



PassCircle

ADMINISTRATOR-HANDBUCH

PassCircle betreiben & verwalten

Installation, Benutzerverwaltung, Active Directory, Sicherung und Betrieb – der komplette Leitfaden für IT und Administration des selbst gehosteten PassCircle-Servers.

Version 1.9.2 · Stand Juli 2026 · © MARIOSIEBERT-IT
Für IT und Betrieb · Fragen: info@mariosiebert-it.de

Installation

Active Directory & SSO

Datensicherung

Zertifikate & HTTPS

Branding & Lizenz

Inhalt

Die Kapitel folgen fortlaufend – von der Architektur über Installation und Benutzerverwaltung bis zu Sicherung, Branding und Fehlerbehebung.

- | | | | |
|----------|--|-----------|-------------------------------|
| 1 | Architektur & Sicherheit im Überblick | 8 | Abteilungen verwalten |
| 2 | Server installieren | 9 | Active Directory anbinden |
| 3 | HTTPS-Zertifikat & Vertrauen | 10 | E-Mail (SMTP) & Einstellungen |
| 4 | Windows-Client verteilen & aktualisieren | 11 | Datensicherung & System-Info |
| 5 | Browser-Erweiterung verteilen | 12 | Branding (Personalisierung) |
| 6 | Benutzer verwalten (Freigabe) | 13 | Editionen, Lizenz & Staffeln |
| 7 | Passwort-Wiederherstellung | 14 | Härtung & Empfehlungen |
| | | 15 | Fehlerbehebung |

1 Architektur & Sicherheit im Überblick

PassCircle ist ein selbst gehosteter, quelloffen betreibbarer Passwort-Tresor nach dem **Zero-Knowledge-Prinzip**. Alle Inhalte werden auf dem Gerät des Nutzers ver- und entschlüsselt; der Server speichert und überträgt ausschließlich Chiffretext.

- **Server:** .NET 8, läuft als Windows-Dienst „PassCircle“. Datenbank ist SQLite unter `%PROGRAMDATA%\PassCircle\passwordsafe.db`. HTTPS ist Standard.
- **Clients:** Web-Client (Blazor WebAssembly), Windows-Client (WebView2), nativer macOS-Client sowie die Browser-Erweiterung für Chrome, Edge und Firefox.
- **Zero-Knowledge:** Schlüsselableitung PBKDF2-SHA256 (600.000 Iterationen), Inhalte AES-256-GCM. Geteilte Bereiche (Abteilungen) werden über ein **RSA-Schlüsselpaar je Nutzer** abgesichert. Der Server sieht nur Ciphertext.
- **Anmeldung:** JWT (Bearer-Token); Rate-Limit gegen Brute-Force; Sicherheits-Header und CSP.

Verschlüsselung „at rest“ (serverseitig)

Zusätzlich zum Zero-Knowledge-Prinzip liegen auch die wenigen serverseitig benötigten Geheimnisse verschlüsselt auf dem Datenträger: die **2FA-Geheimnisse** (TOTP-Secrets) und der **JWT-Signierschlüssel** werden per Windows-**DPAPI/DataProtection** geschützt.

 **Maschinengebunden:** Diese At-Rest-Schlüssel sind an den jeweiligen Rechner gebunden und liegen im Ordner `%ProgramData%\PassCircle`. Bei einem **Rechnerumzug** muss dieser Ordner vollständig mit umziehen – siehe Kapitel 11.

 **Wichtig:** Sichern Sie bei Umzug oder Wiederherstellung nicht nur die Datenbank, sondern das **gesamte Verzeichnis** `%ProgramData%\PassCircle`. Fehlen die DPAPI-Schlüssel, lassen sich 2FA-Geheimnisse und Token-Signierung auf dem neuen Rechner nicht mehr entschlüsseln.

Passkeys

 **Kein Admin-Eingriff nötig:** Passkeys werden pro Benutzer **Zero-Knowledge im Tresor** gespeichert. Es ist keine Server-Konfiguration erforderlich – Nutzer richten sie selbst im Client ein.

2 Server installieren

Voraussetzungen: Windows (x64) mit Administratorrechten für die Installation. Die „Microsoft Edge WebView2 Runtime“ wird nur für den Windows-Client benötigt, nicht für den Server.

- 1 `PassCircle-Server-Setup.exe` ausführen.
- 2 **Port** wählen (Standard 8443; anpassbar, falls belegt).
- 3 Das Setup richtet den Dienst ein, öffnet die **Firewall** für den Port und startet den Dienst.
- 4 Aufruf testen: `https://<server>:<port>/api/health` muss **ok** liefern.



Updates spielen Sie einfach durch Ausführen des neuen Setups ein: Der Dienst wird gestoppt, die Dateien werden ersetzt und das Datenbank-Schema automatisch migriert (kein Datenverlust). Der gewählte Port bleibt in `%PROGRAMDATA%\PassCircle\config.json` erhalten.

3 HTTPS-Zertifikat & Vertrauen

Beim ersten Start richtet der Server eine **eigene Zertifizierungsstelle** ein und stellt sich damit sein TLS-Zertifikat aus. Beides liegt unter `%PROGRAMDATA%\PassCircle\`:

- `ca.pfx` – die **Wurzel** („PassCircle Root CA“, 20 Jahre gültig). Ihr vertrauen die Clients **einmalig**.
- `cert.pfx` – das **Server-Zertifikat** (397 Tage gültig), ausgestellt von der Wurzel. Es enthält alle lokalen IP-Adressen, den Rechnernamen und `localhost`.

Der Server erneuert das Server-Zertifikat automatisch, sobald es sich dem Ablauf nähert (30 Tage vorher) oder sich Namen/IPs geändert haben. **Die Wurzel bleibt dabei unverändert** – die Clients merken von der Erneuerung nichts.



Warum diese Zweiteilung? Browser lehnen Server-Zertifikate mit mehr als **398 Tagen** Laufzeit grundsätzlich ab (Fehler `ERR_CERT_VALIDITY_TOO_LONG`, nicht wegklickbar). Das Server-Zertifikat muss deshalb kurz sein und regelmäßig erneuert werden. Diese Grenze gilt nicht für die Wurzel – deshalb wird nur ihr vertraut, und zwar einmal für 20 Jahre.

Zertifikat auf Clients vertrauen

Damit Browser und Client keine Warnung zeigen, muss die Wurzel als vertrauenswürdig hinterlegt werden:

- **Werkzeug:** `PassCircle-Zertifikat-vertrauen.cmd` (im Client-Ordner bzw. im Startmenü als `PassCircle – Zertifikat vertrauen`) – Server-Adresse/IP eingeben, fertig. Pro PC in der Regel **nur einmal** nötig.
- Der **Client-Installer** versucht dies automatisch.



Beim Update von einer Version vor 1.7.5 stellt der Server einmalig auf die neue Wurzel um (die alten Zertifikate waren 5 Jahre gültig und wurden von Browsern abgelehnt). Danach zeigen bereits eingerichtete Clients zunächst eine Zertifikatswarnung – auf jedem Client einmal „Zertifikat vertrauen“ ausführen, dann ist dauerhaft Ruhe.



Für den sauberen Produktivbetrieb ist alternativ ein Zertifikat einer **internen CA** oder ein offizielles Zertifikat möglich (Pfad in `appsettings.Production.json` hinterlegbar) – dann entfällt das manuelle Vertrauen ganz.

4 Windows-Client verteilen & aktualisieren

- 1 `PassCircle-Client-Setup-<Version>.exe` ausführen; die Server-URL kann vorbelegt werden (`/SERVERURL="https://server:8443"` für stille Installation).
- 2 Der Client speichert die URL unter `%LOCALAPPDATA%\PassCircle\server.url`.
- 3 Benötigt die **WebView2 Runtime** (auf aktuellen Windows meist vorhanden).



Server umgezogen oder Adresse geändert? Der Client prüft beim Start, welche der hinterlegten Adressen erreichbar ist, und nutzt diese automatisch. Ist kein Server erreichbar, erscheint eine Hinweisseite mit **Server-Adresse ändern**. Die Adresse lässt sich außerdem jederzeit mit der Taste **F2** ändern.

Automatische Updates verteilen (Update-Ordner)

Jede Client-Version trägt eine **Build-Nummer**. Im Normalfall müssen Sie nichts tun: Das Server-Setup (Vollversion) bringt das passende Client-Setup mit und legt es bei jedem Server-Update automatisch in den Update-Ordner. Sobald der Server aktualisiert ist, erscheint bei allen Clients mit älterer Version oben **Neue Version verfügbar** – ein Klick lädt und installiert das Update.

Manuell (nur für Zwischen-Updates ohne Server-Update): Das Client-Setup in den Ordner `%PROGRAMDATA%\PassCircle\Update` auf dem Server legen. Der Ordner wird automatisch angelegt; sein Pfad steht auch in der Verwaltung unter *Einstellungen* → *System* → *Client-Update-Ordner* (mit Kopier-Knopf).



Die neueste Version wird **automatisch anhand der höchsten Nummer im Dateinamen** erkannt – alte Setups stören nicht. Optional können Sie eine Datei `notes.txt` daneben legen; ihr Text erscheint als kurze Info in der Meldung.



Der Update-Ordner liegt im gemeinsamen Datenverzeichnis des Servers. Legen Sie dort ausschließlich **geprüfte PassCircle-Setups** ab.

Server-Updates (nur Hinweis – kein automatischer Download)

PassCircle kann Sie – **nur wenn Sie es aktiv einschalten (Standard: aus)** – auf neue **Server-Versionen** aufmerksam machen. Unter *Verwaltung* → *Einstellungen* → *Allgemein* aktivieren Sie „Automatisch nach Server-Updates suchen“. Der Server prüft dann etwa täglich – nur bei Internetverbindung – auf `passcircle.de`, ob eine neuere Version vorliegt. Es wird lediglich eine öffentliche Datei gelesen; es werden **keine Daten übertragen**.



Es wird nichts automatisch installiert. Ein Server-Update führen Sie bewusst selbst durch: das neue Server-Setup herunterladen und ausführen. **Vorher unbedingt eine Sicherung erstellen** (Reiter *Sicherung*).

Automatisch über den Client-Installer (empfohlen). Das Client-Setup bietet die Option „PassCircle-Browser-Addin automatisch in Chrome und Edge einrichten“ (standardmäßig aktiv). Ist sie gewählt, wird die Erweiterung beim nächsten Start von Chrome/Edge **ohne Zutun der Nutzer** installiert (Enterprise-Richtlinie „force-install“) und lässt sich nicht versehentlich entfernen. Gehostet wird sie vom PassCircle-Server selbst unter `/ext/` – kein Web Store, keine Google-/Microsoft-Konten nötig.

- **Voraussetzung:** Das Server-Zertifikat muss dem PC vertraut sein (erledigt das Client-Setup), damit der Browser die Erweiterung über HTTPS laden kann.
- **Native-Messaging:** Das Setup registriert zusätzlich einen kleinen „Native Host“. Über ihn holt die Erweiterung die Sitzung vom laufenden, entsperrten Windows-Client – dadurch Anmeldung ohne zweiten Login. Schlüssel verlassen den Rechner nicht (Zero-Knowledge bleibt gewahrt).
- **Firefox:** Wird über diese Automatik derzeit nicht abgedeckt – dort die Erweiterung manuell laden (siehe Bedienerhandbuch).

 **AD-Benutzer in der Erweiterung anmelden:** Damit sich AD-Benutzer **direkt in der Browser-Erweiterung** anmelden können, muss die Active-Directory-Anbindung im Modus `AD-Passwort (Single Sign-on)` laufen (siehe Kapitel 9). Bei „Eigenes Master-Passwort“ melden sich Nutzer wie gewohnt mit E-Mail und Master-Passwort an.

 **Erweiterung erscheint nicht?** Chrome/Edge installiert sie nur, wenn *drei* Dinge stimmen: Force-Install-Richtlinie gesetzt, Server erreichbar und sein Zertifikat vertraut. Das Client-Setup legt dafür das Werkzeug `PassCircle – Add-in prüfen` (Startmenü) an: Es testet genau diese drei Punkte und nennt den nächsten Schritt. Nach jeder Änderung den Browser **komplett neu starten**.

6 Benutzer verwalten (Freigabe)

Verwaltung → **Benutzer**.

- **Freigabe:** Selbst registrierte Konten erscheinen als „Wartet auf Freigabe“. Sie erhalten (bei aktivem E-Mail-Versand) eine Benachrichtigung und geben mit **Genehmigen** frei bzw. **Ablehnen** (löscht das Konto). Erst danach ist die Anmeldung möglich.
- **Benutzer anlegen:** direkt mit Initial-Passwort; Abteilungen können sofort zugewiesen werden.
- **Rollen/Status:** Aktiv/Deaktiviert, Admin ja/nein (der letzte Admin ist geschützt).
- **2FA zurücksetzen** pro Benutzer möglich.

E-Mail	Name	Status	Admin	Einträge	Aktionen
anna.admin@firma.local	Anna Admin	Aktiv AD	Nein	0	Deaktivieren Admin machen Löschen
bernd.berg@firma.local	Bernd Berg	Aktiv AD	Nein	0	Deaktivieren Admin machen Löschen
clara.chef@firma.local	Clara Chef	Aktiv AD	Nein	0	Deaktivieren Admin machen Löschen
dora.dev@firma.local	Dora Dev	Aktiv AD	Nein	0	Deaktivieren Admin machen Löschen
m.siebert@firma.de	—	Aktiv	Ja	12	Deaktivieren Admin entziehen Löschen

Benutzerverwaltung: ausstehende Registrierungen mit „Genehmigen“/„Ablehnen“; AD-Konten sind mit blauem „AD“-Badge gekennzeichnet.

i AD-Konten kenntlich gemacht: Aus dem Active Directory übernommene Benutzer tragen in der Liste ein blaues **AD**-Badge. Für diese Konten ist der **Passwort-Reset gesperrt** – die Anmeldung erfolgt über das Active Directory bzw. das eigene, beim ersten Login gesetzte Master-Passwort.

Der Schalter „Offene Registrierung“ steuert, ob sich Benutzer überhaupt selbst registrieren können. Einen Registrierungscode gibt es nicht mehr – die Freigabe ersetzt ihn.

7 Passwort-Wiederherstellung

Optional aktivierbar (Verwaltung → Benutzer). Dabei wird der Tresor-Schlüssel jedes Nutzers zusätzlich mit einem Admin-Wiederherstellungsschlüssel hinterlegt. Der Administrator kann dann das Passwort eines Nutzers **ohne Datenverlust** zurücksetzen.



Achtung: Damit wird das Admin-Konto zum „Generalschlüssel“. Unbedingt mit 2FA schützen. Bestehende Nutzer werden erst bei ihrer **nächsten Anmeldung** für die Wiederherstellung hinterlegt.

Verwaltung → **Abteilungen**: anlegen, **umbenennen**, löschen; **Mitglieder** hinzufügen/entfernen und je Mitglied **Schreiben** oder **Nur-Lesen** setzen. Der Administrator verwaltet Abteilungen, ohne selbst deren Inhalte sehen zu müssen (Schlüssel-Hinterlegung über die RSA-Schlüsselpaare der Mitglieder).



Ein Benutzer kann einer Abteilung erst zugewiesen werden, nachdem er sich **einmal angemeldet** hat – dabei wird sein persönliches Schlüsselpaar erstellt.

9 Active Directory anbinden

PassCircle kann Benutzer aus dem **Active Directory** übernehmen (Verwaltung → **Active Directory**, nur Firmen-Version). PassCircle liest **ausschließlich** (AD → PassCircle) und legt für neue Benutzer eine **Einladung** an bzw. – bei SSO – direkt ein Konto.

Einrichtung

- 1 **Verbindung:** AD-Server (Host, z. B. `dc01.firma.local`) und Basis-DN (z. B. `DC=firma,DC=local`) eintragen. Bei Bedarf **LDAPS** aktivieren.
- 2 **Anmeldung am AD:** entweder das **Windows-Konto des Servers** (wenn der PassCircle-Server Mitglied der Domäne ist) oder ein **Lese-Dienstkonto** (Benutzer + Passwort; für Server außerhalb der Domäne). Das Dienstkonto-Passwort wird verschlüsselt gespeichert.
- 3 **Verbindung testen** und speichern.
- 4 **OUs laden** und die Organisationseinheiten anhaken, aus denen Benutzer eingelesen werden sollen (mehrere möglich; Unter-OUs sind eingeschlossen).

Selektiver Import – neue Benutzer per Häkchen wählen

Die **Vorschau** zeigt, was der Abgleich tun würde. Neu ist: Sie müssen nicht mehr zwingend *alle* gefundenen Benutzer übernehmen. In der Vorschau werden **neue Benutzer per Häkchen ausgewählt** – mit `Alle wählen` bzw. `Keine wählen` als Schnellauswahl. Nur die **angehakten** neuen Benutzer werden angelegt und per E-Mail benachrichtigt; nicht angehakte bleiben unberührt und können bei einem späteren Abgleich jederzeit nachgezogen werden.

Der Knopf `Jetzt synchronisieren` sitzt **unter der Liste** und führt den Abgleich für genau die getroffene Auswahl aus.

AD-Vorschau: neue Benutzer per Häkchen auswählen („Alle wählen“/„Keine wählen“); nur ausgewählte werden angelegt und benachrichtigt. Der Synchronisieren-Knopf sitzt unter der Liste.

i Einladungs-Mail mit Installations-Link: Die Einladung an einen AD-Benutzer enthält einen **Installations-Link**. Über ihn richtet der Nutzer den Client ein; dieser **konfiguriert sich beim Setup automatisch auf den Server** – die Server-Adresse muss nicht von Hand eingegeben werden.

Anmeldeverfahren der AD-Benutzer

Unter „Anmeldung der AD-Benutzer“ wählen Sie, wie sich die eingelesenen Benutzer anmelden:

- **Eigenes Master-Passwort (Zero-Knowledge, empfohlen):** Benutzer werden eingeladen und legen beim ersten Login ihr eigenes Master-Passwort fest. Der Server sieht nie ein Passwort und kann die Tresore nicht lesen – Zero-Knowledge bleibt vollständig erhalten.
- **AD-Passwort (Single Sign-on):** Konten werden sofort angelegt; die Anmeldung erfolgt mit dem Windows-/AD-Passwort (auf der Anmeldeseite „AD-Anmeldung“ wählen). Als Anmeldename dient der AD-Benutzername (z. B. `bberg` oder `FIRMA\bberg`), der UPN (`bberg@firma.local`) oder die E-Mail. Bequem, aber **für diese Konten ist Zero-Knowledge nicht garantiert** – der Server kann ihre Tresore technisch entschlüsseln (der Tresor-Schlüssel liegt serverseitig verschlüsselt hinterlegt). Lokal angelegte Konten bleiben unberührt (weiterhin Zero-Knowledge).

i Erweiterung & SSO: Nur im Modus „AD-Passwort (Single Sign-on)“ können sich AD-Benutzer direkt in der Browser-Erweiterung anmelden (siehe Kapitel 5).



Wichtig bei SSO – Sicherung & Umzug: Bei SSO liegen die Tresor-Schlüssel der AD-Konten serverseitig verschlüsselt im Ordner `%ProgramData%\PassCircle\dp-keys` (an diesen Rechner gebunden). Sichern Sie deshalb das **gesamte Verzeichnis** `%ProgramData%\PassCircle` (Datenbank und `dp-keys`). Ein Umzug auf einen **anderen Rechner** erfordert eine **Neu-Provisionierung der SSO-Konten**. Bei rein lokalen Konten (eigenes Master-Passwort) besteht diese Einschränkung nicht.

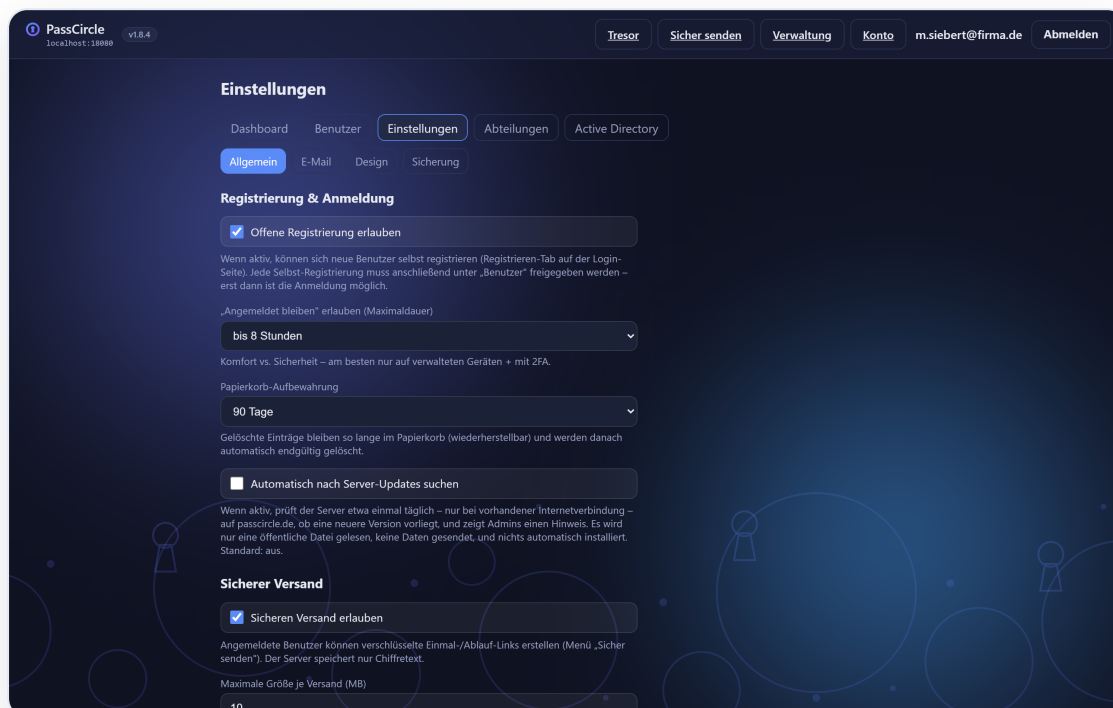
Was der Abgleich macht

- **Neue, ausgewählte** aktive AD-Benutzer (mit E-Mail) → je nach Verfahren Einladung (eigenes Master-Passwort) oder sofort angelegtes Konto (SSO).
- Im AD **deaktivierte** Konten oder Benutzer, die nicht mehr in den gewählten OUs liegen → das zugehörige PassCircle-Konto wird **deaktiviert** (die Tresor-Daten bleiben erhalten).
- **Manuell angelegte** Konten (nicht aus dem AD) werden vom Abgleich nie verändert.



Der Abgleich läuft **manuell** per „Jetzt synchronisieren“. Führen Sie ihn nach Personaländerungen erneut aus und wählen dabei die gewünschten neuen Benutzer aus.

Die Einstellungen sind zur besseren Übersicht in **Reiter** gegliedert: **Allgemein** (Registrierung/Freigabe + System-Infos), **E-Mail**, **Design** (Anmeldemaske & Fußzeile) und **Sicherung**.



Die Verwaltungs-Einstellungen mit ihren Reitern – hier werden Registrierung/Freigabe, E-Mail, Design und Sicherung zentral konfiguriert.

Verwaltung → Einstellungen → **E-Mail**: SMTP-Server, Port, SSL/TLS, Benutzer/Passwort und Absender eintragen. **Test senden** prüft die Konfiguration. E-Mails werden im PassCircle-Design (Logo + Firmenname) verschickt – u. a. Willkommens-, Sicherheits-, Freigabe- und Abteilungs-Benachrichtigungen sowie die AD-Einladung mit Installations-Link (Kapitel 9).

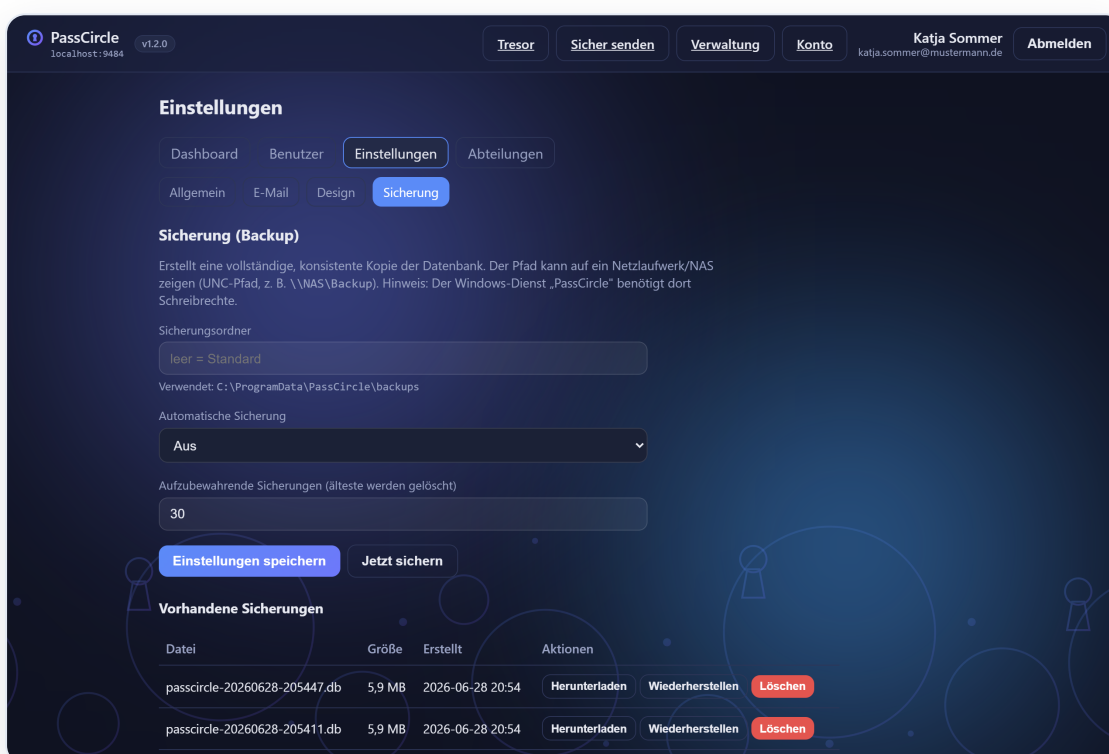


Ohne eingerichtete E-Mail funktionieren die Kernfunktionen weiter; es entfallen lediglich die automatischen Benachrichtigungen (Freigabe-Info, Sicher-senden-Versand per Mail usw.).

11 Datensicherung & System-Info

Verwaltung → Einstellungen → **Sicherung**.

- **Pfad** frei wählbar, auch NAS/Netzlaufwerk als UNC-Pfad (z. B. `\\NAS\Backup`). Der Dienst benötigt dort Schreibrechte.
- **Zeitplan**: stündlich / täglich / wöchentlich zu einer Uhrzeit; **Aufbewahrung** (älteste werden gelöscht).
- **Jetzt sichern**, Liste mit Herunterladen/Löschen.
- **Wiederherstellen / Server-Umzug**: Sicherung (.db) hochladen oder aus der Liste wählen → wird beim nächsten **Dienst-Neustart** eingespielt und ersetzt die aktuelle Datenbank.



Datensicherung: Pfad (auch NAS), Zeitplan, Aufbewahrung und Wiederherstellung.



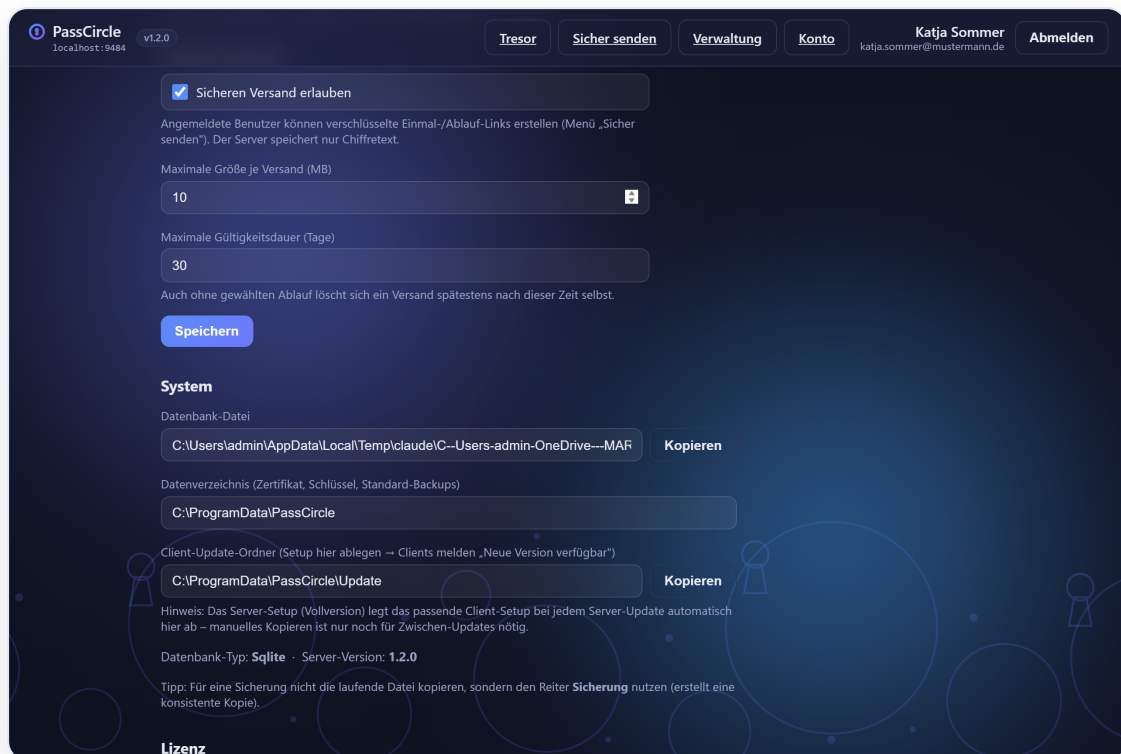
Der Dienst läuft als „LocalSystem“. Für eine NAS-Freigabe braucht dieses Konto Zugriff – **UNC-Pfad statt gemapptem Laufwerk** verwenden.



At-Rest-Schlüssel mitsichern: Die reine `.db`-Sicherung genügt nur für lokale Zero-Knowledge-Konten. Wegen der maschinengebundenen DPAPI-Schlüssel (2FA-Geheimnisse, JWT-Signierung und SSO-Tresorschlüssel, Kapitel 1 & 9) sichern Sie für einen Rechnerumzug das **gesamte Verzeichnis** `%ProgramData%\PassCircle`.

Wo liegt die Datenbank? (System-Info)

Im Reiter **Allgemein** zeigt der Bereich **System** den genauen **Datenbank-Pfad** (per Knopf kopierbar), das Datenverzeichnis, den Datenbank-Typ und die Server-Version. Praktisch für Sicherung, Umzug oder Support.



Reiter „Allgemein“ → „System“: Datenbank-Pfad und Server-Version auf einen Blick.

12 Branding (Personalisierung)

Verwaltung → Einstellungen → **Design** (Anmeldemaske/Fußzeile):

- **Firmenname des Kunden + Kundenlogo** (erscheinen in Leiste und Anmeldeseite; das PassCircle-Logo bleibt als Marke erhalten).
- **Akzentfarbe** (app-weit), Fußzeilen-Text/Autor, Datenschutz-/Homepage-Link.

The screenshot shows the 'Design' settings page in the PassCircle administrator interface. The page has a dark blue theme with white text. At the top, there's a navigation bar with 'PassCircle' logo, version 'v1.2.0', and a user profile 'Katja Sommer' with an 'Abmelden' button. Below the navigation bar, there's a sidebar with 'Einstellungen' and sub-tabs: 'Dashboard', 'Benutzer', 'Einstellungen' (selected), and 'Abteilungen'. Under 'Einstellungen', there are sub-tabs: 'Allgemein', 'E-Mail', 'Design' (selected), and 'Sicherung'. The main content area is titled 'Design – Anmeldemaske & Fußzeile'. It contains several input fields: 'Firmenname des Kunden (Leiste + Anmeldeseite)' with the value 'z. B. Muster GmbH'; 'Fußzeilen-Text / Autor' with the value 'MARIOSIEBERT-IT'; 'Datenschutz-Link (URL)' with the value 'https://.../datenschutz'; 'Homepage-Link (URL)' with the value 'https://mariosiebert-it.de'; 'Akzentfarbe (app-weit)' with a color picker showing '#5b8bf7'; and 'Kunden-Logo – Leiste + Anmeldeseite (max. ~150 KB)' with a file upload button 'Datei auswählen' and the text 'Keine Datei ausgewählt'.

Reiter „Design“: Anmeldemaske, Kundenlogo, Akzentfarbe und Fußzeile anpassen.

So lässt sich PassCircle pro Kunde personalisieren (mandantenfähig gedacht) – ideal auch für IT-Dienstleister mit eigenen Kunden.

PassCircle gibt es in drei Editionen:

Edition	Setup	Umfang
Vollversion	PassCircle-Server-Setup.exe	Für Firmen, Freischaltung per Seriennummer; kompletter Funktionsumfang.
Demo/Test	PassCircle-Server-Setup-Demo.exe	30 Tage voller Umfang; danach Anmeldung gesperrt (Daten bleiben erhalten).
PassCircle Free	PassCircle-Server-Setup-Free.exe	Kostenlos, unbefristet, genau ein Konto, ohne Firmen-Funktionen.

Ein Upgrade von Free/Demo auf die Vollversion ist jederzeit möglich: einfach das normale Server-Setup darüber installieren – alle Daten bleiben erhalten. „PassCircle Free“ richtet sich an **Privatanwender** (ohne Benutzerverwaltung, Abteilungen, Sicherer Versand, E-Mail-Benachrichtigungen, Branding).

Jahreslizenz mit Benutzer-Staffel

Eine Seriennummer schaltet PassCircle für **1 Jahr** frei und enthält die bezahlte **Benutzer-Staffel**: bis **10**, bis **25**, bis **50** Benutzer oder **unbegrenzt** – zusätzlich ist immer **1 Administrator-Konto** frei. Gezählt werden nur aktive, freigegebene Konten; deaktivierte und nicht freigegebene zählen nicht mit.

- Ist die Staffel erschöpft, lassen sich keine weiteren Benutzer registrieren/freigeben/anlegen – eine Seriennummer größerer Staffel hebt das Limit sofort an.
- **Ab 30 Tagen vor Ablauf** erinnert eine Leiste oben an die Verlängerung; der Stand steht unter Verwaltung → Einstellungen → **Lizenz**.
- **Nach Ablauf** ist die Anmeldung gesperrt. Die Anmeldeseite zeigt direkt das Feld „Neue Seriennummer“ – neuen Schlüssel einfügen, ein weiteres Jahr ist freigeschaltet. Firmenname und Daten bleiben erhalten.
- Ältere Seriennummern (vor Version 1.3) ohne Staffel/Laufzeit bleiben unbegrenzt und unbefristet gültig.



Während der Testphase steht oben „Testversion – noch X Tage“. Ein Klick auf den Hinweis führt zur Lizenz-Eingabe.

Für den Betreiber: Der Lizenzschlüssel wird **offline** geprüft (im Server steckt nur ein öffentlicher Prüfschlüssel); Uhr-Rückstellungen erkennt der Server. Gültige Schlüssel erzeugt ausschließlich der Hersteller mit dem privaten Signierschlüssel.

Bereits enthalten: Rate-Limiting der Anmeldung, Sicherheits-Header/CSP, automatisch erzeugter und **at rest verschlüsselter** JWT-Signierschlüssel, verschlüsselte 2FA-Geheimnisse (DPAPI), strenge Token-Prüfung, Zero-Knowledge und Zugriffskontrollen je Abteilung.

Vor dem Einsatz mit echten Kundendaten empfohlen:

- Echtes/internes **CA-Zertifikat** statt selbstsigniert.
- **Zertifikats-PFX-Passwort** vom Standard abändern.
- Optional **Argon2id** als Schlüsselableitung; ein unabhängiger **Penetrationstest**.
- „Angemeldet bleiben“ bewusst steuern (Maximaldauer, nur verwaltete Geräte).
- Admin-Konten mit **2FA** schützen – besonders bei aktiver Passwort-Wiederherstellung (Kapitel 7).
- Regelmäßige **Backups** auf ein separates Ziel (NAS) inkl. des Verzeichnisses `%ProgramData%\PassCircle` + Wiederherstellung testen.

Symptom	Ursache / Lösung
„Ein unerwarteter Fehler ist aufgetreten" / bleibt bei „wird geladen"	Die Seite zeigt „Details:". Häufig: alte Browser-Engine/VM ohne <i>WASM-SIMD</i> (Server updaten). Sonst: Browser aktualisieren, Inkognito ohne Erweiterungen testen (Werbeblocker/AV), Datum/Uhrzeit prüfen.
Zertifikatwarnung „NET::ERR_CERT_..."	Zertifikat auf dem PC vertrauen (Werkzeug „PassCircle – Zertifikat vertrauen"); Server updaten, damit die IP im Zertifikat steht.
2FA „Code ungültig"	Uhrzeit auf Server und Smartphone automatisch/korrekt stellen (<code>w32tm /resync</code>).
Erweiterung: keine Verbindung	Server aktuell (CORS)? Server-Zertifikat im Browser vertraut? Server-Adresse im Zahnrad korrekt?
Erweiterung erscheint gar nicht / „vom Administrator blockiert"	Werkzeug „ PassCircle – Add-in prüfen " (Startmenü) ausführen – prüft Richtlinie, Erreichbarkeit und Zertifikat und nennt den nächsten Schritt. Danach Browser komplett neu starten.
AD-Benutzer kann sich nicht in der Erweiterung anmelden	AD-Anbindung muss im Modus „AD-Passwort (Single Sign-on)" laufen (Kapitel 9). Bei „Eigenes Master-Passwort" mit E-Mail + Master-Passwort anmelden.
Nach Rechnerumzug: 2FA/Token/SSO-Tresore defekt	Es fehlen die maschinengebundenen DPAPI-Schlüssel. Das gesamte Verzeichnis <code>%ProgramData%\PassCircle</code> mitübernehmen; SSO-Konten ggf. neu provisionieren (Kapitel 9/11).
Backup auf NAS schlägt fehl	Der Dienst (LocalSystem) braucht Schreibrechte auf die UNC-Freigabe.