

ADMIN CONSOLE > LOGGA IN MED SSO

SAML 2.0 Configuration

View in the help center:

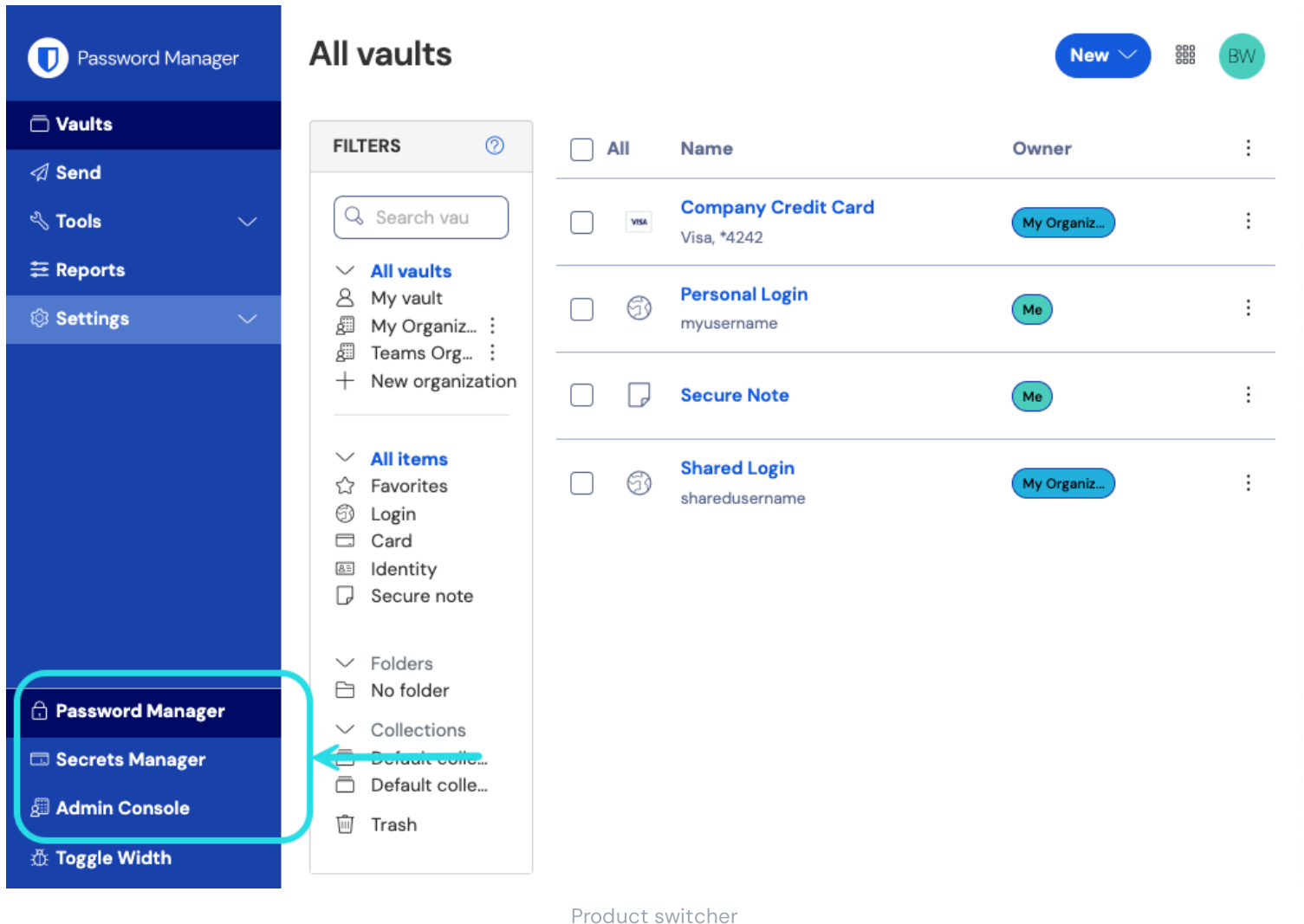
<https://bitwarden.com/help/configure-sso-saml/>

SAML 2.0 Configuration

Step 1: Set an SSO identifier

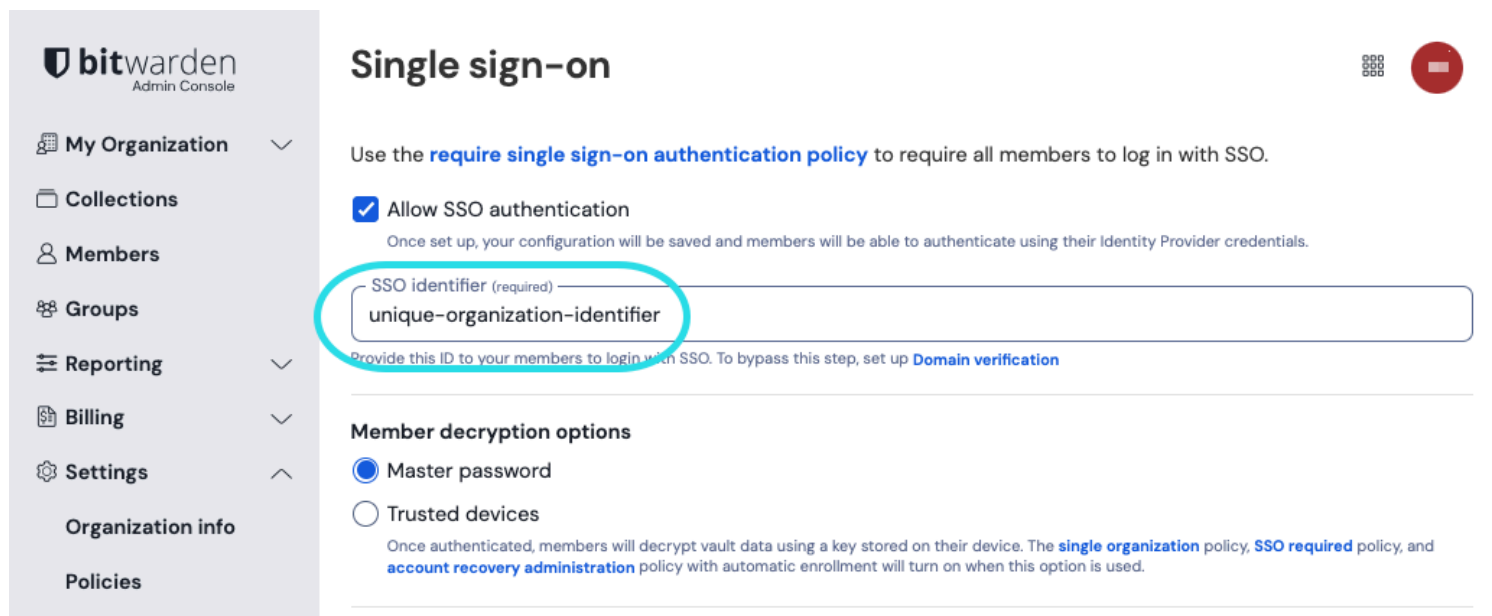
Users who [authenticate their identity using SSO](#) will be required to enter an **SSO identifier** that indicates the organization (and therefore, the SSO integration) to authenticate against. To set a unique SSO Identifier:

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 a 'Password Manager' header and a menu containing 'Vaults', 'Send', 'Tools', 'Reports', 'Settings', 'Password Manager', 'Secrets Manager', 'Admin Console', and 'Toggle Width'. A red rectangle highlights the 'Admin Console' option, with a red arrow pointing to it from the right. The main content area is titled 'All vaults' and features a 'New' button, a grid icon, and a 'BW' profile icon. Below this is a 'FILTERS' section with a search bar and a list of categories: 'All vaults' (expanded), 'My vault', 'My Organiz...', 'Teams Org...', and 'New organization'. Under 'All vaults', there are sub-categories: 'All items' (expanded), 'Favorites', 'Login', 'Card', 'Identity', 'Secure note', 'Folders', 'No folder', 'Collections', 'Default colle...', 'Default colle...', and 'Trash'. The main list displays four vaults: 'Company Credit Card' (Visa, *4242, owned by 'My Organiz...'), 'Personal Login' (myusername, owned by 'Me'), 'Secure Note' (owned by 'Me'), and 'Shared Login' (sharedusername, owned by 'My Organiz...'). Each vault has a checkbox, an icon, a title, a description, an owner, and a three-dot menu. At the bottom of the screenshot, the text 'Product switcher' is visible.

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**.



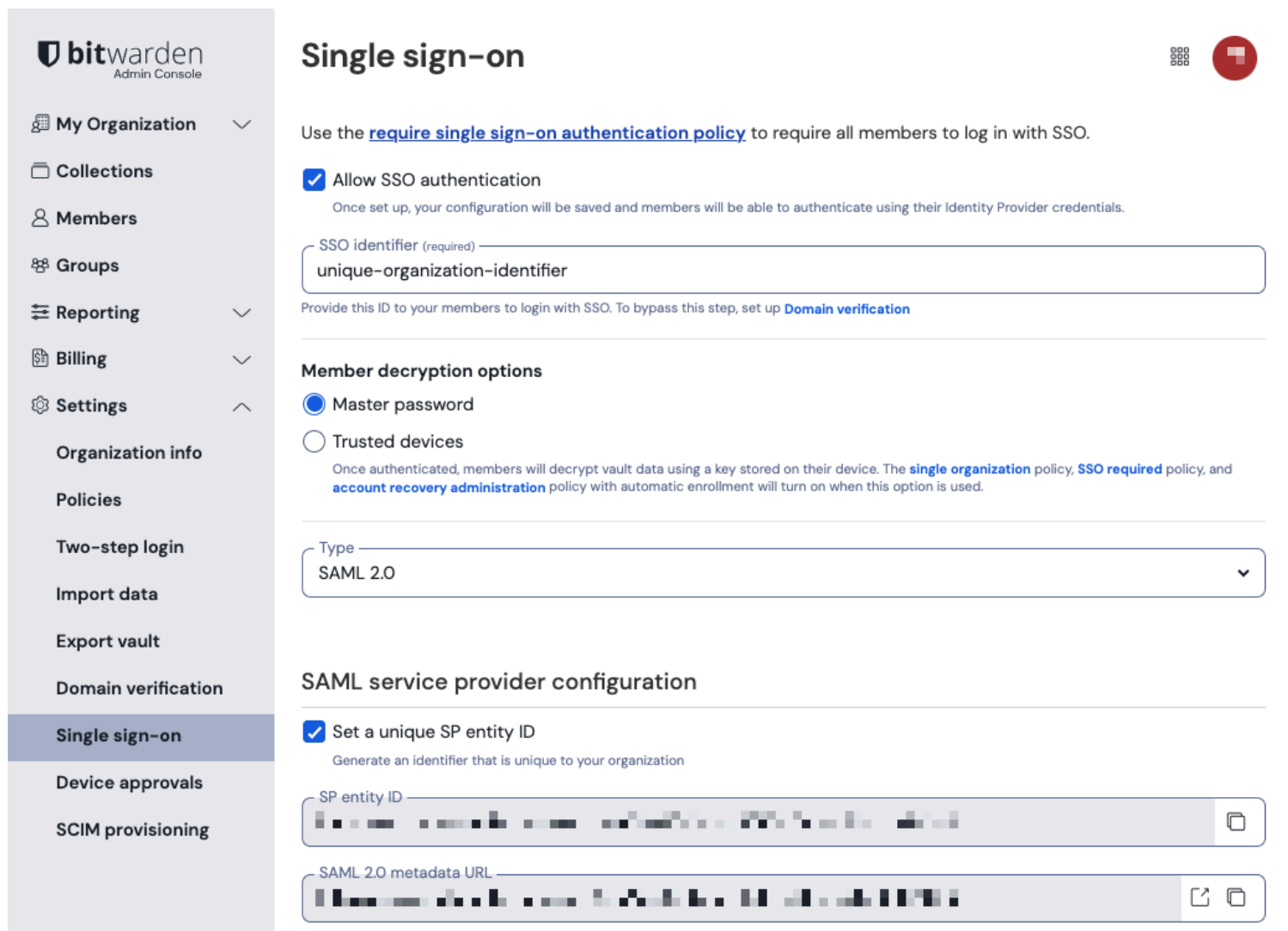
Tip

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:



SAML 2.0 configuration

- From the **Type** dropdown menu, select the **SAML 2.0** option. If you intend to use OIDC instead, switch over to the [OIDC Configuration Guide](#).

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](#).

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
AD FS	AD FS Implementation Guide
Auth0	Auth0 Implementation Guide
AWS	AWS Implementation Guide
Azure	Azure Implementation Guide
Duo	Duo Implementation Guide
Google	Google Implementation Guide
JumpCloud	JumpCloud Implementation Guide
Keycloak	Keycloak Implementation Guide
Okta	Okta Implementation Guide
OneLogin	OneLogin Implementation Guide
PingFederate	PingFederate 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 SAML 2.0, we recommend using one of the [above implementation guides](#) instead of the following generic material.

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

Field	Description
SP Entity ID	<p>(Automatically generated) The Bitwarden endpoint for authentication requests.</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>
SAML 2.0 Metadata URL	<p>(Automatically generated) Metadata URL for the Bitwarden endpoint.</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>
Assertion Consumer Service (ACS) URL	<p>(Automatically generated) Location where the SAML assertion is sent from the IdP.</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>Format Bitwarden will request of the SAML assertion. Must be cast as a string. Options include:</p> <ul style="list-style-type: none"> -Unspecified (default) -Email address -X.509 Subject name -Windows Domain Qualified Name -Kerberos Principal Name -Entity identifier -Persistent -Transient

Field	Description
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests. Options include: <ul style="list-style-type: none">- http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (default)- http://www.w3.org/2000/09/xmldsig#rsa-sha384- http://www.w3.org/2000/09/xmldsig#rsa-sha512
Signing Behavior	Whether/when SAML requests will be signed. Options include: <ul style="list-style-type: none">-If IdP wants authn requests signed (default)-Always-Never
Minimum Incoming Signing Algorithm	Minimum strength of the algorithm that Bitwarden will accept in SAML responses.
Expect signed assertions	Check this checkbox if Bitwarden should expect responses from the IdP to be signed.
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 configured within the Bitwarden login with SSO docker image.

Identity Provider Configuration

Field	Description
Entity ID	(Required) Address or URL of your identity server or the IdP Entity ID. This field is case sensitive and must match the IdP value exactly.
Binding Type	Method used by the IdP to respond to Bitwarden SAML requests. Options include: <ul style="list-style-type: none">-Redirect (recommended)-HTTP POST
Single Sign On Service URL	(Required if Entity ID is not a URL) SSO URL issued by your IdP.

Field	Description
Single log out service URL	Login with SSO currently does not support SLO. This option is planned for future use, however we strongly recommend pre-configuring this field.
X509 Public Certificate	<p>(Required) The X.509 Base-64 encoded certificate body. Do not include the</p> <p>-----BEGIN CERTIFICATE-----</p> <p>and</p> <p>-----END CERTIFICATE-----</p> <p>lines or portions of the CER/PEM formatted certificate.</p> <p>The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters inside this field will cause certificate validation failure. Copy only the certificate data into this field.</p>
Outbound Signing Algorithm	<p>The algorithm your IdP will use to sign SAML responses/assertions. Options include:</p> <ul style="list-style-type: none"> - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (default) - http://www.w3.org/2000/09/xmldsig#rsa-sha384 - http://www.w3.org/2000/09/xmldsig#rsa-sha512
Allow outbound logout requests	Login with SSO currently does not support SLO. This option is planned for future use, however we strongly recommend pre-configuring this field.
Sign authentication requests	Check this checkbox if your IdP should expect SAML requests from Bitwarden 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.

SAML attributes & claims

An **email address is required for account provisioning**, which can be passed as any of the attributes or claims in the following 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	NameID (when not transient) urn:oid:0.9.2342.19200300.100.1.1 Sub UID UPN EPPN	
Email	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	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	