

ADMIN CONSOLE > LOGGA IN MED SSO >

# Setup SSO with Trusted Devices

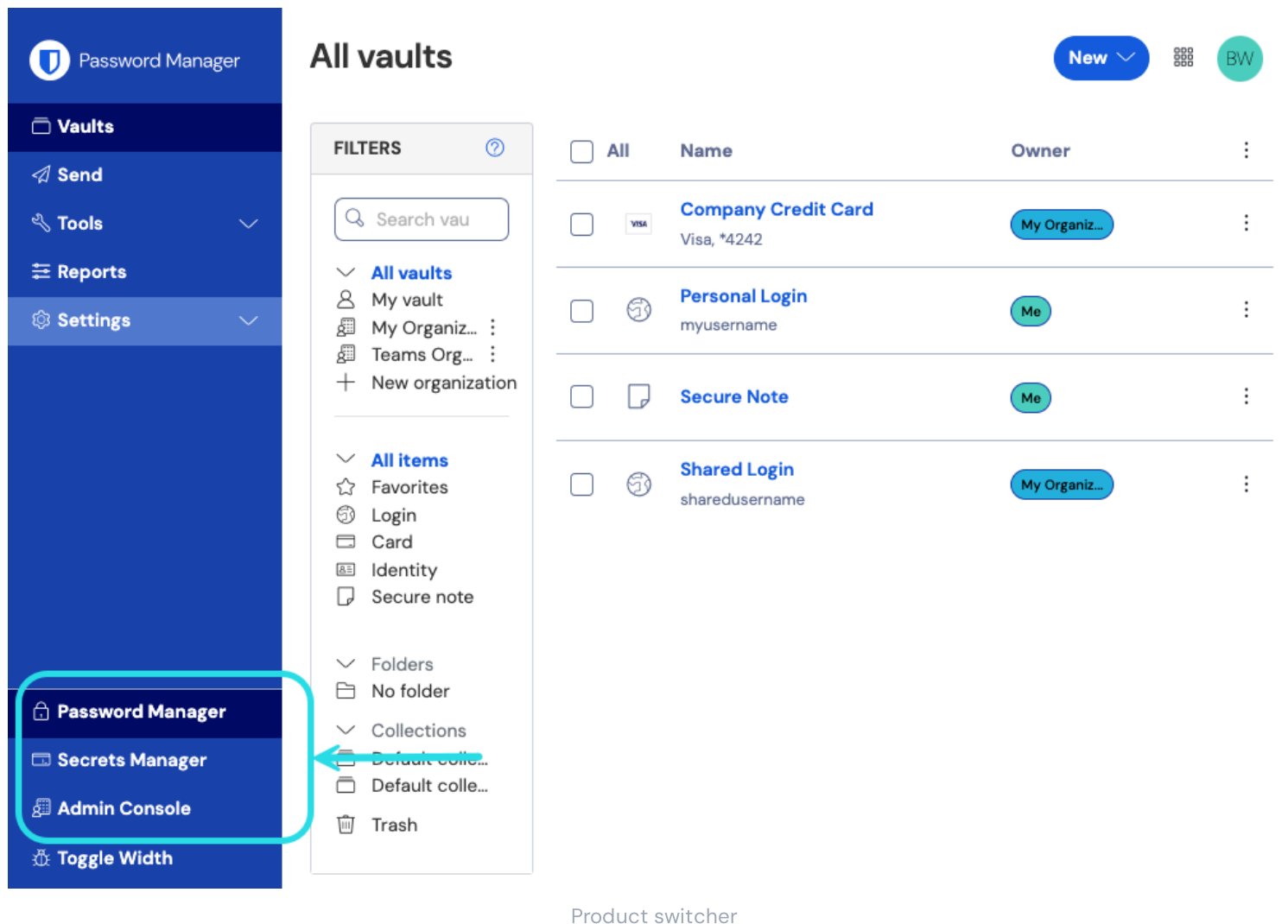
View in the help center:

<https://bitwarden.com/help/setup-sso-with-trusted-devices/>

## Setup SSO with Trusted Devices

This document will walk you through adding [SSO with trusted devices](#) to your organization. You must be an organization owner or admin to complete these steps:

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 Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red box highlights the 'Admin Console' option, with a red arrow pointing to it from the 'Secrets Manager' option. The main content area is titled 'All vaults' and shows a list of vaults with columns for Name and Owner. The vaults listed are: Company Credit Card (Owner: My Organiz...), Personal Login (Owner: Me), Secure Note (Owner: Me), and Shared Login (Owner: My Organiz...). Below the vaults is a 'Product switcher' section.

2. Select **Settings** → **Policies** from the navigation.

3. On the Policies page, activate the following policies which are required for using trusted devices:

- The **Single organization** policy.
- The **Require single sign-on authentication** policy.
- The **Account recovery administration** policy.
- The Account recovery administration policy's **Require new members to be enrolled automatically** option.

#### Note

If you do not activate these policies beforehand, they will be automatically activated when you activate the **Trusted devices** member decryption option. However, if any accounts do not have account recovery enabled, they will need to [self-enroll](#) before they can use [admin approval](#) for trusted devices. Users who enable [account recovery](#) must log in at least once post-account recovery to fully complete the account recovery workflow.

4. Select **Settings** > **Single sign-on** from the navigation. If you haven't setup SSO yet, follow one of our [SAML 2.0](#) or [OIDC implementation](#) guides for help.

5. Select the **Trusted devices** option in the Member decryption options section.

Once activated, users can begin decrypting their vaults with trusted device.

When joining an organization that uses SSO with trusted devices, admins and owners will be prompted to create a master password for redundancy and failover purposes, however members with the user role will not be able to set a master password.

#### Warning

Before migrating from SSO with trusted devices to another member decryption options, please note that:

- When moving from SSO with trusted devices to master password decryption, any organization members without a master password will be prompted the next time they log in to create a master password.
- Moving from SSO with trusted devices to [Key Connector](#) is **not supported**.