

將Azure配置為身份提供程式的FMC SSO

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[IdP配置](#)

[SP配置](#)

[FMC上的SAML](#)

[限制和警告](#)

[設定](#)

[身份提供程式上的配置](#)

[Firepower管理中心上的配置](#)

[高級配置 — RBAC with Azure](#)

[驗證](#)

[疑難排解](#)

[瀏覽器SAML日誌](#)

[FMC SAML日誌](#)

簡介

本文檔介紹如何使用Azure作為身份提供程式(idP)配置Firepower管理中心(FMC)單一登入(SSO)。

安全斷言標籤語言(SAML)是實現SSO的最常見的基礎協定。公司維護一個登入頁面，在其後面是一個身份儲存庫和各種身份驗證規則。它可以輕鬆配置任何支援SAML的Web應用，從而讓您登入到所有Web應用。它也有安全方面的好處，既不會強迫使用者為其需要訪問的每個Web應用保留（並可能重複使用）密碼，也不會將密碼暴露給這些Web應用。

必要條件

需求

思科建議您瞭解以下主題：

- 對Firepower管理中心的基本瞭解
- 對單點登入的基本瞭解

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科Firepower管理中心(FMC)版本6.7.0

- Azure - IdP

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

SAML術語

SAML的配置必須在兩個位置完成：在IdP和SP上。需要配置IdP，使其瞭解使用者想要登入到特定SP時向何處傳送以及如何傳送該資訊。需要配置SP，使其知道可以信任由IdP簽名的SAML斷言。

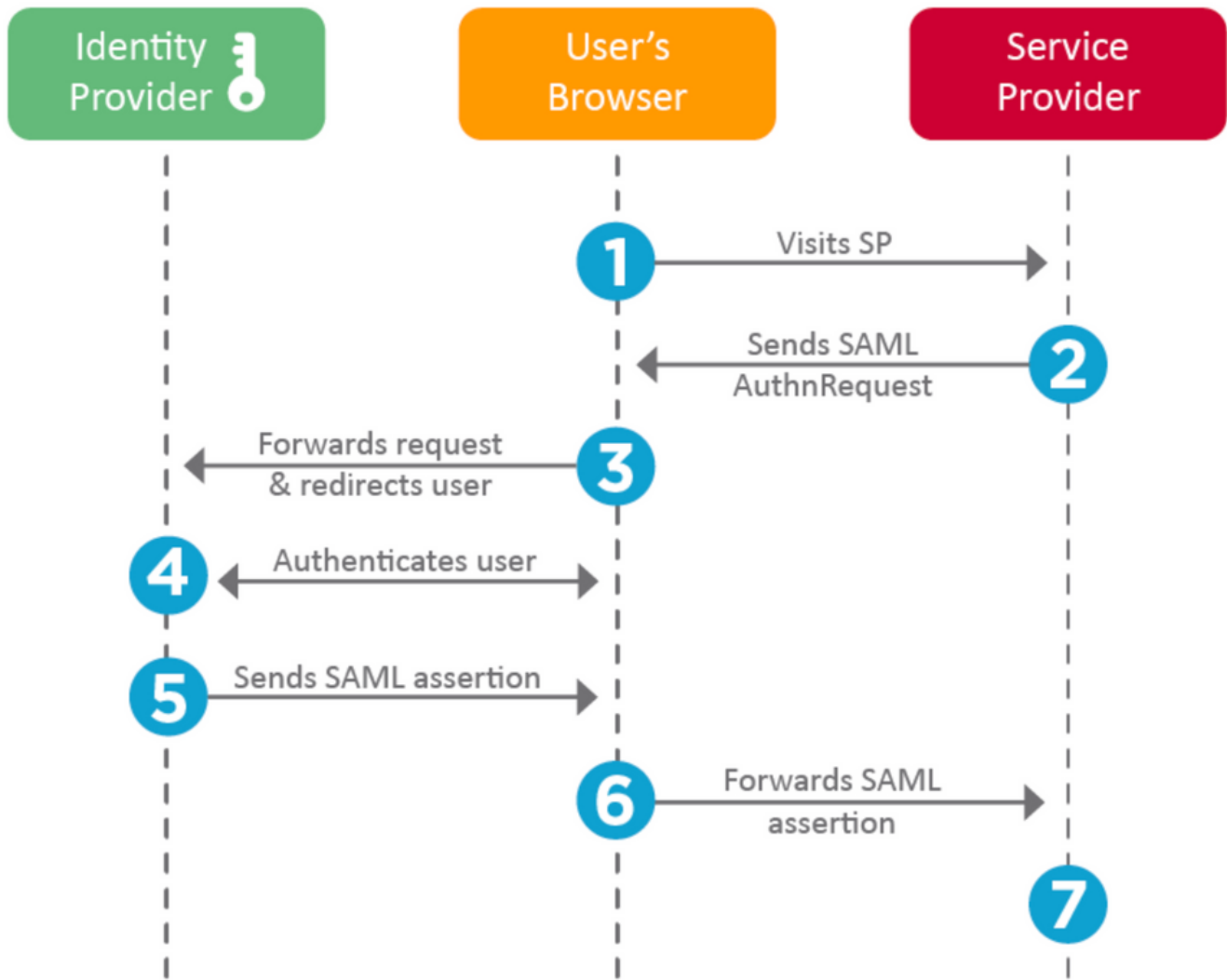
對SAML至關重要的幾個術語的定義：

- 身份提供程式(IdP) — 執行身份驗證的軟體工具或服務（通常通過登入頁和/或儀表板進行視覺化）；檢查使用者名稱和密碼、驗證帳戶狀態、呼叫雙因素等。
- 服務提供商(SP) — 使用者嘗試獲取訪問許可權的Web應用程式。
- SAML斷言 — 通過瀏覽器重定向通過HTTP傳送的斷言使用者身份和通常為其他屬性的消息

IdP配置

SAML斷言的規範、斷言應包含的內容以及斷言的格式設定由SP提供並在IdP中設定。

- EntityID - SP的全域性唯一名稱。格式各異，但看到此值格式化為URL的情況越來越常見。
範例：<https://<FQDN-or-IPaddress>/saml/metadata>
- 斷言使用者服務(ACS)驗證器 — 正規表示式(regex)形式的安全措施，用於確保SAML斷言傳送到正確的ACS。這僅在由SP發起的登入期間起作用，其中SAML請求包含ACS位置，因此，此ACS驗證程式將確保SAML請求提供的ACS位置是合法的。
示例：<https://<FQDN-or-IPaddress>/saml/acs>
- Attributes — 屬性的數量和格式可能大不相同。通常至少有一個屬性nameID，它通常是嘗試登入的使用者的使用者名稱。
- SAML簽名演算法 — SHA-1或SHA-256。不太常用的SHA-384或SHA-512。此處提到此演算法與X.509證書結合使用。



SP配置

與上面部分相反，本節介紹IdP提供的資訊並在SP上設定。

- 頒發者URL - IdP的唯一識別符號。格式化為包含有關IdP資訊的URL，以便SP可以驗證其收到的SAML斷言是從正確的IdP發出的。
 示例：`<saml:Issuer https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/>`
- SAML SSO終結點/服務提供商登入URL — 一個IdP終結點，當SP在此使用SAML請求重定向時啟動身份驗證。
 示例：`https://login.microsoftonline.com/023480840129412-824812/saml2`
- SAML SLO (單一註銷) 終結點 — 一個IdP終結點，它在SP重定向到此處時關閉IdP會話，通常是在按一下**註銷**之後。
 示例：`https://access.wristbandtent.com/logout`

FMC上的SAML

FMC中的SSO功能是從6.7開始引入的。新功能簡化了FMC授權(RBAC)，因為它將現有資訊對映到FMC角色。它適用於所有FMC UI使用者和FMC角色。目前，它支援SAML 2.0規範以及這些支援的IDP

- OKTA
- OneLogin
- PingID
- Azure AD
- 其他 (符合SAML 2.0的任何IDP)

限制和警告

- 只能為全域性域配置SSO。
- HA配對中的FMC需要個別組態。
- 只有本地/AD管理員可以配置單一登入。
- 不支援從Idp啟動的SSO。

設定

身份提供程式上的配置

步驟1. 登入Microsoft Azure。導航到Azure Active Directory > 企業應用程式。

The screenshot shows the Azure Active Directory 'Default Directory | Overview' page. The navigation menu on the left includes 'Overview', 'Getting started', 'Preview hub', 'Diagnose and solve problems', 'Manage' (with sub-items: Users, Groups, External Identities, Roles and administrators, Administrative units (Preview), and Enterprise applications, which is highlighted with a blue box), 'Switch tenant', 'Delete tenant', and 'Create'. The main content area features 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', and a notification banner stating 'Azure Active Directory can help you enable remot...'. The breadcrumb 'Home >' is visible at the top left.

- 步驟2. 在「Non-Gallery Application」下建立新應用程式，如下圖所示。

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](#)

步驟3.編輯已建立的應用程式，然後導覽至Set up single sign on > SAML，如下圖所示。

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

步驟4.編輯基本SAML配置並提供FMC詳細資訊：

- FMC URL: <https://<FMC-FQDN-or-IPAddress>>
- 識別符號 (實體ID) : <https://<FMC-FQDN-or-IPAddress>/saml/metadata>
- 回覆URL: <https://<FMC-FQDN-or-IPAddress>/saml/acs>
- 登入URL: [/https://<FMC-QDN-or-IPaddress>/saml/acs](https://<FMC-QDN-or-IPaddress>/saml/acs)
- RelayState:/ui/login

- 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)

« [Upload metadata file](#) [Change single sign-on mode](#) [Test this application](#) | [Got feedback?](#)

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	Optional

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](#)

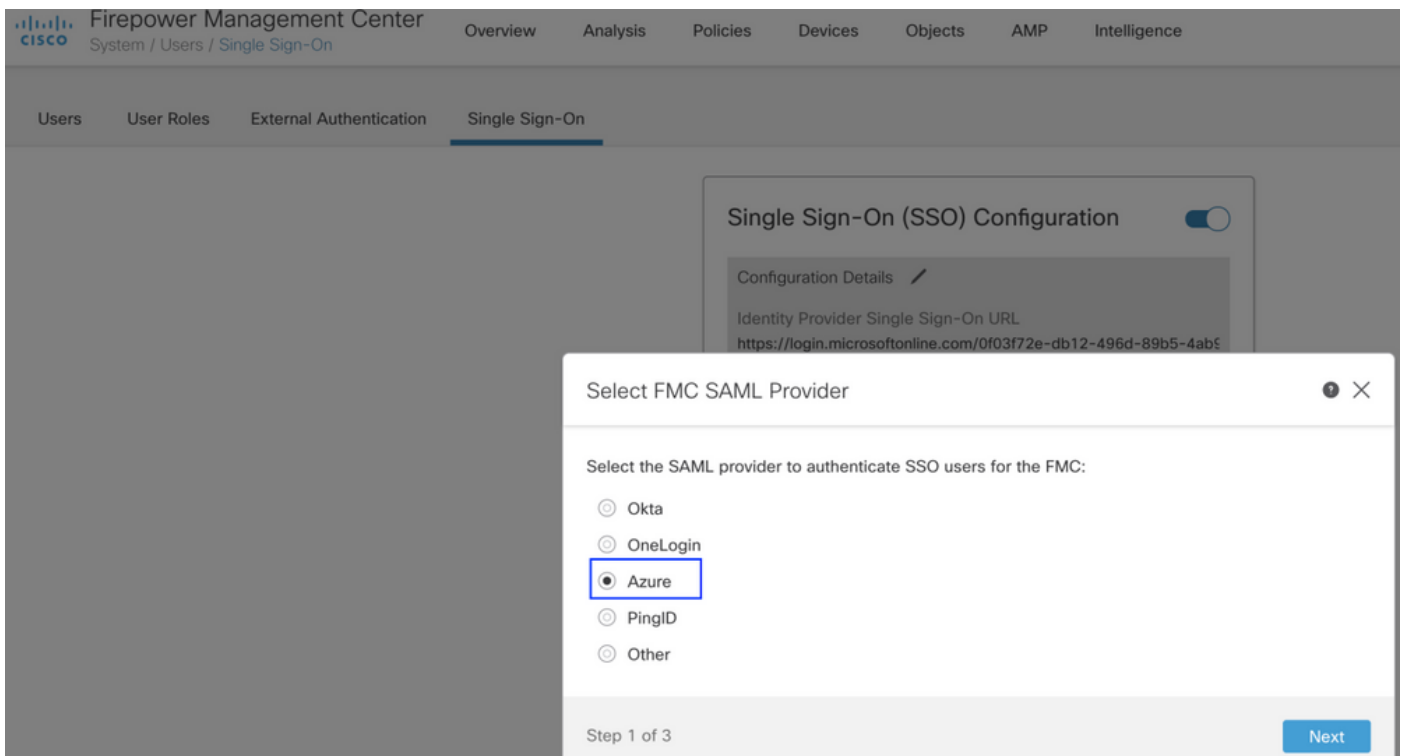
Status	Active
Thumbprint	<div style="background-color: black; width: 100px; height: 15px;"></div>
Expiration	
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

將剩餘部分保留為預設值 — 對於基於角色的訪問，將對此進行進一步討論。

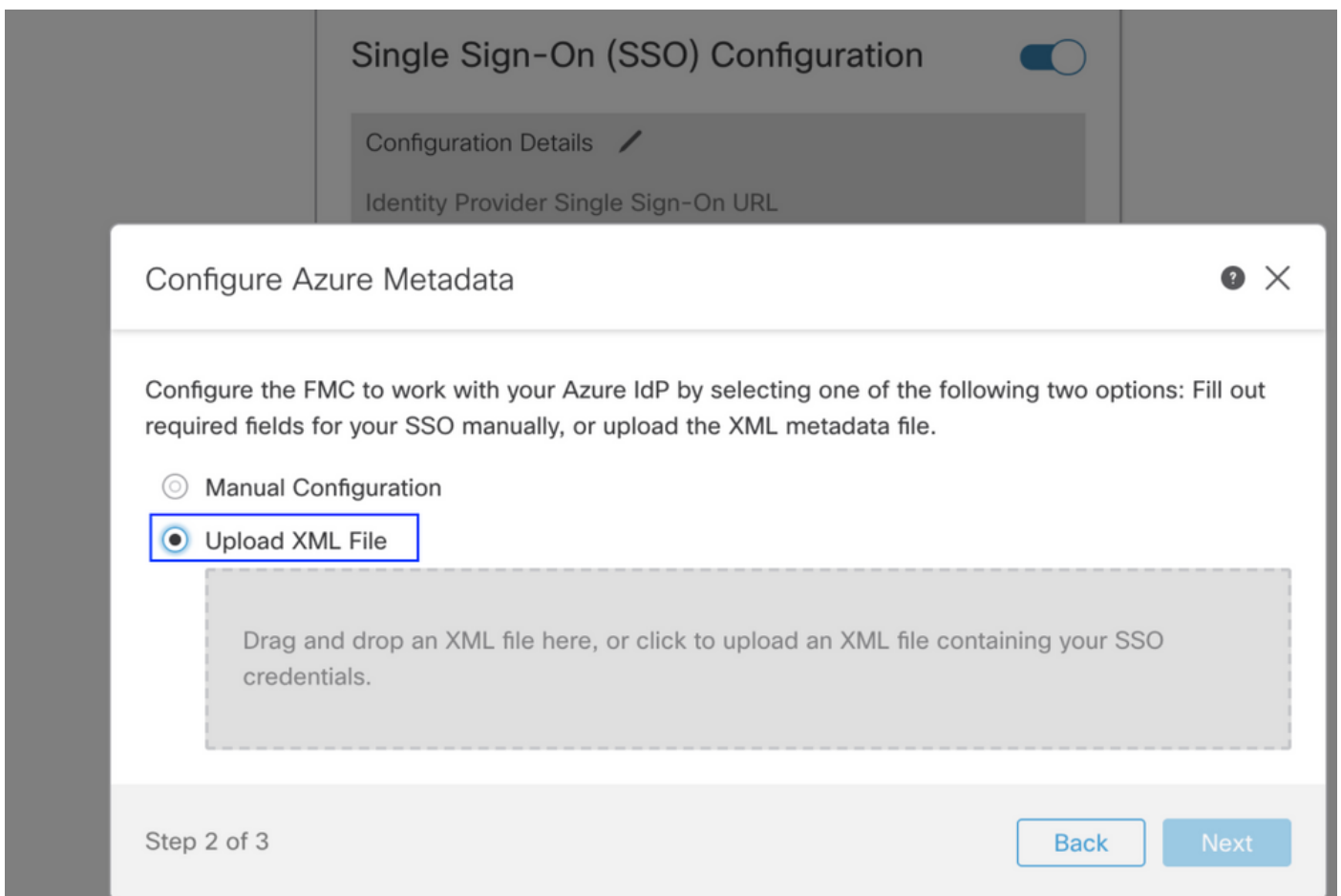
這標籤身份提供程式配置的結束。下載將用於FMC配置的聯合後設資料XML。

Firepower管理中心上的配置

步驟1.登入到FMC，導航到設定>使用者>單點登入並啟用SSO。選擇Azure作為提供程式。



步驟2.在此處上載從Azure下載的XML檔案。它會自動填充所需的所有詳細資訊。



步驟3.驗證組態並按一下**Save**，如下圖所示。

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](#)

高級配置 — RBAC with Azure

若要使用各種角色型別對映到FMC的角色 — 您需要編輯Azure上的應用程式清單以將值分配給角色。預設情況下，角色具有Null值。

步驟1. 導航到建立的Application，然後按一下Single sign-on。

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](#)

步驟2.編輯使用者屬性和宣告。新增名為：角色並選擇值作為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 ***

步驟3. 導覽至<Application-Name> > Manifest。編輯清單。檔案採用JSON格式，預設使用者可供複製。例如 — 此處建立了2個角色：使用者和分析師。

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 }
```

步驟4. 導航到<Application-Name> > Users and Groups。編輯使用者並分配新建立的角色，如下圖所示。

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

步驟4.登入到FMC並在SSO中編輯高級配置。對於，組成員屬性：答 將您在應用程式清單中提供的顯示名稱分配給角色。

▼ 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	

完成後，您應該能夠登入到他們的指定角色。

驗證

步驟1. 從瀏覽器導航至FMC URL: <https://<FMC URL>>。按一下「Single Sign-On」，如下圖所示。



Firepower Management Center

Username

Password

Single Sign-On

Log In

系統會將您重新導向至Microsoft登入頁面，且成功登入將返回FMC預設頁面。

步驟2.在FMC上，導航到**System > Users**，檢視新增到資料庫的SSO使用者。

test1@shbharticisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbharticisco.onmicrosoft.com

Administrator

External (SSO)

疑難排解

驗證SAML身份驗證，這是成功授權所實現的工作流程（此映像為實驗室環境）：

瀏覽器SAML日誌

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日誌

在/var/log/auth-daemon.log上驗證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
```