ADMIN CONSOLE > LOGIN WITH SSO >

Setup SSO with Trusted Devices
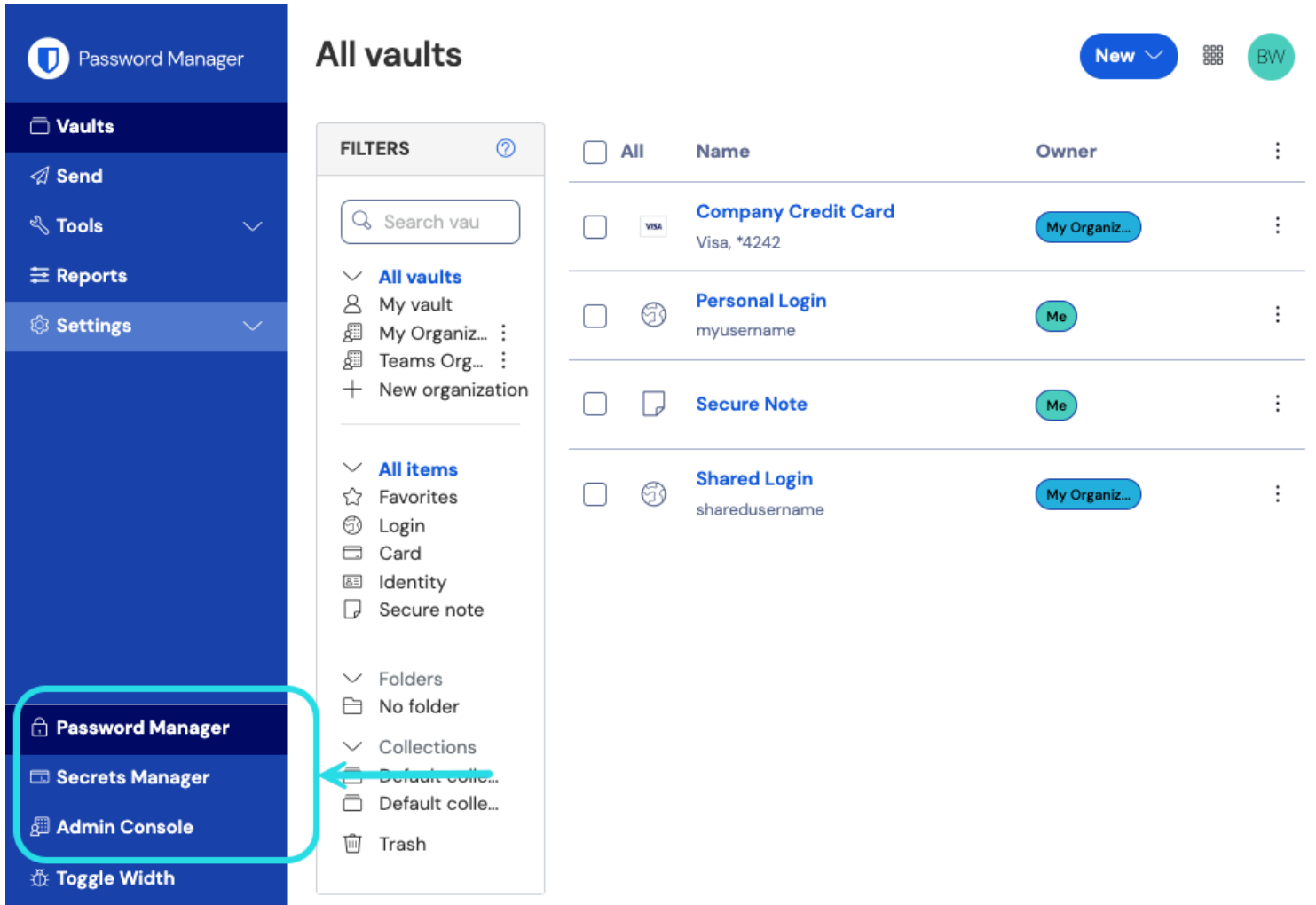
Setup SSO with Trusted Devices

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:

Product switcher

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.

If your desired outcome is to have members without master passwords who can **only** used trusted devices, instruct users to select **Log in → Enterprise SSO** from the organization invite to initiate JIT provisioning. Admins/owners should still use the **Create account** option so that they have master passwords for redundancy and failover purposes.

> ⚠ **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**.