

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

Identify and close security gaps in your online accounts by clicking the reports below.

- Exposed passwords**
Passwords exposed in a data breach are easy targets for attackers. Change these passwords to prevent potential break-ins.
- Reused passwords**
Reusing passwords makes it easier for attackers to break into multiple accounts. Change these passwords so that each is unique.
- Weak passwords**
Weak passwords can be easily guessed by attackers. Change these passwords to strong ones using the password generator.
- Insecure websites**
URLs that start with http:// don't use the best available encryption. Change the login URLs for these accounts to https:// for safer browsing.
- Inactive two-step login**
Two-step login adds a layer of protection to your accounts. Set up two-step login using Bitwarden authenticator for these accounts or use an alternative method.
- Data breach**
Breach accounts can expose your personal information. Secure breached accounts by enabling 2FA or creating a stronger password.

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.

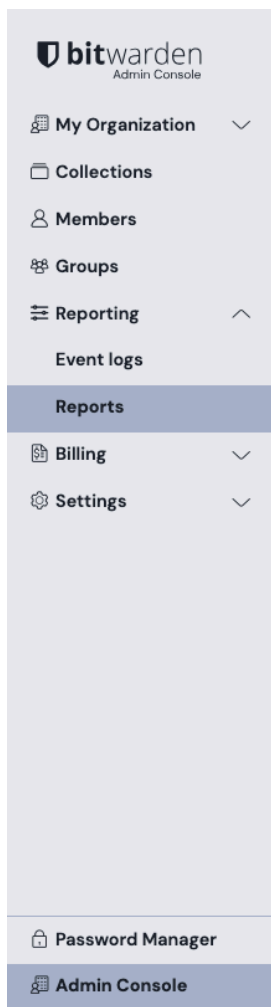
2. Open the Admin Console using the product switcher:

The screenshot shows the Bitwarden interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red circle highlights the 'Admin Console' option. The main area is titled 'All vaults' and features a 'FILTERS' sidebar with a search bar and categories like 'All vaults', 'All items', 'Folders', 'Collections', and 'Trash'. The 'All vaults' category is expanded, showing 'My vault', 'My Organiz...', 'Teams Org...', and 'New organization'. The main content area displays a table of vaults:

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

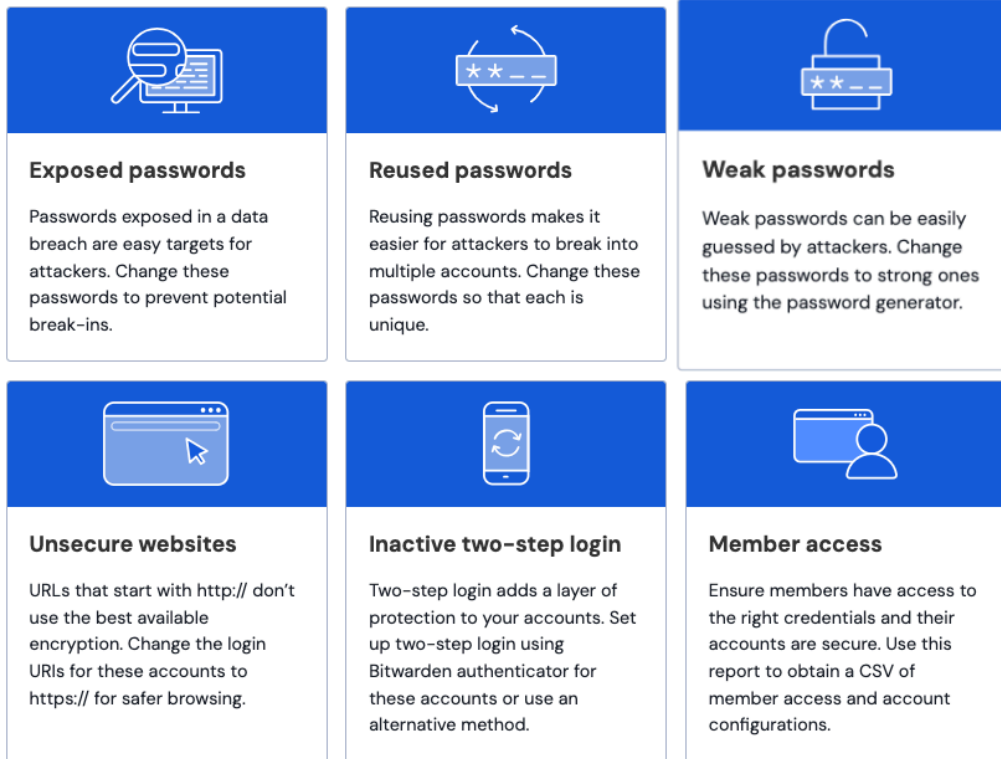
3. In your organization, select **Reporting** → **Reports** from the navigation



- bitwarden Admin Console
- My Organization
- Collections
- Members
- Groups
- Reporting
 - Event logs
 - Reports**
- Billing
- Settings
- Password Manager
- Admin Console

Reports

Identify and close security gaps in your organization's accounts by clicking the reports below.



- Exposed passwords**

Passwords exposed in a data breach are easy targets for attackers. Change these passwords to prevent potential break-ins.
- Reused passwords**

Reusing passwords makes it easier for attackers to break into multiple accounts. Change these passwords so that each is unique.
- Weak passwords**

Weak passwords can be easily guessed by attackers. Change these passwords to strong ones using the password generator.
- Unsecure websites**

URLs that start with http:// don't use the best available encryption. Change the login URLs for these accounts to https:// for safer browsing.
- Inactive two-step login**

Two-step login adds a layer of protection to your accounts. Set up two-step login using Bitwarden authenticator for these accounts or use an alternative method.
- Member access**

Ensure members have access to the right credentials and their accounts are secure. Use this report to obtain a CSV of member access and account configurations.

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:

[Instructions](#)

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

Audit organization member access across groups, collections, and collection items. The CSV export provides a detailed breakdown per member, including information on collection permissions and account configurations.

Members	Groups	Collections	Items
	0	3	7
	2	3	7
	1	1	3

[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](#).