bitwarden | Help Center Article

ADMIN CONSOLE > SINGLE SIGN-ON

JIT Provisioning

View in the help center:
https://bitwarden.com/help/jit-provisioning/

JIT Provisioning

Enterprise organizations using SSO support Just-In-Time (JIT) provisioning of members. No extra configuration, beyond the SAML or OIDC setup processes documented in the **SSO Guides**, is required to support JIT.

Recommended JIT strategy

An optimized JIT provisioning strategy can make for one of the simplest signup processes available for your members. As an administrator, help your members join quickly and easily by noting the following:

- **Do** issue email invitations to members with SCIM, with Directory Connector, or manually.
  - An added benefit of using SCIM or Directory Connector is that groups and group membership can be synced to your organization, which JIT on its own does not support, automatically assigning members to groups for streamlined collection assignment.
- **Do not** allow members to preemptively create Bitwarden accounts before being invited to the organization.

> **Tip**
>
> Invitation-initiated JIT provisioning of new accounts bypasses a few steps that admins or members might otherwise need to take (see **Non-standard signup**). This strategy also ensures that members who should not have master passwords, as a result of a trusted devices or Key Connector implementation, will not have one set on their accounts.

Member signup process

Members provisioned with the **Recommended JIT strategy** will only need to:

1. Select the **Finish account setup** button contained in the organization invitation email.
2. When prompted, log in to their IdP with their SSO credentials. If they have an active session with the IdP, this step is skipped.
3. Depending on your organization's chosen decryption method:
   - If **master password decryption**, create a master password.
   - If **trusted device decryption**, choose whether to remember the device.

Once complete, members will be moved to the `Accepted` state. At that time, they will need to be confirmed by an administrator.

Non-standard signup

In cases that deviate from the **Recommended JIT strategy**, the signup process for members will be somewhat different:

⇒No invitations sent

In cases where invitations were not sent to members, the organization can still be joined with relative ease. Instruct members to follow these instructions, unless they need to join with a pre-existing Bitwarden account, in which case refer to the **Pre-existing account** tab.

> **Tip**
>
> Unless your organization has already claimed a domain, an administrator will need to provide the SSO identifier to members. They'll need to enter it during the signup process.

⇒Pre-existing account

> **⚠ Warning**
>
> A member who needs to follow this process, unlike a member who follows the standard **Member signup process** for an organization that uses trusted device decryption, will have a master password set on their account. If it is required that organization members do not have master passwords, instruct the user to:
>
> 1. Export data from the pre-existing account.
> 2. Delete the pre-existing account.
> 3. JIT provision a new Bitwarden account following the standard **Member signup process**.
> 4. Import data from the pre-existing account to the new one.

In cases where the member needs to join the organization with a pre-existing Bitwarden account:

1. As an administrator, issue an email invitation to the email address associated with the member's Bitwarden account. This member won't be able to join your organization unless through an email invitation.
2. Instruct the user **Accept Invitation** and, on the log in screen the invitation leads to, to log in with their master password. This member won't be able to use SSO until they're confirmed to the organization, even if the Require single sign-on authentication policy is activated.
3. Once confirmed, the member can use SSO to log in and, if the Require single sign-on authentication policy is activated, will be required to do so.