bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO

About Login with SSO

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

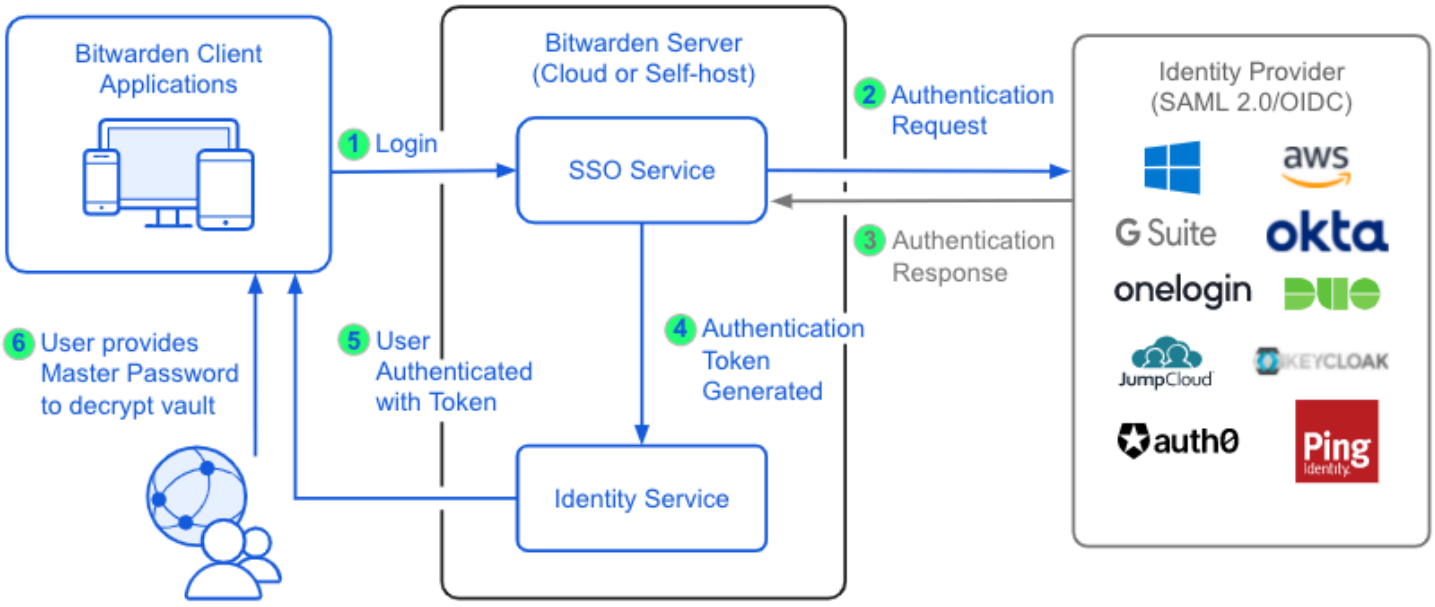
About Login with SSO

What is login with SSO?

Login with SSO is the Bitwarden solution for single sign-on. Using login with SSO, Enterprise organizations can leverage their existing Identity Provider to authenticate users with Bitwarden using the **SAML 2.0** or **Open ID Connect (OIDC)** protocols.

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

In most scenarios, decryption is facilitated by a device key when using SSO with trusted devices or by master password, which users retain sole responsibility for. Organizations self-hosting Bitwarden can alternatively use Key Connector as a means of decrypting vault data.



Login with SSO & Master Password Decryption

> **Note**
>
> Unless you're using trusted devices, login with SSO does not replace the master password and email requirement for logging in. Login with SSO leverages your existing identity provider (IdP) to authenticate you into Bitwarden, however, your master password and email must still be entered in order to decrypt your vault data.
>
> If you're using trusted devices, however, a device-stored encryption key will replace the need to enter a master password to decrypt vault data.

Why use login with SSO?

Login with SSO is a flexible solution that can fit your enterprise's needs. Login with SSO includes:

- SAML 2.0 and OIDC configuration options that support integration with a wide variety of Identity Providers.
- An enterprise policy to optionally require non-owner/non-admin users to log in to Bitwarden with single sign-on.
- Two distinct member decryption options for safe data access workflows.
- "Just-in-time" end-user onboarding via SSO.
- Automatically log in to apps that do not use SSO from your identity provider dashboard.

How do I start using login with SSO?

Login with SSO is available for all customers with an Enterprise organization. If you are new to Bitwarden, we would love to help you through the process of setting up an account and starting your seven day Free trial Enterprise organization with our dedicated signup page:

Start your Enterprise Free Trial

Once you have an Enterprise organization, deployment should include the following steps:

1. Follow one of our SAML 2.0 or OIDC implementation guides to configure and deploy login with SSO with master password decryption.
2. Test the end-user login with SSO experience using master password decryption.
3. (**If self-hosting**) Review our different member decryption options to determine whether using Key Connector might be right for your organization.
4. (**If self-hosting**) If you are interested in implementing Key Connector, contact us and we will help you get started deploying Key Connector.
5. Educate your organization members on how to use login with SSO.