bitwarden | Help Center Article

ADMIN CONSOLE > LOGIN WITH SSO

Login with SSO FAQs

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

Login with SSO FAQs

This article contains frequently asked questions (FAQs) regarding **login with SSO**. For more high-level information about **login with SSO**, refer to about login with SSO

Using login with SSO

Q: Does SSO authentication replace my master password and email?

A: If your organization is using SSO with trusted devices or using Key Connector to self-host decryption keys, the login with SSO workflow does replace the need to enter a master password to log in. In the standard SSO workflow, Bitwarden leverages your existing identity provider (IdP) to authenticate you, however your master password and email must still be entered in order to decrypt your vault data.

Q: Why does login with SSO require my master password?

A: Unless your organization uses SSO with trusted devices, users must enter their master password when logging in with SSO to decrypt their vault, protecting your businesses' critical credentials and secrets.

Login with SSO retains our end-to-end zero knowledge encryption model; nobody at Bitwarden should have access to your vault data and, importantly, **neither should your identity provider**. That's why the Bitwarden login with SSO offering **decouples authentication and decryption**. Your IdP can confirm that Alice is, in fact, Alice, but cannot and should not have the tools to decrypt Alice's vault. Only Alice can have that tool and, in the standard login with SSO flow, it's her master password. Learn how data is decrypted when using SSO with trusted devices instead.

> ⓘ **Note**
>
> Bitwarden offers two solutions for organizations that will allow approved organization members to access their Bitwarden account without using a master password:
>
> **SSO with trusted device** Is a feature that allows organizations using login with SSO to create and store member device encryptions keys, eliminating the need to enter a master password. Learn more about SSO with trusted devices.
>
> **Organizations self-hosting Bitwarden** can leverage Key Connector to serve decryption keys to Bitwarden clients instead of requiring users to decrypt vault data with their master passwords. Learn more here and here.

Q: Will changing my SSO password affect my Bitwarden master password?

A: No, your master password will remain the same. Unless your organization is using SSO with trusted devicesor using Key Connector to self-host decryption keys, your master password must be used to decrypt vault data.

Q: Can I still log in with my master password if my organization has SSO enabled?

A: By default, yes, you can use your email address and master password to login to Bitwarden. However, if your organization enables both the single organization and Single sign-on authentication policies, or if your organization uses Key Connector, all non-administrator users will be required to login with SSO.

Q: How does login with SSO work for new users ("just-in-time")?

A: New users who are authorized to use the Bitwarden application within the IdP and select **Log in** → **Enterprise SSO** on the Bitwarden login page will be placed in the `Accepted` status of their organization until they are confirmed by an administrator.

When that user is assigned to a group manually or via Directory Connector, they will receive access to the appropriate shared items. JIT provisioning is recommended if your desired outcome is to have members without master passwords who can only used trusted devices.

Q: Do I still need to use Bitwarden Directory Connector?

A: If you manage your Bitwarden group and collection assignments directly within Bitwarden, there is no need to leverage the Directory Connector. However, if you would like to have groups and users automatically synchronized with your organizations directory, we recommend using login with SSO in conjunction with Directory Connector for the most complete solution.

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

A: Nope! If your organization is using domain verification you won't need to enter this identifier. Otherwise, admins should distribute the one of following URLs, where `{your-sso-identifier}` is your organization's SSO identifier, to automatically redirect users to the SSO login screen:

- `https://vault.bitwarden.com/#/sso?identifier={your-sso-identifier}` for US cloud-hosted instances
- `https://vault.bitwarden.eu/#/sso?identifier={your-sso-identifier}` for EU cloud-hosted instances
- `https://your.domain.com/#/sso?identifier={your-sso-identifier}` for self-hosted instances

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.

Security

Q: How does login with SSO work with the zero knowledge encryption model?

A: Logging in to Bitwarden with SSO credentials only performs user authentication and does not decrypt user data. In most scenarios, decryption is facilitated by a device key when using SSO with trusted devices or by master password, which users retain sole responsibility for. Organizations self-hosting Bitwarden can alternatively use Key Connector as an alternative means of decrypting vault data. Adding SSO functionality does not introduce any further individually identifiable information into the Bitwarden database.

Billing

Q: What plans offer login with SSO?

A: Our Enterprise plan offers this feature.

Q: How do I upgrade my plan so that I can use login with SSO?

A: In the Admin Console, navigate to the **Subscriptions** → **Billing** page and select **Upgrade Plan**. We highly recommend you test login with SSO by starting a 7 Day Enterprise Free Trial.

Supportability

Q: Does Bitwarden support OAuth 2.0?

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

Q: Will login with SSO work with a self-hosted instance of Bitwarden?

A: Yes! Login with SSO will work with self-hosted instances regardless of whether they are on-premises or in your own cloud, as long as your identity server is reachable from the instance.

Q: Does login with SSO work across hybrid cloud environments?

A: Yes! Login with SSO only requires the ability to connect to your identity provider from your instance of Bitwarden. It can be used with cloud or on-premises identity providers, as well as cloud or self-hosted Bitwarden instances.

Q: If my identity provider is offline, can users login with SSO to authenticate into Bitwarden?

A: If your identity provider is offline, users must log in using their email and master password. This may change in the future as we enable further authentication control mechanisms for organizations.