

ADMIN CONSOLE > LOGIN WITH SSO

OIDC Configuration

View in the help center:

<https://bitwarden.com/help/configure-sso-oidc/>

OIDC Configuration

Step 1: Set an SSO identifier

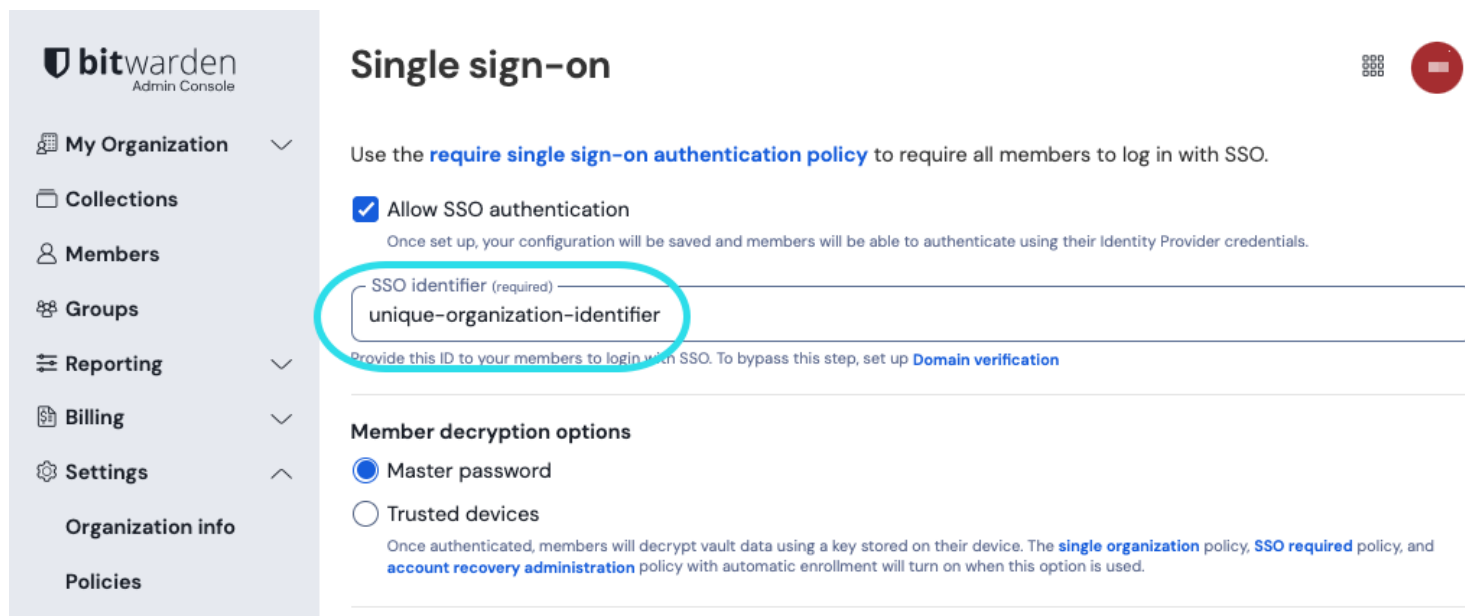
Users who [authenticate their identity using SSO](#) will be required to enter an **SSO identifier** that indicates the organization (and therefore, the SSO integration) to authenticate against. To set a unique SSO Identifier:

1. 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. Below these are three buttons: Password Manager, Secrets Manager, and Admin Console. A red circle highlights the 'Admin Console' button, with a red arrow pointing to it from the 'Product switcher' label below. The main content area is titled 'All vaults' and features a 'New' button and a 'BW' profile icon. Below the title is a 'FILTERS' section with a search bar and a list of vaults: All vaults, My vault, My Organiz..., Teams Org..., and New organization. To the right of the filters is a table of vaults with columns for 'All', 'Name', and 'Owner'. The table lists four vaults: 'Company Credit Card' (owner: My Organiz...), 'Personal Login' (owner: Me), 'Secure Note' (owner: Me), and 'Shared Login' (owner: My Organiz...). Each vault has a checkbox and a list icon.

Product switcher

2. Navigate to **Settings** → **Single sign-on**, and enter a unique **SSO Identifier** for your organization:



Enter an identifier

3. Proceed to **Step 2: Enable login with SSO**.



Tip

You will need to share this value with users once the configuration is ready to be used.

Step 2: Enable login with SSO

Once you have your SSO identifier, you can proceed to enabling and configuring your integration. To enable login with SSO:

1. On the **Settings** → **Single sign-on** view, check the **Allow SSO authentication** checkbox:


Admin Console

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

☐ 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

Signed out callback path

OIDC configuration

- From the **Type** dropdown menu, select the **OpenID Connect** option. If you intend to use SAML instead, switch over the the [SAML Configuration guide](#).



There are alternative **Member decryption options**. Learn how to get started using [SSO with trusted devices](#) or [Key Connector](#).

Step 3: Configuration

From this point on, implementation will vary provider-to-provider. Jump to one of our specific **implementation guides** for help completing the configuration process:

Provider	Guide
Azure	Azure Implementation Guide
Okta	Okta Implementation Guide

Configuration reference materials

The following sections will define fields available during single sign-on configuration, agnostic of which IdP you are integration with. Fields that must be configured will be marked (**required**).



Tip

Unless you are comfortable with OpenID Connect, we recommend using one of the [above implementation guides](#) instead of the following generic material.

Field	Description
Callback Path	(Automatically generated) The URL for authentication automatic redirect. For cloud-hosted customers, this is <code>https://sso.bitwarden.com/oidc-signin</code> or <code>https://sso.bitwarden.eu/oidc-signin</code> . For self-hosted instances, this is determined by your configured server URL , for example <code>https://your.domain.com/sso/oidc-signin</code> .
Signed Out Callback Path	(Automatically generated) The URL for sign-out automatic redirect. For cloud-hosted customers, this is <code>https://sso.bitwarden.com/oidc-signedout</code> or <code>https://sso.bitwarden.eu/oidc-signedout</code> . For self-hosted instances, this is determined by your configured server URL , for example <code>https://your.domain.com/sso/oidc-signedout</code> .
Authority	(Required) The URL of your authorization server ("Authority"), which Bitwarden will perform authentication against. For example, <code>https://your.domain.okta.com/oauth2/default</code> or <code>https://login.microsoft.com/<TENANT_ID>/v2.0</code> .

Field	Description
Client ID	(Required) An identifier for the OIDC client. This value is typically specific to a constructed IdP app integration, for example an Azure app registration or Okta web app .
Client Secret	(Required) The client secret used in conjunction with the client ID to exchange for an access token. This value is typically specific to a constructed IdP app integration, for example an Azure app registration or Okta Web App .
Metadata Address	(Required if Authority is not valid) A Metadata URL where Bitwarden can access authorization server metadata as a JSON object. For example, https://your.domain.okta.com/oauth2/default/.well-known/oauth-authorization-server
OIDC Redirect Behavior	(Required) Method used by the IdP to respond to authentication requests from Bitwarden. Options include Form POST and Redirect GET .
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.

Field	Description
Requested authentication context class reference values	Define authentication context class reference identifiers (<code>acr_values</code>) (space-delimited). List <code>acr_values</code> in preference-order.
Expected "acr" Claim Value in Response	Define the <code>acr</code> claim value for Bitwarden to expect and validate in the response.

OIDC attributes & claims

An **email address is required for account provisioning**, which can be passed as any of the attributes or claims in the below table.

A unique user identifier is also highly recommended. If absent, email will be used in its place to link the user.

Attributes/claims are listed in order of preference for matching, including fallbacks where applicable:

Value	Claim/Attribute	Fallback claim/attribute
Unique ID	Configured Custom User ID Claims NameID (when not transient) urn:oid:0.9.2342.19200300.100.1.1 Sub UID UPN EPPN	
Email	Configured Custom Email Claims Email http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress urn:oid:0.9.2342.19200300.100.1.3 Mail EmailAddress	Preferred_Username Urn:oid:0.9.2342.19200300.100.1.1 UID
Name	Configured Custom Name Claims Name http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3	First Name + " " + Last Name (see below)

Value	Claim/Attribute	Fallback claim/attribute
First Name	DisplayName CN	
	urn:oid:2.5.4.42 GivenName FirstName FN FName Nickname	
Last Name	urn:oid:2.5.4.4 SN Surname LastName	