

Passwortsafe

Worum geht es?

Unter <https://passwortsafe.uni-bremen.de> betreibt die Universität Bremen eine eigene Instanz der Software Vaultwarden, die wiederum die inoffizielle Open-Source-Version von Bitwarden ist (die Unterschiede in den Begrifflichkeiten werden später noch wichtig.)

Hier steht allen Mitarbeitenden der Uni eine plattform- und geräteübergreifende Möglichkeit zur Verfügung, Login-Daten, Notizen, Identitäten und mehr außerhalb öffentlicher Clouds sicher zu speichern.

Zu beachten

Es gibt ein paar Einschränkungen, deren man sich bewusst sein sollte:

- Server-Administratoren haben keinen Zugriff auf Benutzerdaten. Dadurch
 - können keine Passwörter zurückgesetzt werden
 - können keine gelöschten Einträge wiederhergestellt werden
- Vergisst man sein Master-Passwort und kann es auch mit Hilfe des Hinweises (dieser wird ausschließlich per E-Mail versendet) nicht herausfinden, so gibt es nur noch die Möglichkeit, den Benutzer zu löschen und neu anzulegen, wodurch alle Passwörter verloren gehen (außer man hat ein lokales Backup)
- Es wird daher empfohlen, regelmäßig ein solches lokales Backup der Daten zu erstellen und sicher (z.B. mit 7-Zip als passwortgeschütztes Archiv (AES-256 verwenden!)) abzulegen
- Es gibt ein tägliches Backup des Servers, das aber nur bei zentralen Ausfällen zum Einsatz kommt. Einzelne Benutzer oder Daten können nicht wiederhergestellt werden.
- Inaktive Accounts erhalten nach einem Jahr eine einmalige E-Mail-Warnung und werden bei ausbleibender Antwort gelöscht.

Zugangsoptionen

Es gibt mehrere Möglichkeiten auf den Passwortsafe zuzugreifen.

- **Browser-Erweiterungen** (Firefox, Chrome, Edge, Opera): Dies ist das Hauptanwendungsfeld. Zugangsdaten werden gespeichert und automatisch ausgefüllt, sichere Passwörter können direkt erzeugt werden.
- **Smartphone-Apps** (Android, iOS): Funktionell vergleichbar mit den Browser-Erweiterungen; ideal für den mobilen Zugriff.
- **Weboberfläche**: Bietet den größten Funktionsumfang (100%). Verwaltung und Sortierung von Zugangsdaten, Verwaltung von Organisationen usw.
- **Desktop-Apps** (Windows, macOS, Linux): Bieten nach aktuellem Stand gegenüber den Browser-Erweiterungen keine wesentlichen Vorteile.


Einrichtung

Als erstes auf „Konto erstellen“ gehen.

Vaultwarden Web

https://passwordsafe.uni-bremen.de/#/login

Vaultwarden



Anmelden

E-Mail-Adresse (erforderlich)

E-Mail-Adresse merken

Fortsetzen

Konto erstellen

Vaultwarden Web
2026.1.1

A modified version of the Bitwarden® Web Vault for Vaultwarden (an unofficial rewrite of the Bitwarden® server).
Vaultwarden is not associated with the Bitwarden® project nor Bitwarden Inc.

E-Mail-Adresse und Namen eingeben (uni-bremen.de-Adressen werden automatisch akzeptiert).

Konto erstellen | Vaultwarden Web

https://passwortsafe.uni-bremen.de/#/signup

Vaultwarden

Konto erstellen

E-Mail-Adresse (erforderlich)
tstest@uni-bremen.de

Name
Tiberius S. Test

Fortsetzen

Hast du bereits ein Konto? [Anmelden](#)

Vaultwarden Web
2026.1.1


A modified version of the Bitwarden® Web Vault for Vaultwarden (an unofficial rewrite of the Bitwarden® server).
Vaultwarden is not associated with the Bitwarden® project nor Bitwarden Inc.

Anmeldung in der E-Mail bestätigen.

Konto erstellen | Vaultwarden Web X

https://passwortsafe.uni-bremen.de/#/signup

Vaultwarden



Überprüfe deine E-Mail

Folge dem Link in der E-Mail an tstest@uni-bremen.de und fahre mit der Erstellung deines Kontos fort.

Keine E-Mail? [Geh zurück](#), um deine E-Mail-Adresse zu bearbeiten.

Hast du bereits ein Konto? [Anmelden](#)

Vaultwarden Web
2026.1.1

A modified version of the Bitwarden® Web Vault for Vaultwarden (an unofficial rewrite of the Bitwarden® server).
Vaultwarden is not associated with the Bitwarden® project nor Bitwarden Inc.

Sicheres einzigartiges Passwort wählen, passenden Hinweis eingeben.

Lege ein starkes Passwort fest

Schließe die Erstellung deines Kontos ab, indem du ein Passwort festlegst

Master-Passwort (erforderlich)

Wichtig: Dein Master-Passwort kann nicht wiederhergestellt werden, wenn du es vergisst! Mindestens 12 Zeichen.

Stark

Master-Passwort bestätigen (erforderlich)

Master-Passwort-Hinweis

Wenn du dein Passwort vergessen hast, kann der Passwort-Hinweis an deine E-Mail-Adresse gesendet werden. Maximal 43/50 Zeichen.

Bekannte Datendiebstähle auf dieses Passwort überprüfen

Konto erstellen

Browser-Erweiterung installieren

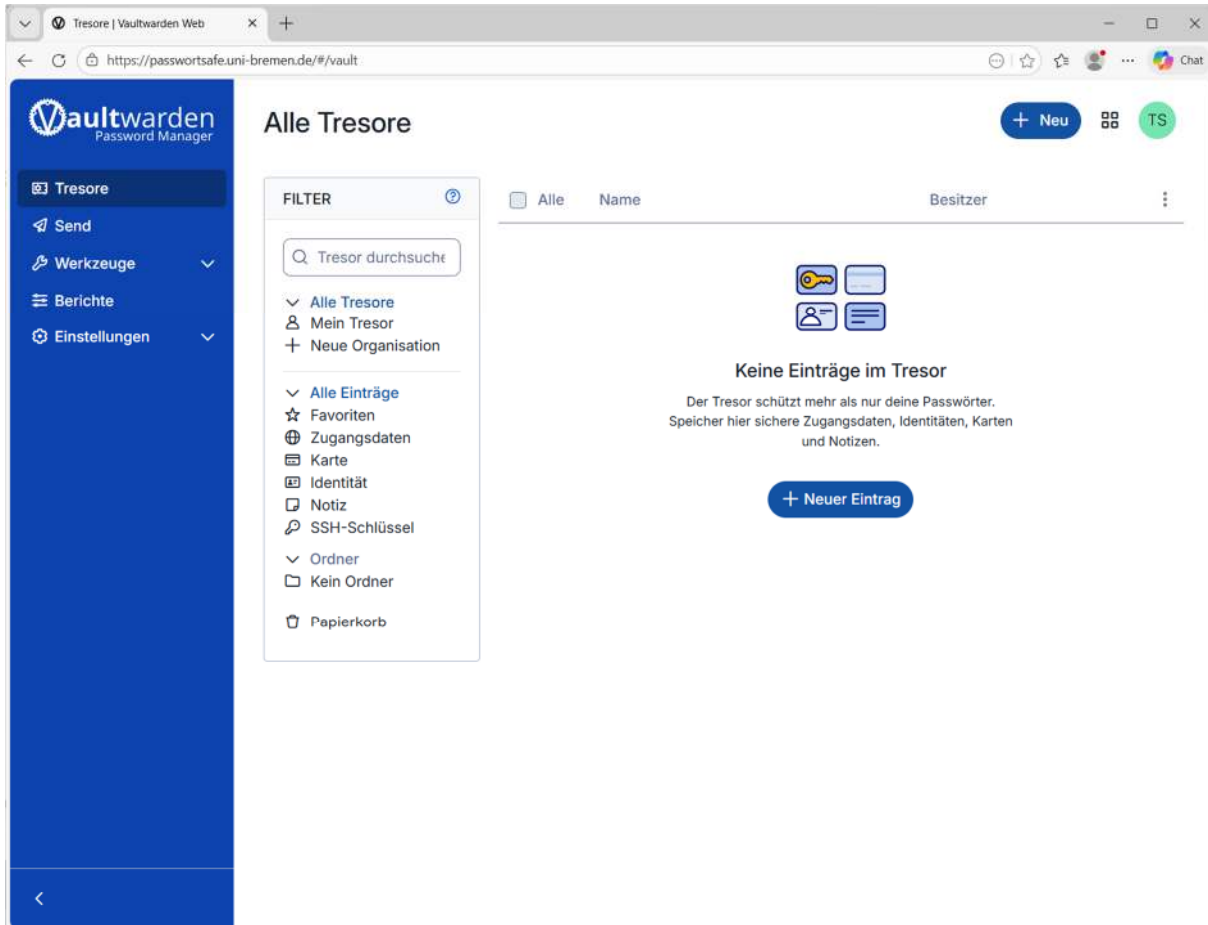
The screenshot shows a web browser window with the address bar displaying "https://passwordsafe.uni-bremen.de/#/setup-extension". The page features the Vaultwarden logo and the headline "Fülle deine Passwörter sicher mit einem Klick automatisch aus". Below this, it says "Lade dir die Bitwarden Browser-Erweiterung herunter und nutze Auto-Ausfüllen noch heute". Three panels illustrate the user flow: "Create an account", a "Vault" interface, and "Sign in". A prominent blue button labeled "Erweiterung herunterladen" is centered, with a link "Später hinzufügen" below it. At the bottom, it states "Vaultwarden Web 2026.1.1" and includes a disclaimer: "A modified version of the Bitwarden® Web Vault for Vaultwarden (an unofficial rewrite of the Bitwarden® server). Vaultwarden is not associated with the Bitwarden® project nor Bitwarden Inc."

(auf Verwaltungs-Rechnern nicht in Edge)

Benutzung

Tresore (Vaults) sind die Orte, an denen Daten sicher abgelegt werden können. Neben Zugangsdaten sind dies vor allem Identitäten (Name, Adresse, etc.) zum automatischen Ausfüllen von Formularen.

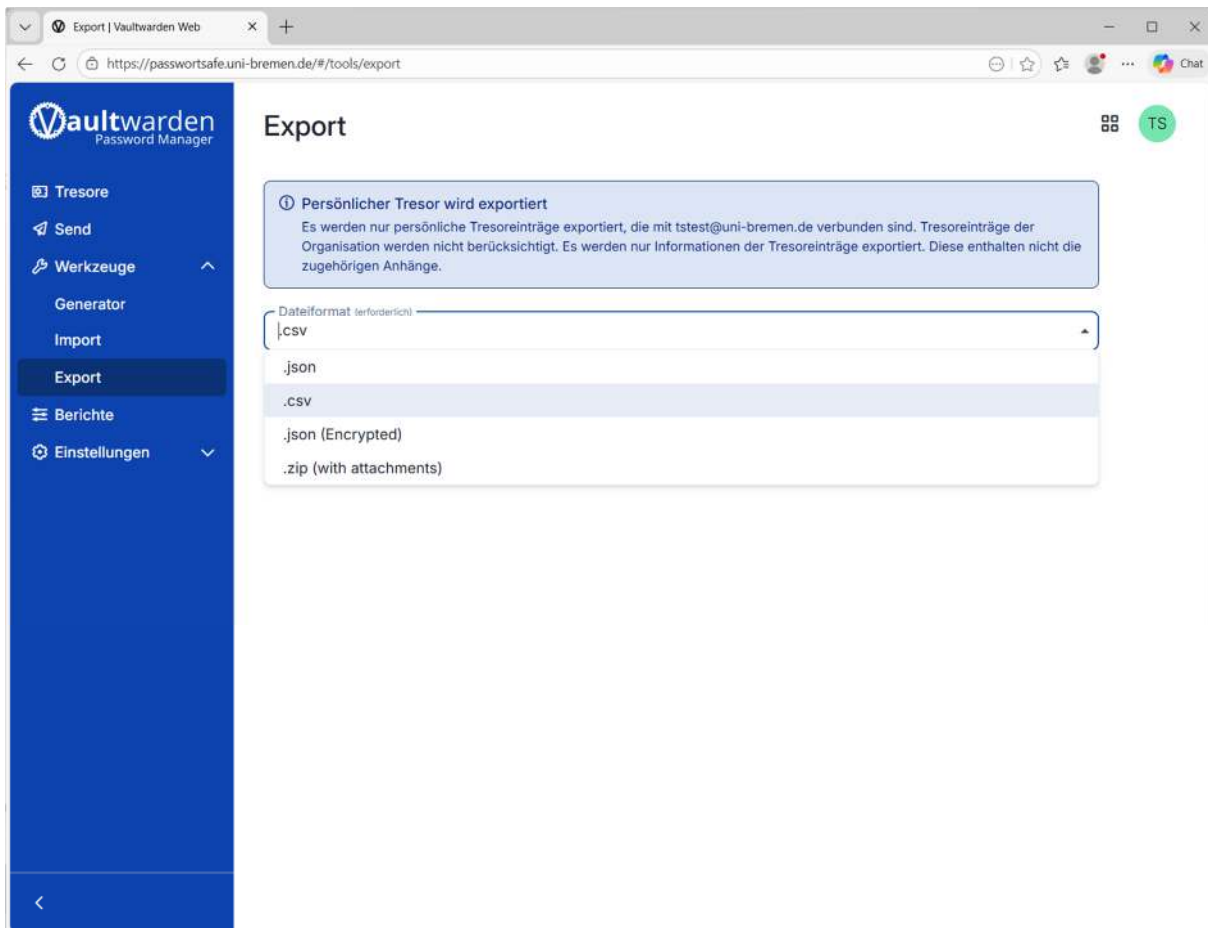
Zugangsdaten können hier händisch eingegeben werden, meistens wird das aber automatisch von der jeweiligen Login-Seite geschehen. Es können Ordner (Folder) zur Sortierung von Einträgen angelegt werden.



Es sollte regelmäßig ein Backup der Daten erfolgen. Dazu gibt es mehrere Formate:

- json (und Encrypted): dient hauptsächlich dazu, wieder in eine Vaultwardn-Instanz importiert zu werden
- csv: Tabelle in Klartext, universeller einsetzbar
- zip: enthält json und ggf Anhänge, nicht verschlüsselt

Die Empfehlung ist, eine CSV zu exportieren und dann mit 7-Zip ein verschlüsseltes Archiv zu erstellen (AES-256 als Algorithmus verwenden) und dieses dann sicher abzulegen. Das CSV muss noch entsprechend entsorgt werden.

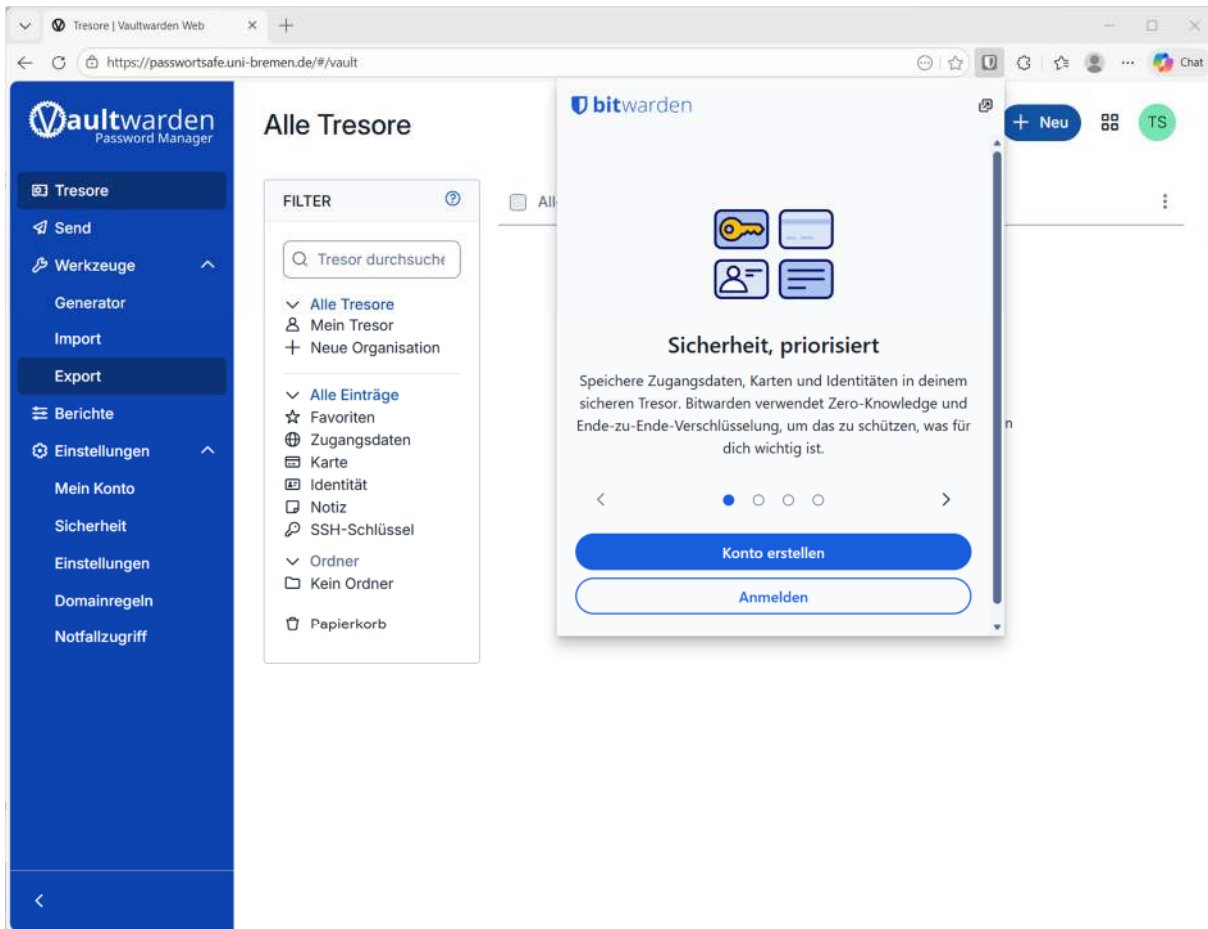


Mit dem Generator können schnell sichere Passwörter erstellt werden. Es ist sinnvoll, sowohl die Sonderzeichen als auch den Kasten „mehrdeutige Zeichen vermeiden“ anzuhaken, für den Fall, dass man mal das Passwort per Hand eingeben muss.

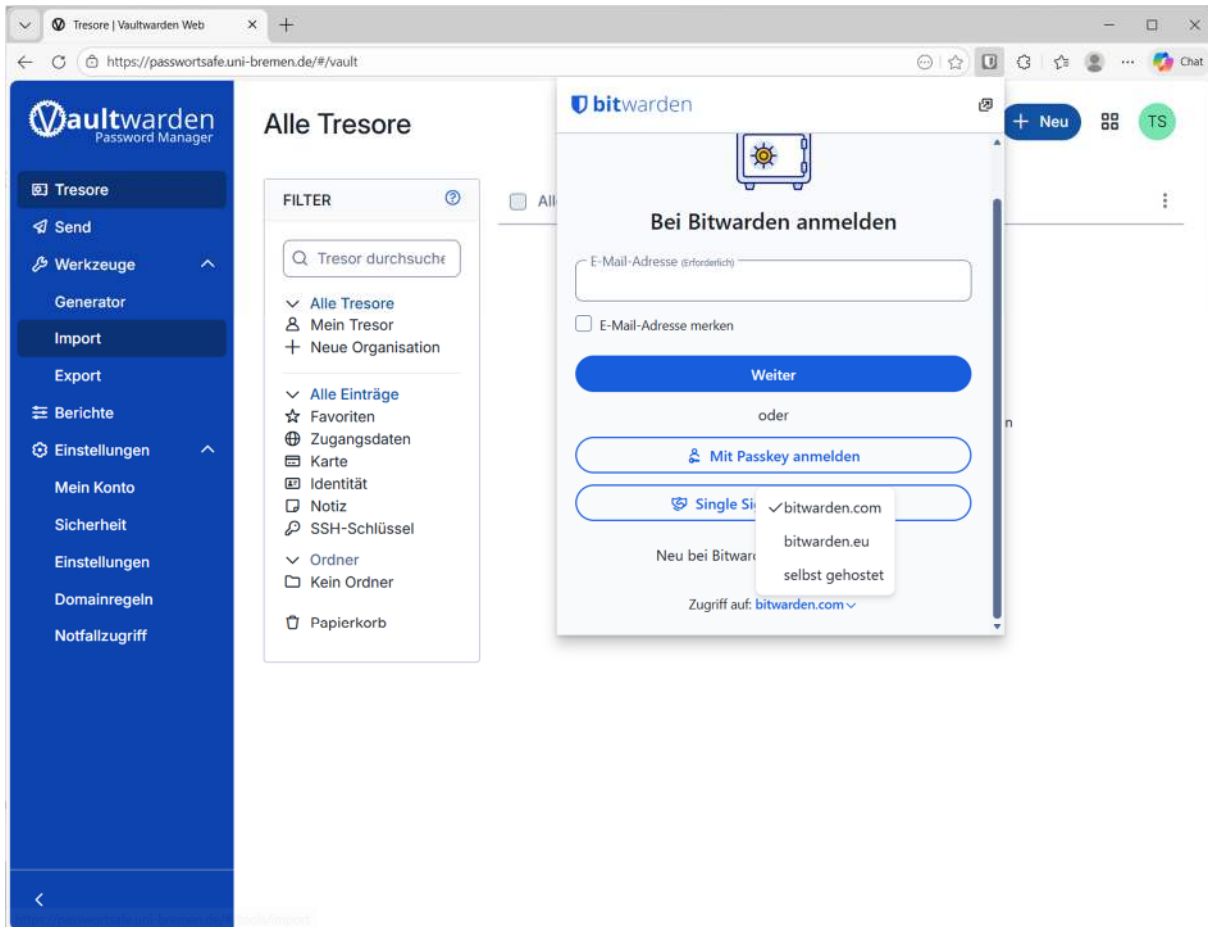
The screenshot shows the 'Generator' tool in the Vaultwarden Password Manager web interface. The browser address bar shows the URL <https://passwordsafe.uni-bremen.de/#/tools/generator>. The interface has a dark blue sidebar on the left with navigation options: Tresore, Send, Werkzeuge, Generator (selected), Import, Export, Berichte, Einstellungen, Mein Konto, Sicherheit, and Notfallzugriff. The main content area is titled 'Generator' and has three tabs: 'Passwort' (selected), 'Passphrase', and 'Benutzername'. A notification box says 'Passwörter schnell erstellen' with a close button. Below it, a generated password 'b2Xg1WJxYZM9E9' is shown with refresh and copy icons. The 'Optionen' section includes a 'Länge' field set to 14, with a note that the value must be between 5 and 128. The 'Einschließen' section has checkboxes for 'A-Z', 'a-z', '0-9', and '!@#%*&+', with the first three checked. Below are 'Mindestanzahl Ziffern' (1) and 'Mindestanzahl Sonderzeichen' (0) fields. A checkbox for 'Mehrdeutige Zeichen vermeiden' is present and unchecked. At the bottom, there is a 'Generator-Verlauf' section.

Browser-Erweiterung

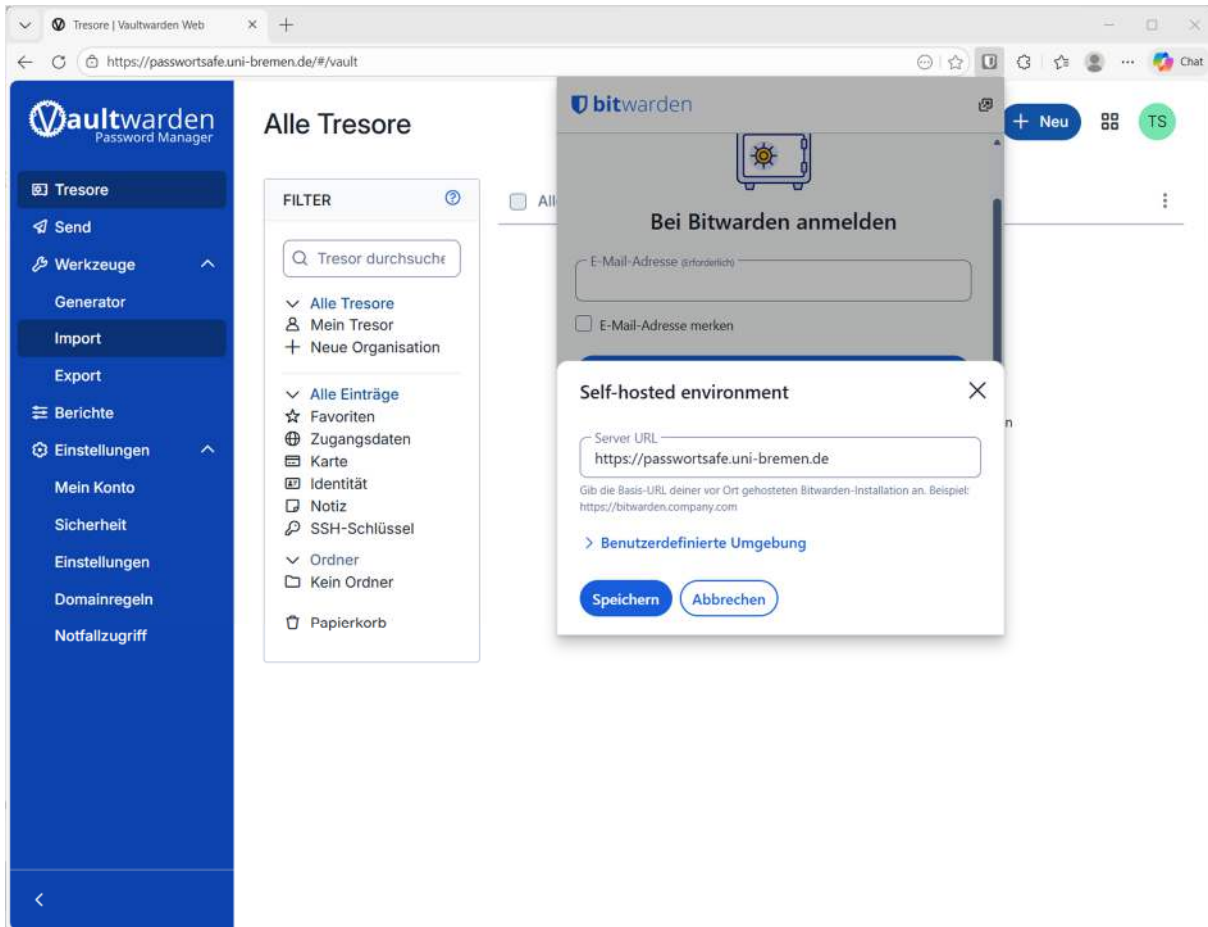
Auf das Icon der Erweiterung in der Browserleiste klicken, „anmelden“ wählen.



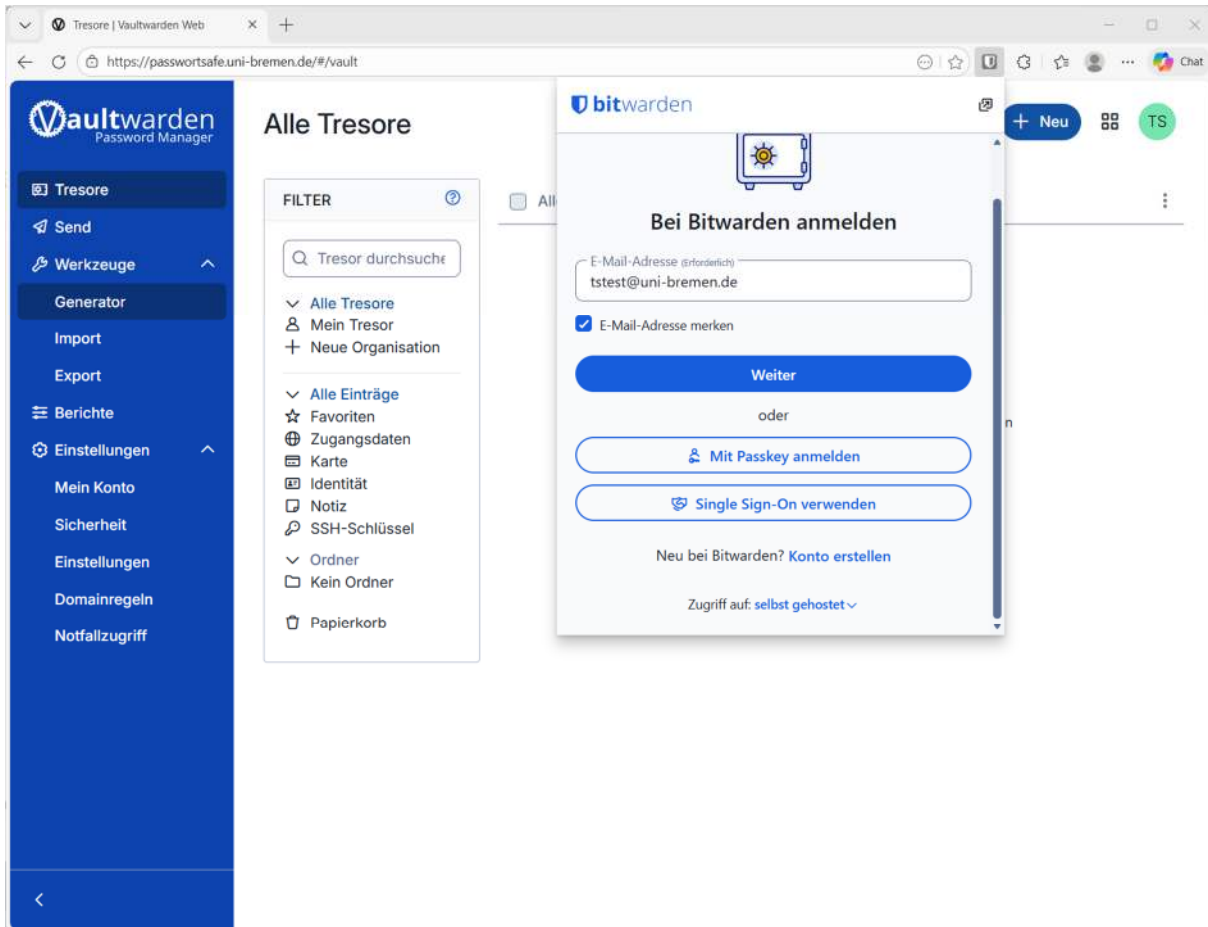
Ganz nach unten scrollen (falls nicht alles angezeigt wird) und bei „Zugriff auf:“ den Eintrag „selbst gehostet“ wählen.



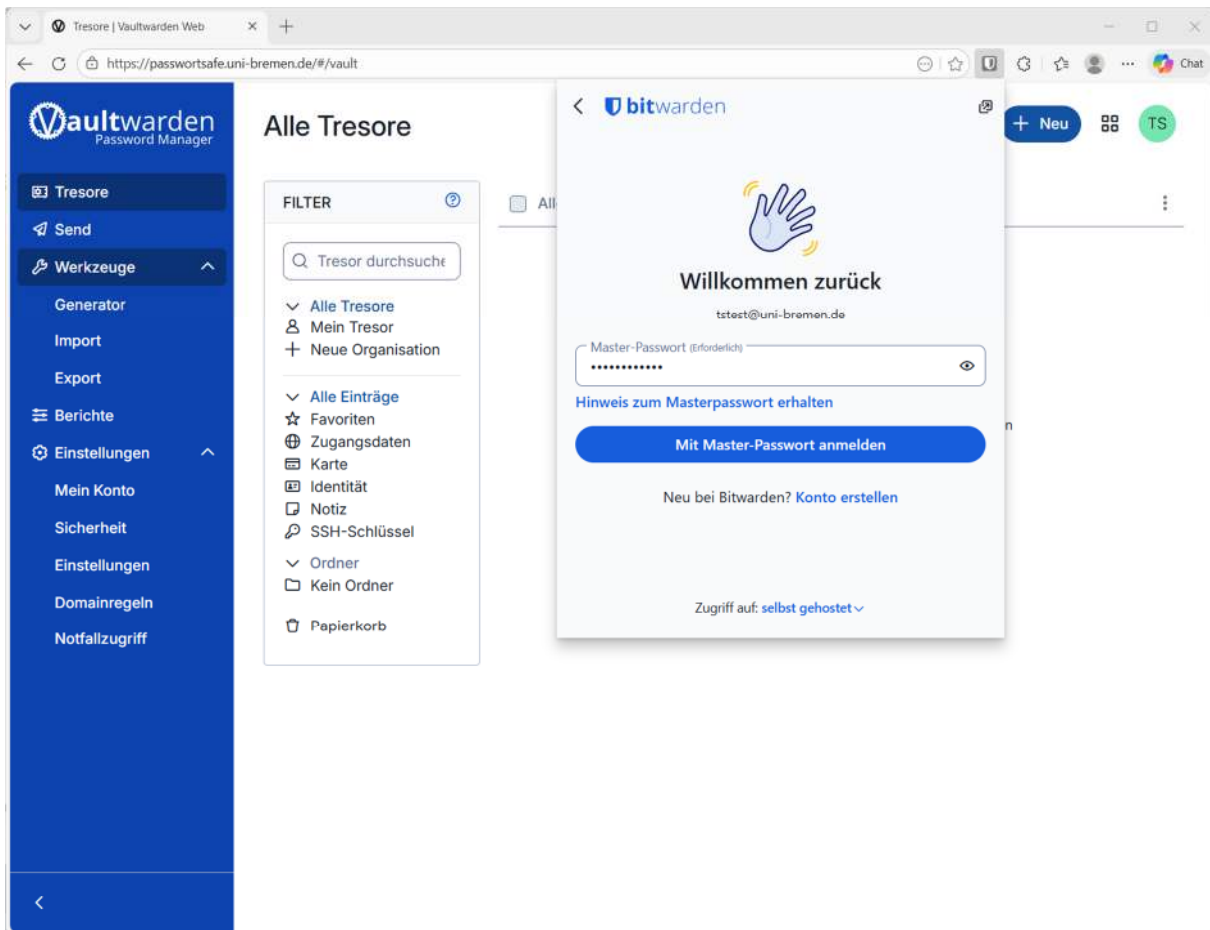
Bei Server URL <https://passwortsafe.uni-bremen.de> eingeben. Es sind keine weiteren Einstellungen nötig.



Die E-Mail-Adresse eingeben, die für die Anmeldung benutzt wurde. „E-Mail-Adresse merken“ anhaken, „weiter“ klicken.

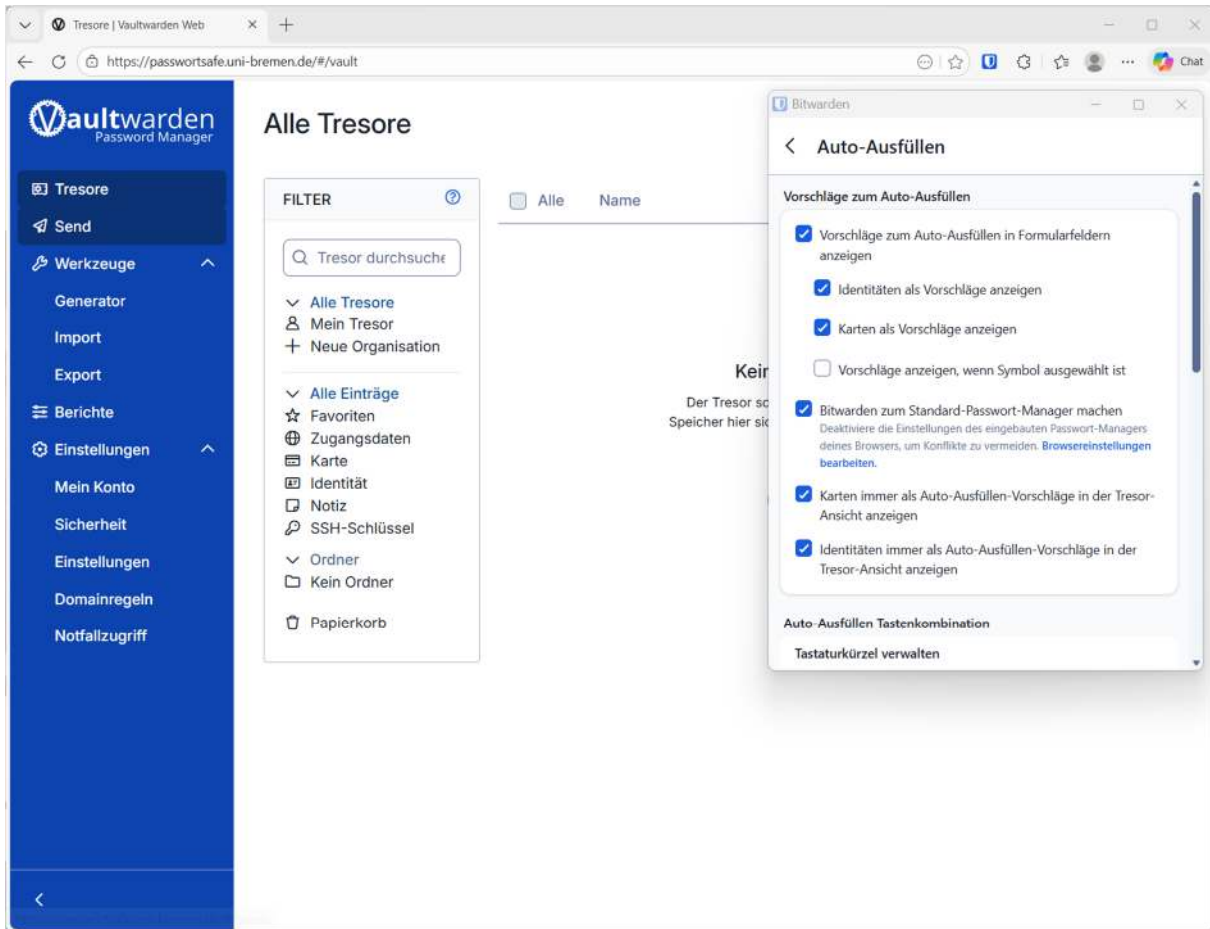


Master-Passwort eingeben, anmelden.



Einstellungen anpassen.

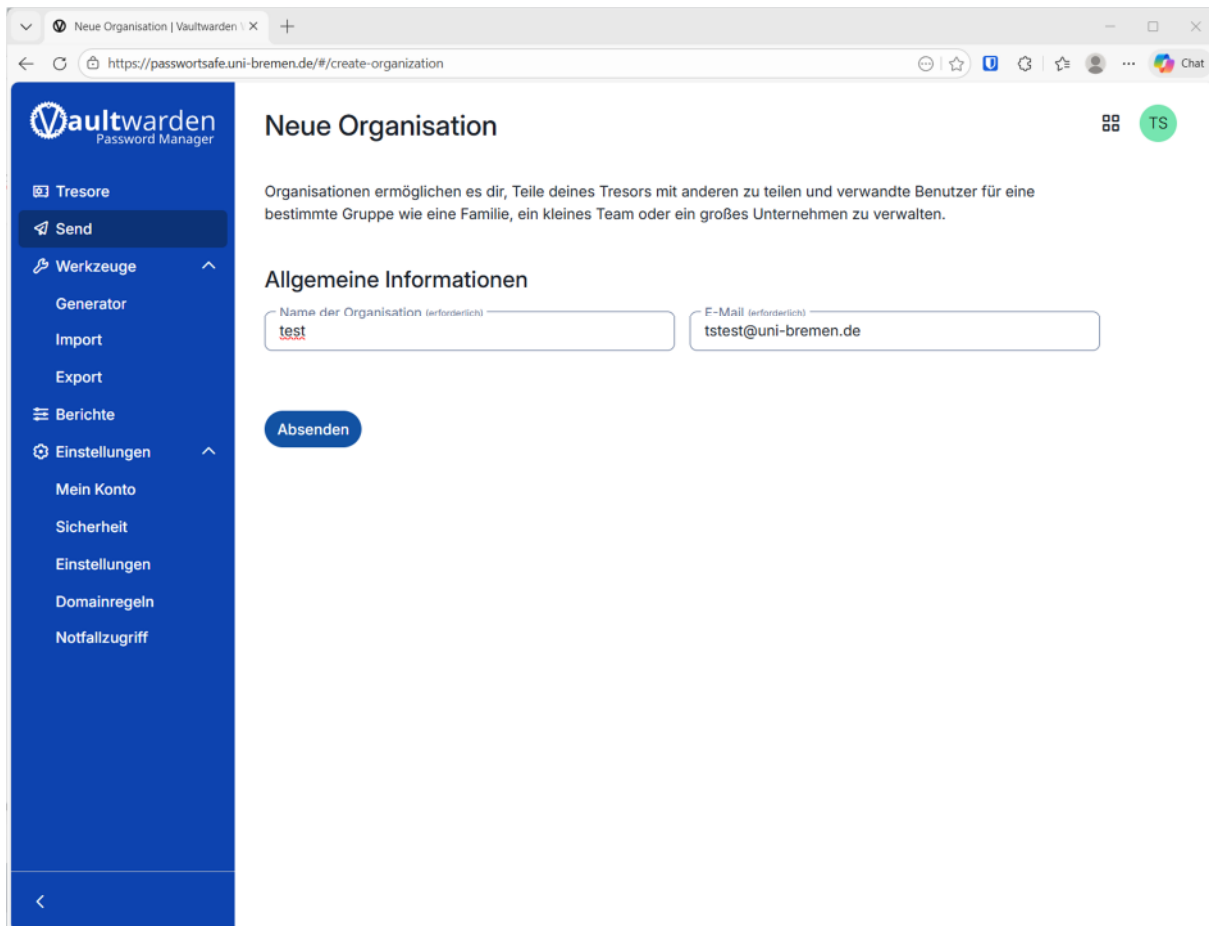
Es wird empfohlen, „Bitwarden zum Standard-Passwort-Manager machen“ auszuwählen und die Auto-Ausfüllen-Option des Browsers zu deaktivieren.



Organisationen

Organisationen sind Gruppen von Usern, die auf gemeinsame Passwörter zugreifen wollen. Der Name muss eindeutig und einzigartig sein. Ein User kann Mitglied in mehreren Organisationen sein.

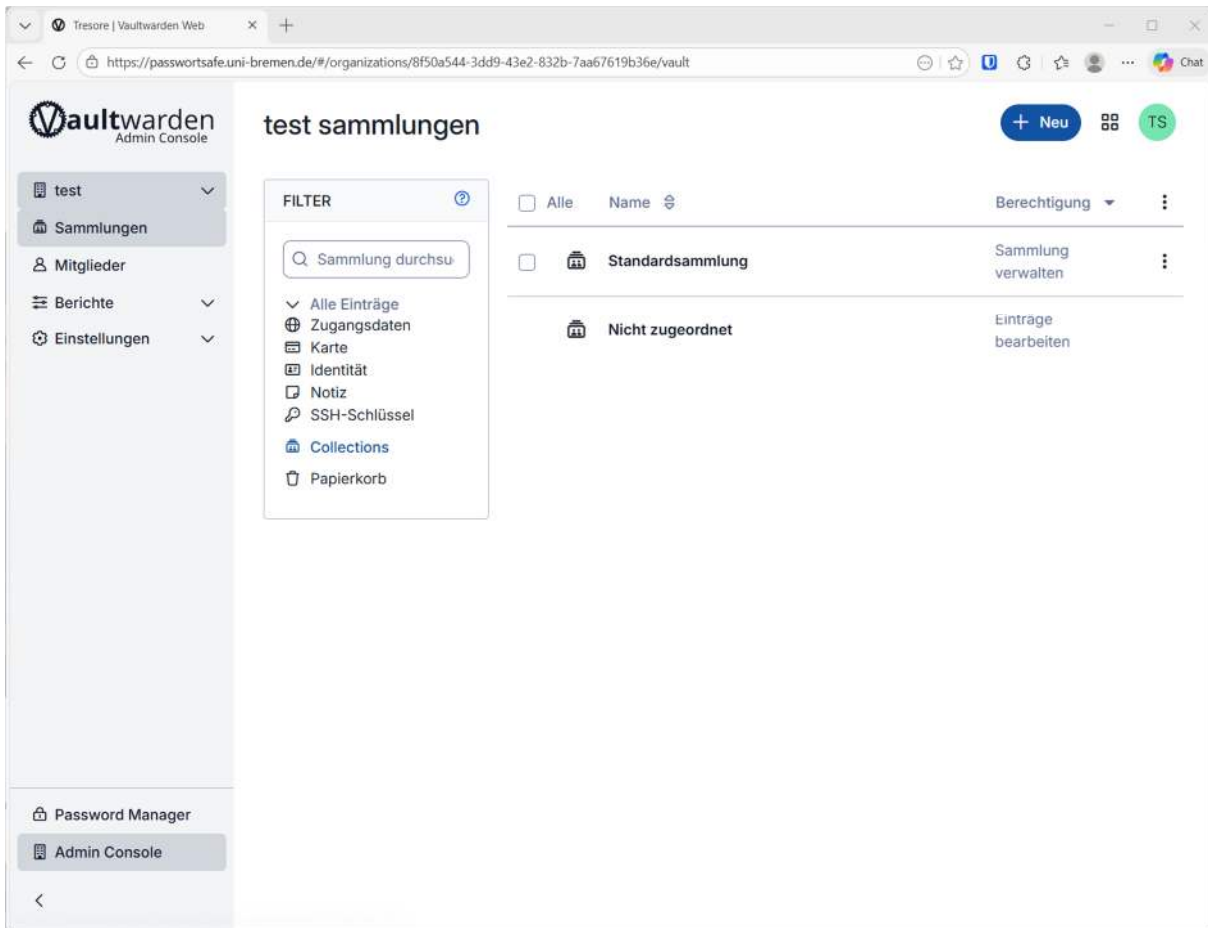
Organisations-Ersteller (Besitzer) und -Administratoren haben **IMMER** Zugriff auf **ALLE** Einträge in der Organisation, aber **NICHT** auf Einträge, die die User außerhalb der Organisation ablegen.



The screenshot shows a web browser window with the URL <https://passwordsafe.uni-bremen.de/#/create-organization>. The page title is "Neue Organisation". On the left is a blue sidebar menu with the Vaultwarden logo and the text "Password Manager". The menu items are: Tresore, Send, Werkzeuge (with a sub-menu arrow), Generator, Import, Export, Berichte, Einstellungen (with a sub-menu arrow), Mein Konto, Sicherheit, Einstellungen, Domainregeln, and Notfallzugriff. The main content area has a heading "Neue Organisation" and a sub-heading "Allgemeine Informationen". Below the heading is a descriptive paragraph: "Organisationen ermöglichen es dir, Teile deines Tresors mit anderen zu teilen und verwandte Benutzer für eine bestimmte Gruppe wie eine Familie, ein kleines Team oder ein großes Unternehmen zu verwalten." There are two input fields: "Name der Organisation (erforderlich)" with the value "test" and "E-Mail (erforderlich)" with the value "tstest@uni-bremen.de". A blue "Absenden" button is located below the input fields. In the top right corner of the page, there is a grid icon and a green circular profile icon with the initials "TS".

Mitglieder werden per E-Mail-Adresse eingeladen und müssen zu dem Zeitpunkt noch kein Konto im Passwortsafe besitzen. Zugriffsrechte können detailliert vergeben werden.

Es können Ersatz-Besitzer deklariert werden, die bei Ausfall des ursprünglichen Besitzers nach Ablauf einer Wartezeit (normalerweise 7 Tage, besser kürzer einstellen) die Organisation komplett übernehmen können. Die Wartezeit ist dazu da, damit niemand bössartig die Kontrolle übernehmen kann, da der Zugriff während dieser Zeit widerrufen werden kann.



Beispiel für die Nutzung einer Organisation:

Drei User (Anna, Bernd und Christina) möchten gemeinsam auf Passwörter zugreifen. Anna legt dazu eine Organisation „AG Schulze“ an und lädt die anderen beiden ein. Sobald sich diese angemeldet haben, muss sie sie noch bestätigen. Sie erstellt 4 Sammlungen (Collections): einen pro User mit entsprechendem Namen und „Alle“ für alle.

Sie ändert die Zugriffsrechte so, dass auf die benannten Ordner nur jeweils der passende User Zugriff hat, während alle auf die Sammlung „Alle“ vollen Zugriff haben. So kann jeder eigene Passwörter sicher ablegen und solche, die alle betreffen, teilen. Sollte nun jemand ausfallen, kann Anna einem anderen User die Rechte auf den entsprechenden Ordner geben, sodass die Passwörter dort verwendet werden können. Später können die Rechte wieder entzogen werden.

Zur Sicherheit macht Anna dann noch Christina zum Ersatz-Besitzerin, falls Anna ausfallen sollte.