

Configure FMC SSO with Azure as Identity Provider

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[IdP Configuration](#)

[SP Configuration](#)

[SAML on FMC](#)

[Limitations and Caveats](#)

[Configure](#)

[Configuration on Identity Provider](#)

[Configuration on Firepower Management Center](#)

[Advanced Configuration - RBAC with Azure](#)

[Verify](#)

[Troubleshoot](#)

[Browser SAML Logs](#)

[FMC SAML Logs](#)

Introduction

This document describes how to configure the Firepower Management Center (FMC) Single Sign-On (SSO) with Azure as Identity Provider (idP).

Security Assertion Markup Language (SAML) is most frequently the underlying protocol that makes SSO possible. A company maintains a single login page, behind it is an identity store and various authentication rules. It can easily configure any web app that supports SAML, which allows you to log in to all web applications. It also has the security benefit of neither forcing users to maintain (and potentially reuse) passwords for every web app they need access to, nor exposing passwords to those web apps.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic Understanding of Firepower Management Center
- Basic understanding of Single Sign-On

Components Used

The information in this document is based on these software versions:

- Cisco Firepower Management Center (FMC) version 6.7.0
- Azure - IdP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SAML Terminologies

Configuration for SAML must be done in two places: at the IdP and at the SP. The IdP needs to be configured so it knows where and how to send users when they want to log in to a specific SP. The SP needs to be configured so it knows it can trust SAML assertions signed by the IdP.

Definition of a few terms that are core to SAML:

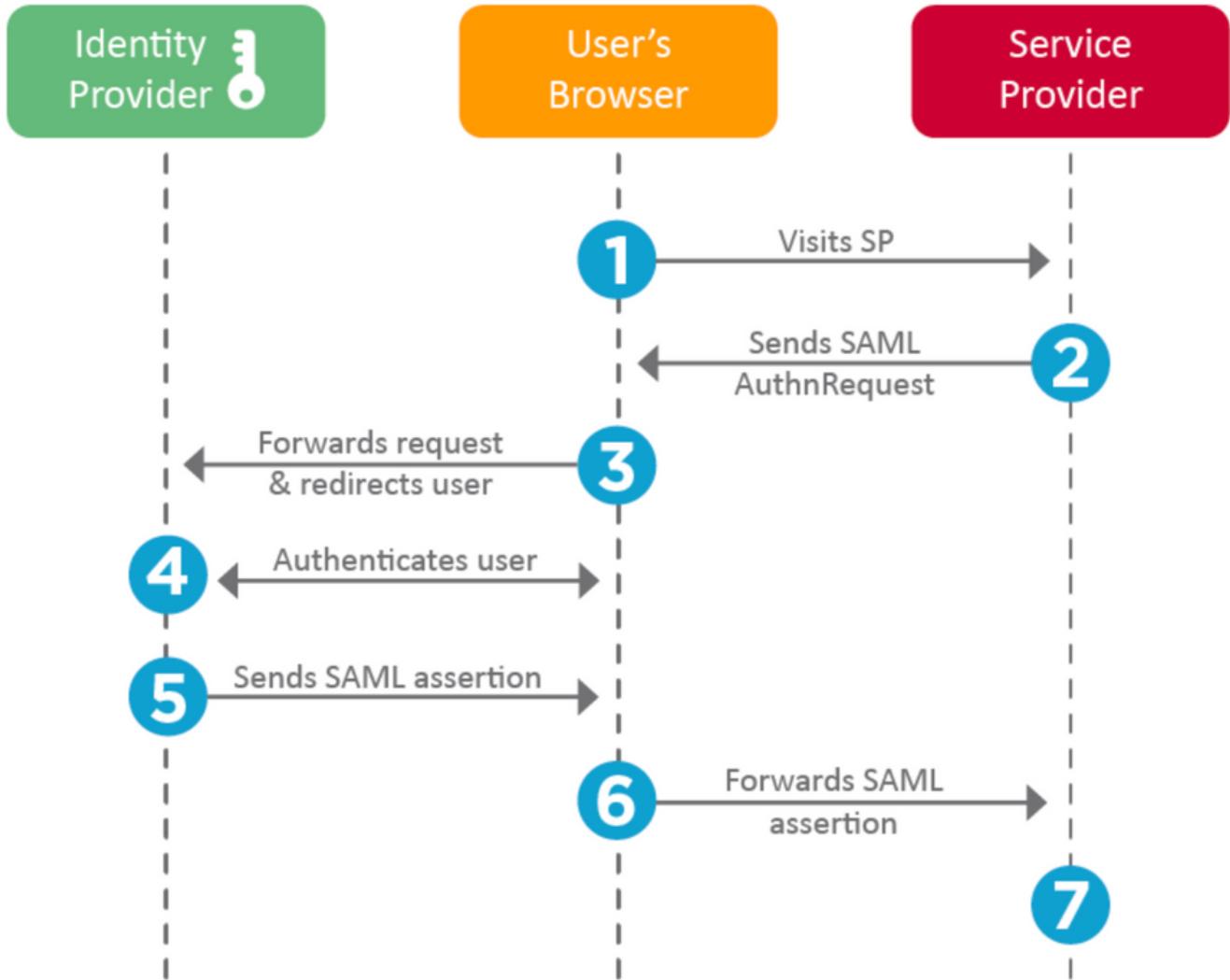
- Identity Provider (IdP) - The software tool or service (often visualized by a login page and/or dashboard) that performs the authentication; checks username and passwords, verify the account status, invokes two-factor, etc.
- Service Provider (SP) - The web application where the user tries to gain access.
- SAML Assertion - A message asserting a user's identity and often other attributes, sent over HTTP via browser redirects

IdP Configuration

Specifications for a SAML assertion, what it should contain, and how it should be formatted, are provided by the SP and set at the IdP.

- EntityID - A globally unique name for the SP. Formats vary, but it's increasingly common to see this value formatted as a URL.
Example: <https://<FQDN-or-IPaddress>/saml/metadata>
- Assertion Consumer Service (ACS) Validator - A security measure in the form of a regular expression (regex) that ensures the SAML assertion is sent to the correct ACS. This only comes into play during SP-initiated logins where the SAML request contains an ACS location, so this ACS validator would ensure that the SAML request-provided ACS location is legitimate.
Example: <https://<FQDN-or-IPaddress>/saml/acs>
- Attributes - The number of and format of attributes can vary greatly. There's usually at least one attribute, the nameID, which is typically the username of the user trying to log in.

- SAML Signature Algorithm - SHA-1 or SHA-256. Less commonly SHA-384 or SHA-512. This algorithm is used in conjunction with the X.509 certificate is mentioned here.



SP Configuration

The reverse of the section above, this section speaks to information provided by the IdP and set at the SP.

- Issuer URL - Unique identifier of the IdP. Formatted as a URL containing information about the IdP so the SP can validate that the SAML assertions it receives are issued from the correct IdP.

Example: <saml:Issuer <https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/>>

- SAML SSO Endpoint / Service Provider Login URL - An IdP endpoint that initiates authentication when redirected here by the SP with a SAML request.

Example: <https://login.microsoftonline.com/023480840129412-824812/saml2>

- SAML SLO (Single Log-out) Endpoint - An IdP endpoint that closes your IdP session when redirected here by the SP, typically after **log out** is clicked.

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

SAML on FMC

The SSO feature in FMC is introduced from 6.7. The new feature simplifies FMC Authorization (RBAC), as it maps the information that exists to FMC Roles. It applies to all FMC UI users and FMC roles. For now, it supports SAML 2.0 Specification, and these supported IDPs

- OKTA
- OneLogin
- PingID
- Azure AD
- Others (Any IDP that conforms to SAML 2.0)

Limitations and Caveats

- SSO can be configured only for the Global Domain.
- FMCs in HA Pair need individual configuration.
- Only Local/AD admins can configure Single Sign-on.
- SSO initiated from Idp is not supported.

Configure

Configuration on Identity Provider

Step 1. Log in to Microsoft Azure. Navigate to **Azure Active Directory > Enterprise Application**.



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

- Step 2. Create **New Application** under Non-Gallery Application, as shown in this image.

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

Add your own application

Name * (i)

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: (i)

SAML-based single sign-on

[Learn more](#)

Automatic User Provisioning with SCIM

[Learn more](#)

Password-based single sign-on

[Learn more](#)

Step 3. Edit the Application that was created and navigate to **Set up single sign on > SAML**, as shown in this image.

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.

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

Step 4. Edit the Basic SAML Configuration and provide the FMC Details :

- FMC URL: <https://<FMC-FQDN-or-IPaddress>>
- Identifier (Entity ID): <https://<FMC-FQDN-or-IPaddress>/saml/metadata>
- Reply URL: <https://<FMC-FQDN-or-IPaddress>/saml/acs>
- Sign on URL: /<https://<FMC-QDN-or-IPaddress>/saml/acs>
- RelayState:/ui/login

Enterprise Application

« [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

| | |
|--|---|
| 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

| | |
|------------------------|------------------------|
| 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

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

Activity

- Sign-ins
- Usage & insights (Preview)
- Audit logs
- Provisioning logs (Preview)

[Access controls](#)

Keep the rest as default - this is further discussed for Role-based access.

This marks the end of the Identity provider configuration. Download the Federation Metadata XML which will be used for FMC Configuration.

Configuration on Firepower Management Center

Step 1. Log in to FMC, navigate to **Settings > Users > Single Sign-On** and Enable SSO. Select **Azure** as Provider.

The screenshot shows the FMC interface with the 'Single Sign-On' tab selected. A modal window titled 'Select FMC SAML Provider' is open, listing providers: Okta, OneLogin, Azure, PingID, and Other. The 'Azure' option is selected and highlighted with a blue border. In the background, the 'Single Sign-On (SSO) Configuration' section is visible, showing the URL <https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab5...>.

Step 2. Upload the XML file downloaded from Azure here. It auto-populates all the details needed.

Single Sign-On (SSO) Configuration

Configuration Details /

Identity Provider Single Sign-On URL

Configure Azure Metadata

Configure the FMC to work with your Azure IdP by selecting one of the following two options: Fill out required fields for your SSO manually, or upload the XML metadata file.

Manual Configuration

Upload XML File

Drag and drop an XML file here, or click to upload an XML file containing your SSO credentials.

Step 2 of 3

Back Next

Step 3. Verify the configuration and click **Save**, as shown in this image.

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

Advanced Configuration - RBAC with Azure

In order to use various role types to map to Roles of FMC - You need to edit the manifest of

Application on Azure to assign values to roles. By default, the roles have value as Null.

Step 1. Navigate to the **Application** that is created and click on **Single sign-on**.

Home > Default Directory | App registrations >

Cisco-Firepower ⚡

Search (Cmd+/) <> Delete Endpoints

Overview : Cisco-Firepower

Quickstart Application (client) ID :

Integration assistant (preview) Directory (tenant) ID :

Object ID :

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 :

i 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 Microsoft Identity Platform.

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](#)

Step 2. Edit the User Attributes and Claims. Add a New claim with Name: **roles** and select the value as **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 | ... |

Step 3. Navigate to **<Application-Name> > Manifest**. Edit the Manifest. The file is in JSON format and a default User is available to copy. For example- here 2 roles are created: User and Analyst.

Cisco-Firepower | Manifest

Search (Cmd+/) <> Save Discard Upload Download Got feedback?

OverviewQuickstartIntegration assistant (preview)

Manage

BrandingAuthenticationCertificates & secretsToken configurationAPI permissionsExpose an APIOwnersRoles and administrators (Preview)Manifest

Support + Troubleshooting

TroubleshootingNew support request

The editor below allows you to update this application by directly modifying its JSON representation.

```

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       }

```

Step 4. Navigate to <Application-Name> > **Users and Groups**. Edit the user and assign the newly created roles, as shown in this image.

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

Step 4. Log in to FMC and edit the Advanced Configuration in SSO. For, Group Member Attribute: assign the **Display name** that you have provided in Application Manifest to the roles.

▼ 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

Once that is done, you should be able to log in to their designated role.

Verify

Step 1. Navigate to the FMC URL from your browser: <https://<FMC URL>>. Click on **Single Sign-On**, as shown in this image.



Firepower Management Center

Username

Password

Single Sign-On

Log In

You are redirected to the Microsoft login page and successful login would return the FMC default page.

Step 2. On FMC, navigate to **System > Users** to see the SSO user added to the database.

test1@shbharticisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbharticisco.onmicrosoft.com

Administrator

External (SSO)

Troubleshoot

Verify the SAML Authentication and this is the workflow you achieve for successful authorization (This image is of a lab environment) :

Browser SAML Logs

```
GET https://10.106.46.191/sso/saml/login
GET https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/saml2?RelayState=7_ni-J1fNA5sEeVvoAuhcvtlH6CWKjxwyGhhxJpArDjKAFMbK-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
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 Logs

Verify the SAML Logs on FMC at `/var/log/auth-daemon.log`

```
root@shbhartic11:~/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/authnmethodsreferences:[http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password] http://schemas.microsoft.com/identity/claims/objectidentifier:[bee2eb18-e129-11df-a04a-42c06f0a3b36] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname:[Test 1] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[test1@shbharticisco.onmicrosoft.com] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:[Guy] mapped_role_uuid:[bee2eb18-e129-11df-a04a-42c06f0a3b36]]
auth-daemon 2020/08/09 04:59:11 I! Redirecting ID : id-56574e8a5f44bdd50102743d2cc9350b75f74d8c, URL : /sso/saml/login
```