Ping Identity OIDC Implementation

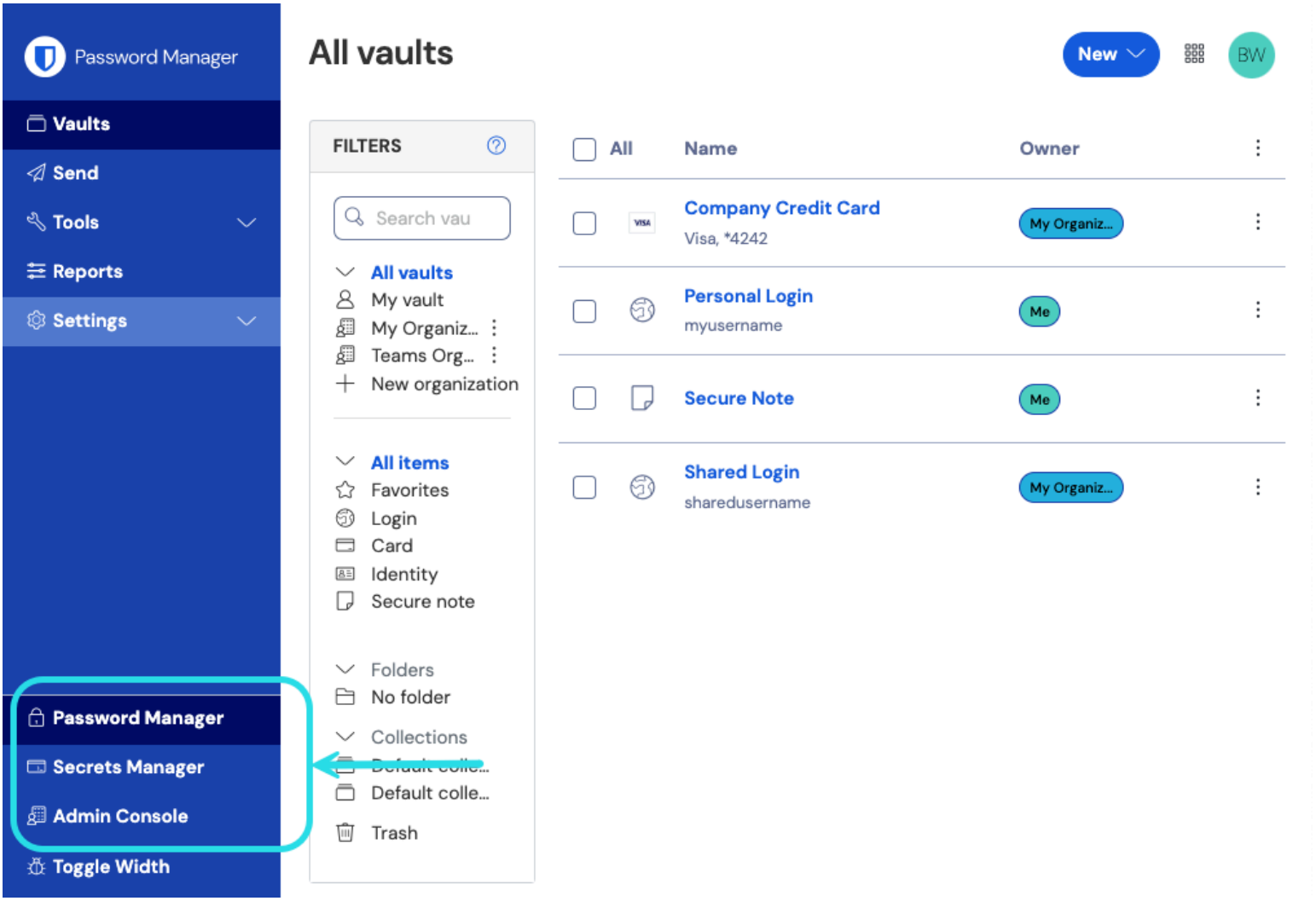
Ping Identity OIDC Implementation

This article contains Ping Identity specific help for configuring Login with SSO via OpenID Connect (OIDC). For help configuring Login with SSO for another OIDC IdP, or for configuring Ping Identity via SAML 2.0, see OIDC Configuration or Ping Identity SAML implementation.

Configuration involves working simultaneously within the Bitwarden web app and the Ping Identity Administrator 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:



Produktwechsler

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

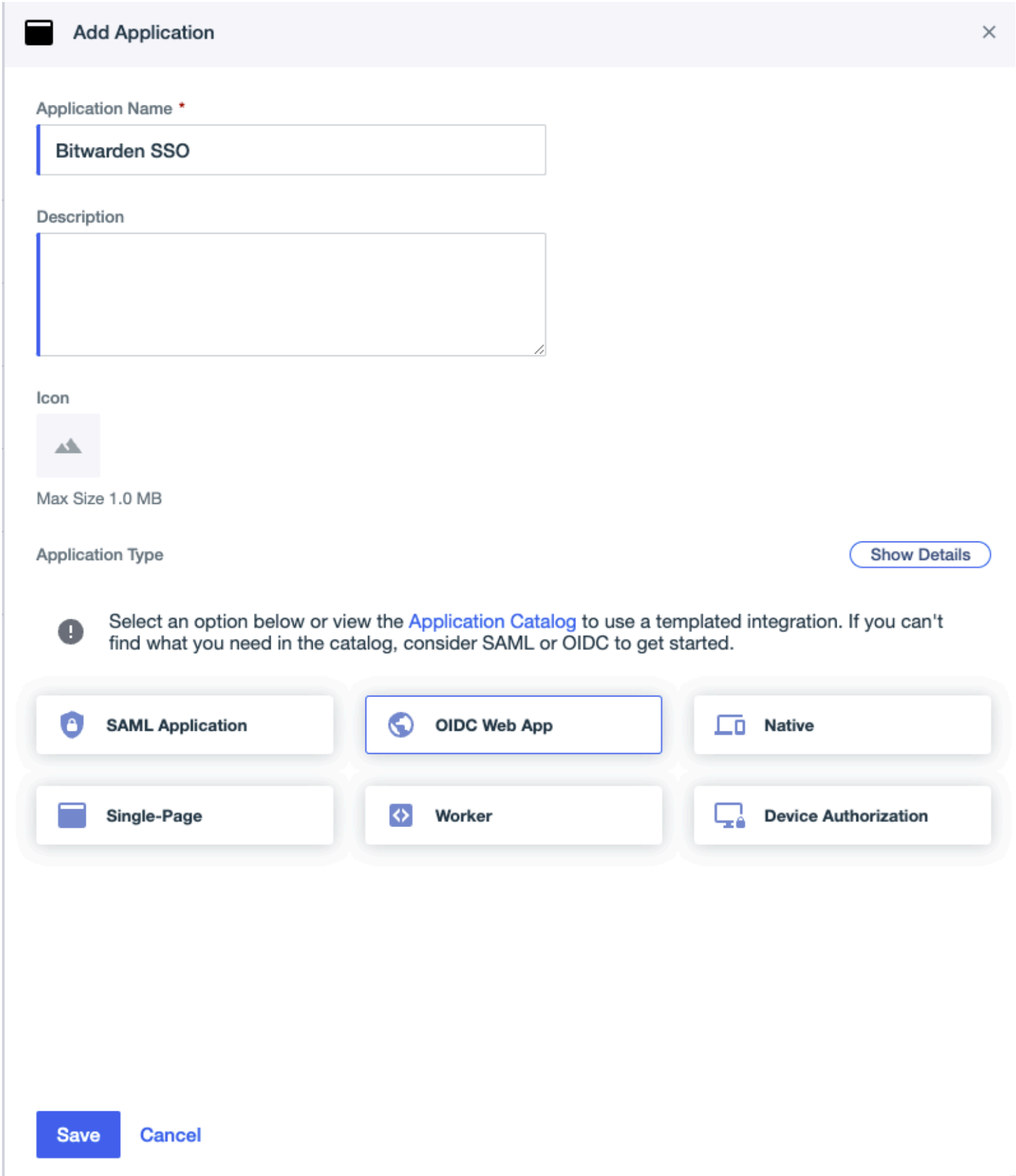
OIDC-Konfiguration

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**
> Es gibt alternative **Mitglied Entschlüsselungsoptionen**. Erfahren Sie, wie Sie mit SSO auf vertrauenswürdigen Geräten oder mit Key Connector beginnen können.

Create OIDC app

In the Ping Identity Administrator Portal, select **Applications** and the ⊕Icon at the top of the screen to open the **Add Application** screen:


Add Application
Application Name *
Bitwarden SSO
Description
Icon
Max Size 1.0 MB
Application Type
Show Details
Select an option below or view the Application Catalog to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.
SAML Application
OIDC Web App
Native
Single-Page
Worker
Device Authorization
Save
Cancel

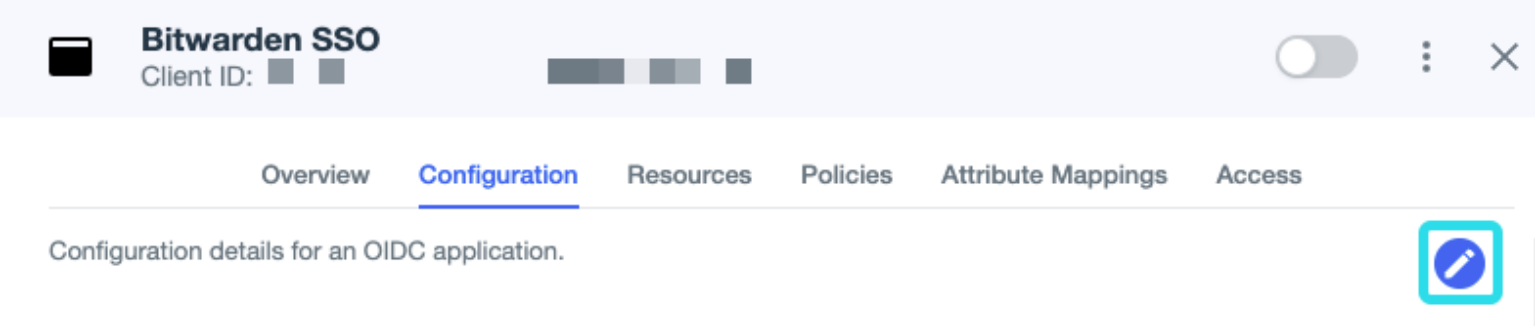
Ping Identity OIDC App

Add application

1. Enter a Bitwarden Specific name in the **Application Name** field. Optionally, add desired description details as needed.
2. Select the **OIDC Web App** option and select **Save** once you have finished.

Configure application

On the Application screen, select the **Configuration** tab and then the edit button located on the top right hand of the screen.



Ping OIDC Configuration Edit

In the edit screen, fill in the following values retrieved from the Bitwarden Single sign-on screen:

Ping Identity Field	Description
Redirect URIs	Copy and paste the **Callback path** value retrieved from the Bitwarden Single sign-on page.
Signoff URLs	Copy and Paste the **Signed out callback path** value retrieved from the Bitwarden Single sign-on page.

Once this step has been completed, select **Save** and return to the **Configuration** tab on the Ping Identity Application screen. No other values on this screen require editing.

Resources

On the Resources tab of the Ping Identity Application screen, select the **edit** icon and enable the following allowed scopes:

- email
- openid

Back to the web app

At this point, you have configured everything you need within the context of Ping Identity. Return to the Bitwarden web app to configure the following fields:

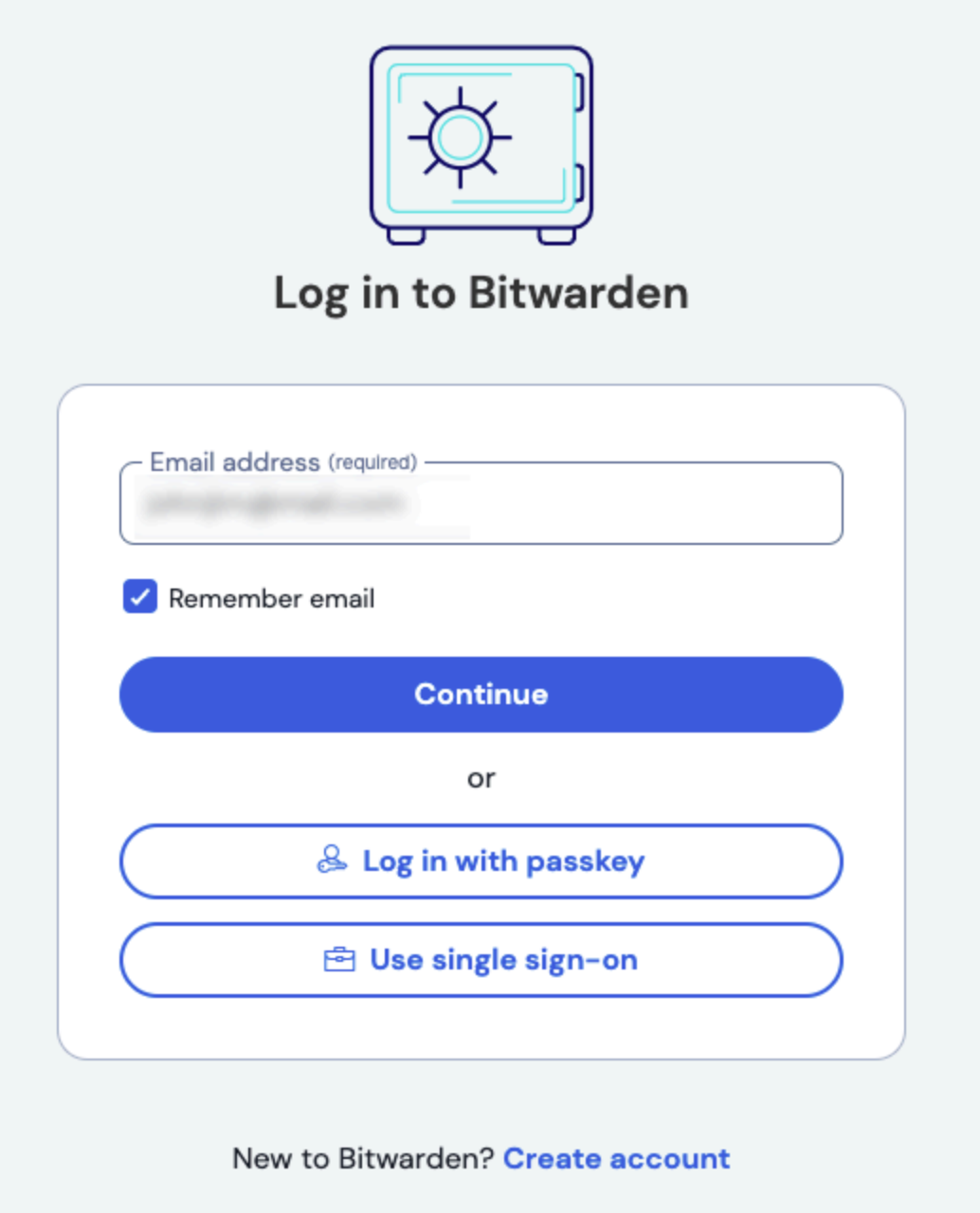
Field	Description
Authority	Enter `https://auth.pingone.eu/<TENANT_ID>`, where `TENANT_ID` is the **Environment ID** on Ping Identity.
Client ID	Enter the App's **Client ID** retrieved from the Application's Configuration tab.
Client Secret	Enter the Secret Value of the created client secret. Select **Generate New Secret** on the application's Configuration tab.
Metadata Address	For Ping Identity implementations as documented, you can leave this field blank.
OIDC Redirect Behavior	Select either **Form POST** or **Redirect GET**.
Get Claims From User Info Endpoint	Enable this option if you receive URL too long errors (HTTP 414), trusted URLS, and/or failures during SSO.
Additional/Custom Scopes	Define custom scopes to be added to the request (comma-delimited).
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**
> Sie können Benutzer dazu auffordern, sich mit SSO anzumelden, indem Sie die Richtlinie für die Authentifizierung mit Single Sign-On aktivieren. Bitte beachten Sie, dass dies auch die Aktivierung der Einzelorganisation-Richtlinie erfordern wird. Erfahren Sie mehr.

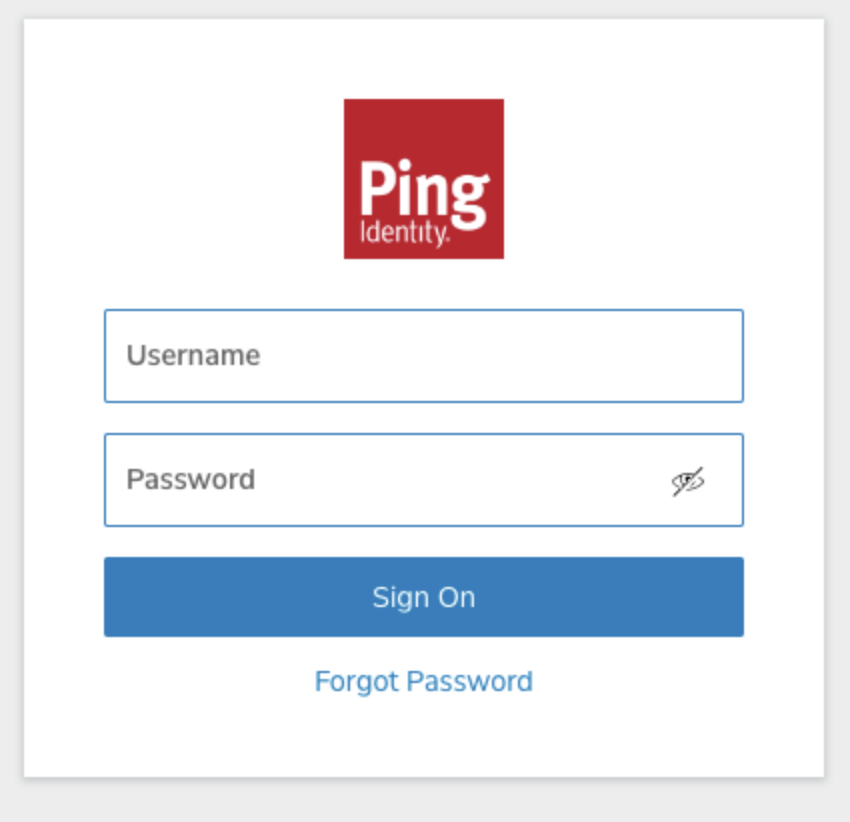
Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address and selecting the **Use single sign-on** button:



Unternehmens Single Sign On und Master-Passwort

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will be redirected to the Ping Identity login screen:



Ping Identity SSO

After you authenticate with your Ping credentials, enter your Bitwarden master password to decrypt your vault!

> **Note**
> Bitwarden unterstützt keine unaufgeforderten Antworten, daher führt das Initiieren von Zugangsdaten von Ihrem IdP zu einem Fehler. Der SSO-Zugangsdaten-Fluss muss von Bitwarden aus initiiert werden.

Next steps

- Educate your organization members on how to use login with SSO.