# SAML Authentication with Entra ID (Azure Portal)

SAML is Open Standard Protocol for exchanging authentication and authorization data between Identity Provider (Auth0, ADFS, Enta ID) and Service Provider (Client Application). SAML is an XML based language.

## Entra ID in Berkley

- Berkley will allow applications that are exclusively used by Berkley employees. Software as a Service (SaaS) applications are the preferred choice due to their cloud-based nature.
- To Setup an application in Berkley ID, the application must be approved from BTS Information security team and the Application must complete TPRM and procurement process.

## Flow

### User Access Attempt:

- If a user tries to access the application through a web browser, they will be redirected to Azure AD to sign in.

### Authentication Request:

- Azure AD prompts the user to sign in, if they are not already authenticated.
- The application generates an authentication request, which includes a SAML request.
- This request is sent to Azure AD.

### User Authentication:

- Azure AD authenticates the user using the credentials provided.
- If successful, Azure AD generates a SAML assertion, which contains information about the user (such as username, email, roles, etc.).
- This assertion is digitally signed by Azure AD to ensure its authenticity and integrity.

### SAML Response:

- Azure AD sends the SAML assertion back to the application in the form of a SAML response.
- This response is sent through the user's browser, typically via HTTP POST.

### User Access Granted:

- The application receives the SAML response and verifies its authenticity by validating the digital signature.
- If the signature is valid and the assertions within the response are acceptable, the application grants access to the user.

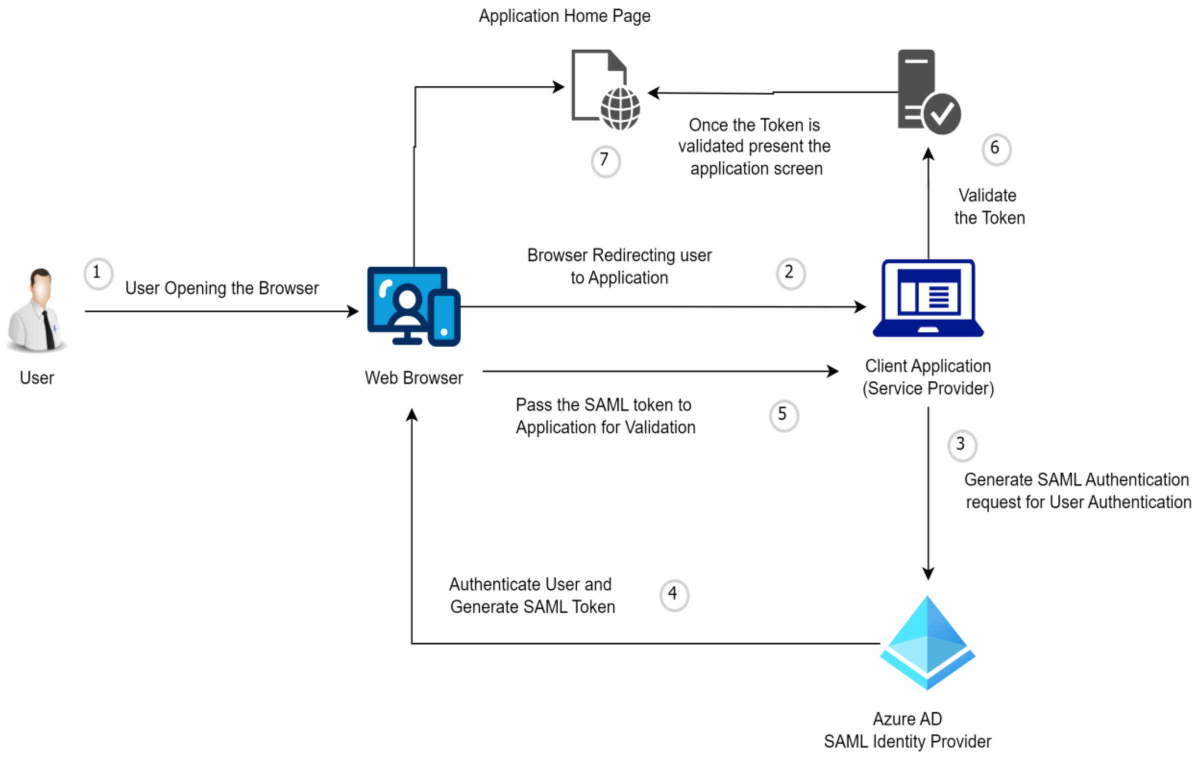
**Session Establishment:**

- Once access is granted, the application establishes a session for the user, allowing them to interact with the application without needing to re-authenticate (until the session expires).

**User Interaction:**

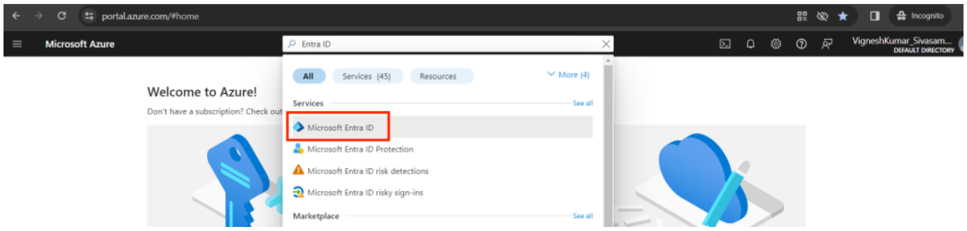
The user can now interact with the application as authenticated.

**Flow Diagram**

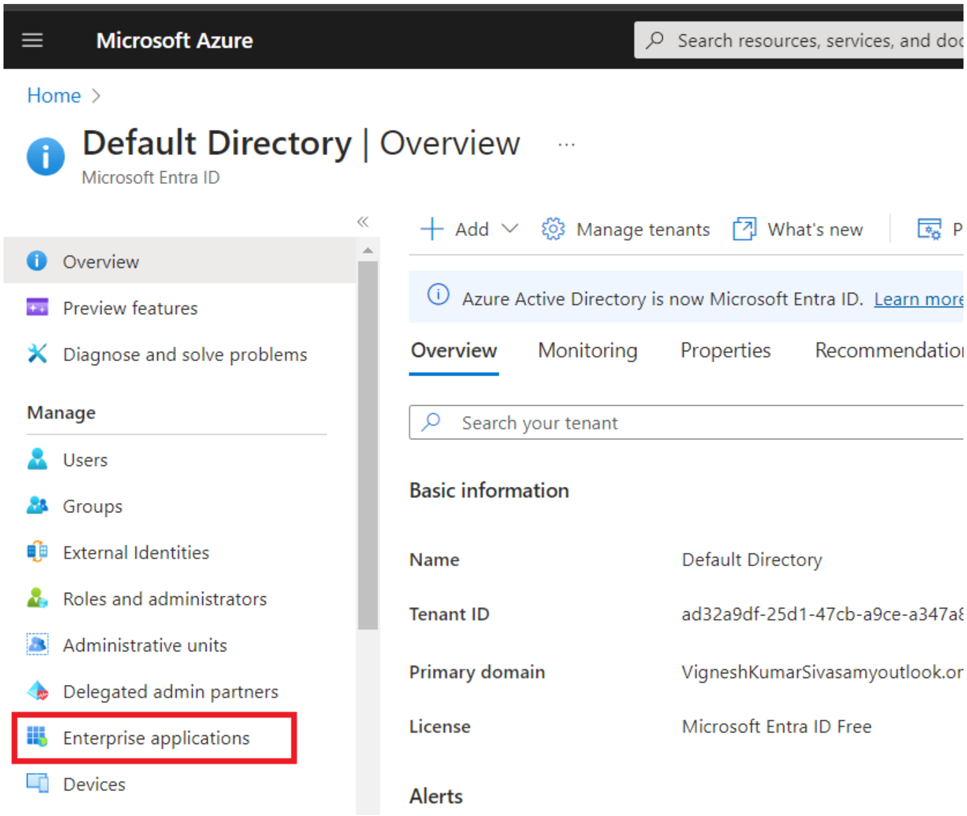

Application Home Page
7
Once the Token is validated present the application screen
6
Validate the Token
1
User Opening the Browser
User
Web Browser
Browser Redirecting user to Application
2
Client Application (Service Provider)
Pass the SAML token to Application for Validation
5
3
Generate SAML Authentication request for User Authentication
Authenticate User and Generate SAML Token
4
Azure AD SAML Identity Provider

## Setup SSO Configuration in Entra ID

1. Open Azure Entra ID Portal and Open “Microsoft Entra ID” Service.



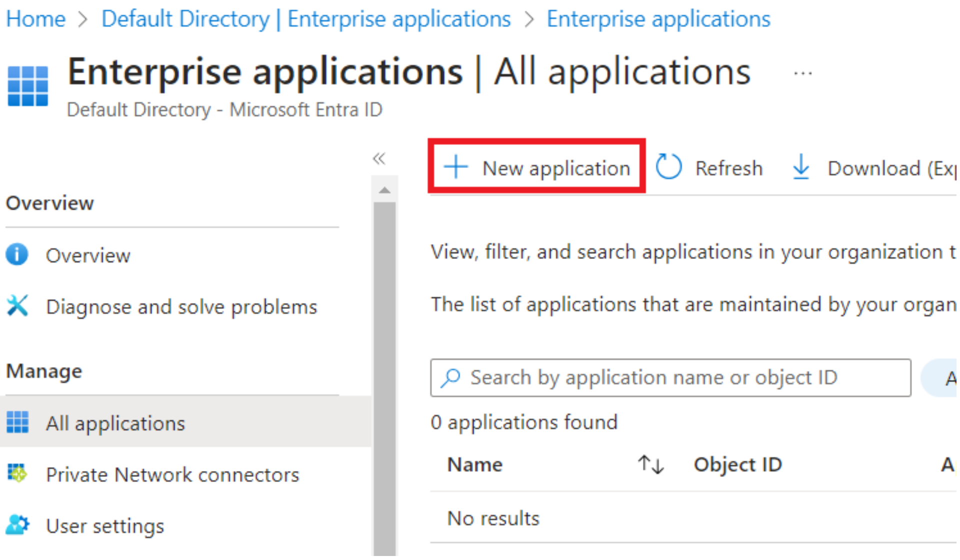
2. Choose “**Enterprise Application**”



Basic information

| | |
|---|---|
| Name | Default Directory |
| Tenant ID | ad32a9df-25d1-47cb-a9ce-a347a8 |
| Primary domain | VigneshKumarSivasamyoutlook.or |
| License | Microsoft Entra ID Free |

3. All the available configured applications will be listed (Currently .


Home > Default Directory | Enterprise applications > Enterprise applications
Enterprise applications | All applications ...
Default Directory - Microsoft Entra ID
Overview
Overview
Diagnose and solve problems
Manage
All applications
Private Network connectors
User settings
New application
Refresh
Download (Ex
Search by application name or object ID
Name
Object ID
A

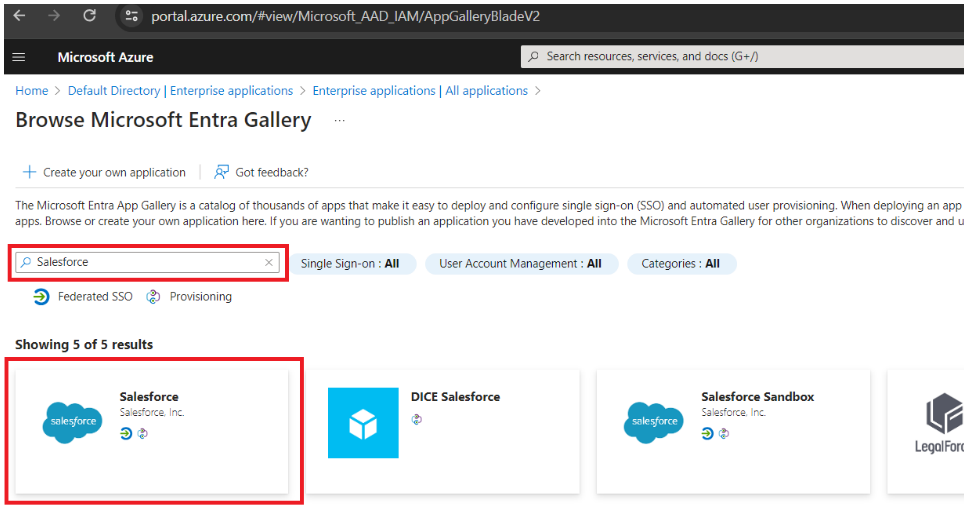
View, filter, and search applications in your organization t

The list of applications that are maintained by your organ

0 applications found

No results

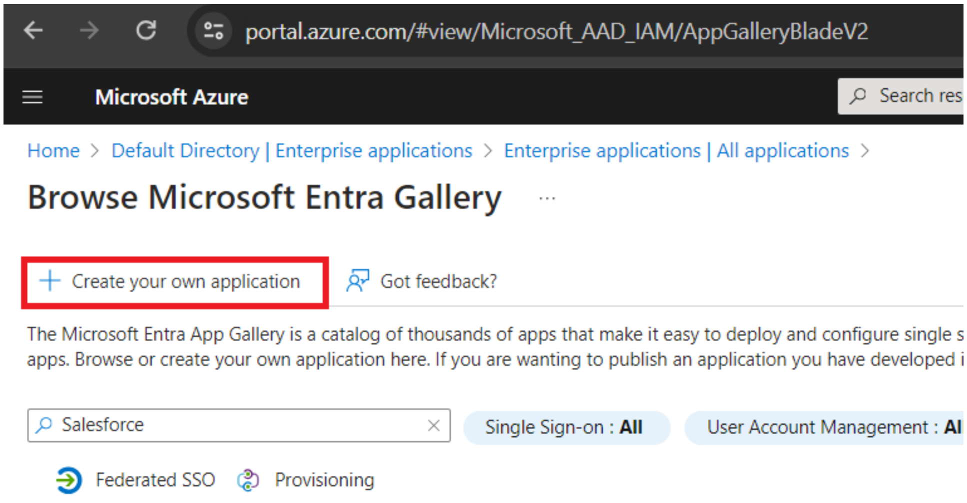
4. Microsoft Entra Gallery will be appear - Microsoft Entra application gallery, is a collection of thousands of software applications pre-integrated with Microsoft Entra ID. Entra ID is a core component of Microsoft Entra, a suite of identity and access management tools. The gallery simplifies the process of adding new applications to your organization's Entra environment. (I choose Salesforce for an Example)


portal.azure.com/#view/Microsoft_AAD_IAM/AppGalleryBladeV2
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | Enterprise applications > Enterprise applications | All applications >
Browse Microsoft Entra Gallery ...
Create your own application
Got feedback?
Salesforce
Single Sign-on : All
User Account Management : All
Categories : All
Federated SSO
Provisioning
Salesforce
Salesforce, Inc.
DICE Salesforce
Salesforce Sandbox
Salesforce, Inc.
LegalForc

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and u

Showing 5 of 5 results

5. If the application is not found, we can use "**Create your own application**" to setup an application



portal.azure.com/#view/Microsoft_AAD_IAM/AppGalleryBladeV2

Microsoft Azure

Home > Default Directory | Enterprise applications > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

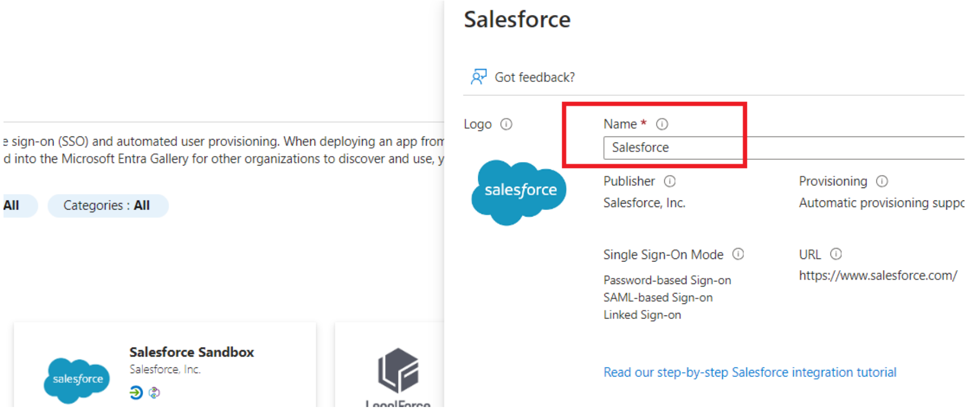
+ Create your own application    Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single s apps. Browse or create your own application here. If you are wanting to publish an application you have developed i

Salesforce    Single Sign-on : **All**    User Account Management : **Al**

Federated SSO    Provisioning

6. Popups will appear to create applications. Add the Name of the application. Name format should be (Company Name-Application Name-Environment) and click “**Create Application**” to proceed



Salesforce

Got feedback?

Logo

Name * : Salesforce

Publisher: Salesforce, Inc.

Provisioning: Automatic provisioning suppc

Single Sign-On Mode: Password-based Sign-on, SAML-based Sign-on, Linked Sign-on

URL: https://www.salesforce.com/

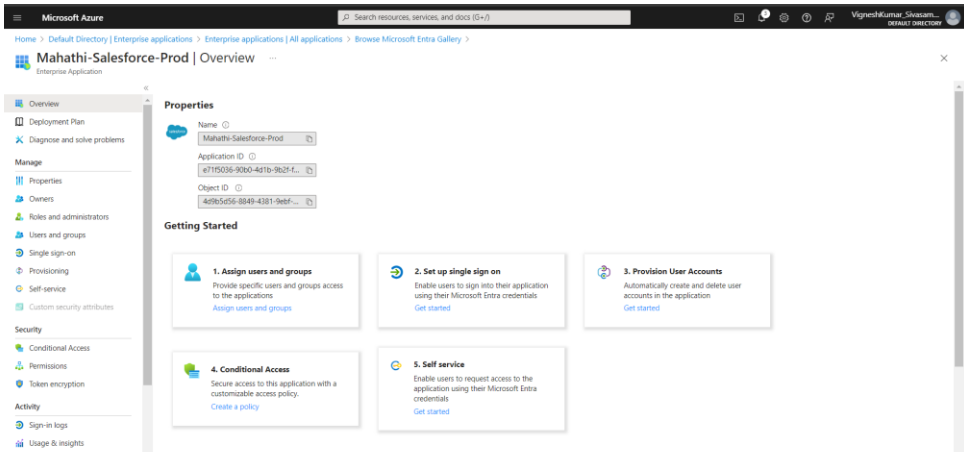
Read our step-by-step Salesforce integration tutorial

e sign-on (SSO) and automated user provisioning. When deploying an app from d into the Microsoft Entra Gallery for other organizations to discover and use, y

All    Categories : All

Salesforce Sandbox
Salesforce, Inc.

7. Application will be created



Properties

Name: Mahathi-Salesforce-Prod

Application ID: e71f5036-90b0-4d1b-9b2f-f...

Object ID: 4d9b5d56-8849-4381-9ebf-...

Getting Started

1. Assign users and groups: Provide specific users and groups access to the applications. Assign users and groups

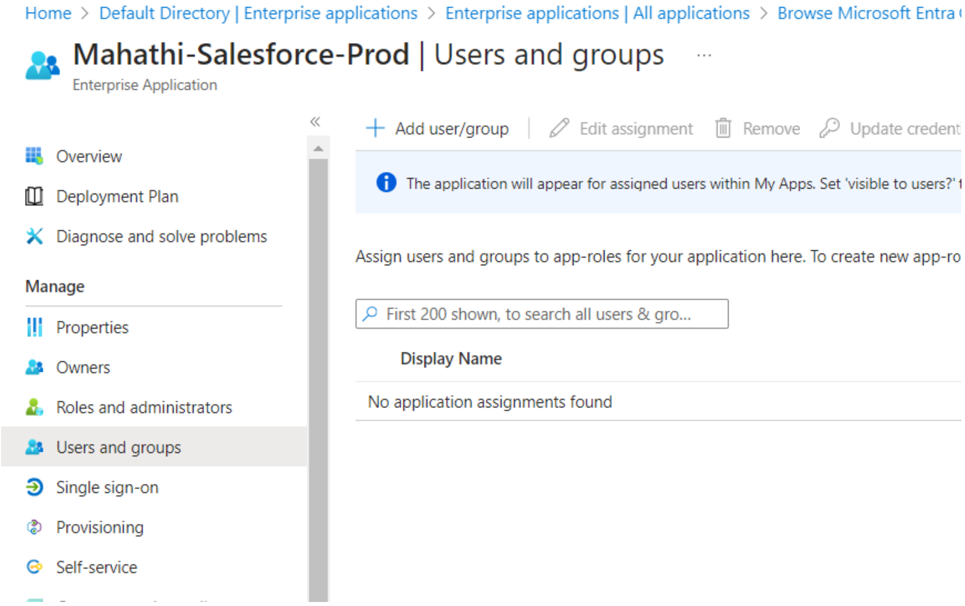
2. Set up single sign on: Enable users to sign into their application using their Microsoft Entra credentials. Get started

3. Provision User Accounts: Automatically create and delete user accounts in the application. Get started

4. Conditional Access: Secure access to this application with a customizable access policy. Create a policy

5. Self service: Enable users to request access to the application using their Microsoft Entra credentials. Get started

8. Click “**Users and Groups**” to add the access control. We can add individual users, or we add AD Groups to allow access to the application. Only specified users or group members can access the application. Add user\group by clicking “Add user/group”



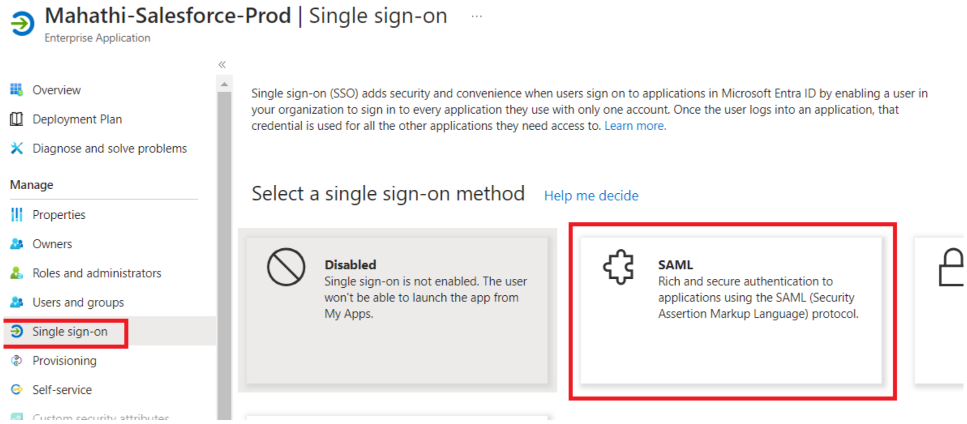
The application will appear for assigned users within My Apps. Set 'visible to users?' t

Assign users and groups to app-roles for your application here. To create new app-ro

First 200 shown, to search all users & gro...

| Display Name |
|---|
| No application assignments found |

9. Click “Single Sign On” and choose “SAML”. Configuration page will appear.



Mahathi-Salesforce-Prod | Single sign-on

Enterprise Application

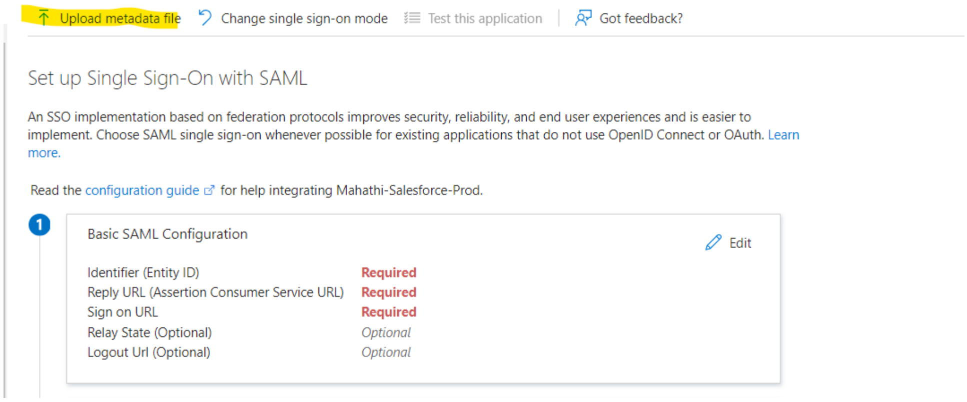
Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

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.

10. If the application team has the metadata, we can upload the metadata to configure all the required configuration by using up. (In general, metadata means It will contain all the required details to setup and SSO).



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Mahathi-Salesforce-Prod.

1 Basic SAML Configuration Edit

| | |
|---|---|
| Identifier (Entity ID) | Required |
| Reply URL (Assertion Consumer Service URL) | Required |
| Sign on URL | Required |
| Relay State (Optional) | *Optional* |
| Logout Url (Optional) | *Optional* |

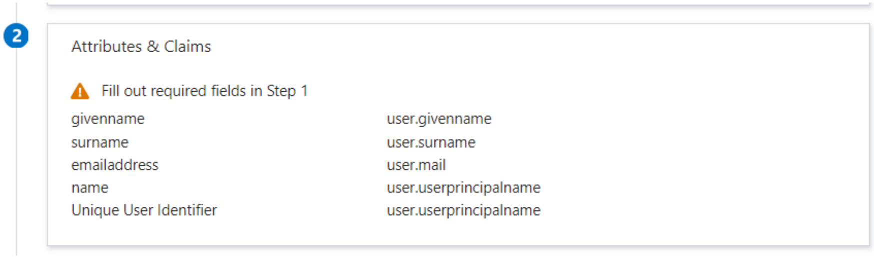
11. If the application team didn’t have the metadata, we need configure the details manually.
12. **Basic SAML Configuration**
    a. **Entity ID -** Entity ID (Entity Identifier) is a unique identifier assigned to each participating entity (such as an Identity Provider or Service Provider) within the SSO ecosystem. It helps in the identification and authentication process during SSO transactions. For example, when a user attempts to access a service, the Service Provider sends a SAML authentication request to the Identity Provider. This request includes the Entity ID of the Service Provider, allowing the Identity Provider to recognize and authenticate the Service Provider. Similarly, when the Identity Provider sends a SAML response with the user's authentication information, it includes the Entity ID of the Identity Provider, allowing the Service Provider to verify the authenticity of the response.

b. **Reply URL or Assertion Consumer Service URL -** Reply URL or ACS URL serves as the location where the Service Provider expects to receive SAML assertions from the Identity Provider during the SSO process. When a user attempts to access a service that requires authentication, the service (known as the Service Provider or SP) redirects the user to the Identity Provider (IdP) for authentication. After the user successfully authenticates with the IdP, the IdP generates a SAML assertion containing information about the user's identity and authentication status.

c. **Sign on URL -** Sign-On URL is the entry point for users to begin the authentication process in an SSO system. Sign-On URL refers to the specific URL or endpoint where users initiate the authentication process to access protected resources or applications. This URL typically leads to the login page

### 13. Attributes and Claims

a. It is a user information piece exchanged between the IdP and SP during the authentication process. These attributes can include user attributes such as username, email address, roles, group memberships, and any other relevant information needed by the SP to make access control decisions or personalize the user's experience.

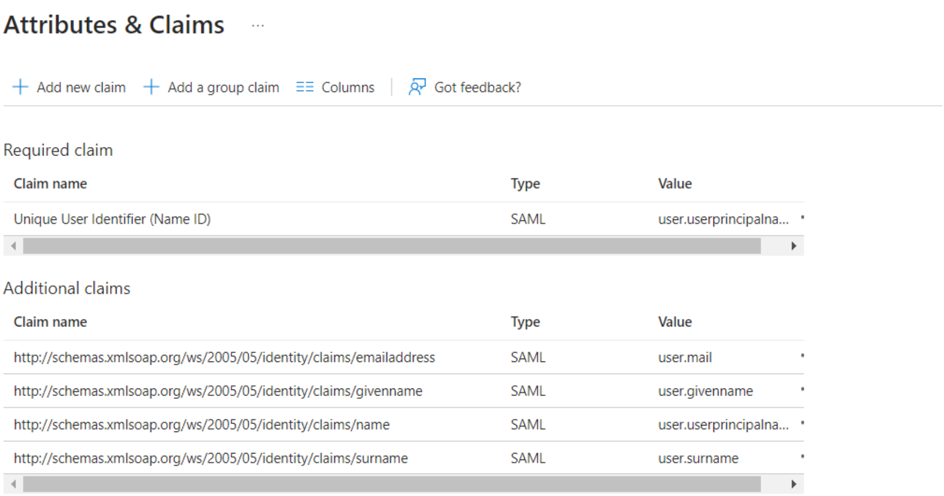


2 Attributes & Claims

⚠ Fill out required fields in Step 1

| | |
|---|---|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

b. We can add additional claims based on the application team requirement with required claim



Attributes & Claims

Required claim

| Claim name | Type | Value |
|---|---|---|
| Unique User Identifier (Name ID) | SAML | user.userprincipalna... |

Additional claims

| Claim name | Type | Value |
|---|---|---|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | SAML | user.mail |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | SAML | user.givenname |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | SAML | user.userprincipalna... |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | SAML | user.surname |

## Conclusion:

In conclusion, implementing Single Sign-On (SSO) through Entra ID offers many advantages in user convenience, efficiency, and centralized authentication management. However, it's crucial to emphasize that the configuration process demands meticulous attention to security measures. Failure to adhere to recommended security protocols and best practices can introduce vulnerabilities into the system, potentially compromising sensitive user data and system integrity.

When configuring SSO with Entra ID, it's imperative to prioritize security at every step of the process. This includes employing robust encryption methods, implementing secure token exchange mechanisms, and enforcing strict access controls.