bitwarden | Help Center Article

PASSWORD MANAGER > IMPORT & EXPORT

Krypterad export

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

Krypterad export

Arkivdata kan exporteras i en krypterad `.json-fil`. Krypterade exportfiler kommer att innehålla valvobjekt från din organisation eller enskilda valv och kommer inte att inkludera sändningar, papperskorgen eller bilagor. Lösenordsskyddade exporter kan skapas med hjälp av webbvalvet eller CLI. Bitwarden tillhandahåller två krypterade exporttyper:

- **Kontobegränsat:** Exportera en krypterad fil som endast kan återimporteras till Bitwarden-kontot eller organisationen som genererade den krypterade exportfilen. Denna process använder den relativa konto- eller organisationskrypteringsnyckeln som är specifik för den begränsade exporten.

- **Lösenordsskyddad:** Exportera en krypterad fil skyddad med ett lösenord som du väljer. Den här filen kan dekrypteras med lösenordet och kan importeras till vilket Bitwarden-konto som helst.
  Det angivna lösenordet är saltat, används för att härleda en krypteringsnyckel med PBKDF2 med 100 000 iterationer, och slutligen sträcks ut med HDKF till en ny krypteringsnyckel, som krypterar dina data, och meddelandeautentiseringskod (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.

Krypterad export kommer att innehålla valvobjekt som inloggningar, kort, säkra anteckningar och identiteter. En krypterad export av följande inloggningsobjekt i klartext:

Bash

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

Kommer se ut ungefär så här:

```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"
      },
      ...
```

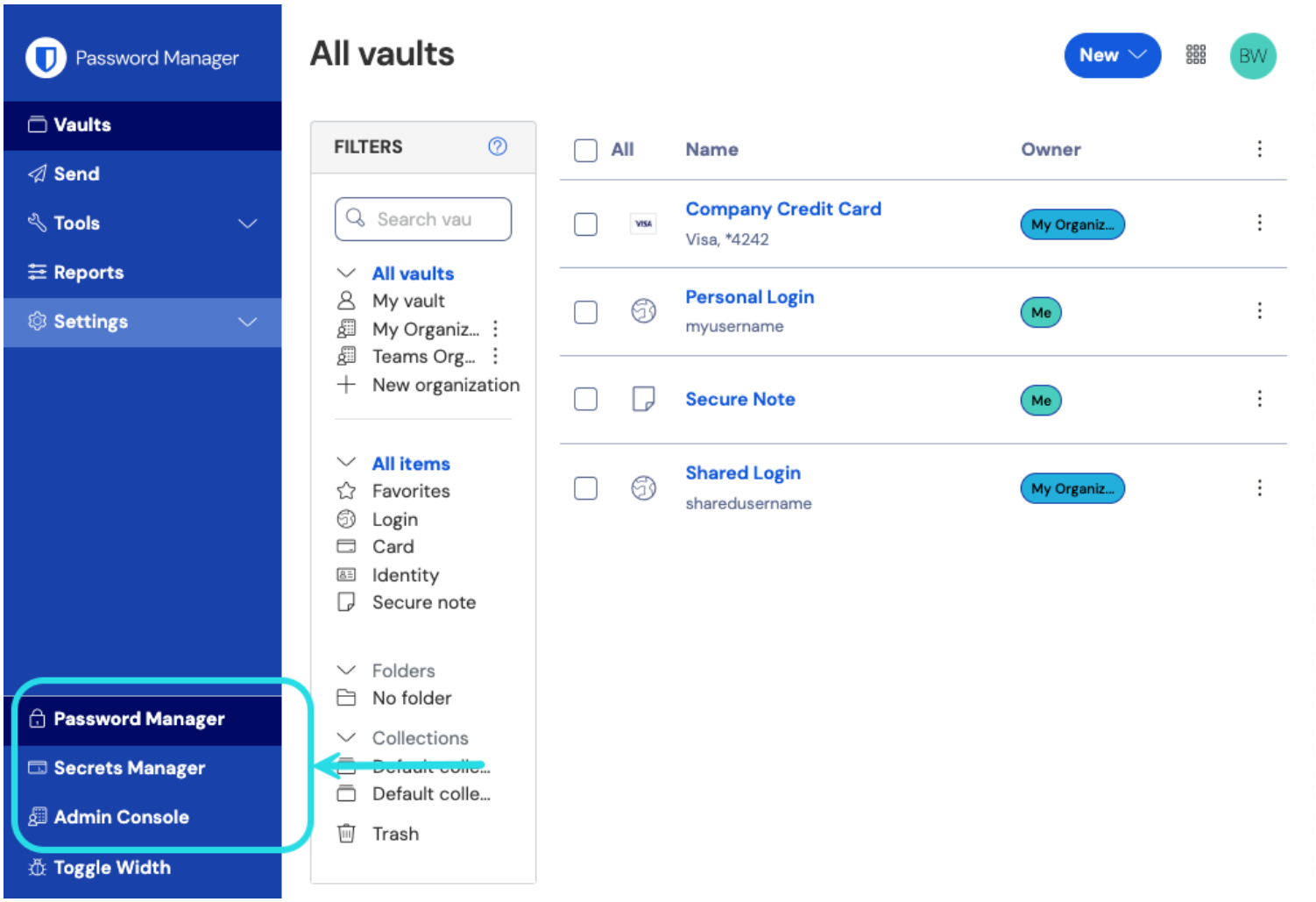
Skapa en krypterad export

Att skapa en krypterad export följer den normala exportproceduren. När du tillfrågas om **filformat** väljer du `.json (krypterad)`:

⇒Webbapp

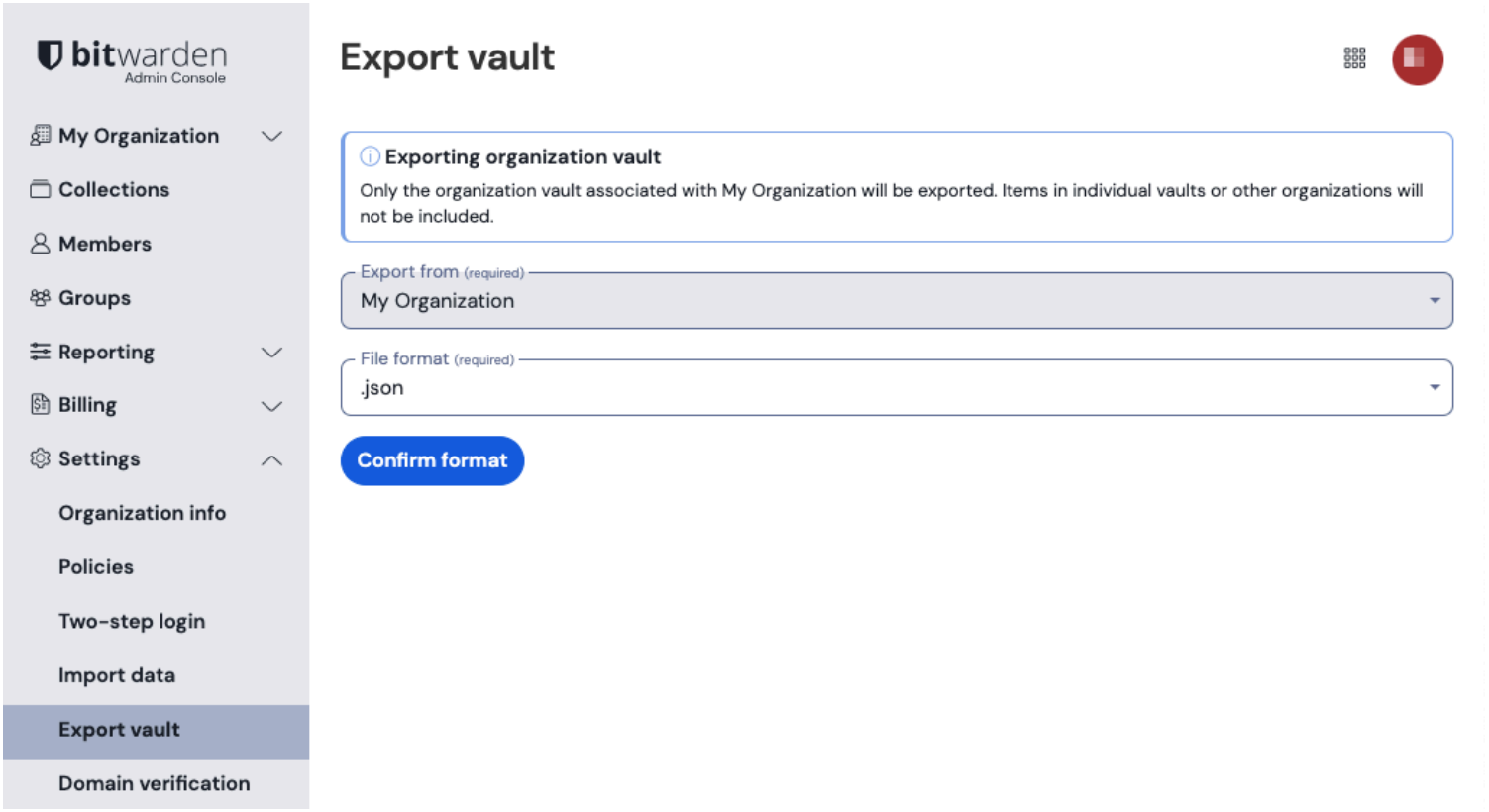
Så här exporterar du organisationsdata från webbappen:

1. Öppna **administratörskonsolen** med hjälp av produktväxlaren:



Product switcher

2. Välj **Exportera → Exportera valv** från navigeringen:



Export organization vault

3. På valvets exportsida väljer du ett **filformat** (`.json`, `.csv` eller `.json (krypterat`)) och väljer **knappen** Bekräfta format.

4. Ange ditt huvudlösenord och välj knappen **Exportera valv**.

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

⇒CLI

> **Tip**
> It is recommended that you sync your vault with `bw sync` before exporting from the CLI.

För att exportera din organisationsdata från CLI, använd exportkommandot med alternativet `--organizationid`. Som standard exporterar `export` ditt valv som en `.csv` och sparar filen i arbetskatalogen, men detta beteende kan ändras med alternativ:

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

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

För mer information, se vår CLI-dokumentation.

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

Importera en krypterad export

Import av en krypterad export följer den normala importproceduren. När du tillfrågas om **filformat** väljer du `.json`:

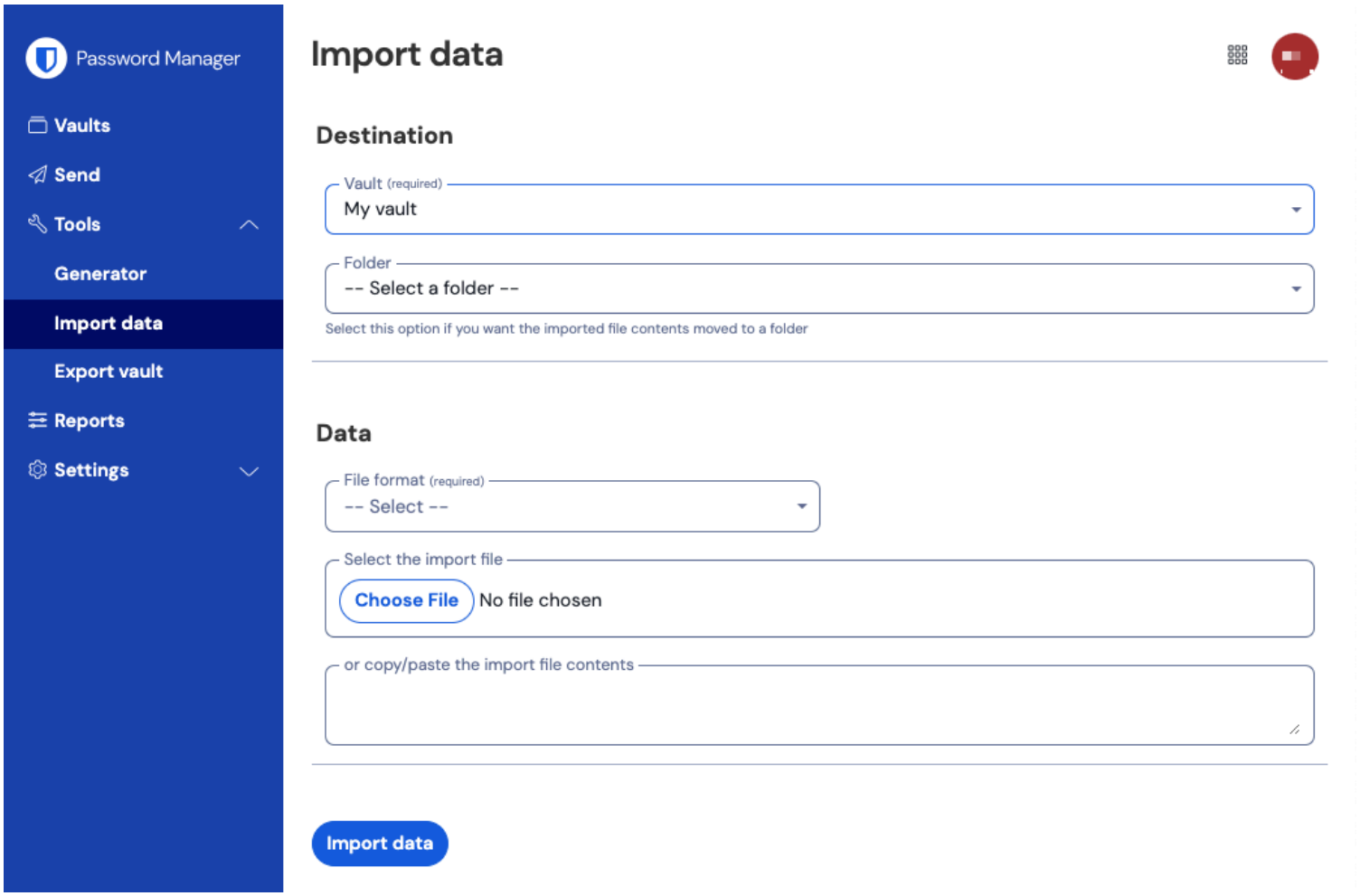
> **Tip**
>
> There is no import option specifically for encrypted exports. A handler will determine that the `.json` file is encrypted and attempt to decrypt the file using either your account's encryption key or encrypted export password.

⇒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

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.