bitwarden | Help Center Article

ADMIN CONSOLE > LOGGA IN MED SSO

Member Decryption Options

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

Member Decryption Options

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.

Member decryption options are used to determine what decryption key will be used to decrypt vault data in scenarios where SSO is handling authentication. Options include:

- **Master password**: Once authenticated, organization members will decrypt vault data using their master passwords.
- **Trusted devices**: Allows users to authenticate with SSO and decrypt their vault using a device-stored encryption key, eliminating the need to enter a master password. Learn more.
- **Key Connector**: Connect login with SSO to your self-hosted decryption key server. Using this option, organization members won't need to use their master passwords to decrypt vault data. Instead, Key Connector will retrieve a decryption key securely stored in a database owned and managed by you.

> **Tip**
>
> Due to the sensitivity of storing decryption keys, the **Key Connector** option is disabled by default and currently only available to organizations self-hosting Bitwarden.
>
> If you're interesting in using Key Connector, check out the About Key Connector and Deploy Key Connector articles and contact us to setup a time for us to help you get started.