RESOURCE CENTER

Choose the Right SSO Login Strategy

Why zero knowledge encryption is fundamental to how Bitwarden designs SSO integrations.

Get the full interactive view at
https://bitwarden.com/resources/choose-the-right-sso-login-strategy/

bitwarden

With cybersecurity as a top priority, many businesses deploy single sign-on (SSO) to reduce the number of employee login IDs and passwords. In addition to increasing security, single-click access through SSO helps improve the user experience and enhance productivity.

Bitwarden understands why enterprises choose to adopt SSO, and offers multiple authentication options to deliver the right configuration for each company's needs.

These implementation offerings align with Bitwarden foundational design goals and our engineering approach, which starts with the concept of zero knowledge encryption.

Additional Resources

Guide: Enterprise Reference Guide to Bitwarden Authentication

Help Article: How to Deploy Login with SSO and Customer Managed Encryption with a Key Connector

Blog: How Zero Knowledge Paves the Way to End-End-Encryption

Explore Bitwarden Login with SSO and customer managed encryption with a free 7-day business trial.

Zero Knowledge Encryption: The Definitive Security Approach

Bitwarden builds on the principle of zero knowledge encryption, which means that everything you store in a Bitwarden vault is encrypted and cannot be viewed by anyone but yourself or authorized users within your company. Most password managers implement a zero knowledge encryption approach albeit to varying degrees. Bitwarden combines end-to-end encryption and complete zero knowledge encryption so nobody, not even Bitwarden, has access.

> *Quick Reference*
>
> *In **end-to-end encryption**, encryption and decryption occurs at the device level. Vault data is encrypted before leaving the phone or computer and decrypted at the destination. Bitwarden uses AES-CBC 256 bit encryption, salted hashing, and PBKDF2 SHA-256 to protect all vault data.*

*With **zero-knowledge encryption**, Bitwarden team members cannot access any of your information. Instead, your data remains end-to-end encrypted with your email and master password.* Of course, not all commercial applications and services are built - or need to be built - with this framework. In non-encrypted applications, usernames and passwords provide access. With no encryption protocol in place, software providers can access any user data stored within the application.

When a user logs into Bitwarden, an encrypted application, two things happen: authentication and decryption. The user must first authenticate themselves to access encrypted vault data, which is then decrypted locally with the user's key, derived from their master password. For the majority of Bitwarden users, their master password enables both of those steps. It serves as the authentication agent as well as the decryption key.

Businesses looking to leverage SSO with Bitwarden should consider the flexible options Bitwarden provides.

Uniquely Handling SSO with Encrypted Applications

With SSO and non-encrypted applications, users authenticate with one set of credentials to access multiple applications. In many cases, that's all corporate end-users need. SSO only takes care of authentication in these cases as there is no encrypted information.

To maintain zero knowledge encryption, Bitwarden separates authentication and decryption into two discrete steps for SSO: authentication through the SSO provider, then decryption and vault access through a master password. As a result, decryption keys never pass through Bitwarden servers and users maintain credentials for SSO, and their own decryption key for Bitwarden.

Maintaining Zero Knowledge Encryption with SSO

To best serve a range of enterprises with differing IT resources and ecosystems, Bitwarden offers two deployment options for integrating its solution with SSO.

SSO with trusted devices

This option provides an enterprise passwordless experience for employees through a trusted device model, bringing ease, speed, and scale to the overall login process. Once their devices are registered and confirmed, a user simply needs to be authenticated with the SSO to access encrypted vault data. An encryption key used as part of the decryption process is securely stored on the device, so once the SSO service authenticates the user, the device is able to decrypt the data without additional user input.

Learn more about SSO with trusted devices here

Login with SSO

Login with SSO uses the SSO provider for authentication and then a Bitwarden master password from the user to decrypt their data. This is the simplest deployment option for IT teams to retain the SSO authentication process, and maintain a unique password for decryption with a zero-knowledge encryption model.

Learn more about login with SSO here

Login with SSO and customer managed encryption

This option integrates the steps to decrypt user data, where IT admins deploy and manage a key connector application (or a key management server) to retain user's encryption keys for Bitwarden vaults.

Through a self-hosted key server, companies store, manage, and automatically deliver the keys to decrypt users' data as they sign into Bitwarden through SSO. The process maintains zero knowledge encryption on the Bitwarden side, and is seamless to users—they login via SSO and immediately access their decrypted Bitwarden vault, all in one step.

Because the key server holds sensitive user data, it's critical that companies understand how to deploy, back up, and maintain the server and implement stringent security policies. Management of cryptographic keys is incredibly sensitive and is only recommended for enterprises with a team and utilizing infrastructure that has already securely deployed and managed a key server.

The most comprehensive SSO integration options available

Bitwarden is committed to protecting businesses and making password security easy for end users. Bitwarden SSO options promote and drive user adoption and simplify the user experience while staying true to the zero-knowledge encryption approach.

When you choose Bitwarden, you get the flexibility of using any identity provider that supports SAML or OpenID standards. The unique combination of choosing your own identity provider, coupled with the SSO options Bitwarden offers, means companies can deploy the right authentication and decryption model with a trusted, open source approach.