

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.

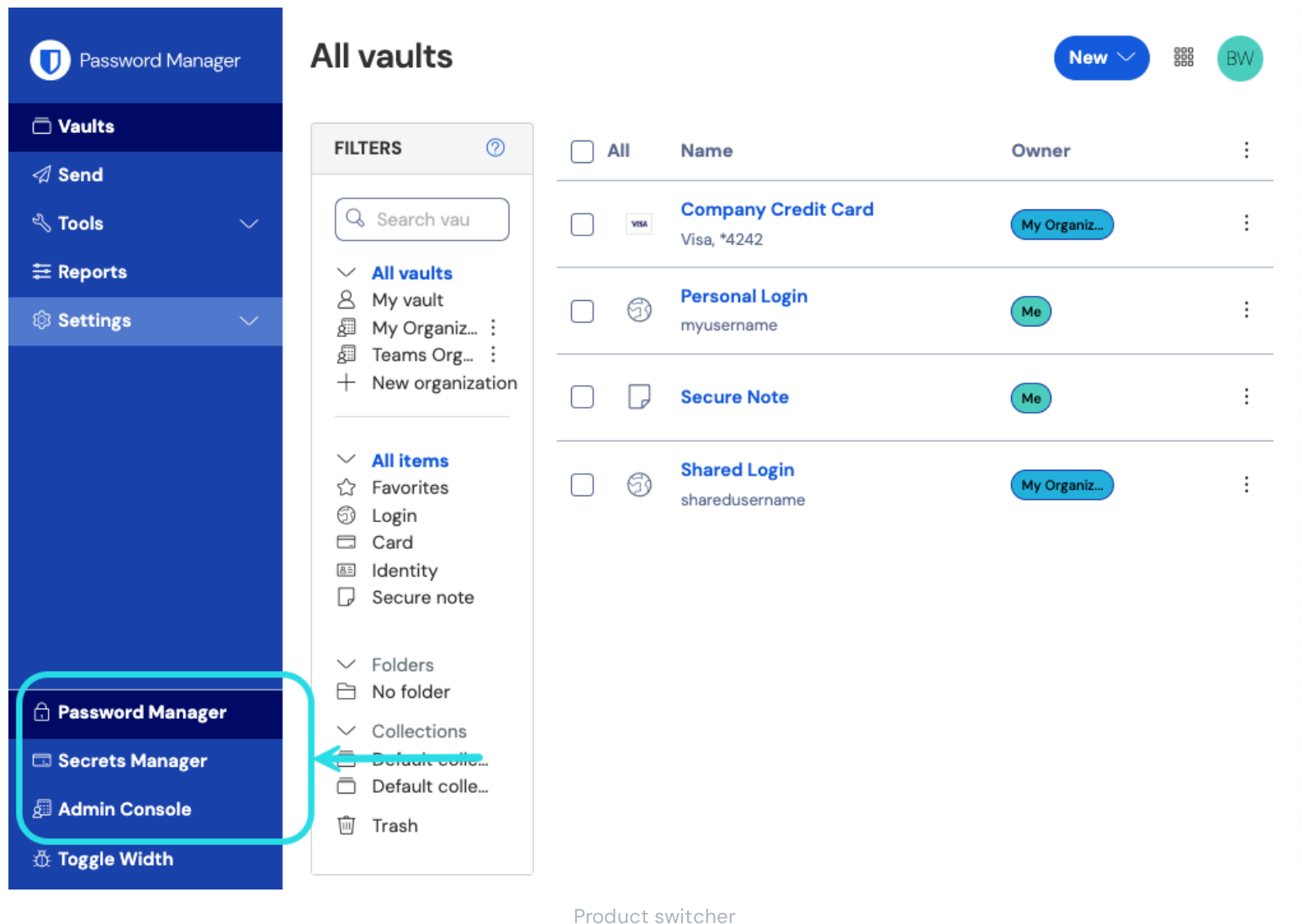


Already an SSO expert? Skip the instructions in this article and download screenshots of sample configurations to compare against your own.

[Download Sample](#)

Open SSO in the web app


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



The screenshot shows the Bitwarden web app interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main area is titled 'All vaults' and contains a table of vaults. A red box highlights the 'Password Manager' option in the sidebar, and a red arrow points to the 'Product switcher' button in the top right corner.

	Filters	Table Headers																			
<ul style="list-style-type: none"> ▼ All vaults <ul style="list-style-type: none"> My vault My Organiz... Teams Org... + New organization ▼ All items <ul style="list-style-type: none"> ★ Favorites 🕒 Login 📅 Card 👤 Identity 📄 Secure note ▼ Folders <ul style="list-style-type: none"> No folder ▼ Collections <ul style="list-style-type: none"> Default colle... Default colle... 🗑️ Trash 	<table> <thead> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Owner</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Company Credit Card Visa, *4242</td> <td>My Organiz...</td> <td>⋮</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Personal Login myusername</td> <td>Me</td> <td>⋮</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Secure Note</td> <td>Me</td> <td>⋮</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Shared Login sharedusername</td> <td>My Organiz...</td> <td>⋮</td> </tr> </tbody> </table>	<input type="checkbox"/>	Name	Owner		<input type="checkbox"/>	Company Credit Card Visa, *4242	My Organiz...	⋮	<input type="checkbox"/>	Personal Login myusername	Me	⋮	<input type="checkbox"/>	Secure Note	Me	⋮	<input type="checkbox"/>	Shared Login sharedusername	My Organiz...	⋮
<input type="checkbox"/>	Name	Owner																			
<input type="checkbox"/>	Company Credit Card Visa, *4242	My Organiz...	⋮																		
<input type="checkbox"/>	Personal Login myusername	Me	⋮																		
<input type="checkbox"/>	Secure Note	Me	⋮																		
<input type="checkbox"/>	Shared Login sharedusername	My Organiz...	⋮																		

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



My Organization

Collections

Members

Groups

Reporting

Billing

Settings

Organization info

Policies

Two-step login

Import data

Export vault

Domain verification

Single sign-on

Device approvals

SCIM provisioning

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

☒ Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)

unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

☒ Master password

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

☐ Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type

SAML 2.0

SAML service provider configuration

☒ Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID

SAML 2.0 metadata URL

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.



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:

Dashboard

Directory

Customizations

Applications

Applications

Self Service

Security

Workflow

Reports

Settings

Applications

Create App Integration

Browse App Catalog

Assign Users to App

More

Search

STATUS			
ACTIVE	0		Okta Admin Console
INACTIVE	6		Okta Browser Plugin
			Okta Dashboard

Okta create app integration

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

Applications

Create a new app integration

Sign-in method

Learn More

☐

OIDC - OpenID Connect

Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☒

SAML 2.0

XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐

SWA - Secure Web Authentication

Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐

API Services

Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

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

Advanced settings

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

Update application username on

Create and update ▼

→ Show Advanced Settings

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 (optional)

LEARN MORE

Name	Name format (optional)	Value
email	Unspecified	user.email
firstname	Unspecified	user.firstName
lastname	Unspecified	user.lastName

Add Another

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:

Settings

[Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ SAML 2.0

Default Relay State

Credentials Details

Application username format

Okta username

Update application username on

Create and update

[Update Now](#)

Password reveal

☐ Allow users to securely see their password
(Recommended)

SAML Signing Certificates

[Generate new certificate](#)

Type	Created	Expires	Status	Actions
SHA-1	Oct 2022	Oct 2032	Inactive ⚠	Actions ▼

[View SAML setup instructions](#)

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[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**:

The following is needed to configure Bitwarden

1 Identity Provider Single Sign-On URL:

```
https://bitwardenhelptest.okta.com/app/bitwardenhelptest_bitwarden_1/exk3fajwkMx07SosA696/sso/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exk3fajwkMx07SosA696
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDsjCCApqgAwIBAgIGAXw253khMA0GCSqGSIb3DQEBCwUAMIGZMQswCQYDVQQGEwJVUzETMBEG  
A1UECAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
```

IdP Values

Assignments

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

← Back to Applications



Bitwarden Login with SSO

Active ▾



[View Logs](#) [Monitor Imports](#)

General

Sign On

Import

Assignments

Assign ▾

[Convert Assignments](#)

Groups ▾

Filters

People

Groups

Priority

Assignment

1

 Everyone

All users in your organization



REPORTS

[Current Assignments](#)

[Recent Unassignments](#)

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.

[Go to self service settings](#)

Requests Disabled

Approval -

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	<p>Paste the downloaded certificate, removing</p> <p>-----BEGIN CERTIFICATE-----</p> <p>and</p> <p>-----END CERTIFICATE-----</p> <p>The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters will cause certification validation to fail.</p>
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.

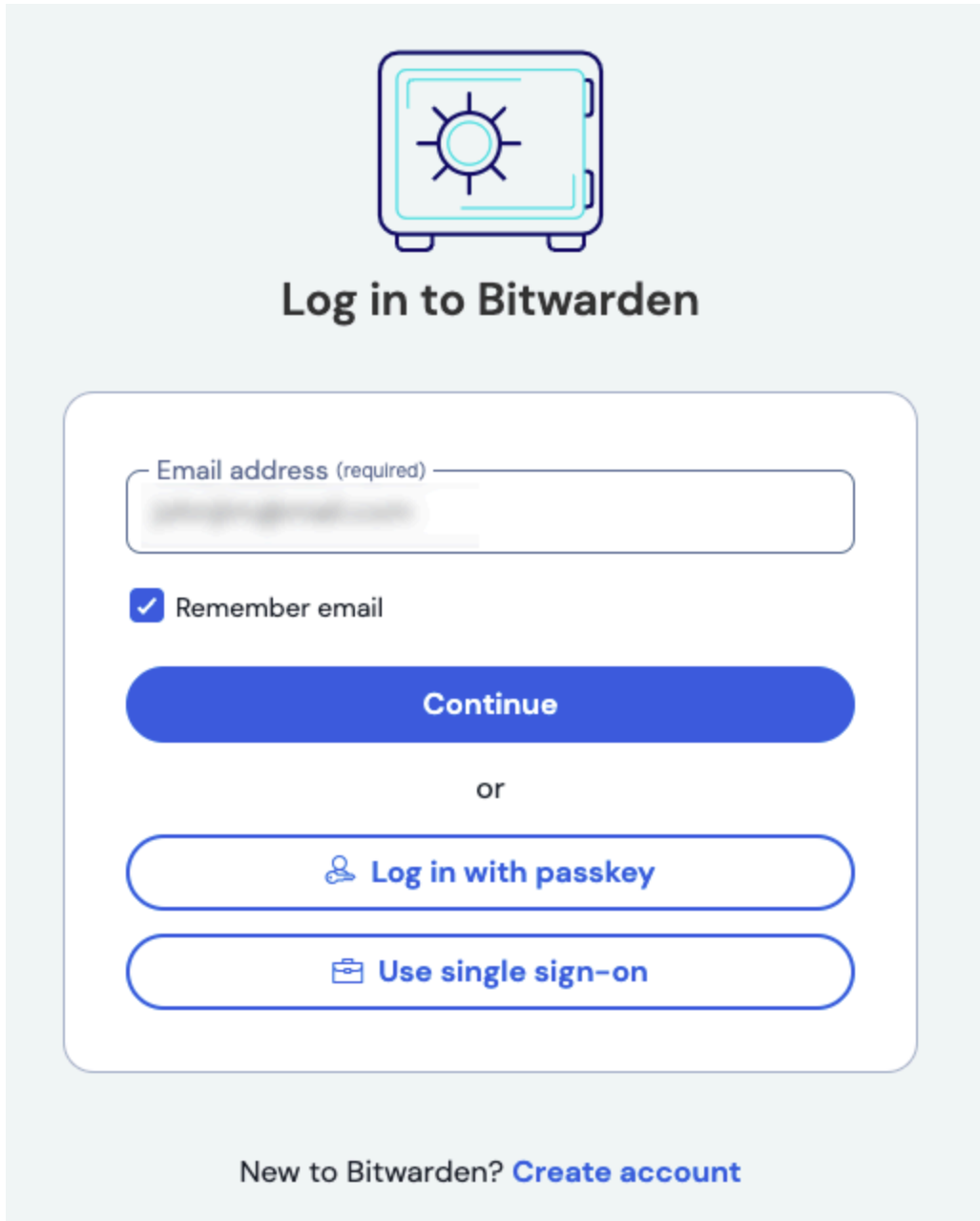
When you're done with the identity provider configuration, **Save** your work.

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

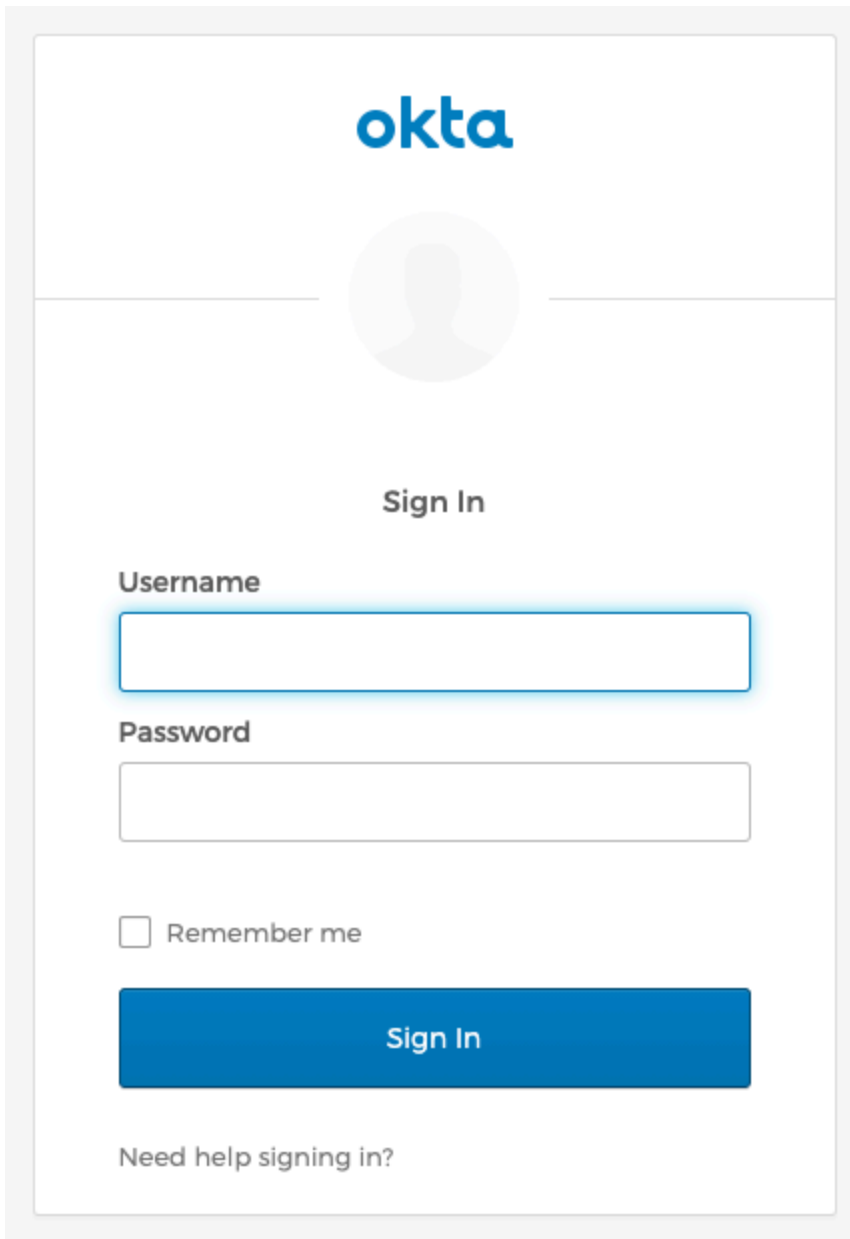
Once your configuration is complete, test it by navigating to <https://vault.bitwarden.com>, entering your email address and selecting the **Enterprise Single-On** button:



The image shows the Bitwarden login interface. At the top is a blue icon of a safe. Below it is the heading "Log in to Bitwarden". The main form contains an "Email address (required)" input field with a blurred placeholder. Below the input is a checked checkbox labeled "Remember email". A large blue "Continue" button is positioned below the checkbox. Underneath the button is the word "or". There are two more buttons: "Log in with passkey" (with a person icon) and "Use single sign-on" (with a briefcase icon). At the bottom of the form is the text "New to Bitwarden? Create account".

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:



The image shows a screenshot of an Okta sign-in interface. At the top is the Okta logo. Below it is a circular placeholder for a user profile picture. The text "Sign In" is centered. There are two input fields: "Username" and "Password". Below the password field is a checkbox labeled "Remember me". A blue "Sign In" button is positioned below the checkbox. At the bottom of the form is a link that says "Need help signing in?".

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.