bitwarden | Help Center Article

PASSWORD MANAGER > IMPORT & EXPORT

Encrypted Exports

View in the help center:
https://bitwarden.com/help/encrypted-export/

Encrypted Exports

Vault data can be exported in an encrypted `.json` file. Encrypted export files will contain vault items from your organization or individual vault, and will not include Sends, trash, or item attachments. Password protected exports can be creating using the web vault or CLI. Bitwarden provides two encrypted export types:

- **Account restricted:** Export an encrypted file that can only be re-imported to the Bitwarden account or organization that generated the encrypted export file. This process utilizes the relative account or organization encryption key specific to the restricted export.

- **Password protected:** Export an encrypted file protected with a password of your choosing. This file can be decrypted with the password and can be imported to any Bitwarden account.
  The specified password is salted, used to derive an encryption key using PBKDF2 with 100,000 iterations, and finally stretched with HDKF into a new encryption key, which encrypts your data, and message authentication code (MAC).

> ⚠ Warning
>
> **Account restricted** exports can not be imported to a different account. Additionally, rotating your account's encryption key will render an account restricted export impossible to decrypt. **If you rotate your account encryption key, replace any old files with new ones that use the new encryption key.**
>
> If you wish to import an encrypted `.json` file onto a different Bitwarden account, select the **Password protected** export type when creating an export.

Encrypted exports will include vault items such as logins, cards, secure notes, and identities. An encrypted export of the following plaintext login item:

```bash
{
      ...
      "login": {
        "username": "mylogin",
        "password": "mypassword",
        "totp": "otpauth://totp/my-secret-key"
      },
      ...
```

Will look something like:

```
Bash

{
      ...
      "login": {
        "username": "9.dZwQ+b9Zasp98dnfp[g|dHZZ1p19783bn1KzkEsA=l52bcWB/w9unvCt2zE/kCwdpiubAOf104
os}",
        "password": "1o8y3oqsp8n8986HmW7qA=oiCZo872b3dbp0nzT/Pw=|A2lgso87bfDBCys049ano278ebdmTe4:",
        "totp": "2CIUxtpo870B)*^GW2ta/xb0IYyepO(*&G(&BB84LZ5ByZxu0E9hTTs6PHg0=8q5DHEPU&bp9&*bns3EYg
ETXpiu9898sxO78l"
      },
      ...
```

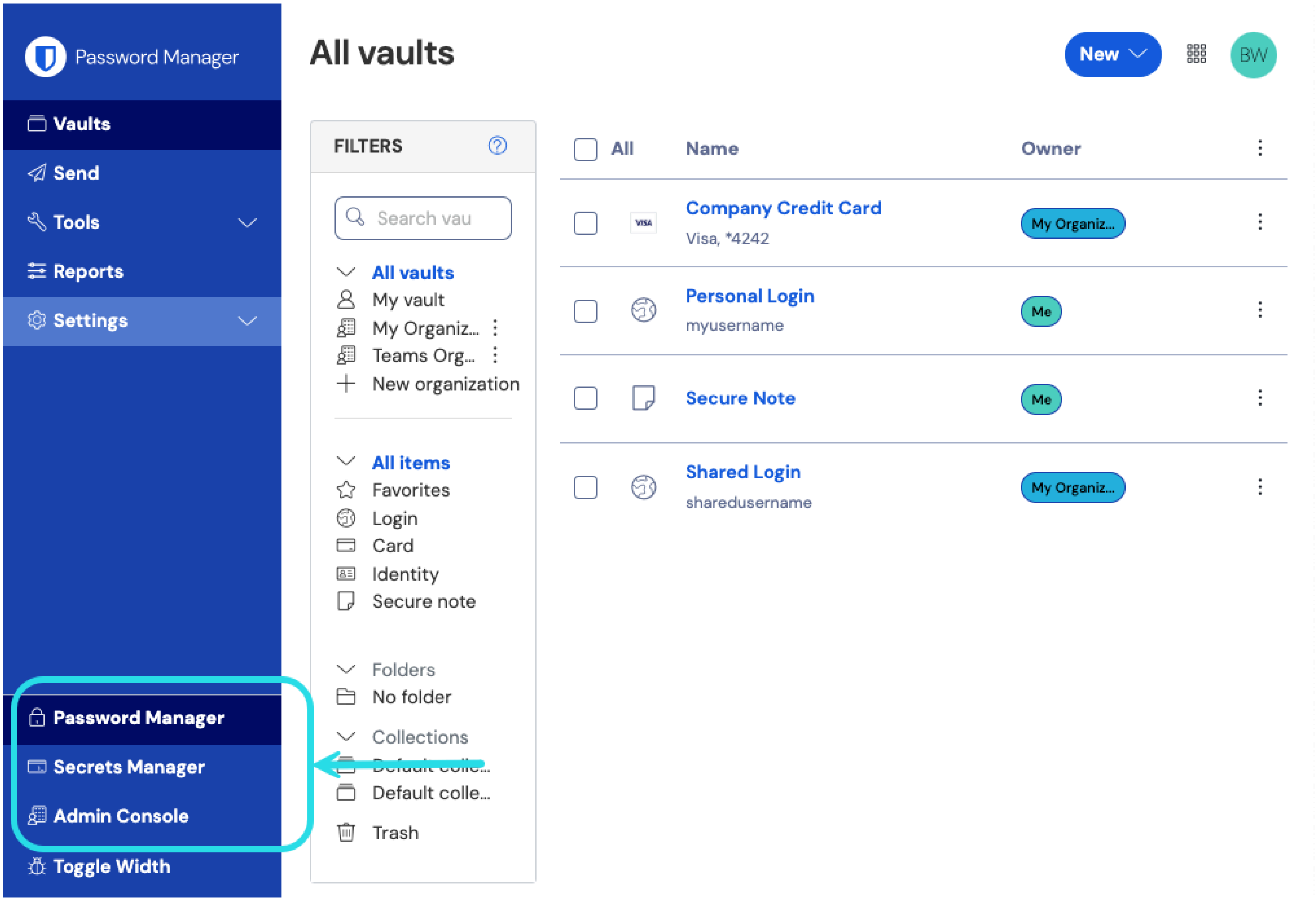
Create an encrypted export

Creating an encrypted export follows the normal export procedure. When prompted for **File Format**, select `.json (Encrypted)`:

⇒Web app

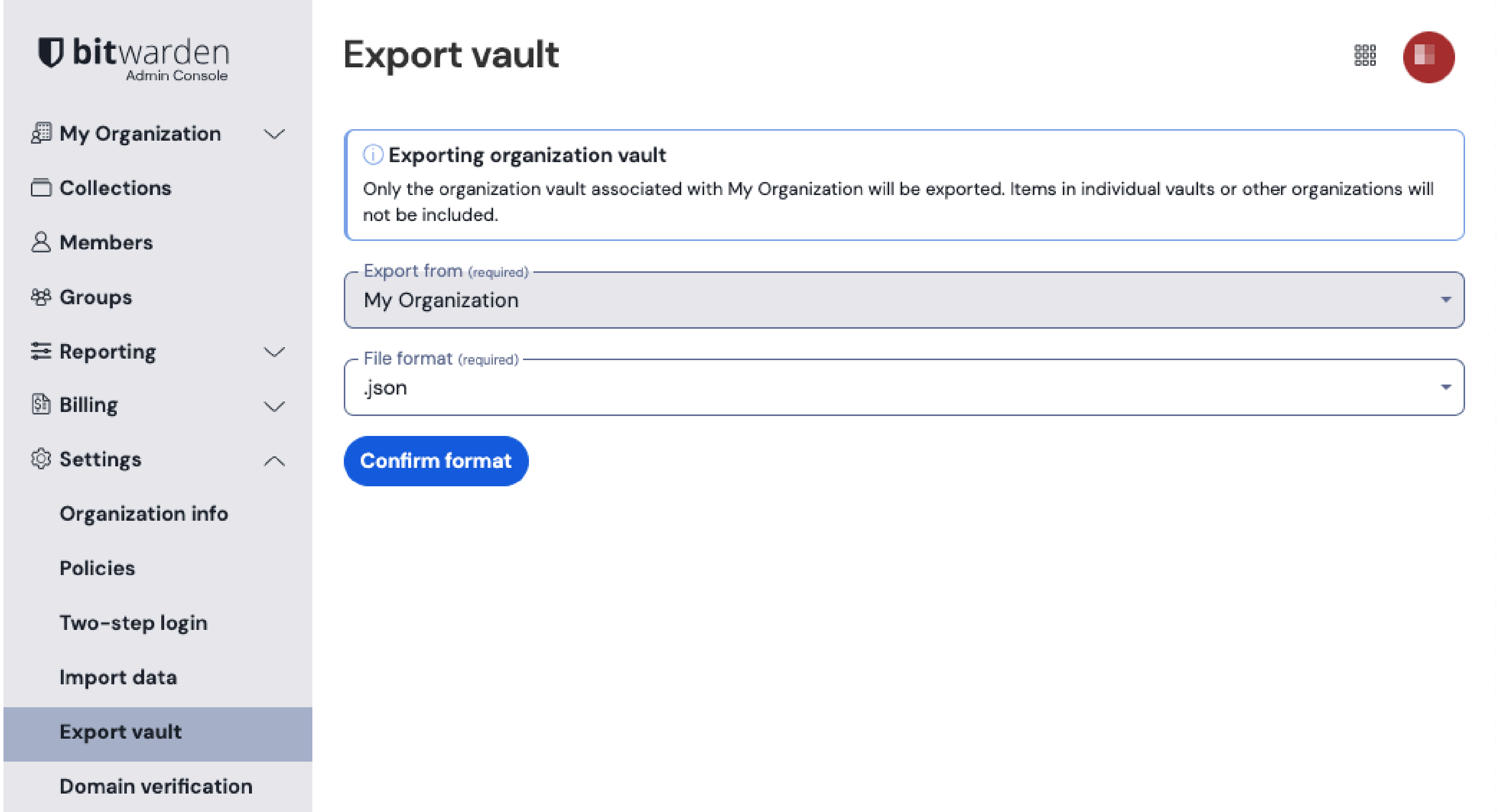
To export your organization data from the web app:

1. Open the **Admin Console** using the product switcher:



Product switcher

2. Select **Export** → **Export vault** from the navigation:



Export vault

Exporting organization vault

Only the organization vault associated with My Organization will be exported. Items in individual vaults or other organizations will not be included.

Export from (required): My Organization

File format (required): .json

Export organization vault

3. On the vault export page, choose a **File format** (`.json`, `.csv`, or `.json (Encrypted)`) and select the **Confirm format** button.

4. Enter your master password and select the **Export vault** button.

> **Note**
>
> Exporting an organization's vault data will be captured by event logs. Learn more.

⇒CLI

To export your organization data from the CLI, use the `export` command with the `--organizationid` option.

By default, `export` will export your vault as a `.csv` and save the file to the working directory, however this behavior can be altered using options:

```bash
bw export my-master-password --organizationid 7063feab-4b10-472e-b64c-785e2b870b92 --output /users/me/documents/ --format json
```

> **Tip**
>
> If you don't know your `organizationid` value off-hand, you can access it at the command-line using `bw list organizations`.

For more detail, see our CLI documentation.

> **Note**
>
> Exporting an organization's vault data will be captured by event logs. Learn more.

Import an encrypted export

Importing an encrypted export follows the normal import procedure. When prompted for **File format**, select `.json`:

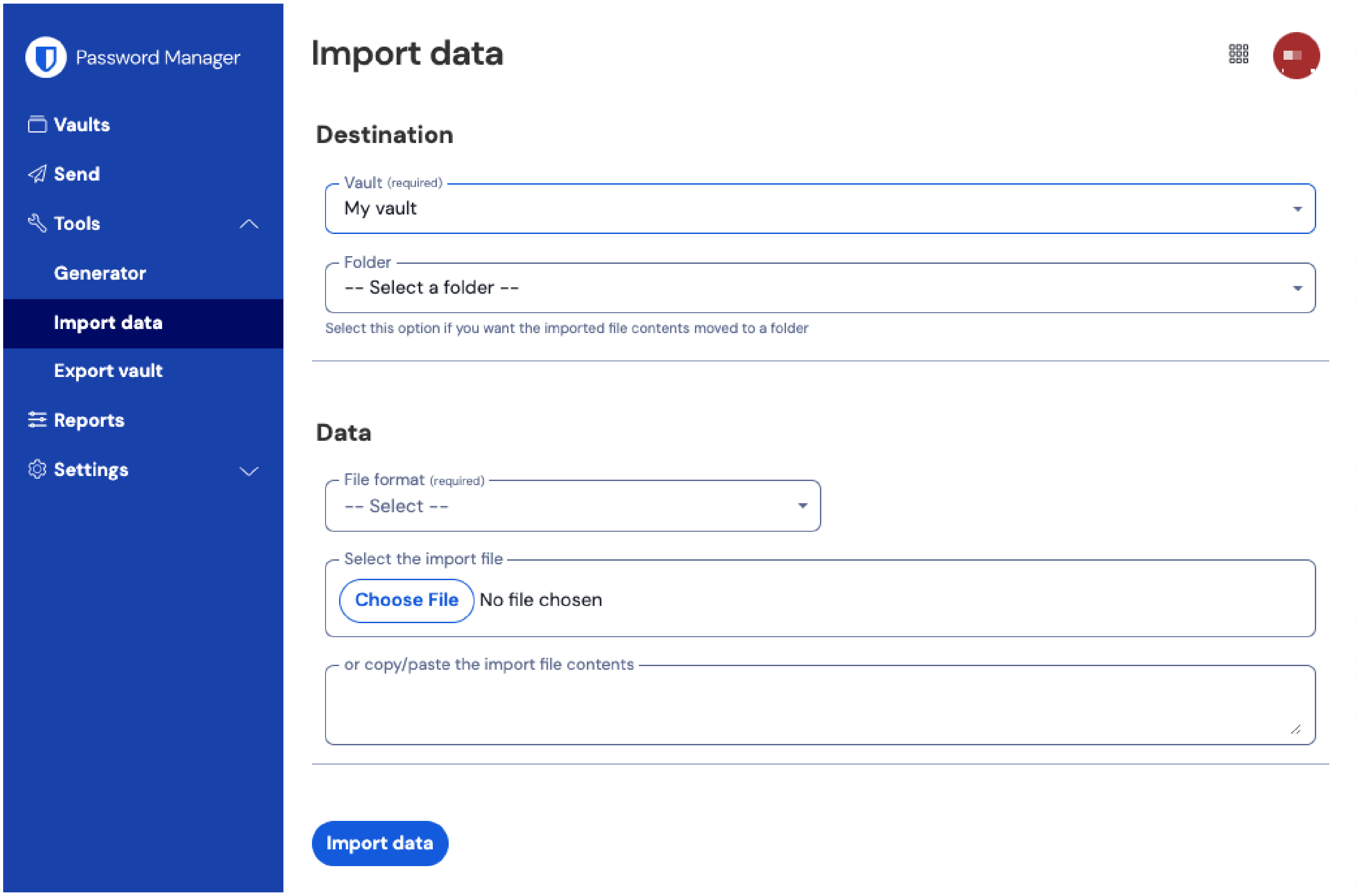
> **Tip**
>
> There is no import option specifically for encrypted exports. A handler will determine that the `.json` file is encrypted and attempt to decrypt the file using either your account's encryption key or encrypted export password.

⇒Web app

To import data to your vault:

1. Log in to the web vault at https://vault.bitwarden.com, https://vault.bitwarden.eu, or `https://your.bitwarden.domain.com` if self-hosting.

2. Select **Tools** → **Import data** from the navigation:



Import data

Destination

Vault (required)
My vault

Folder
-- Select a folder --

Select this option if you want the imported file contents moved to a folder

Data

File format (required)
-- Select --

Select the import file
Choose File No file chosen

or copy/paste the import file contents

Import data

Import data

3. Complete the following fields from the drop down menus:

- **Vault:** Select the import destination such as your individual vault or an organizational vault that you have access to.
- **Folder or Collection:** Select if you would like the imported content moved to a specific folder or organization collection that you have access to.
- **File format:** Select the import file format.

4. Select **Choose File** and add the file to import or copy/paste the contents of your file into the input box.

> ⚠ **Warning**
>
> Importing does not check whether items in the file to import already exist in your vault. If you import multiple files or import files with items already in your vault, **this will create duplicates**.

5. Select **Import data** to trigger the import. If you are importing a password protected `.json` file, enter the password into the **Confirm vault import** window that will appear.

6. After successful import, delete the import source file from your computer. This will protect you in the event your computer is compromised.

Additional items such as file attachments, Sends, and trash will need to be manually uploaded to your vault.

⇒Browser extension

To import data to your vault:

1. In the **Settings** tab, select **Vault** and choose the **Import items** option**.**

2. Complete the following fields from the drop down menus:

   1. **Vault:** Select the import destination such as your individual vault or an organizational vault that you have access to.

   2. **Folder** or **Collection:** Select if you would like the imported content moved to a specific folder or organization collection that you have access to.

   3. **File format:** Select the import file format.

3. Select **Choose File** and add the file to import or copy/paste the contents of your file into the input box.

   > ⚠ **Warning**
   >
   > Importing does not check whether items in the file to import already exist in your vault. If you import multiple files or import files with items already in your vault, **this will create duplicates**.

4. Select **Import Data** to trigger the import. If you are importing a password protected `.json` file, enter the password into the **Confirm Vault Import** window that will appear.

5. After successful import, delete the import source file from your computer. This will protect you in the event your computer is compromised.

⇒Desktop app

To import data to your vault:

1. Select **File** > **Import data**.

2. Complete the following fields from the drop down menus:

   1. **Import destination:** Select the import destination such as your individual vault or an organizational vault that you have access to.

   2. **Folder or Collection:** Select if you would like the imported content moved to a specific folder or organization collection that you have access to.

   3. **File format:** Select the import file format.

3. Select **Choose File** and add the file to import or copy/paste the contents of your file into the input box.

   > ⚠ **Warning**
   >
   > Importing does not check whether items in the file to import already exist in your vault. If you import multiple files or import files with items already in your vault, **this will create duplicates**.

4. Select **Import Data** to trigger the import. If you are importing a password protected `.json` file, enter the password into the **Confirm Vault Import** window that will appear.

5. After successful import, delete the import source file from your computer. This will protect you in the event your computer is compromised.

⇒CLI

To import data to your vault from the CLI, use the following command:

```bash
bw import <format> <path>
```

`bw import` requires a format (use `bw import --formats` to retrieve a list of formats) and a path, for example:

```bash
bw import <format> /Users/myaccount/Documents/mydata.csv
```

After successful import, delete the import source file from your computer. This will protect you in the event your computer is compromised.