bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO >

Okta OIDC Implementation

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

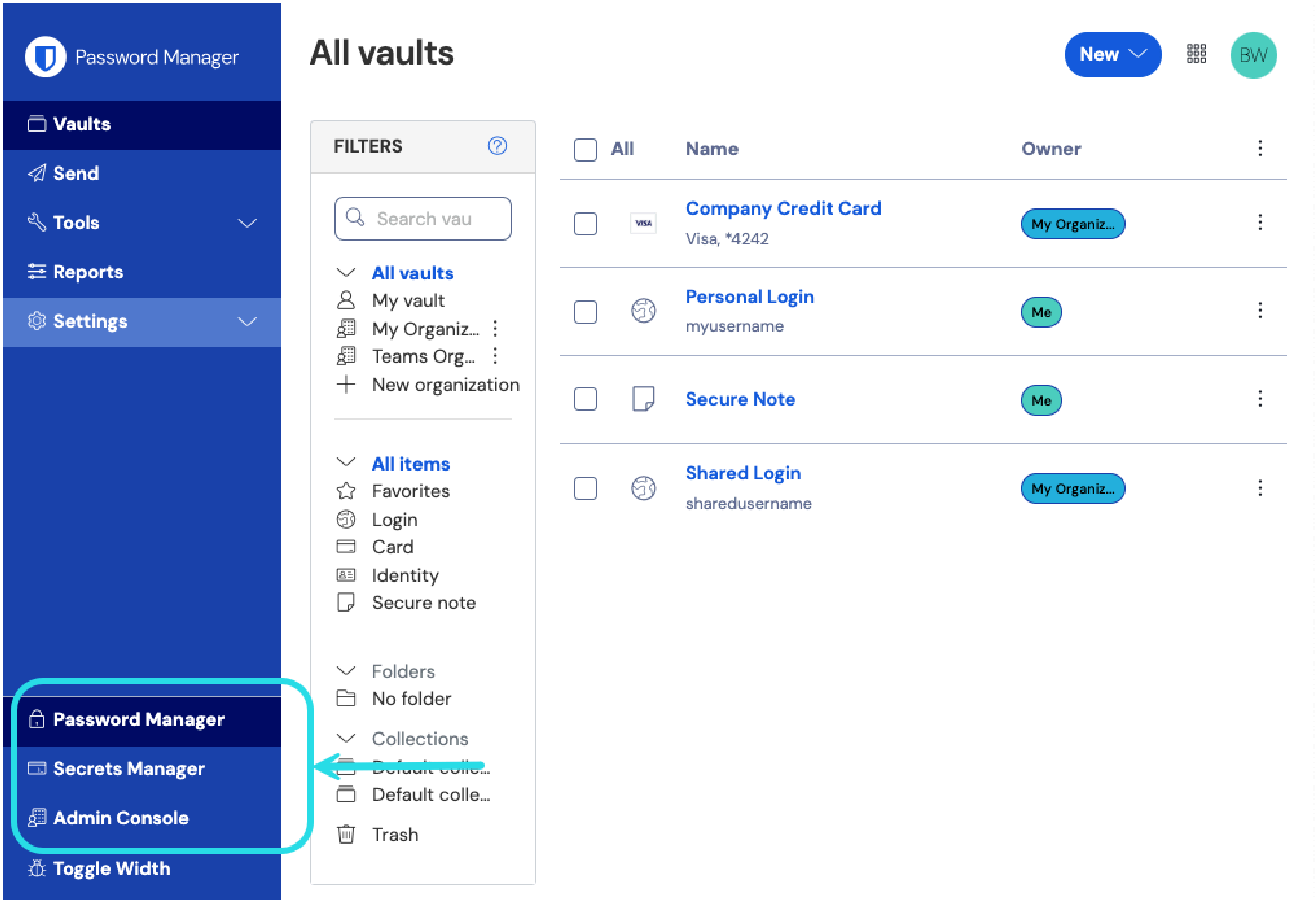
Okta OIDC Implementation

This article contains **Okta-specific** help for configuring login with SSO via OpenID Connect (OIDC). For help configuring login with SSO for another OIDC IdP, or for configuring Okta via SAML 2.0, see OIDC Configuration or Okta SAML Implementation.

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.

Open SSO in the web vault

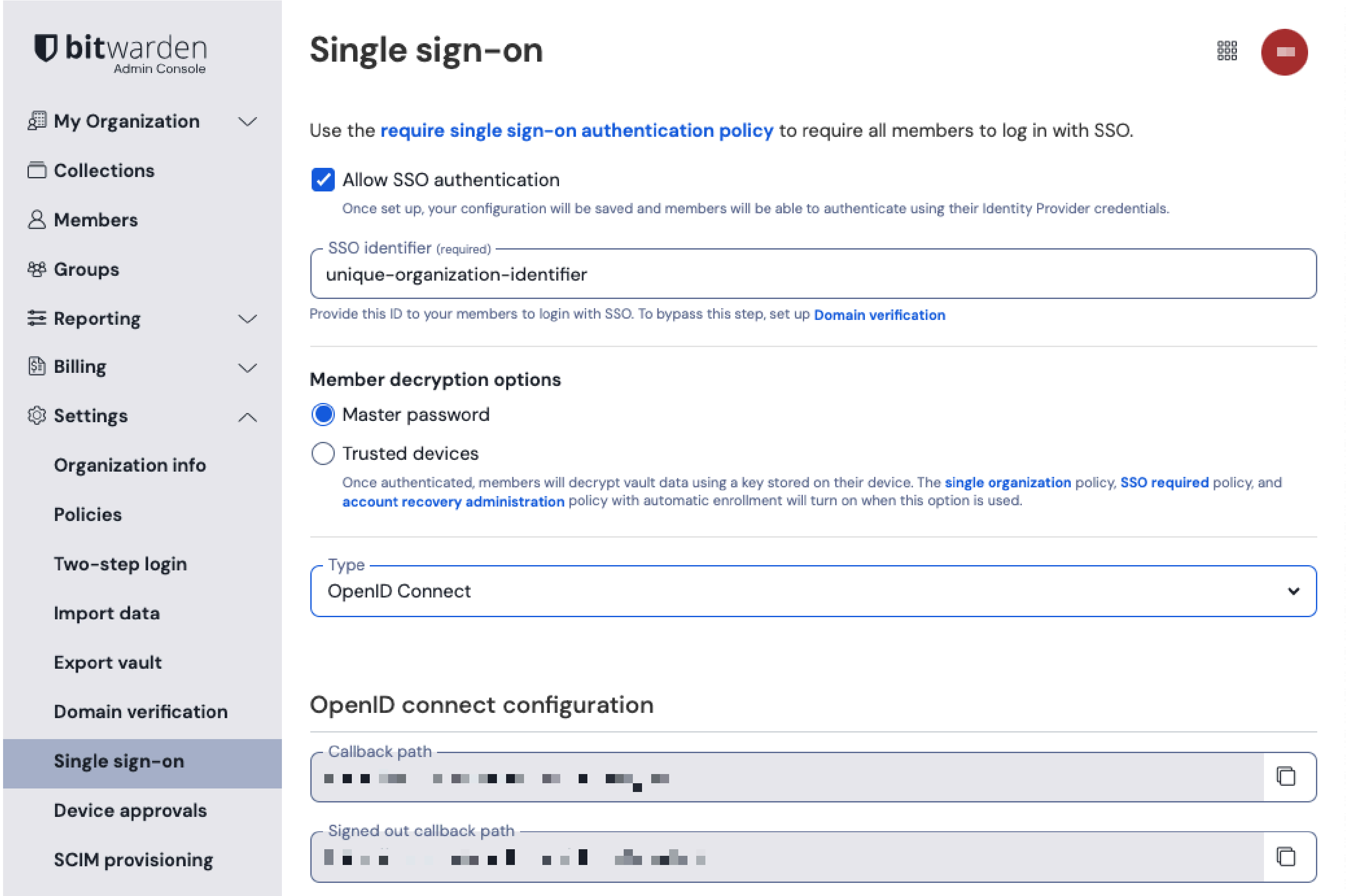
Log in to the Bitwarden web app and open the Admin Console using the product switcher:



All	Name	Owner
□	Company Credit Card Visa, *4242	My Organiz...
□	Personal Login myusername	Me
□	Secure Note	Me
□	Shared Login sharedusername	My Organiz...

Product switcher

Select **Settings** → **Single sign-on** from the navigation:



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

○ 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: OpenID Connect

OpenID connect configuration

Callback path: [redacted]

Signed out callback path: [redacted]

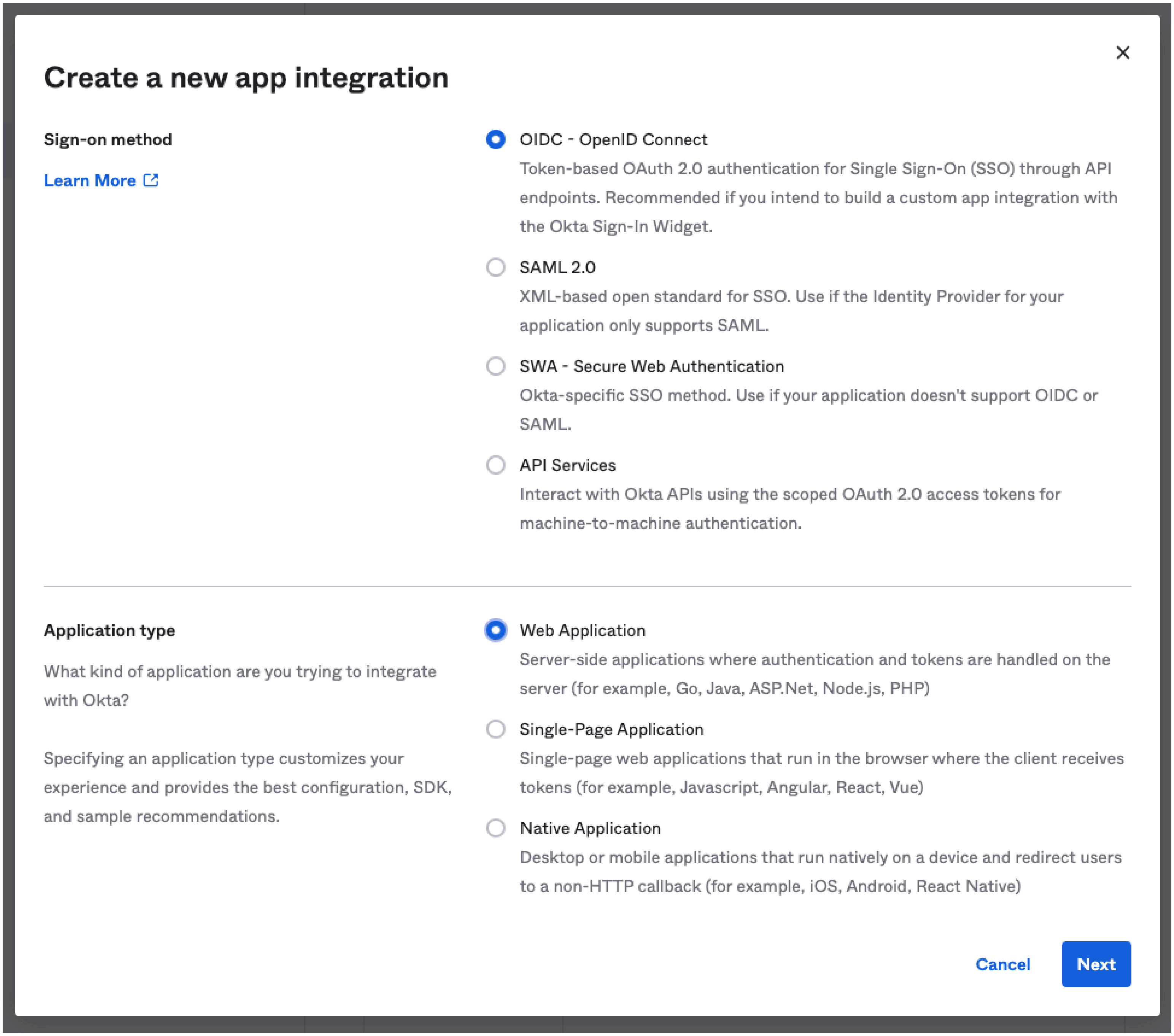
OIDC configuration

If you haven't already, create a unique **SSO identifier** for your organization. Otherwise, you don't need to edit anything on this screen yet, but keep it open for easy reference.

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

Create an Okta app

In the Okta Admin Portal, select **Applications** → **Applications** from the navigation. On the Applications screen, select the **Create App Integration** button. For Sign-on method, select **OIDC - OpenID Connect**. For Application type, select **Web Application**:



Create a new app integration

Sign-on method

● 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.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

● Web Application
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

○ Single-Page Application
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

○ Native Application
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Create App Integration

On the **New Web App Integration** screen, configure the following fields:

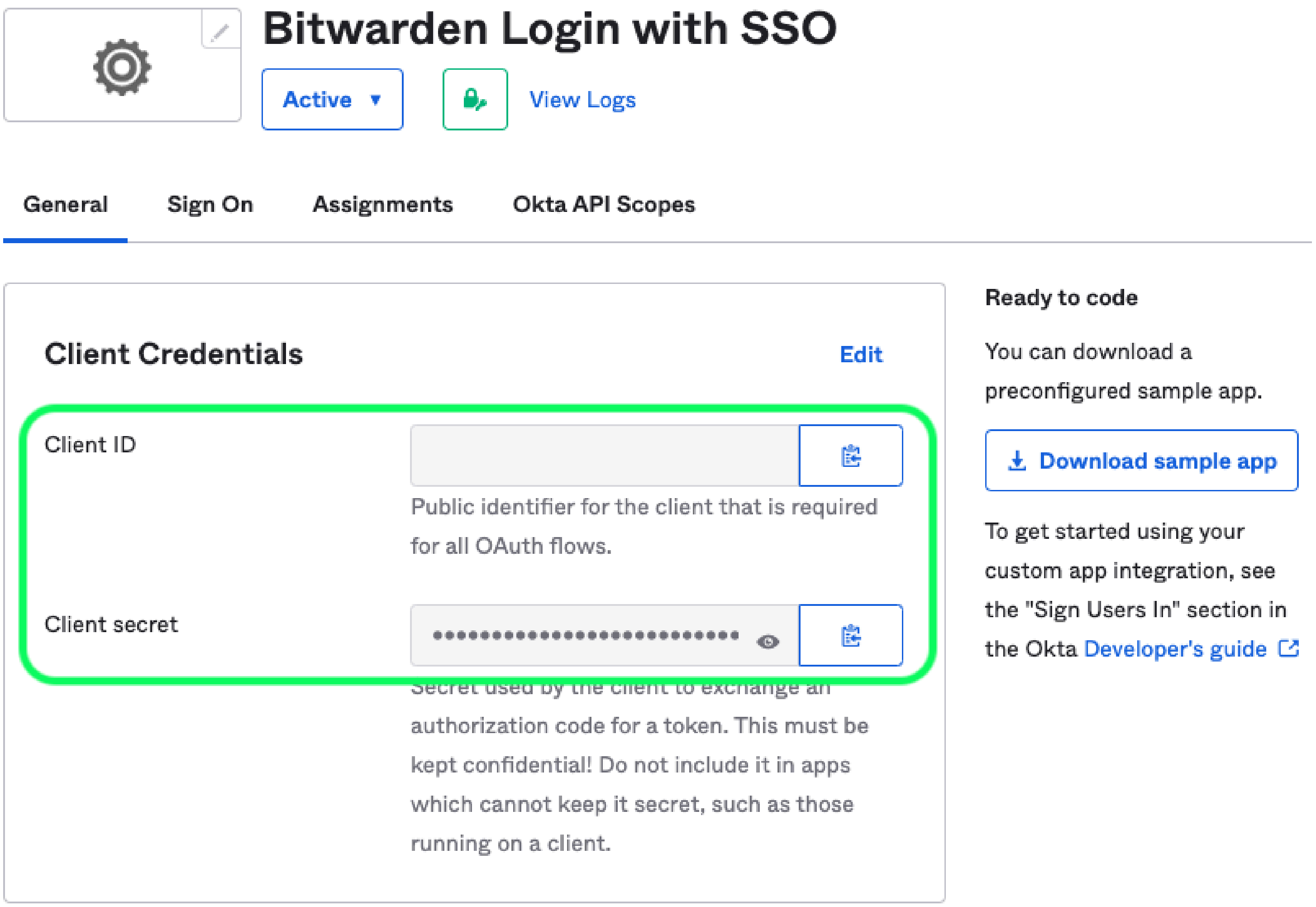
Field	Description
App integration name	Give the app a Bitwarden-specific name.

Field	Description
Grant type	Enable the following grant types: - Client acting on behalf of itself → **Client Credentials** - Client acting on behalf of a user → **Authorization Code**
Sign-in redirect URIs	Set this field to your **Callback Path**, which can be retrieved from the Bitwarden SSO Configuration screen. For cloud-hosted customers, this is `https://sso.bitwarden.com/oidc-signin` or `https://sso.bitwarden.eu/oidc-signin`. For self-hosted instances, this is determined by your configured server URL, for example `https://your.domain.com/sso/oidc-signin`.
Sign-out redirect URIs	Set this field to your **Signed Out Callback Path**, which can be retrieved from the Bitwarden SSO Configuration screen.
Assignments	Use this field to designate whether all or only select groups will be able to use Bitwarden Login with SSO.

Once configured, select the **Next** button.

Get client credentials

On the Application screen, copy the **Client ID** and **Client secret** for the newly created Okta app:



Bitwarden Login with SSO

Active ▾

View Logs

General | Sign On | Assignments | Okta API Scopes

Client Credentials

Edit

Client ID

Public identifier for the client that is required for all OAuth flows.

Client secret

••••••••••••••••••••••••••••

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Ready to code

You can download a preconfigured sample app.

Download sample app

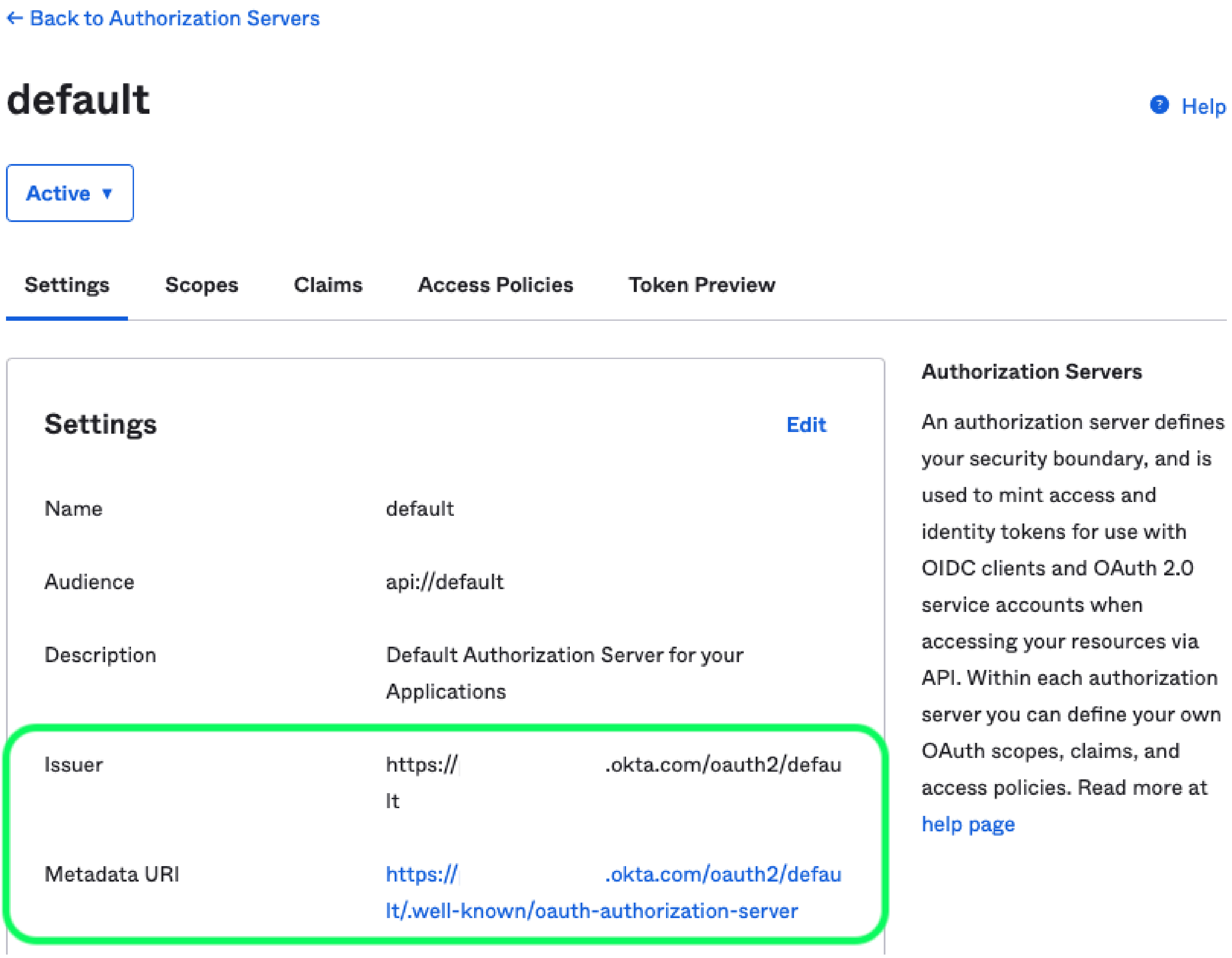
To get started using your custom app integration, see the "Sign Users In" section in the Okta Developer's guide

App Client Credentials

You will need to use both values during a later step.

Get authorization server information

Select **Security** → **API** from the navigation. From the **Authorization Servers** list, select the server you would like to use for this implementation. On the **Settings** tab for the server, copy the **Issuer** and **Metadata URI** values:



← Back to Authorization Servers

default

Help

Active ▾

Settings | Scopes | Claims | Access Policies | Token Preview

Settings

Edit

Name	default
Audience	api://default
Description	Default Authorization Server for your Applications
Issuer	https:// .okta.com/oauth2/default
Metadata URI	https:// .okta.com/oauth2/default/.well-known/oauth-authorization-server

Authorization Servers

An authorization server defines your security boundary, and is used to mint access and identity tokens for use with OIDC clients and OAuth 2.0 service accounts when accessing your resources via API. Within each authorization server you can define your own OAuth scopes, claims, and access policies. Read more at help page

Okta Authorization Server Settings

You will need to use both values during the next step.

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 configure the following fields:

Field	Description
Authority	Enter the retrieved Issuer URI for your Authorization Server.
Client ID	Enter the retrieved Client ID for your Okta app.

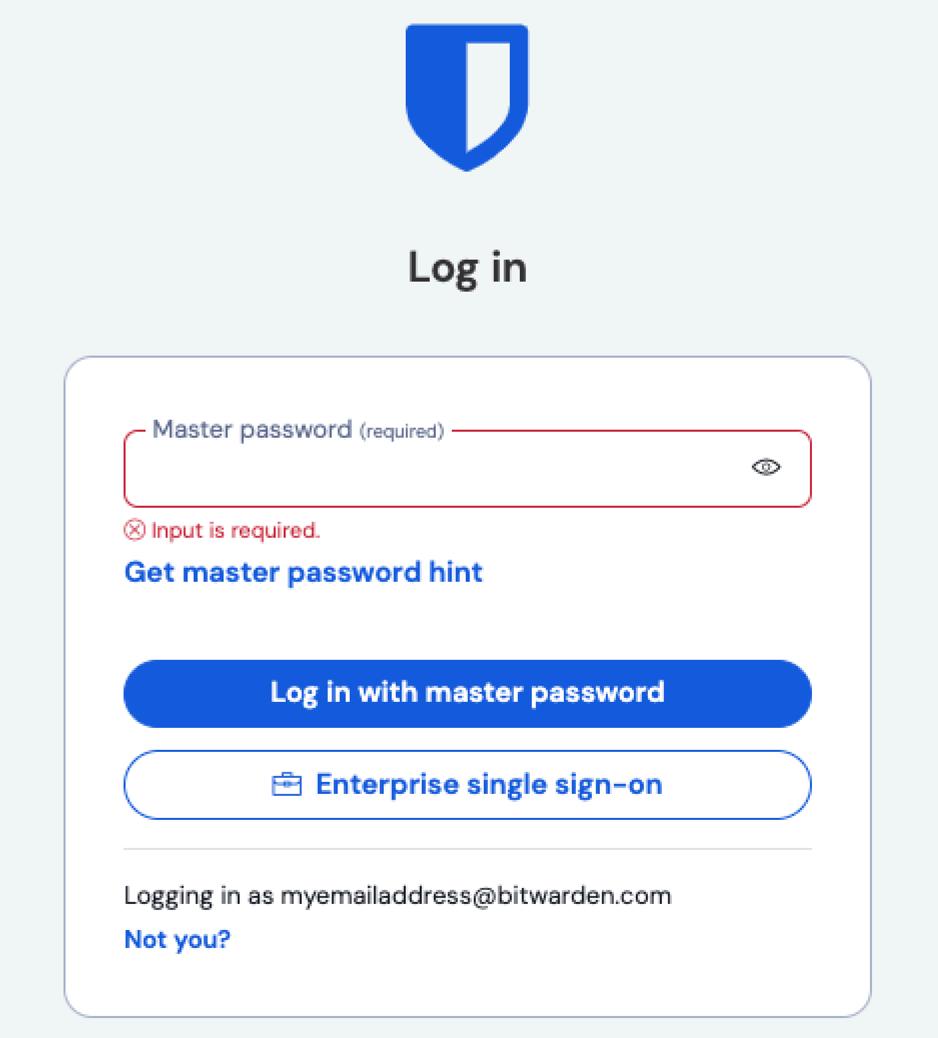
Field	Description
Client Secret	Enter the retrieved Client secret for your Okta app.
Metadata Address	Enter the retrieved Metadata URI for your Authorization Server.
OIDC Redirect Behavior	Select **Redirect GET**. Okta currently does not support Form POST.
Get Claims From User Info Endpoint	Enable this option if you receive URL too long errors (HTTP 414), truncated URLS, and/or failures during SSO.
Additional/Custom Scopes	Define custom scopes to be added to the request (comma-delimited).
Additional/Custom User ID Claim Types	Define custom claim type keys for user identification (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Additional/Custom Email Claim Types	Define custom claim type keys for users' email addresses (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Additional/Custom Name Claim Types	Define custom claim type keys for users' full names or display names (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Requested Authentication Context Class Reference values	Define Authentication Context Class Reference identifiers (`acr_values`) (space-delimited). List `acr_values` in preference-order.
Expected "acr" Claim Value in Response	Define the `acr` Claim Value for Bitwarden to expect and validate in the response.

When you are done configuring these fields, **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, selecting **Continue**, and selecting the **Enterprise Single-On** button:



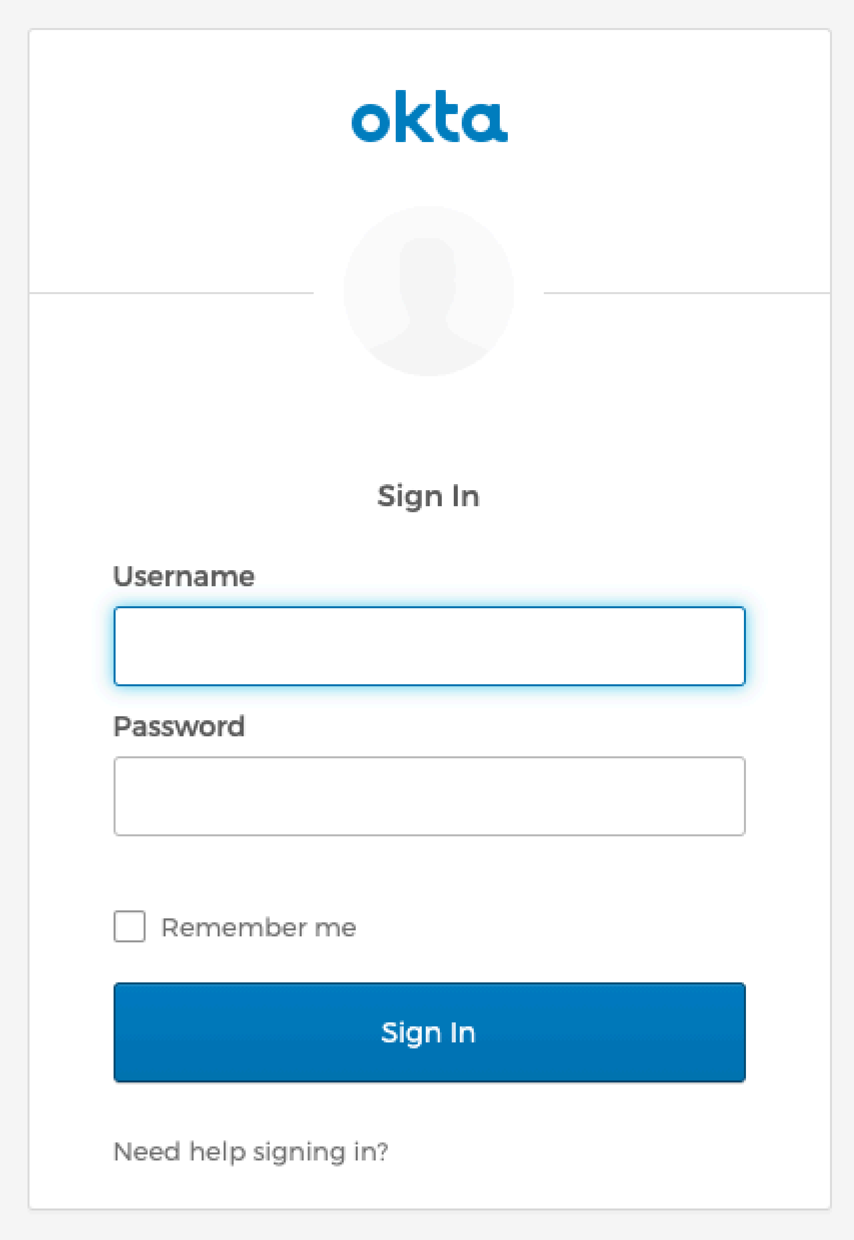
Log in
Master password (required)
Get master password hint
Log in with master password
Enterprise single sign-on
Not you?

Input is required.

Logging in as myemailaddress@bitwarden.com

Log in options screen

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you'll 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.