Funktionen

- Android - Auto-Fill Logins
- Browser-Erweiterungen - Auto-Fill Logins
- Tresor-Berichte

Android - Auto-Fill Logins

> **STATUS: VALID**

Du kannst die Android-App verwenden, um neue Anmeldungen hinzuzufügen und bestehende Anmeldungen im Web und in anderen Apps automatisch auszufüllen. Abhängig von Deiner Version von Android gibt es mehrere Optionen, die aktiviert werden können, um alle Auto-Fill-Szenarien abzudecken. Diese Optionen können in der App unter ***Einstellungen*** aktiviert werden. Wenn sie konfiguriert sind, solltest Du ***Aktiviert*** in grünem Text sehen.

Unterstützte Optionen

01. ***Auto-Fill Service*** verfügbar auf Android 8 und höher.

02. ***Inline Auto-Fill*** auf Android 11 und höher verfügbar.

03. ***Bedienungshilfe verwenden*** auf allen Android-Versionen verfügbar.

04. ***Overlay*** verfügbar auf Android 6 und höher.

Auto-Fill-Dienst

Der Auto-Fill-Service ist nur für Benutzer mit Android 8 und höher verfügbar.

01. Öffne die Bitwarden Android-App.

02. Tippe auf ***Einstellungen***.

03. Tippe auf ***Auto-Fill-***Dienste.

04. Suche Bitwarden in der Liste und aktiviere es.

Der Autofill Service ist jetzt aktiviert und ist kontextsensitiv und wird immer dann angezeigt, wenn Du auf ein Formular stossen, das auf Deinem Gerät automatisch ausgefüllt werden kann.

Inline Auto-Fill

Wenn die Funktion auf einem Android 11 oder höher mit einer unterstützten Tastatur aktiviert ist, ändert ***Inline Auto-Fill*** die ***Auto-Fill***-Präsentation von einem Popup-Fenster in eine in die Tastatur eingebettete Liste.

01. Öffne die Android-App.

02. Tippe auf ***Einstellungen***.

03. Tippe auf ***Auto-Fill-***Dienste.

04. Tippe auf den Schalter ***Inline Auto-Fill verwenden*** (***Auto-Fill***-Dienst muss aktiviert sein).

Bedienungshilfe

Wenn aktiviert, kann die App ein Popup über andere Anwendungen legen, das einige der Funktionen des `Auto-Fill`-Dienstes simuliert.

01. Öffne die Android-App.

02. Tippe auf ***Einstellungen***.

03. Tippe auf ***Auto-Fill-***Dienste.

04. Tippe auf den Schalter ***Bedienungshilfe verwenden***.

05. Suche die App in der Liste und wähle es aus.

Der Dienst ***Bedienungshilfe*** ist jetzt aktiviert und ist kontextsensitiv und wird immer dann sichtbar und/oder verfügbar sein, wenn Du auf ein Formular stossen, das auf Deinem Gerät automatisch ausgefüllt werden kann.

Overlay

Wenn aktiviert, kann die App ein Popup über andere Anwendungen legen, das einige der Funktionen des `Auto-Fill`-Dienstes simuliert.

01. Öffnen Sie die Android-App.

02. Tippe auf ***Einstellungen***.

03. Tippe auf ***Auto-Fill-***Dienste.

04. Tippe auf den Schalter ***Overlay verwenden*** (***Bedienungshilfe*** muss aktiviert sein).

05. Wenn Du Android 11 oder höher verwendest, suche die App in der Liste und wähle es aus.

06. Tippe auf den Schalter ***Anzeige über andere Anwendungen zulassen*** und gehe zurück.

> **Done!**

Browser-Erweiterungen - Auto-Fill Logins

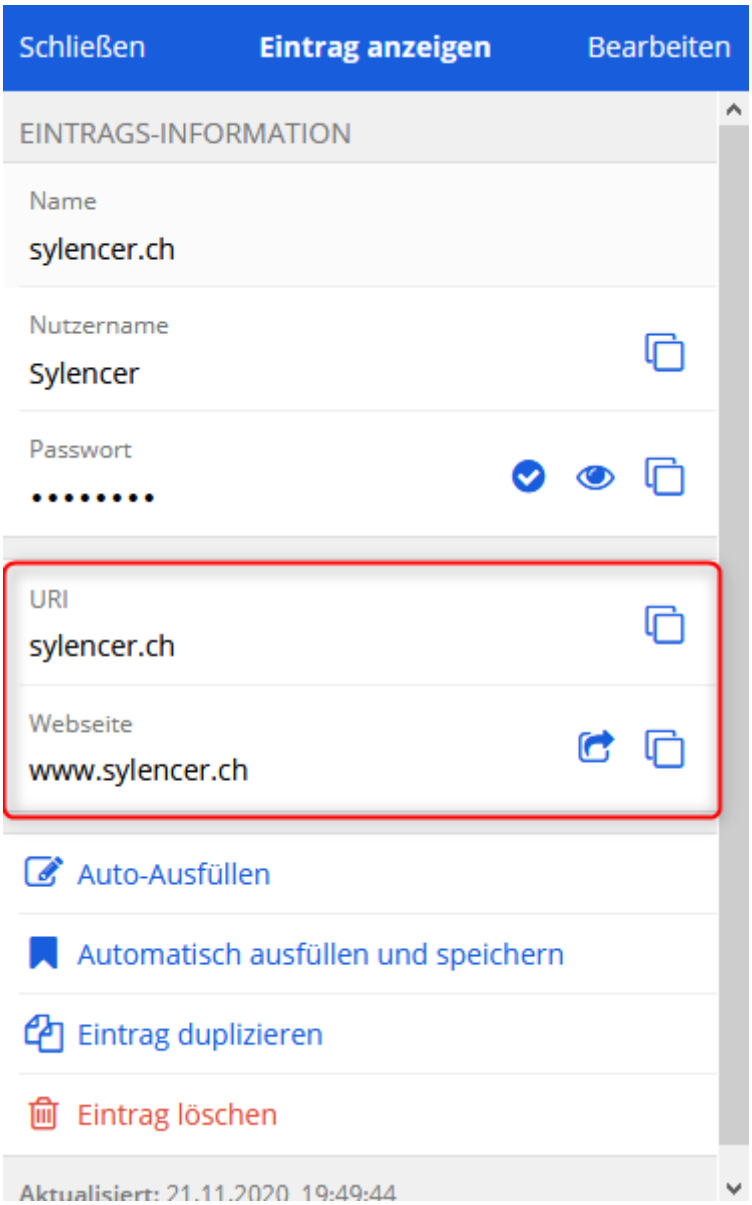
> **STATUS: VALID**

Du kannst die Browser-Erweiterung verwenden, um Anmeldeformulare auf Websites mit Deinen Benutzernamen/E-Mail- und Passwort-Anmeldedaten einfach automatisch auszufüllen.

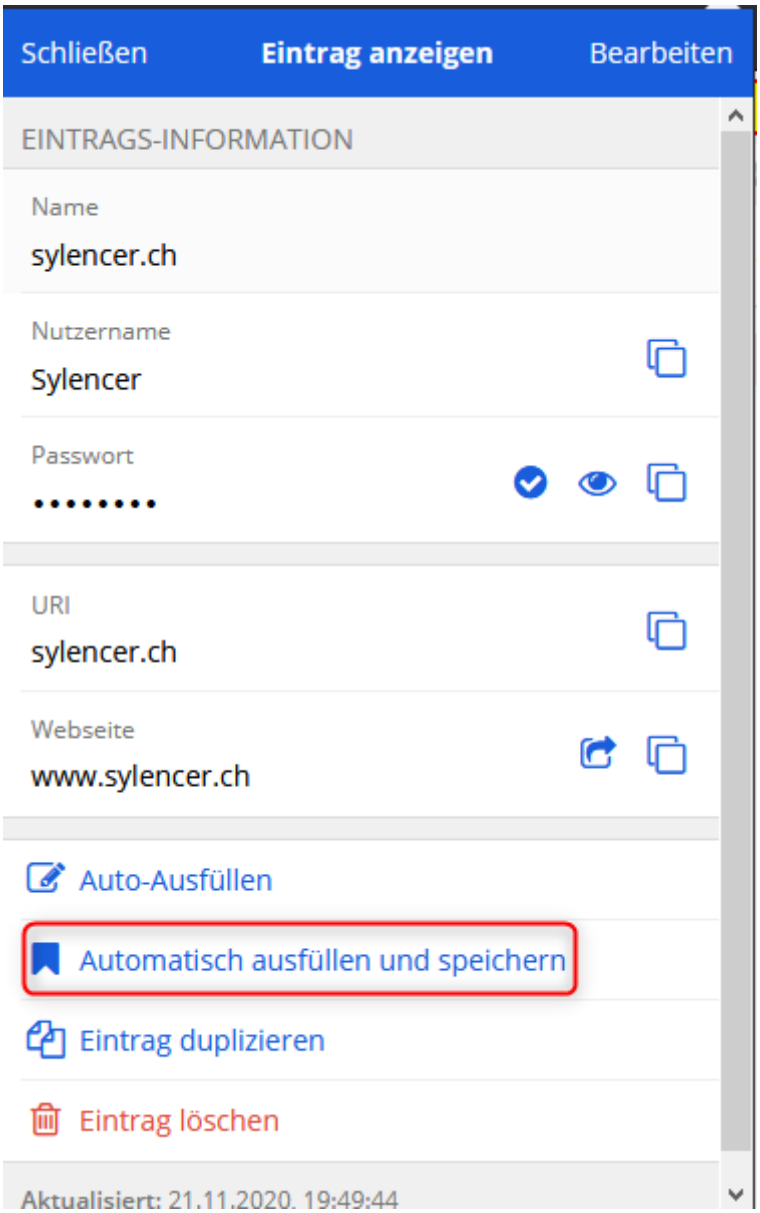
Eine Website zu einem gespeicherten Login hinzufügen

Um die meisten automatischen ***Auto-Fill***-Funktionen zu nutzen, musst Du die ***URL (URI)*** der Website zu den Anmeldedaten hinzufügen, die Du in Sylencer-Password gespeichert hast.

Du kannst die Websites, die mit einem Login verbunden sind, manuell auf der ***Bearbeiten***-Seite für dieses Login bearbeiten. Die ***URI***-Liste zeigt die Websites, die derzeit mit der Anmeldung verknüpft sind. Wenn Du eine neue Anmeldung erstellst, während Du die Website geöffnet hast, wird die Website automatisch in der ***URI***-Liste angezeigt.



Alternativ kannst Du die Anmeldung für die aktuelle Website automatisch ausfüllen und die Website zu dieser Anmeldung hinzufügen, indem Du auf dem Bildschirm ***Element anzeigen*** für diese Anmeldung auf die Schaltfläche ***Automatisch ausfüllen und speichern*** klickst.



How-To Auto-Fill

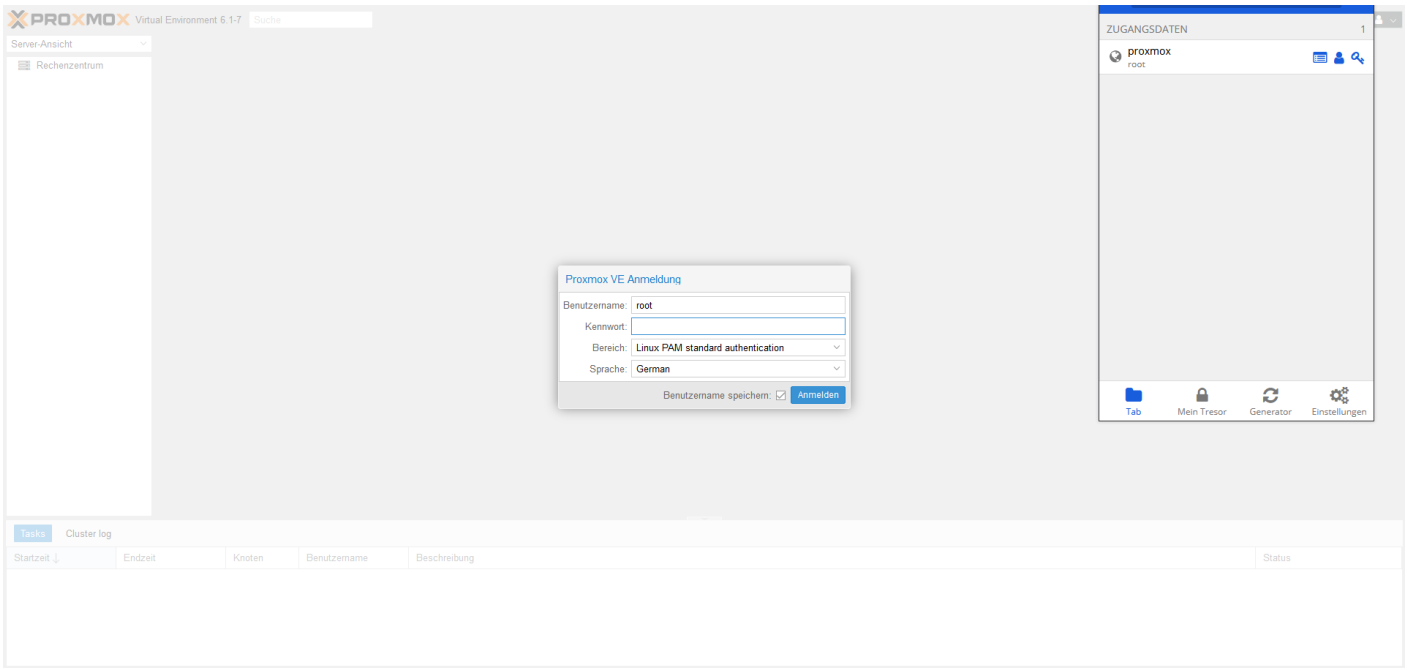
Es gibt eine Vielzahl von Möglichkeiten, mit Sylencer-Password ***Auto-Fill*** durchzuführen.

Popup-Fenster

Die App-Symbol in der Symbolleiste Deines Browsers zeigt die Anzahl der Logins in Deinem Tresor an, die mit der aktuell angezeigten Website übereinstimmen. Wenn Du das Bitwarden-Symbol wählst, wird das Popup-Fenster geöffnet, das standardmässig die Seite ***Aktuelle Registerkarte***

anzeigt. Die Seite ***Aktuelle Registerkarte*** zeigt eine Liste dieser übereinstimmenden Logins.

Wenn Du gerade ein Anmeldeformular auf einer Website anzeigst, führt die Auswahl einer Anmeldung aus der Liste ***Aktueller Reiter*** dazu, dass die Anmeldedaten automatisch in das Anmeldeformular eingetragen werden.

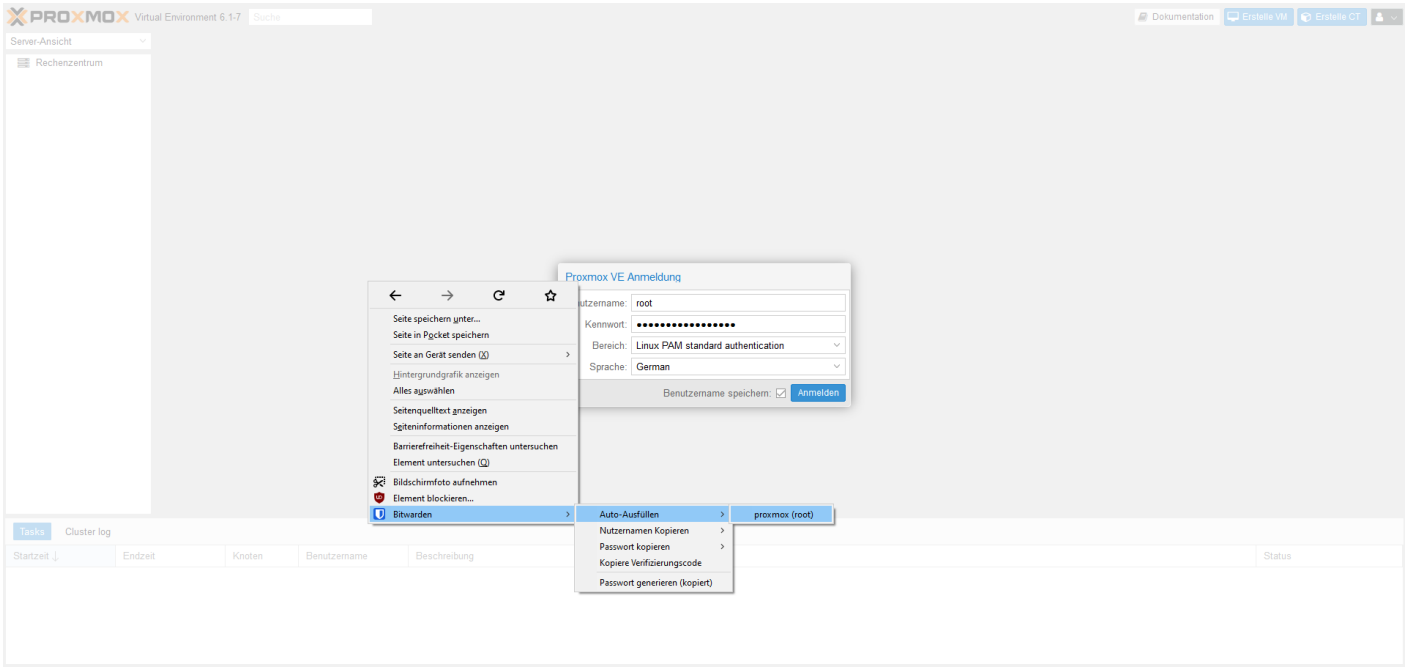


Wenn die Anmeldung nicht auf der Seite Aktuelle Registerkarte erscheint, kannst Du die Anmeldung von Deinem Tresor öffnen und auf die Schaltfläche ***Auto-Fill*** klicken. Dadurch wird die aktuelle Website automatisch ausgefüllt, auch wenn diese Website nicht mit dem Login verknüpft ist.

Rechtsklick

> **Diese Funktion ist derzeit im Safari-Browser nicht verfügbar.**

Die gleiche Liste von Anmeldungen, die bei Verwendung des Popup-Fensters verfügbar sind, ist auch über den Rechtsklick Deines Browsers verfügbar.



Tastaturkürzel (Shortcuts & Hot Keys)

Du kannst eine Reihe von Tastaturkürzeln verwenden, um ein Anmeldeformular schnell und automatisch auszufüllen. Wenn Du das Anmeldeformular anzeigst, drücke die Tastenkombination (siehe unten), und die zuletzt für diese Website verwendete Anmeldung wird automatisch ausgefüllt.

- Windows: ***Ctrl (Strg) + Umschalt + L***
- Linux: ***Ctrl (Strg + Umschalttaste + L***
- macOS: ***Cmd + Umschalt + L***
  - Safari: ***Cmd +*** \ oder ***Cmd + 8*** oder ***Cmd + Umschalt + P***

Wenn ein Shortcut nicht funktioniert, kann dies daran liegen, dass sie bereits von einer anderen Anwendung auf Deinem Gerät verwendet wird. Zum Beispiel wird die *Auto-Fill*-Shortcut unter Windows üblicherweise von der AMD Radeon Adrenaline Software (AMD-Grafiktreiber) beansprucht und kann daher von Sylencer-Password nicht verwendet werden. Du kannst diese Abkürzung freigeben, indem Du sie in der AMD Radeon Software unter *Gaming → Global Settings → Performance Monitoring ändern: Hotkey für die Leistungsprotokollierung umschalten*.

Eine weitere Möglichkeit ist das Öffnen des Popup-Fensters mit Hilfe des Shortcuts (siehe unten). Du kannst dann mit der Tabulatortaste auf die Anmeldung tippen, die Du automatisch ausfüllen möchtest, und dann zur Auswahl ***ENTER*** drücken.

- Windows: ***Ctrl (Strg) + Umschalt + Y***
- Linux: ***Ctrl (Strg) + Umschalt + U***
- macOS: ***Cmd + Umschalt + Y***

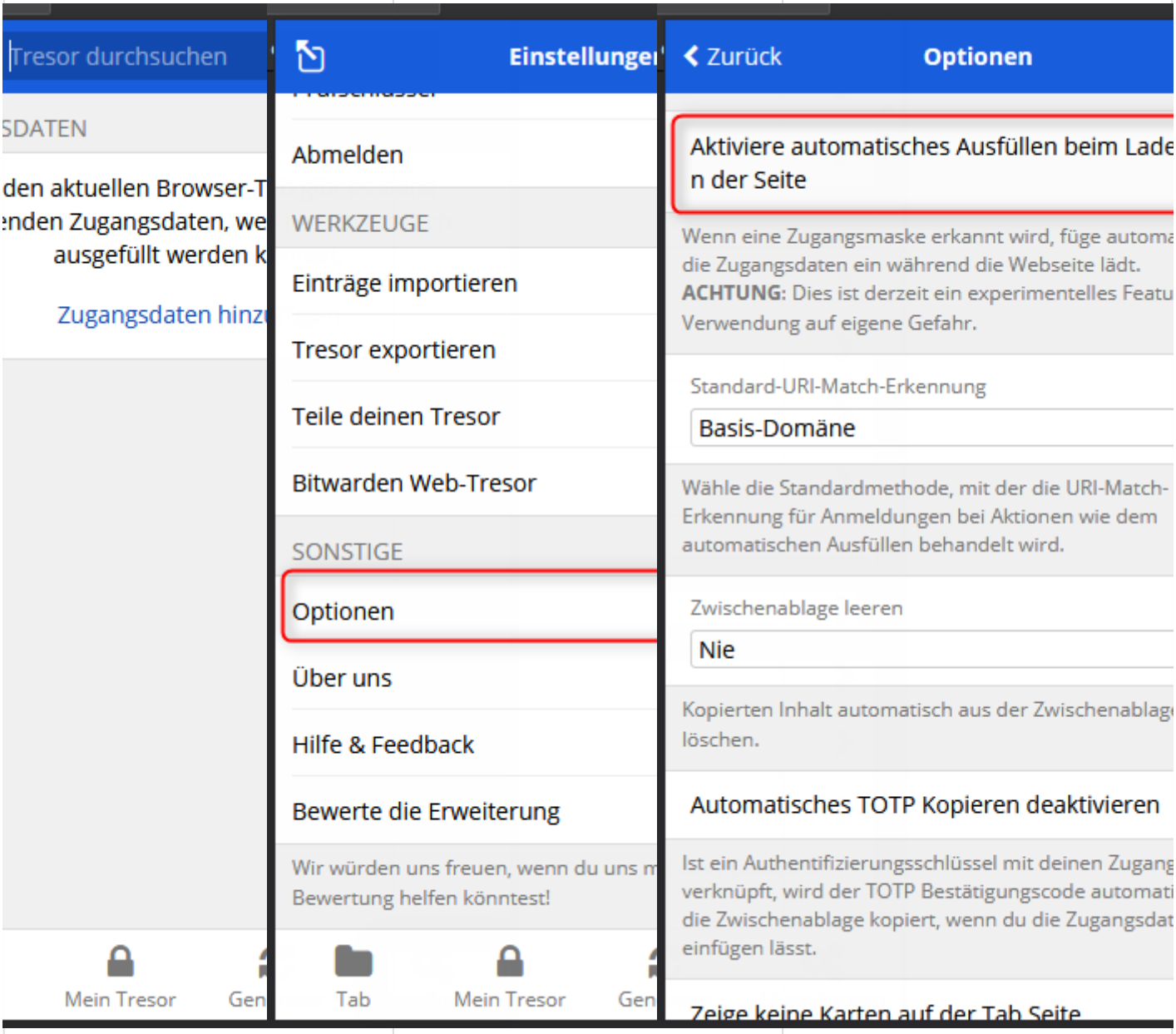
Du kannst diese Tastenkombinationen in den Browsern Chrome, Opera, Edge und Brave leicht anpassen. Navigiere in der Adressleiste zu ***chrome://extensions*** und suche die Schaltfläche ***Tastaturkürzel*** (möglicherweise musst Du nach unten scrollen).

In Firefox musst Du auf die Einstellungsseite der Addons gehen. Klicke unter dem Zahnradsymbol auf die Schaltfläche ***Tastaturkürzel für Erweiterungen verwalten***.

Andere Browser wie Safari und Legacy Edge unterstützen derzeit nicht die Änderung der Standard-Tastaturkürzel für Erweiterungen.

Auto-Fill beim Laden der Seite

Sylencer-Password enthält eine experimentelle Funktion zum Auto-Fill von Anmeldungen unmittelbar nach dem Laden einer Webseite mit einem Anmeldeformular in Deinem Browser. Diese Funktion setzt voraus, dass Du Dich für die Nutzung anmeldest. Du kannst Aktiviere automatisches Ausfüllen beim Laden der Seite unter ***Einstellungen → Optionen*** aktivieren.



Im Falle von mehreren Anmeldungen, die mit der aktuellen Website übereinstimmen, wird die zuletzt verwendete Anmeldung für den ***Auto-Fill*** verwendet. Wenn die falsche Anmeldung automatisch ausgefüllt wird, kannst Du das Popup-Fenster erneut automatisch ausfüllen und die zuletzt verwendete Anmeldung zurücksetzen.

> **Done!**

Tresor-Berichte

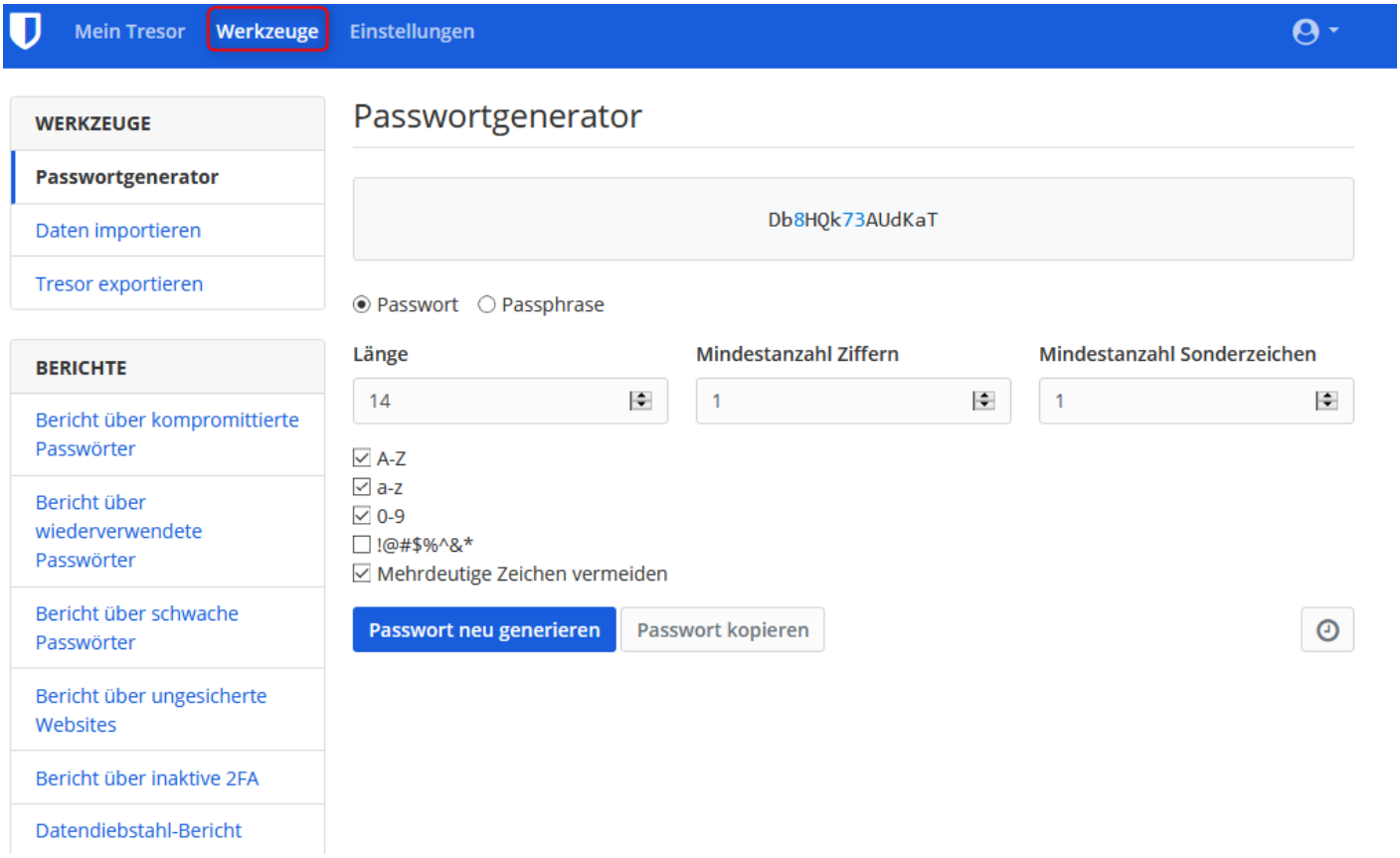
STATUS: VALID

Berichte aufrufen

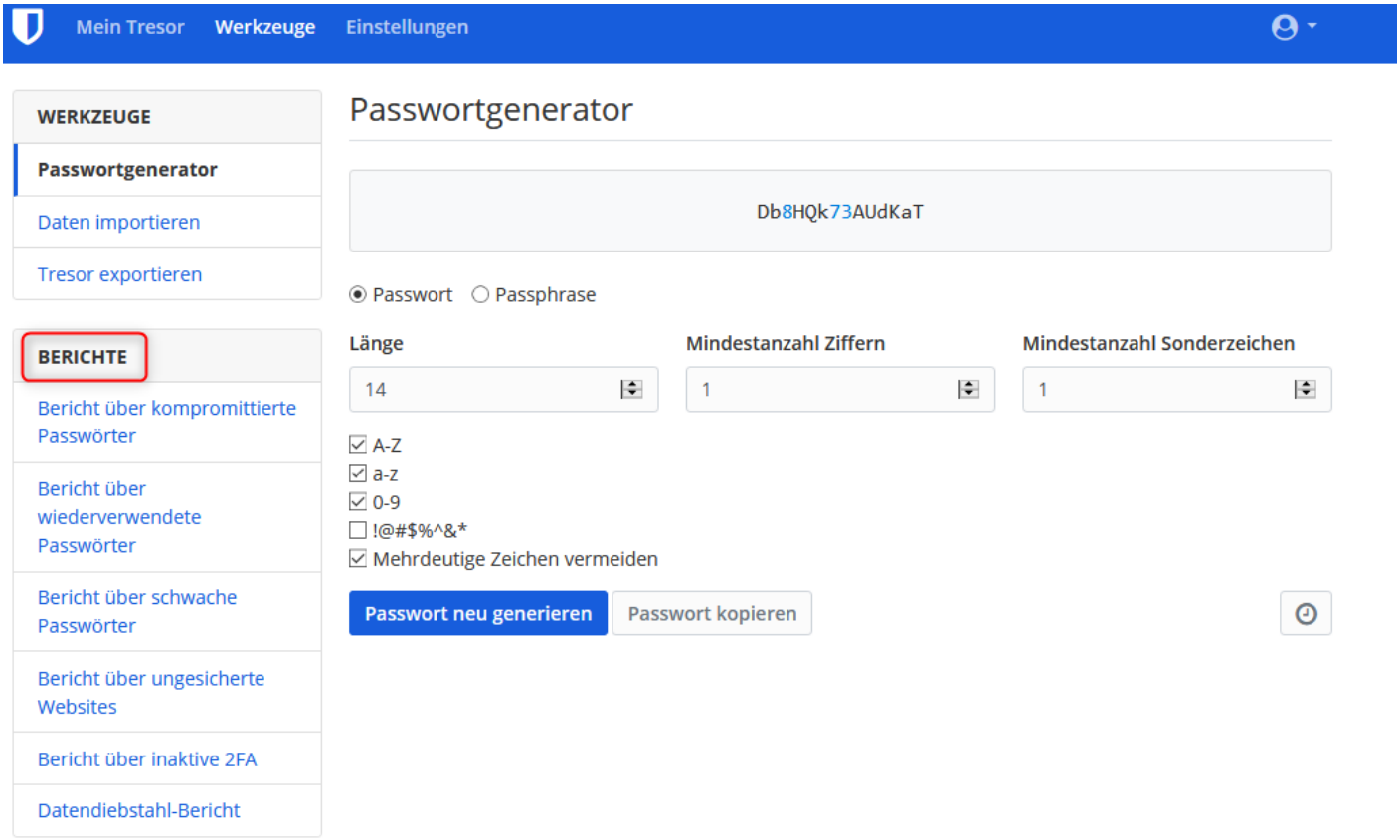
Mit Sylencer-Password kann der Benutzer auf eine Reihe von Berichtswerkzeugen zugreifen, um den Gesamtzustand ihres persönlichen Tresors wie folgt zu bewerten:

01. Logge Dich in den Web-Tresor unter dem URL ***[s. Zugangsdaten]*** ein.

02. Klicke in der oberen Navigationsleiste auf ***Werkezuge***.



03. Suche den Abschnitt ***Berichte***.



04. Wähle den gewünschten Bericht aus.

Verfügbare Berichte

Bericht über kompromittierte Passwörter

Dies sind Passwörter, die in bekannten Datenschutzverletzungen aufgedeckt wurden, die öffentlich veröffentlicht oder im Dark Web verkauft wurden.

Der Bericht verwendet einen vertrauenswürdigen Webdienst, um die ersten 5 Ziffern des Hashes alle Deiner Passwörter in einer Datenbank mit bekannten geleakten Passwörtern zu suchen. Die zurückgegebene übereinstimmende Liste von Hashes wird dann lokal mit dem vollständigen Hash Deiner Kennwörter verglichen. Dieser Vergleich wird nur lokal durchgeführt, um Deine ***k-Anonymität*** zu wahren.

Aber warum verwenden wir nur die ersten 5 Ziffern des Hashwerts Deiner Kennwörter? Wenn der Bericht mit Deinen tatsächlichen Passwörtern durchgeführt wird, ist es egal, ob diese offengelegt werden oder nicht, Du würdst sie freiwillig an den Dienst weitergeben.

Und auch wenn das Ergebnis dieses Berichts nicht bedeutet, dass Dein individuelles Konto kompromittiert wurde, sondern nur, dass Du ein Kennwort verwendest, das in diesen Datenbanken mit exponierten Kennwörtern gefunden wurde, solltest Du es vermeiden, durchgesickerte und nicht eindeutige Kennwörter zu verwenden.

Bericht über wiederverwendete Passwörter

Wenn ein von Dir genutzter Dienst kompromittiert wurde, kann die Wiederverwendung desselben Passworts an anderer Stelle Hackern den Zugriff auf weitere Deiner Online-Konten erleichtern. Du solltest für jedes Konto oder jeden Dienst ein eindeutiges Kennwort verwenden. Der Bericht ***Wiederverwendete Passwörter*** hilft Dir, diese missbräuchlichen Passwörter leicht zu identifizieren.

Bericht über schwache Passwörter

Schwache Kennwörter können leicht von Hackern und automatisierten Tools erraten werden, die zum Knacken von Kennwörtern verwendet werden. Verwende den ***Bericht über schwache Passwörter***, um diese Passwörter schnell zu isolieren. Der Sylencer-Passwortgenerator kann Dir helfen, stärkere Passwörter zu erstellen.

Bericht über ungesicherte Websites

Die Verwendung ungesicherter Websites mit dem ***http://*** Schema kann gefährlich sein. Wenn die Website es erlaubt, solltest Du immer mit dem ***https://*** Schema zugreifen, damit Deine Verbindung verschlüsselt ist.

Bericht über inaktive 2FA

Die Zwei-Faktor-Authentifizierung (2FA) ist eine wichtige Sicherheitseinstellung, die dazu beiträgt, Deine Konten zu schützen. Wenn die Website dies anbietet, solltest Du die Zwei-Faktor-Authentifizierung immer aktivieren. Der Inactive 2FA Report sucht in Deinem Tresor nach Objekten, bei denen Du keinen TOTP-Authentifizierungsschlüssel hinterlegt hast und vergleicht diese dann mit Daten von ***https://twofactorauth.org/***.

Datendiebstahl-Bericht (nur für einzelne Tresore)

Ein ***Bruch*** ist ein Vorfall, bei dem die Daten einer Website illegal von Hackern eingesehen und dann öffentlich veröffentlicht wurden. Mit dem ***Datendiebstahl-Bericht*** kannst Du die Arten von Daten überprüfen, die bei diesen Brüchen kompromittiert wurden (E-Mail-Adressen, Kennwörter, Kreditkarten usw.) und entsprechende Massnahmen ergreifen, wie z. B. das Ändern von Kennwörtern.

> **Done! Herzlichen Glückwunsch! Du hast soeben Deine Passwörter auf die Sicherheit überprüft und Gegenmassnahmen ergriffen.**