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:

Password Manager	All vaults		New 💛 🗱 BW
🗇 Vaults	FILTERS 🕐	All Name	Owner
🗇 Send		Ali Name	Owner
🖏 Tools 🛛 🗸 🗸	Q Search vau	Company Credit Card Visa, *4242	My Organiz
茬 Reports ⑫ Settings ──	 ✓ All vaults △ My vault ④ My Organiz : 	Personal Login myusername	Me
	 Teams Org : + New organization 	Secure Note	Me
	 ✓ All items ☆ Favorites ④ Login □ Card Identity □ Secure note 	Shared Login sharedusername	My Organiz
Password Manager	 ✓ Folders ➡ No folder 		
🗔 Secrets Manager	Collections		
🗿 Admin Console	 Default colle Trash 		
🖞 Toggle Width			
		Product switcher	

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

D bit warden		Single sign-on	000	0
B My Organization	\sim	Use the require single sign-on authentication policy to require all members to log in with SSO.		
		Allow SSO authentication		
A Members		Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.		
뿅 Groups	(SSO identifier (required) unique-organization-identifier		
₽ Reporting	\sim	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification		
🕅 Billing	\sim	Member decryption options		
Settings	\sim	Master password		
Organization info Policies		Trusted devices Once authenticated, members will decrypt vauit data using a key stored on their device. The single organization policy, SSO require account recovery administration policy with automatic enrollment will turn on when this option is used.	d policy,	and
Enter an identifier				

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

Q TipYou 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** \rightarrow **Single sign-on** view, check the **Allow SSO authentication** checkbox:

D bit warden	Single sign-on 🗰 🔁
$\#$ My Organization $~~ \lor$	Use the require single sign-on authentication policy to require all members to log in with SSO.
Collections	✓ Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
뿅 Groups	SSO identifier (required) unique-organization-identifier
\rightleftharpoons Reporting \lor	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
🗟 Billing \checkmark	Member decryption options
 	Master password
Organization info	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.
Policies	account recovery administration policy with automatic enforment will tarr on when this option is used.
Two-step login	С Туре
Import data	OpenID Connect ~
Export vault	
Domain verification	OpenID connect configuration
Single sign-on	Callback path
Device approvals	•
SCIM provisioning	Signed out callback path

OIDC configuration

2. From the **Type** dropdown menu, select the **OpenID Connect** option. If you intend to use SAML instead, switch over the the SAML Configuration guide.

⊘ Tip

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

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.

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

Field	Description
Metadata Address	<pre>(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</pre>
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.
Requested authentication context class reference values	Define authentication context class reference identifiers (acr_values) (space-delimited). List ac r_values in preference-order.
Expected "acr" Claim Value in Response	Define the acr 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 DisplayName CN	First Name + " " + Last Name (see below)
First Name	urn:oid:2.5.4.42 GivenName FirstName FN FName Nickname	
Last Name	urn:oid:2.5.4.4 SN Surname LastName	