bitwarden | Help Center Article

SJÄLVHOTELL > KEY CONNECTOR

About Key Connector

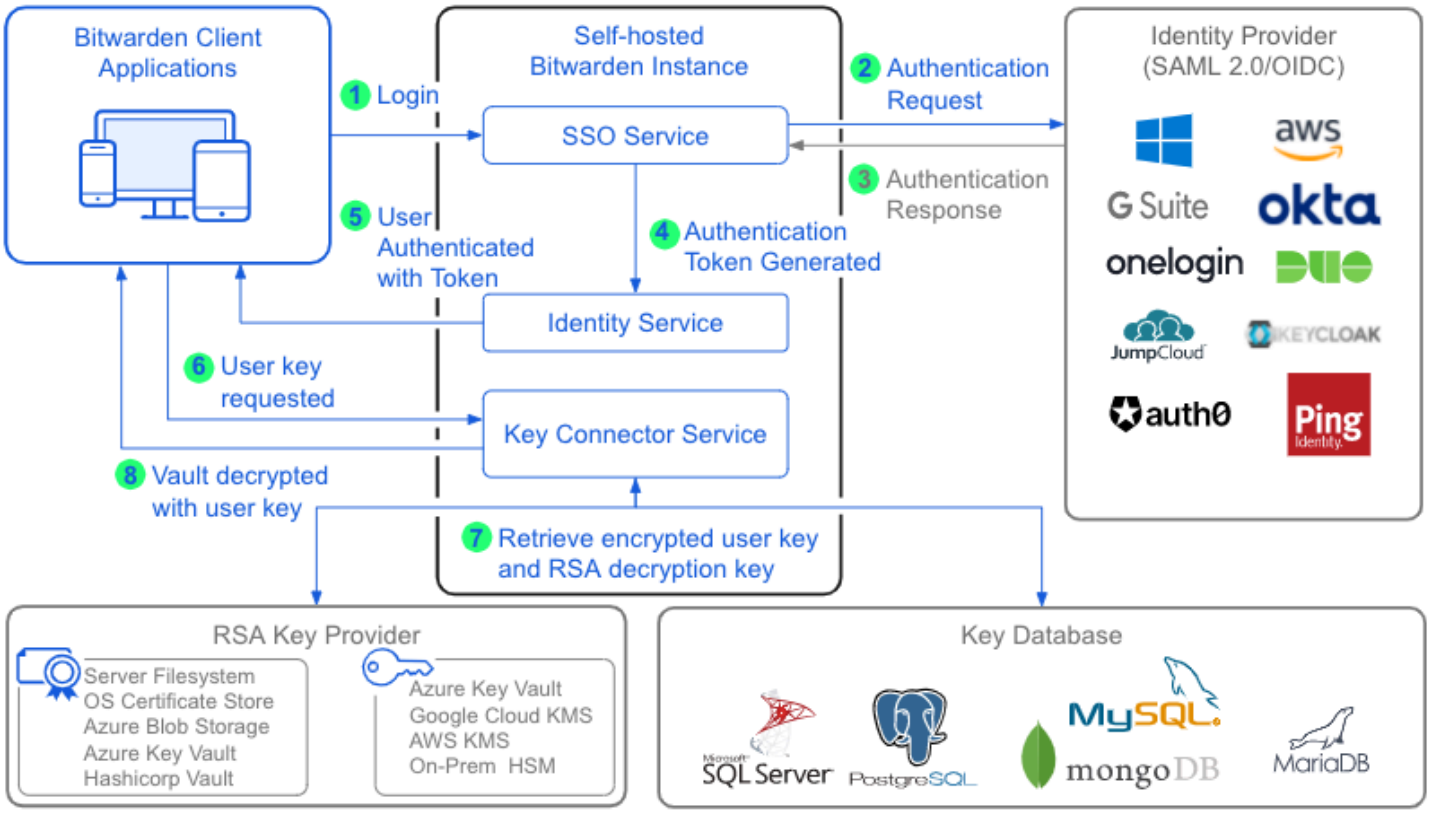
View in the help center:
https://bitwarden.com/help/about-key-connector/

About Key Connector

Key Connector is a self-hosted application that facilitates customer-managed encryption (CMS), allowing an enterprise organization to serve cryptographic keys to Bitwarden clients.

Key Connector runs as a docker container on the same network as existing services, and can be used with login with SSO to serve cryptographic keys for an organization as an alternative to requiring a master password for vault decryption (learn more). Bitwarden supports deployment of one Key Connector for use by one organization for a self-hosted instance.

Key Connector requires connection to a **database where encrypted user keys are stored** and an **RSA Key Pair to encrypt and decrypt stored user keys**. Key Connector can be configured with a variety of database providers (for example, MSSQL, PostgreSQL, MySQL) and key pair storage providers (for example, Hashicorp Vault, Cloud KMS Providers, On-prem HSM devices) in order to fit your business's infrastructure requirements.



Key Connector Architecture

Why use Key Connector?

In implementations that leverage master password decryption, your identity provider handles authentication and a member's master password is required for vault decryption. This separation of concerns is an important step that ensures that only an organization member has access to the key which is required to decrypt your organization's sensitive vault data.

In implementations that leverage Key Connector for decryption, your identity provider still handles authentication, but vault decryption is handled by Key Connector. By accessing an encrypted key database (see the above diagram), Key Connector provides a user their decryption key when they log in, without requiring a master password.

We often refer to Key Connector implementations as leveraging **Customer-Managed Encryption**, because your business has sole responsibility for the management of the Key Connector application and of the vault decryption keys it serves. For enterprises ready to deploy and maintain a customer-managed encryption environment, Key Connector facilitates a streamlined vault login experience.

Impact on master passwords

Because Key Connector replaces master password-based decryption with customer-managed decryption keys, organization members will be **required to remove the master password from their account**. Once removed, all vault decryption actions will be conducted using the stored user key. Besides logging in, this will have some impacts on offboarding and on other features you should be aware of.

> ⚠ **Warning**
>
> Currently, there is not a way to re-create master passwords for accounts that have removed them.
>
> For this reason, organization owners and admins are not able to remove their master password and must continue using their master password even if using SSO. It is possible to elevate a user who has removed their master password to owner or admin, however we **strongly recommend** that your organization always have at least one owner with a master password.

Impact on organization membership

Key Connector requires users to remove their master passwords and instead uses a company-owned database of cryptographic keys to decrypt users' vaults. Because master passwords can not be re-created for accounts that have removed them, this means that once an account uses Key Connector decryption it is for all intents and purposes **owned by the organization**.

These accounts **may not leave the organization**, as in doing so they would lose any means of decrypting vault data. Similarly, if an organization administrator removes the account from the organization, the account will lose any means of decrypting vault data.

Impact on other features

Feature	Impact
Verification	There are a number of features in Bitwarden client applications that ordinarily require entry of a master password in order to be used, including exporting vault data, changing two-step Login settings, retrieving API keys, and more. **All these features** will replace master password confirmation with email-based TOTP verification.
Vault lock/unlock	Under ordinary circumstances, a locked vault can be unlocked using a master password. When your organization is using Key Connector, locked client applications can only be unlocked with a PIN or with biometrics. If neither PIN nor biometrics are enabled for a client application, the vault will always log out instead of lock. Unlike unlocking, logging in **always** requires a connection to your self-hosted server (learn more).

Feature	Impact
Master password re-prompt	When Key Connector is being used, master password re-prompt will be disabled for any user that has removed their master password as a result of your Key Connector implementation.
Admin password reset	When Key Connector is being used, admin password reset will be disabled for any user that has removed their master password as a result of your Key Connector implementation.
Emergency access	When Key Connector is being used, the emergency access account takeover option will be disabled for any user that has removed their master password as a result of your Key Connector implementation. Trusted emergency contacts may still **View** a grantor's individual vault data, subject to the established emergency access workflow.
Change email	When Key Connector is being used, a user's vault email address cannot be changed.

How do I start using Key Connector?

In order to get started using Key Connector for customer-managed encryption, please review the following requirements:

> ⚠ **Warning**
>
> Management of cryptographic keys is incredibly sensitive and is **only recommended for enterprises with a team and infrastructure** that can securely support deploying and managing a key server.

In order to use Key Connector you must also:

- Have an Enterprise organization.
- Have a self-hosted Bitwarden server.
- Have an active SSO implementation.
- Activate the single organization and require single sign-on policies.

If your organization meets or can meet these requirements, including a team and infrastructure that can support management of a key server, contact us and we will activate Key Connector.