bitwarden | Help Center Article

PASSWORD MANAGER > VAULT ADMINISTRATION

Vault Health Reports

View in the help center:
https://bitwarden.com/help/reports/

Vault Health Reports

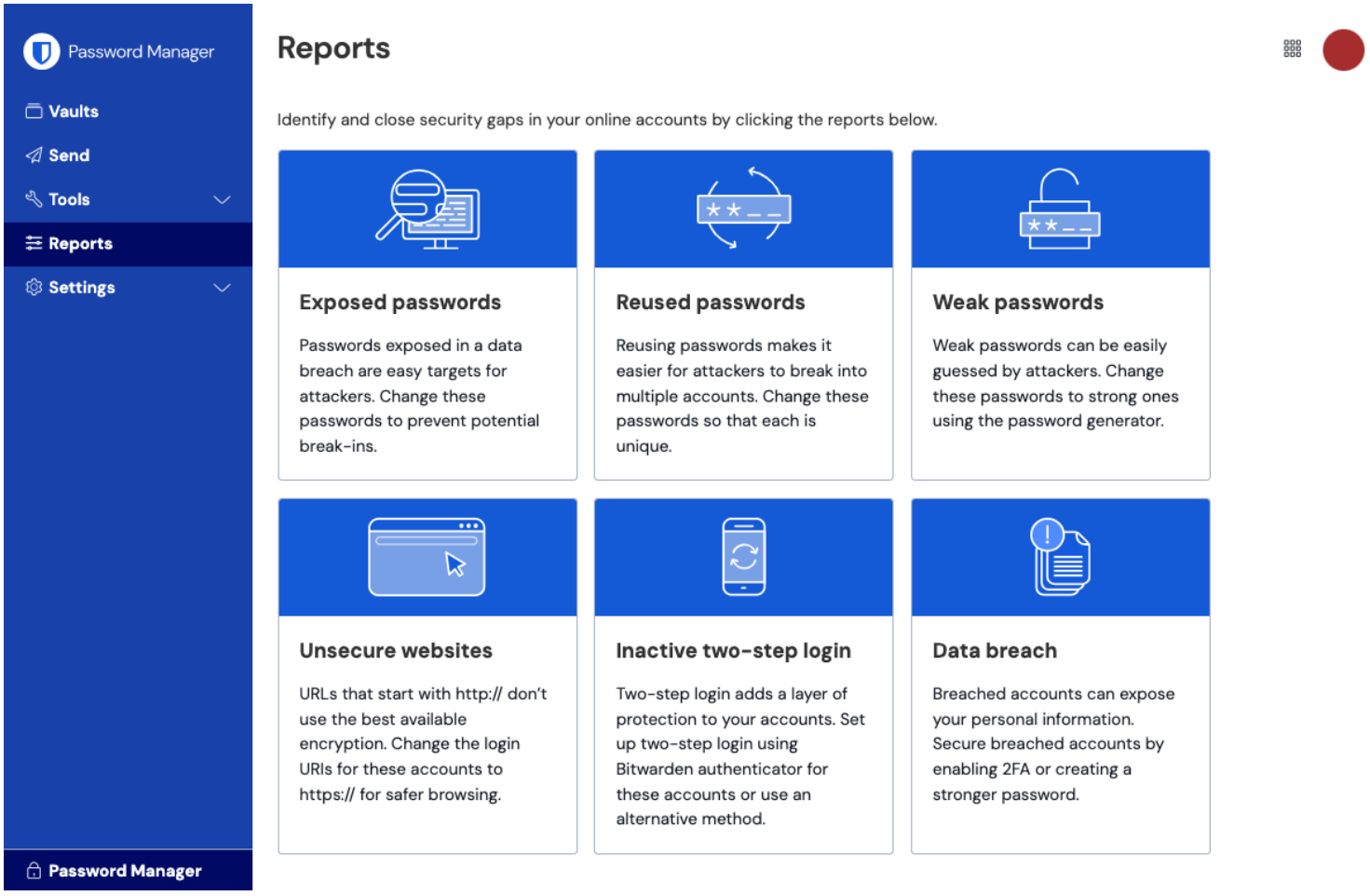
Vault health reports can be used to evaluate the security of your Bitwarden individual or organization vault. Reports, for example the Reused Passwords and Weak Passwords report, are run locally on your client. This allows offending items to be identified, without Bitwarden ever having access to unencrypted versions of this data.

> **Note**
>
> Most vault health reports are only available for premium users, including members of paid organizations (families, teams, or enterprise), but the Data Breach report is free for all users.

View a report

To run any vault health report for your **individual vault**:

1. Log in to the web app and select **Reports** from the navigation:



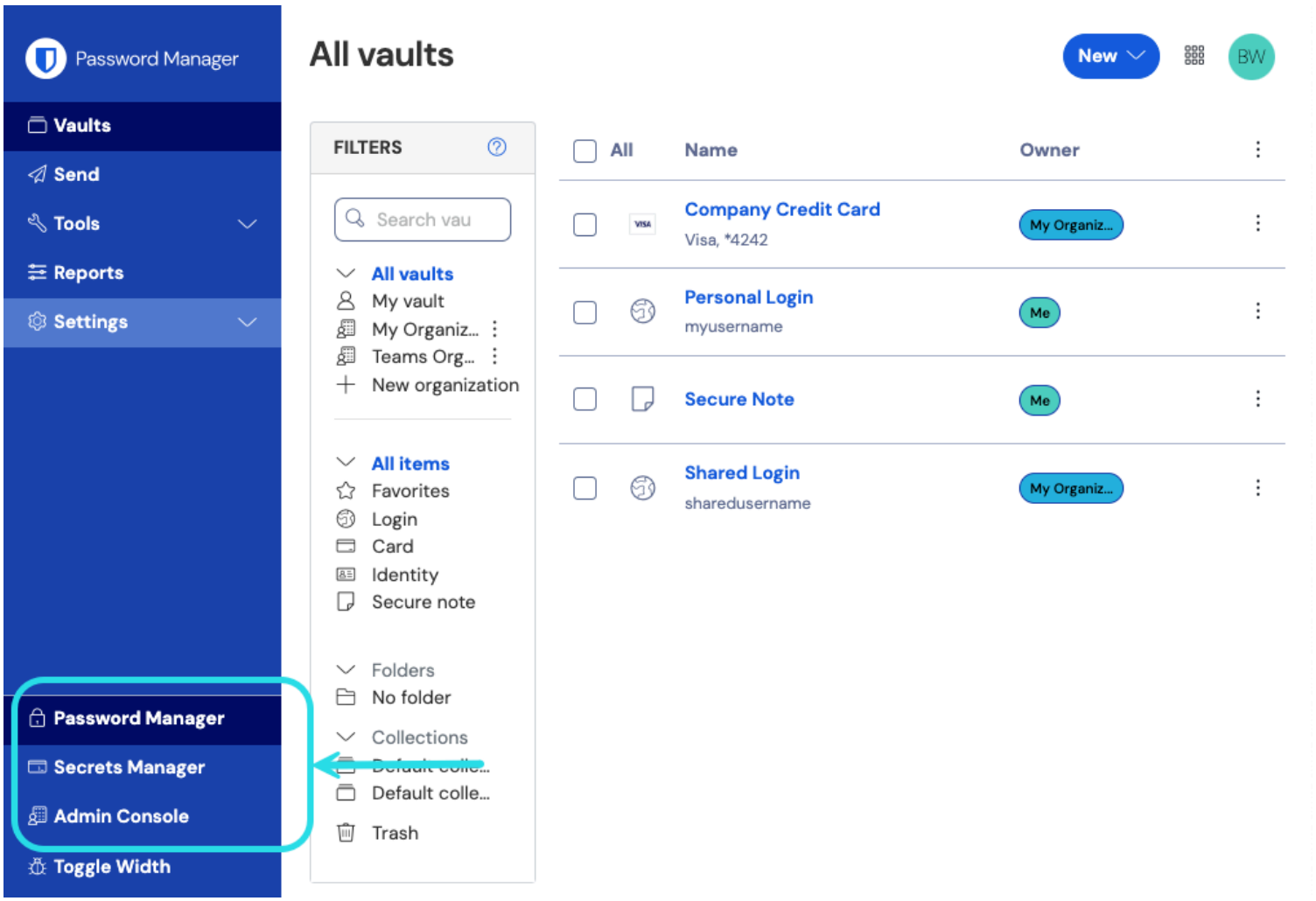
Reports page

2. Choose a report to run.

To run any vault health report for your **organization vault**:

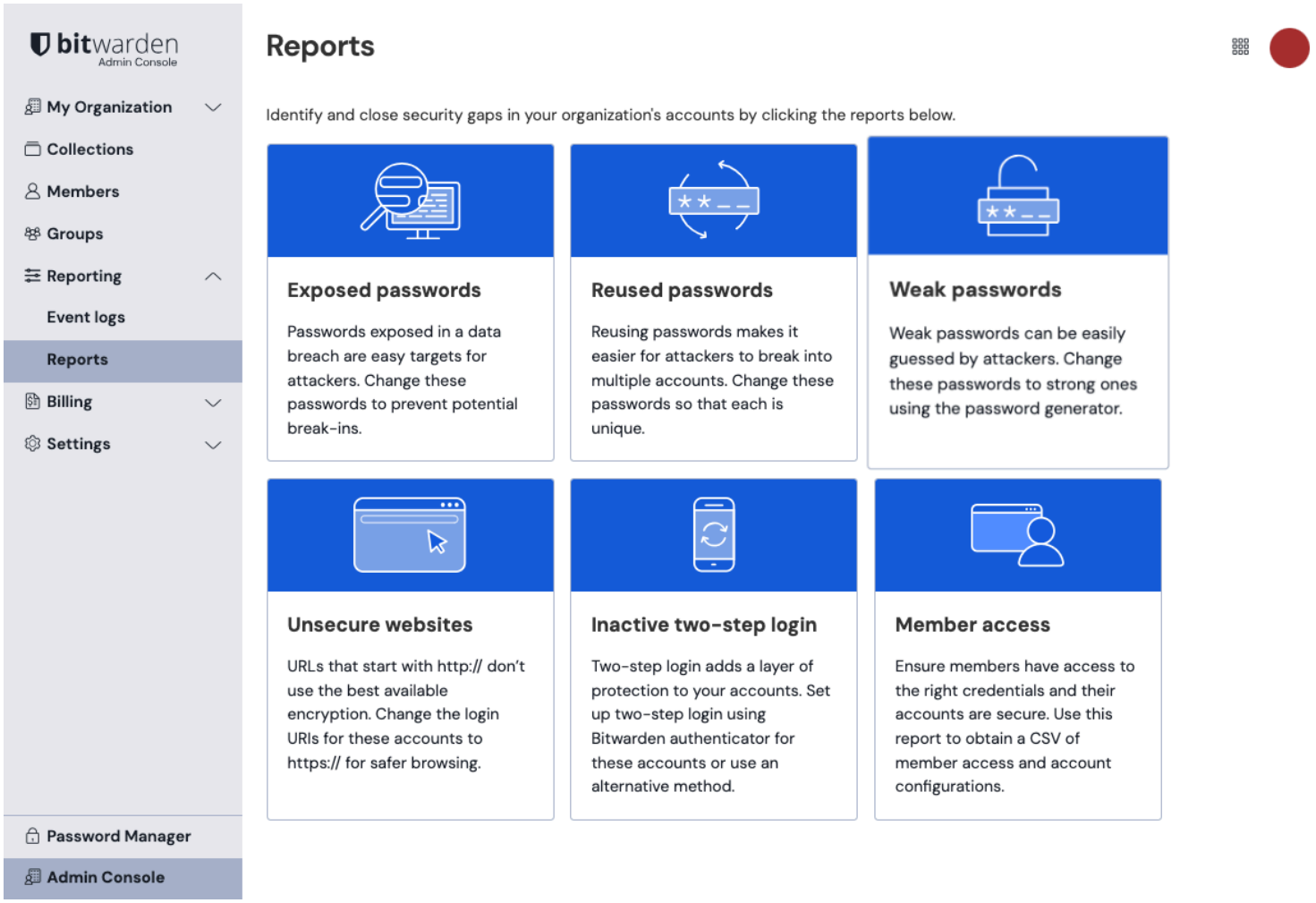
1. Log in to the Bitwarden web app.

2. Open the Admin Console using the product switcher:



Product switcher

3. In your organization, select **Reporting** → **Reports** from the navigation



Organization reports

4. Choose a report to run.

Available reports

Exposed Passwords report

The Exposed Passwords report will identify passwords that have been uncovered in known data breaches that were released publicly or sold on the dark web by hackers.

This report uses a trusted web service to search the first five digits of the hash of all your passwords in a database of known leaked passwords. The returned matching list of hashes is then locally compared with the full hash of your passwords. That comparison is only done locally to preserve your k-anonymity.

Once identified, you should create a new password for offending accounts or services.

> **Tip**
>
> Why use the first five digits of password hashes?
>
> If the report was performed with your actual passwords, it doesn't matter if they were exposed or not, you would be voluntarily leaking it to the service. This report's result may not mean your account has been compromised, rather that you are using a password that has been found in these databases of exposed passwords, however you should avoid using leaked and non-unique passwords.

Reused Passwords report

The Reused Passwords report identifies non-unique passwords in your vault. Reusing the same password for multiple services can allow hackers to easily gain access to more of your online accounts when one service is breached.

Once identified, you should create a unique password for offending accounts or services.

Weak Passwords report

The Weak Passwords report identifies weak passwords that can easily be guessed by hackers and automated tools that are used to crack passwords, sorted by severity of the weakness. This report uses zxcvbn for password strength analysis.

Once identified, you should use the Bitwarden password generator to create a strong password for offending accounts or services.

Unsecured Websites report

The Unsecured Websites report identifies login items that use unsecured (`http://`) schemes in URIs. It's much safer to use `https://` to encrypt communications with TLS/SSL. To learn more, see using URIs.

Once identified, you should change offending URIs from `http://` to `https://`.

Inactive 2FA report

The Inactive 2FA report identifies login items where:

- Two-factor authentication (2FA) via TOTP is available from the service
- You have not stored a TOTP authenticator key

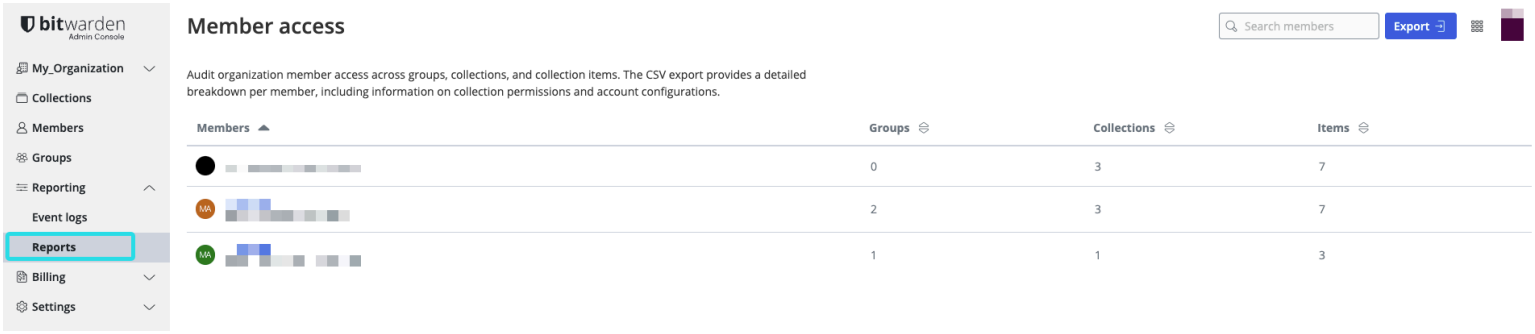
Two-factor authentication (2FA) is an important security step that helps secure your accounts. If any website offers it, you should always enable 2FA. Offending items are identified by cross-referencing URI-data with data from https://2fa.directory/.

Once identified, setup 2FA using the `Instructions` hyperlink for each offending item:

Report Instructions

Member access

Enterprise organizations can use the member access report to review a list of **Groups**, **Collections** and **Items** that organization members have access to.



Member access report

Using the Member access report you can:

- View the total number of Groups, Collections, and Items each user has access to.
- Use Search members to search an individual member on the Member access page.
- Create a CSV Export using the **Export** button. The CSV export includes a detailed list of each members **Group** and **Collection access**, as well as **Collection Permissions**, **Two-Step Login**, and **Account Recovery** status.

Data Breach report (individual vaults only)

The Data Breach report identifies compromised data (email addresses, passwords, credit cards, DoB, and more) in known breaches, using a service called Have I Been Pwned (HIBP).

When you create a Bitwarden account, you'll have the option to run this report on your master password before deciding to use it. To run this report, the first five digits of a hash of your master password is sent to HIBP and compared to stored exposed hashes. Your master password itself is never exposed by Bitwarden.

A “breach” is defined by HIBP as "an incident where data is inadvertently exposed in a vulnerable system, usually due to insufficient access controls or security weaknesses in the software". For more information, refer to HIBP's FAQs documentation.

Note

If you are self-hosting Bitwarden, in order to run the data breach report in your instance you will need to buy an HIBP subscription key that will authorize you to make calls to the API, obtained here.

Once you have the key, open your `./bwdata/env/global.override.env` and REPLACE the placeholders value for `globalSettings__hibpApiKey` with your purchased API key:

```bash
globalSettings__hibpApiKey=REPLACE
```

For more information, see configure environment variables.