User documentation Vaultwarden

22.11.2026 18:14:31

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::Passwortmanager	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	07:39:46 - 11.11.2026

Schlüsselwörter

Password Password-Manager Passwort Passwort-Manager

Lösung (öffentlich)

General information:

Vaultwarden is the centrally available password manager at TU Dresden. It is intended to facilitate the storage and secure management of individual user passwords, as well as the sharing of jointly used passwords. Its main feature is storing usernames, passwords (including the associated URL), notes, and, if applicable, attachments such as certificates in a single data record. You can also create new data records, including new passwords, and generate a new secure password with flexible length and character selection.

You can create organizations for your specific organizational units and teams and flexibly grant permissions to individuals or groups within the organization or within the collections and subcollections it contains. In addition, you can store your own user passwords in encrypted form in "My Vault."

Possible uses include:

-

Management of and access to shared passwords (labs, projects, teams)

-

Mapping of substitution arrangements

-

Management of private passwords in a private vault

-

Creation and storage of new password records using the password generator

Access and organization:

You can find Vaultwarden starting November 9, 2026, at [1]passwords2.tu-dresden.de.

Access is granted via the VPN network and through Single Sign-On (SSO) using your ZIH login; a master password is then set for the account.

Please note: The master password encrypts and decrypts all your passwords stored in Vaultwarden – please make sure to remember it!

There is a separate [2]FAQ-Article on how to set up an emergency contact for resetting the master password.
If you do not set up an emergency contact, your account can be deleted centrally if you forget your master password. You can then re-register.

Within Vaultwarden, you can create an "organization" to share passwords with others. Within organizations, passwords can be organized into collections for better clarity and management.

For your own personal passwords, use "My vault". There, you can use folders to improve clarity.

Once you've created an organization or become an administrator or owner of an organization, you'll gain access to the "Admin Console" in the bottom-left corner. That's where you can manage members and groups.

Members can be managed individually or as a group, and permissions can be set separately for each collection:
[3]https://bitwarden.com/help/collection-permissions/

Roles and permissions:
-

Organization owner → appoint or demote other owners; interact with users and collections in any way; view event logs

-

Administrator → create groups; interact with users and collections in any way; view event logs

-

Manager → can only view collections assigned by owners or admins; can grant permissions to users within these collections

-

User → access to assigned collections; no interaction with user permissions

When you create a new collection via "+New", you can use "Edit access" to directly set access for members or groups to the new collection. Please note:

-

There is no inheritance as in Passwork; permissions must be assigned down the hierarchy on a folder-by-folder basis.

-

Collections are not traditional folders; entries can be assigned to multiple collections.

-

Permissions are always set on folders (collections); permissions cannot be set for individual entries or passwords.

Editing collection permissions:

-

Open the collection, then click on the small arrow icon next to the collection name at the very top -> Access, review, and set

-

In the list of collections, click the three-dot menu next to the collection name -> Access

The following permissions are available:

View items

User/group can view all items, including password fields

View items, hidden passwords

User/group can view items; passwords can be used via autofill, but viewing or copying is not possible

Edit items

User/group can create items, edit existing items, including password fields

Edit items, hidden passwords

User/group can create items, edit existing items, excluding password fields

Manage collection

User/group can manage access to the collection for other users/groups; creating new collections is not possible

Security and theme:

Click on "Security" to set the timeout for your Vaultwarden web application. You can also change your master password, manage device access, and view API keys here.

The "Appearance" menu option lets you set the theme (light/dark) and language for your Vaultwarden.

Desktop app and plugin

Browser plugin via Bitwarden for Safari, Chrome, and Firefox

-

Desktop app via Bitwarden for macOS, Linux, and Windows

Once you've downloaded and installed the plugin or app, scroll to the very bottom of the window, select "Self-hosted" under "Access to", and enter the URL https://passwords2.tu-dresden.de. Then log in with your TUD account via Single Sign-On (SSO) and enter your Vaultwarden master password.

Bitwarden: Login with Desktop App or Plugin Bitwarden: fill in the URL in Desktop App or Plug in

Vaultwarden uses an interface with Have I Been Pwned (HIBP) so that users can check whether their passwords have been compromised. A password generator is available for creating new entries.

[1] https://passwords2.tu-dresden.de/
[2] https://tickets.tu-dresden.de/otrs/customer.pl?Action=CustomerFAQZoom;ItemID=1639
[3] https://bitwarden.com/help/collection-permissions/