RESOURCE CENTER

Enterprise Reference Guide to Bitwarden Authentication

Outlining critical capabilities around Bitwarden authentication and SSO offerings

Get the full interactive view at https://bitwarden.com/resources/reference-guide-bitwarden-authentication/

bitwarden

Authentication type	What is it?	Deployment considerations *All authentication deployment options align with the Bitwarden end-to-end, zero knowledge encryption model*
SSO with trusted devices	For a passwordless experience, employees use their SSO credentials to authenticate and decrypt in a single step. Registered, trusted devices are able to decrypt vaults and confirm and accept new devices. Once a device is trusted it does not need approval again.	Selecting this option will allow employees to log in and decrypt their vaults without needing a password. Trusted devices are registered and can confirm logins and extend trust to other devices. On account creation, the SSO provider will authenticate the user and register logging-in client as the first trusted device, allowing it to decrypt the vault. Additional trusted devices can be registered with approval from the Bitwarden desktop app, mobile app, web app, or by a Bitwarden administrator. Each trusted device has an individual device encryption key, and zero-knowledge, end-to-end encryption and security is maintained across devices. Additional resources: Set up SSO with trusted devices Enterprise passwordless SSO brings better productivity and user sign in experience for employees
Login with SSO	User authentication is separated from vault decryption by leveraging your company's identity provider to authenticate users into their Bitwarden vault and using master passwords for decryption of vault data.	This option supports identity providers using SAML 2.0 or OpenID Connect standards. Selecting this option means that anytime an employee logs into Bitwarden using SSO, they'll need to use their master password to decrypt their vault, protecting your businesses' critical credentials and secrets. Additional resources: Configure Your Organization Using Login with SSO Setting up Login with SSO

Authentication type	What is it?	Deployment considerations *All authentication deployment options align with the Bitwarden end-to-end, zero knowledge encryption model*
Login with SSO and customer-managed encryption	Employees use their SSO credentials to authenticate and decrypt all in a single step. This option shifts retention of the users master passwords to companies requiring the business to deploy a key connector to store the user keys.	For companies with widely adopted SSO implementations, and the desire to integrate authentication and decryption in an on-premises solution, Bitwarden offers SSO with customer-managed encryption. In this scenario, companies manage a key connector agent. This requires a connection to a database that stores encrypted user keys, and an RSA key pair to encrypt and decrypt those keys. This approach maintains a zero knowledge encryption architecture because no decryption keys pass through Bitwarden servers at any point. 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. SSO with customer-managed encryption is available for customers self-hosting Bitwarden. Additional resources: Whitepaper: Choose the Right SSO Login Strategy Help article: Login with SSO and Customer Managed Encryption - deploying the key connector
Login with Bitwarden	Employees use their email and master password to login and decrypt their Bitwarden vault.	For companies that want to get started quickly, login with Bitwarden allows employees to use their unique email and master password to access their vault. It is perfect for companies that do not yet centrally manage authentication or use an identity provider. Administrators can manually invite employees into Organizations and shared Collections, or use the Bitwarden Directory Connector to synchronize LDAP groups Additional resources: Five Best Practices for Password Management

Authentication type	What is it?	Deployment considerations *All authentication deployment options align with the Bitwarden end-to-end, zero knowledge encryption model* Getting Started with Bitwarden
Login with device	Employees use their email to login and then confirm the login from a second, authenticated device (mobile app or desktop app) that securely shares the vault encryption key on approval.	Login with device is an available option to all employees after they have logged in with email and master password at least once on the device. This allows employees to quickly log back in to all of their Bitwarden clients after first logging into their mobile or desktop app. Additional resources: Help Article: Login with Device