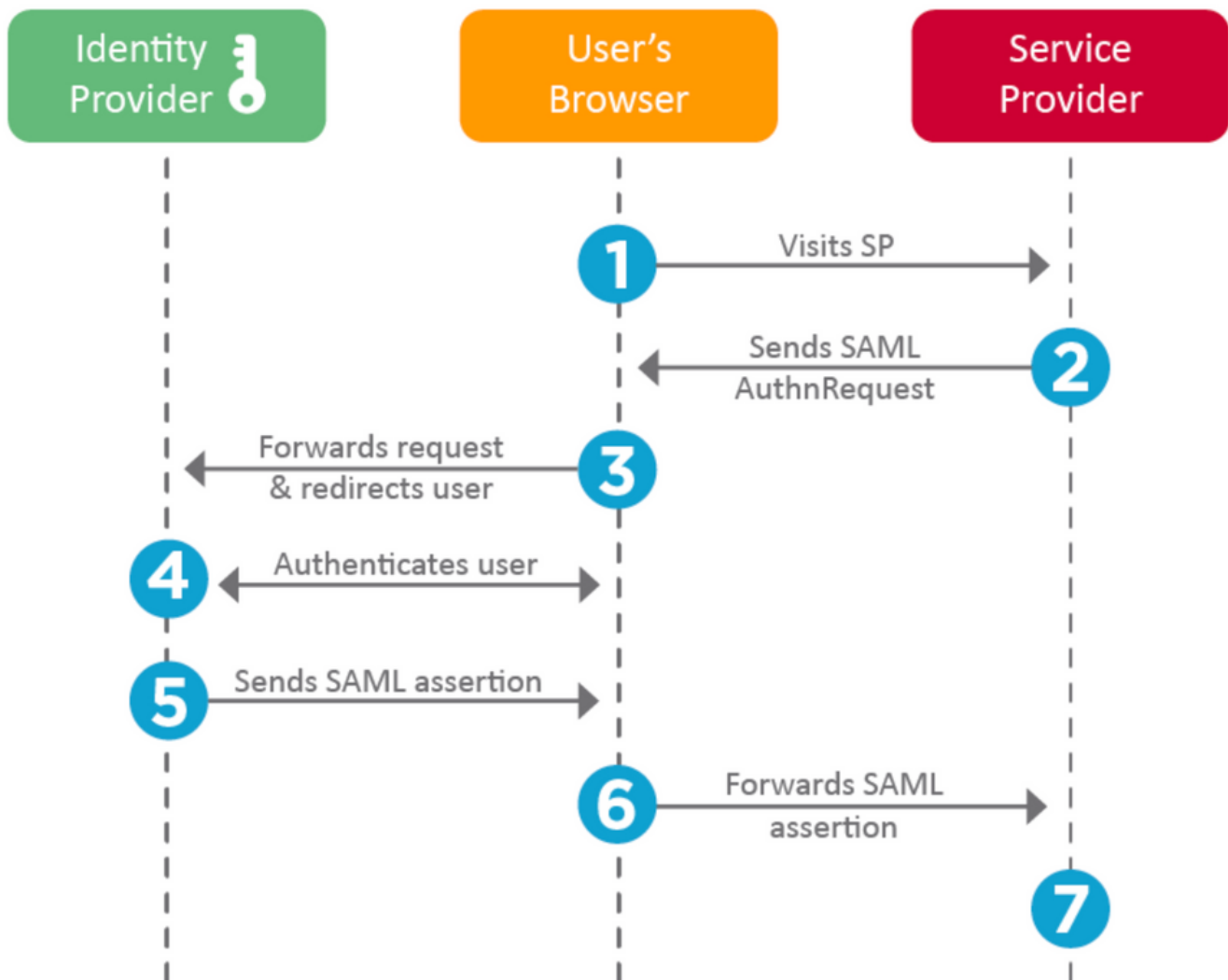
- Identitätsanbieter (Identity Provider, IDP) - Das Software-Tool oder -Service (häufig durch eine Anmeldeseite und/oder ein Dashboard visualisiert), das die Authentifizierung durchführt. überprüft Benutzernamen und Kennwörter, überprüft den Kontostatus, ruft zwei Faktoren auf usw.
- Service Provider (SP) - Die Webanwendung, auf die der Benutzer zugreifen möchte.
- SAML-Assertion - Eine Nachricht, die die Identität eines Benutzers und häufig andere Attribute bestätigt und über HTTP über Browser weitergeleitet wird.

IDP-Konfiguration

Die Spezifikationen für eine SAML-Assertion, was sie enthalten sollte und wie sie formatiert werden soll, werden vom SP bereitgestellt und auf der IdP festgelegt.

- EntityID - Ein global eindeutiger Name für den SP. Die Formate variieren, aber dieser Wert wird immer häufiger als URL formatiert angezeigt.
Beispiel: <https://<FQDN-oder-IP-Adresse>/saml/Metadaten>
- Assertion Consumer Service (ACS) Validator - Eine Sicherheitsmaßnahme in Form eines regulären Ausdrucks (Regex), die sicherstellt, dass die SAML-Assertion an den richtigen ACS gesendet wird. Dies wird nur bei von einem Service Provider initiierten Anmeldungen angewendet, bei denen die SAML-Anforderung einen ACS-Speicherort enthält. Dieser ACS-Validierungssteuerelement würde also sicherstellen, dass der von der SAML-Anforderung bereitgestellte ACS-Standort legitim ist.
Beispiel: <https://<FQDN-oder-IP-Adresse>/saml/acs>

- Attribute: Anzahl und Format der Attribute können stark variieren. In der Regel gibt es mindestens ein Attribut, die nameID, also in der Regel den Benutzernamen des Benutzers, der sich anmelden möchte.
- SAML Signature Algorithm - SHA-1 oder SHA-256. Weniger häufig SHA-384 oder SHA-512. Dieser Algorithmus wird zusammen mit dem X.509-Zertifikat verwendet.



SP-Konfiguration

Auf der Rückseite des Abschnitts oben finden Sie Informationen, die von der IdP bereitgestellt und am SP festgelegt wurden.

- Issuer URL - Eindeutige ID des IdP. Formatiert als URL mit Informationen über das IdP, sodass der SP überprüfen kann, ob die erhaltenen SAML-Assertionen von der richtigen IdP ausgegeben werden.
Beispiel: `<saml:Issuer https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/ >`
- SAML SSO-Endpoint/Dienstanbieter-Anmeldungs-URL - Ein IdP-Endpoint, der die Authentifizierung initiiert, wenn der SP mit einer SAML-Anforderung hierhin umgeleitet wird.
Beispiel: <https://login.microsoftonline.com/023480840129412-824812/saml2>
- SAML SLO-Endpoint (Single Log-out) - Ein IDP-Endpoint, der Ihre IDP-Sitzung schließt, wenn dieser vom Service Provider weitergeleitet wird, in der Regel nachdem Sie auf **das** Feld

"Log out" (Abmelden) geklickt haben.

Beispiel: <https://access.wristbandtent.com/logout>

SAML auf FMC

Die SSO-Funktion in FMC wird ab 6.7 eingeführt. Die neue Funktion vereinfacht die FMC-Autorisierung (RBAC), da sie die vorhandenen Informationen den FMC-Rollen zuordnet. Sie gilt für alle Benutzer der FMC-Benutzeroberfläche und alle FMC-Rollen. Derzeit unterstützt sie die SAML 2.0-Spezifikation und diese unterstützten IDPs

- OKTA
- OneLogin
- PingID
- Azure AD
- Andere (Alle IDP, die SAML 2.0 entsprechen)

Einschränkungen und Bedenken

- SSO kann nur für die globale Domäne konfiguriert werden.
- FMCs im HA-Paar benötigen eine individuelle Konfiguration.
- Nur lokale/AD-Administratoren können die einmalige Anmeldung konfigurieren.
- Von Idp initiierte SSO wird nicht unterstützt.

Konfiguration

Konfiguration für Identitätsanbieter

Schritt 1: Melden Sie sich bei Microsoft Azure an. Navigieren Sie zu **Azure Active Directory > Enterprise Application**.

Default Directory | Overview

Azure Active Directory

Overview

Getting started

Preview hub

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units (Preview)

Enterprise applications

Switch tenant Delete tenant Create

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

- Schritt 2: Erstellen Sie **neue Anwendung** unter Anwendung ohne Galerie, wie in diesem Bild gezeigt.

[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](#)

Schritt 3: Bearbeiten Sie die erstellte Anwendung, und navigieren Sie zu **Set up single sign on > SAML (Single Sign-On > SAML einrichten)**, wie in diesem Bild gezeigt.

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

Schritt 4: Bearbeiten Sie die grundlegende SAML-Konfiguration, und stellen Sie die FMC-Details bereit:

- FMC-URL: <https://<FMC-FQDN-oder-IP-Adresse>>
- Kennung (Element-ID): <https://<FMC-FQDN-or-IP-Adresse>/saml/Metadaten>
- URL antworten: <https://<FMC-FQDN-oder-IP-Adresse>/saml/acs>
- URL registrieren: <https://<FMC-QDN-oder-IP-Adresse>/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 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

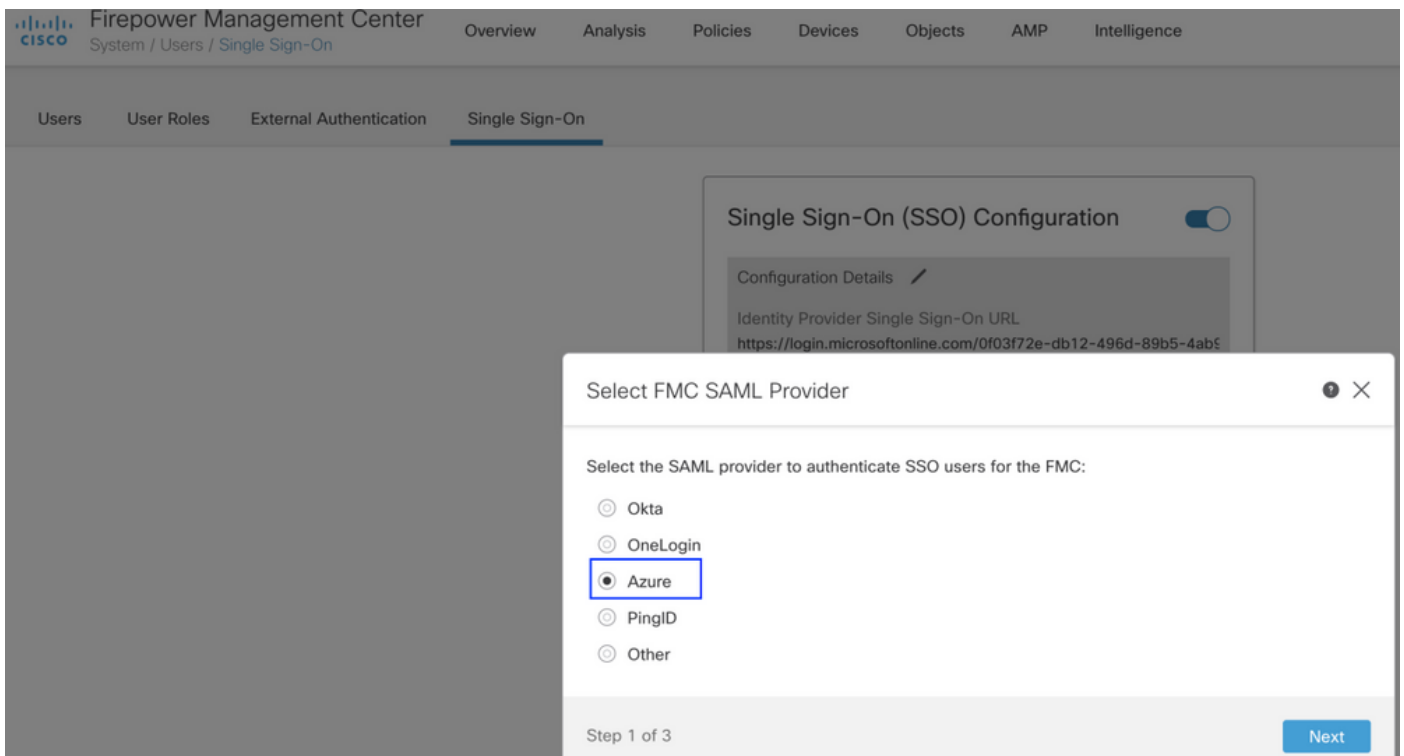
Status	Active
Thumbprint	[REDACTED]
Expiration	[REDACTED]
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Behalten Sie den Rest als Standard bei - dies wird für rollenbasierten Zugriff weiter erläutert.

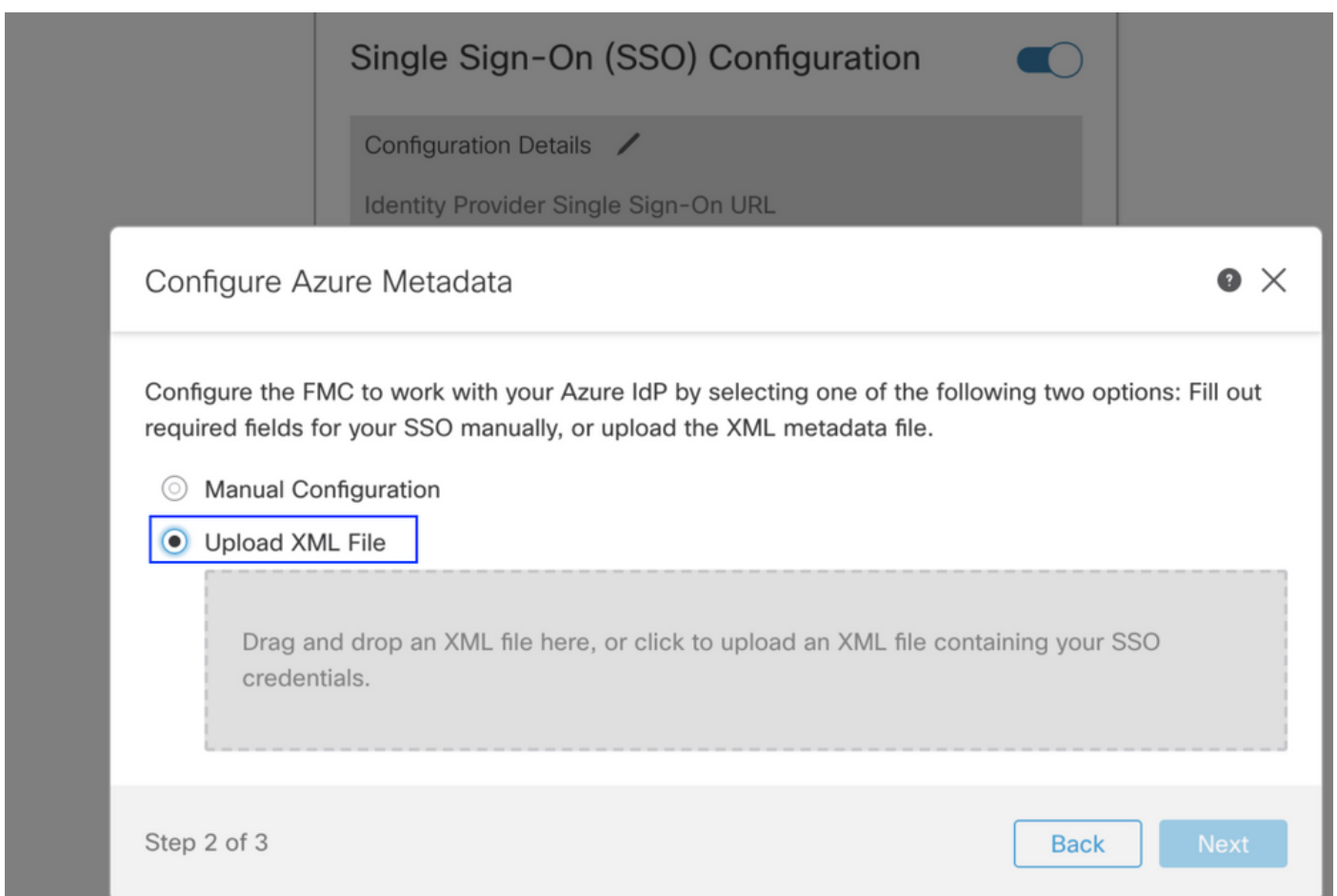
Damit ist die Konfiguration des Identitätsanbieters beendet. Laden Sie die Federation Metadata XML herunter, die für die FMC-Konfiguration verwendet wird.

Konfiguration des FirePOWER Management Center

Schritt 1: Melden Sie sich bei FMC an, navigieren Sie zu **Einstellungen > Benutzer > Single Sign-On** und Enable SSO. Wählen Sie **Azure** als Provider aus.



Schritt 2: Laden Sie hier die XML-Datei aus Azure herunter. Hier werden alle erforderlichen Informationen automatisch eingegeben.



Schritt 3: Überprüfen Sie die Konfiguration, und klicken Sie auf **Speichern**, wie in diesem Bild gezeigt.

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](#)

Erweiterte Konfiguration - RBAC mit Azure

Um verschiedene Rollentypen zu verwenden, um den Rollen von FMC zuzuordnen - Sie müssen das Anwendungsmanifest auf Azure bearbeiten, um den Rollen Werte zuzuweisen. Standardmäßig haben die Rollen den Wert Null.

Schritt 1: Navigieren Sie zur **Anwendung**, die erstellt wird, und klicken Sie auf **Single Sign-on (Einmalige Anmeldung)**.


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 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](#)

Schritt 2: Bearbeiten Sie die Benutzerattribute und Ansprüche. Neuen Antrag mit Name hinzufügen: **Rollen** und wählen den Wert als **user.assignedroles** aus.

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 ***

Schritt 3: Navigieren Sie zu **<Anwendungsname> > Manifest**. Bearbeiten des Manifests Die Datei ist im JSON-Format, und es steht ein Standardbenutzer zum Kopieren zur Verfügung. Beispiel: Hier werden zwei Rollen erstellt: Benutzer und Analyst.

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     {
23       "allowedMemberTypes": [
24         "User"
25       ],
26       "description": "User",
27       "displayName": "User",
28       "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",
29       "isEnabled": true,
30       "lang": null,
31       "origin": "Application",
32       "value": "User-1"
33     },
34   ]
35 }
```

Schritt 4: Navigieren Sie zu **<Anwendungsname> > Benutzer und Gruppen**. Bearbeiten Sie den Benutzer, und weisen Sie die neu erstellten Rollen zu, wie in diesem Bild gezeigt.

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

Schritt 4: Melden Sie sich bei FMC an, und bearbeiten Sie die erweiterte Konfiguration in SSO. Für Gruppenmitgliedschaft-Attribut: eineSignieren Sie den **Anzeigenamen**, den Sie im Anwendungsmanifest bereitgestellt haben, den Rollen.

▼ 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	

Anschließend sollten Sie sich bei der zugewiesenen Rolle anmelden können.

Überprüfung

Schritt 1: Navigieren Sie in Ihrem Browser zur FMC-URL: <https://<FMC URL>>. Klicken Sie auf **Single Sign-On**, wie in diesem Bild gezeigt.



Firepower Management Center

Username

Password

Single Sign-On

Log In

Sie werden zur Microsoft-Anmeldeseite umgeleitet, und bei erfolgreicher Anmeldung wird die FMC-Standardseite zurückgegeben.

Schritt 2: Navigieren Sie auf dem FMC zu **System > Users**, um den SSO-Benutzer anzuzeigen, der der Datenbank hinzugefügt wurde.

test1@shbhartisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbhartisco.onmicrosoft.com

Administrator

External (SSO)

Fehlerbehebung

Überprüfen Sie die SAML-Authentifizierung. Dies ist der Workflow, der für eine erfolgreiche Autorisierung erreicht wird (dieses Bild ist in einer Laborumgebung gespeichert):

SAML-Browserprotokolle

GET	https://10.106.46.191/sso/saml/login	
GET	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/saml2?RelayState=7_ni-J1fNA5eEeVvoAuhcviH6CwKjxwyGhvxJpArDjKAFMbK-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-Protokolle

Überprüfen Sie die SAML-Protokolle auf dem FMC unter `/var/log/auth-daemon.log`.

```
root@shbharti1ffncl1:/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/authnmethodsreferences:[http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password]
http://schemas.microsoft.com/identity/claims/objectid:[redacted] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[test@shbhartiCisco.onmicrosoft.com] http://schemas.xmlsoap.org/w
.microsoft.com/identity/claims/objectid:[redacted] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[redacted] 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
```