Contents

Overview
Download And Installation
Configuration Steps
1. Configure Azure AD as IDP
2. Configure Magento as SP
3. Attribute Mapping
4. Role Mapping
Additional Resources

SAML Single Sign-On into Magento using Azure AD | Azure Active Directory SSO | Login using Azure AD

Azure AD (Azure Active Directory) Single Sign-On (SSO) login for Magento [SAML] can be achieved by using our **Magento SAML SP Single Sign-On (SSO) plugin**. Our SSO solution will make Magento SAML 2.0 compliant Service Provider establishing trust between the Magento site and Azure AD to authenticate users using Azure AD. Our Magento Single Sign-On (SSO) solution helps to secure Magento sites behind the SSO login so that users are authenticated using Best Azure AD / Azure B2C / Office 365 / Microsoft 365 login credentials. Seamless support for advanced SSO features like Attribute / Role Mapping etc.

Here we will go through a guide to configure SAML Single Sign-On SSO login between Magento site and Azure AD by considering **Azure AD as IdP** (Identity Provider) and **Magento as SP** (Service Provider). Our SSO plugin provides Unlimited user authentications from Azure AD / Azure B2C. To know more about features we provide in our Magento SAML Single Sign-On (SSO) plugin, you can **click here**.

Pre-requisites : Download And Installation

Installation using Composer:

- Purchase the **miniOrange SAML Single Sign-On - SAML SSO Login** extension from magento marketplace.
- Go to My profile -> My Purchases
- Please ensure you are using correct access keys (My Profile - Access Keys)
- Paste the access keys in your auth.json file inside your project
- Use the below command to add the extension to your project.

```
"composer require miniorange/saml-sso-login:version2"
```

- You can see the module name and list of versions in the selector below the extension module name.
- Run the following commands on command prompt to enable the extension.

```
php bin/magento setup:di:compile

php bin/magento setup:upgrade
```

Manual Installation:

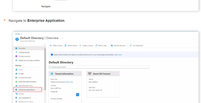
- Download the **miniOrange SAML Single Sign-On - SAML SSO Login** extension.
- Unzip all contents of the zip inside the MinOrangeSP directory.

```
{Root Directory of Magento}/app/code/MinOrange/SP
```

- Run the following commands on command prompt to enable the extension

```
php bin/magento setup:di:compile

php bin/magento setup:upgrade
```

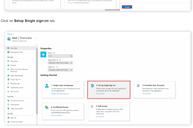


Steps to configure Azure AD SAML Single Sign-On (SSO) Login into Magento

1. Setup Azure AD as IdP (Identity Provider):

Follow the steps below to configure Azure AD as SP for Magento

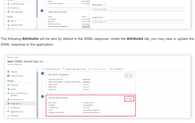
1. Configure Azure AD as IdP
   - In the Magento SAML SP SSO plugin, navigate to **Service Provider Metadata** tab. In this tab you will find the SP metadata such as SP Entity ID and ACS (Assertion Consumer Service) URL which are required to configure Azure AD as the Identity Provider.



Azure AD setup through Enterprise Applications | Azure AD setup through App Registrations

- Log in to **Azure AD Portal**
- Select **Azure Active Directory**

- Navigate to **Enterprise Application**.

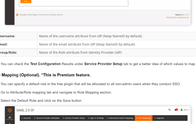


- Click on **New Application** button.

- Click on **Create your own Application**.

- Enter your app's name, then go to the **Non-gallery application** section and click the **Create** button.

- Click on **Setup Single sign-on** tab.



- Select the **SAML**, tab.

- After clicking **Edit**, from the Service Provider Metadata tab of the plugin, enter the **SP Entity ID** to **Identifier** and the **ACS URL** to **Reply URL**.

- The following **Attributes** will be sent by default in the SAML response. Under the **Attributes** tab, you may view or update the claims sent in the SAML response to the application.

- To get the Endpoints you'll need to configure your Service Provider, copy the **App Federation Metadata** url.

- **Assign users and groups to your SAML application**
  - To add a user or group, go to the **Users and Groups** tab and select **Add user/group**.

  - To assign the required user, go to **Users** and then go to **Select**.

  - In the **Select Role** section, you may also designate a role to your application.
  - You've successfully set up Azure AD SAML IdP (Identity Provider) to enable Azure AD SSO on your Magento site.

2. Configure Magento as SP (Service Provider):

- Copy **SAML Entity ID, SAML Single-Sign-On Endpoint URL, and a X.509 certificate** from Federation Metadata document and paste it in **SP Entity ID or Issuer, Single Sign-on Service URL, a X.509 Certificate** fields respectively in the plugin.

SP Entity ID or Issuer	SAML Entity ID in the Federation Metadata document
Single Sign-On Service URL	SAML Single Sign-On Endpoint URL in the Federation Metadata document
X.509 Certificate	X.509 Certificate in the Federation Metadata document

- Click on **Save** button to save all your settings.

- To check if your Magento as SP is configured correctly, click the **Test Configuration** button.

3. Attribute Mapping (Optional) : This is Premium feature.

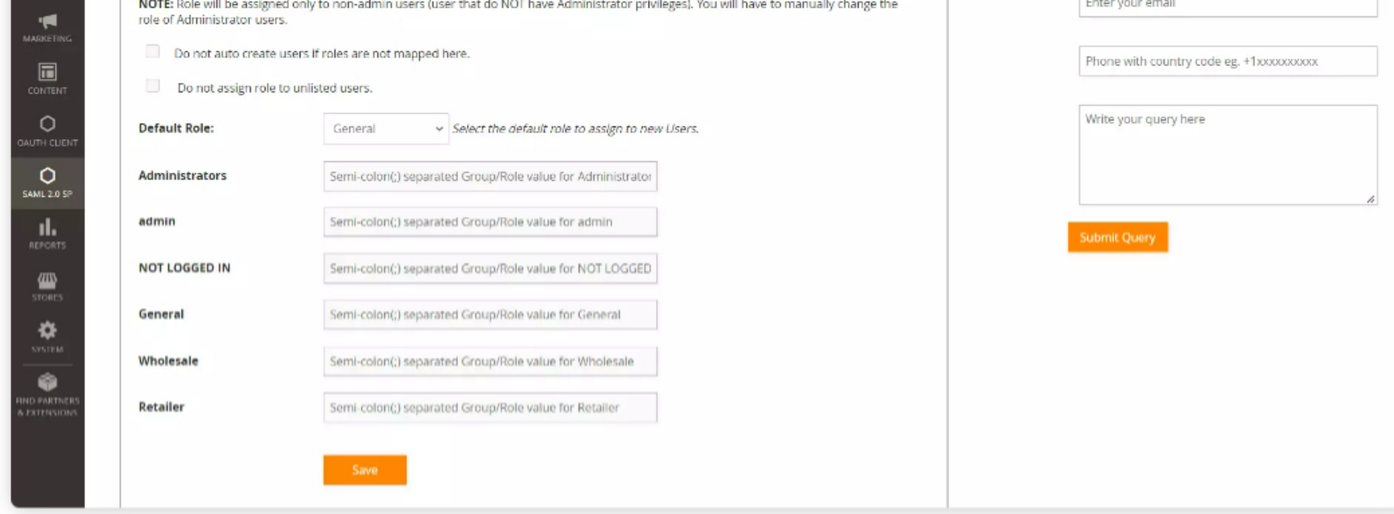
- Attributes are user details that are stored in your Identity Provider
- Attribute Mapping helps you to get user attributes from your Identity Provider (IdP) and map them to Magento user attributes like firstname, lastname etc.
- While auto-registering the users in your Magento site these attributes will automatically get mapped to your Magento user details.
- Enter **NameID** (an be mapped to Magento's Email and Username characteristics with the free plugin. Multiple user attributes from the IdP) on the other hand, can be mapped to Magento attributes in the premium version of the plugin. You can map custom attributes that you've added to your IdP in addition to the default attributes.
- Where user particular SSO, the NameID value sent by the IdP will get mapped to the email and the username of the Magento user.

Username:	Name of the username attribute from IdP (keep NameID by default)
Email:	Name of the email attribute from IdP (keep NameID by default)
GroupRole:	Name of the Role attribute from Identity Provider (IdP)

- You can check the **Test Configuration** Results under **Service Provider Setup** tab to get a better idea of which values to map here.

4. Role Mapping (Optional) : This is Premium feature.

- You can specify a default role in the free plugin that will be allocated to all non-admin users when they conduct SSO.
- Go to Attribute/Role mapping tab and navigate to Role Mapping section.
- Select the Default Role and click on the Save button.



In this Guide, you have successfully configured **Azure AD SAML Single Sign-On (Azure AD SSO Login)** choosing **Azure AD as IdP** and **Magento as SP** using **Magento SAML Sigle Sign-On (SSO) Login plugin** .This solution ensures that you are ready to roll out secure access to your Magento site using **Azure AD login** credentials within minutes.

Additional Resources

- What is Single Sign-On (SSO) Login?
- Azure AD SSO | Azure Single Sign-On (SSO) Login
- Azure AD - Overview
- Configure Azure AD as Identity Provider (IdP) for SSO Login
- Azure AD - What is Azure Active Directory?
- Magento SAML Single Sign On (SSO) Plugin.

If you are looking for anything which you cannot find, please drop us an email on **magentosupport@xecurify.com**

miniOrange

+1 978 658 9387 (US)
+91 97178 45846 (India)

info@xecurify.com

STAY CONNECTED

SIGN UP FREE

Product

Single Sign On
Identity Brokering
OAuth / OpenID Connect Server
Multi Factor Authentication
Adaptive Authentication
User Provisioning
Directory Services

Solutions

SAML Solutions
OAuth Solutions
2FA Solutions
Mobile Solutions
Directory Integrations
Federation Integrations
Windows Solutions
SSO Connectors
Secure Browser SSO
View All

Why miniorange

Our Success Stories
Content Library
Videos
FAQs
Forum

Company

Overview
News
Partners
Customers
Contact Us

Hello there!
Need Help? We are right here!

@ Copyright 2022 miniOrange. All Rights Reserved.