

# Integrating Bitwarden SSO / SCIM with Microsoft Entra ID using SAML 2.0

With Trusted Devices Encryption and Domain Verification

SSO Identifier: `bitwarden-saml`  
Enterprise App: `bw-saml-az`

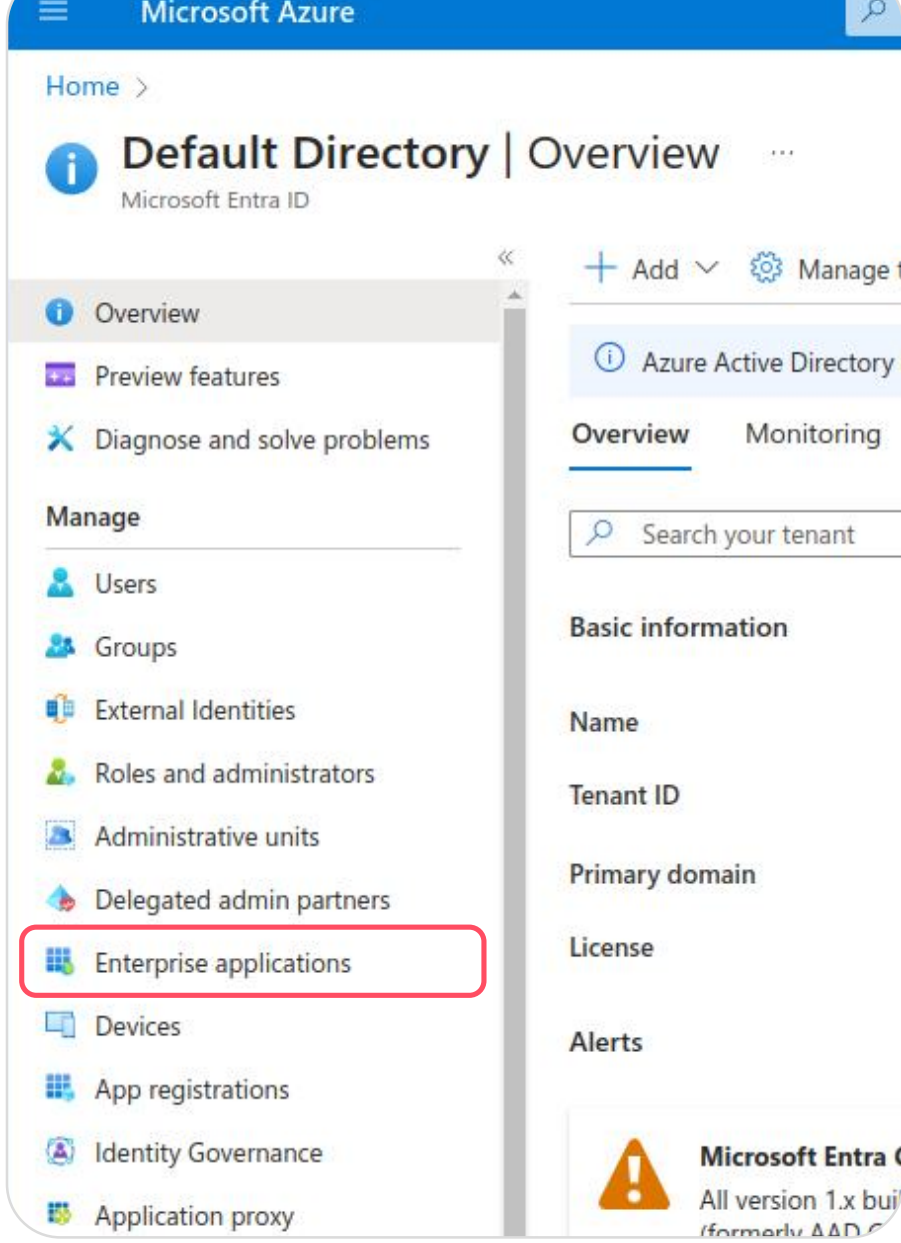
## Links:

- <https://bitwarden.com/help/about-sso/>
- <https://bitwarden.com/help/about-scim/>
- <https://bitwarden.com/help/domain-verification/>
- <https://bitwarden.com/help/about-trusted-devices/>
- <https://bitwarden.com/help/saml-microsoft-entra-id/>

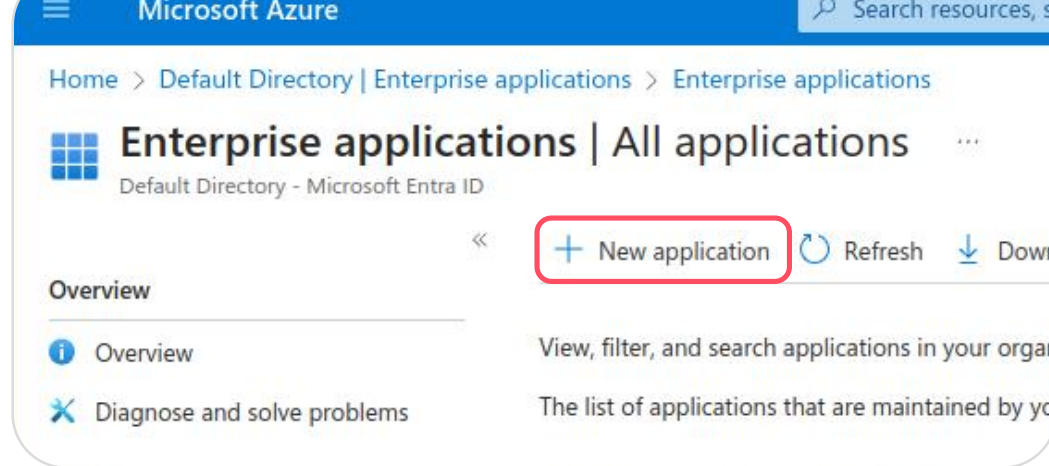
## 1 Create Enterprise Application

Azure Portal: go to Microsoft Entra ID

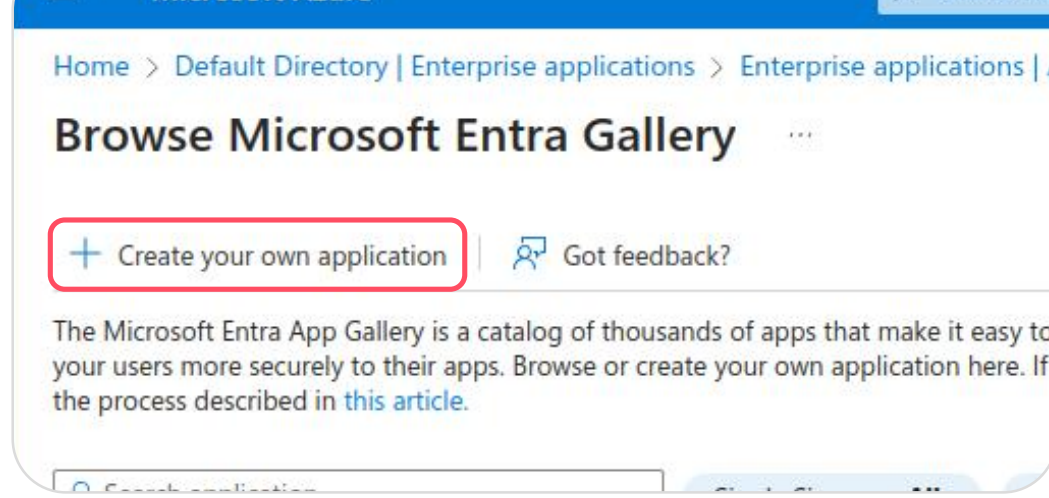
### 1.1 Select Enterprise applications:



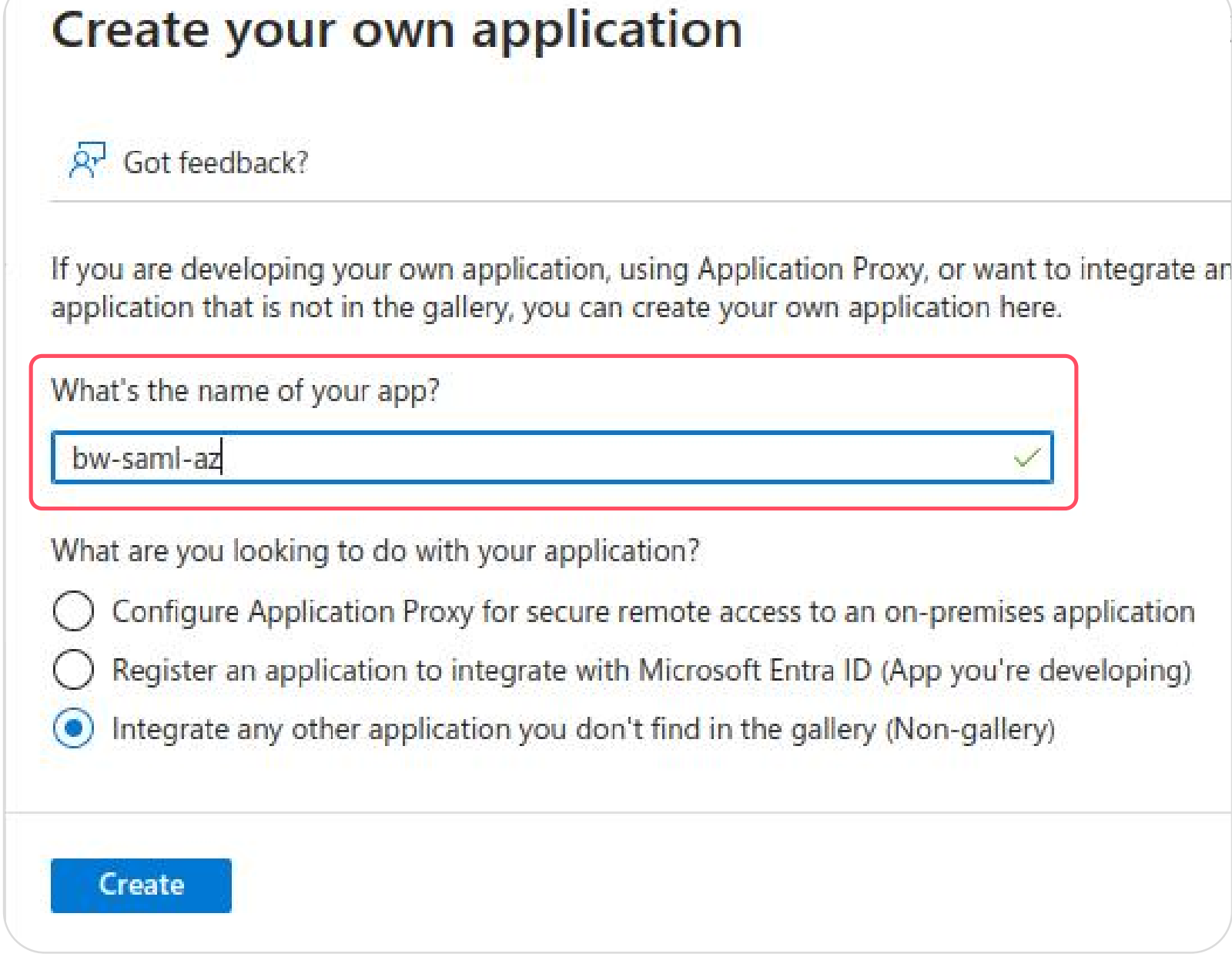
### 1.2 Select the New application button:



### 1.3 Click Create your own application:



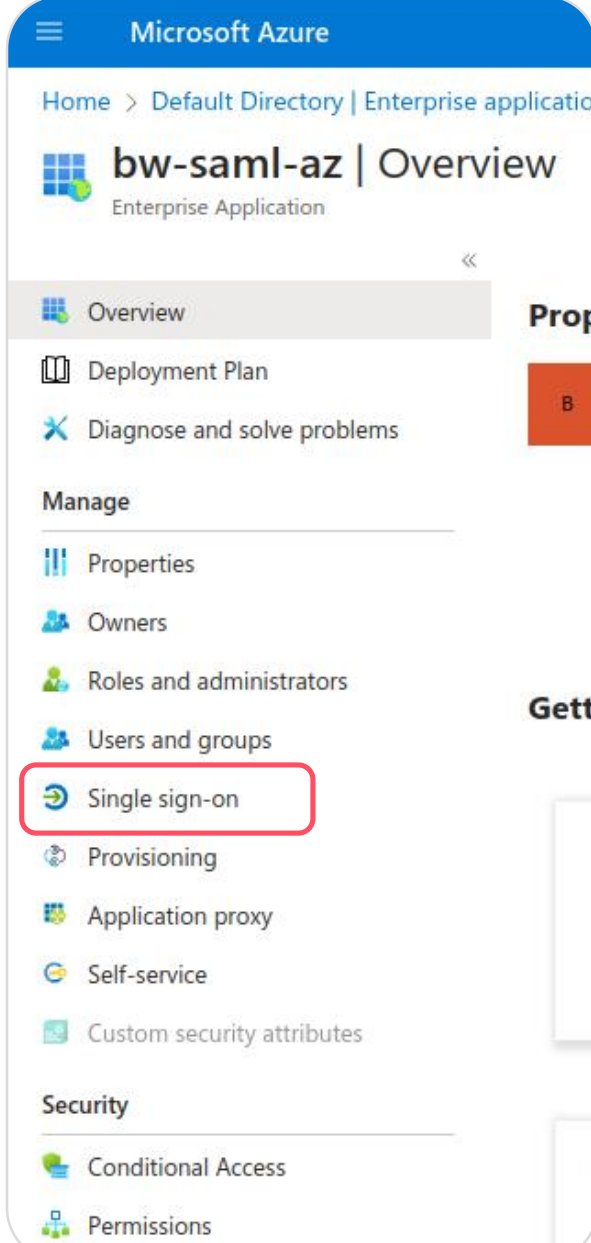
### 1.4 Give this application a unique name:



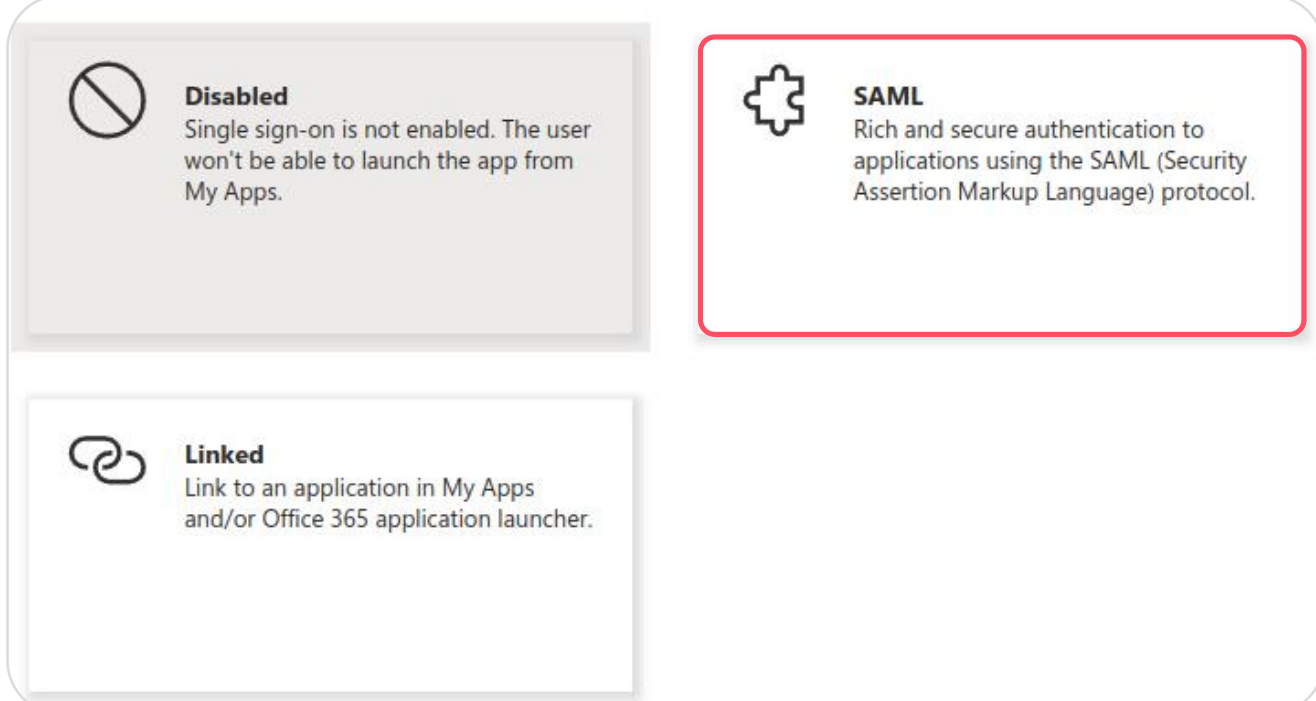
## 2 Enable Sign-On

Prepare your AZ app to

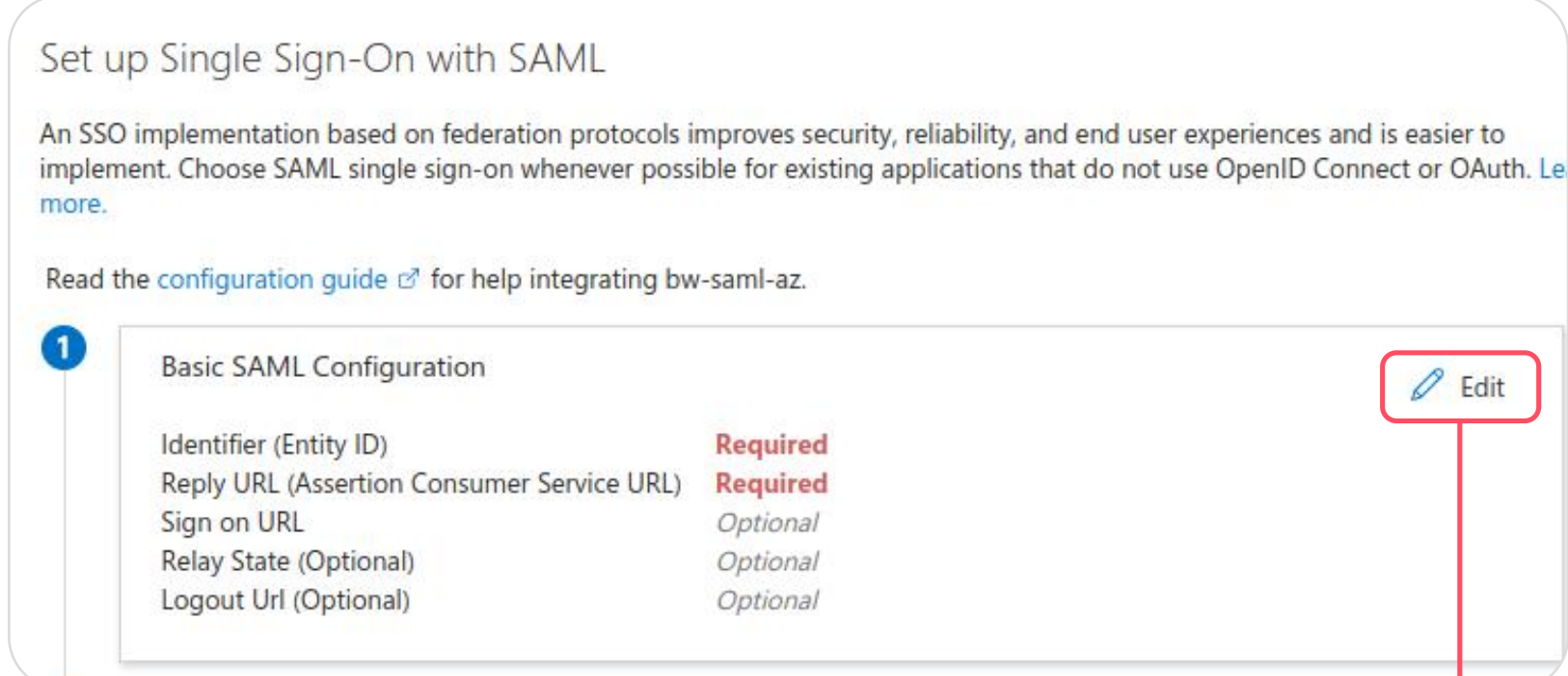
### 2.1 Click Single sign-on:



### 2.2 On the Single Sign-On screen, select SAML:

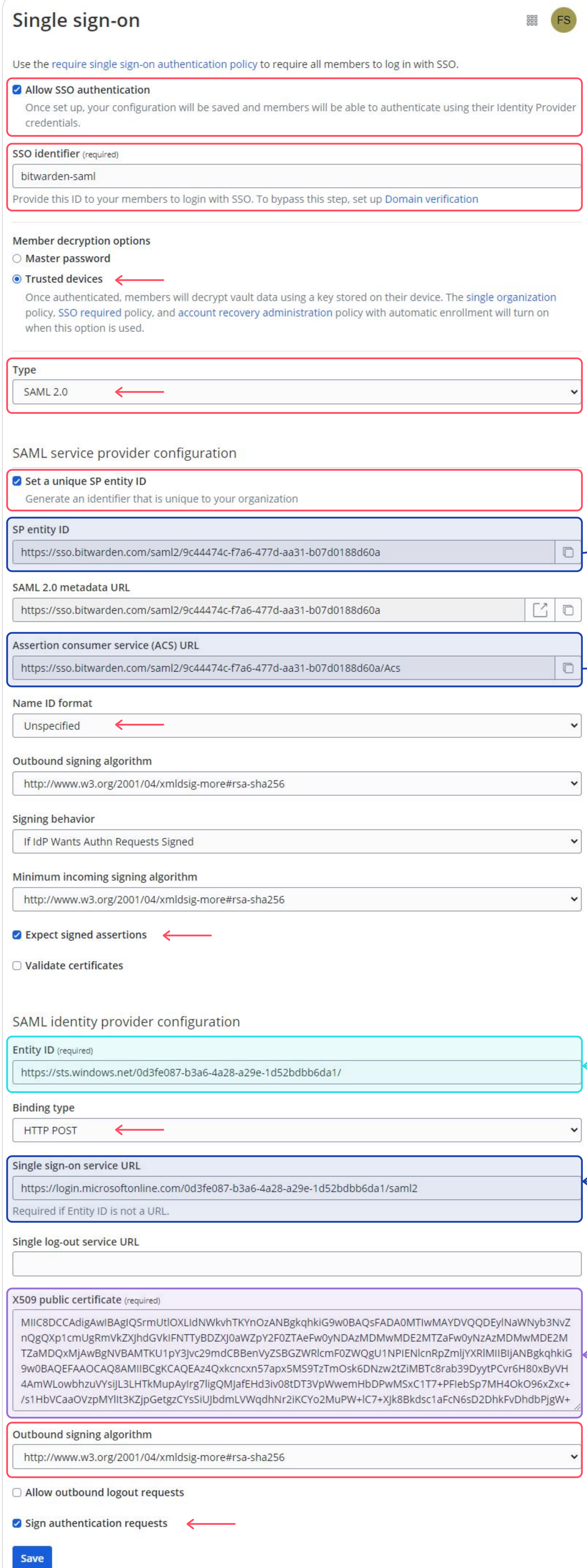


### 2.3 Click on Edit to edit Basic SAML Configuration:

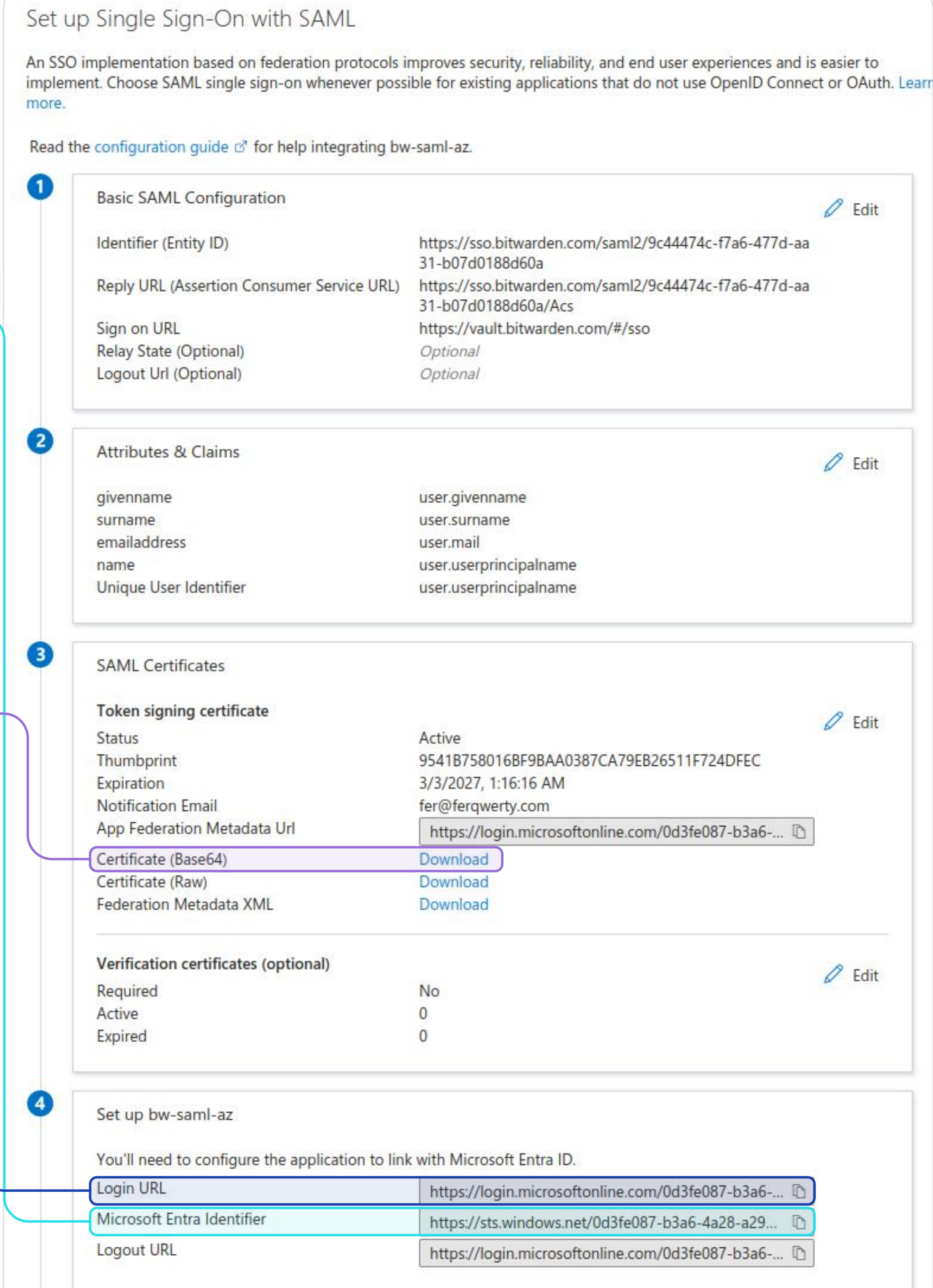
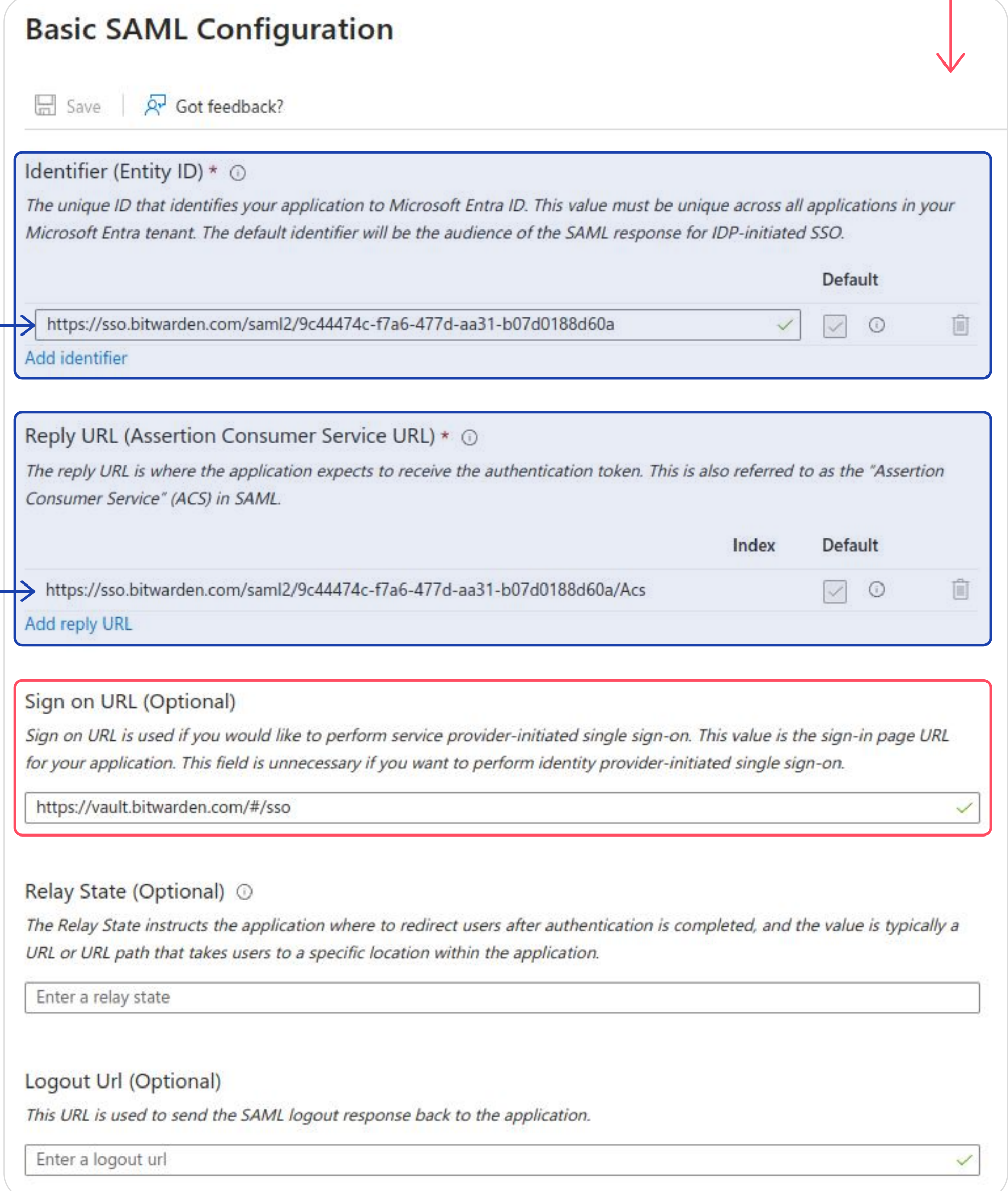


## 3 Configure Bitwarden Settings and Azure SAML Configuration

In your Bitwarden instance, navigate to your organization's Settings → Single sign-on screen.



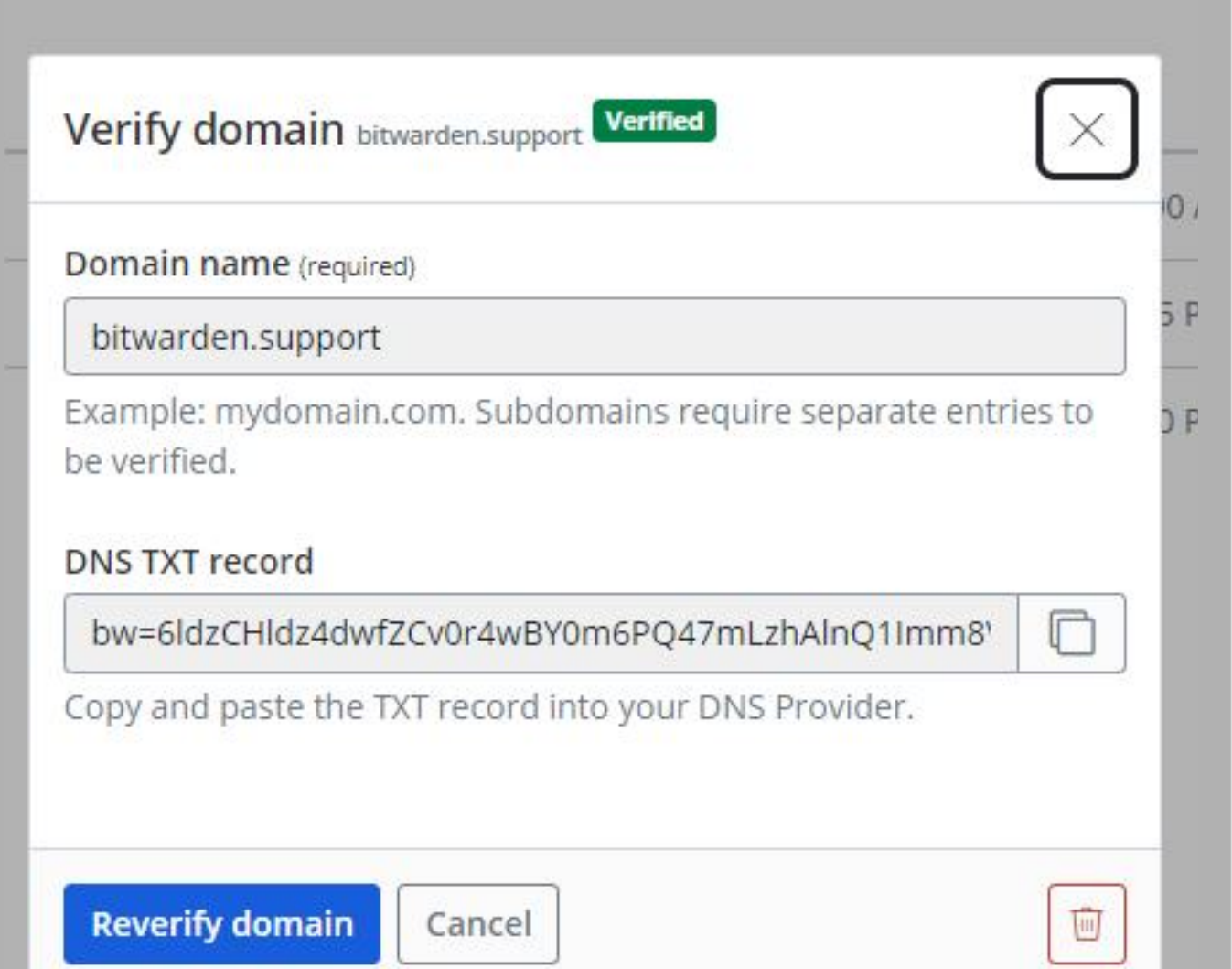
On Azure → Edit Basic SAML Configuration.



## 4 Verify Domain

Once bitwarden's ownership is verified, @bitwarden.support accounts will be able to bypass SSO ID step during login.

### Domain verification



## 5 SCIM Provisioning

Accept requests from your identity provider (IdP) for user and group provisioning and de-provisioning.

