bitwarden | Help Center Article

ADMIN CONSOLE > SINGLE SIGN-ON

SSO FAQs

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

SSO FAQs

This article contains frequently asked questions (FAQs) regarding **SSO**. For more high-level information about SSO, refer to About Single Sign-On.

Everyday use

Q: Will changing my IdP password change my Bitwarden master password?

A: No, a user's master password it will not change when they change the password they use for the IdP.

Q: Can I still authenticate with my master password if my organization uses SSO?

A: Unless the organization has activated the Require single sign-on authentication policy, members with the user role can still authenticate with a master password if they have one, however some decryption options might remove or prevent them from having a master password.

Q: Do I need to enter my SSO identifier every time I login?

A: No. Bookmark this page with your identifier included in the URL, for example `https://vault.bitwarden.com/#/sso?identifier=my-identifier` so that you don't have to enter it each time you log in. Administrators can also set up a claimed domain to automatically bypass this step for members if they have an email address with a matching domain.

Configuration

Q: Is SSO compatible with SCIM or Directory Connector?

A: Yes. Organizations may choose to leverage either of these to sync groups and group memberships.

Q: How do I change pre-generated SSO configuration values?

A: Pre-generated SSO configuration values including **SP Entity ID**, **SAML 2.0 Metadata URL**, **ACS URL**, and **Callback Path** can be changed in self-hosted environments by changing the `url:` value in `.bwdata/config.yml` and running the `./bitwarden.sh rebuild` command to apply your change.

These cannot be changed on Cloud, however cloud organizations can set whether to generate a unique or generic **SP Entity ID** from the Single Sign-on configuration page.

Q: What is the SSO identifier used for?

A: The SSO identifier is used in some member login workflows to indicate the organization to be logged in to with SSO. This value can human-readable and should indicate to members that it's attached to your organization. Administrators can set up a claimed domain to automatically bypass this step for members if they have an email address with a domain that matches the one they've claimed.

Supportability

Q: Does Bitwarden support OAuth 2.0?

A: Bitwarden supports OpenID Connect, but does not support OAuth at this time.

Q: Will SSO work with a self-hosted Bitwarden server?

A: Yes, as long as the identity server is reachable by the server.

Q: Will SSO work across hybrid cloud environments?

A: Yes, as long as the identity server is reachable by the server.

Q: If my identity provider goes offline, can members still authenticate?

A: If the identity provider goes offline, members can log in using email and master password if they have master passwords and if the organization's policy options permit.