

SELF-HOSTING

Migration Procedures

A decorative graphic consisting of numerous thin, light blue wavy lines that create a sense of motion and depth, filling the lower half of the page.

Migration Procedures

This article will walk you through procedures for transitioning from cloud to self-hosted, from self-hosted to cloud, and from one self-hosted server to another:

⇒ Cloud to self-hosted

To migrate from the cloud to a self-hosted server:

1. [Install and deploy](#) Bitwarden to your server. At a high-level, this procedure involves:
 1. [Configuring a domain](#) for Bitwarden.
 2. Installing [Docker and Docker Compose](#).
 3. Running the [installation shell script](#).
 4. [Configuring your environment](#) to setup the admin portal, an SMTP server connection, and more.
2. Start your server by running `./bitwarden.sh start`.
3. Open the cloud web vault and [download your license](#).

💡 Tip

There are separate files for an [organization license](#) and an [individual license](#). **You don't need both license files.** If you are migrating an organization, you only need to retrieve the organization license and must be an [organization owner](#) to do so.

4. Still in the cloud web vault, [export your individual vault data](#), [export your organization vault data](#), or [secrets data](#). If you are migrating an organization, encourage your end-users to export their individual vaults as well.
5. Open your self-hosted web vault and create an account. This account **must use the same email address** as the cloud account you downloaded the license with.
6. Still in your self-hosted web vault, upload your [license](#).

💡 Tip

There are separate locations in which to upload an [organization license](#) or an [individual license](#). As before, only upload the one that's relevant for you.

7. Still in the self-hosted web vault, import your [individual vault data](#), [organization vault data](#), or [secrets data](#).

📌 Note

Importing data to an organization will automatically re-create your [collections](#) and add the relevant vault items to them.

Organizations-only next steps

If you are migrating an organization to a self-hosted server, continue with the following steps:

1. **(Enterprise organizations only)** Re-implement your [enterprise policy](#) specifications and/or configure [login with SSO](#).
2. Manually [re-create user groups](#) in your self-hosted web vault and assign them to the proper collections.

3. Start [inviting users to your organization manually](#) or using [directory connector](#).

⇒Self-hosted to cloud

To migrate from a self-hosted server to the cloud:

1. Create a full backup of the `./bwdata` directory of your self-hosted Bitwarden server. In particular, you will need access to `./bwdata/core/attachments` to manually upload [file attachments](#) to the cloud (**Step 5**).

💡 Tip

If users are exporting their individual vaults over a period of time, you may need to re-sync the items from your `./bwdata/core/attachments` directory to your backup location and upload any new items in the event that they change during the cut-over period.

2. In your self-hosted web vault, [export your individual vault data](#) or [export your organization vault data](#). If you are migrating an organization, encourage your end-users to export their individual vaults as well.
3. Open the cloud web vault. Most users will have previously created cloud accounts for billing purposes, so log in to that account. If you were previously a free user without a cloud account for billing, create an account now.

💡 Tip

If you are migrating an organization, you will already have a cloud organization established for billing and licensing purposes. For smoothest transition, we recommend using this already-established organization rather than [creating a new one](#).

4. Still in the cloud web vault, import data to your [individual vault](#) or [organization vault](#).

📌 Note

Importing data to an organization will automatically re-create your [collections](#) and add the relevant vault items to them.

5. Manually upload [file attachments](#) to your individual or organization vault.

Organizations-only next steps

If you are migrating an organization to the cloud, continue with the following steps:

1. (**Enterprise organizations only**) Re-implement your [enterprise policy](#) specifications and/or configure [login with SSO](#).
2. Manually [re-create user groups](#) in the cloud and assign them to the proper collections.
3. Start [inviting users to your organization manually](#) or using [directory connector](#).

⇒Host to host

💡 Tip

These instructions are currently only for migration from one Linux self-hosted server to another Linux self-hosted server.

To migrate from one self-hosted Bitwarden server to another:

1. Stop your existing Bitwarden server by running `./bitwarden.sh stop`. When you run this command, Bitwarden will go down for anyone currently using it.
2. Make a full copy of the `./bwdata` directory of the **old** server. This copy will be used to recreate your configuration, database, attachments, and more, for the new server.
3. [Install and deploy](#) Bitwarden to your new server.
4. Once the new Bitwarden server is set up, replace the newly-created `./bwdata` directory with the copy from the old server.
5. Print the new Bitwarden server's UID by running `id -u bitwarden`.
6. Open the file `./bwdata/env/uid.env` and check that the listed values match what was printed in the previous step. If they do not match, replace **both** values with the result of `id -u bitwarden`.
7. If you specified a different server domain during **Step 2**, edit the following:
 - In `./bwdata/config.yml`, change the `url:` value to the new domain.
 - In `./bwdata/env/global.override.env`, change `globalSettings__baseServiceUri__vault=` to the new domain.
8. Run `./bitwarden.sh rebuild` to apply changes to `config.yml` and `global.override.env`.
9. Start your Bitwarden server with `./bitwarden.sh start`.

⇒ Cloud to cloud

To migrate from one Bitwarden cloud server to another, for example, from a [US server](#) to [EU server](#):

1. [Export your organization vault](#) and instruct all organization members to [export their individual vaults](#).

Tip

Laden Sie einzelne Dateianhänge für Tresor-Einträge herunter und notieren Sie, zu welchen Einträgen sie gehören.

2. Create a new Bitwarden account in the desired region and start a trial organization. Bitwarden support will be able to migrate your subscription to the new region (see **Step 4**).
3. Set up your new organization, configuring things like enterprise policies, login with SSO, constructing group-collection relationships, and inviting users with Directory Connector or SCIM. For help, refer to the [Proof-of-Concept Checklist](#).
4. [Contact Bitwarden support](#) to move your new organization off of trial and resume your subscription in your new region.
5. Import your organization vault data obtained in **Step 1**, and instruct organization members to import their individual vaults as well.

Note

Laden Sie die in **Schritt 1** erhaltenen Dateianhänge manuell wieder hoch zu den Tresor-Einträgen, mit denen sie verbunden waren.

Migration FAQs

Q: Do I need to migrate?

A: Migrating regions is not required. The region selector allows organizations to specify the geographic location of vault data. Features and functions are identical across regions.

Q: Is there a process for migrating?

A: Bitwarden regions are distinct cloud environments. Bitwarden cannot migrate accounts from one region to another for customers. A script is available for organizations to help facilitate migrations. Subscriptions can be transferred from one region to another region by [contacting us](#).

Q: What does the migration script do?

A: The script works with the Bitwarden CLI to move data from one installation to another. Instructions are available in [this article](#). This script migrates all organization vault data, including attachments, as well as member roles (excluding the custom role), and collections permissions assigned both to members and groups. The script also automatically recreates your groups in the new organization if you're not using directory integration for automatic provisioning. Note that this does not include the migration of individual user vaults.

Q: What does a manual migration look like?

A: A complete manual migration involves creating a new account in the preferred region and beginning the new organization creation process. Once the new organization is configured, re-invite users, and then export vault data from your old organization and import into the new one. Users will need to manually export/import their individual vaults.