Comp-Sys Informatik AG
Glutz-Blotzheim-Strasse 1
4500 Solothurn
032 653 70 77

# Tresor11
# Benutzerhandbuch

COMP-SYS
0 Probleme. 1 Lösung.

Inhalt

## Was ist Tresor11?

Tresor11 ist eine in unserem Rechenzentrum gehostete Applikation zur sicheren Verwaltung und Verwahrung von Passwörtern. Die Applikation basiert auf dem Open-Source-Derivat des berühmten Passwort-Managers «Bitwarden» namens «Vaultwarden». Entsprechend finden sich weitere Informationen in den Dokumentationen dieser beiden Applikationen (siehe weiterführende Links am Ende dieses Dokuments).

## Wichtige Informationen

**Comp-Sys hat keinen Zugriff auf Ihren Tresor, noch können wir vergessene oder verlorene Masterpasswörter zurücksetzen.** Sie sind selbst für die Verwaltung Ihres Tresors zuständig. Lediglich Benutzerlöschungen können bei uns angefragt werden. Stellen Sie demnach sicher, dass Sie Ihr Masterpasswort nicht vergessen/verlieren können. Denken Sie auch daran, dass die Kenntnis Ihres Masterpassworts Zugriff auf Ihren kompletten Tresor ermöglicht (Ausnahme: Multi-Faktor-Authentifizierung). Wählen Sie also ein starkes, kryptisches Passwort.

Es wird empfohlen, in regelmässigen Abständen eine Sicherung Ihres Tresors zu exportieren und sicher abzulegen.

## Zugriff und Einrichtung

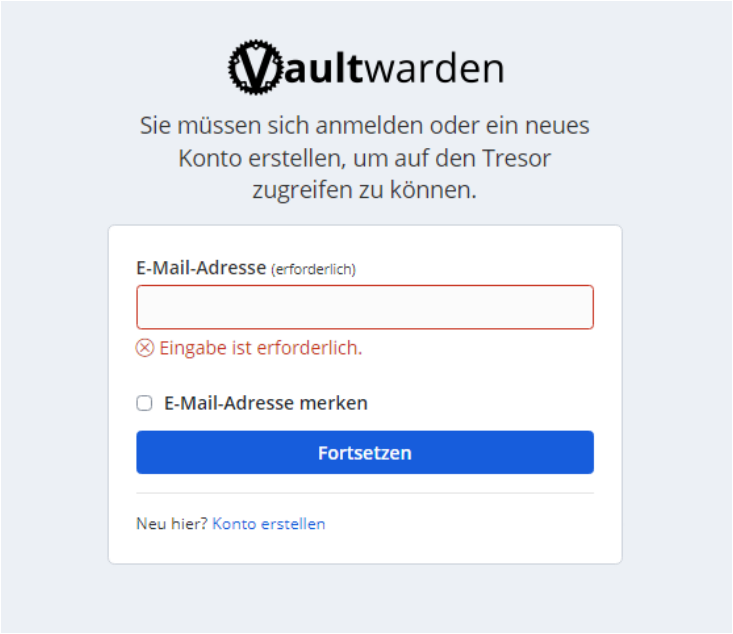
Tresor11 muss weder heruntergeladen noch installiert werden. Der Service befindet sich in unserem Rechenzentrum.

### Zugriff über Browser direkt

Sie können ihren individuellen Tresor11 direkt über einen beliebigen Browser erreichen, indem Sie den von uns erhaltenen Link zu Ihrem Tresor in die Adressleiste eingeben. Diese Zugriffsart wird im Folgenden «Web-Tresor» genannt.

Beachten sie, dass Sie den Link immer über «https://» und nicht über «http://» ansteuern. Die Seite ist zwar über http einsehbar, jedoch kann man sich so nicht anmelden, da der Tresor nur verschlüsselte Verbindungen zulässt.

Nach dem Aufrufen des Links sollten Sie folgende Seite in Ihrem Browser sehen können:




Sie können sich nun mit Ihrer E-Mail-Adresse und Ihrem Masterpasswort einloggen.

## Zugriff über Browser-Plugin

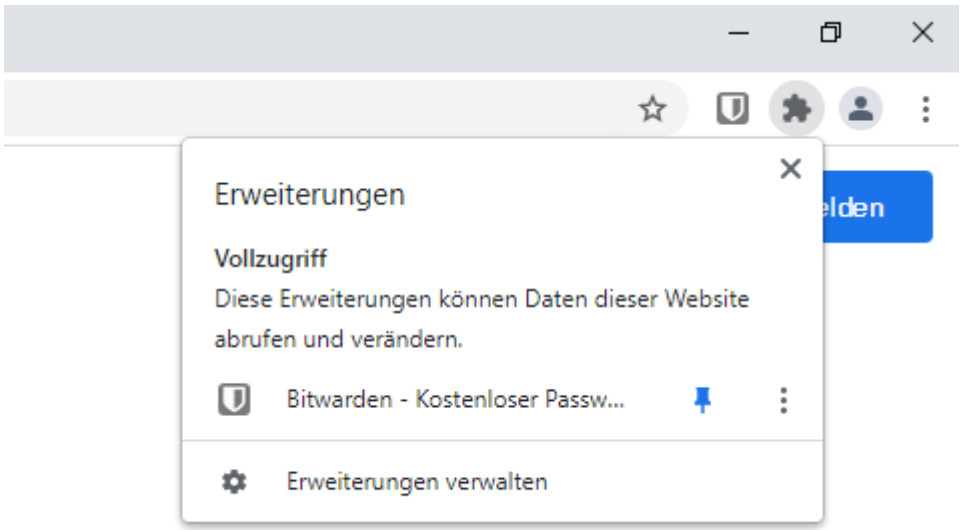
Der Tresor11 kann auch über das Bitwarden Browser-Plugin erreicht werden. Dieses ist für die meisten gängigen Browser verfügbar. Je nachdem, welchen Browser man verwendet, muss das Plugin unterschiedlich beschafft werden:

- Für Microsoft Edge lässt sich das Plugin aus dem Microsoft Store herunterladen:
  Bitwarden - Kostenloser Passwortmanager – Microsoft Edge Addons

- Für andere Chromium-basierte Webbrowser (Opera, Chrome, Brave usw.) kann die Bitwarden Browser Extension aus dem Google Chrome Web Store verwendet werden:
  Bitwarden - Free Password Manager - Chrome Web Store (google.com)

- Für Mozilla Firefox lässt sich das Plugin von der offiziellen Firefox Browser Add-Ons Seite laden:
  Bitwarden - Free Password Manager – Get this Extension for Firefox (en-US) (mozilla.org)

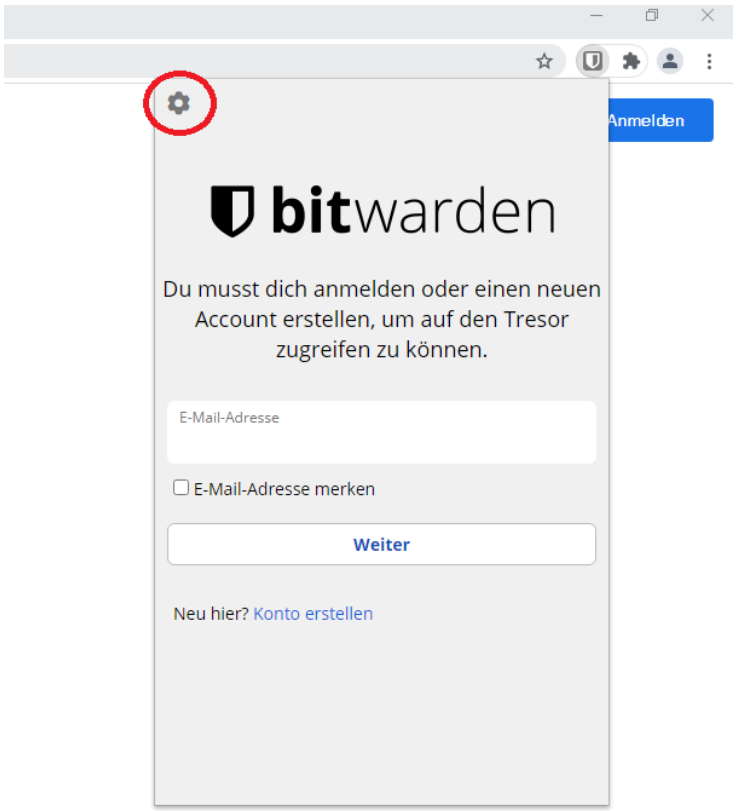
Nachdem das Plugin installiert wurde, kann es über die Browsererweiterungen aufgerufen werden. Dort kann es ebenfalls angepinnt werden, so dass sich das entsprechende Symbol gleich dauerhaft oberhalb der Lesezeichenleiste Ihres Browsers befindet.
Nachfolgend sehen Sie einen Screenshot der angepinnten Erweiterung Bitwarden in Google Chrome. Bitte beachten Sie, dass die Oberfläche je nach Browser variieren kann.

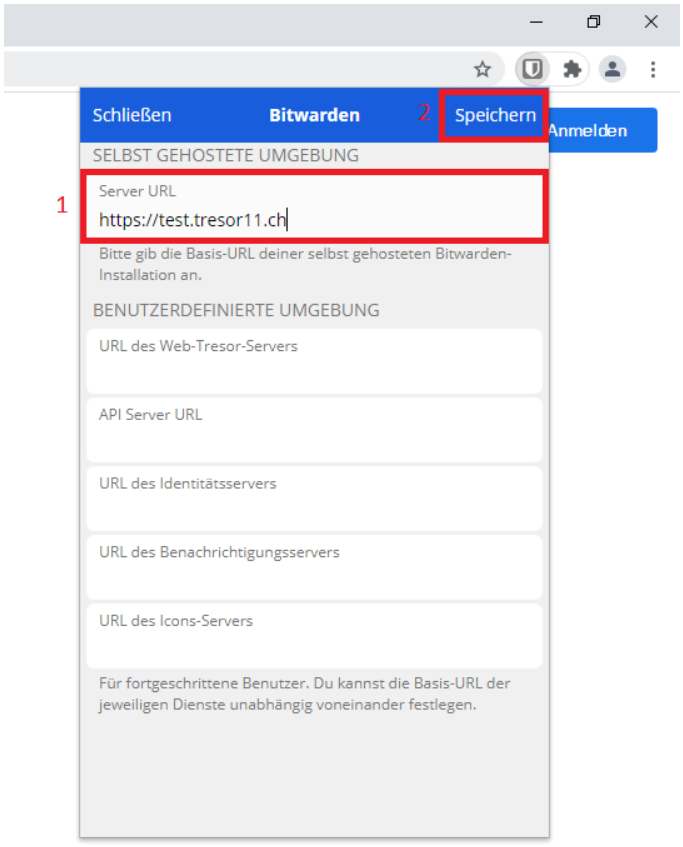



Wenn das Symbol der Erweiterung nun angeklickt wird, öffnet sich die Eingabemaske Ihres neuen Passwortmanagers. Bei der ersten Verwendung muss dieses Plugin so konfiguriert werden, dass es auf Ihren Tresor11 zugreift. Klicken Sie dazu bitte auf das Zahnrad-Symbol in der oberen linken Ecke des Plugin-Pop-Ups (siehe nächste Abbildungen).

Danach können Sie unter «Server URL» den Link ihrer persönlichen Tresor11-Instanz eintragen («https://» nicht vergessen!). Den Rest der Einstellungen unter «Benutzerdefinierte Umgebung» sollten Sie leer lassen.

Nachdem die Server URL eingetragen wurde, oben rechts mit «Speichern» bestätigen. Nun werden Sie zurück zur Anmeldemaske geleitet, auf der Sie sich nun mit Ihrem Benutzeraccount und Masterpasswort anmelden können. Sehen Sie dazu die nachfolgenden Screenshots.


Anmelden
bitwarden
Du musst dich anmelden oder einen neuen Account erstellen, um auf den Tresor zugreifen zu können.
E-Mail-Adresse
E-Mail-Adresse merken
Weiter
Neu hier? Konto erstellen

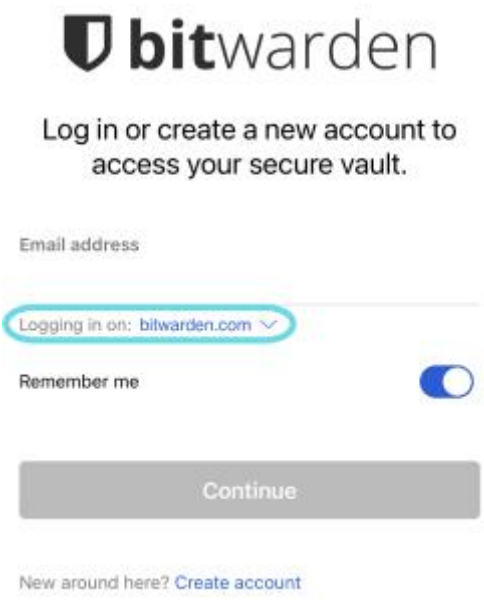

Schließen
Bitwarden
2
Speichern
Anmelden
SELBST GEHOSTETE UMGEBUNG
1
Server URL
https://test.tresor11.ch
Bitte gib die Basis-URL deiner selbst gehosteten Bitwarden-Installation an.
BENUTZERDEFINIERTE UMGEBUNG
URL des Web-Tresor-Servers
API Server URL
URL des Identitätsservers
URL des Benachrichtigungsservers
URL des Icons-Servers
Für fortgeschrittene Benutzer. Du kannst die Basis-URL der jeweiligen Dienste unabhängig voneinander festlegen.

## Zugriff via Bitwarden-App: Tresor11 für Ihr Smartphone

Nebst dem Zugriff über das Web-Login und/oder das Browser-Plugin besteht ebenfalls die Möglichkeit, den Tresor11 auf dem Smartphone zu verwenden.
Da die verwendete Software mit den Bitwarden-Produkten kompatibel ist, wird hierfür die App «Bitwarden Passwordmanager» von «Bitwarden Inc.» verwendet.
Diese lässt sich im entsprechenden App-Store finden und herunterladen (PlayStore für Android, App-Store für iPhone). Achten Sie darauf, dass Sie effektiv die offizielle Bitwarden-App der Bitwarden Inc. und kein Imitat herunterladen. Der Hersteller der App ist im Store ersichtlich.

Nachdem die App heruntergeladen wurde muss – wie beim Browser-Plugin auch – der Server für die Verbindung der App festgelegt werden (wenn nichts eingegeben wird, navigiert die App automatisch zu bitwarden.com).

Dazu klicken Sie auf das Drop-Down-Menu mit «bitwarden.com» und geben im Feld **Server URL** die Adresse Ihres persönlichen Tresors ein (analog zum Browser-Plugin; siehe oben).



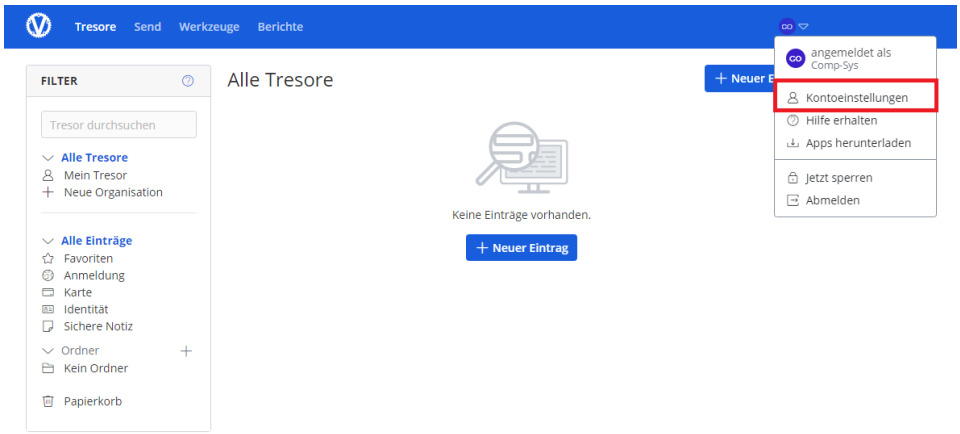

Wie Ihre anderen Apps können Sie den Tresor11 nebst Zugriff mit Passwort auch mit Biometrie (FaceID, Fingerabdruck) entsperren, sofern Sie dies auf Ihrem Smartphone eingerichtet haben.

Navigieren Sie dazu in der App im unteren Reiter auf «Einstellungen», danach auf «Kontosicherheit». Unter «Entsperroptionen» können Sie nun die Ihrem Smartphone zur Verfügung stehenden Optionen ein- oder ausschalten.

## Masterpasswort ändern

Nach dem ersten Zugriff auf Ihren Tresor11 empfehlen wir, das von uns erhaltene Initial-Masterpasswort zu ändern. Dazu müssen Sie sich in Ihren Web-Tresor11 einloggen. Dort finden Sie oben rechts ihr individuelles Benutzersymbol. Dieses können Sie anklicken, um von da aus zu Ihren «Kontoeinstellungen» zu navigieren. Dort können Sie unter dem Reiter «Sicherheit» ein neues Masterpasswort festlegen.

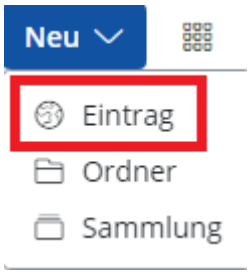
Bitte beachten Sie unbedingt unsere Erläuterungen zu Passwortsicherheit weiter unten in diesem Dokument.




## Einträge hinzufügen

Es ist einfach, Ihrem Tresor11 neue Einträge hinzuzufügen.

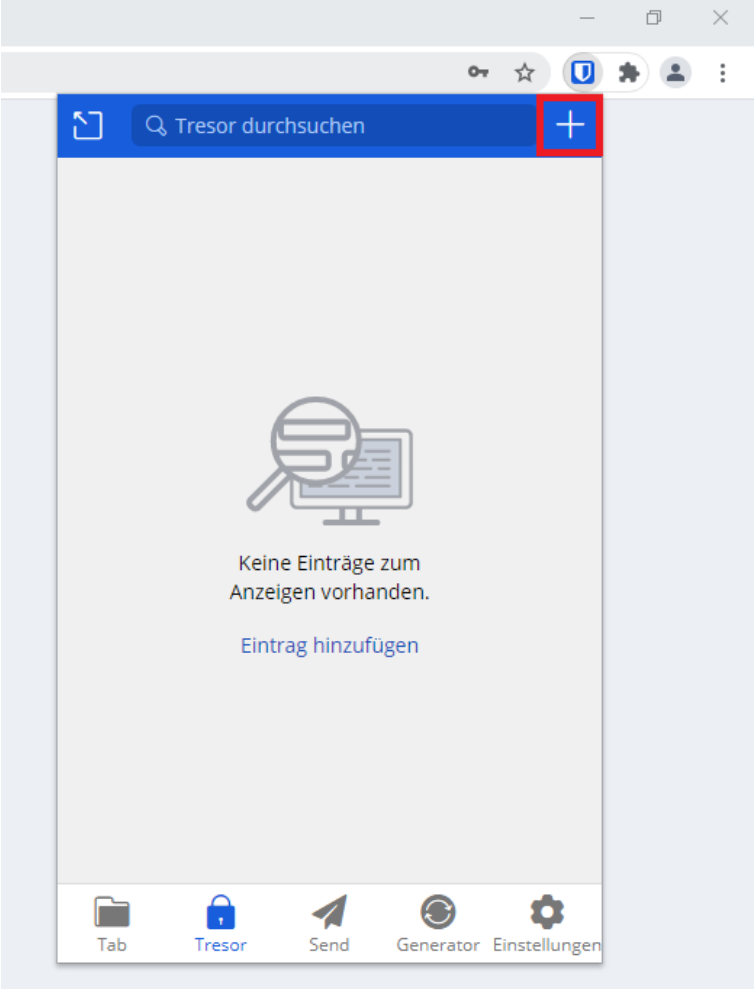
Wenn Sie sich im Web-Tresor befinden (im Reiter «Tresore»), klicken Sie auf Neu und danach auf «Eintrag».




Im folgenden Fenster können Sie nun neue Einträge Ihrem Tresor11 hinzufügen. Nebst Anmeldedaten lassen sich auch Bank-/Kreditkarteninformationen, Identitäten und sichere Notizen verwahren.

Nachdem Sie alle Informationen eingegeben haben, müssen Sie nur noch am Ende der Seite auf Speichern klicken. Sie haben gerade erfolgreich Ihrem Tresor11 einen Eintrag hinzugefügt.

Um einen Eintrag via Browser-Plugin hinzuzufügen, klicken Sie auf das «+»-Symbol in ausgeklapptem Plugin, wie auf folgendem Screenshot ersichtlich.

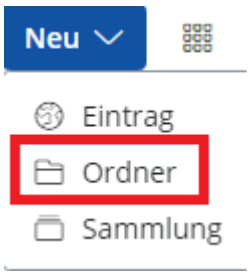



Nachfolgend können Sie analog zum Web-Tresor die entsprechenden Angaben eintragen und im Anschluss mit **Speichern** bestätigen.

## Ordner hinzufügen und verwalten

Tresor11 bietet die Möglichkeit, seine Einträge in Ordnern zu organisieren.

Um einen neuen Ordner im Web-Tresor zu erstellen, klicken Sie auf denselben Button wie beim Anlegen eines neuen Eintrags, wählen aber dann «Ordner» statt «Eintrag».



Geben Sie dem Ordner einen Namen und drücken Sie auf «Speichern». Sie haben erfolgreich einen neuen Ordner erstellt.

Um einen neuen Ordner via Browser-Plugin zu erstellen, müssen Sie zuerst auf den Reiter «Einstellungen», dann auf «Tresor», danach auf «Ordner» und schlussendlich wieder aufs «+»-Symbol klicken. Wie vorhin dem Ordner einen Namen geben und mit «Speichern» bestätigen.

Wenn Sie sich in Ihrem privaten Nutzer-Tresor befinden, wird der Ordner in diesem angelegt (sowohl per Web-Login als auch per Browser-Plugin).

Organisationsordner lassen sich nur via Web-Login erstellen. Navigieren Sie dazu zuerst in die Admin-Konsole der Organisation und verfahren Sie danach gleich wie beim Anlegen von User-Ordnern.

## Sammlungen hinzufügen und verwalten

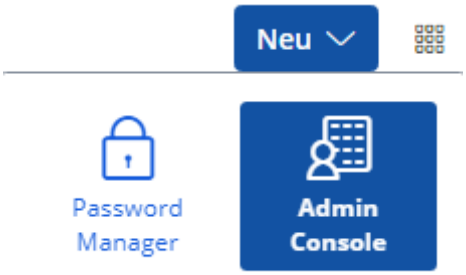
Sammlungen können gleich verwaltet werden wie Ordner. Sehen Sie dazu das vorangegangene Kapitel. Sammlungen ermöglichen es, mehrere Ordner zu logischen Strukturen zu gruppieren. Sammlungen können ebenfalls geteilt/freigegeben werden.

# Benutzer- und Organisationsverwaltung

## Benutzer verwalten

### Neue Benutzer hinzufügen

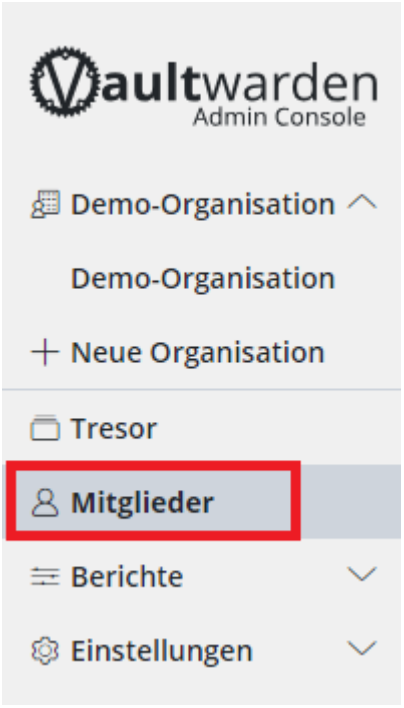
Neue Benutzer können nur über eine bestehende Organisation vom Organisationsadministrator eingeladen werden.
Melden Sie sich dazu mit dem Organisationsadministrator im Web-Tresor an. Dort navigieren Sie auf das Symbol mit den 3x3 Punkten neben Ihrem Profilicon und wählen «Admin Console».




In der Admin-Konsole werden alle Organisationseinstellungen vorgenommen, u.a. auch das Einladen/Entfernen von (neuen) Mitgliedern, die Verwaltung und Delegation von Ordnern/Sammlungen, Sicherungen und vieles mehr.

Sobald Sie auf die Admin-Konsole gewechselt haben, klicken Sie im linken Reiter auf «Mitglieder». Danach wird oben rechts neben dem Benutzericon ein «+ Mitglied einladen»-Button ersichtlich sein.

**1:**




**2:**


Geben Sie im darauffolgenden Fenster die E-Mail-Adresse des einzuladenden Benutzers ein, wählen Sie die Mitgliederrolle aus und klicken Sie auf «Speichern».

Die eingeladene Person erhält daraufhin eine Mail mit einem Registrationslink, mit welchem sie sich ein Konto im Tresor11 erstellen kann. Der Link kann auch genutzt werden, um einer Organisation mit einem bereits bestehenden Tresor11-Konto beizutreten.

Nach der Registration/Anmeldung muss der Organisationsadministrator das frisch registrierte/beigetretene Mitglied in der Organisations-Mitgliederverwaltung (Screenshot oben, Punkt 2) noch bestätigen. Danach ist das neue Konto einsatzbereit.

## Benutzer entfernen

In der Organisations-Mitgliederverwaltung können zudem Benutzer auch wieder aus der Organisation entfernt werden. Dazu müssen Sie nur auf die 3 Punkte neben dem Benutzer klicken und dann «X Entfernen» auswählen.

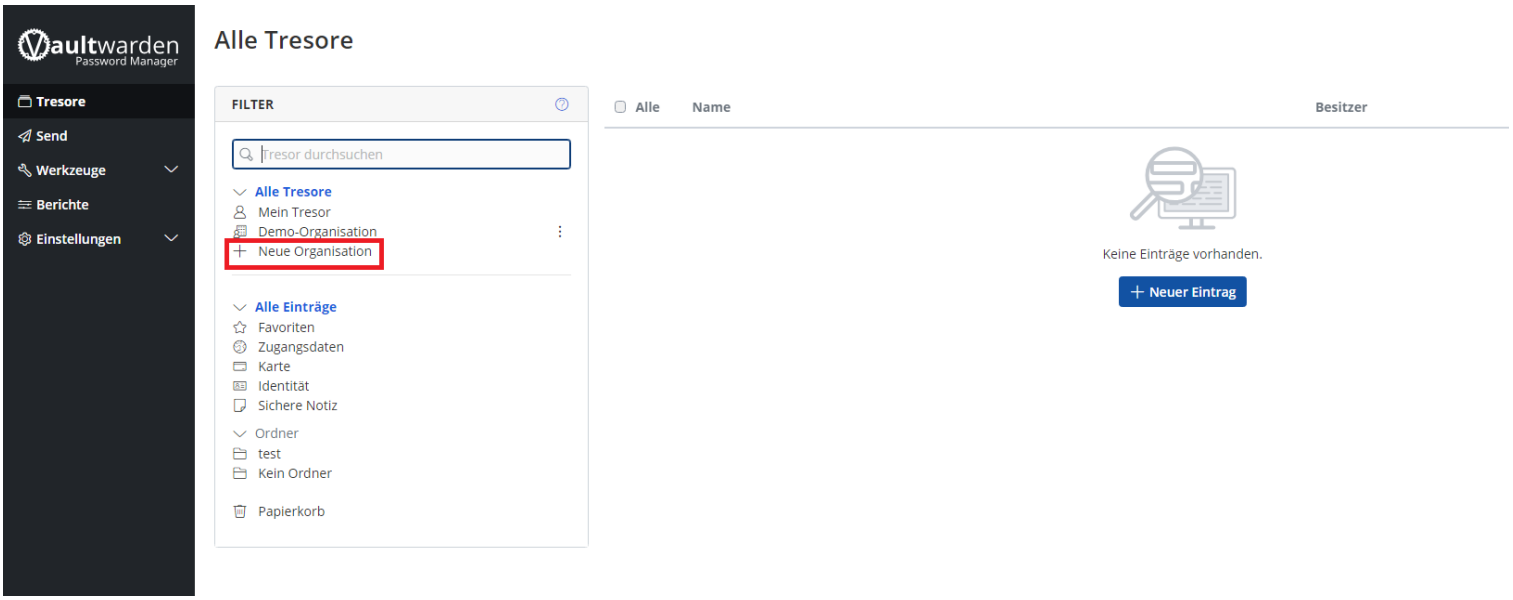
Benutzeraccounts zu löschen ist nicht möglich. Wenn Sie einen Benutzer löschen möchten, wenden Sie sich bitte an unseren Support.

# Organisationen verwalten

## Neue Organisation erstellen

Das Erstellen neuer Organisationen ist lediglich dem Admin-Benutzer vorbehalten (der erste Benutzer Ihres Tresors, der von uns initial erstellt und Ihnen übermittelt wird). Diese Einstellung stellt eine Sicherheitsmassnahme dar, da Admins von Organisationen neue Mitglieder zum Tresor11 einladen können.

Wenn Sie eine neue Organisation erstellen wollen, loggen Sie sich mit einem berechtigen Benutzer in Ihren Webtresor ein und klicken im Reiter «Tresore» (quasi Ihre «Startseite», nachdem Sie sich eingeloggt haben) auf «+ Neue Organisation». Im folgenden Fenster können Sie den gewünschten Organisationsnamen und die E-Mail des Organisationsadmins angeben und im Anschluss die Organisation erstellen.



## Organisation wechseln

Wenn Sie in Ihrer Organisation mehr als eine Organisation haben, können Sie in der Admin-Konsole zwischen einzelnen Organisationen hin- und her wechseln:


# Sicherheit

## Passwortsicherheit

### Was macht ein sicheres Passwort aus?

Wird ein Angriff gegen ein Konto versucht, kann dieser sehr simpel aufgebaut sein. Es werden einfach alle möglichen

Kombinationen versucht. Folglich müsste für ein Passwort mit den zehn Zahlen (0-9) und einer Länge von 3 Zeichen nur 1'000 Versuche gemacht werden. (10^3, Alle Zahlen von 000-999)

Anhand dieses kurzen Beispiels merken wir bereits, dass ein optimales Passwort möglichst viele verschiedene und eine möglichst grosse Anzahl an Zeichen verwendet.

Aber was genau macht ein gutes Passwort aus? Hier einige Punkte:
- Anzahl an Zeichen (möglichst grosse Anzahl)
- Verschiedene Zeichen (z.B. Sonderzeichen, Klein-, Grossbuchstaben und Zahlen verwenden)
- Keine Wörter oder Namen benutzen.
- Keine logischen Muster oder bekannte Systeme (z.B. qwertz, abcdefg… , 1234567…, a1b2c3…)
- Nicht mehrfach vorhanden.

(Verwenden Sie für jedes Log-In ein individuelles, einzigartiges Passwort.)

Vermutlich denken Sie sich nun, dass es unmöglich ist all diese Punkte zu beachten und sich solche Passwörter dennoch zu merken. Dies ist auch nicht schlimm.

Mit Hilfe des Tresor11, benötigen Sie nur noch ein einziges Passwort. Die anderen können Sie sich verschlüsselt in ihrem Tresor abspeichern.

### Masterpasswort

Nebst der Tatsache, dass das Masterpasswort möglichst sicher aufgebaut sein sollte (siehe Beschreibung zu Passwortsicherheit oben) ist es wichtig zu beachten, dass das Masterpasswort nicht im Passwortmanager des Browsers (und auch sonst nirgends) abgespeichert werden sollte.

Es sollten keine Fotos des aufgeschriebenen Passwortes gemacht werden; ebenso sollte das Passwort nicht in einer Textdatei auf einem Computer abgelegt sein. Im Idealfall hat das Masterpasswort keinen Berührungspunkt zum Internet und befindet sich lediglich in Ihrem Gedächtnis oder physisch aufgeschrieben und sicher verwahrt.

Wichtig ist auch, dass Sie ein Masterpasswort wählen, welches Sie bisher nirgends in Verwendung haben. Passwortwiederholungen sind zu vermeiden.

Der Tresor11 verlangt mindestens 12 Zeichen für Passwörter.

### Passwortgenerator

Der Tresor11 bietet einen Passwortgenerator zur Erzeugung von sicheren, kryptischen und randomisierten Passwörtern an. Dieser kann sowohl über den Webtresor im Register «Werkzeuge», dann «Generator» als auch über das Browser-Plugin unter dem Menüpunkt «Generator» aufgerufen werden.

Dort kann entsprechend konfiguriert werden, wie lange die generierten Passwörter sein und welche Zeichen sie enthalten sollen. Empfohlen werden Passwörter mit allen Zeichentypen (Klein- und Grossbuchstaben, Zahlen und Sonderzeichen) und einer Länge von ab 20 Zeichen.

## Notfallzugriff

Der Tresor11 bietet die Möglichkeit eines Notfallzugriffes an. Somit können Sie eine E-Mail-Adresse/eine Person berechtigen, im Notfall (vergessenes/verlorenes Masterpasswort) Zugriff auf Ihren Tresor anzufordern. Wenn Sie diese Funktion nutzen möchten, gehen Sie wie folgt vor:

Melden Sie sich bei Ihrem Webtresor an.

Navigieren Sie über das Profilicon oben rechts zu Ihren «Kontoeinstellungen» und dann im linken Register auf «Notfallzugriff».

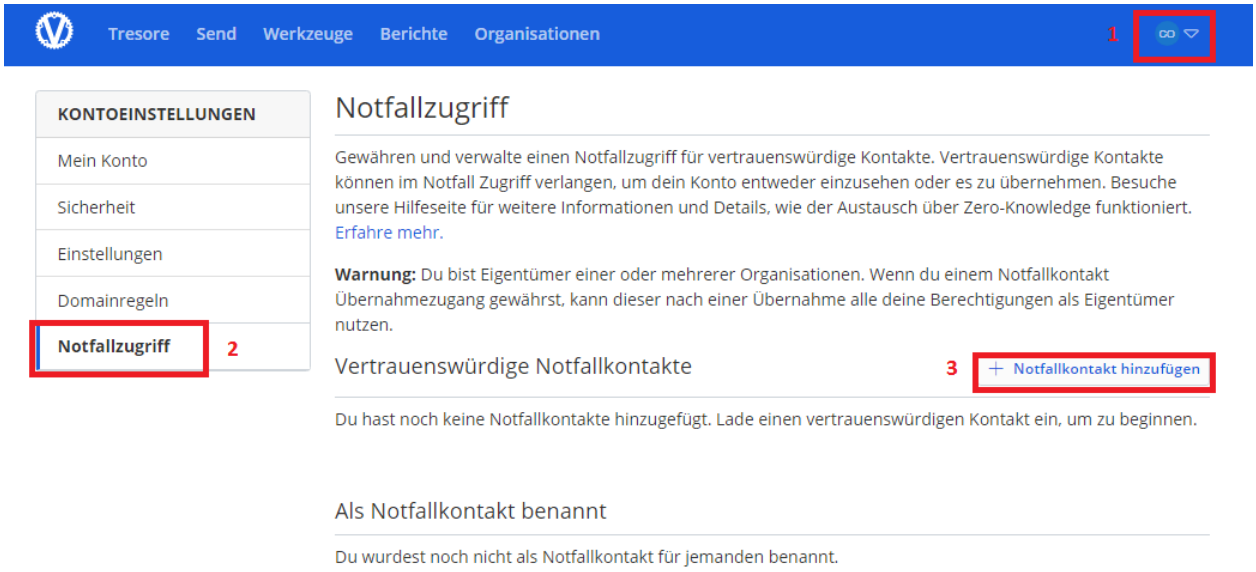
Im Folgenden klicken Sie auf «+ Notfallkontakt hinzufügen». Sie können im Anschluss den Typ des Notfallzugriffs wählen:
Entweder erhält der Notfallkontakt im Notfall Zugriff auf die in Ihrem persönlichen Tresor gespeicherten

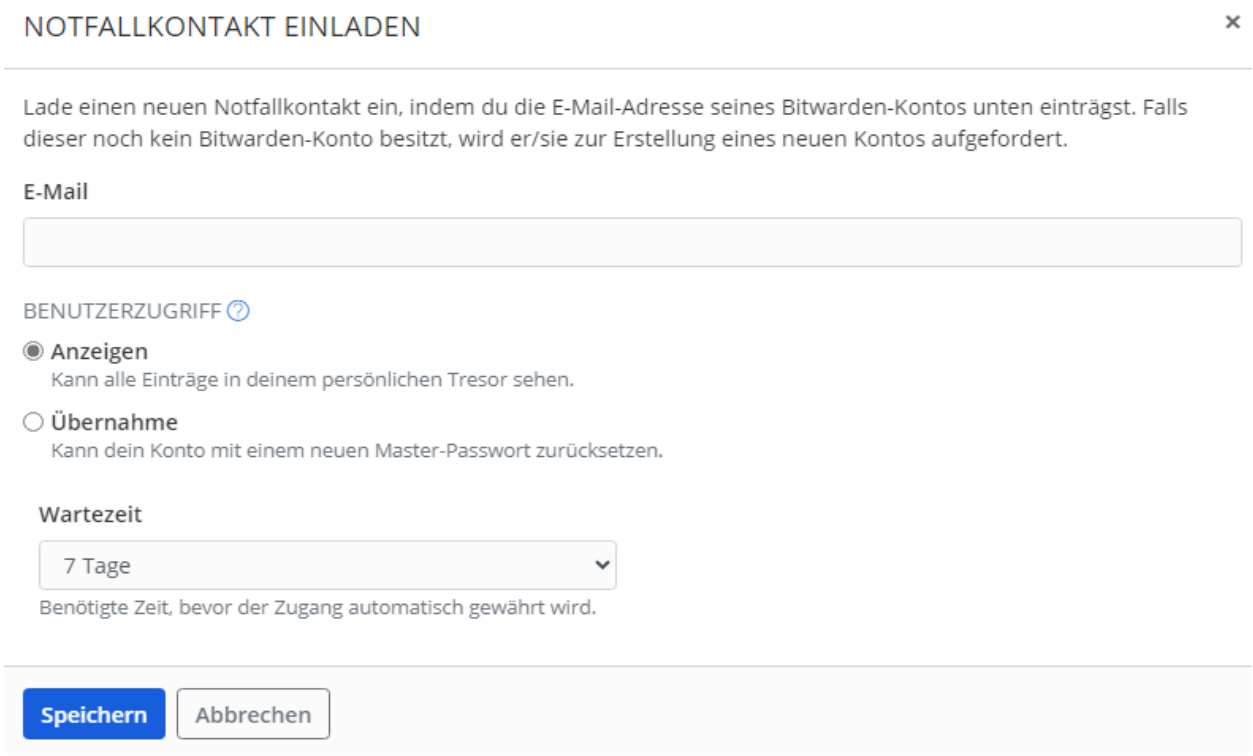
Passwörter (Typ «Anzeigen») oder der Notfallkontakt erhält die Möglichkeit, das Masterpasswort ihres Kontos im Notfall zurückzusetzen. Im Anschluss können Sie noch die «Wartezeit» auswählen. So lange dauert es, im Falle, dass Sie einen Notfall bestätigen, bis der Notfallzugriff ausgelöst wird. Während dieser Zeitspanne können Sie den Notfallzugriff noch abbrechen/widerrufen.

Wichtig: Es kann nur ein Notfallkontakt angegeben werden, der ebenfalls über ein Tresor11-Konto in Ihrem Tresor verfügt.

Sobald die Wartezeit verstrichen ist oder wenn Sie den Notfallzugriff vorzeitig genehmigen, erhält Ihr Notfallkontakt eine Benachrichtigung. Diese enthält Anweisungen, wie er auf den Notfallzugriff zugreifen kann.

Ihr Notfallkontakt kann nun auf den Notfallzugriff zugreifen, um Ihre gespeicherten Passwörter zu erhalten. Dies sollte nur in Notfällen geschehen, wenn Sie keinen Zugriff mehr auf Ihr Tresor11-Konto haben.






## Tresor-Export

Der Tresor11 bietet die Möglichkeit, seinen gesamten Inhalt in eine Datei zu exportieren. Dies kann als Sicherung oder zu Migrationszwecken zu einem anderen Passwortmanager verwendet werden. Dabei können sowohl Benutzertresore als auch Organisationstresore exportiert werden.
Ausserdem können unterschiedliche Typen von Exportdateien erstellt werden (Klartext, verschlüsselt und accountgebunden, verschlüsselt und mit einem Passwort abgesichert).

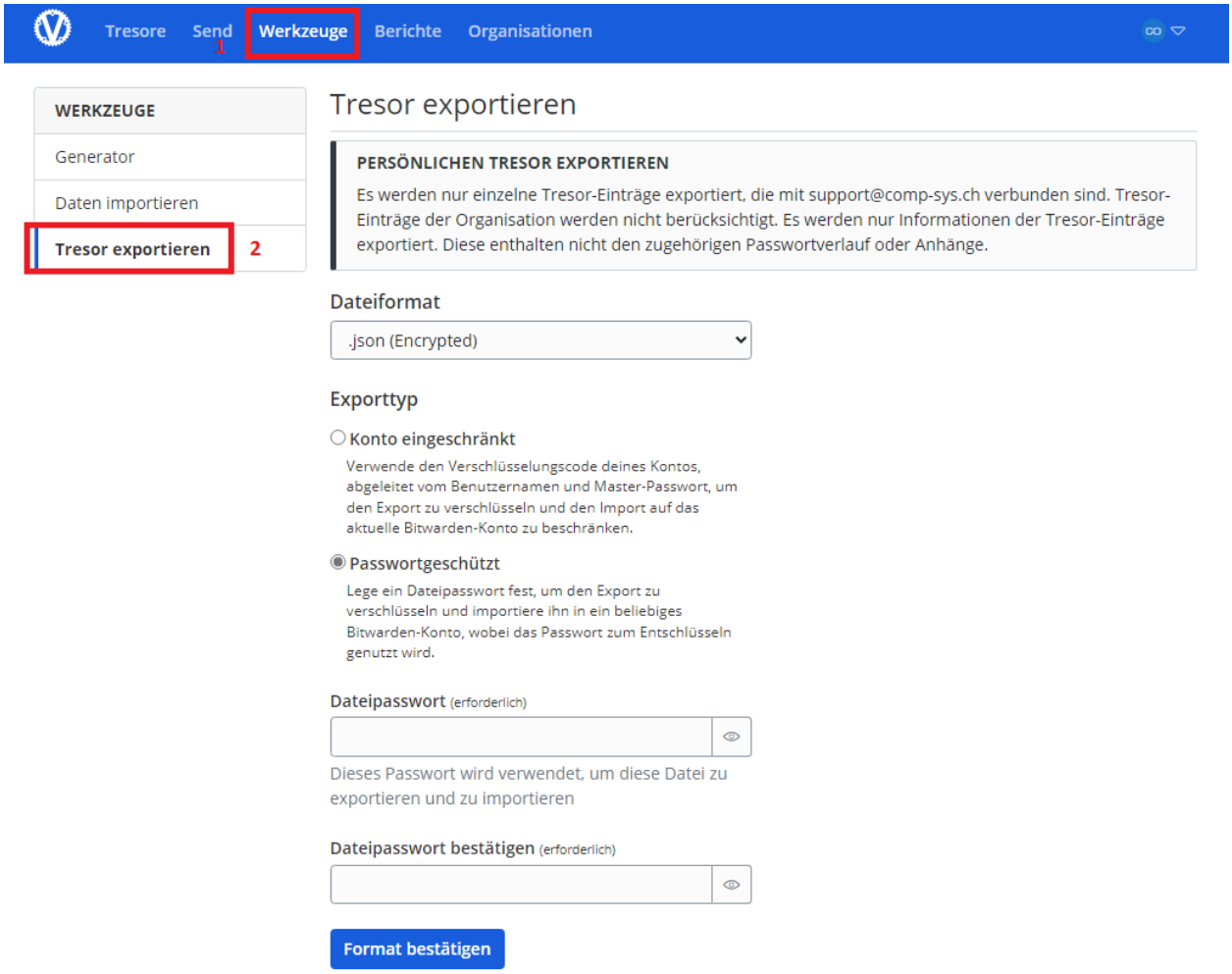
Wir empfehlen dabei immer die letzte Variante zu wählen und den Export mit einem Passwort abzusichern. Wenn Sie den Tresor accountgebunden exportierten, dann kann die Exportdatei nur in das Benutzerprofil mit der exakten ID in genau dem Tresor importiert werden, indem die Datei erstellt wurde. Ein mit Passwort abgesicherter Export kann in jedem beliebigen Passwortmanager wiederhergestellt werden (auch in einem neuen Tresor11).

Ebenfalls besteht die Möglichkeit eines unverschlüsselten Exports, indem alle Passwörter im Klartext sichtbar sind. Dies kann nützlich sein z.B. für einen Ausdruck, um diesen dann in einem physischen Safe zu verwahren. Unverschlüsselte Exports sind insofern riskant, dass jemand, der an die Datei gelangt, alle Passwörter einsehen kann. Entsprechend sollten solche Dateien nie länger als nötig aufbewahrt werden (nur für einen Ausdruck über einen bekannten, lokalen Drucker, dann komplett bereinigen; nicht nur in den Papierkorb; nirgends hochladen).

## Export eines Benutzertresors

Um Ihren persönlichen Tresor zu exportieren, loggen Sie sich zuerst in Ihrem Web-Tresor ein und navigieren dann im oberen Register auf «Werkzeuge», dann im Anschluss im linken Register auf «Tresor exportieren».

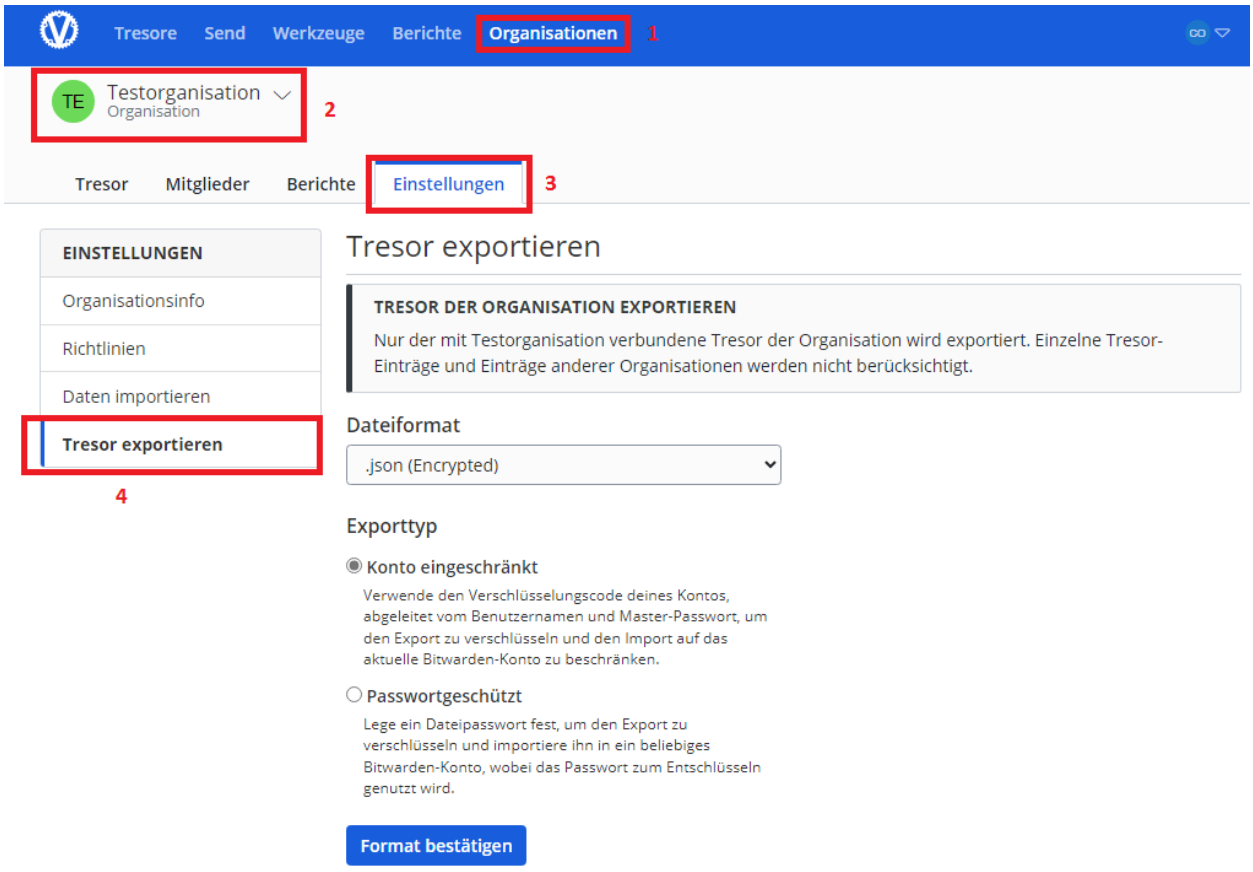
Als Dateiformat empfehlen wir «.json (Encrypted)» und für den Exporttyp wählen Sie bitte «Passwortgeschützt» aus. Im Anschluss können Sie der exportierten Datei ein Verschlüsselungspasswort zuweisen (Achtung: Wenn Sie das Passwort vergessen, ist die Datei nutzlos).
Klicken Sie im Anschluss auf «Format bestätigen». Ihr Browser sollte nun die verschlüsselte Datei herunterladen.



## Export eines Organisationstresors

Der Export eines Organisationstresors funktioniert analog zum Export eines Benutzertresors; jedoch findet sich das Menü an einem anderen Ort.

Wenn Sie einen Organisationstresor exportieren möchten, navigieren Sie in Ihrem Web-Tresor zur Admin-Konsole, dann wählen Sie die Organisation aus, deren Tresor Sie exportieren möchten, wählen im mittleren Register «Einstellungen» und dann im linken Register «Tresor exportieren». Der restliche Ablauf ist identisch zum Ablauf des Benutzertresorexports (siehe oben).



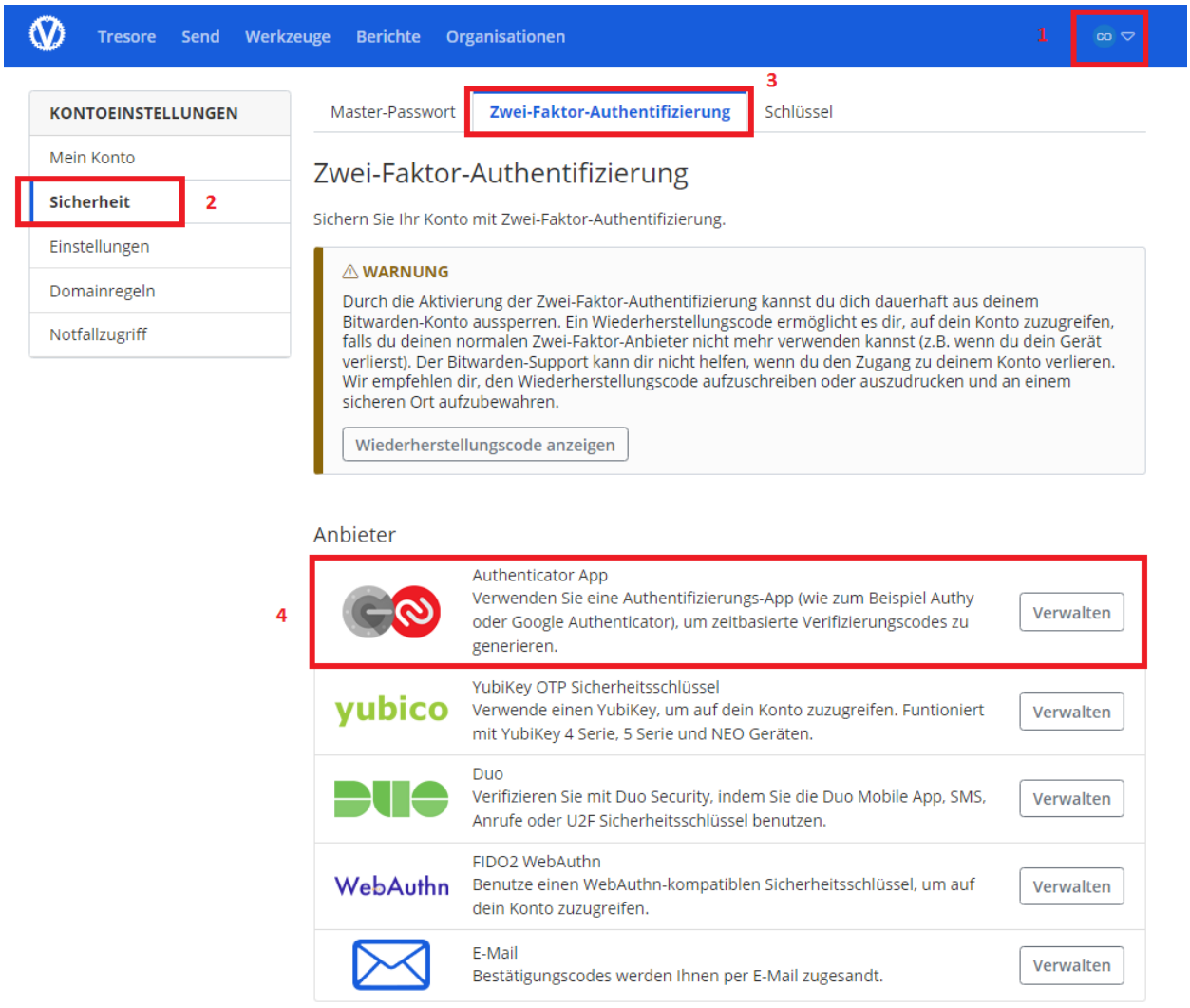
## 2-Faktor-Authentifizierung

Die 2-Faktor-Authentifizierung (im Folgenden «MFA» genannt) fügt Ihren Accounts eine weitere Sicherheitsebene hinzu und kann über den Web-Tresor aktiviert werden.

Wenn MFA aktiv ist, wird zum Login ein weiterer Identifikationsfaktor benötigt. Dazu wird das Mobiltelefon mit einer entsprechenden Authentifizierungs-App verwendet. So reicht das Masterpasswort allein für einen Login in Ihren Tresor11 nicht mehr aus.

Die Aktivierung von MFA wird ausdrücklich empfohlen, um die Sicherheit Ihrer Konten zu erhöhen.

Um MFA zu aktivieren, navigieren Sie zu Ihren «Kontoeinstellungen» über Ihr Profilicon oben rechts, dann im linken Register zu «Sicherheit» und im zentralen Register dann zu «Zwei-Faktor-Authentifizierung».
Wählen Sie dann «Authenticator App» aus (auch andere Zusatzfaktoren wären möglich, wir empfehlen jedoch eine App).



## Kontowiederherstellungsverwaltung

Der Tresor11 bietet eine Funktion zur Wiederherstellung von Konten bei vergessenen Passwörtern. So kann der Admin-User die Masterpasswörter von zusätzlichen Usern zurücksetzen.

Beachten Sie: Das Masterpasswort des Admin-Users kann **nicht** zurückgesetzt werden. Bewahren Sie dieses Passwort in jedem Fall sicher auf, ansonsten droht vollständiger Passwortverlust.

Folgende Abschnitte beschreiben, wie die Kontowiederherstellung konfiguriert und verwaltet werden kann.

### Einrichten der Kontowiederherstellungsverwaltung

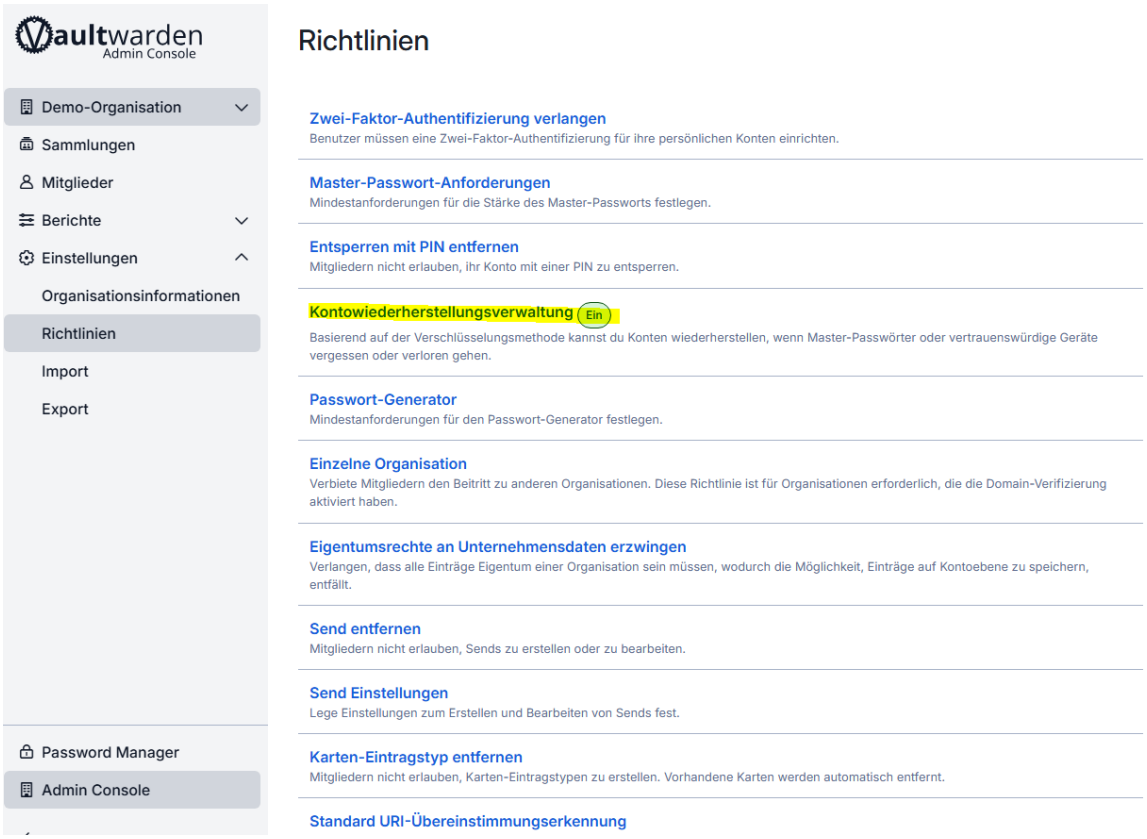
**Wenn Sie Ihren Tresor nach dem 20.03.2026 von uns erhalten haben, sind diese Einstellungen bereits gesetzt. In diesem Fall können Sie zum nächsten Kapitel «Verwenden der Kontowiederherstellungsverwaltung» springen.**

**Wenn Sie die Kontowiederherstellung auf einem älteren Tresor selbst aktivieren, müssen die User, die bereits Mitglieder der Organisation sind, aus der Organisation entfernt und erneut eingeladen werden. Erst dann ist die Passwortwiederherstellung bei diesen Profilen aktiviert.**

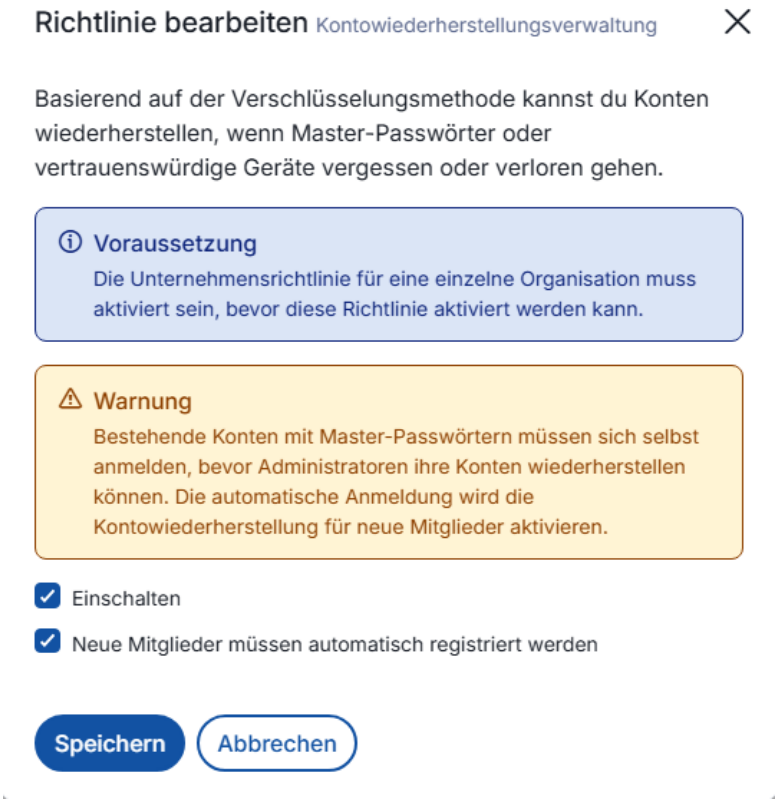
Damit Passwörter von Benutzern zurückgesetzt werden können, muss die Kontowiederherstellungsverwaltung erst aktiviert werden. Dies wird folgendermassen konfiguriert:

1. An Ihrem Tresor11 mit dem Admin-Benutzer anmelden.
2. Unten links auf «Admin Console» umstellen.

3. Im Menu zu «Einstellungen > Richtlinien» wechseln und «Kontowiederherstellungsverwaltung» anklicken.



4. Im nächsten Fenster Richtlinie «Einschalten» und «Neue Mitglieder müssen automatisch registriert werden» anhaken und «Speichern».




## Verwenden der Kontowiederherstellungsverwaltung

Bei aktiver Kontowiederherstellungsverwaltung erscheint bei eingeladenen Usern in der Mitglieder-Übersicht ein Schlüssel-Symbol unter «Richtlinien». Das Symbol weist darauf hin, dass das Passwort dieses Users zurückgesetzt werden kann, da die Kontowiederherstellungsverwaltung aktiv ist.


Mit einem Klick auf die 3 Punkte beim Eintrag des betroffenen Users kann dann «Konto wiederherstellen» ausgewählt werden.

Danach kann vom Admin für den betroffenen Benutzer ein neues Masterpasswort gesetzt werden.

## Weitere Informationen

Weitere Informationen zu Funktionen des Tresors können den offiziellen Dokumentationen entnommen werden.

1. Offizielle Bitwarden-Dokumentation:
   Password Manager Overview | Bitwarden Hilfe-Center
2. Offizielle Vaultwarden-Dokumentation:
   Home · dani-garcia/vaultwarden Wiki · GitHub