bitwarden | Help Center Article

DOCS › ADMIN CONSOLE › SINGLE SIGN-ON

About Single Sign-On

View in the help center https://bitwarden.com/help/about-sso/

About Single Sign-On

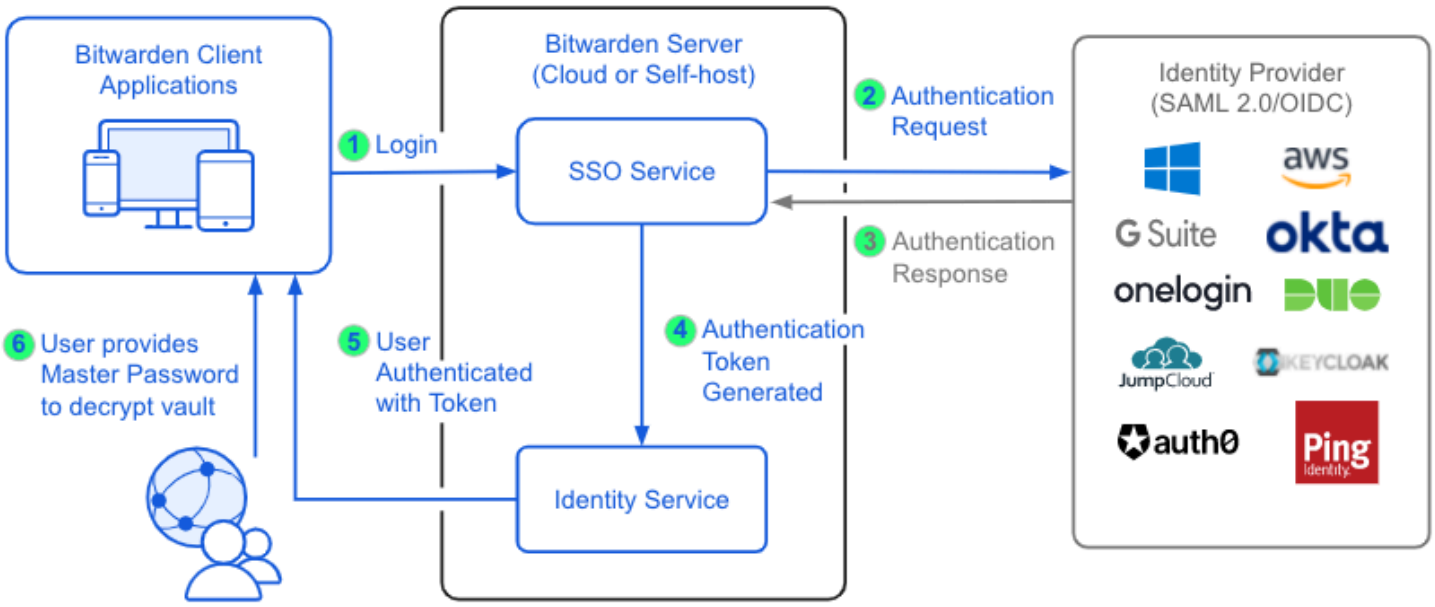
Using single sign-on (SSO), Enterprise organizations can leverage their existing Identity Provider (IdP) to authenticate members with Bitwarden. SSO for Enterprise organizations include:

- SAML 2.0 and OIDC configuration options that support integration with a wide variety of IdPs.
- An enterprise policy to optionally **require** non-administrative members to log in to Bitwarden with SSO.
- An enterprise policy to optionally allow easier auto-fill in non-SSO apps launched from your IdP.
- Several distinct member decryption options for safe data access workflows.
- Just-In-Time (JIT) provisioning of members via SSO.

Tip

Using SSO with Bitwarden retains our zero-knowledge encryption model. Nobody at Bitwarden has access to your data and, similarly, **neither should your Identity Provider**. That's SSO **decouples authentication and decryption**. In all implementations, your Identity Provider cannot and will not have access to the decryption key needed to decrypt vault data.

While authentication is handled via your IdP, decryption of your data is controlled by one of several decryption methods.



SSO and master password decryption

If you're new to Bitwarden, start a 14-day Enterprise free trial to begin testing SSO. We recommend this following steps when testing SSO:

1. Configure your SSO integration using one of the **SSO Guides** for your chosen IdP. If your IdP isn't listed, you can use the generic SAML or generic OIDC guide.
2. Test the member login experience using master password decryption.
3. Assess whether a different member decryption options would fit your implementation, and if so begin configuration of that decryption option.
4. Provide information to members, based on the specifics of your implementation, about how to log in with SSO.