Bitwarden Passwortmanager



Bitwarden ist eine App zum Verwalten von Passwörtern, Zugangsdaten und sicheren Notizen. Diese können verschlüsselt zwischen verschiedenen Geräten synchronisiert werden.

Die App kann auf allen iPads installiert werden.

Warum einen Passwortmanager verwenden?

Passwörter sollen möglichst lang, komplex und unaussprechlich sein, um nicht erraten werden zu können. Allerdings lassen sich sichere Passwörter wie `tA9^i7HuZo9URr$w` nur schlecht merken. Eine Lösung können Passwort-Manager sein, wie sie z.B. iPads oder auch viele Browser von Haus aus bieten. Die Verwendung einer separaten Passwort-Manager-App bietet noch weitere Vorteile:

- Passwörter können über mehrere Geräte und Browser synchron gehalten werden
- unsichere Passwörter können erkannt werden
- sichere Passwörter können automatisch erzeugt werden
- man muss sich nur ein „Master-Passwort“ merken
- kann One-Time-Passwörter (OTP) für Zwei-Faktor-Authentifizierung generieren

Die App Bitwarden ist ein bewährter Passwortmanager mit ausgereiften Funktionen. Sie kann mit verschiedenen Speicherdiensten verbunden werden um die Passwörter verschlüsselt zu synchronisieren. Am GGD steht für schulische Zwecke der Dienst Vaultwarden zur Verfügung.

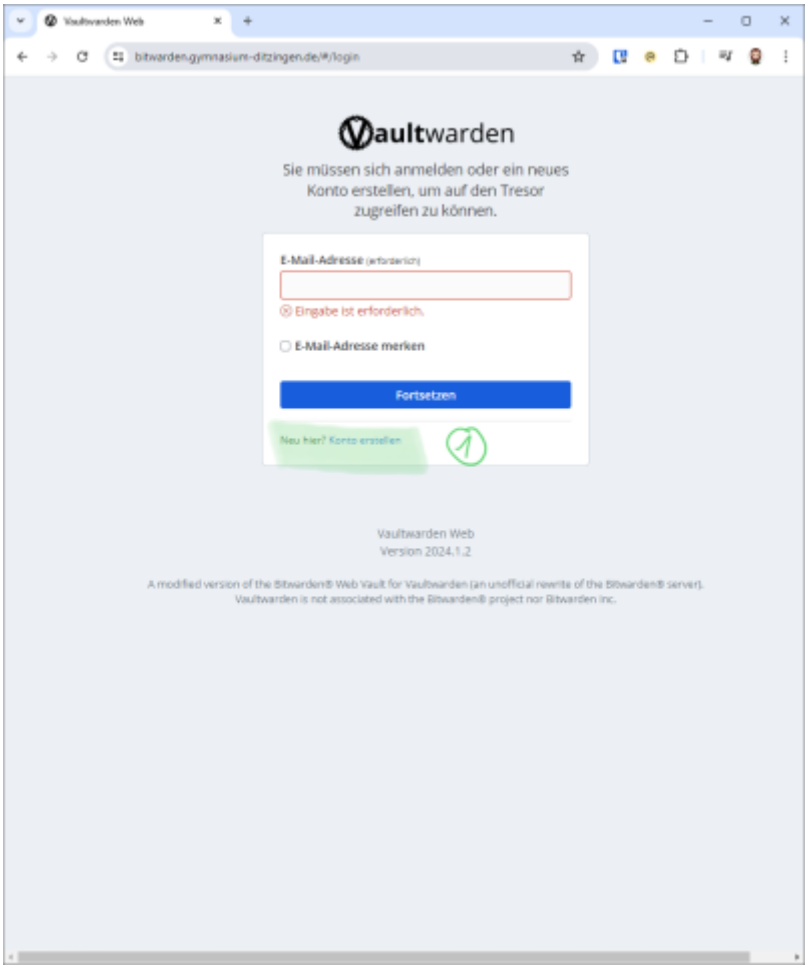
Dabei wird der Passwortspeicher als „vault“ oder Tresor bezeichnet. Diese Datei wird verschlüsselt synchronisiert und stets nur lokal enstchlüsselt (auch im Browser).

Eine ausführliche Anleitung des Herstellers gibt es hier: https://bitwarden.com/de-de/help/

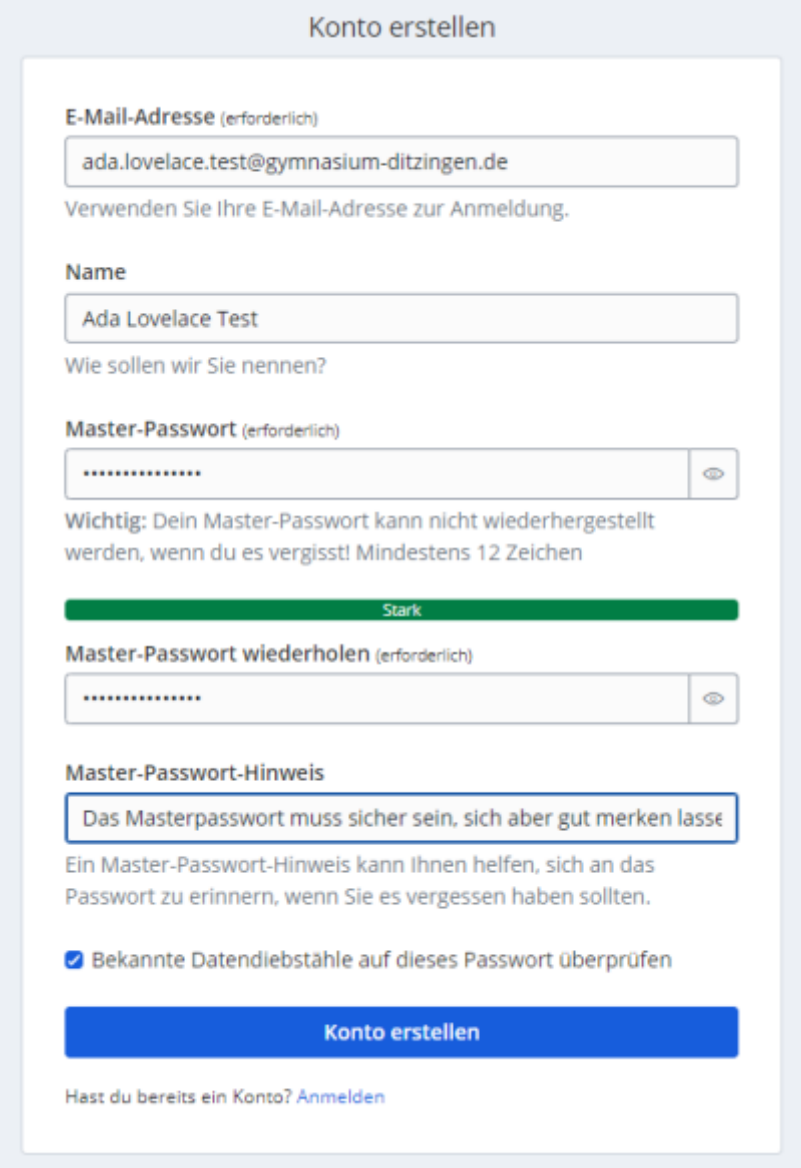
> **Haftungsausschluss**
>
> Das GGD stellt die App „Bitwarden“ und den Dienst „Vaultwarden“ für schulische Zwecke zur Verfügung. Wie für alle anderen Dienste auch, gilt: Nutzende sind selbst für die Sicherung ihrer Daten verantwortlich! (vgl.
>
> Nutzungsordnung
>
>)
>
> Das Admin-Team und das GGD übernehmen keine Verantwortung für verlorengegangene Daten, die in Bitwarden oder Vaulwarden gespeichert wurden oder für Daten die aufgrund von Fehlern oder Fehlbedienung der App Bitwarden oder des Dienstes Vaultwarden unzugänglich georden sind.

Account einrichten

Bevor Bitwarden genutzt werden kann, muss zunächst unter https://bitwarden.gymnasium-ditzingen.de ein Account angelegt werden.



1 Zunächst auf „Konto erstellen“ klicken.



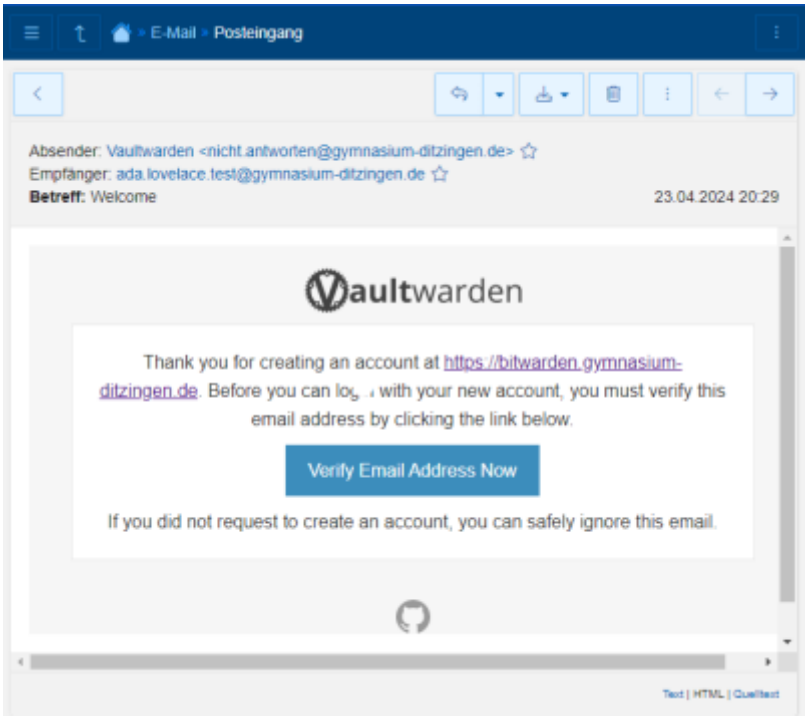
Die Daten zur Registrierung eingeben.

Schulische Mailadresse verwenden

Zur Registrierung können nur schulische Mailadressen verwendet werden!

Master-Passwort klug wählen

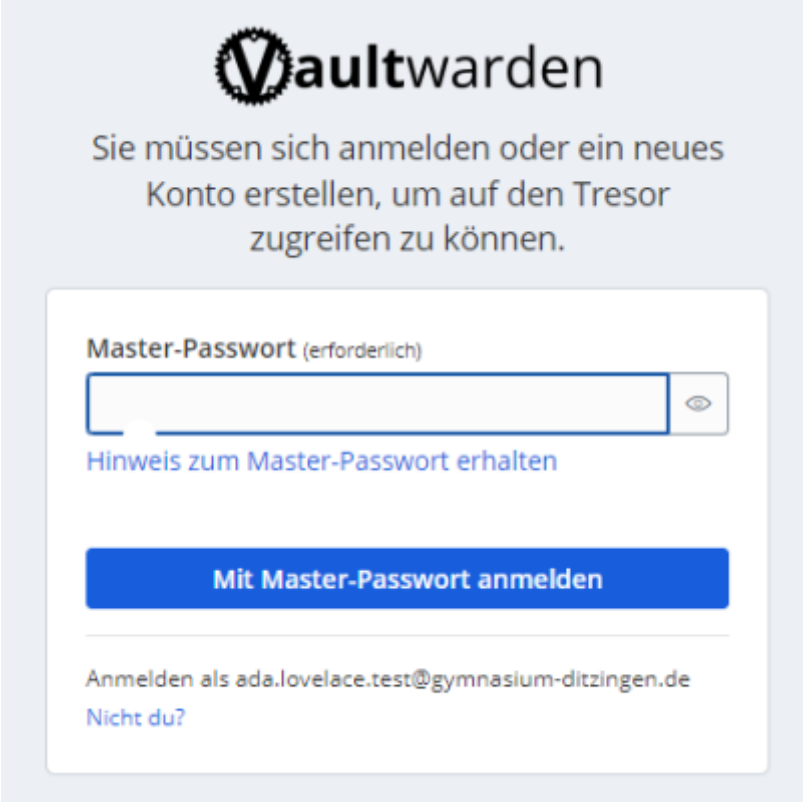
Das Master-Passwort schützt alle gespeicherten Passwörter vor den Zugriffen anderer. Es sollte ebsodners sicher sein und muss mindestens 12 Zeichen haben. **Achtung!**, Ohne das Master-Passwort kann man nicht mehr auf Bitwarden zugreifen. Auf gar keinen Fall vergessen! An einem sicheren Ort notieren und aufbewahren. **Tipp:** Einen Satz ausdenken und z.B. die Anfangsbuchstaben der Wörter als Passwort verwenden. Geeignete Buchstaben durch Zahlen bzw. Sonderzeichen ersetzen.

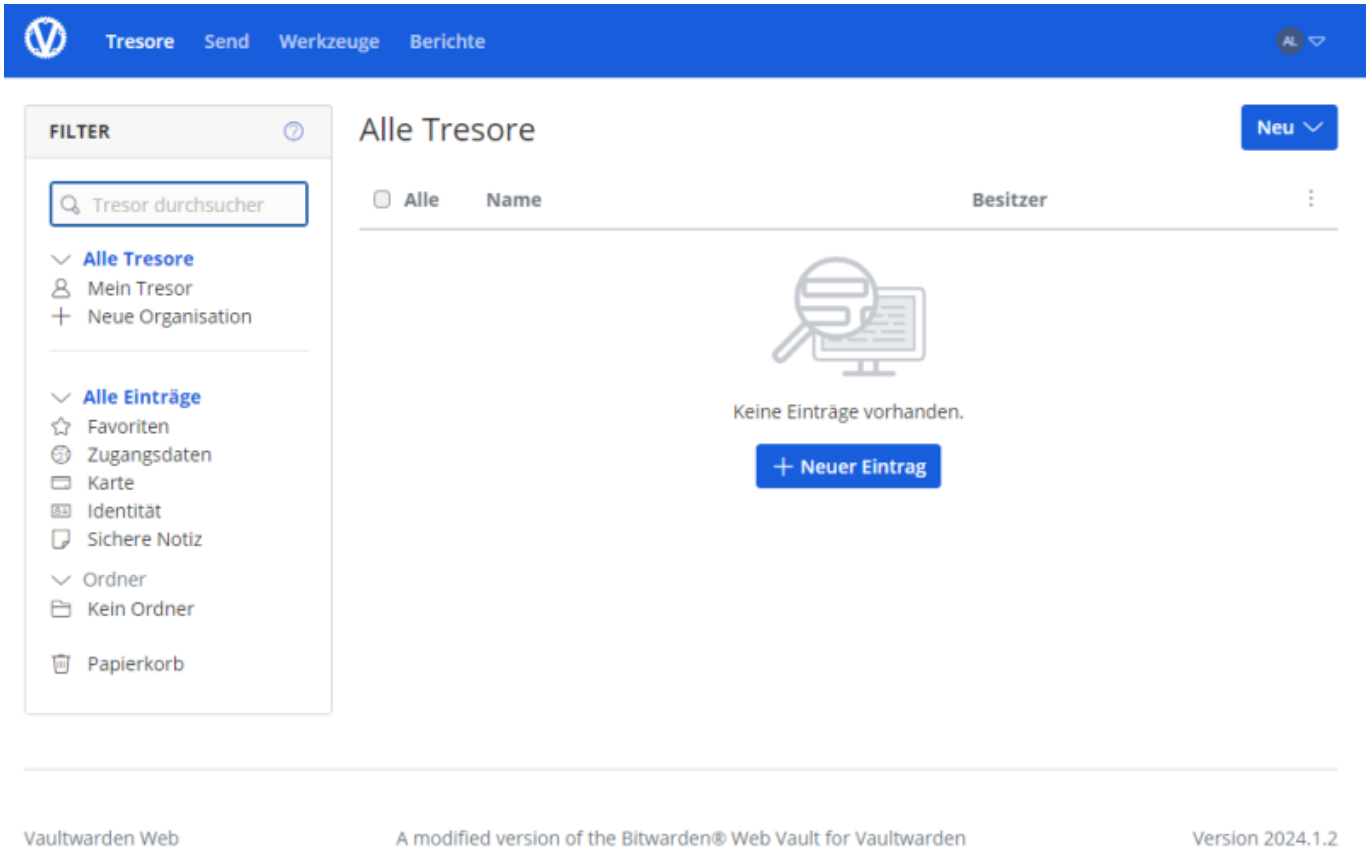


Die angegeben Mailadresse muss aus Sicherheitsgründen bestätigt werden. Dazu auf den Link in der Mail klicken. Aus technischen Gründen kann diese Mail derzeit nur auf Englisch verschickt werden.

Nun unter https://bitwarden.gymnasium-ditzingen.de mit der registrierten Mail-Adresse und dem Master-Passwort anmelden.



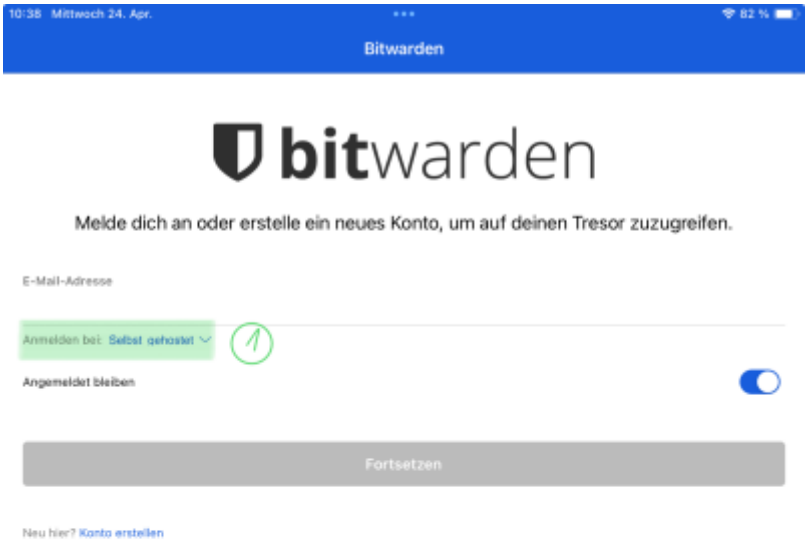


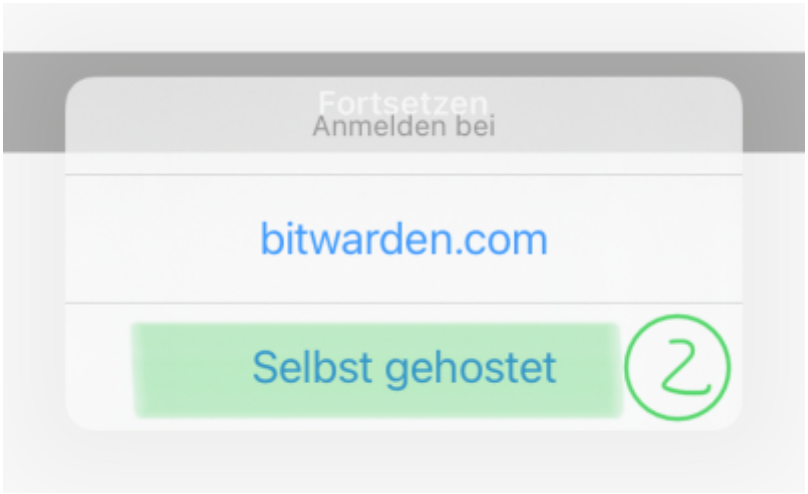


Der Passwort-Tresor kann nun (im Browser) genutzt werden.

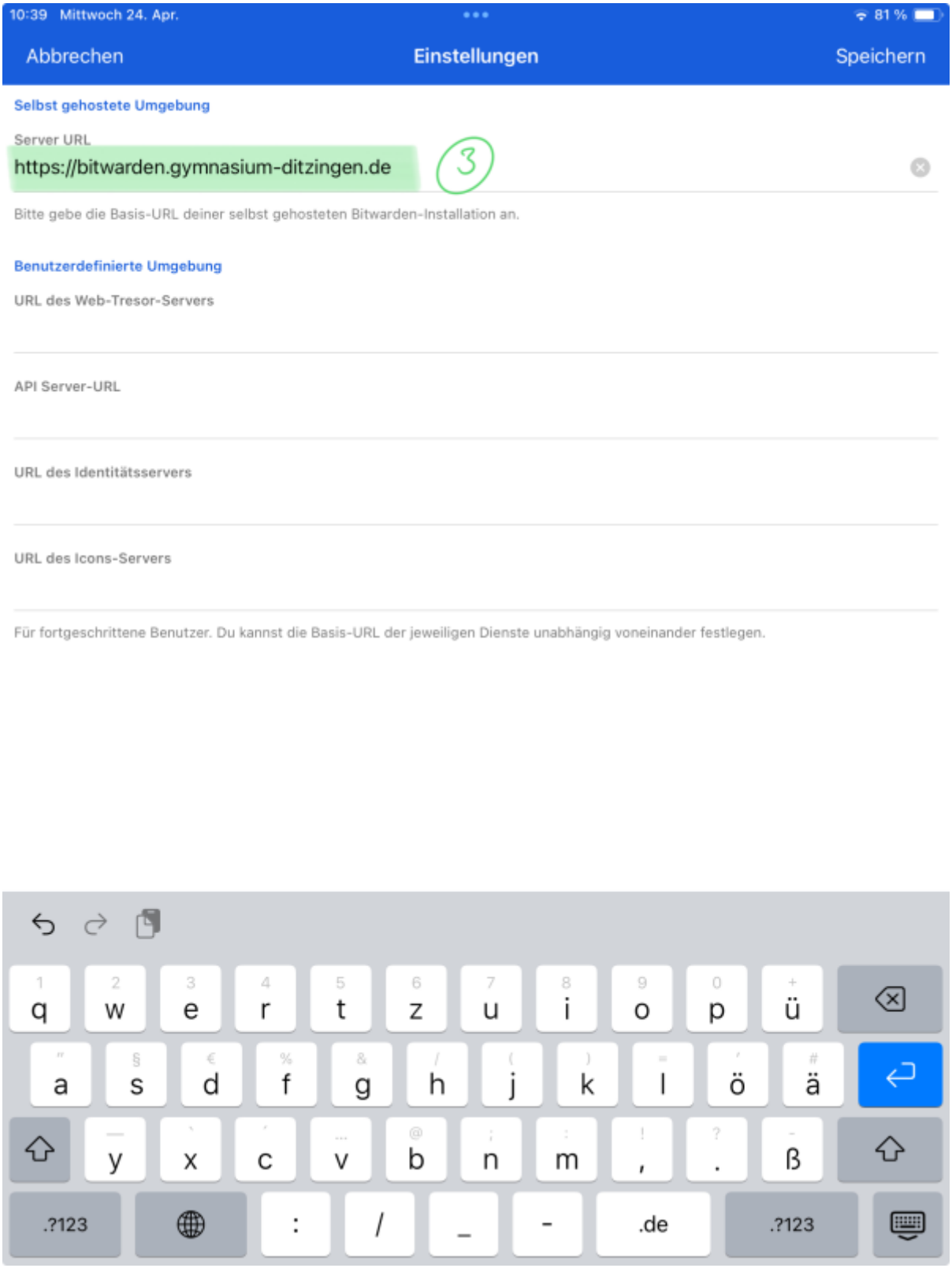
App einrichten

Um die Passwortmananer-App auf dem iPad einzurichten die App öffnen. Bitwarden bietet die Möglichkeit kommerziell betriebende Server oder selbstbetriebene Server für die Synchronisation zu verwenden. Das GGD betreibt für schulische Zwecke einen eigenen Vaultwarden-Server unter https://bitwarden.gymnasium-ditzingen.de. Die App muss zunächst mit diesem Server verbunden werden.

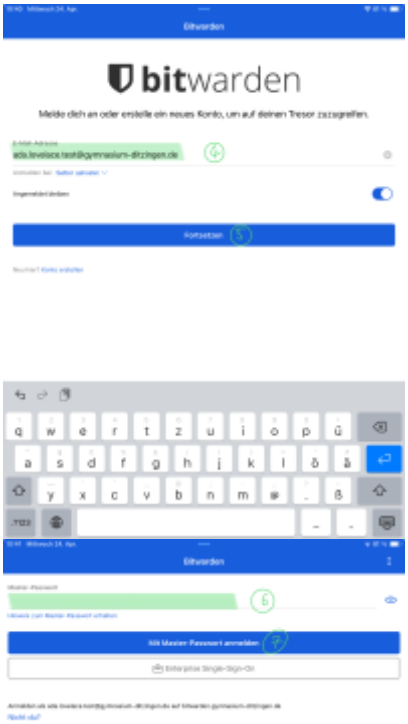




Dazu in der App auf „selbst gehostet“ **1** klicken und im sich danach öffnenden Auswahldialog erneut auf „selbst gehostet“ **2** klicken.



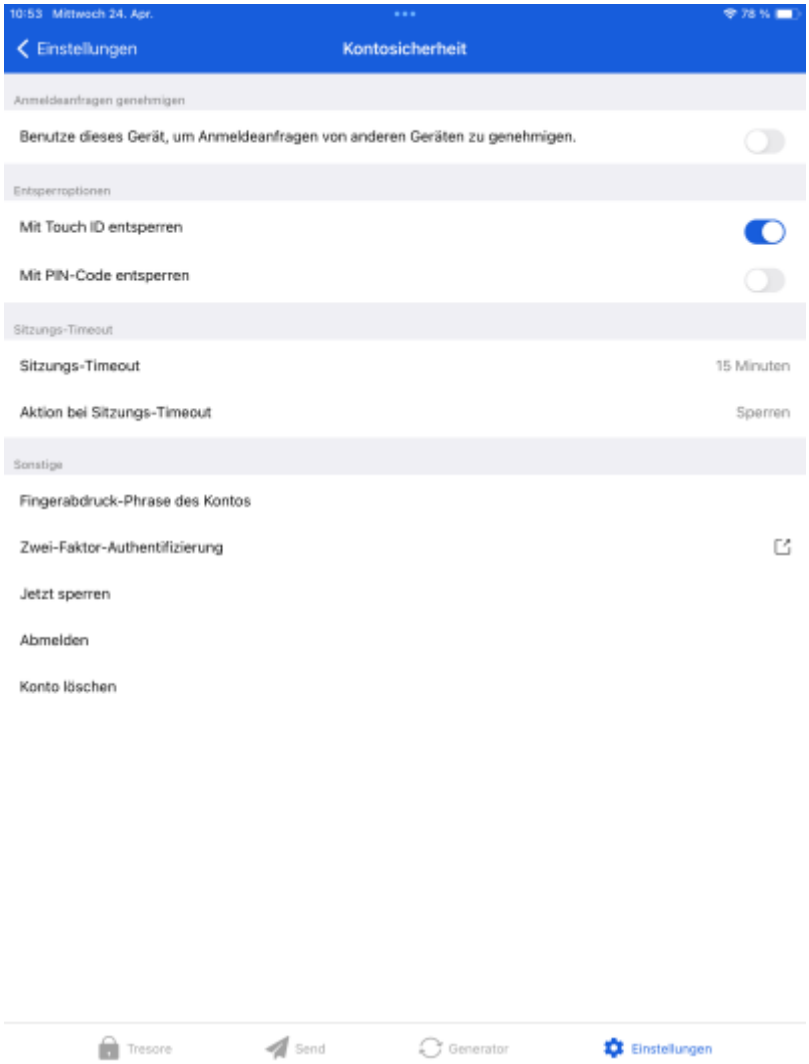
In den Einstellungen muss nur unter „Server-URL“ **3** die Adresse https://bitwarden.gymnasium-ditzingen.de eingetragen werden. Dann auf „Speichern“ klicken.



Nun kann die App mit dem zuvor eingerichteten Account verbunden werden: dazu Mailadresse und Masterpasswort eingeben und „Mit Master-Passwort anmelden“ antippen.

Touch ID und Code verwenden

> **Tipp: Touch-ID**
>
> Das Master-Passwort muss jedes mal eingegeben werden, um den Passwort-Tresor zu entschlüsseln. Man kann stattdessen aber den Fingerabdruck über Touch-ID verwenden.

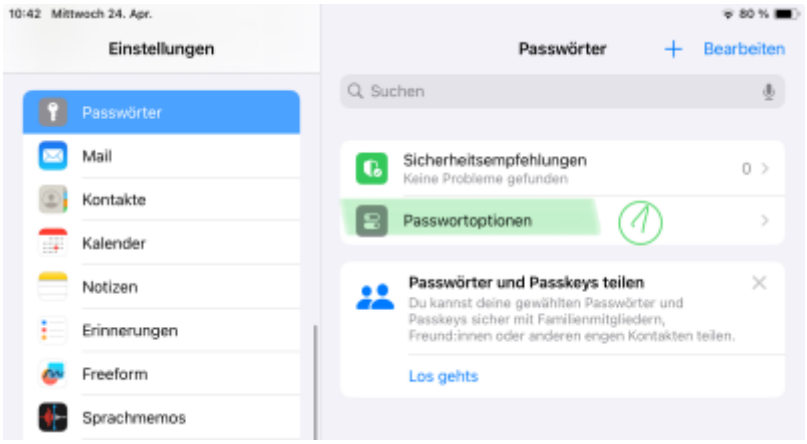


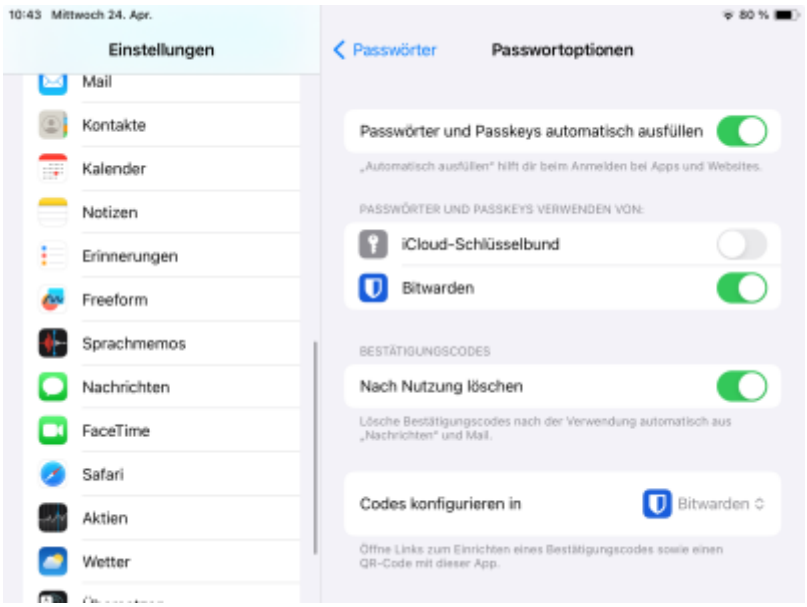
Dazu in der Bitwarden-App auf Einstellungen > Kontosicherheit gehen und „Mit Touch ID entsperren aktivieren“. Es ist auch möglich die PIN des iPads als weitere Entsperrmöglichkeit des Passwort-Tresors zu verwenden.

Bitwarden als Standard-Passwortmanager einrichten

In den Standardeinstellungen speichert ipadOS Passwörter in seinem internen Speicher und sucht auch nur dort danach. Diese Passwörter werden genutzt um Anmeldefelder in Webseiten und Apps automatisch auszufüllen. Man kann ipadOS so einstellen, dass für das automatische Ausfüllen stattdessen Bitwarden verwendet wird.

Dazu in der **Einstellungen-App** auf **Passwörter** und „Passwort-Optionen“„ **1** gehen und Bitwarden als Passwortspeicher aktivieren (vgl. Abbildung).





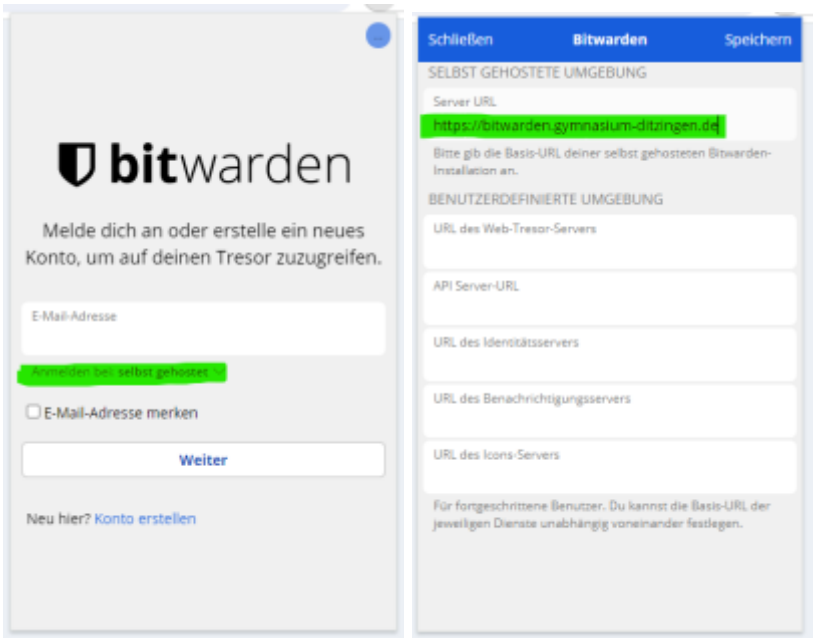
weitere Clients

Bitwarden ist auch als App erhältlich für

- Windows
- MacOS
- Linux
- iOs
- Android

Browser-Plugins sind verfügbar für alle gängigen Browser (Firefox, Chrome, Safari, Opera, Vivaldi, Brave, ...)

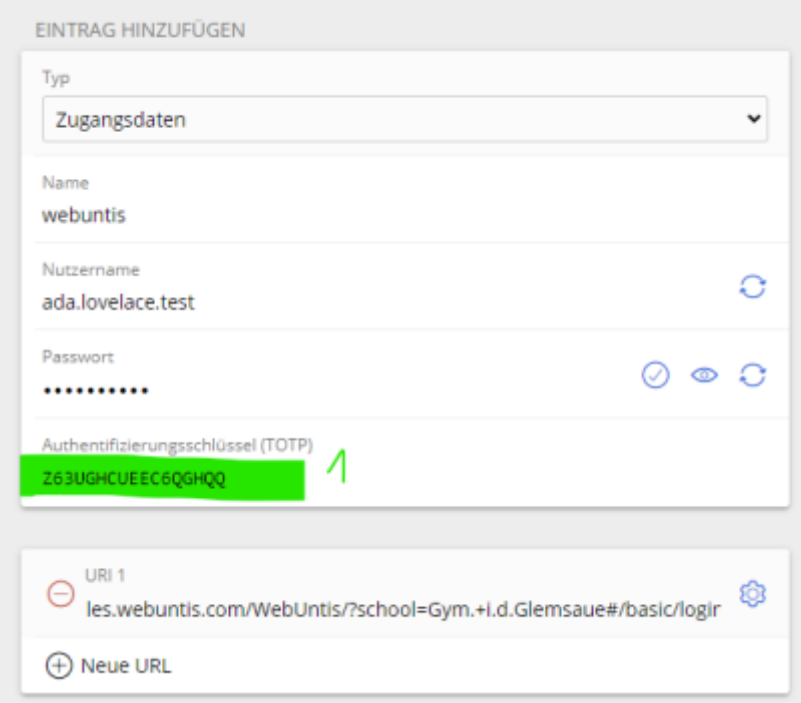
> **korrekten Server einstellen**
>
> In allen Clients muss jeweils **„selbst gehostet“** bei `Anmelden bei` ausgewählt werden und die Url des Vaultwarden-Dienstes (**https://bitwarden.gymnasium-ditzingen.de**) als `Server-URL` eingetragen werden.



Zwei-Faktor-Authentifizierung einrichten

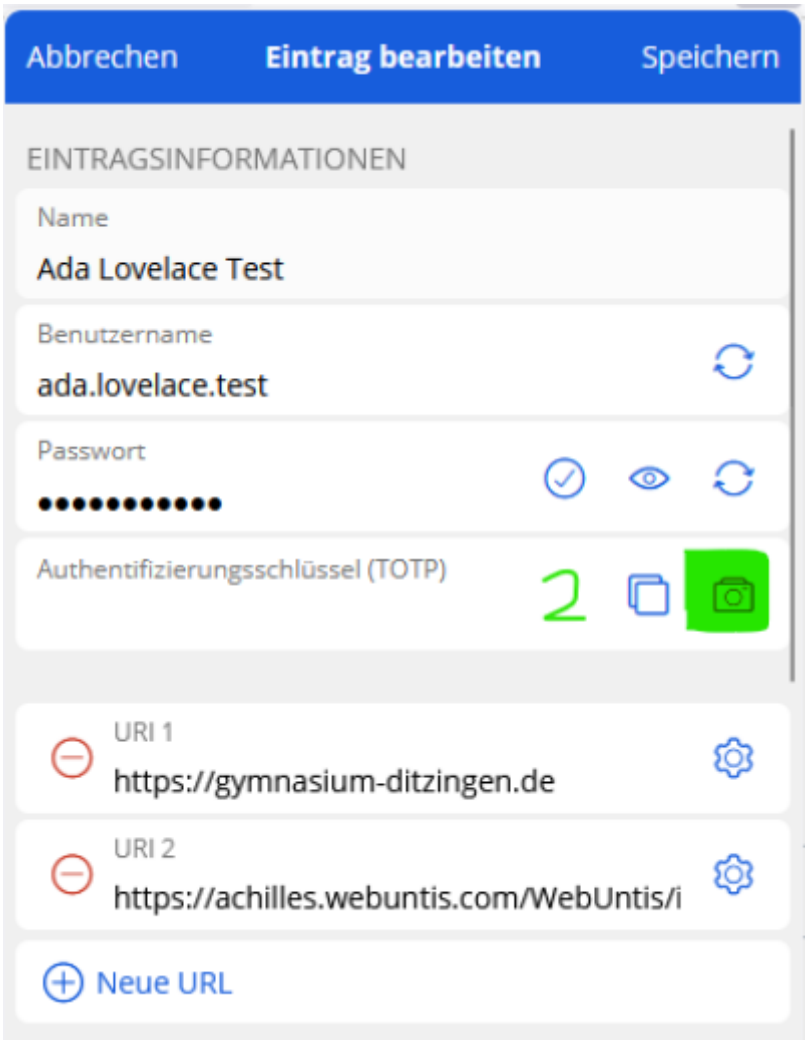
Bitwarden kann auch dazu verwendet werden, um Zugänge zu Diensten mit einem 2. Faktor abzusichern (Zwei-Faktor-Authentifizierung (2FA)). Dazu muss der Schlüssel manuell in den Passworteintrag in Bitwarden kopiert werden. Bitwarden generiert daraus dann ein zeitabhängiges Einmalpasswort (TOTP). Inzwischen (Nov. 24) kann man das auch per QR-Code.





Die meisten Plattformen bieten den Schlüssel für die Zwei-Faktor-Authentifizierung als QR-Code an, die dann mit Schlüsselgenerator-Apps wie FreeOTP Authenticator abfotografiert werden können. UPDATE (28.11.24 Wei): Die Bitwarden-App kann das auch.

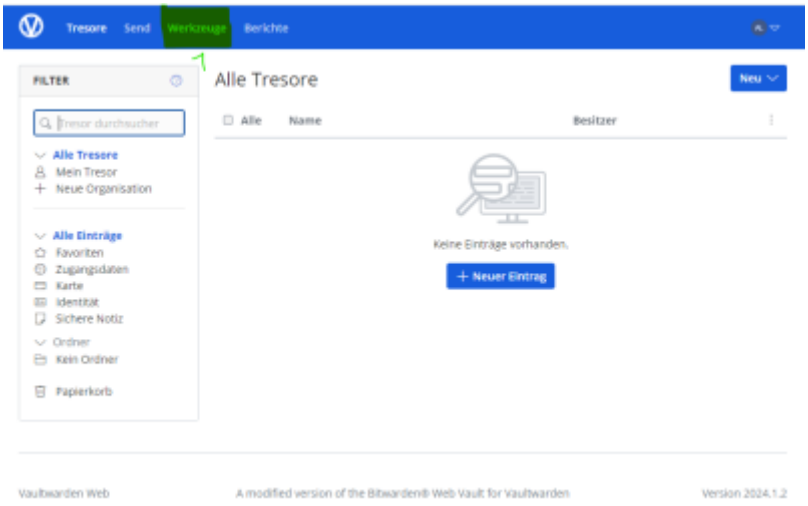
~~Für den Eintrag in die Bitwarden-App muss der Schlüssel jedoch als Klartext **1** kopiert und in das Feld `Authentifizierungsschlüssel (TOTP)` **(1)** kopiert werden.~~



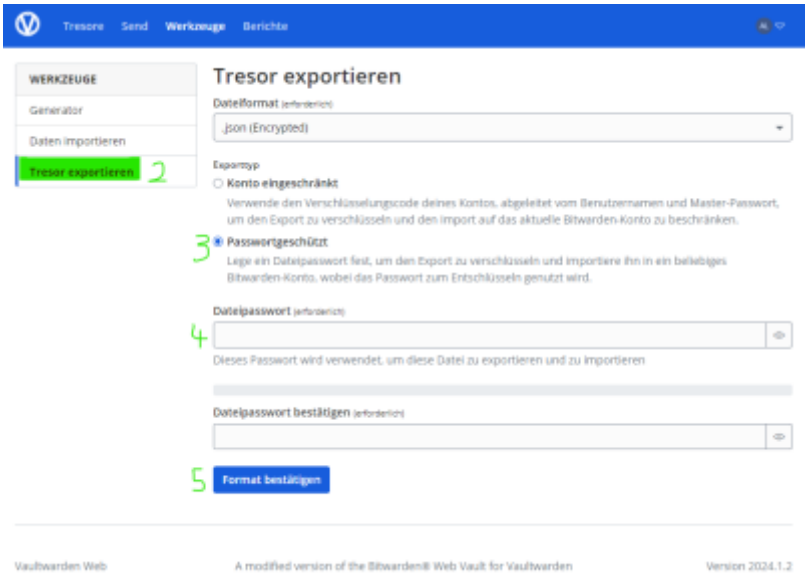
In den Bitwarden-Browser-Plugins kann der QR-Code auch direkt von der Webseite übernommen werden **(2)**.

Backup erstellen

Unter https://bitwarden.gymnasium-ditzingen.de in Vaultwarden anmelden.



Den Reiter „Werkzeuge“ **1** wählen.



Dort auf „Tresor exportieren“ gehen und sinnvolle Einstellungen für den Export wählen. Empfehlenswert ist der mit einem Passwort verschlüsselte Export **3**. Das Passwort **4** kann, muss aber nicht das MAster-Passwort sein. Mit Klick auf **5** „Format bestätigen“ wird eine verschlüsselte Textdatei heruntergeladen. Diese kann auf allen bitwarden-kompatiblen Servern wiederhergestellt werden, also auch nach Ende der Schulzugehörigkeit weitergenutzt werden.

Backup verschlüsseln!

Man kann zwar aus Vaultwarden die Passwörter unverschlüsselt exportieren, dies ist allerdings gefährlich. Wer auch immer Zugriff auf die unverschlüsselte Datei erhält, hat alle Passwörter!