Bitwarden Passwortmanager ?

Bitwarden ist ein Passwortmanager zur sicheren Verwaltung der ZKB-Accounts über verschiedene Geräte/Teams hinweg. Er kann zusätzlich zur Verwaltung privater Passwörter genutzt werden, so lange diese Infrastruktur bereitsteht und ihr für die ZKB/das HdS arbeitet.

Passwörter werden verschlüsselt auf dem zentralen Server (dem zusammenkunft.berlin-Cloudron) gespeichert. Nur mittels Master-Passwort kann auf diese zugegriffen werden.

Ersteinrichtung von Bitwarden

Um einen Account zu erstellen, braucht ihr einen Einladungslink. Diesen bekommt ihr von einem Bitwarden-Admin (aktuell Clemens) auf Anfrage in euer persönliches Postfach. Der Link ist **sieben Tage** gültig.

Das nun zu vergebende Passwort ist euer **Master-Passwort** und das einzige, was ihr euch ab jetzt merken müsst. Es sollte also sicher sein: nirgends sonst verwendet, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, nicht euer Geburtsdatum ... hilfreich ist ein Merksatz, z.B. "Mein Auto steht seit Januar 2017 in der Garage." > `MAs$01/17@dG`

> Sichert euer Master-Passwort: ob in der Apple-Schlüsselverwaltung oder auf einem Zettel im Portemonnaie (aber bitte ohne Hinweis wo es eingegeben werden muss). Hauptsache ihr findet es wieder und es ist nicht für Dritte direkt "verwendbar".

In der Web-App könnt ihr nun eigene Passwörter hinzufügen.

Sobald euer Account vom Bitwarden-Admin bestätigt wurde, könnt ihr die füer euch freigegebenen Passwörter sehen. Es gibt verschiedene Sammlungen, die unterschiedlichen **Nutzendengruppen** entsprechen: Praktikum, Kommunikation, Pioniernutzung, Vorstand. Wenn ihr nicht alle Passwörter sehen könnt, die ihr braucht, müsst ihr eine:n Admin bitten, euch weiteren Gruppen zuzuordnen.

Passwort zurücksetzen / Notfallzugriff einrichten

Account löschen und neu einrichten

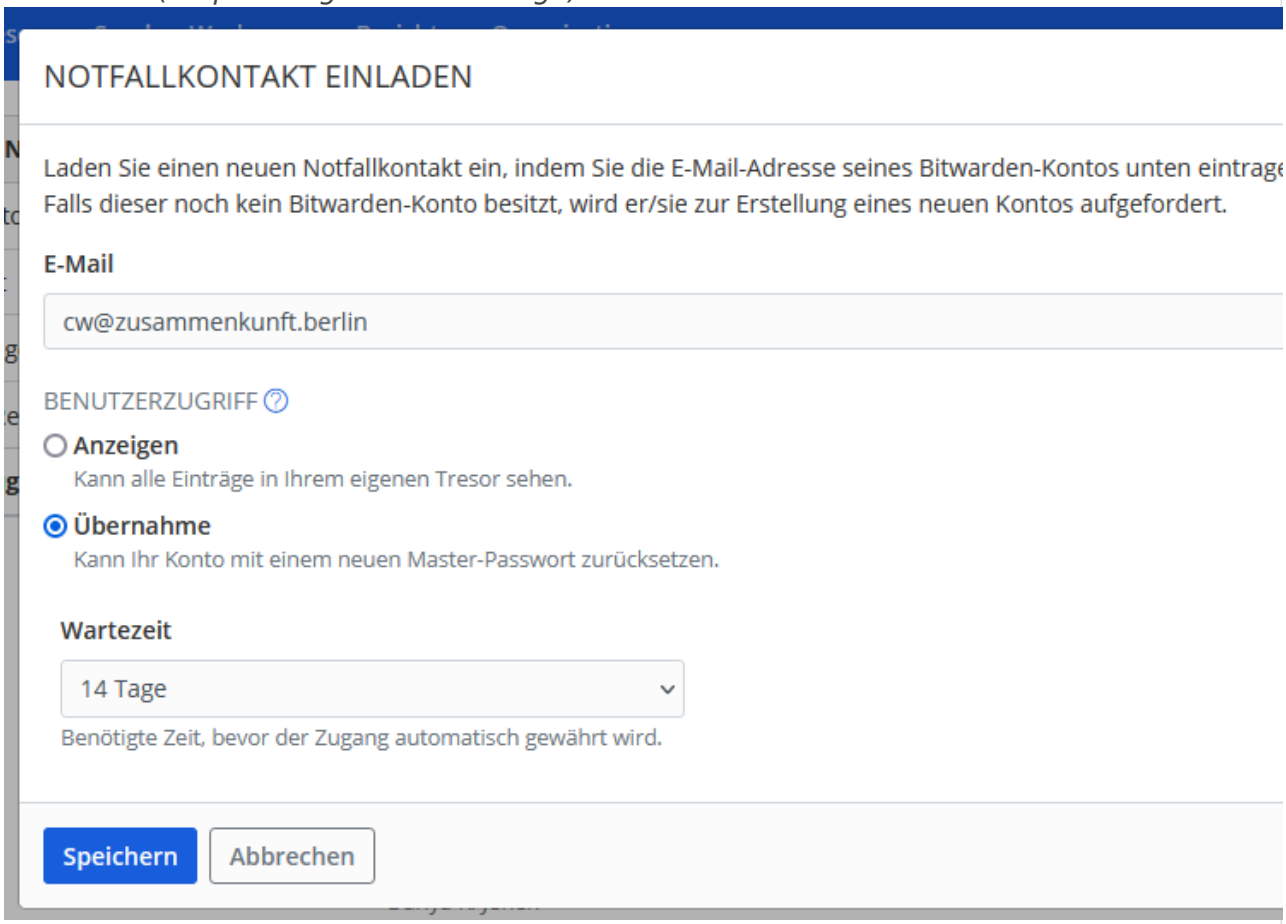
Es gibt **keine Möglichkeit, euer Passwort per E-Mail zurücksetzen zu lassen** wie bei den meisten Web-Apps. Die einzige Möglichkeit ist, Vorzusorgen, indem ein Notfallkontakt (siehe unten) eingerichtet wird.

Der Account kann nur gelöscht und neu eingerichtet werden. Die persönlichen Passwörter gehen dadurch verloren. So geht es:

1. Account löschen: https://keys.zusammenkunft.berlin/#/recover-delete
2. Admin um erneute Einladung zur Organisation bitten
3. Ersteinrichtung erneut durchführen
4. Notfallzugriff einrichten

Notfallzugriff/Notfallkontakt einrichten

1. 1. Auf https://keys.zusammenkunft.berlin/ einloggen
   2. ◫ (Account-Kreis oben rechts) → Kontoeinstellungen
   3. in der Liste links: `Notfallzugriff` → `+ Notfallkontakt hinzufügen`
   4. E-Mail-Adresse eines ZKB-Kontakts mit Bitwarden-Account eintragen (z.B. cw@zusammenkunft.berlin),
      Benutzerzugriff: Übernahme
      Wartezeit: *(Empfehlung: 7 oder 14 Tage)*



Euer Notfallkontakt bekommt nun eine E-Mail mit einem Bestätigungenslink. Sobald der Link geklickt ist, wechselt der Status auf **Akzeptiert**.

5. Erst, wenn ihr im selben Menü euren Kontakt noch mal bestätigt (…-Menü → Bestätigen), ist der Notfallkontakt fertig eingerichtet.

> Eure Vertrauensperson kann nun im Notfallzugriff-Menü den Zugriff auf euren Bitwarden-Account anfordern. Ihr bekommt dann eine E-Mail und habt dann 7 oder 14 Tage Zeit (je nach Einstellung), die Anforderung abzulehnen oder direkt anzunehmen.

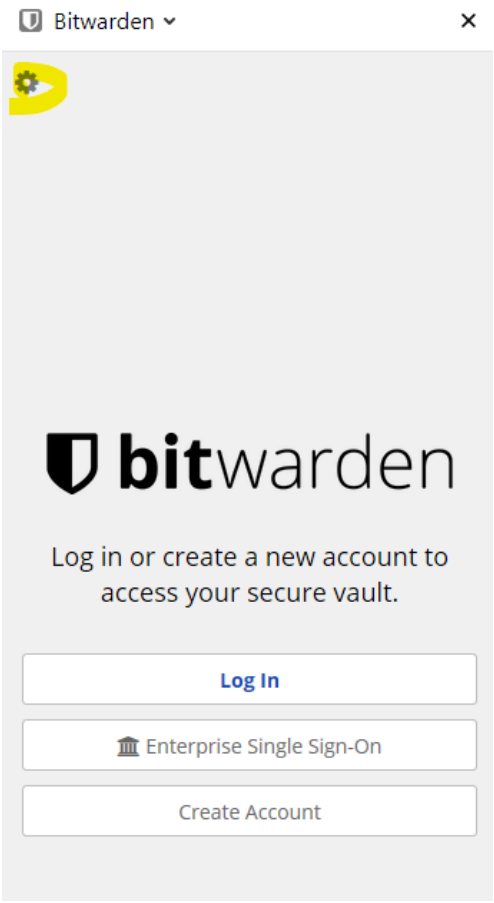
> Wenn nichts unternommen wird, kann der Account nach Ablauf der Wartezeit übernommen werden.

Einrichtung von Apps

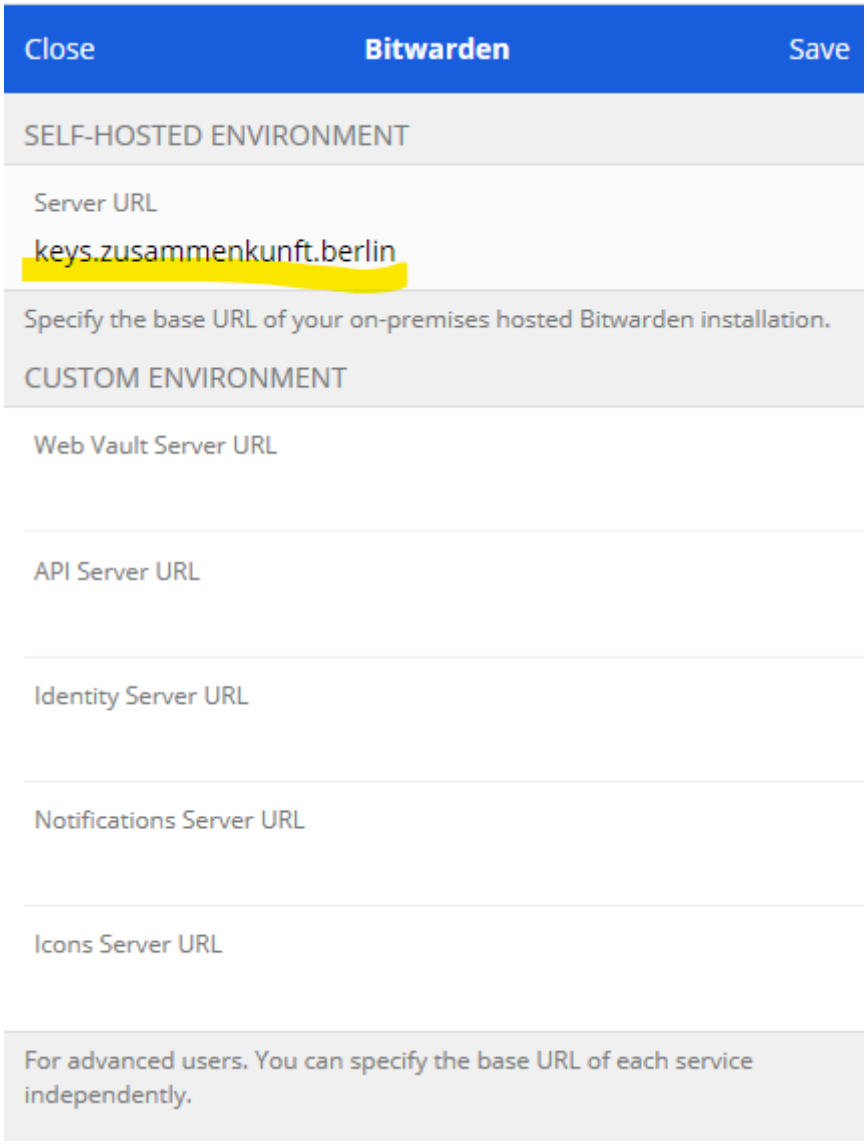
Es gibt Apps für Mobilgeräte und Desktop-Computer und Browser-Erweiterungen – deren Installation ist empfehlenswert, da dadurch die Passwörter direkt ausgefüllt werden können.

⚠ Um sich nach der Installation das erste Mal mit dem Server zu verbinden, muss zunächst der **ZKB-Server manuell eingegeben** werden:

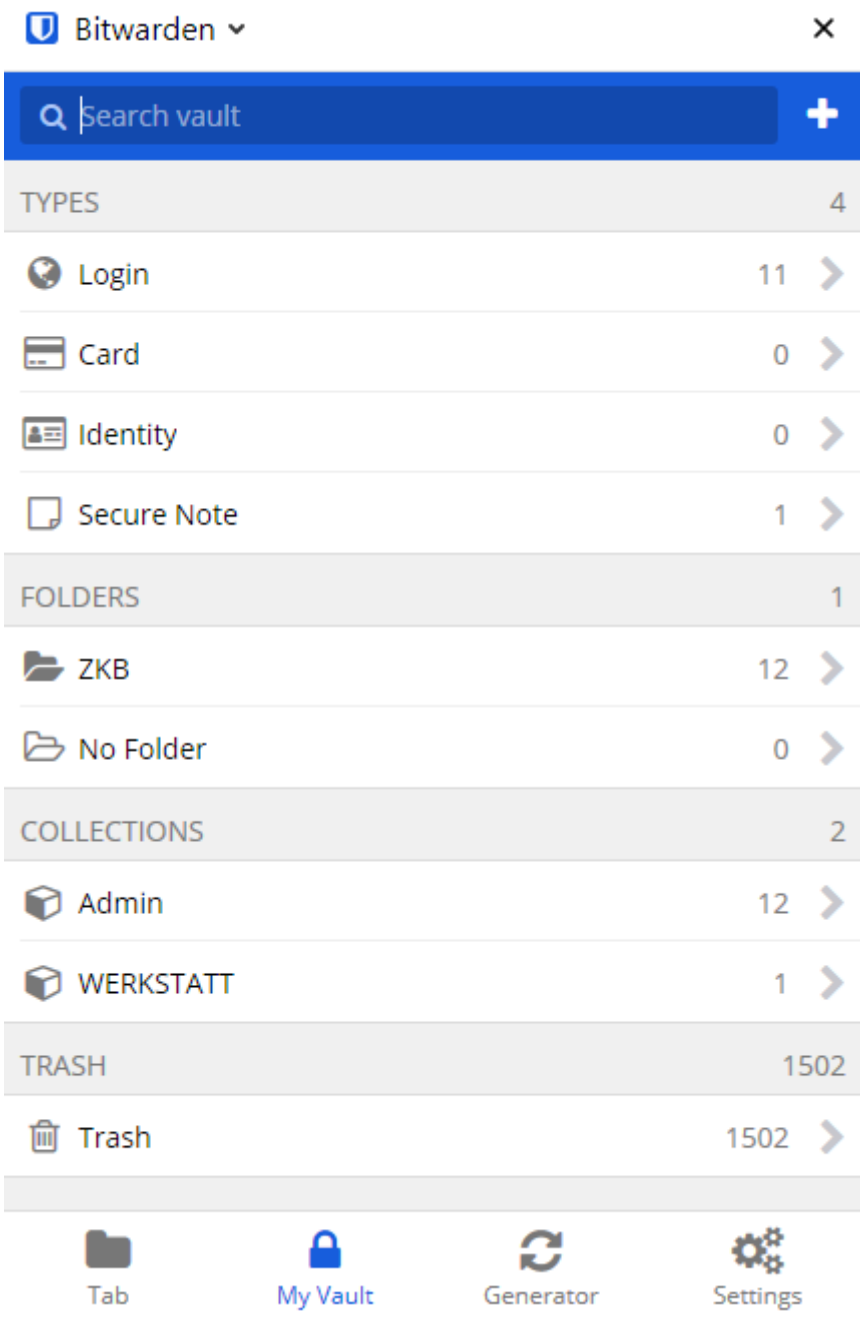
1. auf das **Einstellungsrädchen** klicken (hier Beispiel Firefox-Erweiterung, in den Apps funktioniert es genau so):



2. `keys.zusammenkunft.berlin` bei "Server URL" eintragen



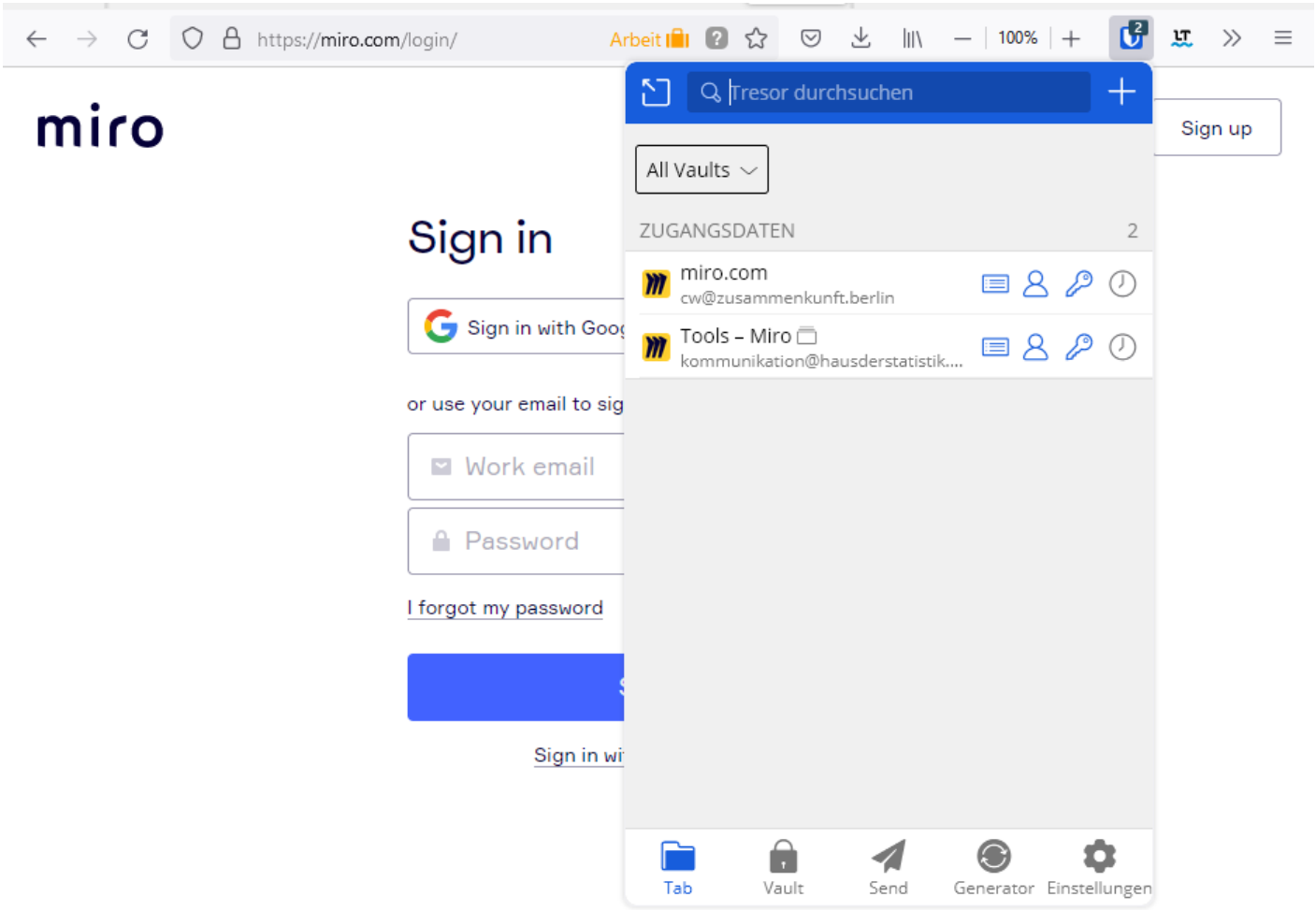
3. "Log In" → mit E-Mail-Adresse und eurem zuvor auf keys.zusammenkunft.berlin vergebenen **Master-Passwort** anmelden. Nun könnt ihr eure eigenen Passwörter und die für euch freigegebenen sehen:



Installation und Benutzung der Browser-Erweiterung

Für alle gängigen Browser gibt es hier die entsprechenden Plugins (direkt: Firefox / Safari / Chrome).

Nach der Installation und Einrichtung (wie oben), kann über die Bitwarden-Schaltfläche Benutzername/Passwort direkt mit einem Klick auf den richtigen Eintrag ausgefüllt werden. In diesem Beispiel wird sowohl ein persönlicher Account als auch der ZKB-Account angeboten.



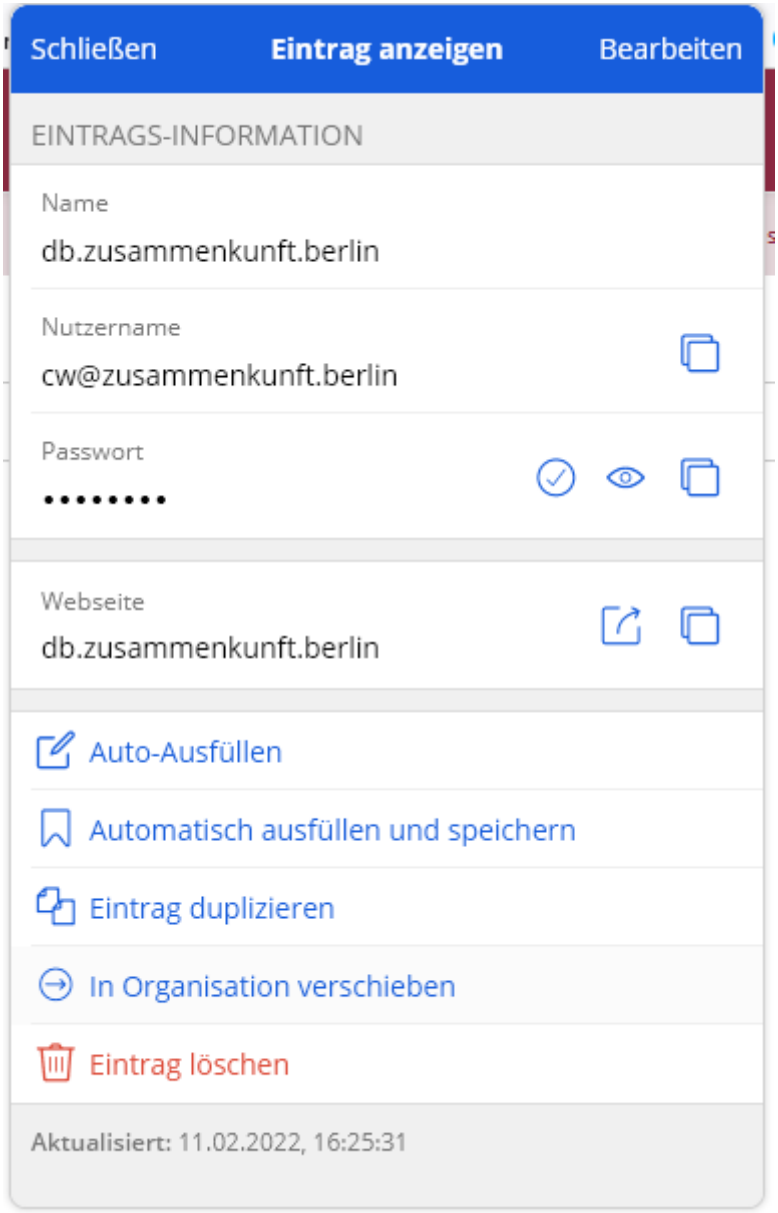
Ein Klick auf den Eintrag füllt dann das Passwort aus. Oder mit Klick auf □□ = Benutzernamen kopieren; Klick auf □□= Passwort kopieren.

Neuen Eintrag hinzufügen

manuell: auf □ klicken und `Benutzername`, `Passwort` und `URL` eintragen.

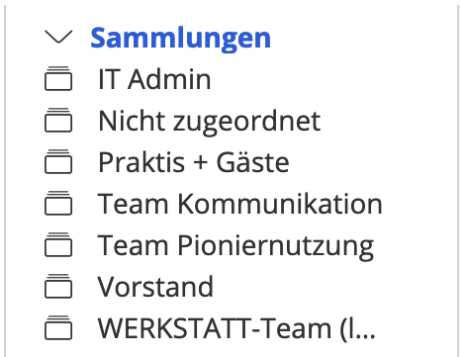
automatisch: Auf neue Login-Seite gehen, Benutzernamen und Passwort eintragen und einloggen. Das Bitwarden-Browser-Addon fragt anschließend, ob das neue Passwort gespeichert werden soll. → Speichern klicken.

> WICHTIG: Anschließend Passwort-Eintrag im Manager suchen und auf **In Organisation verschieben** klicken und die entsprechende Collection auswählen. Sonst bleibt das Passwort nur für euch persönlich gespeichert.



Administratives

Es werden Collections für die verschiedenen Teams/Nutzer:innengruppen verwendet. Diese sind aktuell (2024-04-10):



Revision #8
Created 2020-10-19 11:12:05 UTC by clemens.weise
Updated 2024-04-10 13:12:43 UTC by clemens.weise