



PassCircle

BEDIENER-HANDBUCH

PassCircle bedienen

Alles für den täglichen Umgang mit Ihrem Tresor: anmelden, Zugänge sicher speichern und generieren, Formulare per Browser-Erweiterung ausfüllen und Passwörter geschützt mit Kolleginnen, Kollegen und Externen teilen – Schritt für Schritt erklärt.

Version 1.9.2 · Stand: Juli 2026 · © MARIOSIEBERT-IT

Handbuch für Anwenderinnen und Anwender · Fragen an info@mariosiebert-it.de

 Tresor & Ordner

 Authenticator (2FA)

 Browser-Erweiterung

 Passkeys

Inhalt

- | | | | |
|----------|---------------------------------------|-----------|---------------------------------------|
| 1 | Was ist PassCircle? | 7 | Abteilungen (geteilte Bereiche) |
| 2 | Registrieren & Anmelden | 8 | Import & Export |
| 3 | Zwei-Faktor-Authentifizierung (2FA) | 9 | Browser-Erweiterung |
| 4 | Der Tresor: Ordner, Einträge, Anhänge | 10 | Passkeys |
| 5 | Sicher senden | 11 | Zugriff per App (Windows, Mac, Handy) |
| 6 | Konto: Name & Master-Passwort | | |

Was ist PassCircle?

PassCircle ist ein sicherer Passwort-Tresor für Unternehmen. Sie speichern Zugangsdaten – Benutzername, Passwort, URL, Notizen und sogar Dateien – verschlüsselt an einem Ort und rufen sie über den Browser, einen Windows- oder Mac-Client oder die Browser-Erweiterung ab. So brauchen Sie sich nur noch **ein einziges Passwort** zu merken: Ihr Master-Passwort.

Zero-Knowledge – was heißt das?

Alle Inhalte werden **auf Ihrem Gerät** ver- und entschlüsselt. Der Server speichert ausschließlich unlesbare (verschlüsselte) Daten. Der Schlüssel wird aus Ihrem **Master-Passwort** abgeleitet und verlässt Ihr Gerät nie. Das bedeutet: Selbst der Betreiber des Servers kann Ihre Passwörter nicht lesen.



Wichtig: Ihr Master-Passwort ist der Generalschlüssel zu allem. Ein Administrator kann es nur im Notfall zurücksetzen (falls Ihre Firma die Wiederherstellung aktiviert hat) – ansonsten gibt es keinen zweiten Weg. Wählen Sie ein **starkes und zugleich einprägsames** Passwort und geben Sie es niemals weiter.

2 Registrieren & Anmelden

Konto erstellen

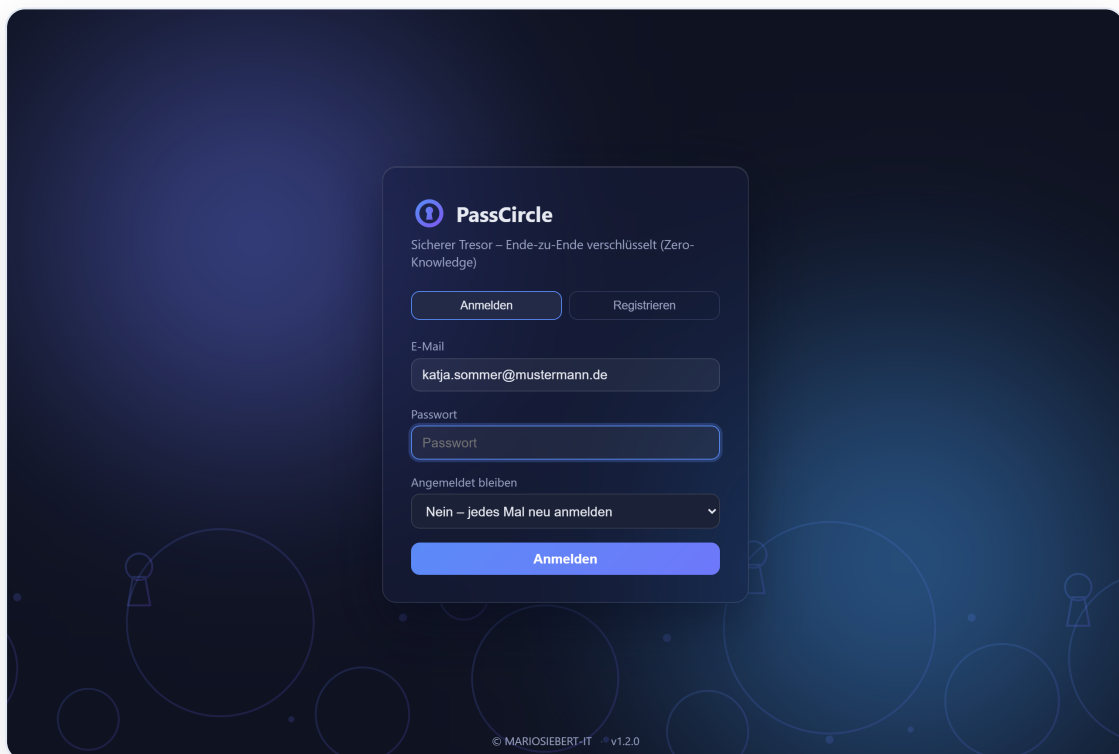
Öffnen Sie die PassCircle-Adresse Ihres Unternehmens im Browser (z. B.

<https://safe.firma.de:8443>). Je nach Einstellung Ihres Administrators gibt es zwei Wege:

- **Selbst registrieren:** Reiter **Registrieren** → E-Mail, Anzeigename und Master-Passwort (mindestens 8 Zeichen) eingeben → **Konto erstellen**. Ihr Konto muss anschließend von einem Administrator **freigegeben** werden – Sie können sich erst danach anmelden.
- **Vom Admin angelegt:** Sie erhalten Ihre E-Mail-Adresse und ein Initial-Passwort. Bitte ändern Sie dieses nach der ersten Anmeldung unter **Konto**.

Anmelden

E-Mail und Master-Passwort eingeben → **Anmelden**. Ist die Zwei-Faktor-Anmeldung (2FA) aktiv, geben Sie zusätzlich den aktuellen Code aus Ihrer Authenticator-App ein.



Die Anmelde- und Registrierungsmaske von PassCircle.

Angemeldet bleiben

Auf vertrauenswürdigen, gesperrten Geräten können Sie **Angemeldet bleiben** (z. B. 4 oder 8 Stunden) wählen, damit Sie nicht bei jedem Öffnen das Passwort neu eingeben müssen. Die maximale Dauer legt Ihr Administrator fest.

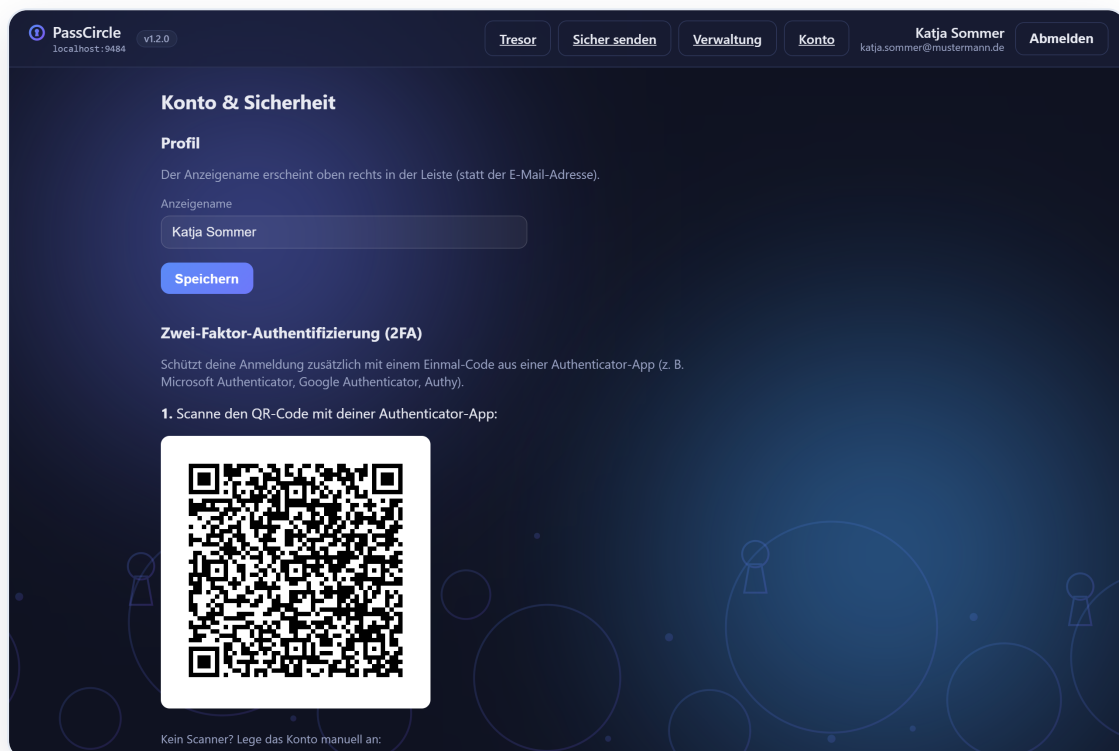


Auf gemeinsam genutzten PCs sollten Sie „Angemeldet bleiben“ nicht verwenden – dort ist die normale Anmeldung mit anschließender Abmeldung sicherer.

3 Zwei-Faktor-Authentifizierung (2FA)

Die 2FA schützt Ihr Konto zusätzlich mit einem Einmal-Code aus einer Authenticator-App (Microsoft- oder Google-Authenticator, Authy und andere). Selbst wer Ihr Master-Passwort kennt, kommt ohne diesen Code nicht hinein.

- 1 Öffnen Sie **Konto & Sicherheit** → **2FA einrichten**.
- 2 Scannen Sie den QR-Code mit Ihrer Authenticator-App (oder geben Sie den angezeigten Schlüssel manuell ein).
- 3 Geben Sie den aktuellen 6-stelligen Code ein → **Aktivieren**.



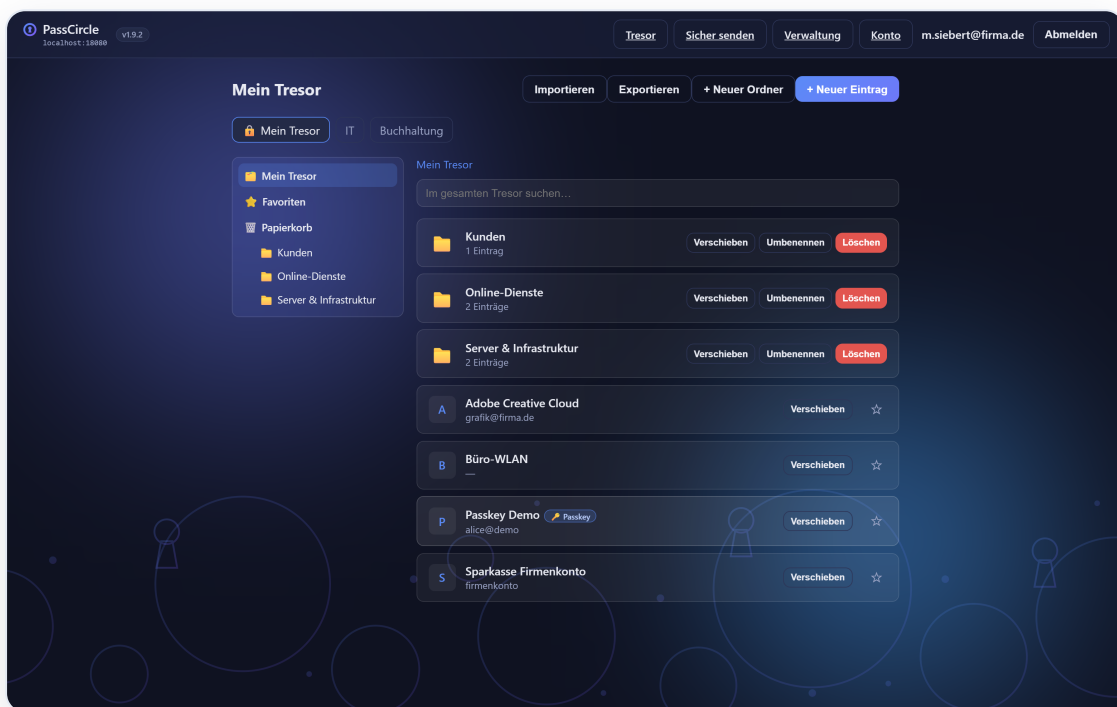
2FA-Einrichtung: QR-Code scannen und mit dem aktuellen Code bestätigen.



Tipp: TOTP-Codes hängen von der Uhrzeit ab. Falls „Code ungültig“ erscheint, prüfen Sie, ob die Uhrzeit auf Smartphone und Server automatisch und korrekt eingestellt ist.

Aufbau

Links sehen Sie den **Ordner-Baum**, oben den Klickpfad (Breadcrumb), rechts den Inhalt des gewählten Ordners. Ganz oben schalten Sie zwischen **Mein Tresor** (nur für Sie sichtbar) und Ihren **Abteilungen** um (falls vorhanden). In der Kopfleiste oben rechts steht Ihr **Anzeigenname** (darunter klein die E-Mail-Adresse) – so ist auf einen Blick erkennbar, wer angemeldet ist. Auf dem Smartphone ordnet sich die Leiste automatisch zweizeilig an.



Der Tresor: links der Ordner-Baum mit „ Favoriten“ und „ Papierkorb“, rechts die Einträge.

Ordner & Unterordner

- **Neuer Ordner:** legt einen Ordner im aktuell geöffneten Ordner an – beliebig tief verschachtelbar, z. B. „Kunde Müller ▶ VPN“.
- Ordner **umbenennen** oder **verschieben** über die Schaltflächen an der Ordnerzeile bzw. die Ordner-Auswahl im Editor.
- **Löschen** eines Ordners entfernt auch dessen gesamten Inhalt. Ist der Ordner nicht leer, warnt PassCircle ausdrücklich („Achtung – Datenverlust“) und nennt die Anzahl der enthaltenen Unterordner und Einträge; erst nach Bestätigung wird gelöscht (der Inhalt landet im Papierkorb, siehe unten).

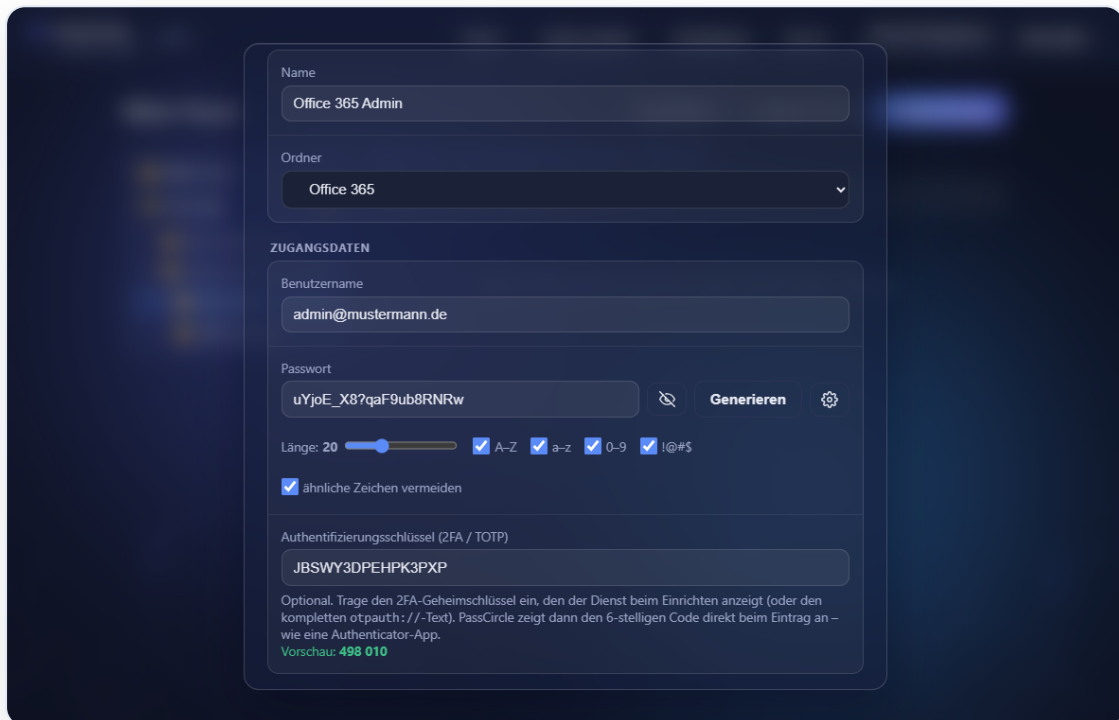
Eintrag anlegen

+ Neuer Eintrag öffnet das Eintrags-Fenster. Es ist in klar benannte Bereiche gegliedert: **Eintragsdetails** (Name, Ordner), **Zugangsdaten** (Benutzername, Passwort,

Authentifizierungsschlüssel), **Auto-Ausfüllen-Optionen** (Website-URL für die Browser-Erweiterung), **Weitere Optionen** (Notizen) und **Anhänge**. Speichern – fertig.

Passwort-Generator

Neben dem Passwortfeld erzeugt **Generieren** ein sicheres Passwort. Über das **Zahnrad** blenden Sie die Optionen ein: Länge, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen und „ähnliche Zeichen vermeiden“. Ist bereits ein Passwort eingetragen, **fragt PassCircle vor dem Ersetzen nach** – ein vorhandenes Passwort wird also nie versehentlich überschrieben. Das Passwortfeld ist standardmäßig maskiert und lässt sich über das Auge-Symbol einblenden.

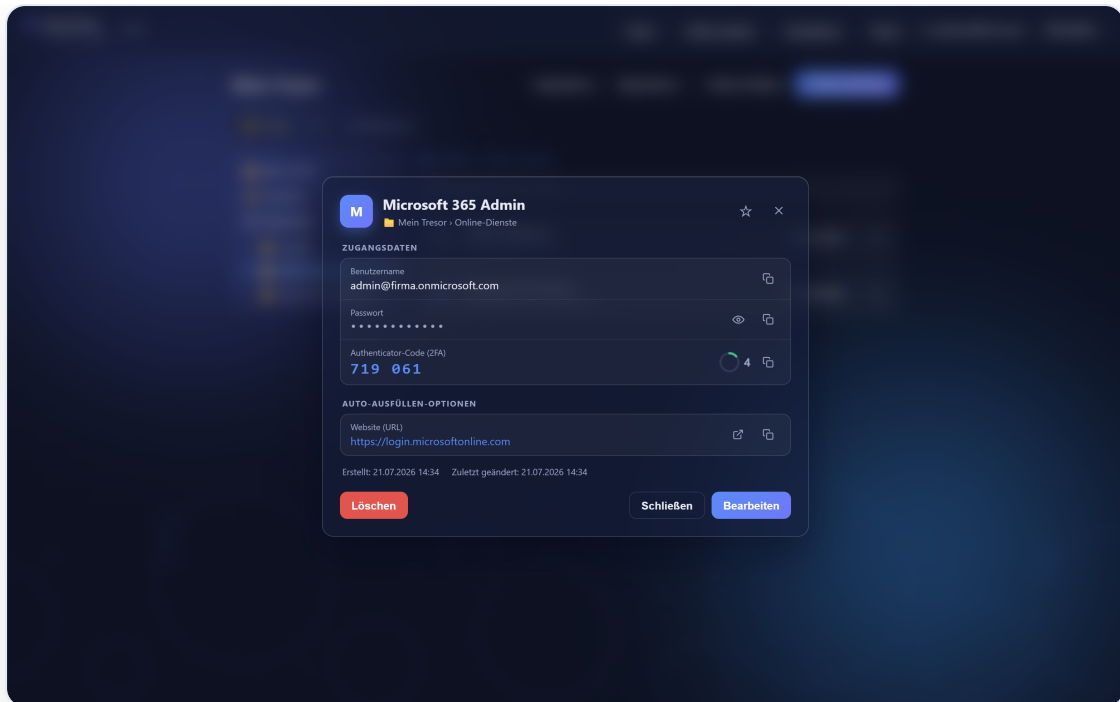
The image shows a dark-themed user interface for an entry editor. At the top, there are two input fields: 'Name' with the value 'Office 365 Admin' and 'Ordner' with a dropdown menu showing 'Office 365'. Below these is a section titled 'ZUGANGSDATEN'. It contains a 'Benutzername' field with 'admin@mustermann.de'. The 'Passwort' field shows a generated password 'uYjoE_X87qaF9ub8RNRw' and has a 'Generieren' button and a gear icon. Below the password field, there are checkboxes for 'Länge: 20' (with a slider), 'A-Z', 'a-z', '0-9', and '!@#\$', all of which are checked. There is also a checkbox for 'ähnliche Zeichen vermeiden' which is checked. At the bottom of the 'ZUGANGSDATEN' section is an 'Authentifizierungsschlüssel (2FA / TOTP)' field with the value 'JBSWY3DPEHPK3PXP'. Below this field, there is a small text block explaining that users can enter a 2FA secret key or a full otpauth://... URL, and that PassCircle will then display a 6-digit code directly at the entry. A 'Vorschau: 498 010' is shown in green.

Eintrags-Editor mit ausgeklappten Generator-Optionen (Zahnrad).

Authenticator-Schlüssel (2FA-Codes direkt am Eintrag)

Zu jedem Eintrag können Sie einen **Authenticator-Schlüssel** hinterlegen – also den geheimen 2FA-Schlüssel, den ein Dienst beim Einrichten der Zwei-Faktor-Anmeldung anzeigt. PassCircle berechnet dann den **6-stelligen Einmal-Code direkt beim Eintrag** – genau wie eine Authenticator-App, nur gleich neben dem Passwort. Sie müssen für die Anmeldung also nicht mehr zum Handy greifen.

- Im Editor das Feld **„Authenticator-Schlüssel (2FA / TOTP)“** ausfüllen: entweder den Base32-Schlüssel (z. B. **JBSW Y3DP EHPK 3PXP**) oder den kompletten **otpauth://...**-Text. Eine kleine Vorschau zeigt sofort, ob der Schlüssel gültig ist.
- In der Eintrags-Ansicht erscheint der aktuelle Code **direkt unter dem Passwort**, mit einem Ring, der die verbleibenden Sekunden bis zum nächsten Code anzeigt, und einem „Kopieren“-Knopf.



Die Eintrags-Ansicht: der Authenticator-Code erscheint mit Countdown-Ring direkt unter dem Passwort; oben Ordnerpfad und Favoriten-Stern.



Der Authenticator-Schlüssel wird – wie alles andere – Zero-Knowledge verschlüsselt gespeichert. Er verlässt Ihren Rechner nie im Klartext.

Datei-Anhänge

An jeden Eintrag können Sie Dateien anhängen (Screenshots, PDFs und mehr, bis 20 MB pro Datei). Auch Anhänge werden Zero-Knowledge verschlüsselt. Anhänge sind möglich, sobald der Eintrag einmal gespeichert wurde.

Eintrag bearbeiten

Name
Firmen-Mail (Office 365)

Ordner
Kunde Mustermann GmbH

Benutzername
m.mustermann@mustermann.de

Passwort
S9klvP2r\$Lm8qW **Generieren** ⚙️

Länge: 20 ☒ A-Z ☒ a-z ☒ 0-9
☒ !@#\$ ☒ ähnliche Zeichen vermeiden

Authenticator-Schlüssel (2FA / TOTP)
JBSWY3DPEHPK3XP

Optional. Trage den 2FA-Geheimschlüssel ein, den der Dienst beim Einrichten anzeigt (oder den kompletten otpauth://-Text). PassCircle zeigt dann den 6-stelligen Code direkt beim Eintrag an – wie eine Authenticator-App.
Vorschau: 754 677

URL
https://outlook.office.com

Notizen

Datei-Anhänge am Eintrag – verschlüsselt, bis 20 MB je Datei.

Favoriten (Stern)

Häufig gebrauchte Zugänge markieren Sie mit einem **Stern** – so sind sie mit einem Klick erreichbar, ohne durch die Ordner zu suchen. Klicken Sie in der Liste oder in der Eintrags-Ansicht auf das Stern-Symbol; es wechselt von ☆ zu ★.

- Oben im Ordner-Baum gibt es den Eintrag „**★ Favoriten**“ mit einem kleinen Zähler. Ein Klick zeigt alle markierten Einträge auf einmal – auch quer über verschiedene Ordner hinweg.
- Erneutes Klicken auf den Stern entfernt den Eintrag wieder aus den Favoriten.
- Favoriten funktionieren in „Mein Tresor“ und in Abteilungen, in denen Sie Schreibrechte haben.

Benutzen: Kopieren, Öffnen, Suchen

- Eintrag anklicken → Ansicht mit **Kopieren** für Benutzername und Passwort (mit kurzer Bestätigung „kopiert“).
- **URL öffnen:** Der Button **Öffnen** startet die Adresse im Standard-Browser.
- **Suche** oben durchsucht alle Ordner; jeder Treffer zeigt seinen Ordnerpfad.

Ordner & Einträge verschieben

Zum Umsortieren gibt es zwei Wege – beide fragen vorher nach, damit nichts versehentlich verrutscht:

- **Ziehen mit der Maus:** Einen Eintrag oder Ordner einfach auf den Ziel-Ordner ziehen – entweder im Ordner-Baum links oder auf eine Ordner-Zeile in der Liste. Das gültige Ziel wird beim Ziehen hervorgehoben. Ein Ablegen auf „**Mein Tresor**“ schiebt das Element zurück auf die Hauptebene.
- **Knopf „Verschieben“:** An jedem Eintrag und Ordner. Er öffnet eine Ziel-Auswahl und funktioniert überall – auch auf **Smartphone und Tablet**, wo Ziehen nicht möglich ist.

Ordner wandern immer **mit ihrem gesamten Inhalt**. Ein Ordner lässt sich nicht in seinen eigenen Unterordner ziehen – das wird gar nicht erst angeboten. Verschieben funktioniert in „Mein Tresor“ und in allen Abteilungen, in denen Sie Schreibrechte haben.

Papierkorb (Löschen mit Sicherheitsnetz)

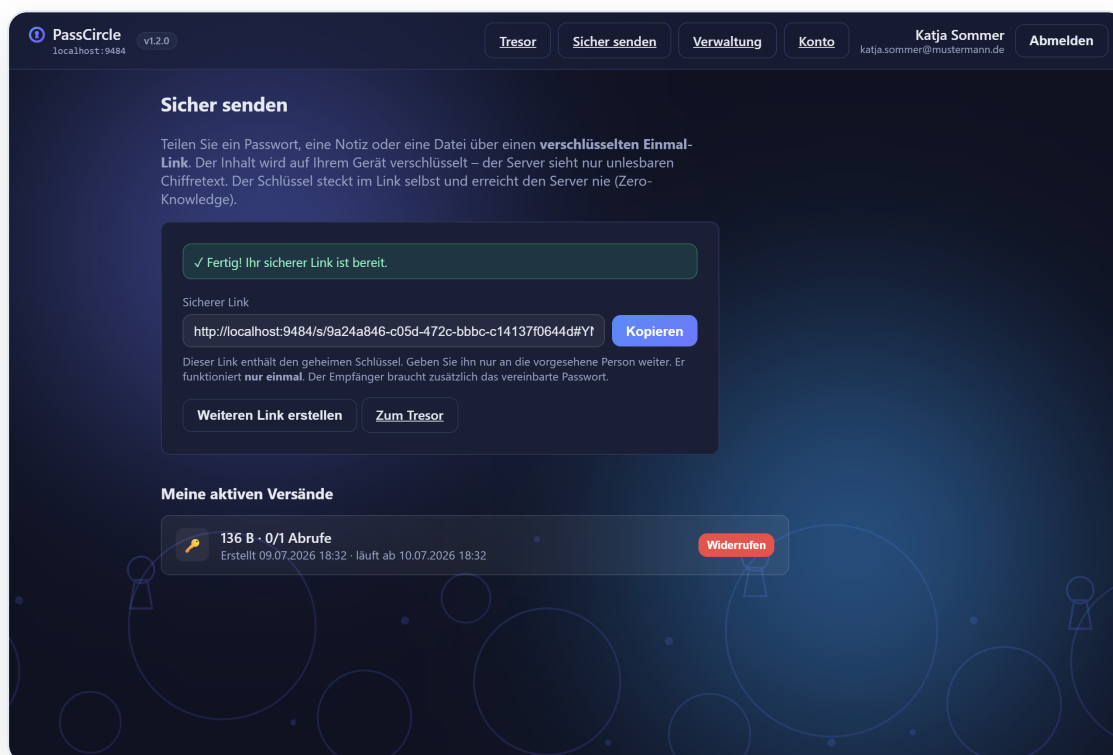
Einträge und Ordner werden **nie sofort endgültig gelöscht**: Beim Löschen fragt PassCircle nach einem **Grund** (Pflichtfeld) und verschiebt den Eintrag in den  **Papierkorb** im Ordner-Baum. Von dort lässt er sich jederzeit **wiederherstellen** – erst nach Ablauf der Aufbewahrungsfrist (Standard 90 Tage) wird er automatisch endgültig entfernt.

- Beim Löschen eines **Ordners** wandert der gesamte Inhalt mit einem gemeinsamen Grund in den Papierkorb; beim Wiederherstellen kommt die Ordnerstruktur unverändert zurück.
- Der Papierkorb zeigt zu jedem Eintrag **Grund, Löschdatum und verbleibende Tage** bis zur endgültigen Löschung. Der Grund ist – wie alle Inhalte – Zero-Knowledge verschlüsselt.
- **Endgültig löschen** (einzeln oder „Papierkorb leeren“) ist jederzeit möglich; das kann nicht rückgängig gemacht werden.
- In **Abteilungen** zeigt der Papierkorb zusätzlich, **wer** einen Eintrag gelöscht hat. Nur-Lese-Mitglieder können weder löschen noch wiederherstellen.

5 Sicher senden (verschlüsselte Einmal-Links)

Mit **Sicher senden** (oben in der Leiste) teilen Sie ein Passwort, eine Notiz oder eine Datei mit Externen – über einen Link, der **zeitlich befristet** ist und/oder sich nach einer begrenzten Zahl von Abrufen **selbst löscht**. Der Inhalt wird auf Ihrem Gerät verschlüsselt; der Server speichert nur unlesbaren Chiffretext. Der Schlüssel steckt im Link (hinter dem #): Wenn Sie den Link **selbst kopieren und weitergeben**, erreicht er den Server nie.

- 1 **Inhalt wählen:** „Text / Passwort“ oder „Datei“.
- 2 **Passwort-Schutz:** ein zusätzliches Passwort, das der Empfänger braucht. Teilen Sie es **getrennt vom Link** mit (z. B. telefonisch). Für den E-Mail-Versand aus PassCircle ist es **Pflicht**.
- 3 **Gültigkeit & Abrufe:** z. B. „1 Tag“ und „1× (danach gelöscht)“.
- 4 **Sicheren Link erzeugen** → Link kopieren und weitergeben, oder – falls E-Mail eingerichtet und ein Passwort gesetzt ist – direkt aus PassCircle versenden.



„Sicher senden“: der fertige verschlüsselte Link samt Übersicht „Meine aktiven Versände“ mit Widerruf.



Warum beim E-Mail-Versand ein Passwort Pflicht ist: Der Link enthält den Schlüssel. Verschickt PassCircle ihn per E-Mail, liegt er anschließend im Postfach des Empfängers – ohne zusätzliches Passwort könnte dort jeder den Inhalt öffnen. Mit Passwort ist der Link allein wertlos: Zum Entschlüsseln werden *beide* Teile gebraucht, und das Passwort geht auf einem anderen Weg (Telefon, SMS, Messenger) an den Empfänger. **Das Passwort niemals per E-Mail mitschicken.**

Der Empfänger öffnet den Link im Browser (ohne PassCircle-Konto), gibt bei Bedarf das Passwort ein und klickt **Inhalt anzeigen**. Bei Einmal-Links ist der Inhalt danach gelöscht. Unter „Meine aktiven Versände“ sehen Sie Ihre laufenden Links und können sie jederzeit **widerrufen**.



Ein falsches Passwort wird bereits auf dem Gerät des Empfängers erkannt und verbraucht keinen Abruf. Die Grenzen (maximale Größe, maximale Gültigkeit, an/aus) legt Ihr Administrator fest.

Anzeigename ändern

Konto & Sicherheit → **Profil** : Hier legen Sie Ihren **Anzeigenamen** fest oder ändern ihn. Er erscheint oben rechts in der Leiste statt der E-Mail-Adresse.

Master-Passwort ändern

Konto & Sicherheit → **Passwort ändern** : aktuelles Passwort, neues Passwort (zweimal). Ihr gesamter Tresor bleibt erhalten – intern wird nur der Schlüssel neu verpackt.

„Konto & Sicherheit“: Anzeigename, Master-Passwort ändern und 2FA einrichten.



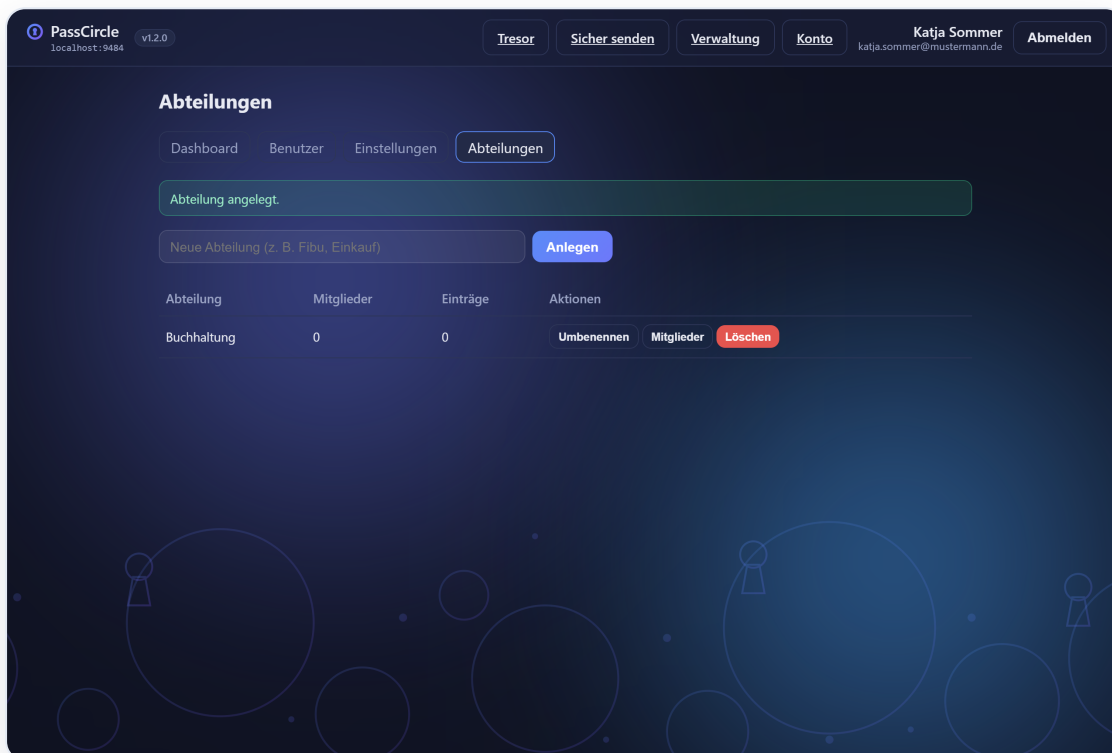
Achtung: Ein Wechsel des Master-Passworts hebt eine eingerichtete automatische Anmeldung (Windows-Entsperrung, Kapitel 11) auf **allen** Geräten auf – sie muss danach neu aktiviert werden.

7 Abteilungen (geteilte Bereiche)

Abteilungen sind gemeinsame Tresore für Teams. Ein Administrator legt sie an und weist Mitglieder zu. Je Mitglied gibt es **Schreib-** oder **Nur-Lese-Recht**. Auch Abteilungen unterstützen Ordner und Anhänge. Sie erscheinen oben als eigene Reiter neben „Mein Tresor“.



Damit ein Administrator Sie einer Abteilung zuweisen kann, müssen Sie sich **einmal angemeldet** haben (dabei wird Ihr persönlicher Schlüssel erstellt).



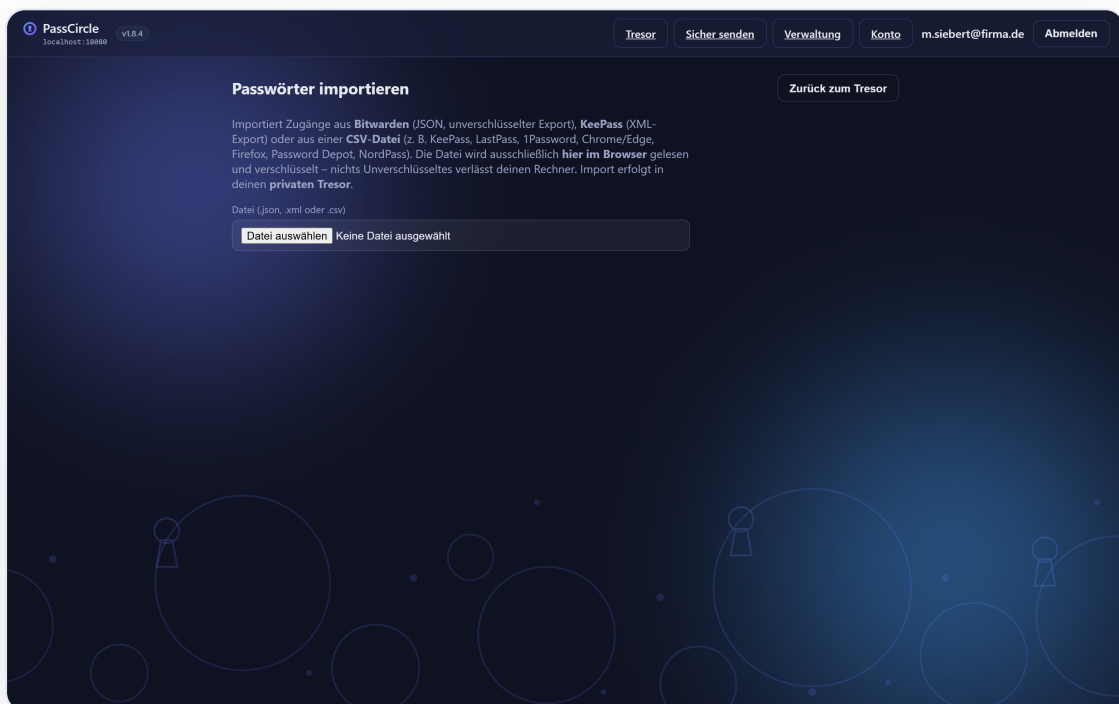
Admin-Ansicht: Abteilungen anlegen und Mitglieder mit Lese-/Schreibrecht zuweisen.

Daten importieren

In „Mein Tresor“ → **Importieren**. Unterstützt werden:

- **Bitwarden:** unverschlüsselter *JSON*-Export – inklusive Ordner (auch verschachtelt).
- **KeePass:** XML-Export – inklusive Ordnerstruktur und, falls vorhanden, Authenticator-Schlüssel (TOTP).
- **CSV** aus LastPass, Chrome, Password Depot und anderen – die Spalten werden automatisch erkannt.

Zielordner ist wählbar, die Ordnerstruktur wird übernommen. Alles läuft im Browser (Zero-Knowledge).



Import: Datei wählen, Zielordner festlegen, Ordnerstruktur übernehmen.

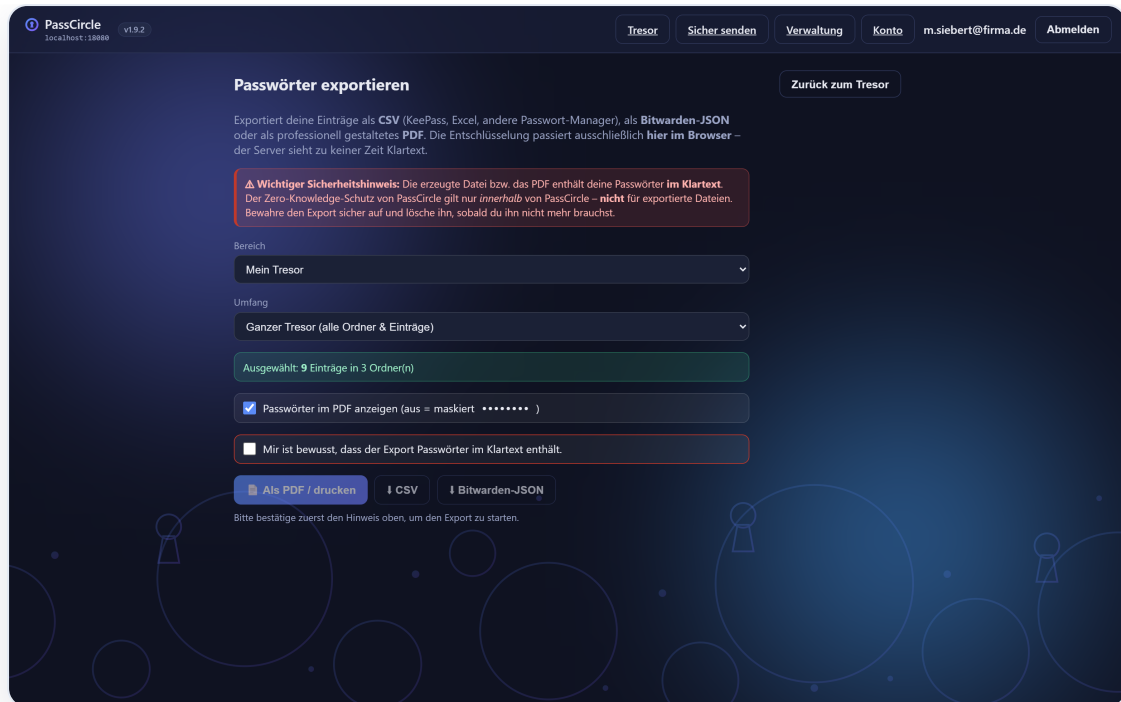


Die Export-Datei Ihres alten Programms enthält Klartext-Passwörter. Nach dem Import bitte **sicher löschen**.

Bitwarden-Export erstellen: Bitwarden → Tools → Tresor exportieren → Format „json“ (unverschlüsselt).

Daten exportieren

Umgekehrt können Sie Ihren Tresor auch **exportieren** – z. B. für ein Backup oder den Umzug in ein anderes Programm. Zur Wahl stehen **CSV**, **Bitwarden-kompatibles JSON** und ein sauber gestaltetes, druckfertiges **PDF**. Sie können „Mein Tresor“ und einzelne Abteilungen getrennt exportieren.



Export als CSV, Bitwarden-JSON oder gestaltetes PDF – jeweils mit klarem Sicherheitshinweis.



Eine Export-Datei enthält Ihre Passwörter **im Klartext**. Bewahren Sie sie nur kurz und sicher auf und löschen Sie sie danach zuverlässig.

Die Erweiterung schlägt auf Anmeldeseiten passende Zugänge vor, füllt Benutzernamen und Passwort aus und speichert neue Zugänge direkt in Ihren Tresor.

Installieren

- **Automatisch:** In vielen Firmen richtet die IT die Erweiterung zentral ein – dann ist sie nach dem nächsten Browser-Start einfach da, ohne dass Sie etwas tun müssen.
- **Manuell (Chrome/Edge):** `chrome://extensions` → Entwicklermodus → „Entpackte Erweiterung laden“ → Ordner `browser-extension` wählen.
- **Firefox:** `about:debugging` → „Temporäre Erweiterung laden“ → `manifest.json`.

macOS: Chrome und Edge installieren die Erweiterung automatisch über ein Konfigurationsprofil vom Server (per Doppelklick bestätigen oder per MDM verteilen). Safari wird derzeit noch nicht unterstützt.

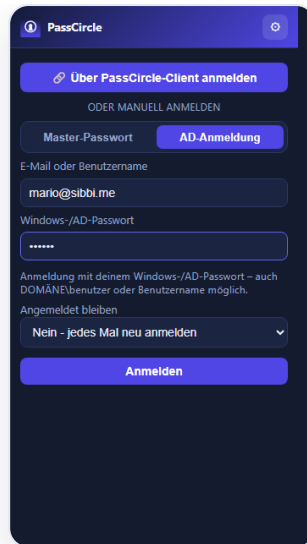
Anmeldung über den PassCircle-Client (bequem)

Ist der **Windows-Client** installiert und angemeldet, erkennt die Erweiterung das automatisch: Sie ist **ohne eigene Anmeldung** sofort einsatzbereit. Server-Adresse und Sitzung übernimmt sie vom laufenden Client. Im Tresor-Fenster steht dann „ Angemeldet über den PassCircle-Client“.

Eigenes Anmeldefenster – auch ohne laufenden Client (neu in 1.9.0)

Neu: Die Erweiterung kann sich jetzt **auch ganz ohne laufenden Windows-Client anmelden**. Sie brauchen also weder den Client noch ein geöffnetes Browserfenster mit PassCircle – ein Klick auf das PassCircle-Symbol öffnet ein eigenes, kleines Anmeldefenster:

- Beim **ersten Mal** geben Sie Server-Adresse (über das **Zahnrad**) sowie E-Mail bzw. Benutzernamen und Master-Passwort ein. Beides – Server und E-Mail/Benutzername – wird **gemerkt**.
- Danach genügt beim Anmelden nur noch das **Master-Passwort**.
- Ein **Umschalter „Master-Passwort“ / „AD-Anmeldung“** erlaubt die Anmeldung mit dem Windows-/AD-Passwort – die zweite Option erscheint nur, wenn Ihr Server sie anbietet.
- Mit **Angemeldet bleiben** bleibt die Erweiterung für die von Ihrer IT erlaubte Dauer entsperrt.



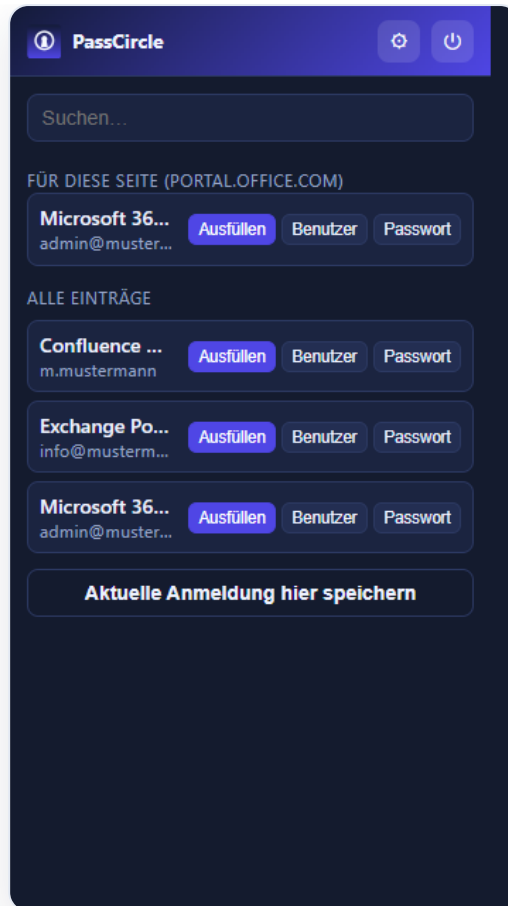
Das eigene Anmeldefenster der Erweiterung: gemerkte E-Mail, danach nur noch das Master-Passwort, Umschalter für die AD-Anmeldung.

Automatisches Ausfüllen

- Auf Seiten mit gespeicherten Zugängen erscheint das **PassCircle-Symbol im Eingabefeld** – ein Klick zeigt alle passenden Zugänge; die Auswahl füllt Benutzername und Passwort.
- Der Vorschlag erscheint auch automatisch, sobald Sie ins Feld klicken.

Neue Zugänge speichern

Melden Sie sich mit einem neuen Zugang an, fragt PassCircle „In PassCircle speichern?“ – mit Ordner-Auswahl. Neue Einträge landen in „Mein Tresor“.



Die Browser-Erweiterung mit Vorschlägen „Für diese Seite“ und der Gesamtliste aller Einträge.

Hinweis: Der Server muss erreichbar sein und sein Zertifikat dem Browser vertraut werden. Abteilungs-Zugänge werden angezeigt und ausgefüllt.

10 Passkeys

Passkeys sind der moderne, passwortlose Nachfolger des klassischen Logins: Statt eines Passworts bestätigen Sie die Anmeldung mit einem geheimen Schlüssel, der niemals die Website erreicht – das macht Phishing praktisch unmöglich. PassCircle kann über die **Browser-Erweiterung** Passkeys **speichern** und zum **Anmelden** verwenden – Zero-Knowledge verschlüsselt in Ihrem Tresor.

- 1 Wählen Sie auf einer Website **Passkey einrichten** (oft „Mit Passkey anmelden" oder „Passwortlos anmelden").
- 2 PassCircle bietet an, den Passkey zu **speichern** – bestätigen Sie das. Der Passkey wird verschlüsselt in Ihrem Tresor abgelegt.
- 3 Beim nächsten Login meldet PassCircle Sie **per Klick** an – kein Passwort mehr nötig.

Gespeicherte Passkeys erscheinen als ganz normale **Einträge im Tresor**, gekennzeichnet mit  **Passkey**. So haben Sie Passwörter und Passkeys an einem Ort und auf jedem Ihrer Geräte, an denen PassCircle angemeldet ist.

i Gut zu wissen: Passkeys funktionieren in **Chrome und Edge**; in **Firefox** ist die Unterstützung eingeschränkt. Ist PassCircle gerade **gesperrt oder nicht angemeldet**, übernimmt automatisch die native Passkey-Verwaltung Ihres Betriebssystems bzw. Browsers – Sie bleiben also immer handlungsfähig.

- **Windows-Client:** eigenständige App, die PassCircle in einem eigenen Fenster öffnet. URL-Links öffnen im Standard-Browser.
- **Mac:** PassCircle steht als **nativer Mac-Client** bereit. Alternativ lässt es sich als App aus dem Browser installieren: in *Safari* die Adresse öffnen → Menü *Ablage* → *Zum Dock hinzufügen*; in *Chrome/Edge* → Menü → *Installieren*. Danach läuft PassCircle als eigene App mit Icon im Dock.
- **Smartphone:** Adresse im Browser öffnen und „Zum Home-Bildschirm hinzufügen“. Der Zugriff von unterwegs läuft in der Regel über ein VPN.

Versionsanzeige & automatische Update-Meldung (Windows-Client)

Oben in der Leiste steht neben „PassCircle“ stets die **aktuell verwendete Version** (z. B. **v1.9.0**) – so erkennen Sie sofort, welche Version läuft. Stellt Ihr Administrator eine neuere Client-Version bereit, erscheint nach der Anmeldung der Hinweis **„Neue Version verfügbar“**, und die Versionsanzeige wird farbig hervorgehoben. Ein Klick lädt das passende Setup direkt vom Server herunter und startet die Installation. Im normalen Browser erscheint der Update-Hinweis nicht – dort ist die Anwendung immer aktuell.

Windows-Entsperrung (automatische Anmeldung)

Im Windows-Client können Sie sich künftig **automatisch mit Ihrem angemeldeten Windows-Benutzer** anmelden – ohne jedes Mal das Master-Passwort einzugeben. So aktivieren Sie es:

- 1 Einmal normal mit Master-Passwort anmelden.
- 2 **Konto & Sicherheit** → Abschnitt **„Windows-Entsperrung (dieser PC)“**.
- 3 Optional **„mit Windows Hello bestätigen“** anhaken (PIN, Fingerabdruck oder Gesicht) → **Auf diesem PC aktivieren**.

Ab dem nächsten Start meldet der Client Sie automatisch an. Technisch wird Ihr Tresor-Schlüssel dabei **lokal per Windows-DPAPI** an Ihren Windows-Benutzer gebunden gespeichert – er verlässt den PC nie und der Server sieht ihn weiterhin nicht (Zero-Knowledge bleibt).



Abmelden setzt die automatische Anmeldung nur bis zum nächsten Programmstart aus. Zum dauerhaften Aufheben **Auf diesem PC deaktivieren** wählen. Diese Funktion gibt es nur im Windows-Client, nicht im Browser.



Sicherheitshinweis: Wer Zugriff auf Ihre *angemeldete* Windows-Sitzung hat, kann den Tresor öffnen – mit Windows Hello ist eine zusätzliche Bestätigung nötig. Ein Wechsel des Master-Passworts hebt die Windows-Entsperrung auf **allen** Geräten auf; sie muss dann neu aktiviert werden.