

SAML Authentication with Enta 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.

Enta 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.

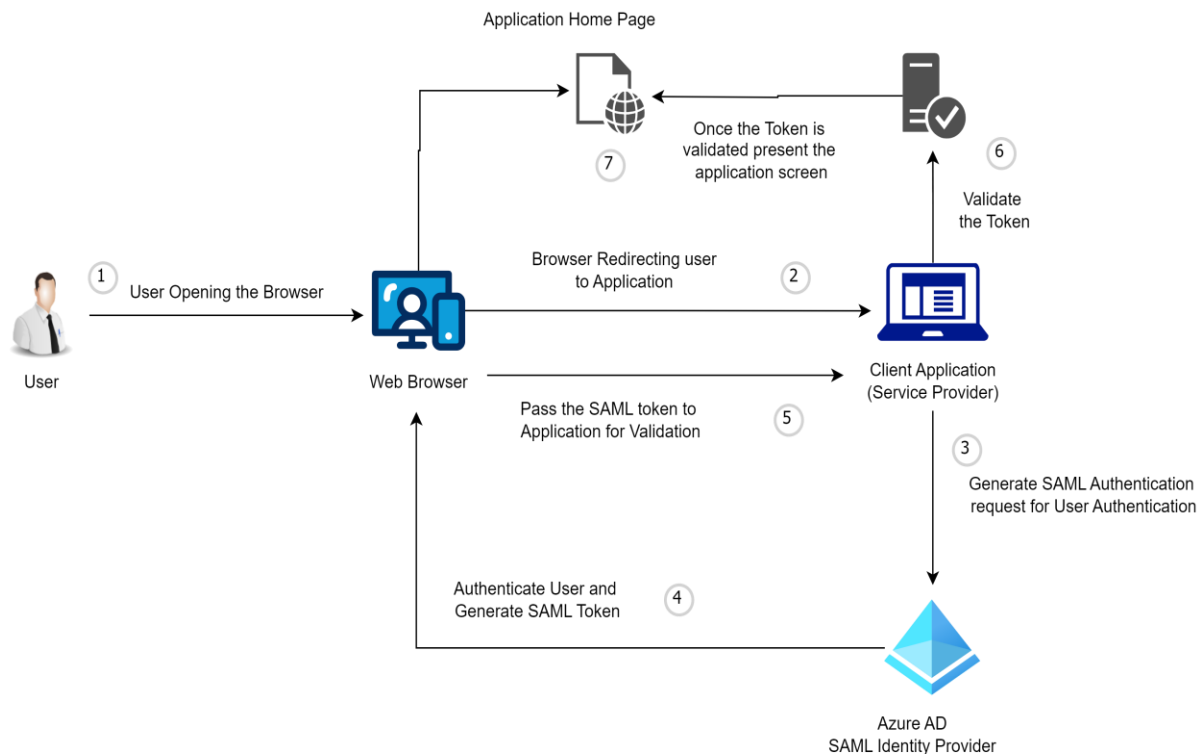
Session Establishment:

- 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:

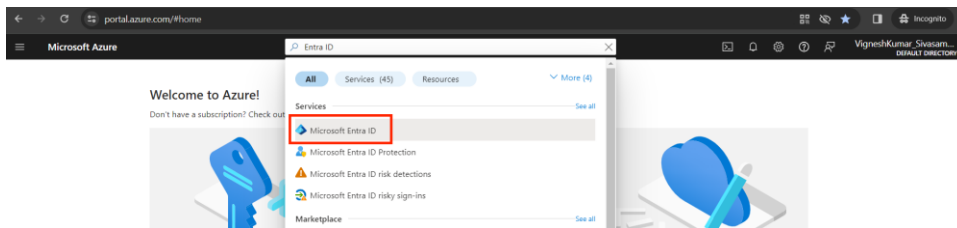
The user can now interact with the application as authenticated.

Flow Diagram

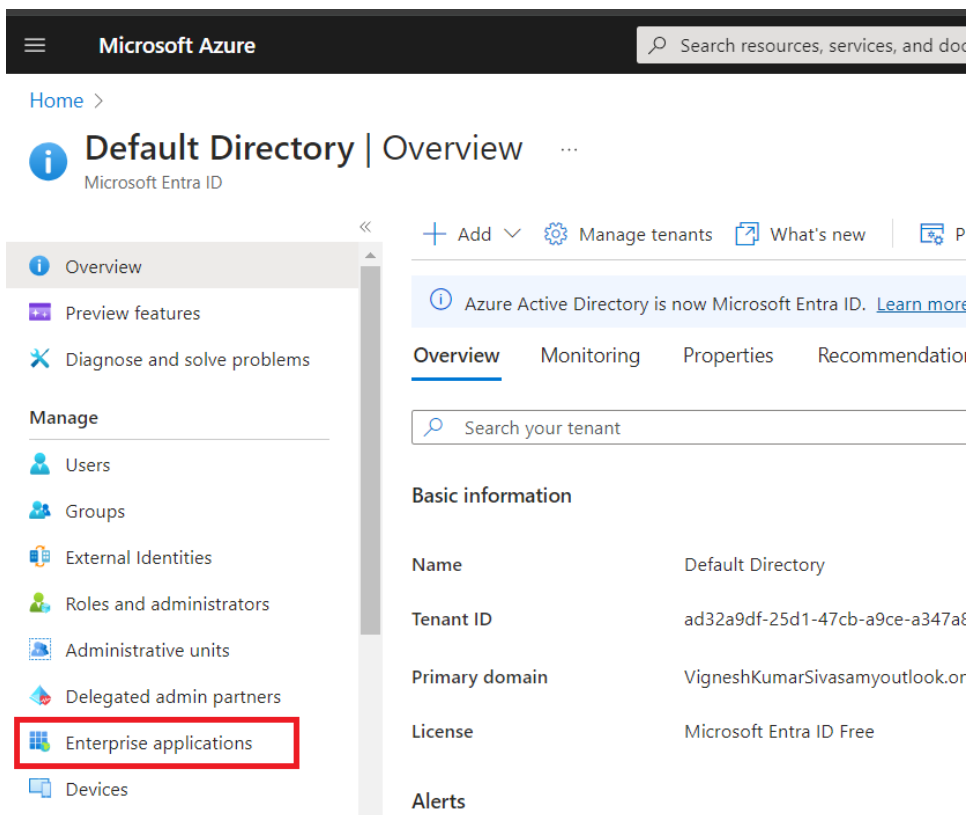


Setup SSO Configuration in Entra ID

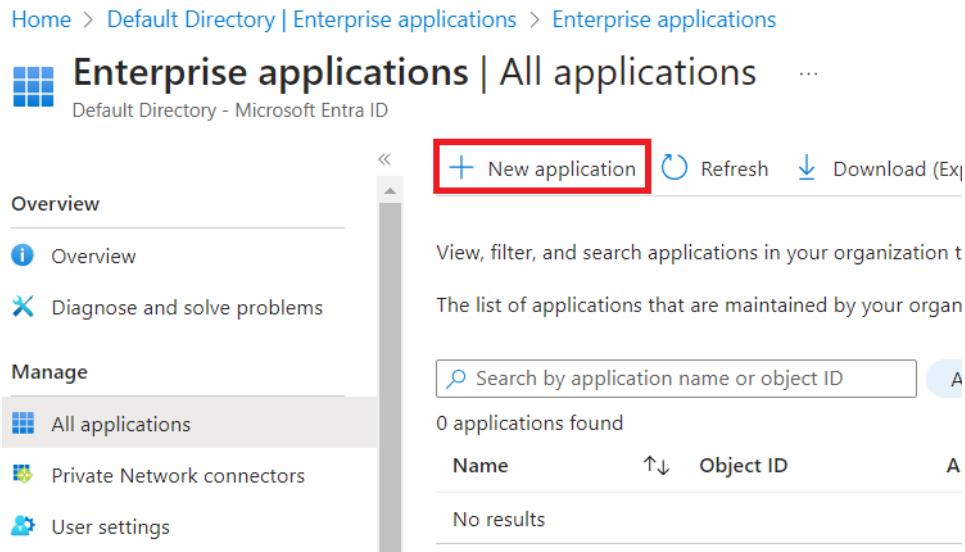
1. Open Azure Entra ID Portal and Open “Microsoft Entra ID” Service.



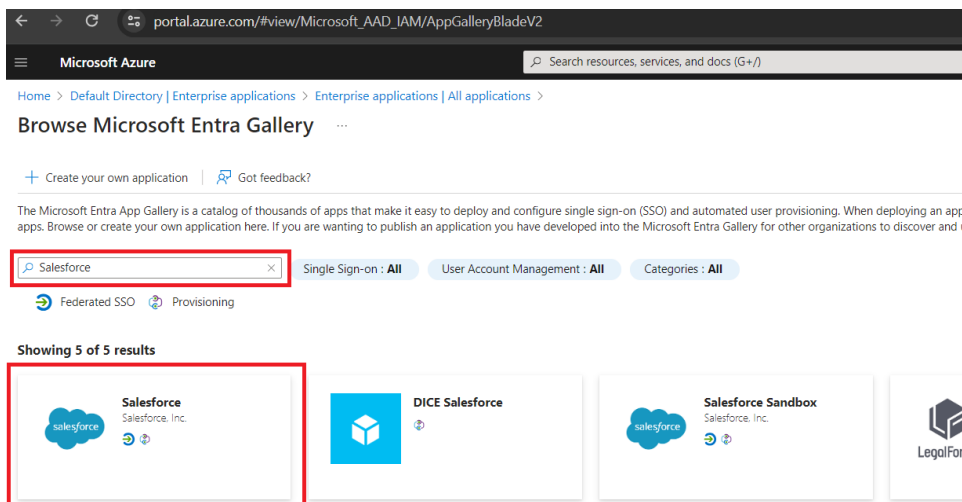
2. Choose “Enterprise Application”



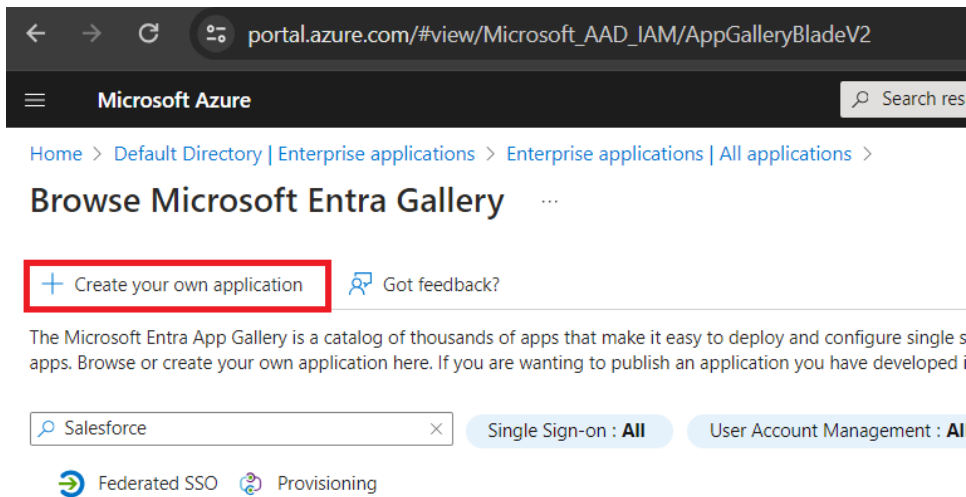
3. All the available configured applications will be listed (Currently .



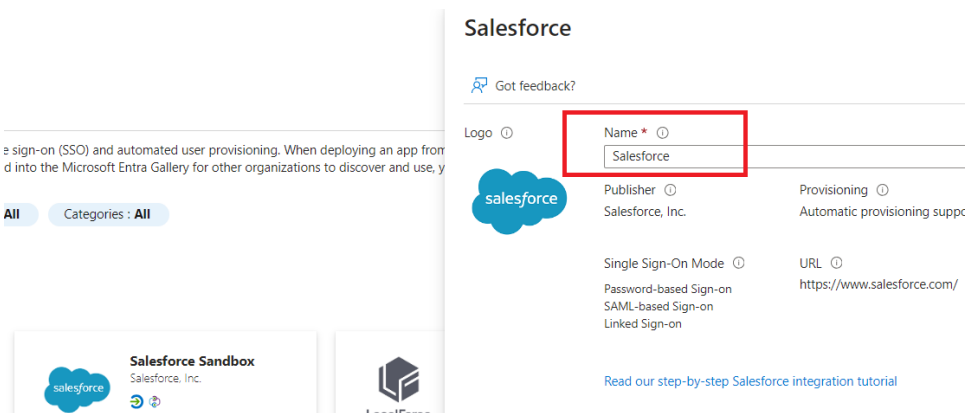
4. Microsoft Entra Gallery will be appear - Microsoft Entra application gallery, is a collection of thousands of software applications pre-integrated with Microsoft Entra ID. Entra ID is a core component of Microsoft Entra, a suite of identity and access management tools. The gallery simplifies the process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



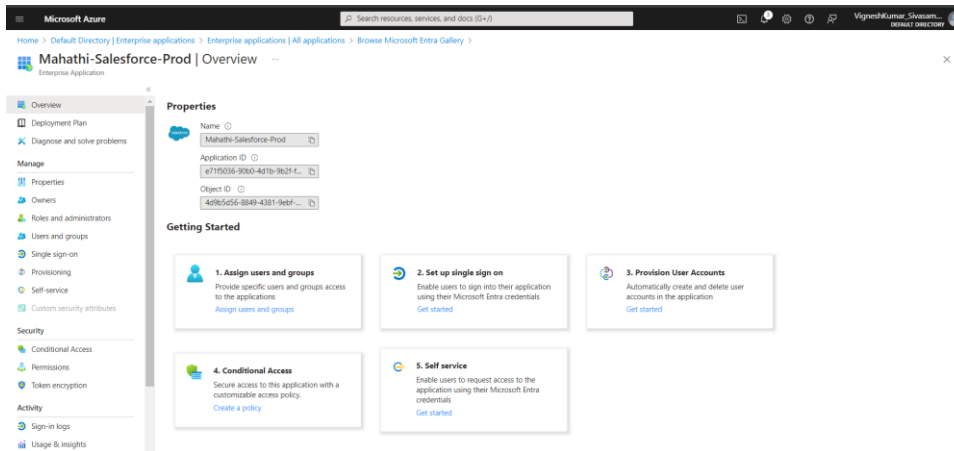
5. If the application is not found, we can use “**Create your own application**” to setup an application



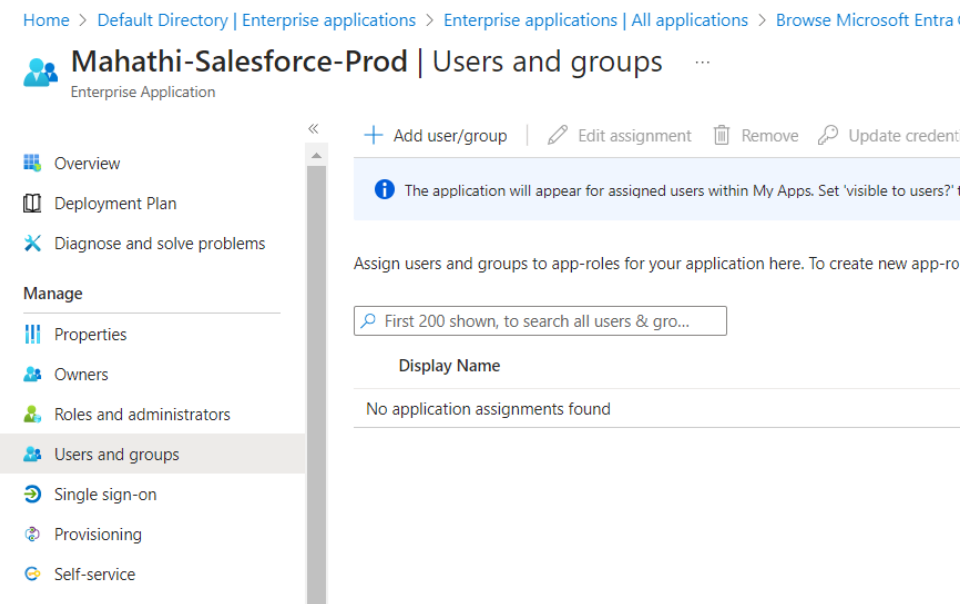
6. Popups will appear to create applications. Add the Name of the application. Name format should be (Company Name-Application Name-Environment) and click **“Create Application”** to proceed



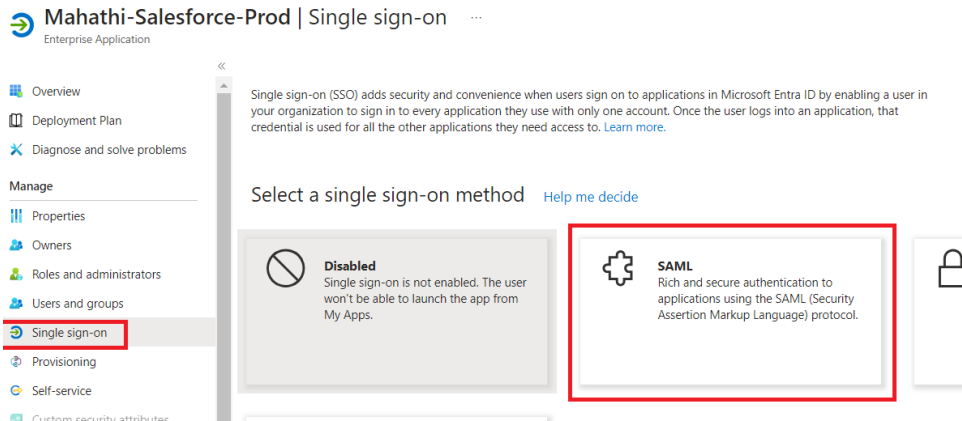
7. Application will be created



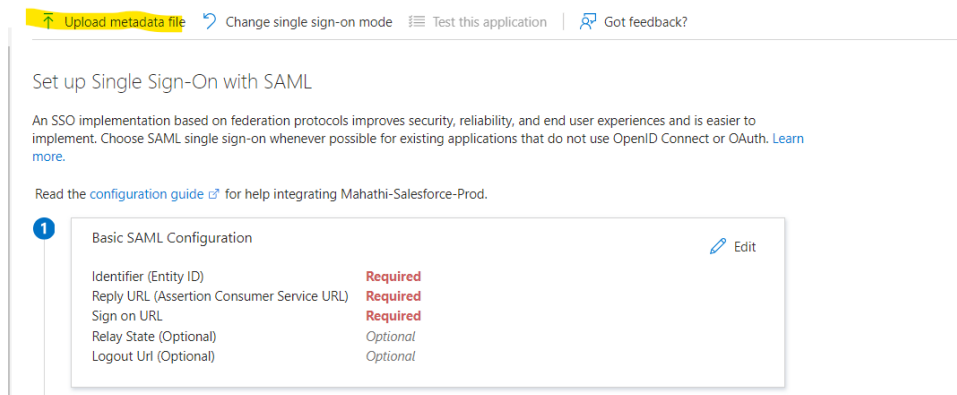
8. Click **“Users and Groups”** to add the access control. We can add individual users, or we add AD Groups to allow access to the application. Only specified users or group members can access the application. Add user\group by clicking **“Add user/group”**



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



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).



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 ...

+ Add new claim + Add a group claim Columns | Got feedback?

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.