bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO >

Okta SAML Implementation

View in the help center:
https://bitwarden.com/help/saml-okta/

Okta SAML Implementation

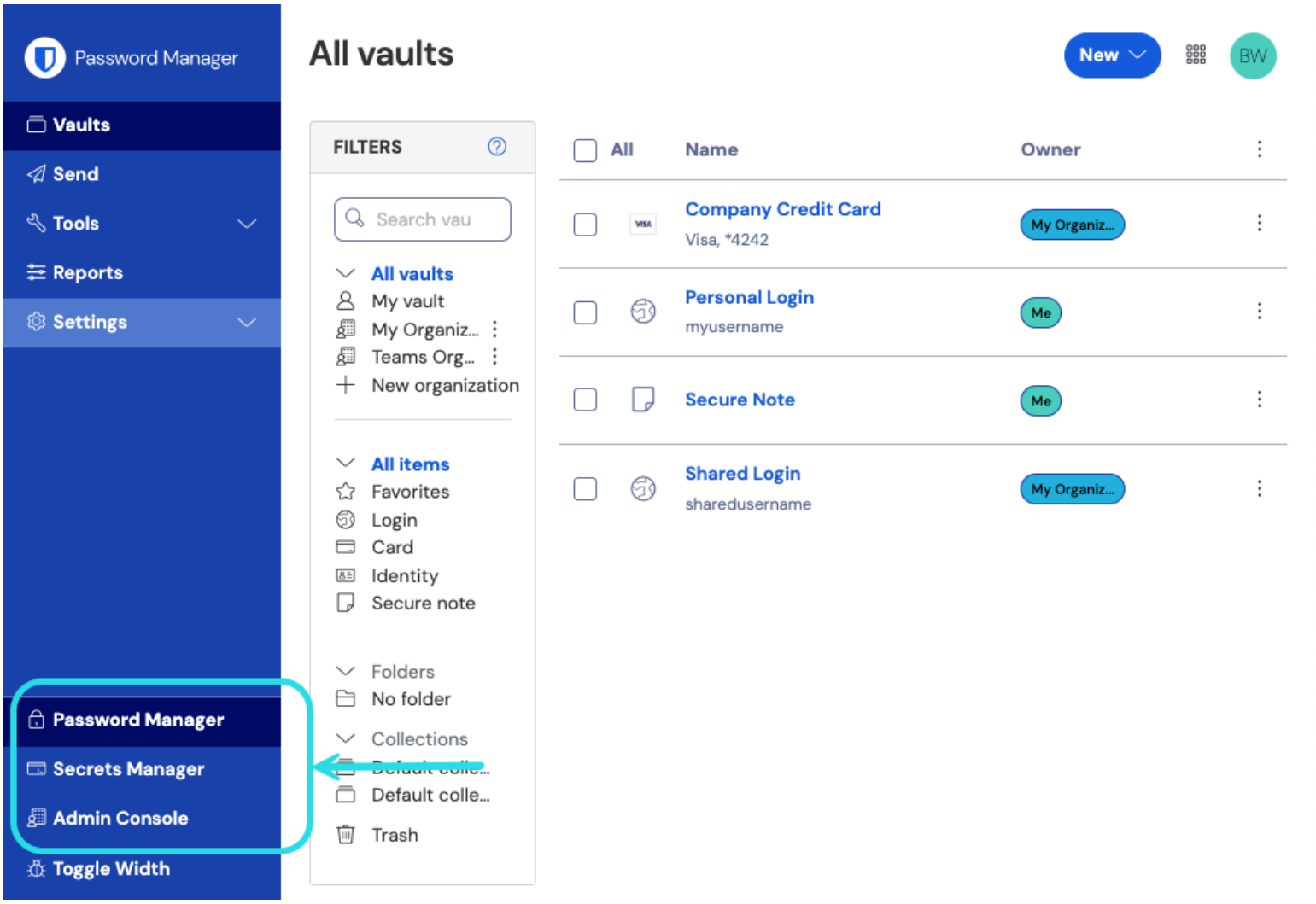
This article contains **Okta-specific** help for configuring Login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

Configuration involves working simultaneously within the Bitwarden web app and the Okta Admin Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

> **Tip**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

Open SSO in the web app

Log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

Open your organization's **Settings** → **Single sign-on** screen:

SAML 2.0 configuration

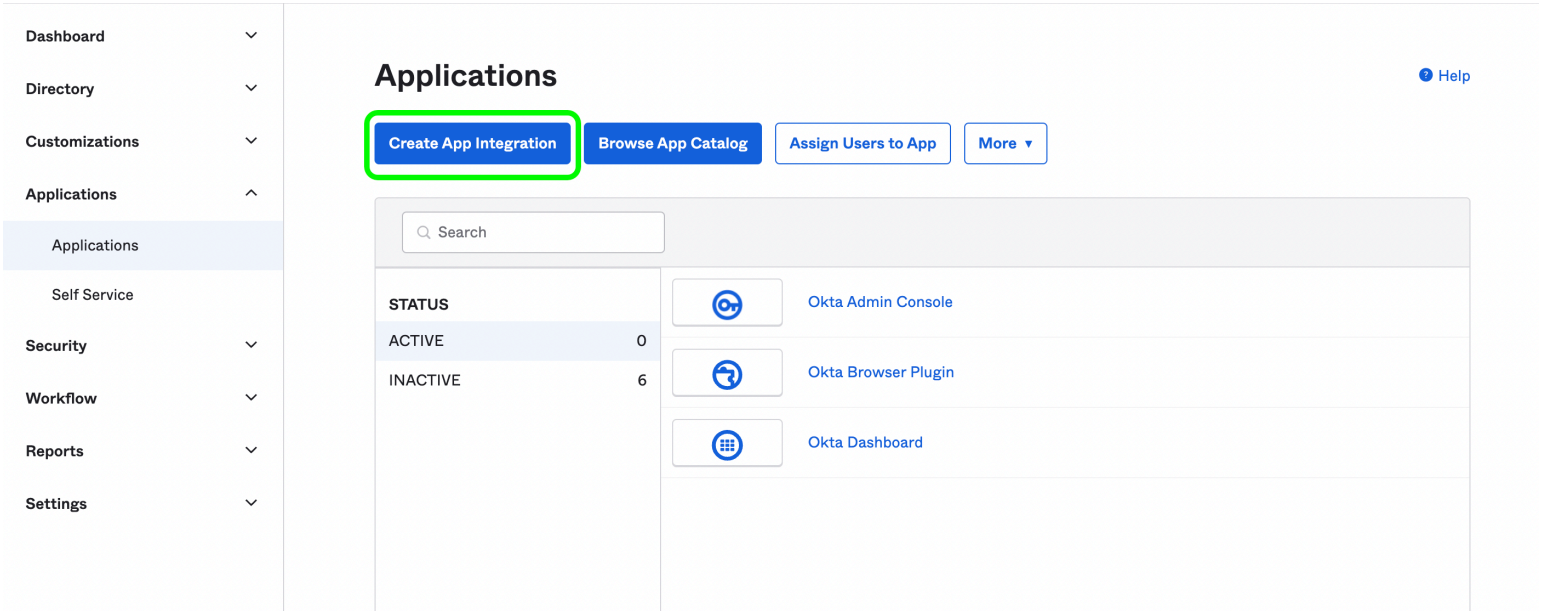
If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.

> **Tip**
>
> There are alternative **Member decryption options**. Learn how to get started using SSO with trusted devices or Key Connector.

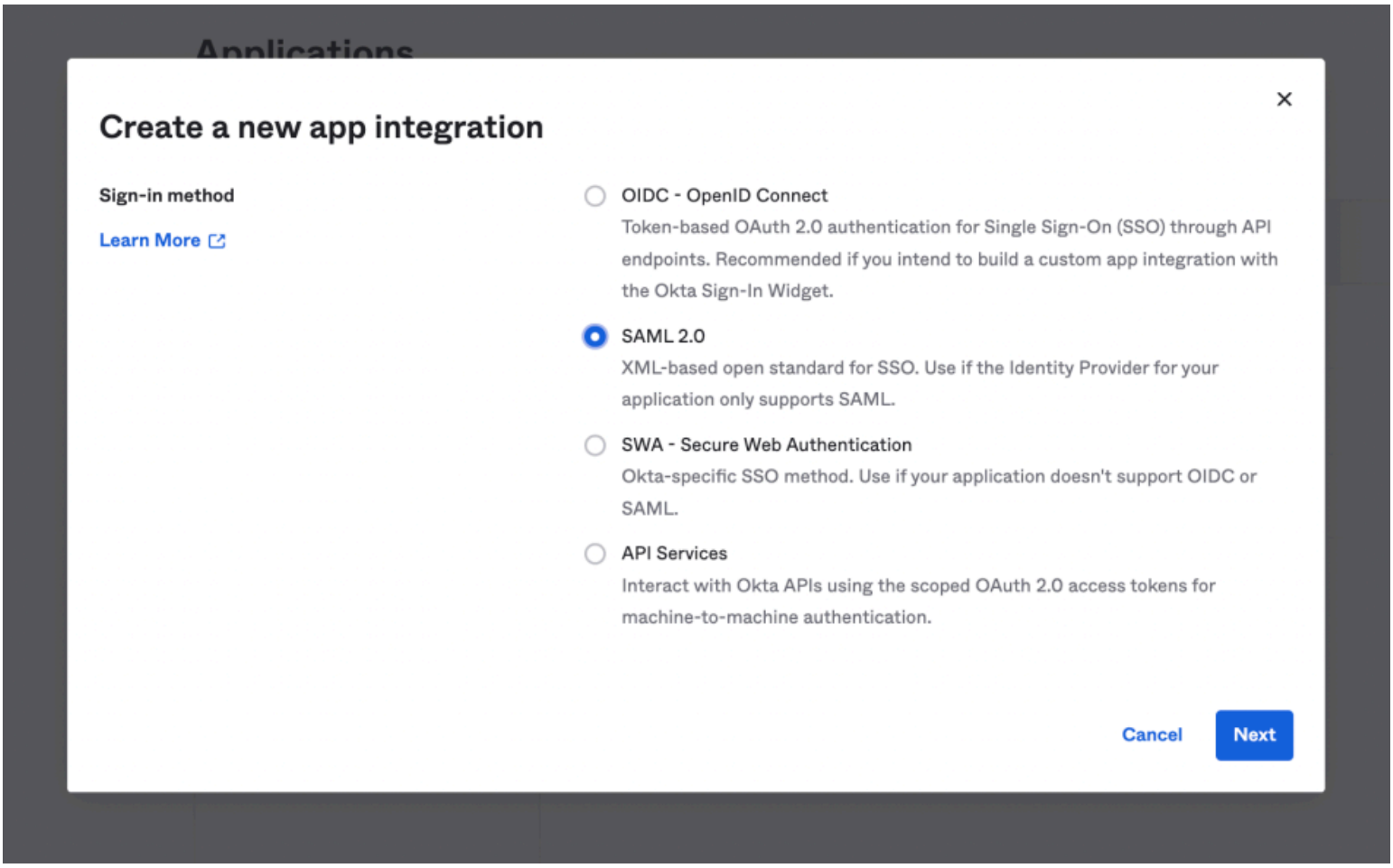
Create an Okta application

In the Okta Admin Portal, select **Applications → Applications** from the navigation. On the Applications screen, select the **Create App Integration** button:



Okta create app integration

In the Create a New Application Integration dialog, select the **SAML 2.0** radio button:



SAML 2.0 radio button

Select the **Next** button to proceed to configuration.

General settings

On the **General Settings** screen, give the application a unique, Bitwarden-specific name and select **Next**.

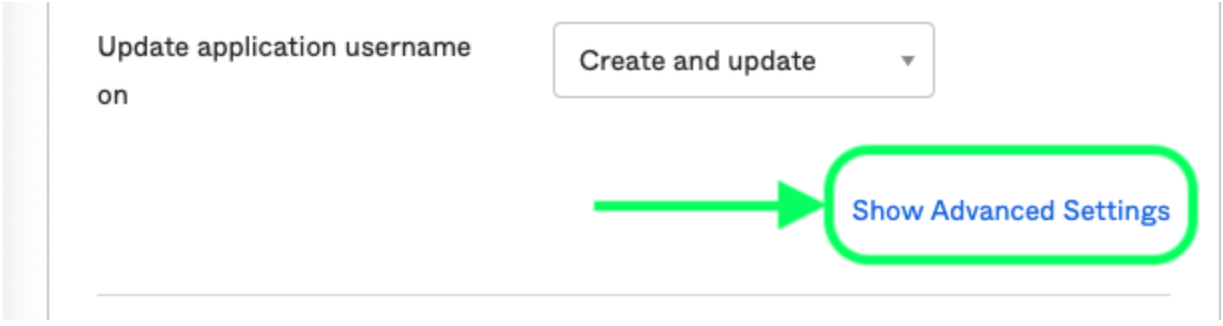
Configure SAML

On the **Configure SAML** screen, configure the following fields:

Field	Description
Single sign on URL	Set this field to the pre-generated **Assertion Consumer Service (ACS) URL**. This automatically-generated value can be copied from the organization's **Settings** → **Single sign-on** screen and will vary based on your setup.
Audience URI (SP Entity ID)	Set this field to the pre-generated **SP Entity ID**. This automatically-generated value can be copied from the organization's **Settings** → **Single sign-on** screen and will vary based on your setup.
Name ID format	Select the SAML NameID format to use in SAML assertions. By default, **Unspecified**.
Application username	Select the Okta attribute users will use to login to Bitwarden, typically **Email**.

Advanced settings

Select the **Show Advanced Settings** link and configure the following fields:

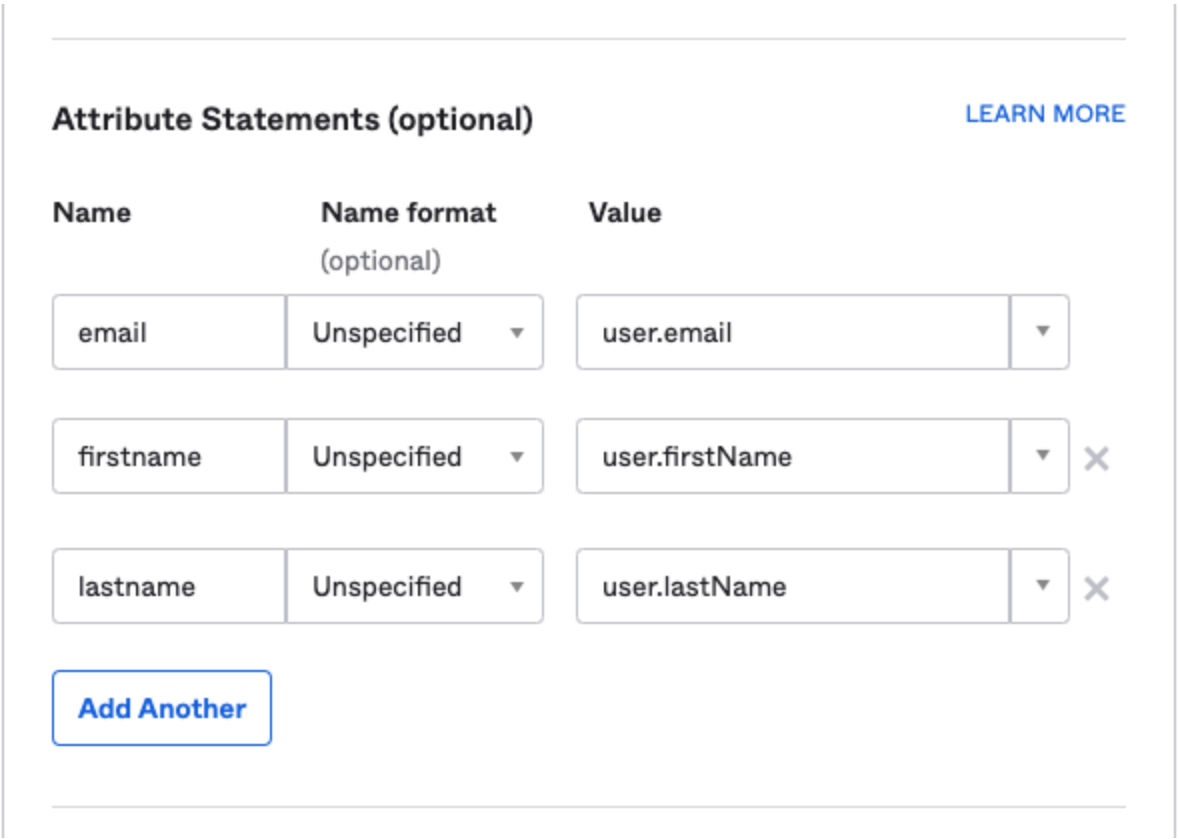


Advanced Settings

Field	Description
Response	Whether the SAML response is signed by Okta.
Assertion Signature	Whether the SAML assertion is signed by Okta.
Signature Algorithm	The signing algorithm used to sign the response and/or assertion, depending on which is set to **Signed**. By default, `rsa-sha256`.
Digest Algorithm	The digest algorithm used to sign the response and/or assertion, depending on which is set to **Signed**. This field must match the selected **Signature Algorithm**.

Attribute statements

In the **Attribute Statements** section, construct the following SP → IdP attribute mappings:

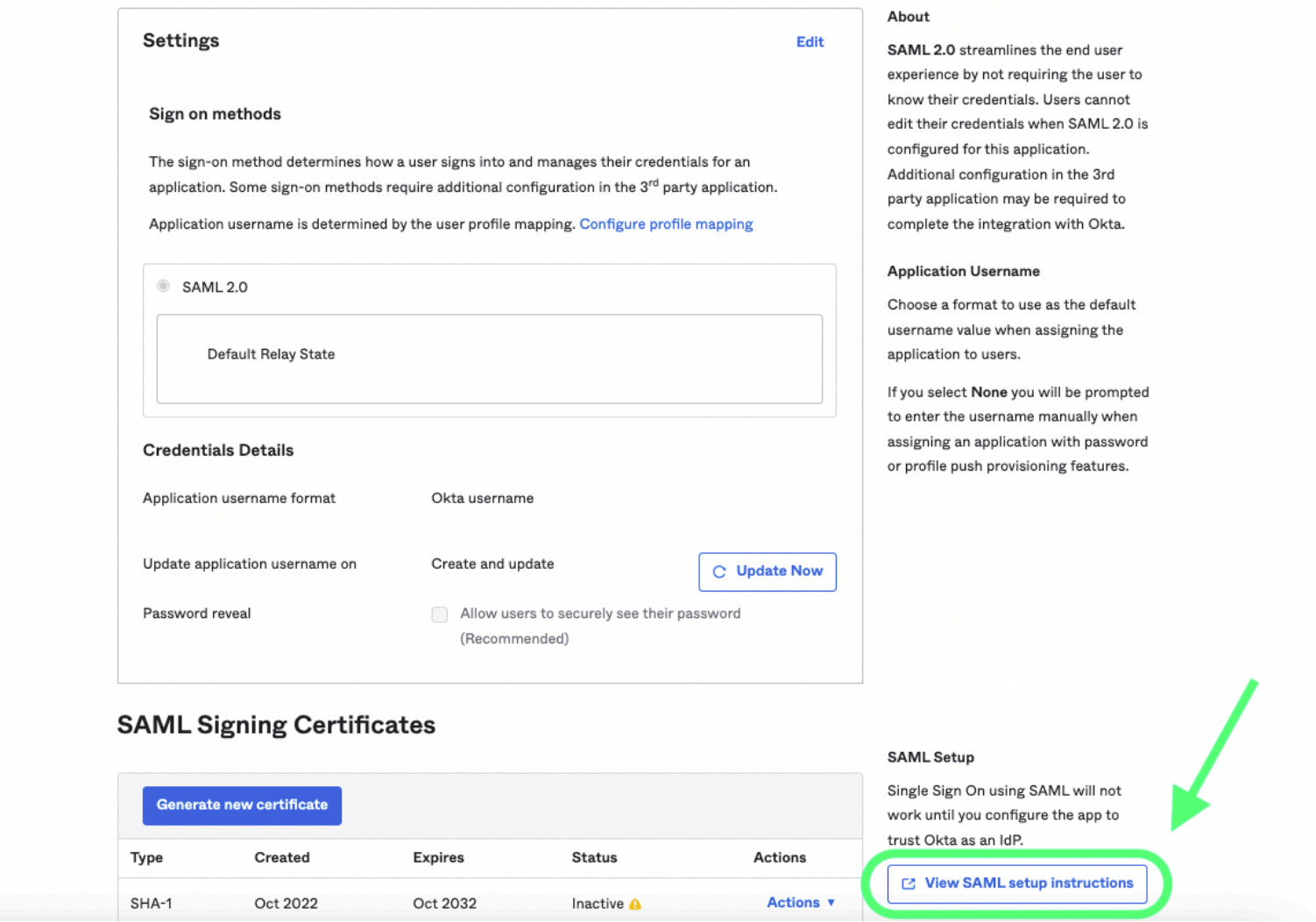


Attribute Statements

Once configured, select the **Next** button to proceed to the **Feedback** screen and select **Finish**.

Get IdP values

Once your application is created, select the **Sign On** tab for the app and select the **View Setup Instructions** button located on the right side of the screen:



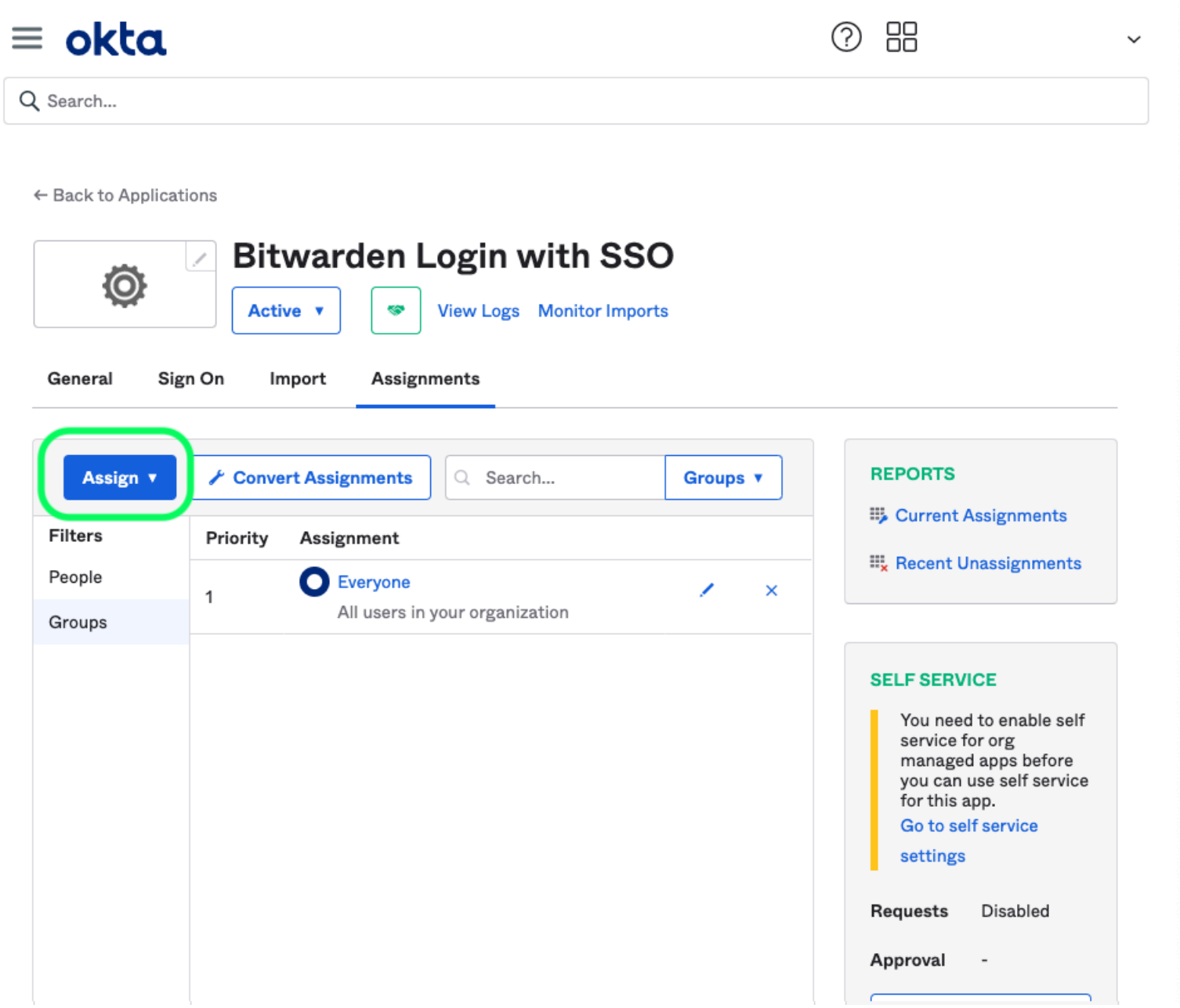
View SAML setup instructions

Either leave this page up for future use, or copy the **Identity Provider Single Sign-On URL** and **Identity Provider Issuer** and download the **X.509 Certificate**:

IdP Values

Assignments

Navigate to the **Assignments** tab and select the **Assign** button:



Assigning Groups

You can assign access to the application on a user-by-user basis using the **Assign to People** option, or in-bulk using the **Assign to Groups** option.

Back to the web app

At this point, you have configured everything you need within the context of the Okta Admin Portal. Return to the Bitwarden web app to complete configuration.

The Single sign-on screen separates configuration into two sections:

- **SAML service provider configuration** will determine the format of SAML requests.
- **SAML identity provider configuration** will determine the format to expect for SAML responses.

Service provider configuration

Configure the following fields according to the choices selected in the Okta Admin Portal during app creation:

Field	Description
Name ID format	Set this to whatever the Name ID format specified in Okta, otherwise leave **Unspecified**.
Outbound signing algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing behavior	Whether/when SAML requests will be signed.
Minimum incoming signing algorithm	Set this to the Signature Algorithm specified in Okta.
Expect signed assertions	Check this box if you set the Assertion Signature field to **Signed** in Okta.
Validate certificates	Check this box when using trusted and valid certificates from your IdP through a trusted CA. Self-signed certificates may fail unless proper trust chains are configure within the Bitwarden login with SSO docker image.

When you're done with the service provider configuration, **Save** your work.

Identity provider configuration

Identity provider configuration will often require you to refer back to the Okta Admin Portal to retrieve application values:

Field	Description
Entity ID	Enter your **Identity Provider Issuer**, retrieved from the Okta Sign On Settings screen by selecting the **View Setup Instructions** button. This field is case sensitive.
Binding Type	Set to **Redirect**. Okta currently does not support HTTP POST.

Field	Description
Single Sign On Service URL	Enter your **Identity Provider Single Sign-On URL**, retrieved from the Okta Sign On Settings screen.
Single Log Out Service URL	Login with SSO currently **does not** support SLO. This option is planned for future development, however you may pre-configure it if you wish.

X509 Public Certificate	Paste the downloaded certificate, removing
	`-----BEGIN CERTIFICATE-----`
	and
	`-----END CERTIFICATE-----`
	The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters **will cause certification validation to fail**.

Outbound Signing Algorithm	Select the Signature Algorithm selected during Okta app configuration. If you didn't change the Signature Algorithm, leave the default (`rsa-sha256`).
Allow outbound logout requests	Login with SSO currently **does not** support SLO.
Want Authentication Requests Signed	Whether Okta expects SAML requests to be signed.

Note

When completing the X509 certificate, take note of the expiration date. Certificates will have to be renewed in order to prevent any disruptions in service to SSO end users. If a certificate has expired, Admin and Owner accounts will always be able to log in with email address and master password.

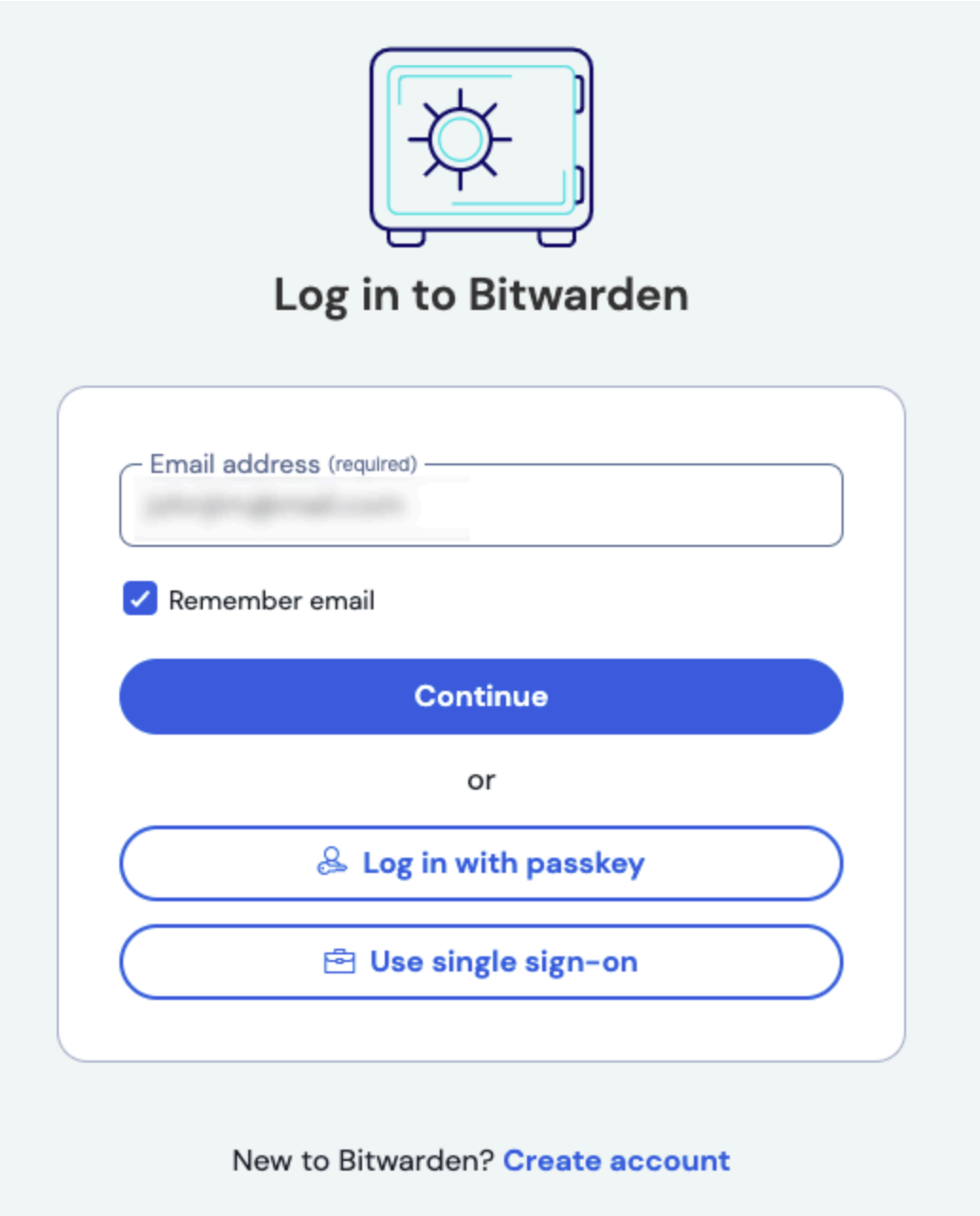
When you're done with the identity provider configuration, **Save** your work.

Tip

You can require users to log in with SSO by activating the single sign-on authentication policy. Please note, this will require activating the single organization policy as well. Learn more.

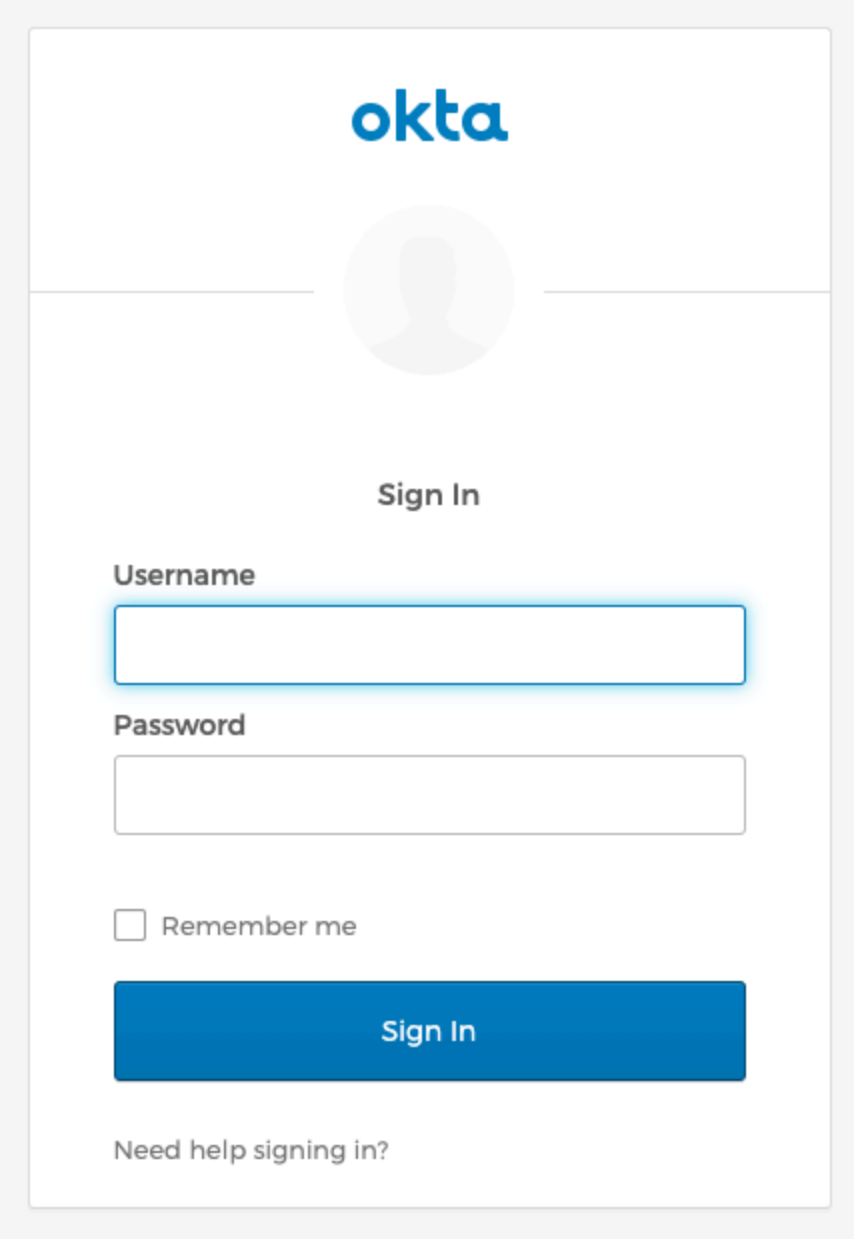
Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address and selecting the **Enterprise Single-On** button:



Log in options screen

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will be redirected to the Okta login screen:



Log in with Okta

After you authenticate with your Okta credentials, enter your Bitwarden master password to decrypt your vault!

Note

Bitwarden does not support unsolicited responses, so initiating login from your IdP will result in an error. The SSO login flow must be initiated from Bitwarden. Okta administrators can create an Okta Bookmark App that will link directly to the Bitwarden web vault login page.

1. As an admin, navigate to the **Applications** drop down located on the main navigation bar and select **Applications**.
2. Click **Browse App Catalog**.
3. Search for **Bookmark App** and click **Add Integration**.
4. Add the following settings to the application:
    1. Give the application a name such as **Bitwarden Login**.
    2. In the **URL** field, provide the URL to your Bitwarden client such as `https://vault.bitwarden.com/#/login` or `your-self-hostedURL.com`.
5. Select **Done** and return to the applications dashboard and edit the newly created app.
6. Assign people and groups to the application. You may also assign a logo to the application for end user recognition. The Bitwarden logo can be obtained here.

Once this process has been completed, assigned people and groups will have a Bitwarden bookmark application on their Okta dashboard that will link them directly to the Bitwarden web vault login page.