

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

With Trusted Devices Encryption and Domain Verification

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

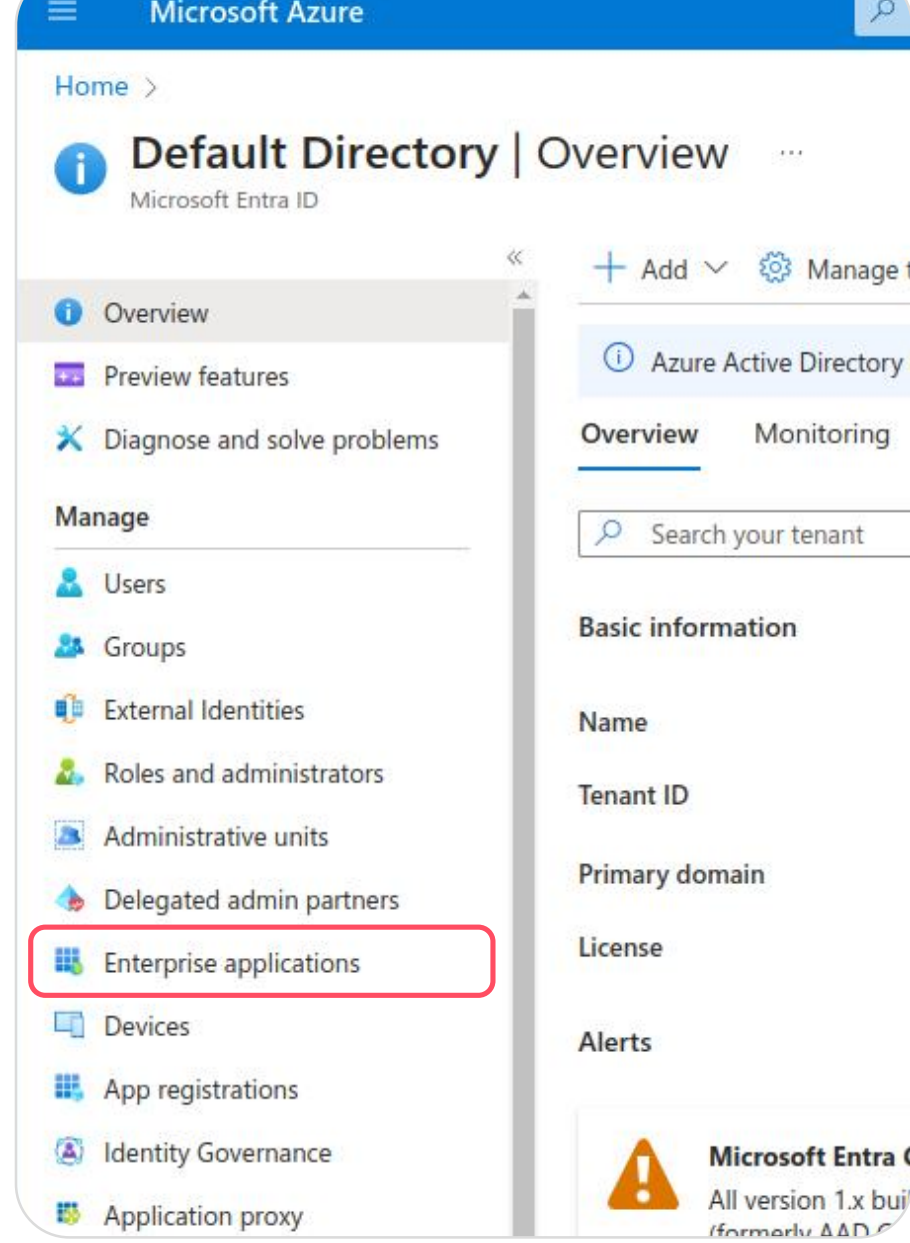
Links:

<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/>

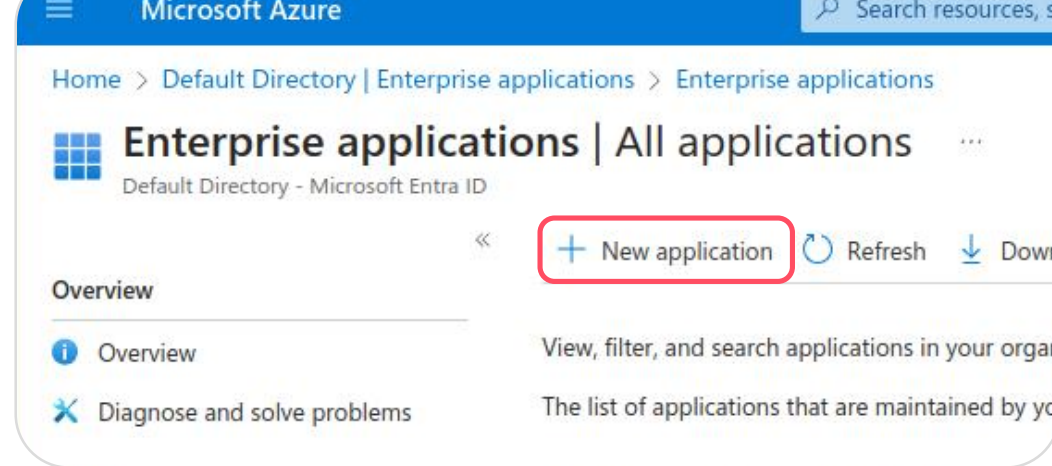
1 Create Enterprise Application

Azure Portal: go to Microsoft Entra ID

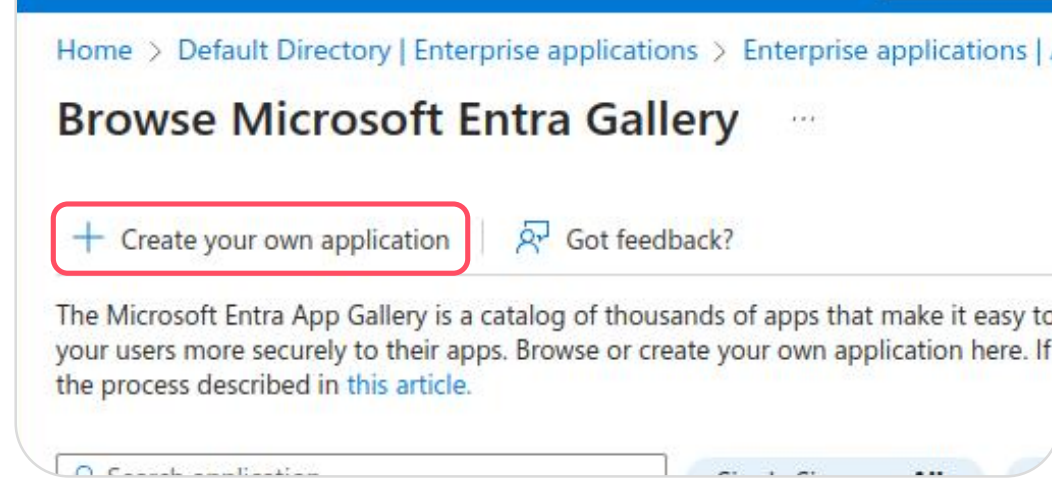
1.1 Select Enterprise applications:



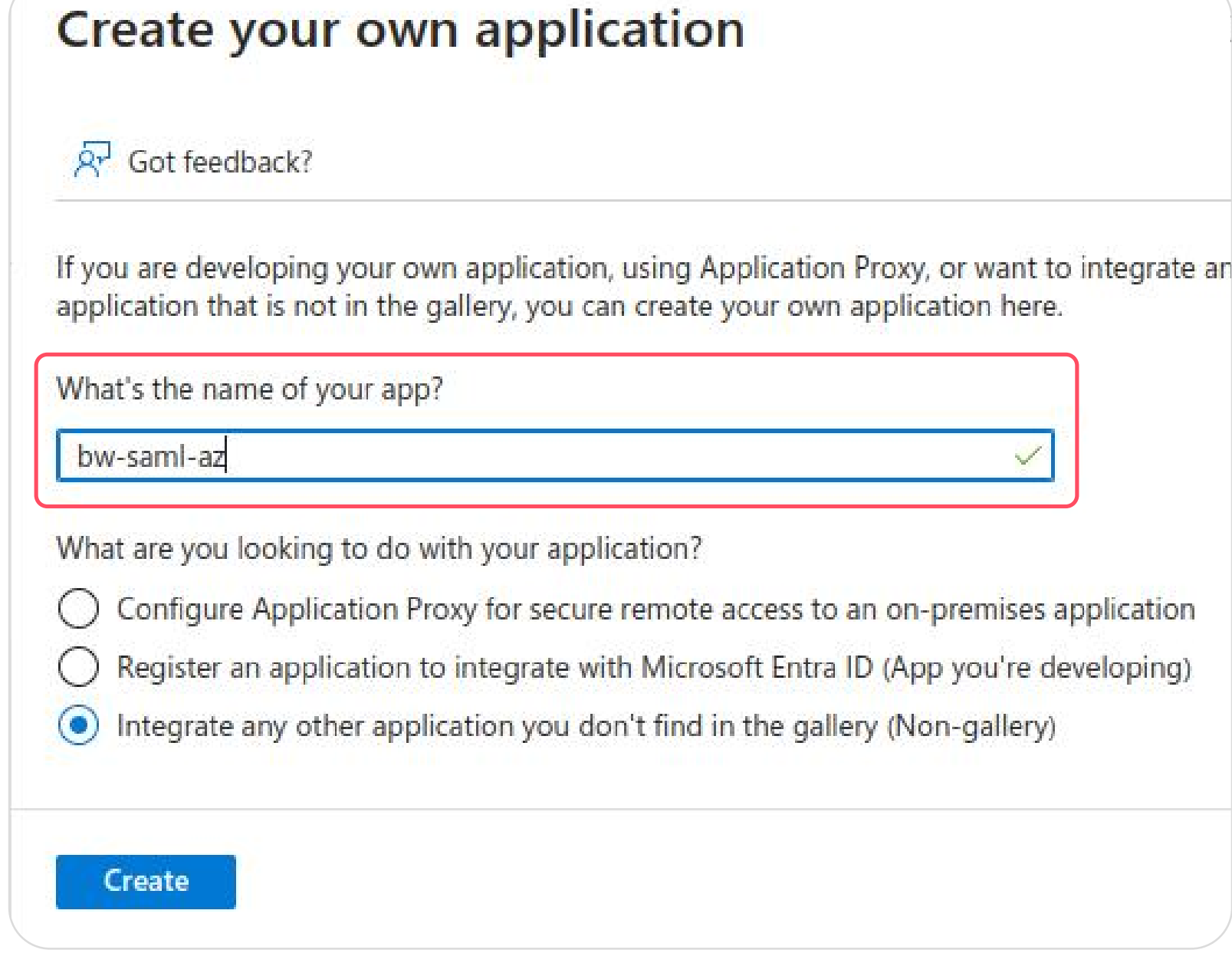
1.2 Select the New application button:



1.3 Click Create your own application:



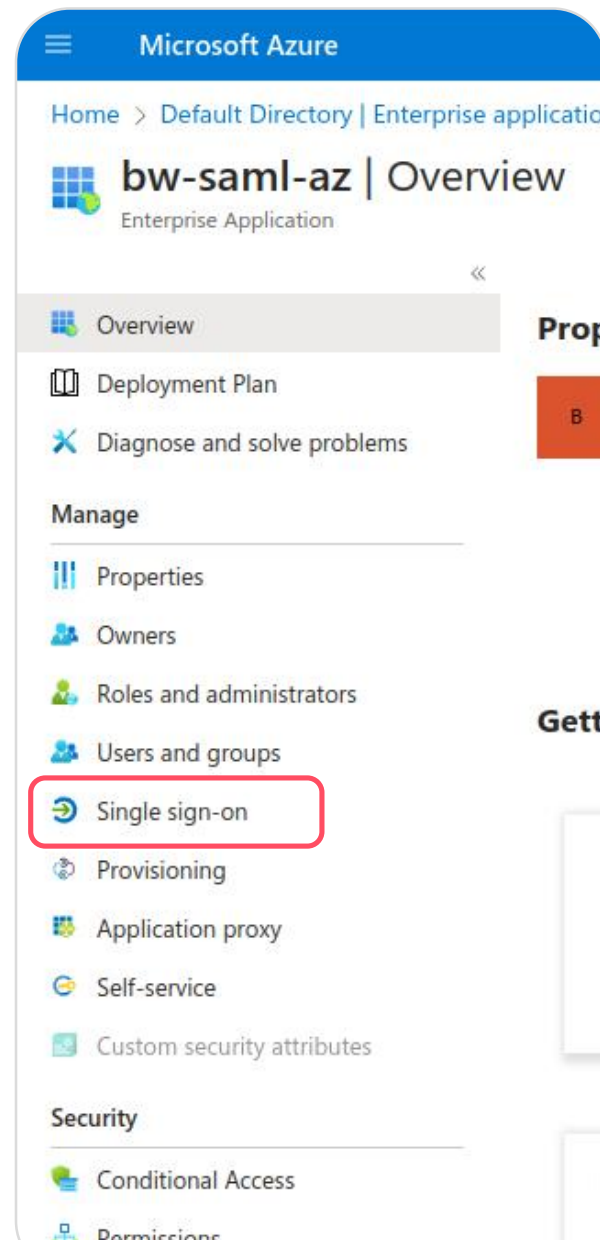
1.4 Give this application a unique name:



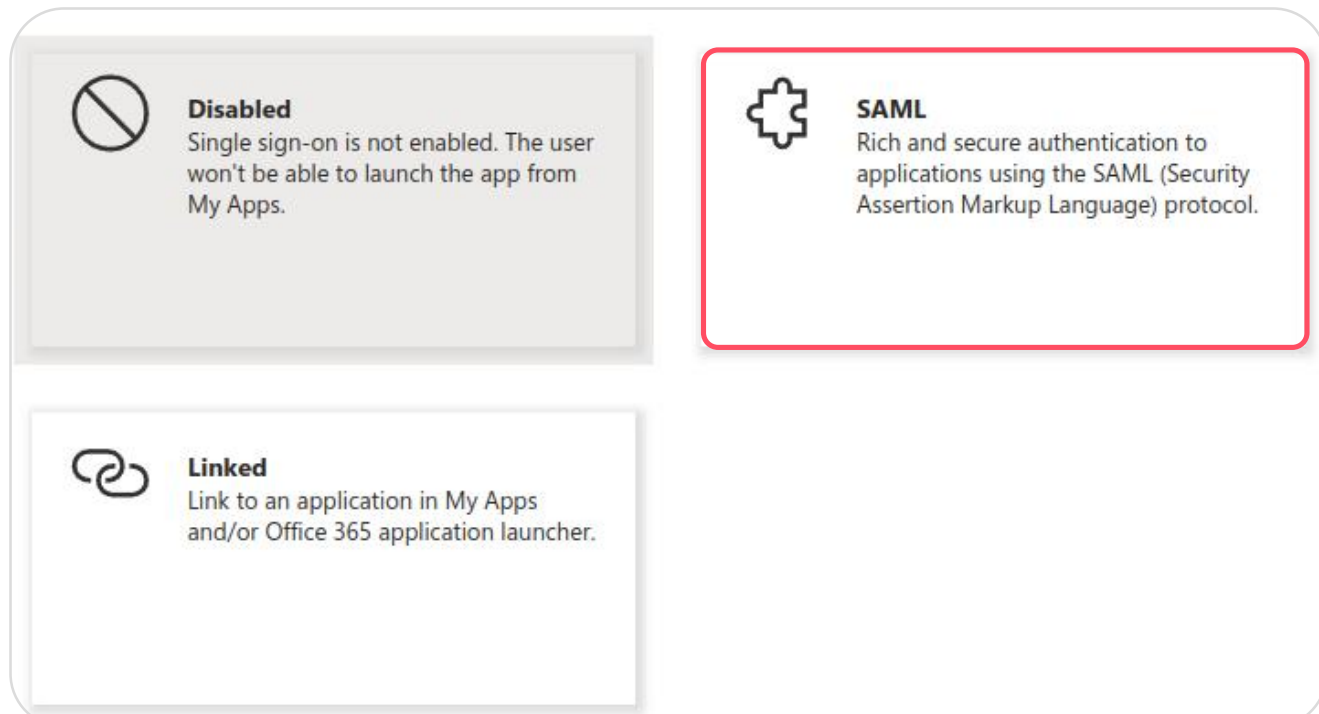
2 Enable Sign-On

Prepare your AZ app to

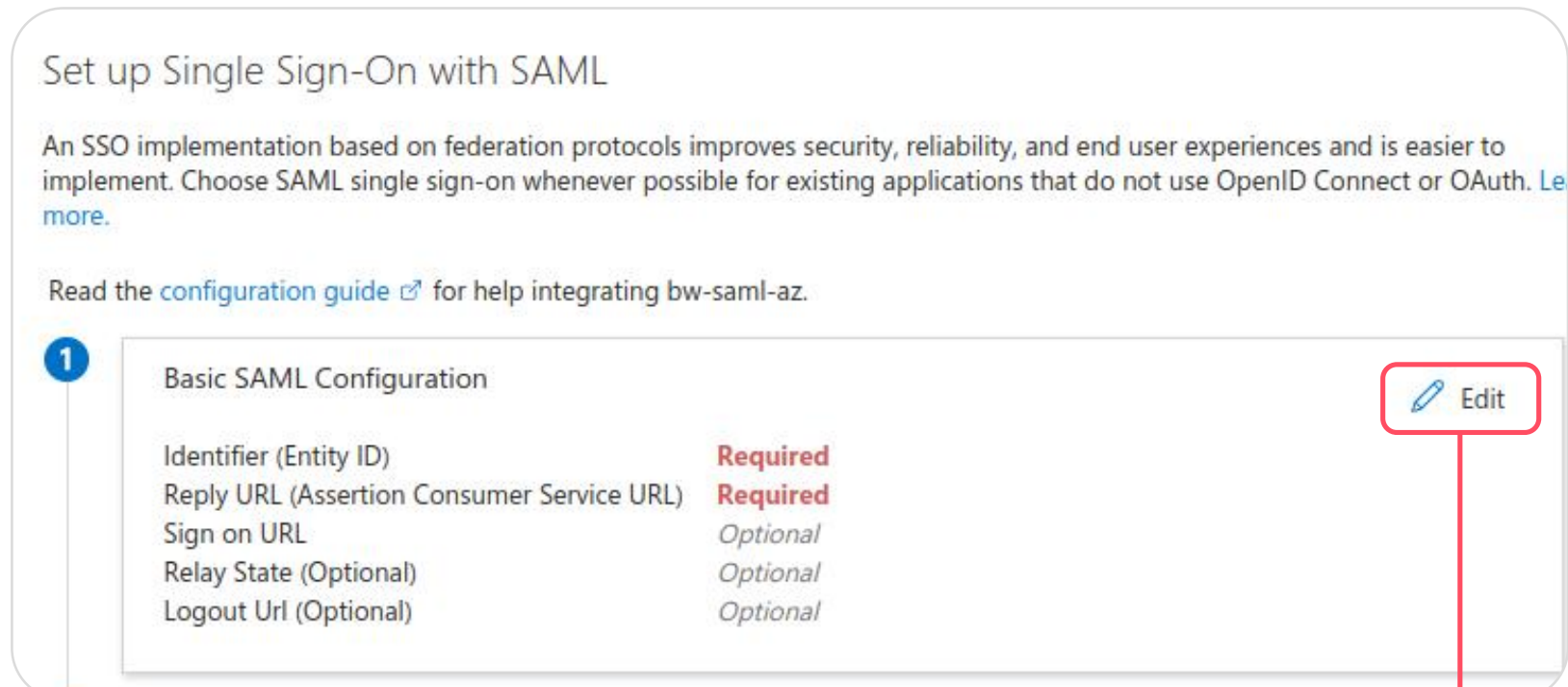
2.1 Click Single sign-on:



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

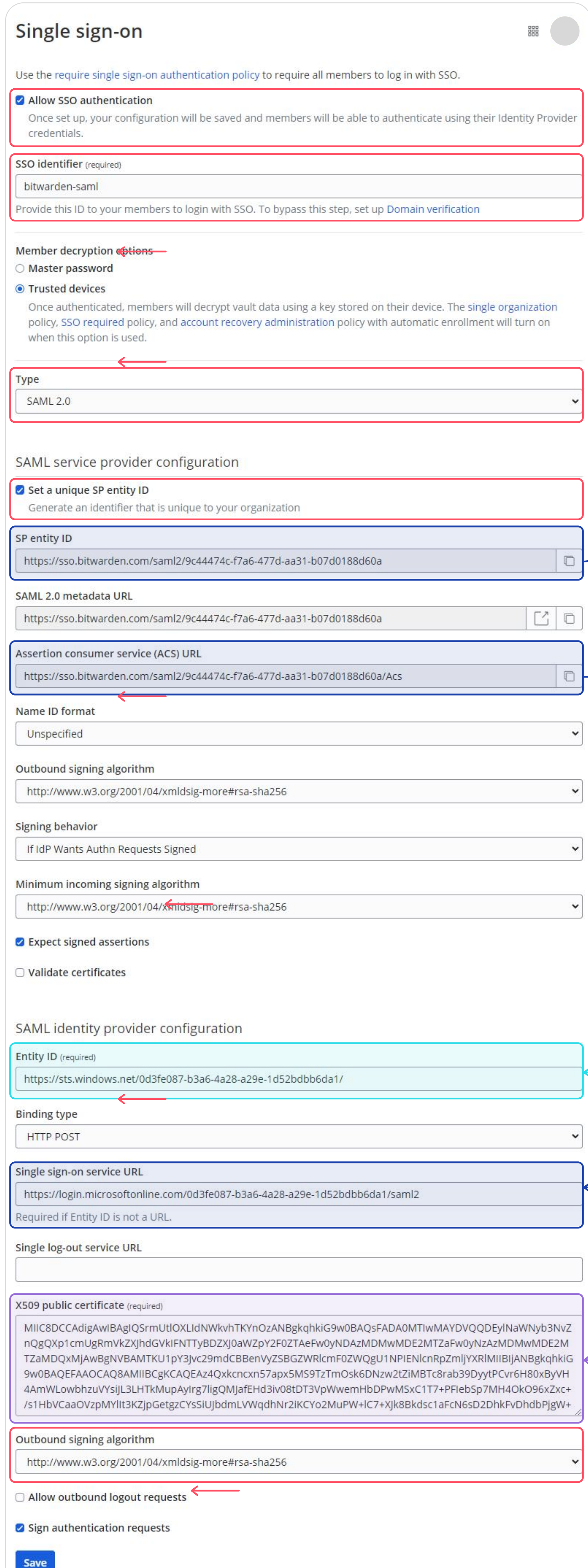


2.3 Click on Edit to edit Basic SAML Configuration:

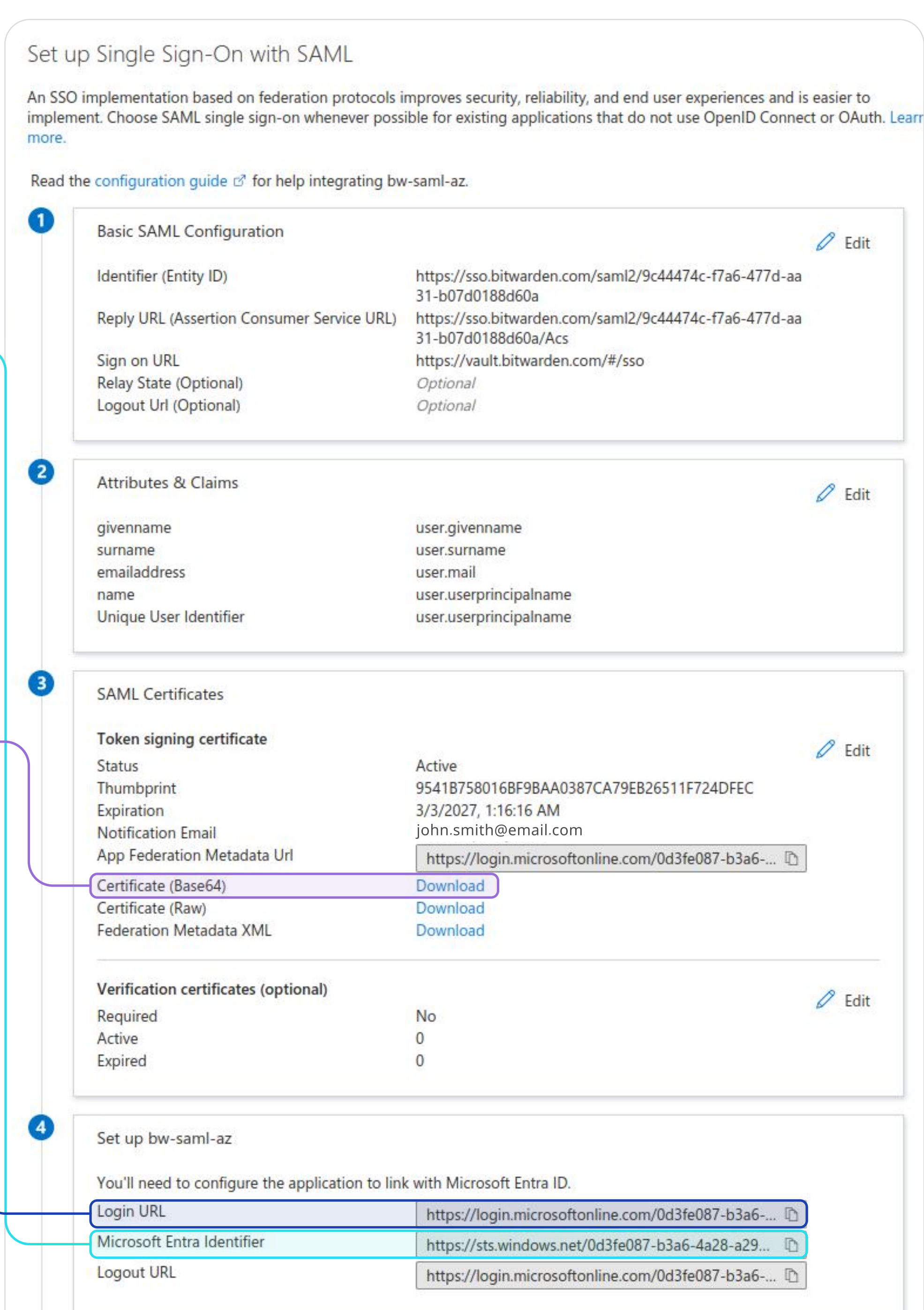
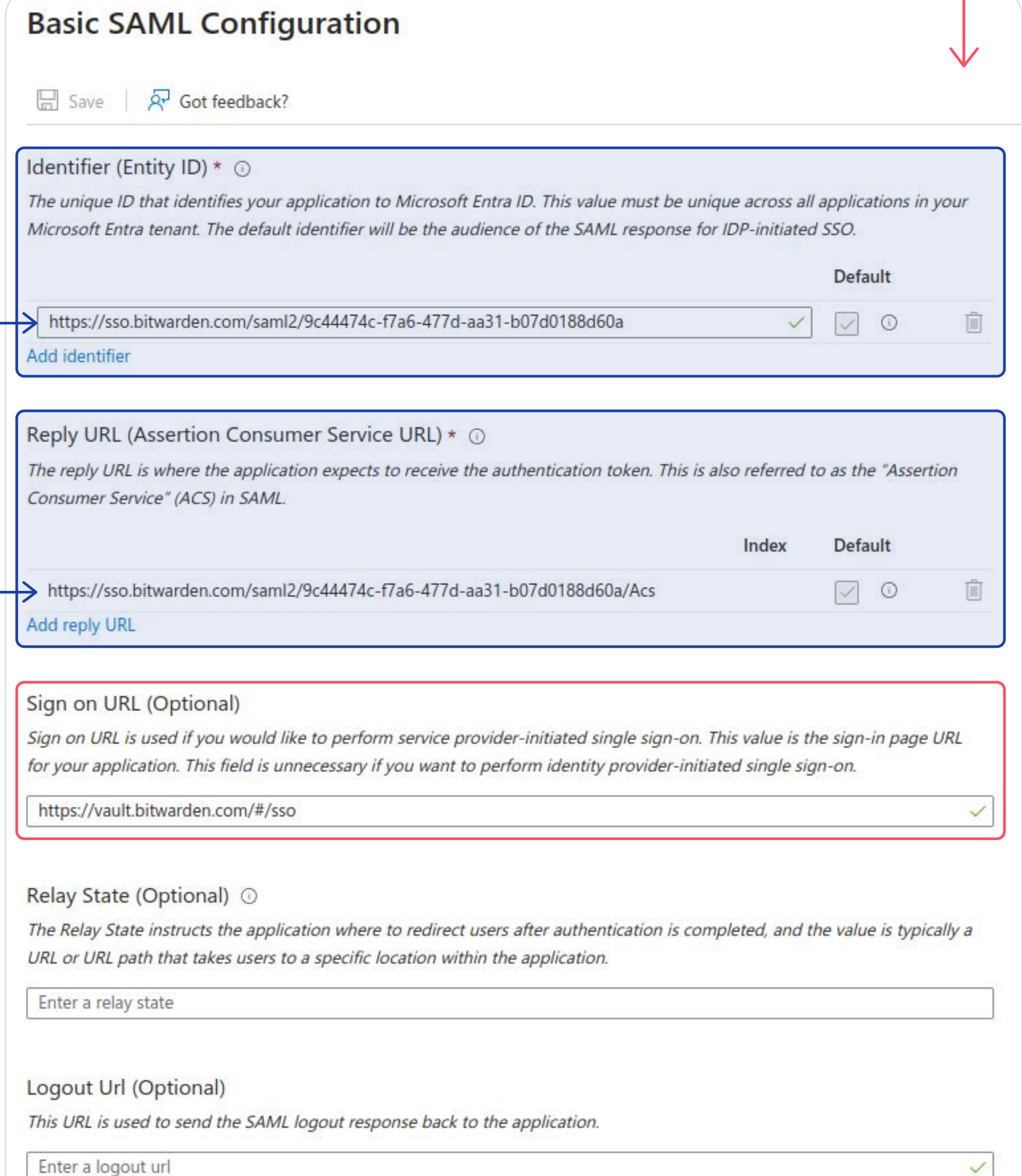


3 Configure Bitwarden Settings and Azure SAML Configuration

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



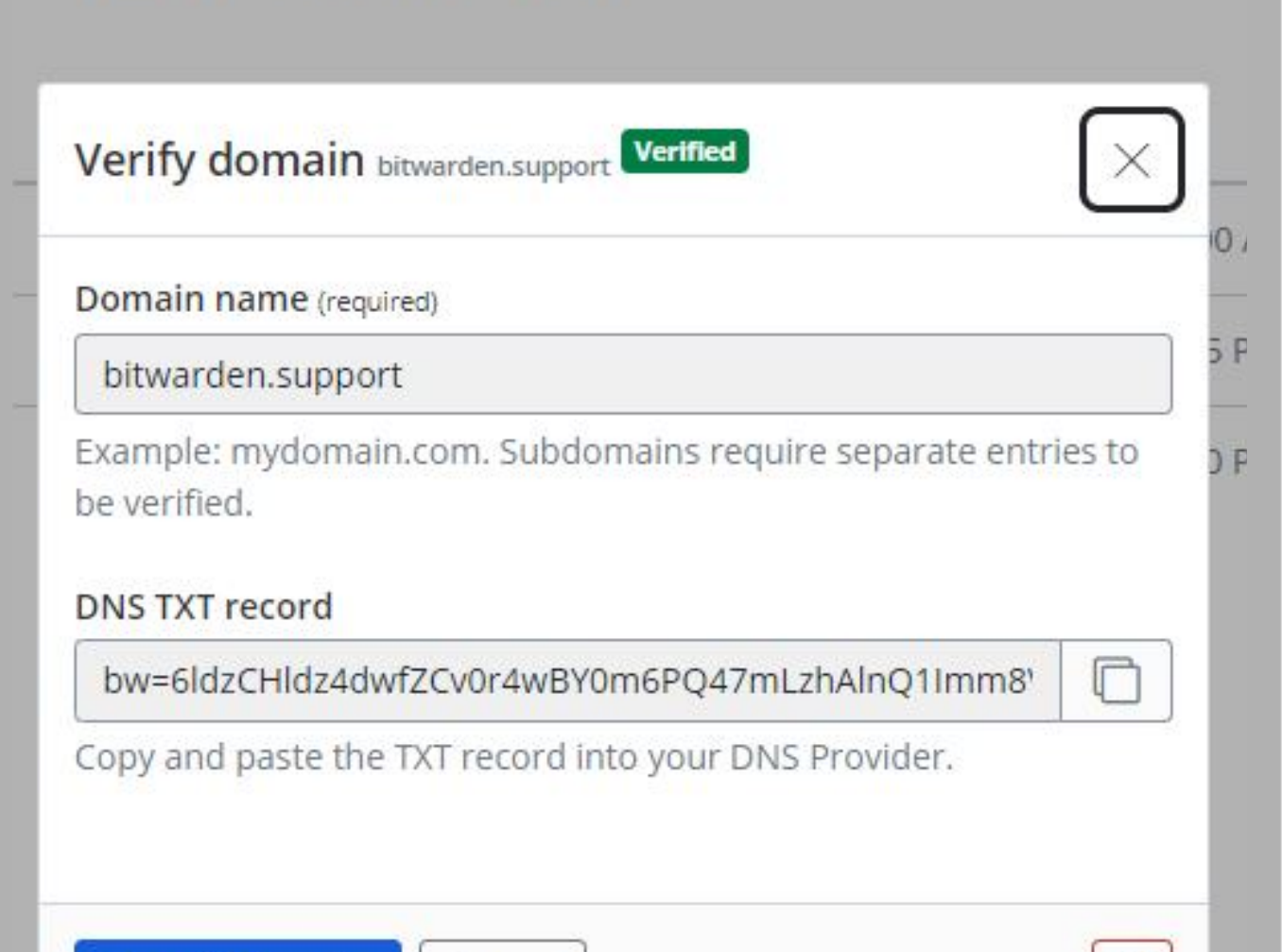
On Azure → Edit Basic SAML Configuration.



4 Verify Domain

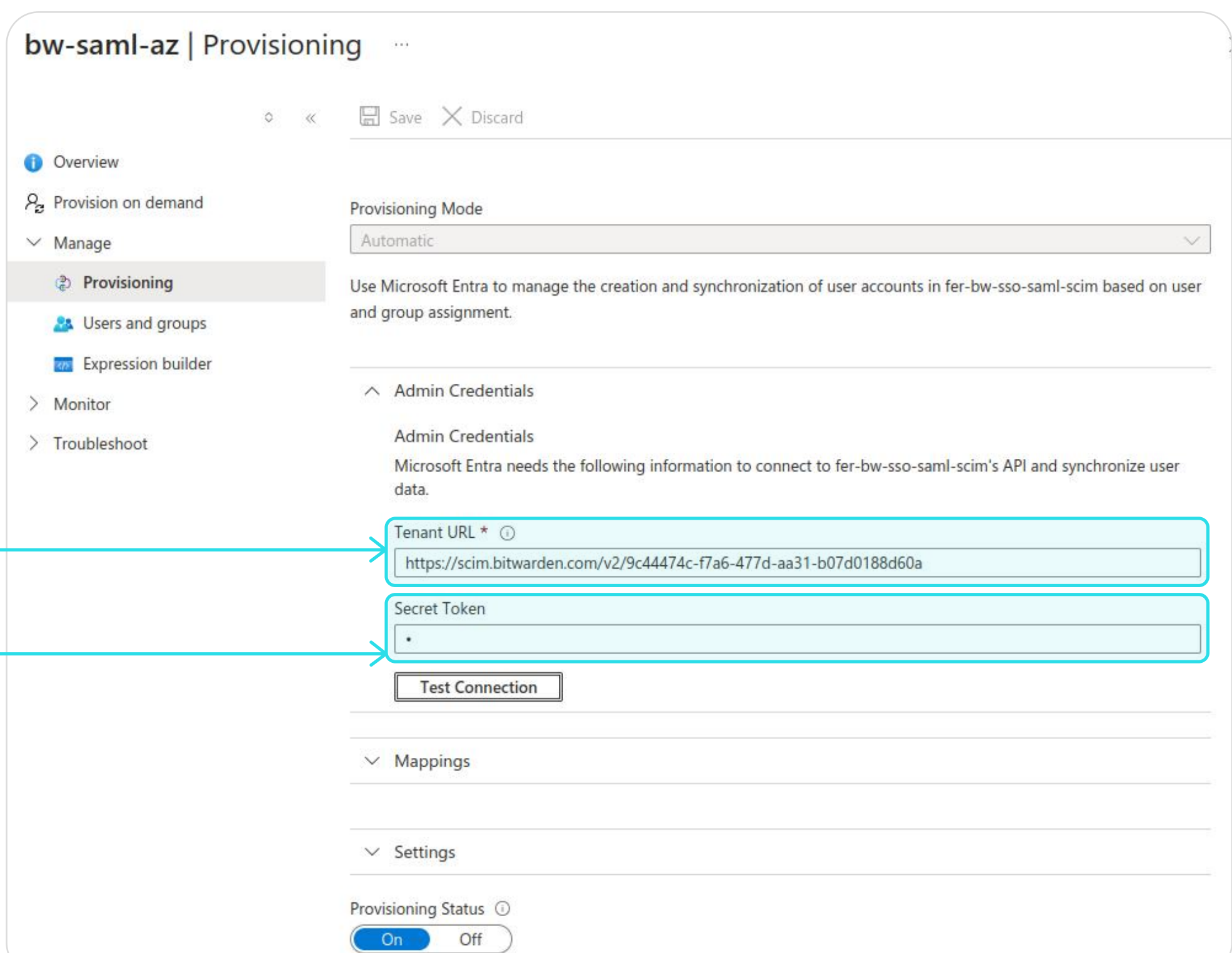
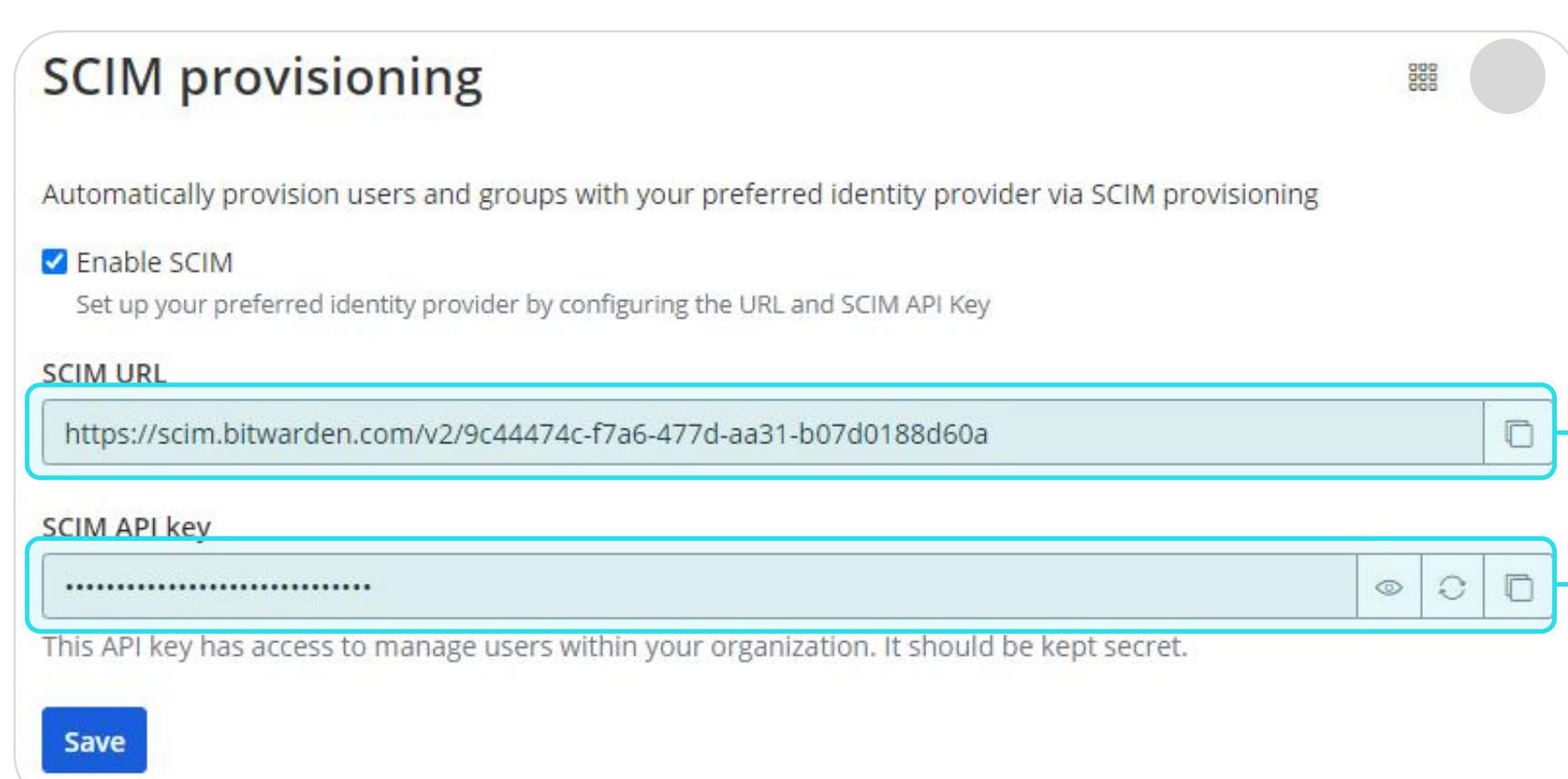
Once bitwarden's ownership is verified, @bitwarden.support accounts will be able to bypass SSO ID step during login.

Domain verification



5 SCIM Provisioning

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



With Trusted Devices Encryption and Domain Verification

Azure Portal: go to Microsoft Entra ID

1.4 Give this application a unique name:

Home > Default Directory | Enterprise applications > Enterprise applications |

Browse Microsoft Entra Gallery

+ Create your own application Get feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to... your users more securely to their apps. Browse or create your own application here. If... the process described in [this article](#).

Find an app or service

Create your own application

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?



What are you looking to do with your application?

- ☐ Configure Application Proxy for secure remote access to an on-premises application
- ☐ Register an application to integrate with Microsoft Entra ID (App you're developing)
- ☒ Integrate another application you don't find in the gallery (Non-gallery)

Create

Enable sign

2.3 Click on Edit to edit Basic SAML Configuration:

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 bw-saml-az.

1

Basic SAML Configuration	
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

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

On Azure → Edit Basic SAML Configuration.

Basic SAML Configuration

Save

Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://sso.bitwarden.com/saml2/9c44474c-f7a6-477d-aa31-b07d0188d60a

Add identifier

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index

Default

https://sso.bitwarden.com/saml2/9c44474c-f7a6-477d-aa31-b07d0188d60a/Acs

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

https://vault.bitwarden.com/#/sso

Relay State (Optional)

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url

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 bw-saml-az.

- ### Basic SAML Configuration

Identifier (Entity ID)	https://sso.bitwarden.com/saml2/9c44474c-f7a6-477d-aa31-b07d0188d60a
Reply URL (Assertion Consumer Service URL)	https://sso.bitwarden.com/saml2/9c44474c-f7a6-477d-aa31-b07d0188d60a/Acs
Sign on URL	https://vault.bitwarden.com/#/sso
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- ### Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- ### SAML Certificates

Token signing certificate

Status	Active
Thumbprint	954187580168F9BAA0387CA79EB26511F724DFEC
Expiration	3/3/2027, 1:16:16 AM
Notification Email	john.smith@gmail.com
App Federation Metadata Url	https://login.microsoftonline.com/0d3fe087-b3a6-...

Certificate (Base64) [Download](#)

Certificate (Raw) [Download](#)

Federation Metadata XML [Download](#)

Verification certificates (optional)

Required	No
Active	0
Expired	0
- ### Set up bw-saml-az

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com/0d3fe087-b3a6-...
Microsoft Entra Identifier	https://sts.windows.net/0d3fe087-b3a6-4a28-a29-...
Logout URL	https://login.microsoftonline.com/0d3fe087-b3a6-...

Verify Domain

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

A screenshot of a web browser showing a modal window for domain verification. The modal has a title "Verify domain" and a status "Verified" in a green box. Below the title is a text input field containing "bitwarden.support". Underneath the input field is a paragraph of text: "Example: mydomain.com. Subdomains require separate entries to be verified." Below this text is a section titled "DNS TXT record" with a text input field containing the record value "bw=6ldzCHldz4dwfZCv0r4wBY0m6PQ47mLzhAlnQ11mm8". To the right of the input field is a copy icon. Below the input field is a paragraph of text: "Copy and paste the TXT record into your DNS Provider." At the bottom of the modal are two buttons: "Reverify domain" and "Cancel". The modal is set against a blurred background of a web page.

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

bw-saml-az | Provisioning

Overview

Provision on demand

Manage

Provisioning

Users and groups

Expression builder

Monitor

Troubleshoot

Save

Discard

Provisioning Mode

Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in fer-bw-ssso-saml-scim based on user and group assignment.

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to fer-bw-ssso-saml-scim's API and synchronize user data.

Tenant URL *

https://scim.bitwarden.com/v2/9c44474c-f7a6-477d-aa31-b07d0188d60a

Secret Token

*

Test Connection

Mappings

Settings

Provisioning Status

On Off