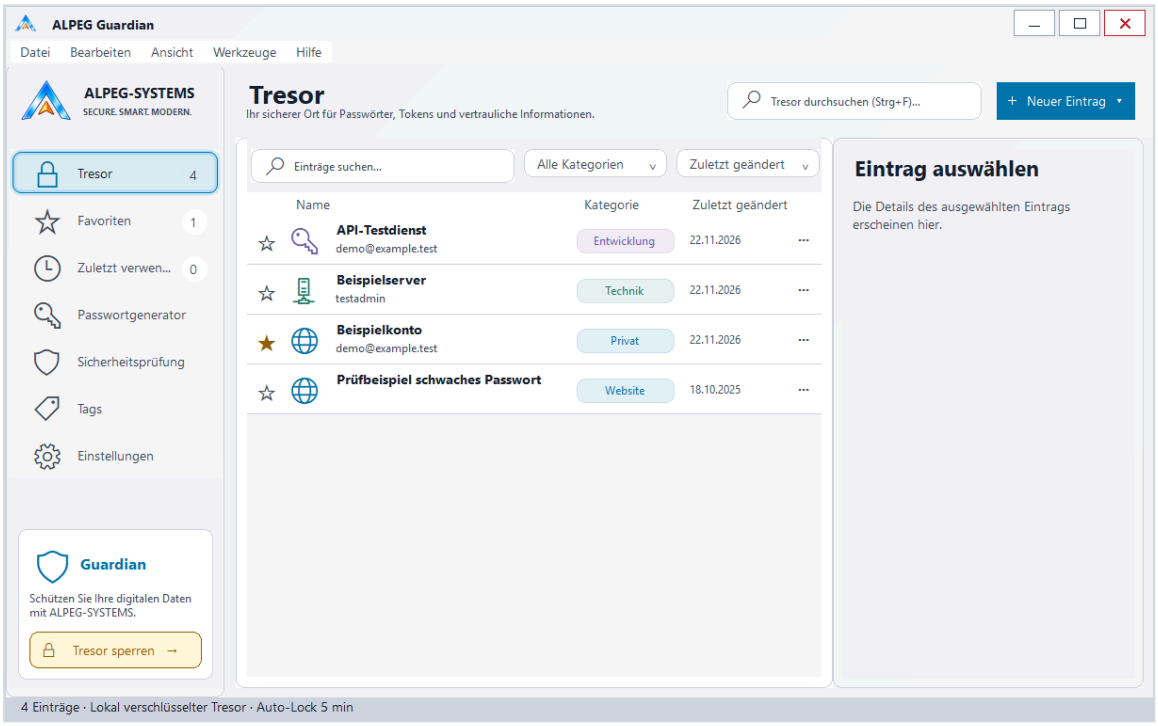
Guardian

Version 1.6.0

Ein lokaler Tresor. Free und Pro.



Ausgabe 1.0 · 22. November 2026
Arbeitsabläufe, Programmaufnahmen und vollständiger Funktionsvergleich
Speichern · Schützen · Verwalten · Wiederherstellen

WEGWEISER

Inhaltsverzeichnis

01 · Willkommen bei Guardian

02 · Installation und erster Start

03 · Oberfläche und Navigation

04 · Free, Pro und Zusatzdienste

05 · Tresor und Eintragstypen

06 · Das Masterpasswort

07 · Verschlüsselung und Schutzgrenzen

08 · Dateien, Speicherort und Sperrdatei

09 · Einen neuen Tresor erstellen

10 · Öffnen, wechseln und vergessen

11 · Sperren, Pausen und Auto-Lock

12 · Einträge erstellen und bearbeiten

13 · Notizen, Kategorien und Tags

14 · Zusatzfelder und Anhänge

15 · Anhänge und ältere Eintragsstände

16 · Suchen, Favoriten und zuletzt verwendet

17 · Details, Quick View und Kontextmenü

18 · Kopieren und Zwischenablage

19 · Passwörter erzeugen

20 · TOTP einrichten und verwenden

21 · Auto-Type und deaktiviertes Browser-Autofill

22 · Lokale Sicherheitsprüfung

23 · Freiwillige Online-Passwortprüfung

24 · Verschlüsselte Backups und Wiederherstellung

> Kapitel sind direkt anklickbar. Free bleibt ohne Konto nutzbar. Einige Pro-Funktionen benötigen zusätzlich einen eingerichteten Dienst.

WEGWEISER

Inhaltsverzeichnis · Fortsetzung

25 · KDBX- und CSV-Export

26 · Masterpasswort ändern

27 · KeePass-Migration

28 · Browserdaten per CSV übernehmen

29 · Weitere Importformate und Konflikte

30 · Importvorschau sicher übernehmen

31 · Batchmigration und Zuordnung (Pro)

32 · Secret Inventory (Pro)

33 · Verwaltungsdaten bearbeiten

34 · Credential Lifecycle und Erinnerungen

35 · Abhängigkeiten dokumentieren

36 · Rotation vorbereiten (Pro)

37 · Rotation prüfen und abschließen

38 · Website-Bereinigung (Pro)

39 · Bereinigung bewusst entscheiden

40 · Leak-Monitoring einrichten (Pro)

41 · Monitoring im Hintergrund

42 · Persönliche Quellen und Abdeckung

43 · Sicherheitszentrale: Status und Integrität

44 · Audit-Nachweise ausgeben

45 · Lokale Pro-Richtlinien

46 · Datenschutz und Übertragungen

47 · Koordinationsdienst und Geräte

48 · Gerätevertrauen und Widerruf

> Kapitel sind direkt anklickbar. Free bleibt ohne Konto nutzbar. Einige Pro-Funktionen benötigen zusätzlich einen eingerichteten Dienst.

WEGWEISER

Inhaltsverzeichnis · Fortsetzung

49 · Arbeitsbereiche und Rollen

50 · Verschlüsselte Einträge freigeben

51 · Notfallkopien und Wartefristen

52 · Empfang und Freigabestatus

53 · Zusätzliche Dienst-Monitoringquelle

54 · Separater Decoy-Tresor (Pro)

55 · Konto und Pro-Lizenz aktivieren

56 · Geräteplätze und Offlinefrist

57 · Konto verloren oder Anmeldung fehlerhaft

58 · Einstellungen und Bedienverhalten

59 · Updates und vollständiges Beenden

60 · Hilfebibliothek und historische Hinweise

61 · Kommandozeile: Voraussetzungen

62 · Kommandozeile: Befehle und Ergebnisse

63 · Tastaturkürzel

64 · Fehler gezielt eingrenzen

65 · Notfallplan für Ihren Tresor

66 · Gute Arbeitsabläufe

67 · Funktionsvergleich · 1

68 · Funktionsvergleich · 2

69 · Funktionsvergleich · 3

70 · Funktionsvergleich · 4

71 · Funktionsvergleich · 5

72 · Funktionsvergleich · 6

> Kapitel sind direkt anklickbar. Free bleibt ohne Konto nutzbar. Einige Pro-Funktionen benötigen zusätzlich einen eingerichteten Dienst.

WEGWEISER

Inhaltsverzeichnis · Fortsetzung

73 · Funktionsvergleich · 7

74 · Funktionsvergleich · 8

75 · Funktionsvergleich · 9

76 · Funktionsvergleich · 10

77 · Funktionsvergleich · 11

78 · Funktionsvergleich · 12

79 · Funktionsvergleich · 13

80 · Begriffe und Kontakt

81 · Lizenzen und Dokumentstand

> Kapitel sind direkt anklickbar. Free bleibt ohne Konto nutzbar. Einige Pro-Funktionen benötigen zusätzlich einen eingerichteten Dienst.

EINSTIEG · KAPITEL 01

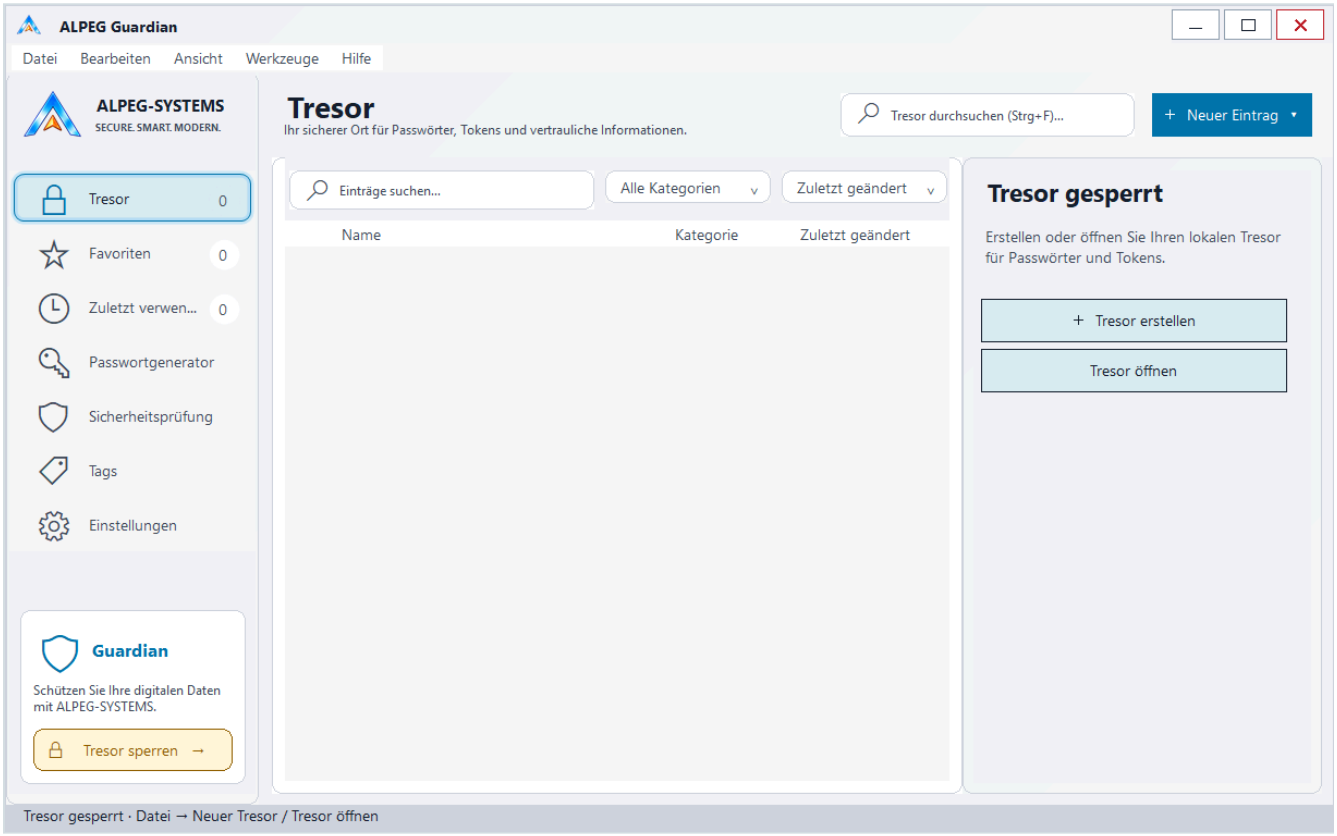
Willkommen bei Guardian

Ihr lokaler Tresor für Logins, API-Schlüssel, Notizen, Server und WLAN.

Dieses Handbuch beschreibt **ALPEG Guardian 1.6.0 für Windows x64**: die ohne Konto nutzbare Free-Basis und zusätzliche Pro-Funktionen in derselben Anwendung.

Arbeitsabläufe, tatsächliche Schutzgrenzen und erforderliche Zusatzdienste sind getrennt erklärt. Das anklickbare Inhaltsverzeichnis führt direkt zum passenden Kapitel.

> **Dokumentausgabe 1.0 · 22. November 2026.** Alle Aufnahmen stammen aus den ausgelieferten 1.6.0-Programmbibliotheken mit einem isolierten Beispieltresor. Konten, Inhalte und Lizenzangaben sind synthetisch. Keine echten Zugangsdaten sind abgebildet.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Installation und erster Start

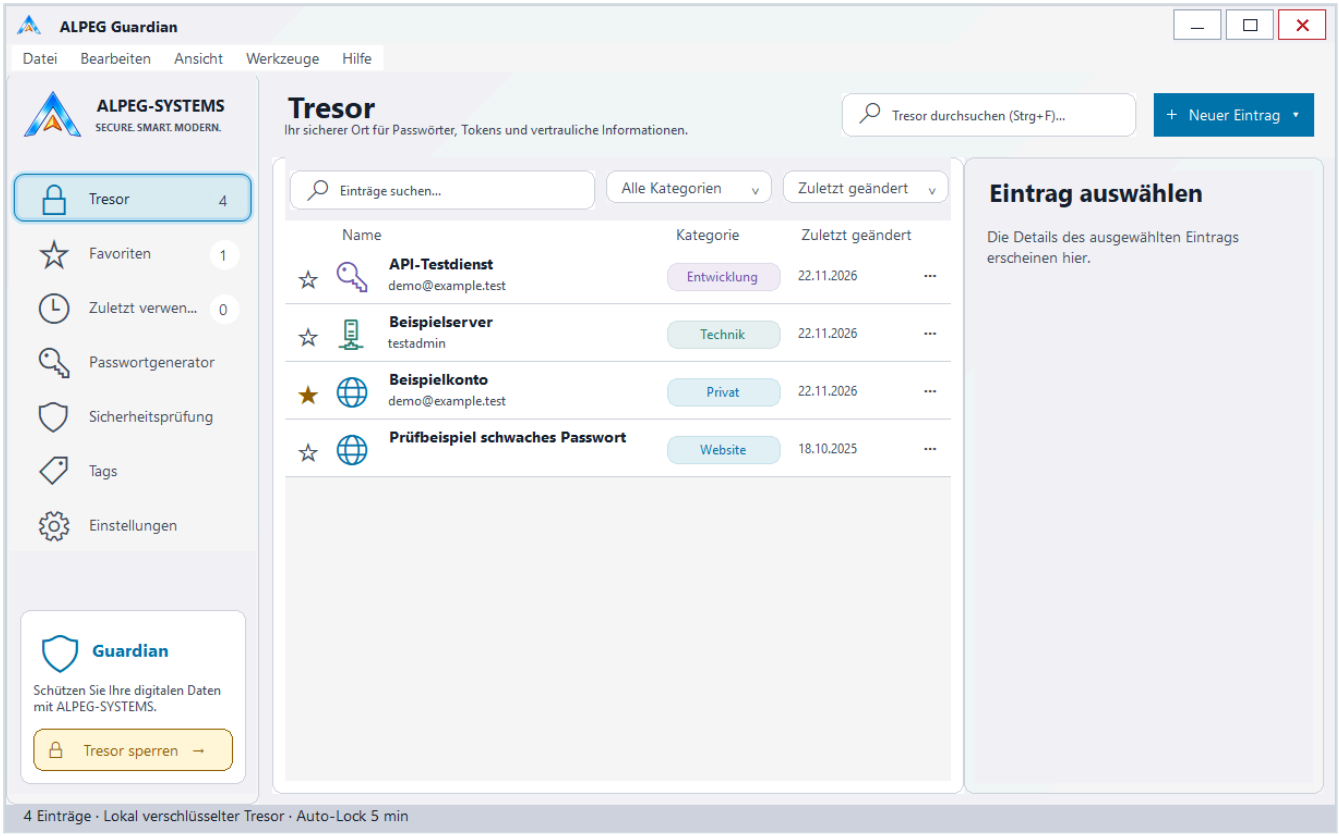
1. Laden Sie den gemeinsamen Guardian-Installer ausschließlich aus dem offiziellen ALPEG-Angebot oder Ihrem persönlichen Downloadlink. Free und Pro benötigen keine getrennten Installationen.
2. Beenden Sie vor einem Upgrade Guardian vollständig über Datei → Beenden und sichern Sie den bisherigen Tresor verschlüsselt.
3. Starten Sie das Windows-x64-Setup und bestätigen Sie Windows-Abfragen selbst. Der Standardordner ist Program Files\ALPEG-SYSTEMS\GuardianPro. Die benötigte Laufzeit wird mitgeliefert.
4. Starten Sie Guardian. Für Free benötigen Sie kein Konto. Legen Sie einen eigenen Tresor an oder öffnen Sie eine vorhandene .agv-Datei.
5. Prüfen Sie nach einem Upgrade Version und Inhalt. Frühere Backups zunächst behalten.

Der Programmordner und Ihr Datenordner sind getrennt. Änderungen an der Installation ersetzen keine Sicherung der Tresordatei und ihres Masterpassworts.

> Bewahren Sie Download und Kennwort nicht als Ersatz für Ihre Tresorsicherung auf. Neue Downloadlinks erzeugen keine neue Lizenz. Persönliche Links: 48 Stunden gültig, nach bewusstem Start 24 Stunden Wiederaufnahme und höchstens eine Übertragung gleichzeitig.

Oberfläche und Navigation

Links: Tresor, Favoriten, zuletzt verwendete Einträge und Werkzeuge. **Mitte:** Suche, Kategorieauswahl und Eintragsliste. **Rechts:** Details. Strg+F fokussiert die Suche; Strg+Alt+D schaltet das Detailpanel um. Der Tresor bleibt lokal.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Free, Pro und Zusatzdienste

Bereich	Einordnung
Lokaler Tresor und Einträge	Ohne Konto nutzbar: Erstellen, Öffnen, Bearbeiten, Generator, TOTP, lokale Sicherheitsprüfung, Suche und Organisation.
Sicherung und Migration	Basisimport, verschlüsseltes Backup, Wiederherstellung und KDBX-/CSV-Export bleiben zugänglich.
Pro-Verwaltung	Website-Bereinigung, Inventar, Lifecycle, Abhängigkeiten, Rotation und erweiterte Migration benötigen gültige Pro-Rechte für entsprechende Änderungen.
Monitoring	Zusätzliche bewusste Aktivierung; persönliche Treffer verlangen geeignete eigene Quellen. Ein öffentlicher Vorfallkatalog reicht nicht.
Team / Freigaben / Notfallkopien	Benötigen einen getrennt eingerichteten Koordinationsdienst, registrierte Geräte und verifizierte Geräteschlüssel.
Browserintegration	In dieser ausgelieferten Version deaktiviert. Kein funktionierendes Browser-Autofill oder Passkey-Retrofit zugesagt.

> Das Lizenzkonto ersetzt weder das Masterpasswort noch eine zusätzliche Dienstregistrierung. Ein Pro-Lizenzende löscht keine lokalen Tresore; Basisbearbeitung, Sicherung und Export bleiben erhalten. Der vollständige aktuelle Funktionsvergleich steht im Anhang.

Tresor und Eintragstypen

Ein Tresor ist Ihre verschlüsselte Guardian-Datei (.agv). Sie öffnen ihn mit Ihrem Masterpasswort. Die lokale Datei benötigt kein Cloudkonto.

Website/Login: Benutzername, Passwort und geprüfte Website. API-Key: Zugangstoken eines Dienstes. Secure Note: vertrauliche Notizen. Server: Serverzugang. WiFi: WLAN-Zugang. Kategorien ordnen Einträge; Tags erlauben mehrere Zuordnungen.

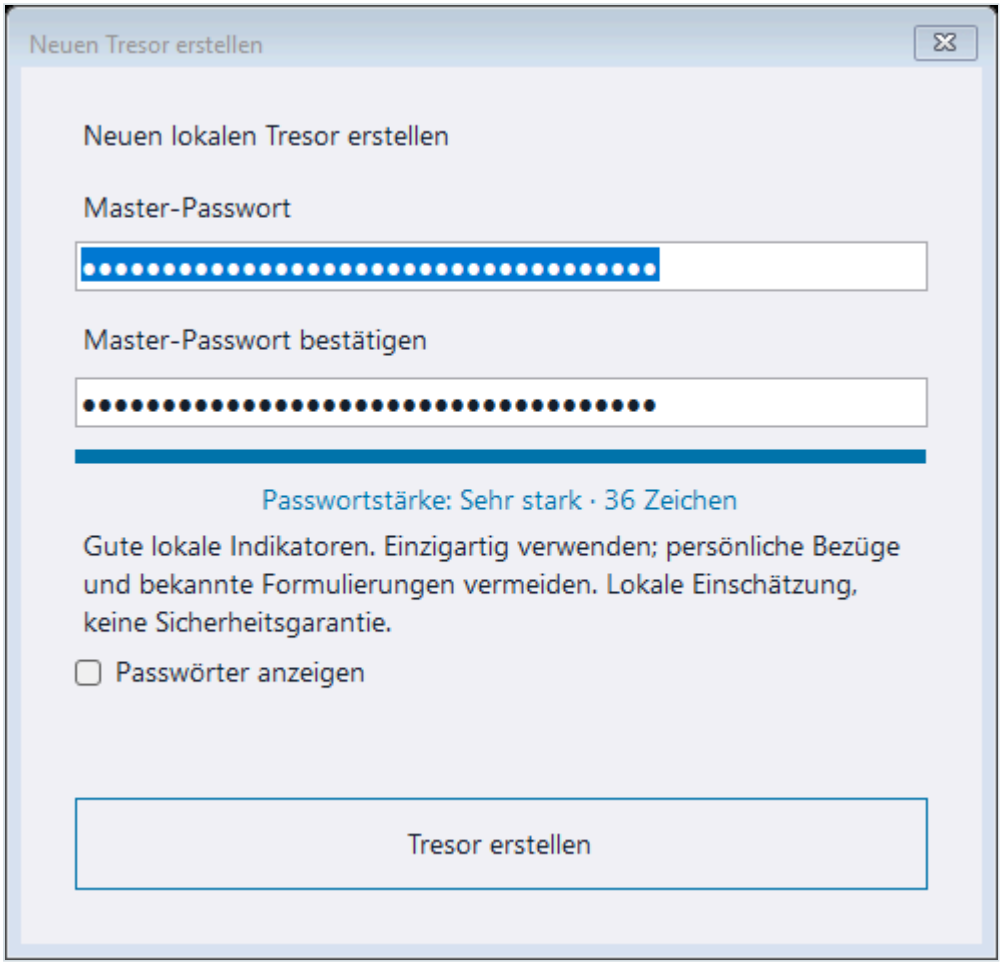
Passwörter und TOTP bleiben in der Liste verborgen. Rechts können Sie Details prüfen und Werte bewusst kopieren. Ein entsperrter Tresor hält Daten im Arbeitsspeicher. Sperren Sie Guardian, wenn Sie den Arbeitsplatz verlassen.

Das Masterpasswort

Das Masterpasswort schützt Ihren gesamten Tresor. Guardian verlangt beim Erstellen und Ändern mindestens 12 Zeichen. Für wichtigen Schutz verwenden Sie ein deutlich längeres, einzigartiges Passwort ohne persönliche Bezüge. Bewahren Sie es sicher außerhalb des Tresors auf. Es gibt keinen Passwortreset und keine Hintertür.

Die Stärkeanzeige bewertet lokal Länge sowie einige bekannte Muster und Wiederholungen. Sie ist eine konservative Orientierung und kein vollständiger Wörterbuchtest, keine Entropiemessung und keine Garantie. Es werden dafür keine Passwörter übertragen.

Ein langes, zufällig generiertes Passwort kann trotzdem unsicher sein, wenn es wiederverwendet oder veröffentlicht wurde. Die Einzigartigkeit prüft der Sicherheitsprüfung.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Verschlüsselung und Schutzgrenzen

Guardian verwendet Argon2id zur Schlüsselableitung und AES-256-GCM für authentisierte Verschlüsselung. Argon2id nutzt in dieser Version 64 MiB Speicher, drei Durchläufe und zwei parallele Spuren. Die Tresordatei enthält verschlüsselte Nutzdaten, keine Klartextpasswörter.

Die Stärkeanzeige betrifft Ihr Passwort; sie ändert nicht den Verschlüsselungsalgorithmus. Authentisierung schützt davor, unbemerkt veränderte Daten zu öffnen. Bei falschem Passwort oder beschädigter Datei erhalten Sie dieselbe Fehlermeldung.

Ein kompromittiertes Windows-Konto, Schadsoftware oder eine bereits entsperrte Sitzung können Daten gefährden. Halten Sie Windows aktuell. Auch Zwischenablageverlauf und Drittprogramme können eigene Kopien erzeugen.

Dieses Handbuch behauptet keine unabhängige Sicherheitszertifizierung. Die Browserintegration ist in der ausgelieferten Version deaktiviert.

Dateien, Speicherort und Sperrdatei

Der Tresor ist eine verschlüsselte **.agv-Datei**. Wählen Sie einen bekannten lokalen Speicherort außerhalb des Programmordners. Guardian merkt den zuletzt geöffneten Tresor; „Anderen Tresor öffnen“ wechselt zu einer anderen Datei.

.bak ist der vorherige verschlüsselte Speicherstand, nicht eine unabhängige Datensicherung. **.lock** schützt gegen gleichzeitigen Schreibzugriff. Löschen Sie diese Datei nicht während einer geöffneten Sitzung.

Benutzereinstellungen und zusätzliche lokale Verwaltungsdaten liegen standardmäßig unter `%LOCALAPPDATA%\ALPEG-SYSTEMS\GuardianPro`. Einige Zusatzdaten sind an das Windows-Benutzerkonto gebunden. Eine bloße Kopie dieser Dateien auf ein anderes Windows-Konto ist deshalb keine zugesagte Wiederherstellungsmethode.

Tresore mit Anhängen, Zusatzfeldern oder vollständigen Verlaufsschnappschüssen verwenden AGV-Hüllversion 2. Version 1 und 2 werden gelesen; ältere Programme können Version 2 ablehnen.

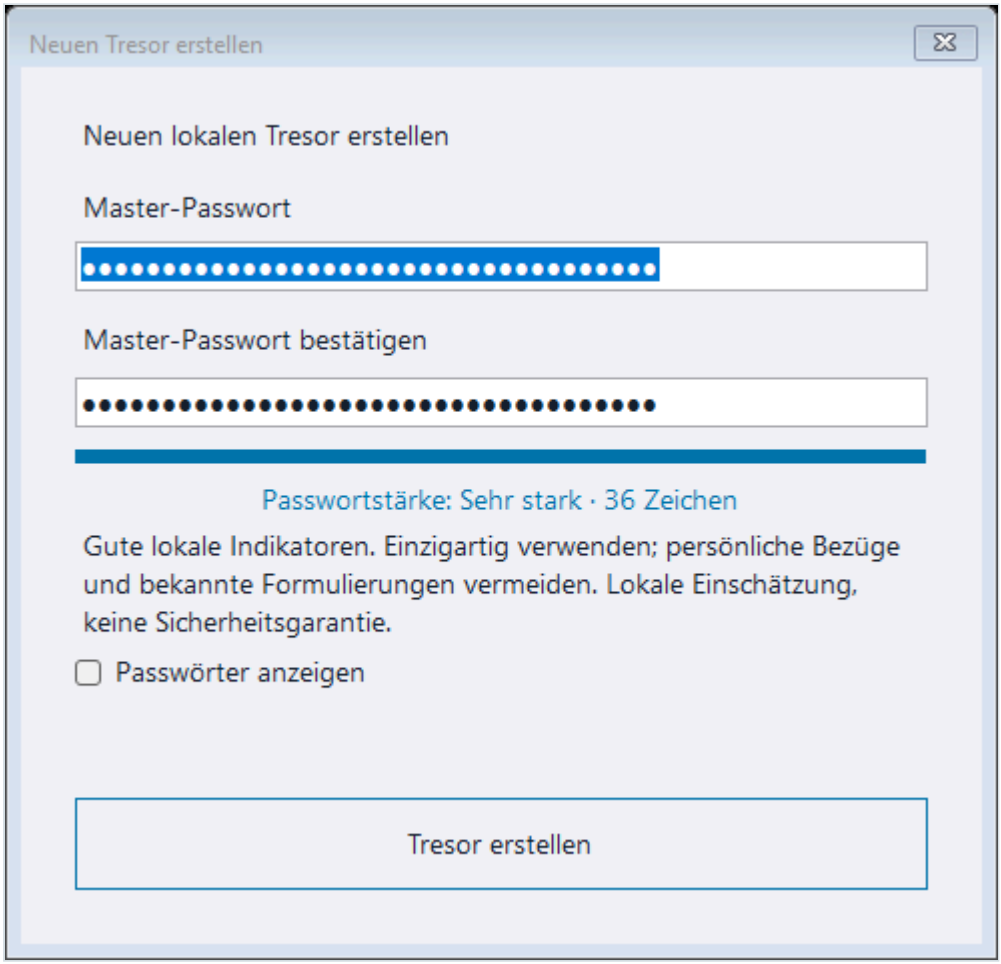
> Nach Änderung des Masterpassworts brauchen ältere Backups weiterhin das damalige Kennwort. Bewahren Sie mehrere überprüfte Sicherungsstände auf.

Einen neuen Tresor erstellen

1. Starten Sie Guardian. Wählen Sie Datei → Neuer Tresor.
2. Wählen Sie einen lokalen Speicherort und einen Dateinamen.
3. Geben Sie ein neues Masterpasswort ein. Die Stärkeanzeige hilft bei der Wahl. Enter führt zur Bestätigung.
4. Geben Sie dasselbe Passwort im zweiten Feld ein und klicken Sie Tresor erstellen.
5. Fügen Sie einen Eintrag über Neuer Eintrag hinzu oder wählen Sie Import / Migration.
6. Erstellen Sie ein verschlüsseltes Backup auf einem anderen Datenträger.

Bei „Passwörter stimmen nicht überein“ prüfen Sie beide Eingaben und gegebenenfalls die Anzeigeoption. Abbrechen verändert keinen Tresor.

Beim nächsten Start öffnen Sie die .agv-Datei über Datei → Tresor öffnen und geben Ihr Masterpasswort ein.

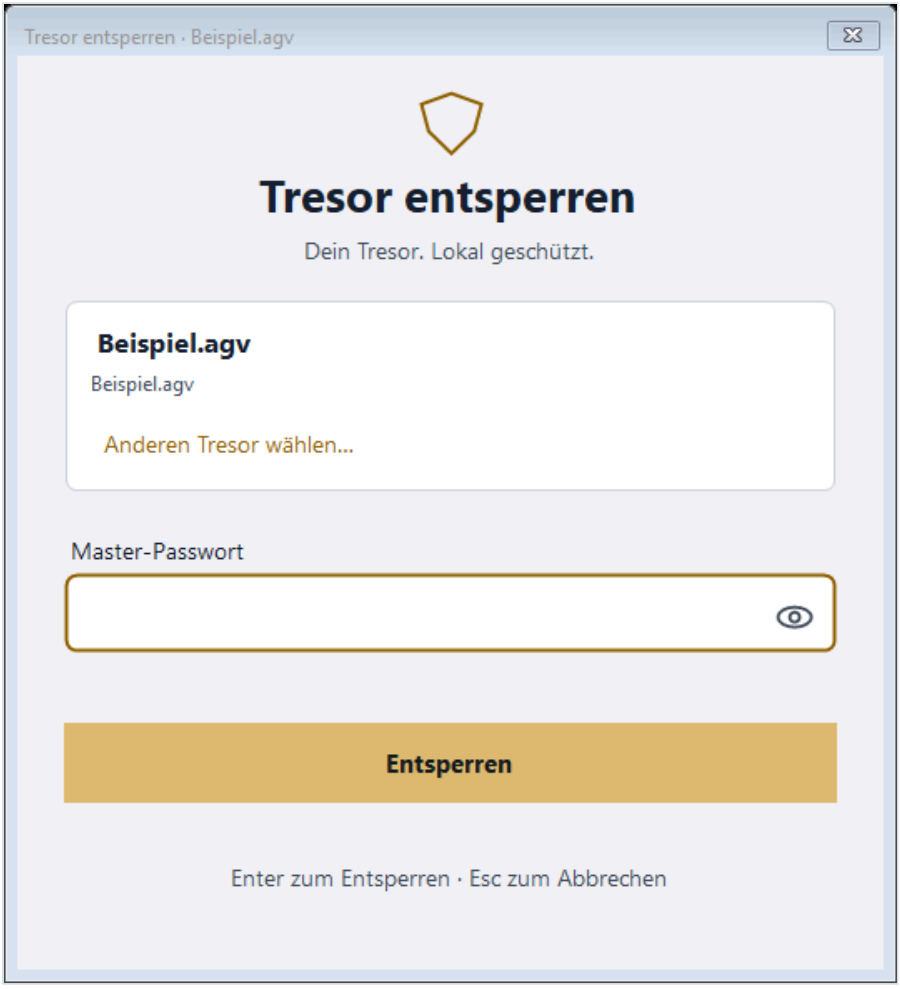


Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Öffnen, wechseln und vergessen

1. Öffnen Sie die .agv-Datei über Datei → Tresor öffnen oder wählen Sie den gemerkten Tresor.
2. Geben Sie das zu dieser Datei gehörende Masterpasswort ein. Die Augen-Schaltfläche blendet die Eingabe bei Bedarf ein; schützen Sie dabei Ihren Bildschirm.
3. „Anderen Tresor öffnen“ dient dem bewussten Wechsel. Der bisherige Tresor wird dabei nicht gelöscht.
4. „Gemerkten Tresor vergessen“ entfernt die gespeicherte Auswahl, nicht die Tresordatei.
5. Prüfen Sie bei einem Fehler Dateiauswahl und Tastaturlayout. Versuchen Sie eine bekannte Sicherung mit ihrem damaligen Masterpasswort.

> Falsches Passwort und beschädigte Datei können absichtlich gleich aussehen. Guardian und das Lizenzkonto können ein vergessenes Masterpasswort nicht zurücksetzen.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

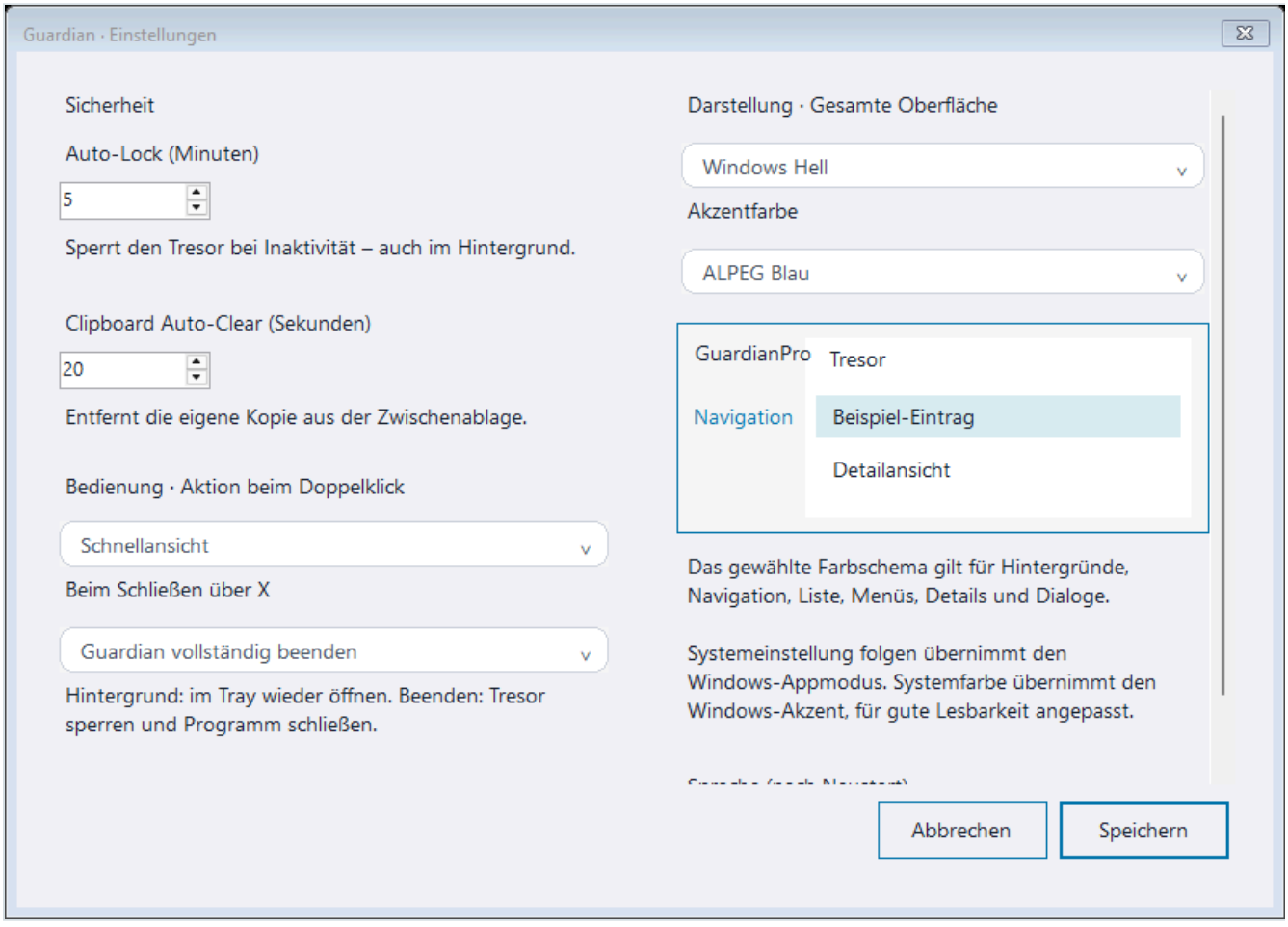
Sperren, Pausen und Auto-Lock

Strg+L, Datei → Sperren oder „Tresor sperren“ schließt den entschlüsselten Zugriff. Windows-Sitzungssperren werden ebenfalls berücksichtigt. Sperren beendet eine laufende Verwaltungsansicht, statt Geheimnisse darin offen zu halten.

In den Einstellungen wählen Sie Auto-Lock zwischen 1 und 60 Minuten. Die Zeit richtet sich nach Inaktivität und läuft auch im Hintergrund weiter. Die Standardvorgabe ist fünf Minuten.

Prüfen Sie, ob das rote X Guardian beendet oder in den Infobereich verschiebt. Im Traymodus läuft die Anwendung weiter; Datei → Beenden beendet sie unabhängig von dieser Einstellung.

> Auto-Lock schützt keine Kopien, die bereits in andere Programme eingefügt, exportiert oder als unabhängige Datei gespeichert wurden. Sperren Sie den Tresor vor einer unbeaufsichtigten Pause selbst.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

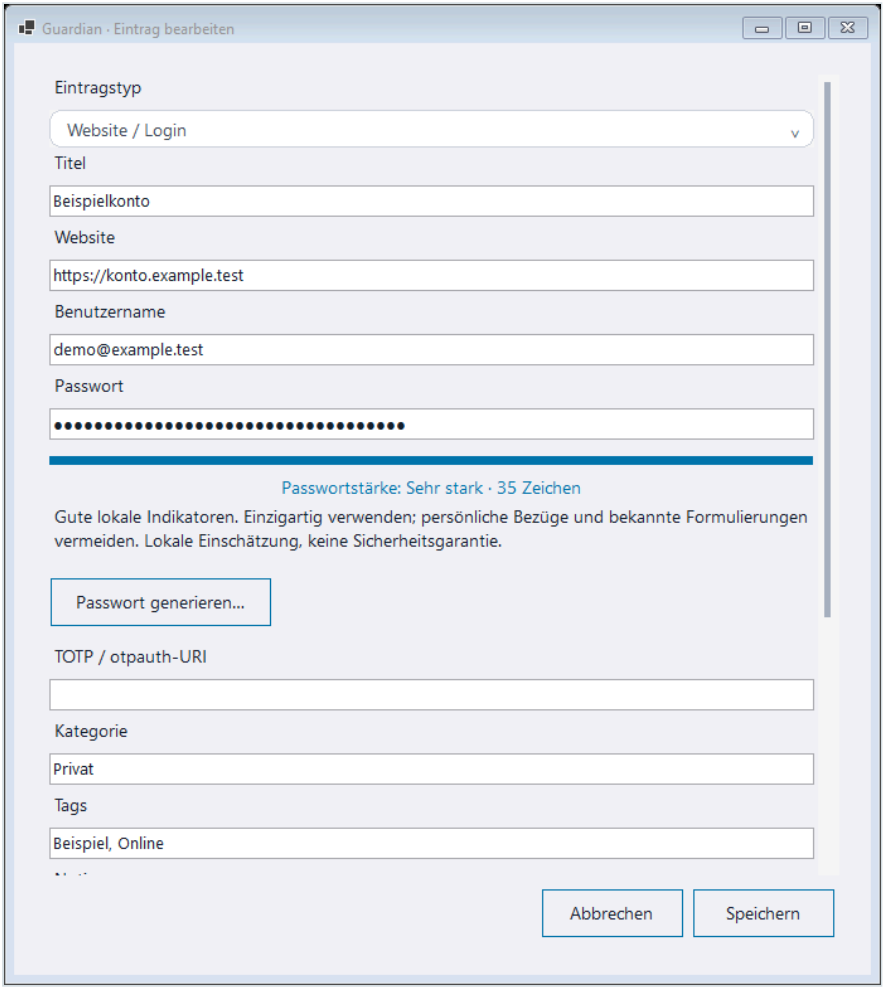
Einträge erstellen und bearbeiten

Neuer Eintrag oder Ctrl+N erstellt einen Eintrag. Wählen Sie Typ, Titel, Website, Benutzername und Passwort. Kategorien und Tags helfen später bei der Suche.

Zum Ändern wählen Sie einen Eintrag und Ctrl+E. Die Stärkeanzeige reagiert beim Tippen. Passwort generieren öffnet den Generator; Übernehmen setzt den Wert in den Editor. Speichern schreibt die Änderung in den verschlüsselten Tresor. Abbrechen verwirft die Eingabe.

Wichtig: Ein neues Passwort im Tresor ändert nichts beim Anbieter. Führen Sie die Passwortänderung in dessen Kontoeinstellungen durch und speichern Sie danach den neuen Wert in Guardian. Prüfen Sie anschließend den Login.

Bei Änderungen von Passwort, Benutzername oder Notizen bewahrt History den bisherigen Stand im Tresor. History enthält sensible Daten. Backups können ältere Passwörter weiterhin enthalten.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

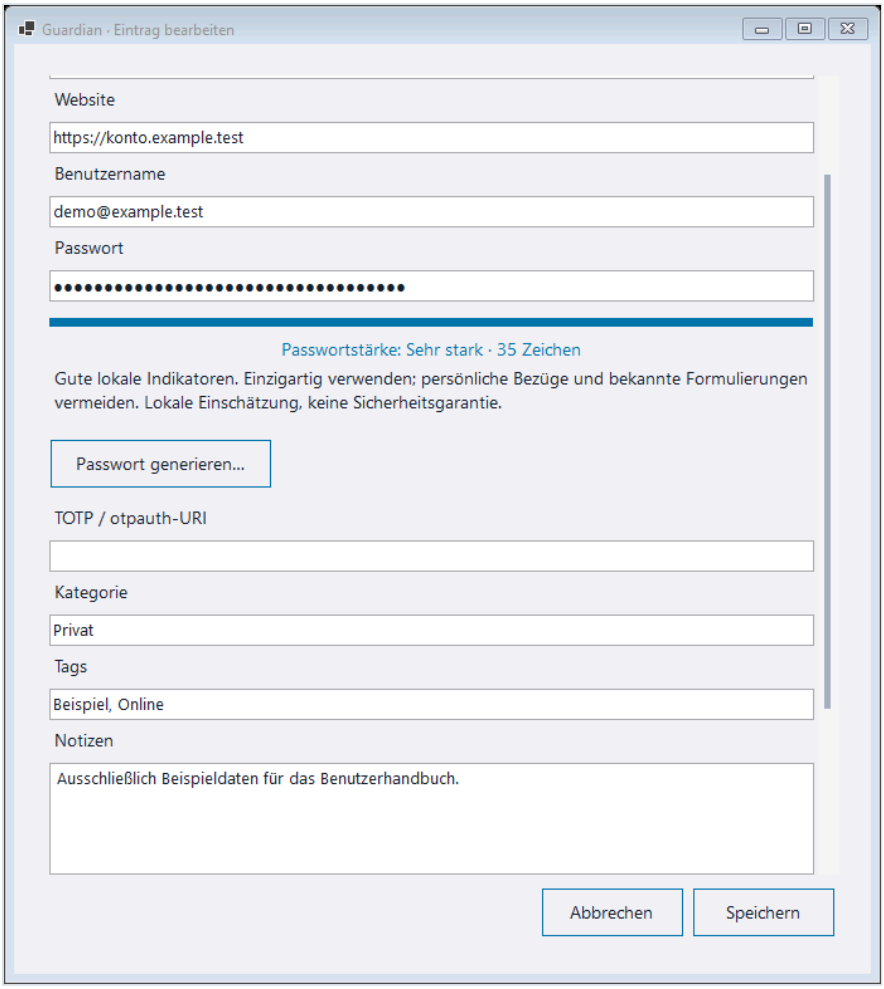
Notizen, Kategorien und Tags

Der Editor enthält unter den Zugangsfeldern TOTP, Kategorie, Tags und Notizen. Scrollen Sie bei kleinerem Fenster nach unten; die Schaltflächen Speichern und Abbrechen bleiben am unteren Rand.

Nutzen Sie Kategorien für stabile Bereiche und Tags für mehrere Zuordnungen. Notizen können vertrauliche Zusatzinformationen enthalten und werden im Tresor gespeichert. In einer ausdrücklich geöffneten Quick View können Notizen sichtbar sein.

Eine Änderung des Passwortfeldes ändert kein Passwort beim Anbieter. Speichern Sie neue Zugangsdaten erst im passenden Ablauf und testen Sie den tatsächlichen Login.

> Abbrechen verwirft die Eingaben des Editors. Prüfen Sie nach „Speichern“ den richtigen Eintrag; sensible historische Werte können weiterhin verschlüsselt vorhanden sein.



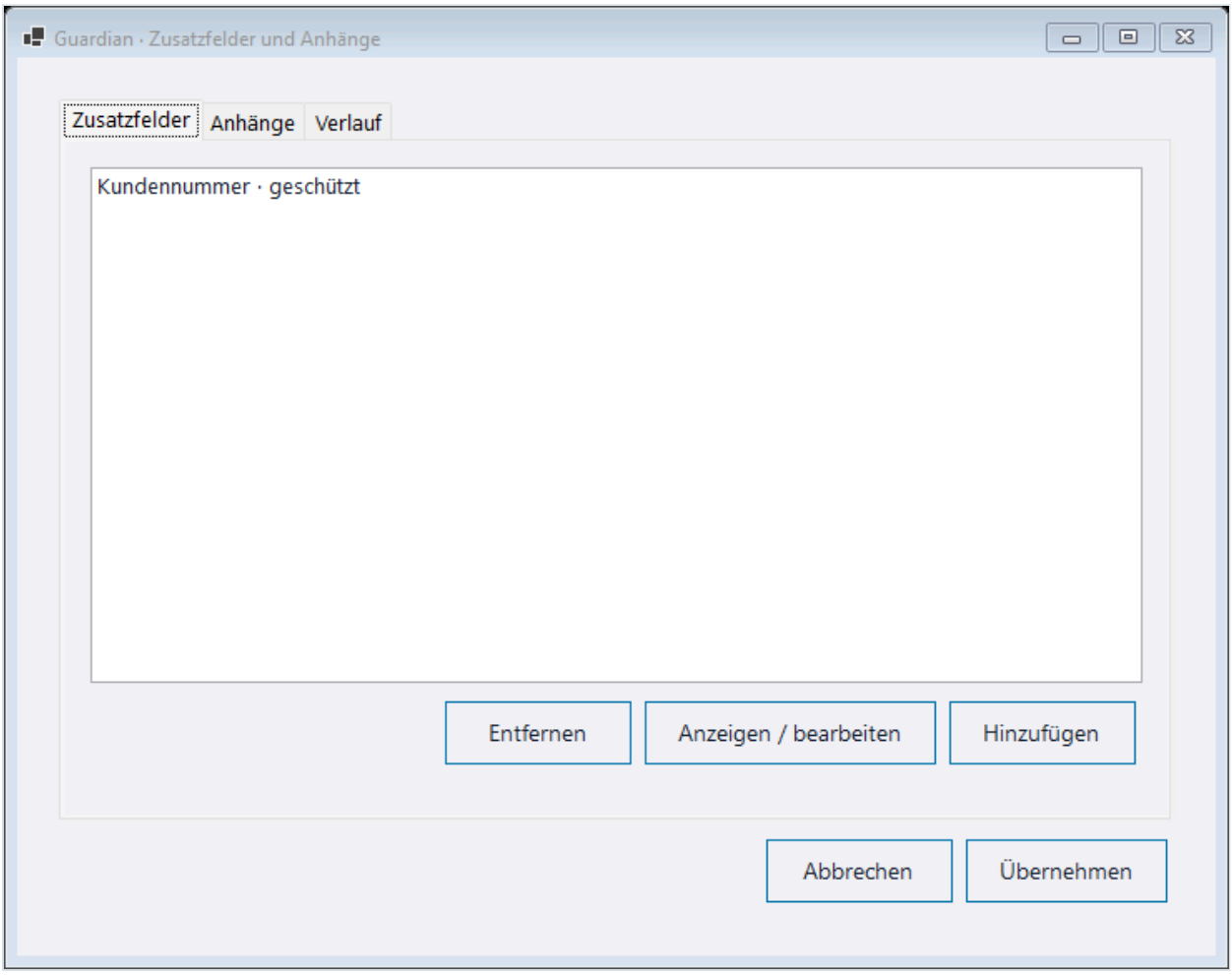
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Zusatzfelder und Anhänge

1. Eintrag bearbeiten und „Zusatzfelder und Anhänge“ öffnen.
2. Im Register Zusatzfelder benannte Werte hinzufügen oder bearbeiten. Listen zeigen nicht ungefragt die Feldwerte.
3. Im Register Anhänge Dateien hinzufügen, in einen gewählten Ordner exportieren oder aus dem aktuellen Eintrag entfernen.
4. Änderungen im Zusatzdialog übernehmen und danach den Eintragseditor speichern. Abbrechen verwirft die noch nicht übernommenen Änderungen.

Anhänge erhöhen die Tresorgröße. Die verschlüsselte Gesamthülle ist auf 64 MiB begrenzt; eine zu große Speicherung wird abgelehnt und die bisherige Datei bleibt erhalten.

> Aus dem Tresor exportierte Anhänge liegen am Ziel als gewöhnliche Dateien vor. „Entfernen“ ist keine sichere Vernichtung sämtlicher Kopien, Backups oder früherer Eintragsstände.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

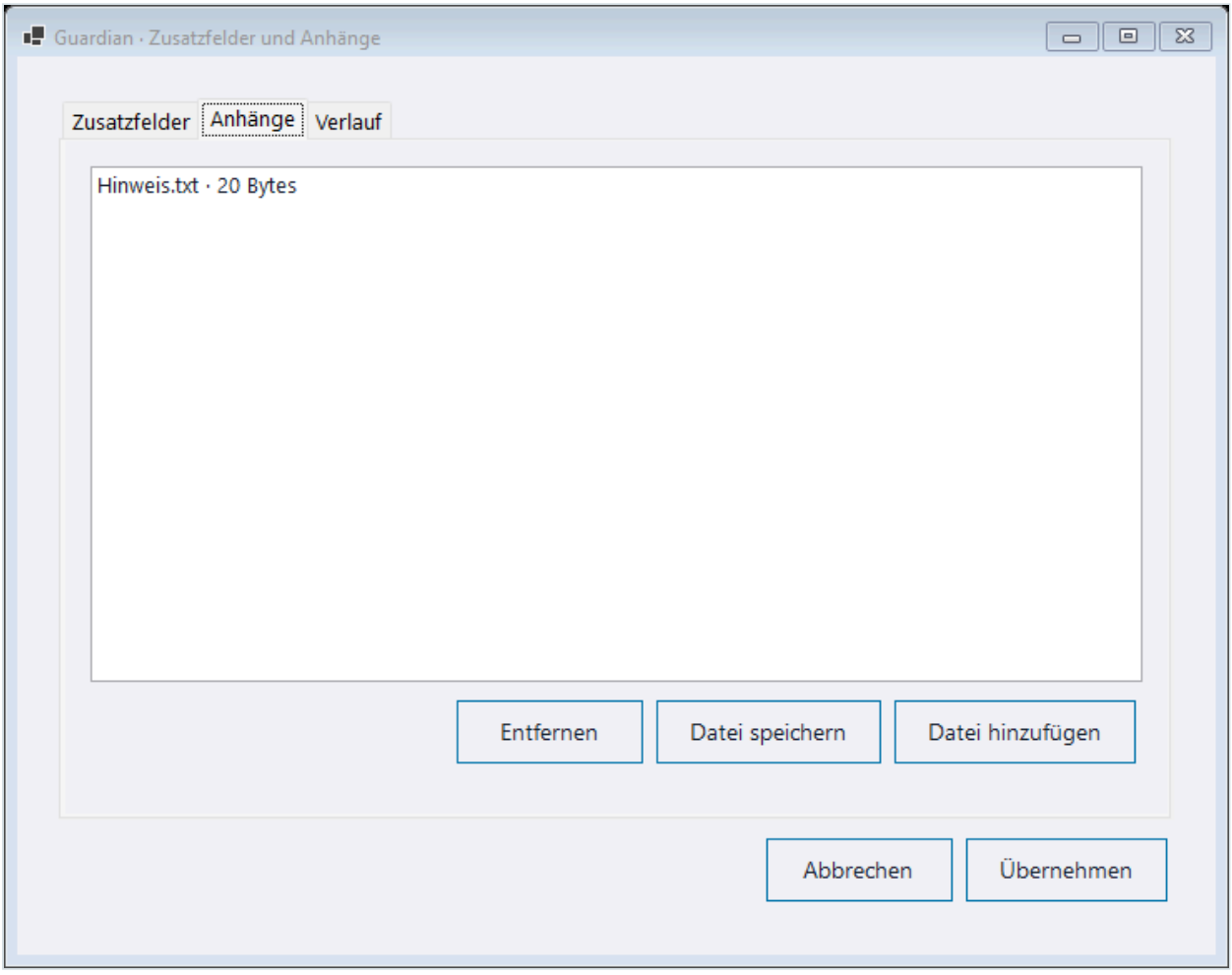
Anhänge und ältere Eintragsstände

Das Anhangsregister listet vorhandene Dateien. Ein bewusst gewählter Export legt deren Inhalt außerhalb des Tresors ab. Prüfen Sie Ziel, Dateiname und Herkunft, bevor Sie einen exportierten Anhang öffnen.

Guardian bewahrt bei relevanten Eintragsänderungen frühere Stände. Die History-Übersicht informiert über diese Änderungen; vollständige ältere Einträge können über die Zusatzdatenansicht lesend geprüft werden.

Historische Ansichten sind keine Aufforderung, alte Zugangsdaten wieder beim Anbieter zu aktivieren. Frühere Werte können bereits widerrufen sein.

> Verlauf und Sicherungen können alte Passwörter oder vorbereitete Rotationswerte enthalten. Behandeln Sie auch historische Daten als vertraulich.



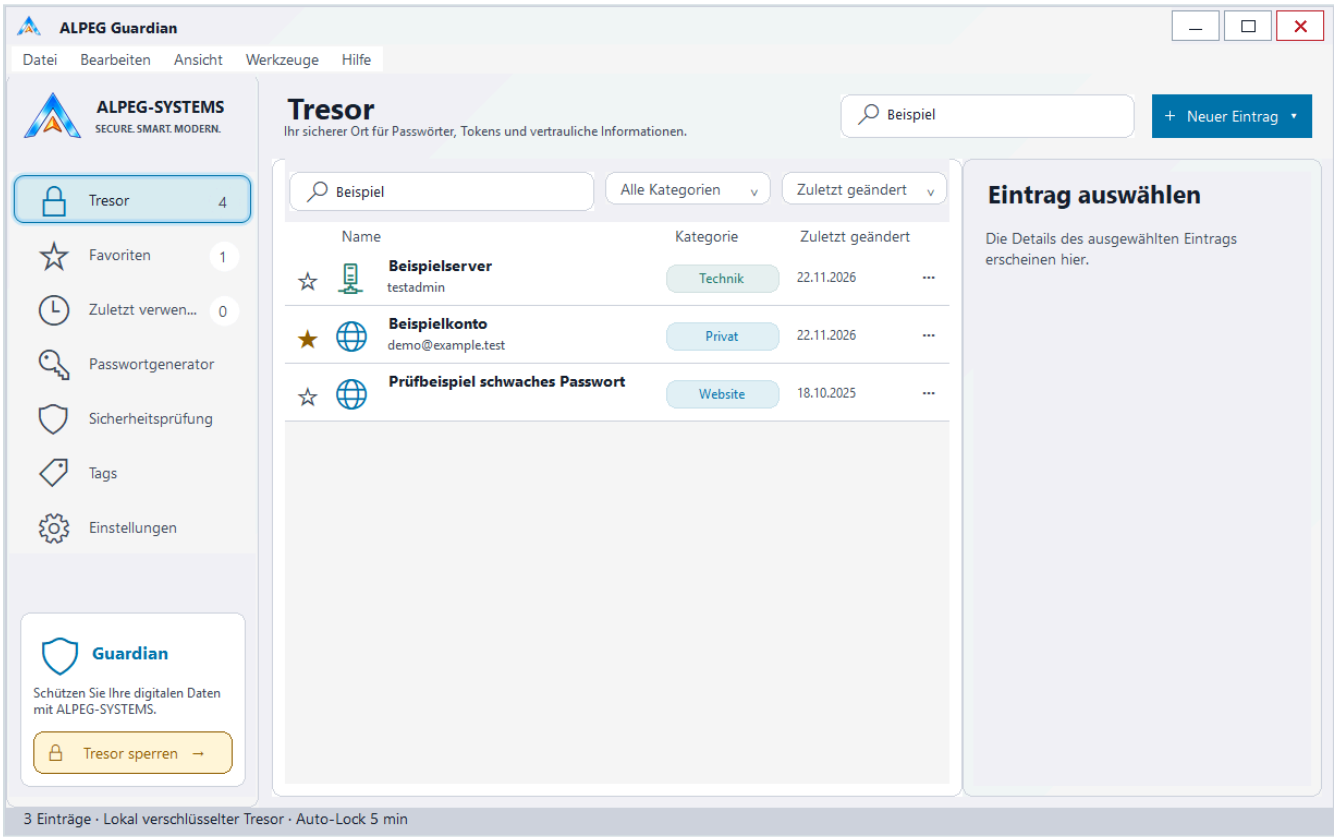
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Suchen, Favoriten und zuletzt verwendet

1. Mit Strg+F die Suche öffnen und einen Teil von Titel, Website oder Benutzername eingeben.
2. Kategorieauswahl und Sortierung verwenden, um den Bestand einzugrenzen. Filter leeren, falls ein Eintrag scheinbar fehlt.
3. Eintrag über Stern bzw. Favorit-Aktion markieren; „Favoriten“ zeigt diese Auswahl.
4. „Zuletzt verwendet“ zeigt von Guardian bewusst genutzte Einträge.

Die lokale Nutzungsaufzeichnung ist kein vom Anbieter bestätigter Login und keine Browserhistorie. Bei Importen kann eine belastbare letzte Nutzung fehlen.

> Die normale Suche dient dem Auffinden von Einträgen. Sie ist kein vollständiger Scanner über sämtliche verschlüsselten Zusatzdaten und Anhänge.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

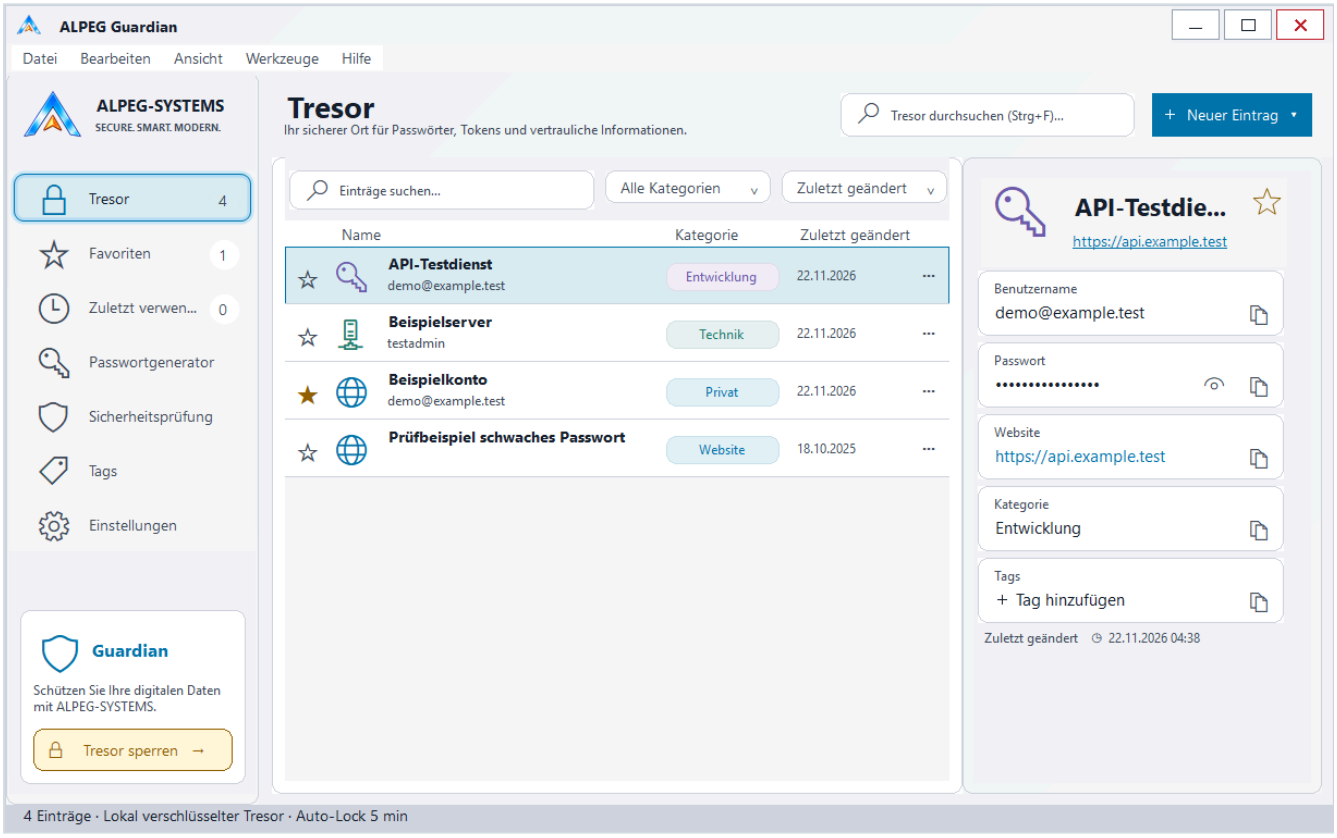
Details, Quick View und Kontextmenü

Markieren Sie einen Eintrag, um seine Details rechts zu sehen. **Leertaste** öffnet Quick View mit Titel, Website, Benutzername und Notizen; das Passwort wird darüber nicht ausgegeben.

Im Kontextmenü finden Sie unter anderem Website öffnen, Kopieraktionen, Bearbeiten, Duplizieren, Favorit, History, Tags und Löschen. Ein HTTPS-Link öffnet die Website im Standardbrowser; der Nutzer führt Anmeldung und Bestätigungen selbst aus.

„Duplizieren“ bereitet eine eigenständige Kopie zur Bearbeitung vor. Prüfen Sie Titel und Identität vor dem Speichern. Beim Löschen wird der Eintrag aus dem aktuellen Tresor entfernt, nicht automatisch beim Anbieter oder aus älteren Backups.

> Nicht jede sichtbare historische Browseraktion ist in dieser Veröffentlichung funktionsfähig. Browser-Autofill bleibt deaktiviert; verwenden Sie bewusste Kopieraktionen.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Kopieren und Zwischenablage

Strg+C kopiert den Benutzernamen, **Strg+Umschalt+C** das Passwort und **Strg+Umschalt+O** den aktuellen TOTP-Code. Jede Kopieraktion ist eine bewusste Ausgabe eines Geheimnisses.

Die Auto-Clear-Frist beträgt in den Einstellungen 5 bis 120 Sekunden, standardmäßig 20 Sekunden. Guardian löscht seine aktuelle eigene Kopie, wenn sie noch unverändert vorliegt. Später von Ihnen kopierter fremder Text bleibt erhalten.

Guardian kennzeichnet diese Kopien gegen Windows-Zwischenablageverlauf und Cloud-Übertragung. Andere Anwendungen und bereits eingefügte Kopien liegen außerhalb dieser Kontrolle.

> Fügen Sie Zugangsdaten nur in das richtige Ziel ein. Auto-Clear kann bereits gelesene, eingefügte oder von anderen Programmen gespeicherte Inhalte nicht zurückholen.

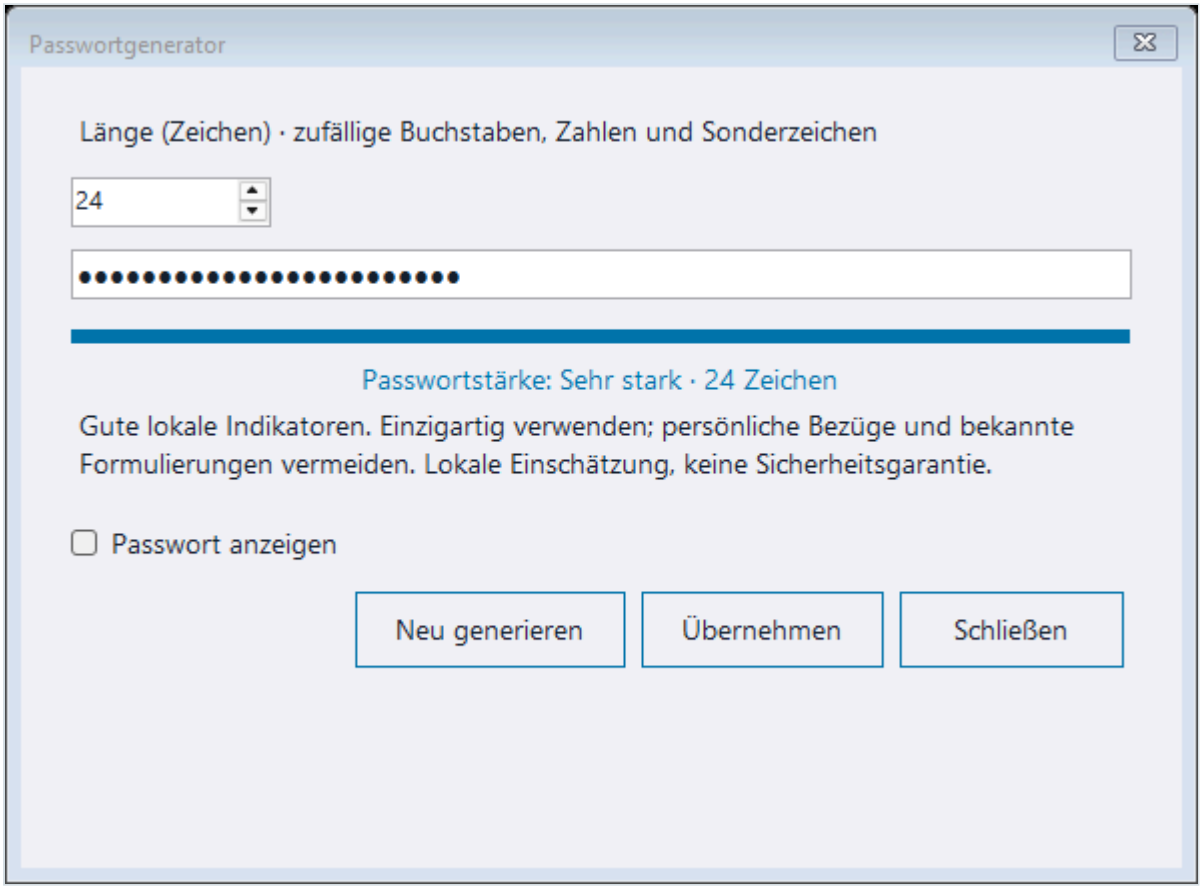
Passwörter erzeugen

Öffnen Sie Werkzeuge → Passwortgenerator oder links Password Generator.

Ein zufälliges Passwort wird sofort erzeugt, zunächst maskiert. Die Standardlänge beträgt 24 Zeichen. Wählen Sie 14 bis 128 Zeichen und klicken Sie Neu generieren. Der Generator verwendet kryptografisch sichere Zufallszahlen und Buchstaben, Zahlen sowie Sonderzeichen.

Kopieren überträgt den Wert in die Zwischenablage. Eine Meldung bestätigt dies; Auto-Clear entfernt die eigene Kopie nach der eingestellten Zeit. Im Eintragseditor ersetzt Übernehmen das Passwortfeld. Schließen übernimmt nichts.

Beachten Sie die Regeln des Zielanbieters. Einige Dienste begrenzen Länge oder erlaubte Zeichen. Die lokale Stärkeanzeige ist eine Orientierung; nutzen Sie jedes Passwort nur für ein Konto.



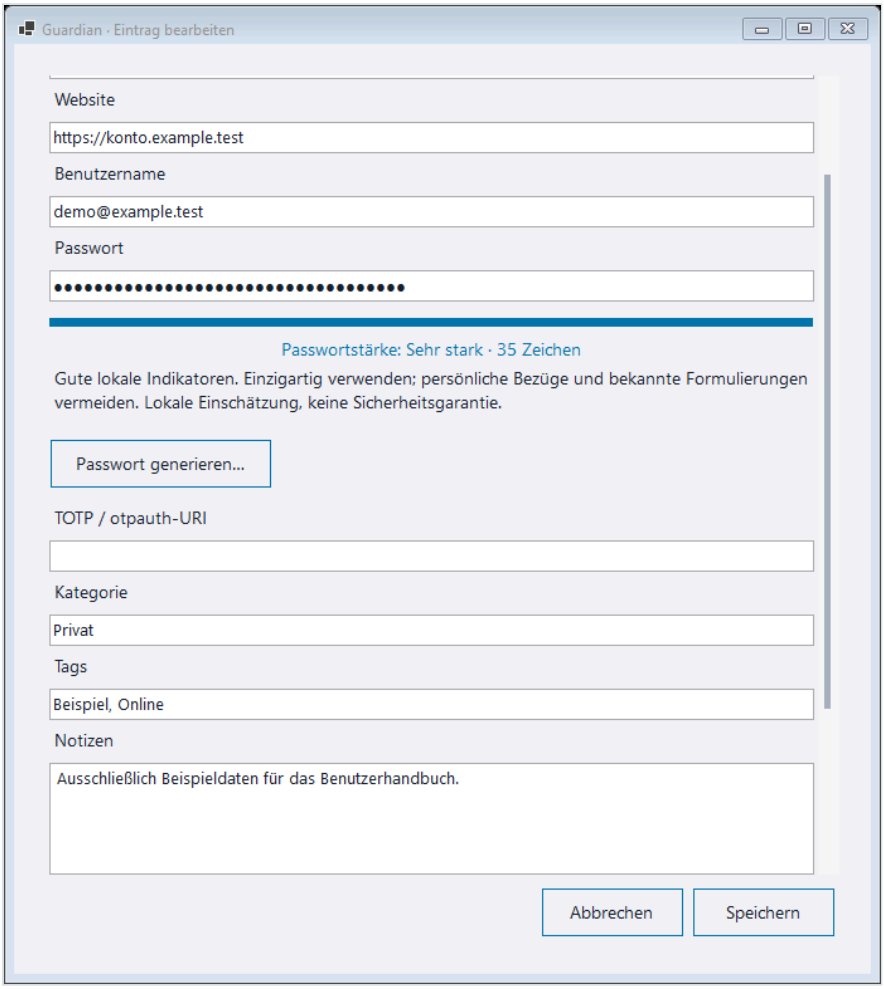
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

TOTP einrichten und verwenden

Guardian berechnet sechsstellige TOTP-Codes mit SHA1 und 30-Sekunden-Intervall. Hinterlegen Sie ein Base32-Secret oder eine passende otpauth-URI. SHA256, acht Stellen und andere Intervalle werden derzeit nicht unterstützt.

Prüfen Sie beim Einrichten den Code gegen einen unabhängigen Authenticator. Stimmen Codes nicht überein, prüfen Sie die Windows-Uhrzeit, das Secret und die Anbieterparameter. Kopieren Sie TOTP über die dafür vorgesehene Aktion.

Passwort und zweiter Faktor im selben Tresor sind bequem, verringern aber die Trennung der Faktoren. Bewahren Sie Wiederherstellungscodes zusätzlich sicher außerhalb des Tresors auf.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Auto-Type und deaktiviertes Browser-Autofill

Auto-Type

Strg+Umschalt+T bietet nach einer Warnung eine verzögerte Eingabe von Benutzername, Tab und Passwort in das aktive Fenster. Prüfen Sie das Ziel sorgfältig und üben Sie zunächst mit künstlichen Werten. Das Verfahren authentifiziert die Zielanwendung nicht. Eine Tresorsperre während des Countdowns verhindert die Ausgabe.

Browserintegration

Die ausgelieferte 1.6.0-Version hat die lokale Browserintegration deaktiviert. Hinweise in älteren Programm-Hilfetexten zu manueller Erweiterungsinstallation und Browser-Passkeys beschreiben diesen freigegebenen Stand nicht.

Installieren Sie dafür keine alten Kandidaten-Erweiterungen nach historischen Anleitungen. Browsermigration per exportierter CSV ist davon getrennt und weiterhin nutzbar.

> Auto-Type ist keine Browser-Domainprüfung. Lassen Sie das Ziel nicht während der Wartezeit unbemerkt wechseln. Das Handbuch verspricht keine aktive Browser-Autofill-Funktion.

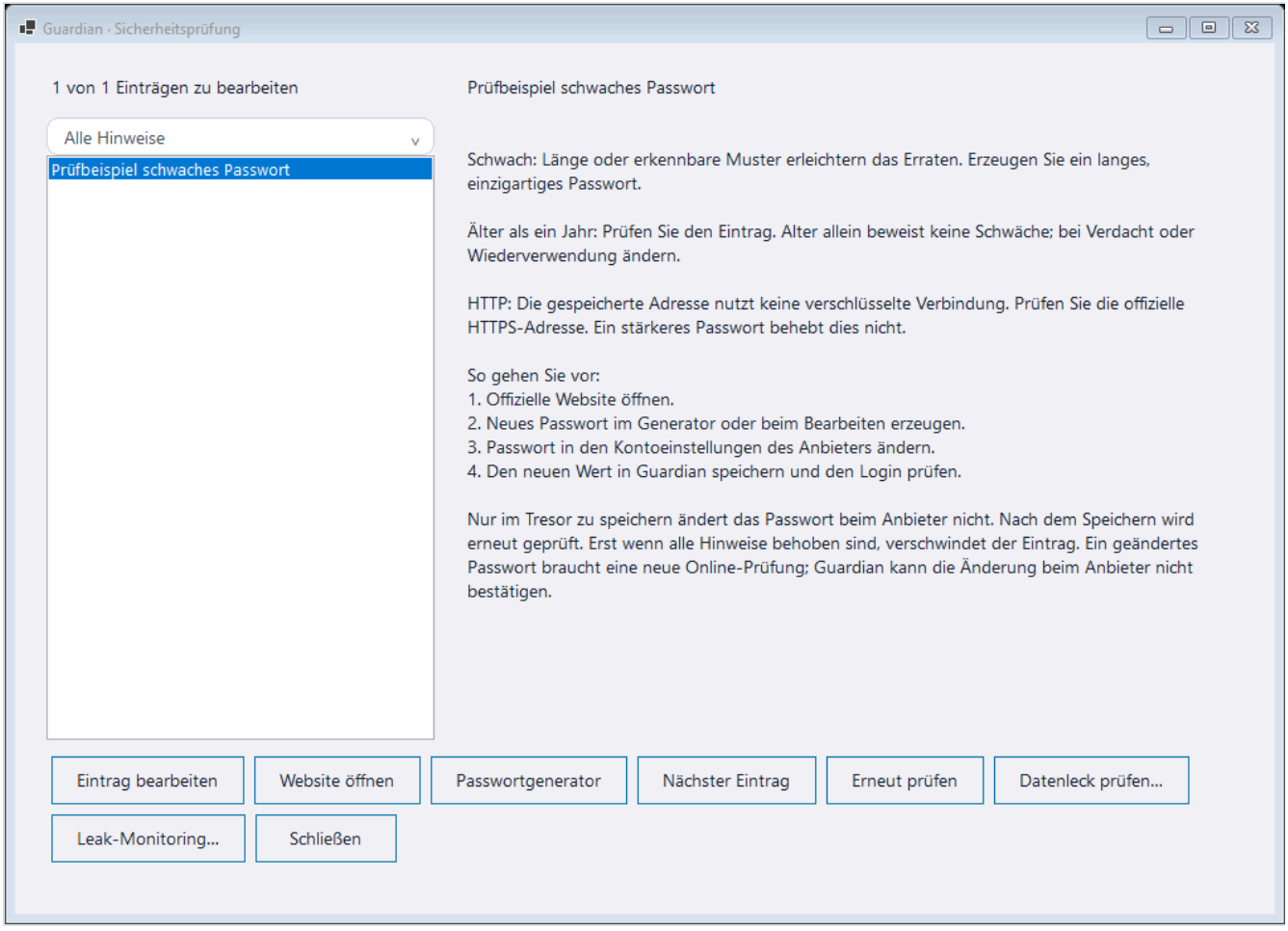
Lokale Sicherheitsprüfung

Öffnen Sie Werkzeuge → Sicherheitsprüfung. Links stehen Einträge mit offenen Hinweisen, rechts Ursachen und konkrete Schritte. Es werden keine Passwörter in der Aufgabenliste angezeigt.

Schwach: Länge oder Muster verbessern. Wiederverwendet: alle aufgeführten Konten jeweils mit einem eigenen Passwort versehen. HTTP: die offizielle sichere Website prüfen. Fehlende Website: gültige Adresse eintragen. Alter: prüfen, nicht automatisch als unsicher behandeln.

Mit Website öffnen, Passwortgenerator und Eintrag bearbeiten arbeiten Sie einen Fund ab. Ändern Sie das Passwort zuerst beim Anbieter; Speichern in Guardian allein genügt nicht. Nach dem Speichern wird erneut geprüft. Ohne verbleibende Hinweise verschwindet der Eintrag. Nächster Eintrag führt durch die Liste.

Datenleck prüfen benötigt Ihre ausdrückliche Zustimmung und Internet. Nur ein Hashpräfix wird übertragen; der Anbieter sieht Ihre IP. Treffer werden in der Aufgabenliste markiert. Ein geändertes Passwort benötigt eine neue Prüfung. Keine Treffer beweisen keine Sicherheit.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Freiwillige Online-Passwortprüfung

1. Tresor öffnen und „Kompromittierte Passwörter prüfen (Online)“ oder die entsprechende Aktion der Sicherheitsprüfung wählen.
2. Datenschutzhinweis lesen und die Verbindung ausdrücklich erlauben.
3. Ergebnis prüfen. Ein Treffer erfordert eine Passwortänderung beim Anbieter und anschließend die Aktualisierung des Tresors.
4. Nach Änderung erneut prüfen. Bei Verbindungsfehlern nicht von einer erfolgreichen Prüfung ausgehen.

Übertragen werden nur die ersten fünf Zeichen eines SHA-1-Hashes an Pwned Passwords; der vollständige Vergleich geschieht lokal. Der Anbieter sieht dennoch Ihre IP-Adresse. Eine neue Prüfung kann bei geänderten Passwörtern nötig sein.

> Keine Treffer sind keine Sicherheitsgarantie. Die Passwortprüfung ist nicht dasselbe wie persönliche E-Mail-/Dark-Web-Betroffenheitsprüfung und verändert keine Konten automatisch.

Verschlüsselte Backups und Wiederherstellung

Backup erstellen: Datei → Backup, anderen Datenträger und neuen Dateinamen wählen. Das Backup bleibt verschlüsselt. Schließen Sie den Tresor vor einer manuellen Kopie.

Wiederherstellen: Datei → Recovery aus Backup, Backupdatei wählen, damaliges Masterpasswort eingeben und einen neuen Zieldateinamen wählen. Guardian prüft das Backup und überschreibt keinen bestehenden Tresor. Öffnen Sie den wiederhergestellten Tresor und prüfen Sie Stichproben.

Die automatische .bak ist nur der vorherige Speicherstand und liegt auf demselben Datenträger. Bei Geräteverlust hilft sie nicht. Bewahren Sie mehrere externe Backupstände auf und testen Sie die Wiederherstellung.

Nach Masterpasswortänderungen bleiben alte Backups mit dem alten Passwort geschützt. Ein neues Backup erstellen und die benötigten alten Passwörter sicher verwahren. Ohne passendes Passwort ist keine Wiederherstellung möglich.

Der verschlüsselte KDBX-Export erhält Zusatzfelder, Anhänge und Verlauf. CSV enthält nur Standardfelder; diese Zusatzdaten fehlen darin. Der Exportdialog warnt vor dem Erstellen einer CSV-Datei.

KDBX- und CSV-Export

1. Öffnen Sie den gewünschten Tresor und wählen Sie Datei → Export KDBX / CSV.
2. Wählen Sie Format und neuen Zielpfad. Ein KDBX-Export verlangt ein bewusst festgelegtes Exportkennwort.
3. Prüfen Sie die Ausgabe mit einer passenden Anwendung und kontrollieren Sie Anzahl sowie wichtige Zusatzdaten.
4. Bewahren Sie Klartextausgaben nicht ungeschützt auf und geben Sie sie nicht ungeprüft weiter.

Ein verschlüsseltes AGV-Backup erhält den Guardian-Tresorstand. KDBX dient der Übertragbarkeit; spezielle Guardian-Verwaltungsdaten werden über unterstützte Zusatzfelder transportiert. CSV kann nicht alle Anhänge, Historien und Pro-Metadaten erhalten.

> **CSV enthält Klartextgeheimnisse.** Eine normale Löschung auf SSDs garantiert keine physische Entfernung. Export und Backup sind auch bei fehlenden Pro-Rechten für Ihre lokalen Daten vorgesehen.

Masterpasswort ändern

Öffnen Sie den Tresor und Werkzeuge → Master-Passwort ändern. Geben Sie das neue Passwort zweimal ein. Prüfen Sie die Stärkeanzeige und speichern Sie es an einem sicheren Ort außerhalb des Tresors.

Guardian verschlüsselt den aktuellen Tresor mit einem neu abgeleiteten Schlüssel. Erstellen Sie danach ein neues externes Backup und testen Sie das Wiederöffnen. Frühere .bak- und Backupdateien behalten ihr damaliges Passwort.

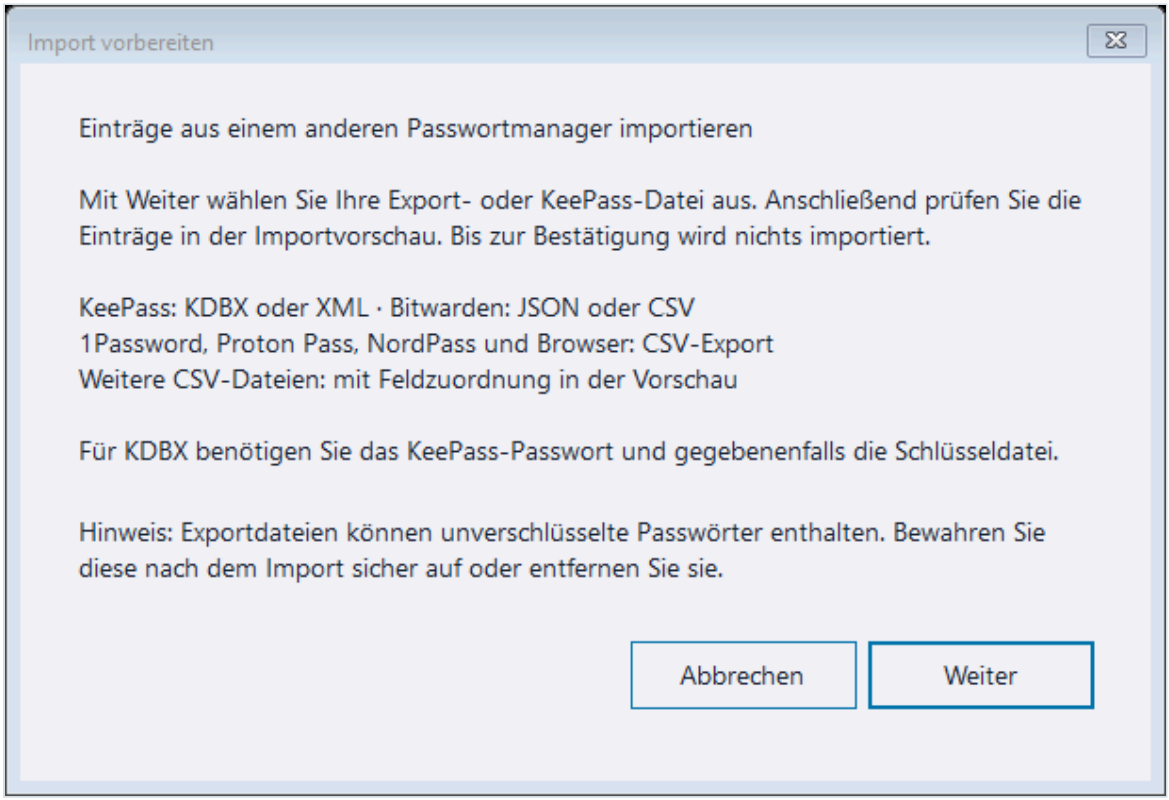
Die Funktion ändert keine Passwörter Ihrer gespeicherten Konten. Ein vergessenes Masterpasswort kann nicht zurückgesetzt werden.

KeePass-Migration

1. Öffnen Sie zuerst Ihren Ziel-Tresor in Guardian.
2. Wählen Sie Datei → Import / Migration → Weiter.
3. Wählen Sie Ihre KeePass-.kdbx-Datei oder einen KeePass-XML-Export.
4. Für KDBX geben Sie das KeePass-Masterpasswort ein.
5. Auf „Verwendet der KeePass-Tresor außer dem MasterKey eine Schlüsseldatei?“ wählen Sie Nein, wenn Sie nur ein Passwort nutzen. Ja ist ausschließlich für eine zusätzliche Datei. Wählen Sie dann diese Datei aus.
6. Prüfen Sie Feldzuordnung und Vorschau. Dubletten/Konflikte werden standardmäßig übersprungen.
7. Bestätigen Sie Importieren. Optional starten Sie danach den Sicherheitsprüfung.

Guardian ändert Ihre KeePass-Datei nicht. Prüfen Sie den Import zunächst mit Beispieldaten. Unterstützt sind Passwort und optionales Keyfile; Windows-Kontobindung und andere Spezialverfahren sind nicht zugesagt. XML-Exporte können unverschlüsselte Secrets enthalten.

AGTE übernimmt KDBX 3.1, 4.0 und 4.1 einschließlich Eintragsanhängen, Zusatzfeldern und vollständigen älteren Einträgen. Unter Eintrag bearbeiten → Zusatzfelder und Anhänge lassen sich diese Daten und der Verlauf ansehen. Auto-Type, Plugin-Einstellungen und datenbankweite Metadaten werden nicht übernommen. Warnungen und übersprungene Dubletten beachten. Schlüsseldateien zusätzlich zum Passwort werden unterstützt; kontogebundene oder Plugin-Schlüssel nicht.



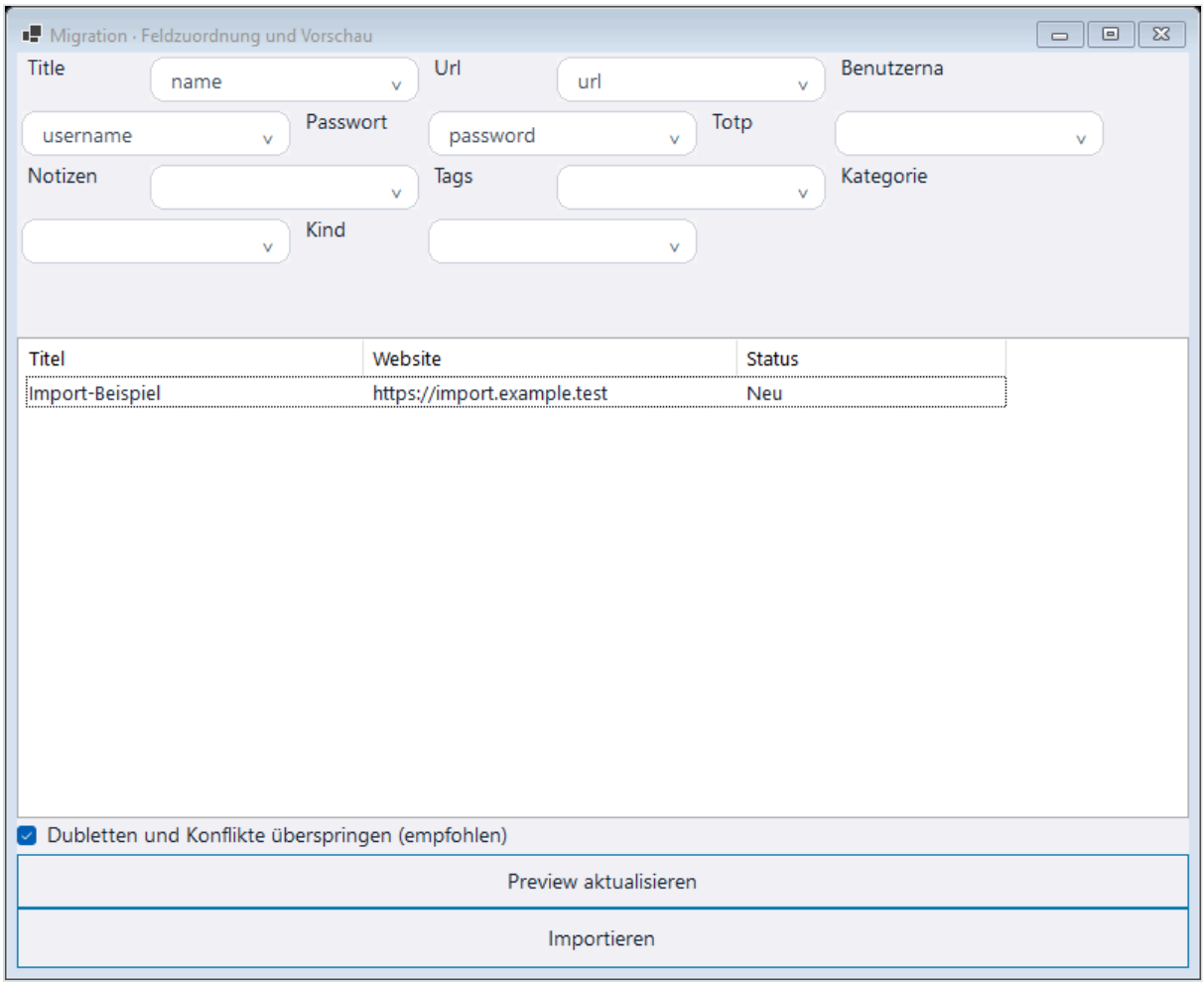
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Browserdaten per CSV übernehmen

1. Erstellen Sie im Passwortmanager Ihres Browsers einen CSV-Export. Der Browser kann dafür eine Windows-Bestätigung verlangen.
2. Öffnen Sie den Ziel-Tresor und Datei → Import / Migration → Weiter.
3. Wählen Sie die CSV-Datei.
4. Kontrollieren Sie die Zuordnung von Titel, Website, Benutzername und Passwort. In der Vorschau werden keine Passwörter angezeigt.
5. Prüfen Sie Dubletten und bestätigen Sie den Import. Testen Sie anschließend einzelne Logins.

Guardian liest in dieser Version Browserprofile nicht direkt aus. Browsermigration erfolgt über Exportdateien. Chrome/Edge/Brave verwenden Chromium-Passwortexporte; bei Firefox verwenden Sie den CSV-Export des Passwortmanagers. Exportfunktionen können je Browserversion anders angeordnet sein.

Die CSV enthält Klartextpasswörter. Teilen Sie sie nicht und bewahren Sie sie nicht ungeschützt auf. Eine normale Löschung garantiert auf SSDs keine physische Entfernung.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

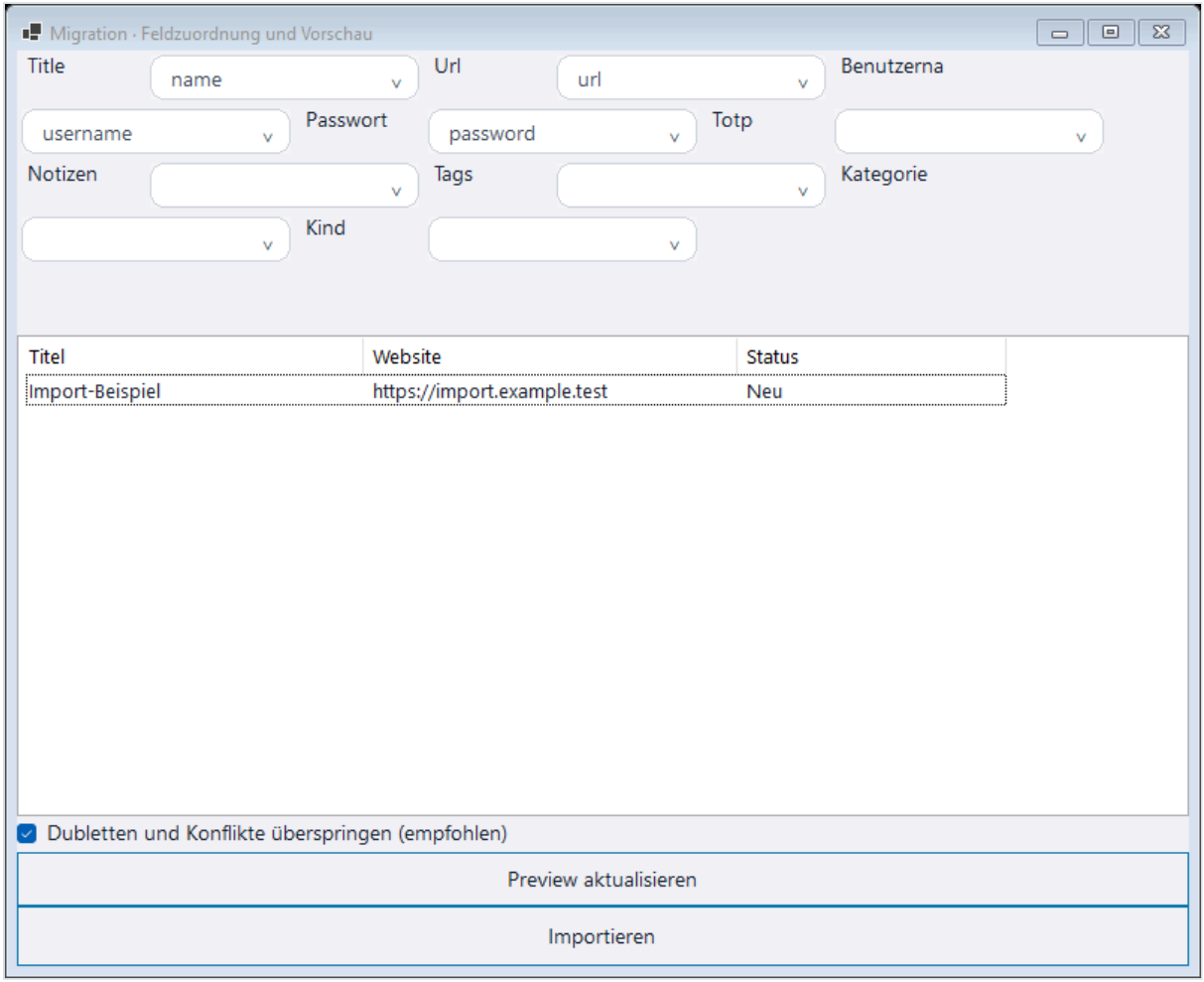
Weitere Importformate und Konflikte

Bitwarden: JSON oder CSV verwenden. 1Password, Proton Pass und NordPass: CSV-Export verwenden. Generic CSV erlaubt eigene Spalten über die Feldzuordnung. Native 1PUX- und andere proprietäre Archive werden nicht vollständig unterstützt.

Wählen Sie Datei → Import / Migration. Die Vorschau zeigt Titel, Website und Status. Passen Sie falsch erkannte Spalten an und klicken Sie Preview aktualisieren.

Standardmäßig überspringt Guardian identische Loginidentitäten bzw. Konflikte. Lassen Sie diese Einstellung bei der ersten Migration aktiv; vergleichen Sie betroffene Einträge vor einem erneuten Import.

TOTP kann als unterstütztes Base32-Secret oder otpauth-URI übernommen werden. Nicht unterstützte Parameter werden abgelehnt. Prüfen Sie Anzahl und Stichproben nach dem Import. Vor erneutem Import ein Backup erstellen.

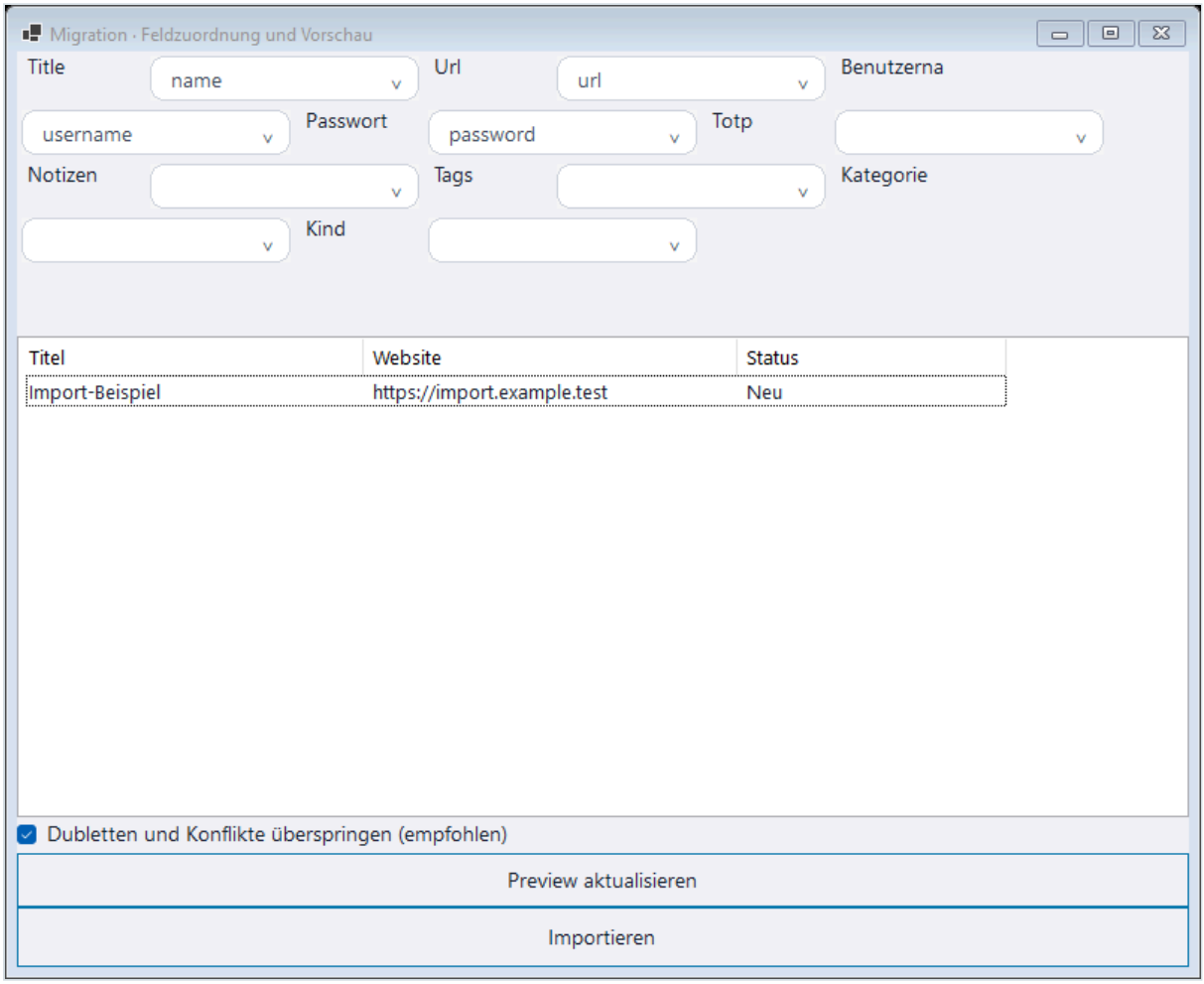


Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Importvorschau sicher übernehmen

1. Vor der Migration eine verschlüsselte Kopie des Ziel-Tresors anlegen.
2. Quellformat auswählen und gegebenenfalls dessen Kennwort und zusätzliche Schlüsseldatei angeben.
3. Feldzuordnung und Vorschau prüfen. Nach Änderungen „Vorschau aktualisieren“ verwenden.
4. Dubletten und Konflikte zunächst überspringen. Anzahl und Meldungen kontrollieren.
5. Nach Übernahme Stichproben prüfen und die ursprüngliche Quelle vorerst unverändert behalten.

> CSV und viele JSON-/XML-Exporte enthalten Klartextgeheimnisse. Guardian liest keine Browserprofile direkt aus. Proprietäre Komplettarchive anderer Anbieter werden nicht pauschal unterstützt.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

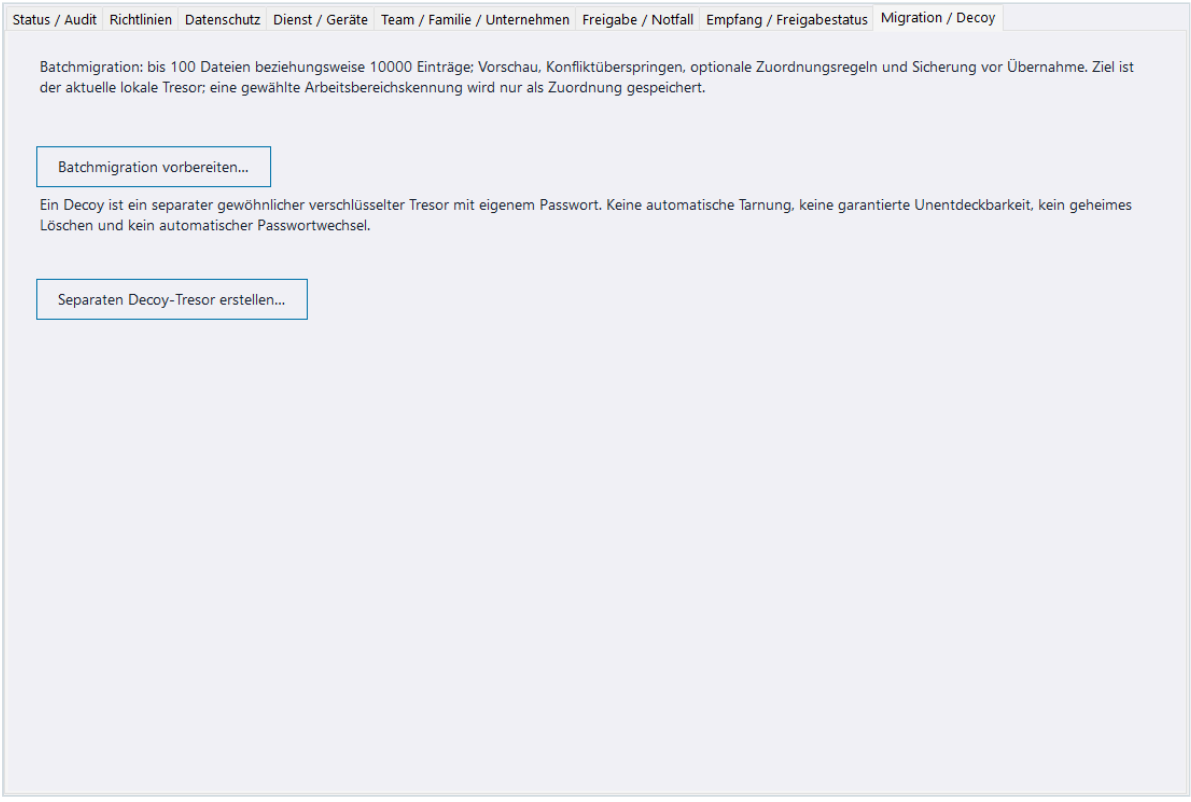
Batchmigration und Zuordnung (Pro)

Unter Migration / Decoy können bis 100 CSV-, JSON-, XML- oder KDBX-Dateien mit insgesamt 10000 Zeilen vorbereitet werden. KDBX-Passwort und gegebenenfalls Schlüsseldatei werden interaktiv abgefragt. JSON-Zuordnungsregeln verbinden Zielfelder mit Quellspalten. Unzugeordnete Felder bleiben erhalten. Der Bericht enthält Mengen und Feldnamen, keine Feldwerte; prüfen Sie daher auch sensible Spaltenbezeichnungen vor dem Teilen.

Historische Versionen können ausdrücklich nur aus neu importierten Einträgen entfernt werden. Quellen und bestehende Einträge bleiben erhalten. Konflikte werden übersprungen. Vor Übernahme wird eine neue verschlüsselte Sicherung angelegt. Ein nach der Vorschau geänderter Tresor erfordert eine neue Vorschau. Eine gewählte Arbeitsbereichskennung ist eine Zuordnung, kein Upload.

1. Pro-Sicherheitszentrale über Inventar oder Lifecycle öffnen und Migration / Decoy wählen.
2. Batchmigration vorbereiten, Quellen und optionale Zuordnungsregeln auswählen.
3. Vorschau und Konflikte prüfen; bei zwischenzeitlicher Tresoränderung erneut vorschauen.
4. Zusätzliche verschlüsselte Sicherung anlegen und erst dann übernehmen.

> Ein Arbeitsbereichsbezug ist eine lokale Zuordnung, kein automatischer Upload. Historienbereinigung betrifft nur neu importierte Einträge. Berichte enthalten Mengen und Feldnamen; auch Spaltennamen können sensibel sein.

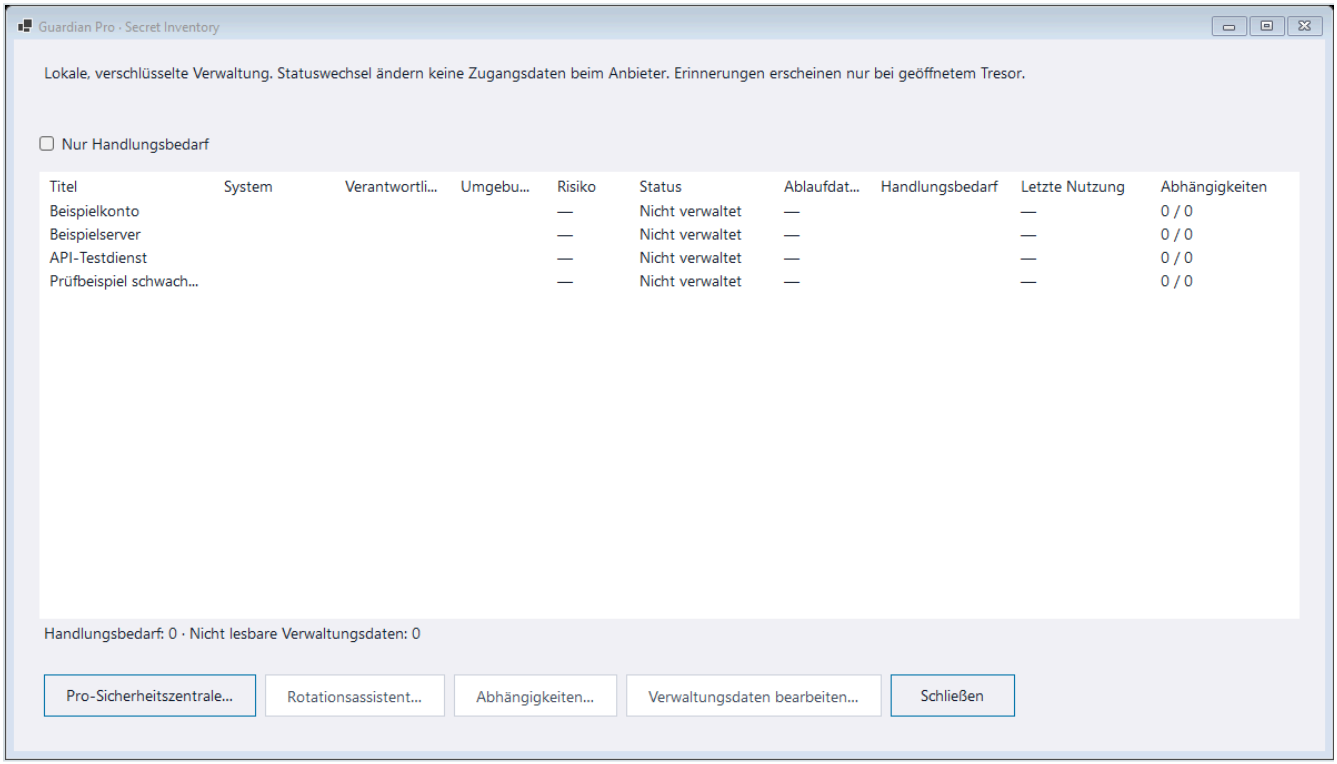


Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Secret Inventory (Pro)

Werkzeuge → Secret Inventory öffnet die lokale Übersicht. Wählen Sie einen Eintrag und Verwaltungsdaten bearbeiten. Zweck, System, Verantwortlicher, Umgebung, Risiko und ein optionales Ablaufdatum werden im verschlüsselten Tresor gespeichert. Die letzte Nutzung stammt aus Guardians lokaler Nutzungsaufzeichnung und ist keine vom Anbieter bestätigte Aktivität. Nicht verwaltete Einträge werden ausdrücklich so angezeigt.

Zum Bearbeiten wird die bestehende, signierte Guardian-Pro-Berechtigung erneut geprüft. Nach Lizenzende bleiben vorhandene Daten in der Übersicht lesbar und über verschlüsselte Backups oder KDBX exportierbar. Die CSV-Ausgabe enthält diese Zusatzdaten nicht. Der Pro-Editor verändert keine Zugangsdaten beim Anbieter.



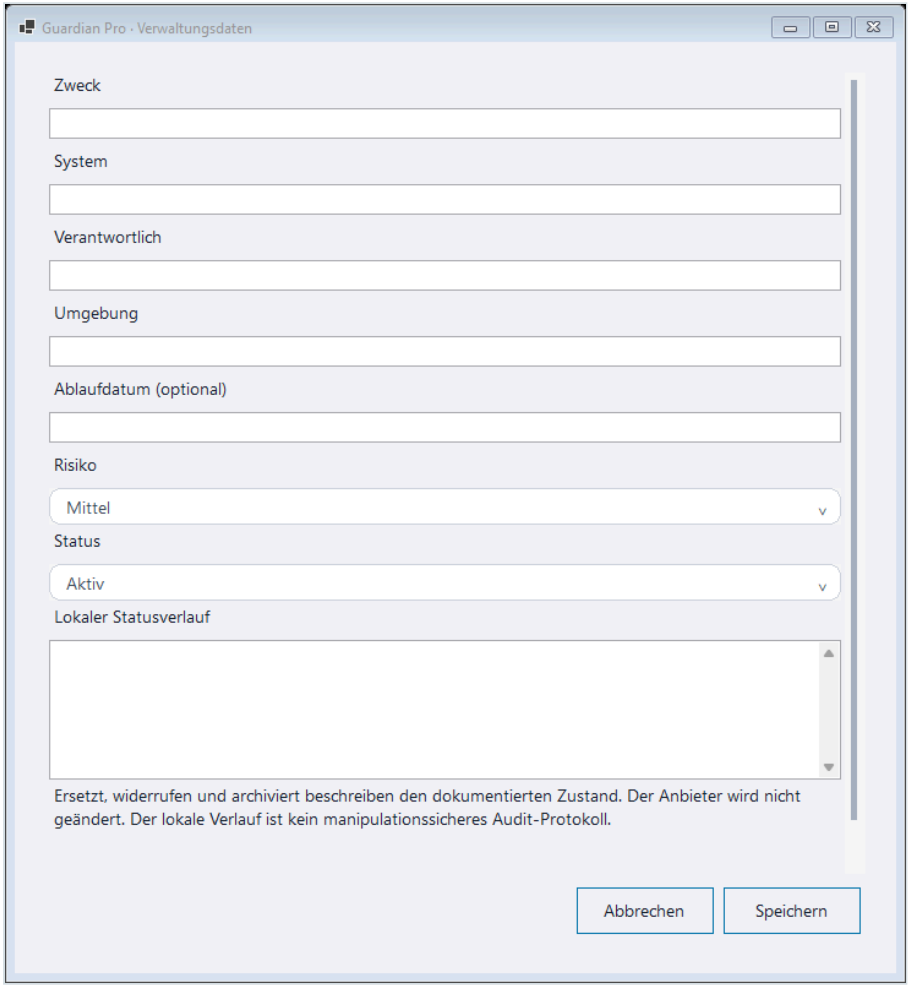
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Verwaltungsdaten bearbeiten

1. Im Inventar einen Eintrag wählen und „Verwaltungsdaten bearbeiten“ öffnen.
2. Zweck, System, verantwortliche Person, Umgebung, Risiko und optionales Ablaufdatum eintragen.
3. Status bewusst wählen und speichern.
4. Nach Änderungen auf neue oder erledigte Lifecycle-Hinweise achten.

Die lokale letzte Nutzung ist kein bestätigter Login beim Anbieter. Verwaltungsfelder werden verschlüsselt im Tresor aufbewahrt; sie ändern keine externen Zugänge.

> Vorhandene Metadaten bleiben nach Ende einer Pro-Berechtigung lesbar. AGV-Backup und unterstützter KDBX-Export sind die umfassenden Übertragungswege; CSV erhält diese Daten nicht vollständig.



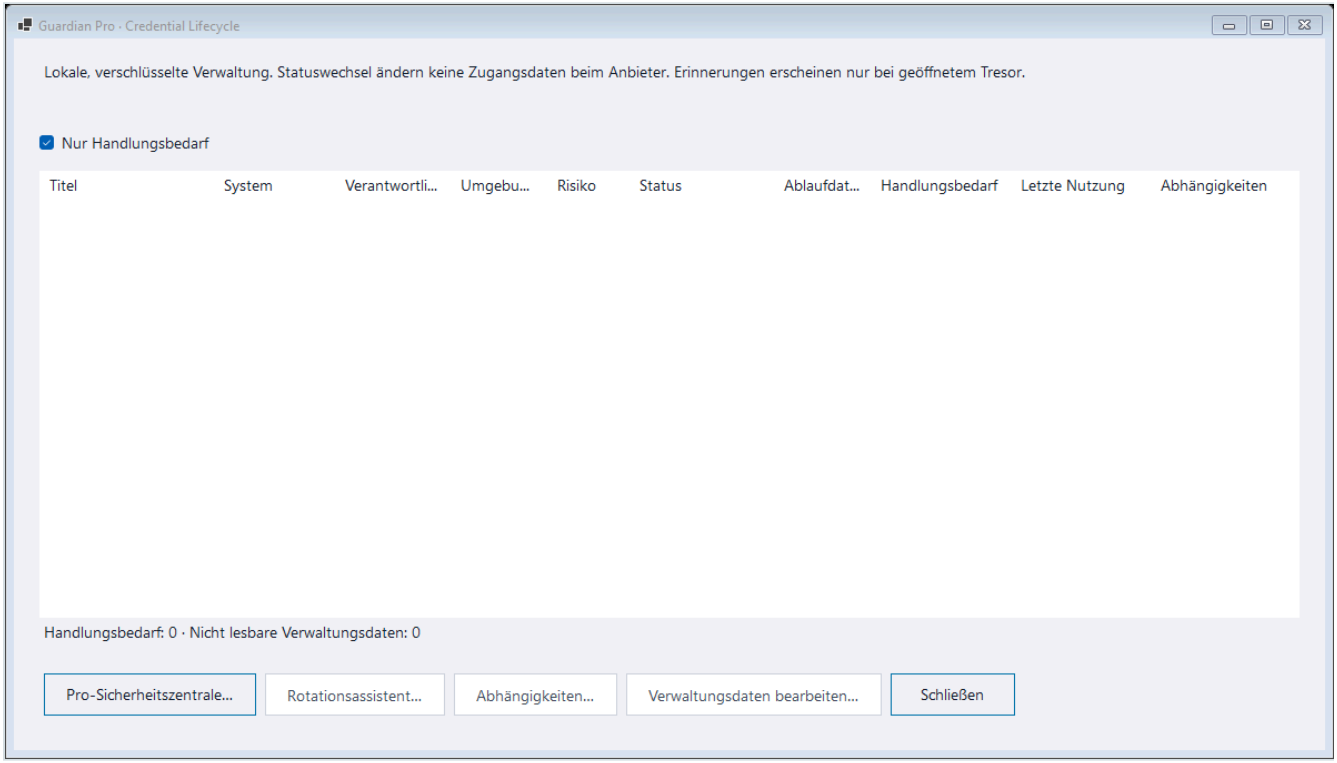
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Credential Lifecycle und Erinnerungen

Werkzeuge → Credential Lifecycle zeigt standardmäßig Einträge mit Handlungsbedarf. Ein Ablaufdatum innerhalb von 30 Tagen oder der Status Erneuerung fällig führt zu einem Hinweis. Bei geöffnetem Tresor erscheint die Anzahl zusätzlich in der Statusleiste. Es gibt keine Hintergrundüberwachung bei geschlossenem Guardian und keine E-Mail- oder Betriebssystembenachrichtigung. Datumsgrenzen beziehen sich auf das lokale Kalenderdatum.

Aktiv und Erneuerung fällig können ineinander wechseln. Ersetzt oder widerrufen kann nur noch archiviert werden. Archivierte Einträge werden nicht automatisch reaktiviert oder gelöscht. Für ein tatsächlich neues Zugangsmittel legen Sie einen neuen Eintrag an. Änderungen beim Anbieter müssen Sie selbst durchführen und anschließend dokumentieren.

Der lokale Verlauf protokolliert Statuswechsel und Zeitpunkte. Er ist kein manipulationssicherer oder externer Auditnachweis. Frühere Angaben bleiben in der verschlüsselten Eintragshistorie.



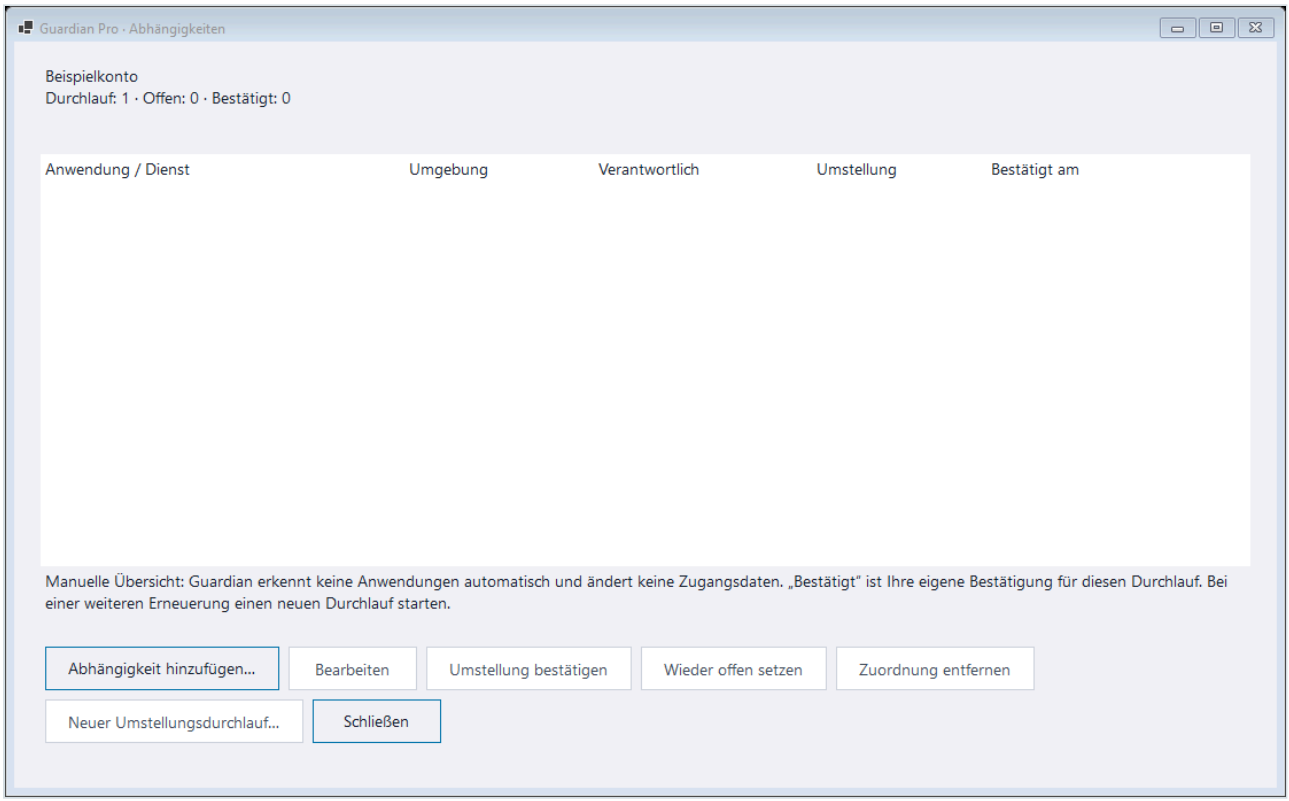
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Abhängigkeiten dokumentieren

Werkzeuge → Secret Inventory oder Credential Lifecycle öffnen. Einen Zugang auswählen und Abhängigkeiten anklicken. Mit Abhängigkeit hinzufügen erfassen Sie eine Anwendung oder einen Dienst, optional Umgebung, Verantwortlichen und Hinweise. Es findet keine automatische Erkennung statt. Speichern legt die Zuordnung verschlüsselt im Tresor ab.

Jede neue oder geänderte Zuordnung ist zunächst offen. Stellen Sie den Zugang beim jeweiligen Dienst selbst um und prüfen Sie die Funktion. Erst danach Umstellung bestätigen anklicken. Diese manuelle Bestätigung erhält ein Datum und gilt nur für den aktuellen Durchlauf; Guardian prüft das externe System nicht. Wieder offen setzen hebt die Bestätigung auf. Wenn ein weiterer Passwort- oder Schlüsselwechsel ansteht, starten Sie einen neuen Umstellungsdurchlauf. Alle Zuordnungen sind dann wieder offen; vorherige Bestätigungen bleiben in der Eintragshistorie. Der Durchlauf startet nicht automatisch bei Passwortänderungen.

Offene Zuordnungen erscheinen unter Nur Handlungsbedarf in Credential Lifecycle, auch ohne Ablaufdatum. Zuordnung entfernen löscht nur diese Beziehung, niemals den Zugang oder das Konto beim Anbieter. Ohne gültige Pro-Lizenz bleiben die vorhandenen Angaben lesbar und über KDBX oder verschlüsselte Backups exportierbar. CSV enthält diese Zusatzdaten nicht.

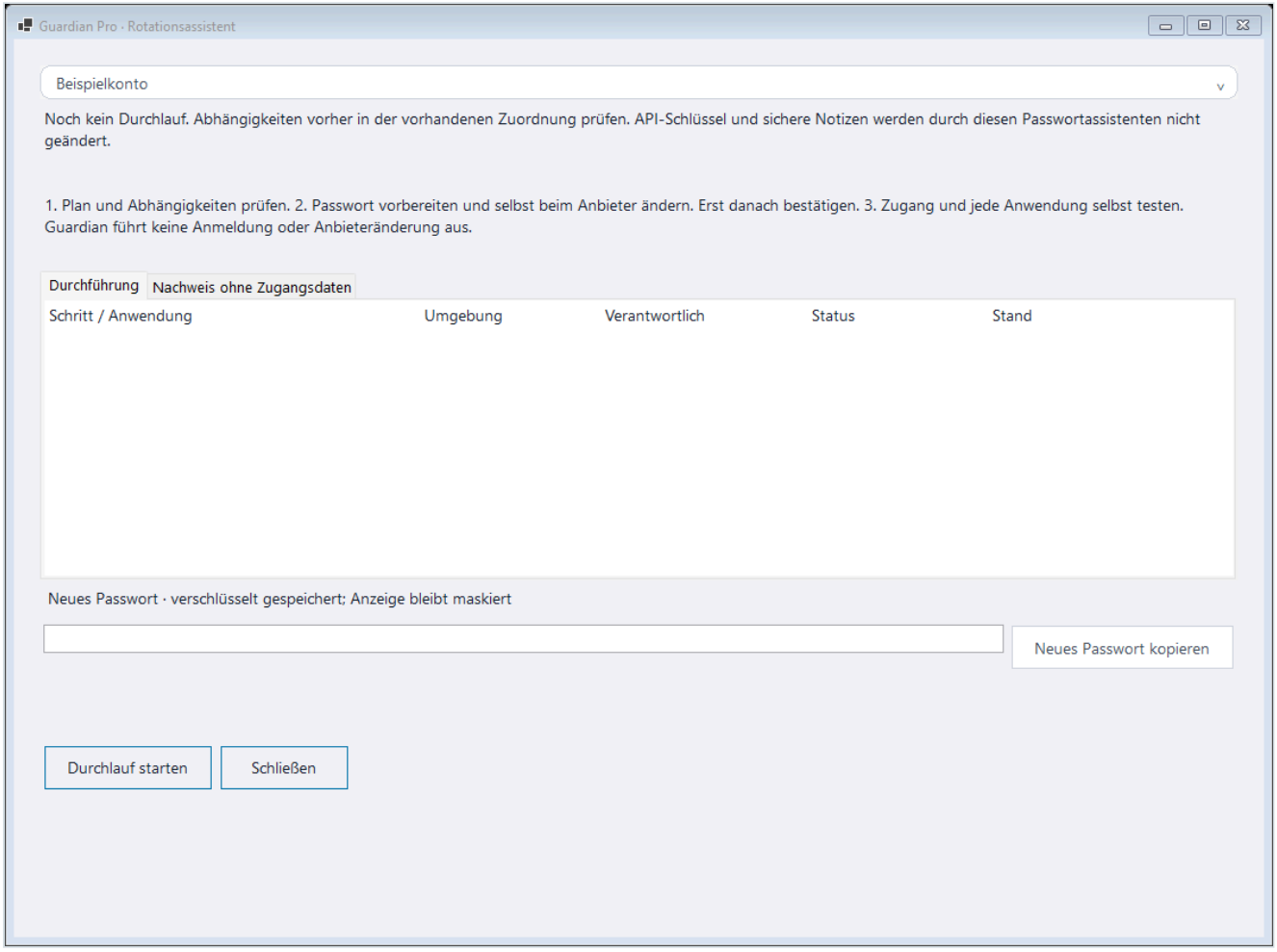


Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Rotation vorbereiten (Pro)

1. Im Inventar oder Lifecycle betroffene Einträge wählen und den Rotationsassistenten öffnen.
2. Abhängigkeiten prüfen und Durchlauf starten. Bestätigungen gelten für diesen Durchlauf.
3. Für Login-, Server- oder WLAN-Passwörter einen Kandidaten vorbereiten. Für API-Schlüssel einen tatsächlich vom Anbieter neu ausgegebenen Wert verwenden.
4. Der Kandidat bleibt zunächst verschlüsselt im Plan und ersetzt noch nicht das gespeicherte Zugangspasswort.
5. Änderung beim Anbieter selbst durchführen und erst nach Erfolg ausdrücklich bestätigen.

> Guardian erzeugt keine nutzbaren API-Schlüssel fremder Anbieter und meldet sich nicht automatisch an. Wenn extern bereits geändert wurde, bei einem lokalen Fehler nicht unbedacht einen neuen Wert erzeugen.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

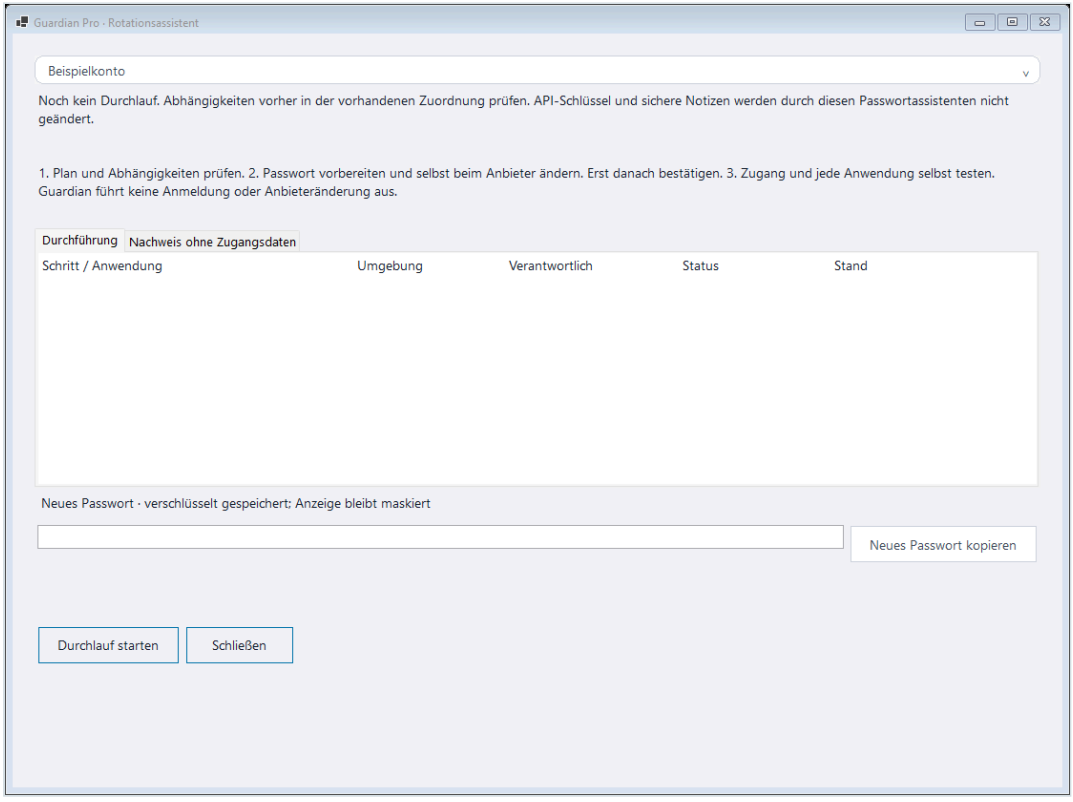
Rotation prüfen und abschließen

Der Rotationsassistent unterstützt Login, Server, WiFi und API-Key. Für API-Schlüssel übernehmen Sie einen vom Anbieter neu ausgegebenen Wert im maskierten Eingabefeld. Guardian erzeugt keine funktionierenden API-Schlüssel fremder Dienste. Neue Werte bleiben zunächst nur als verschlüsselter Kandidat im Plan. Die eingestellte Pro-Mindestlänge gilt bei neuen Vorbereitungen.

Ändern beziehungsweise erstellen Sie den Zugang beim Anbieter selbst und bestätigen Sie die erfolgreiche Umstellung ausdrücklich. Danach stellen Sie jede abhängige Anwendung um und bestätigen einen eigenen Funktionstest. Erst wenn alle Schritte geprüft sind, prüfen Sie beim Anbieter, dass das alte Passwort nicht mehr funktioniert beziehungsweise widerrufen den alten API-Schlüssel. Bestätigen Sie „Alten Zugang deaktiviert bestätigen…“ und schließen Sie den Durchlauf ab.

Guardian führt weder Provideränderung noch Widerruf automatisch aus. Scheitert ein erneuter Test, wird eine vorhandene Stilllegungsbestätigung ungültig. Verschlüsselte Historie bleibt zur Wiederherstellung erhalten. Frühere 1.4-Pläne können übernommen werden; ein in 1.5 weiterbearbeiteter Plan ist in 1.4 nicht mehr zur Bearbeitung geeignet.

> Unterbrechung schließt nur die Ansicht; der verschlüsselte Plan bleibt erhalten. „Vor Änderung verwerfen“ ausschließlich verwenden, wenn beim Anbieter noch nichts geändert wurde. Bei unklarem Stand zuerst die tatsächliche Gültigkeit klären.



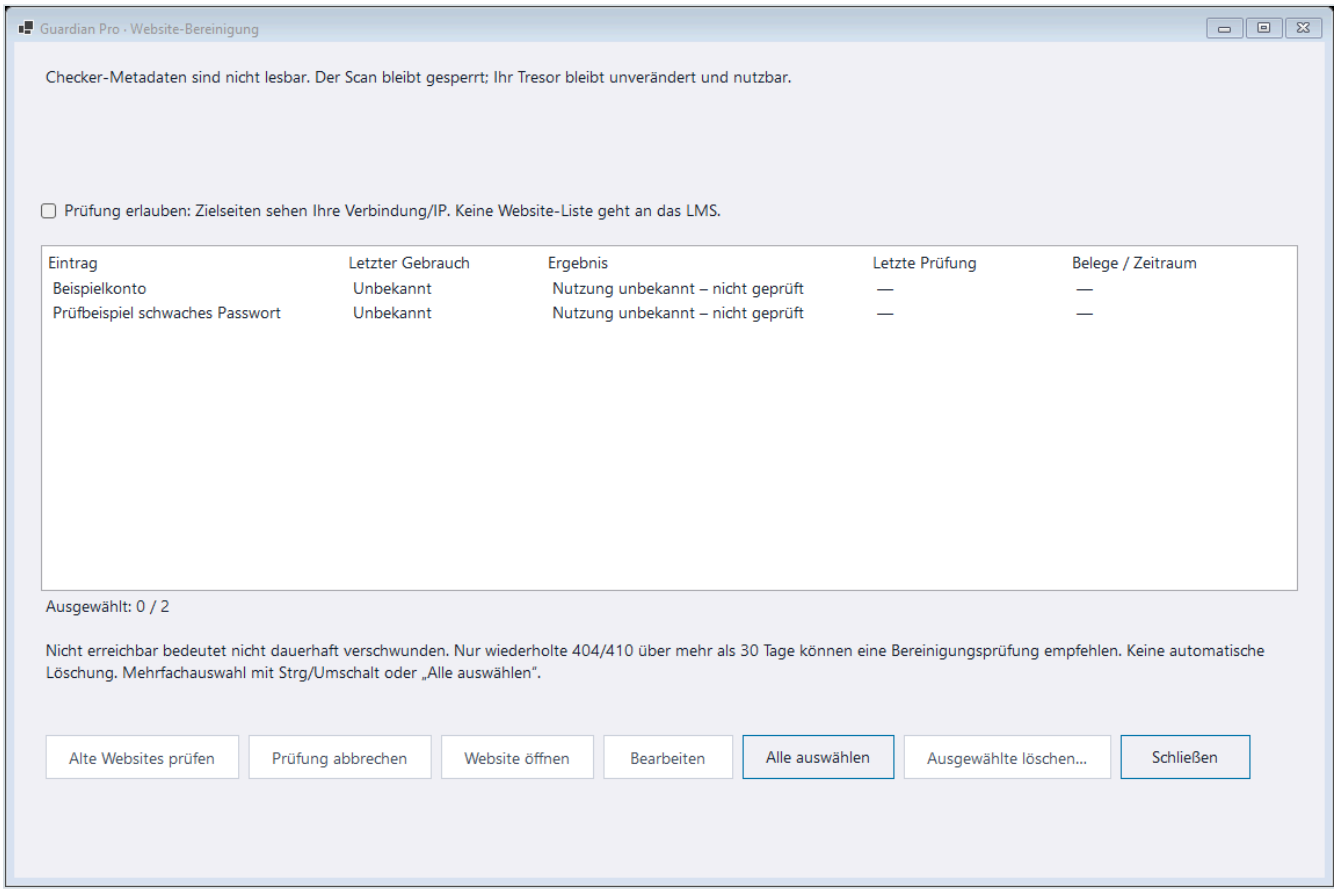
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Website-Bereinigung (Pro)

Werkzeuge → Website-Bereinigung: Zuerst Prüfung erlauben aktivieren, danach Alte Websites prüfen. Es werden ausschließlich öffentliche HTTPS-Origins mit bekanntem letztem Gebrauch vor mehr als zwei Jahren geprüft. Einträge mit unbekannter oder neuerer Nutzung werden mit einem Grund übersprungen. Fortschritt und Abschluss nennen geprüfte Websites, unbekannte Nutzung, neuere Nutzung, unsichere Ziele und die 24-Stunden-Pause. Ein leerer Prüflauf ist kein Fehler. Prüfung abbrechen oder Entfernen des Einwilligungshakens stoppt weitere Anfragen.

Mehrere Einträge mit Strg/Umschalt oder Alle auswählen markieren. Ausgewählte löschen öffnet eine gemeinsame Bestätigung. Standard ist genau eine zusätzliche verschlüsselte Sicherung für die gesamte Auswahl. Alternativ ist Entfernen ohne zusätzliche Sicherungsdatei nach ausdrücklicher Bestätigung möglich. Vorhandene Sicherungen und die automatische letzte Tresorversion (.bak) können frühere Daten weiterhin enthalten. Dies ist kein sicheres Vernichten aller Kopien. Beim Anbieter werden keine Konten gelöscht.

Einzelne Verbindungsfehler sind keine Löschbegründung. Nur wiederholte 404/410 über mehr als 30 Tage können eine manuelle Bereinigungsprüfung empfehlen; es wird nie automatisch gelöscht.



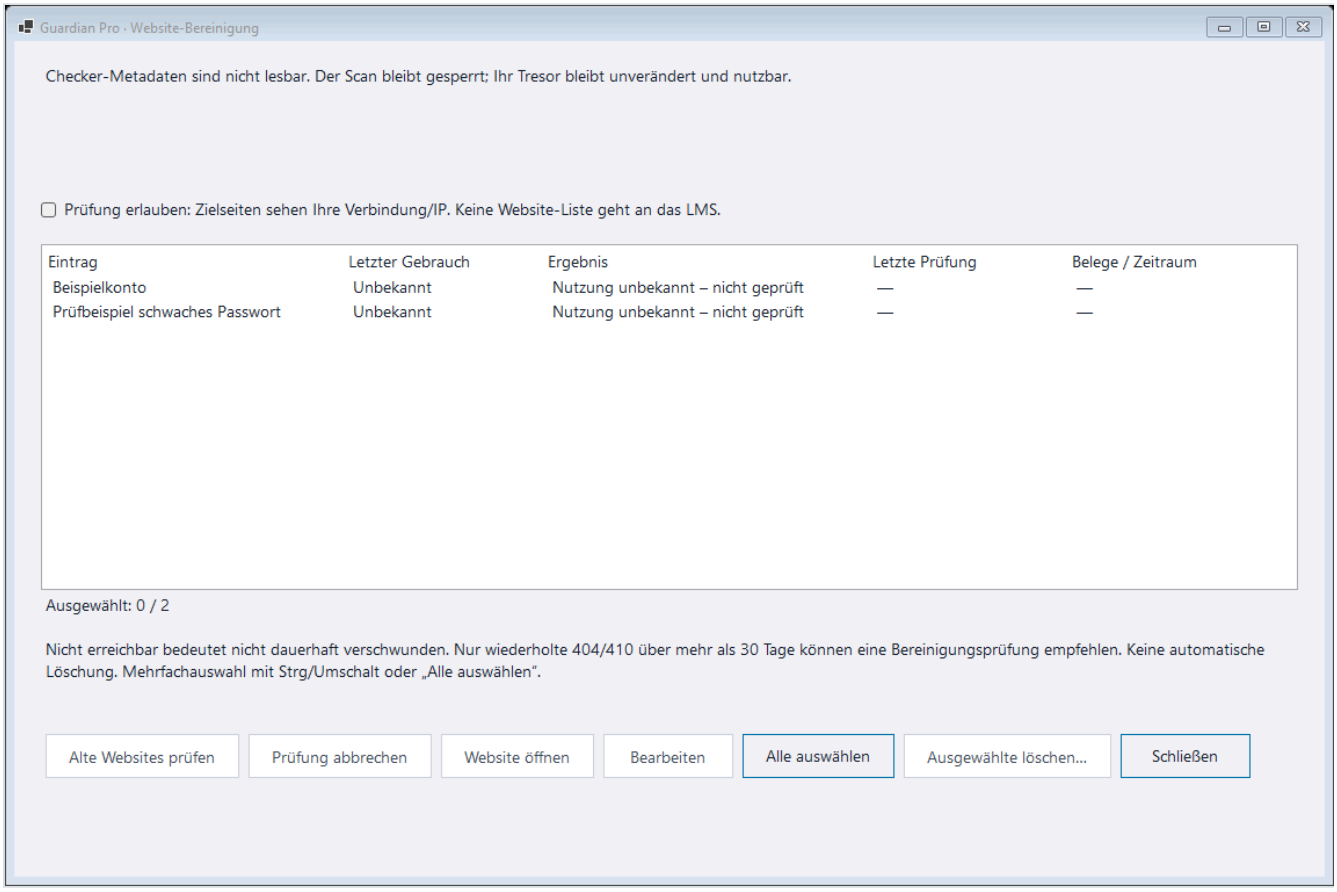
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Bereinigung bewusst entscheiden

Unbekannte letzte Nutzung bedeutet nicht „alt“. Geprüft werden nur geeignete öffentliche HTTPS-Ziele mit bekanntem Gebrauch vor mehr als zwei Jahren. Ziele sehen Ihre Verbindung. Die 24-Stunden-Pause und Abbruchmeldungen sind zu beachten.

1. Befund, wiederholte Beobachtungen und Zeitraum lesen.
2. Passende Einträge mit Strg / Umschalt oder „Alle auswählen“ markieren.
3. „Ausgewählte löschen“ und die gemeinsame Bestätigung prüfen. Standardmäßig eine zusätzliche verschlüsselte Sicherung für die gesamte Auswahl erstellen.
4. Nur bewusst bestätigen. Eine Entfernung ohne zusätzliche Datei ist eine ausdrückliche Entscheidung, keine empfohlene Grundeinstellung.

> Ein einzelner Fehler ist keine Löschbegründung. Wiederholte 404/410 über mehr als 30 Tage können nur eine manuelle Prüfung empfehlen. Guardian löscht keine Anbieter-Konten und vernichtet keine früheren Kopien.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

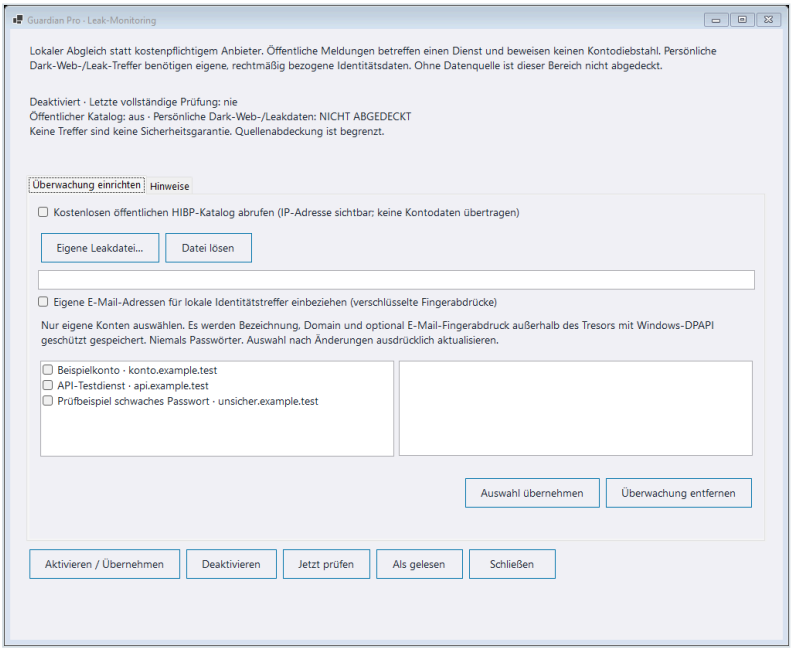
Leak-Monitoring einrichten (Pro)

Öffnen: Werkzeuge → Sicherheitsprüfung → Leak-Monitoring. Eigene Konten links auswählen und Auswahl übernehmen. Optional E-Mail-Fingerabdrücke ausdrücklich einbeziehen. Rechts stehen die tatsächlich überwachten Einträge. Passwörter und Masterpasswort werden nicht gespeichert oder übertragen. Die Überwachung speichert Domain, Bezeichnung und optionale E-Mail-Fingerabdrücke außerhalb des Tresors, geschützt mit Windows-DPAPI. Das ist eine bewusste zusätzliche Datenspeicherung für die Prüfung bei gesperrtem Tresor.

Datenquellen: Optionaler kostenloser öffentlicher Have-I-Been-Pwned-Katalog (CC BY 4.0, https://haveibeenpwned.com/). Dabei wird die IP-Adresse sichtbar, jedoch keine Domain, E-Mail-Adresse oder Passwortliste übermittelt. Der Dienstkatalog beweist keine persönliche Betroffenheit. Persönliche Treffer werden ausschließlich lokal anhand einer eigenen rechtmäßig bezogenen JSON-Leakdatei abgeglichen. Ohne eigene Identitätsdaten ist persönliches Dark-Web-Monitoring NICHT ABGEDECKT. Guardian sammelt keine gestohlenen Zugangsdaten und besitzt keine vollständige Dark-Web-Datenbank. Der eigene Datenbestand muss spätestens alle sieben Tage aktualisiert werden; sonst erscheint ein Fehler statt einer Entwarnung. Format: docs/help/monitoring-feed-format.md.

Aktivieren / Übernehmen: bewusste Freigabe für Hintergrundprüfung und Windows-Autostart. Prüfung alle sechs Stunden; bei Fehlern Wiederholung mit wachsendem Abstand (15 Minuten bis sechs Stunden). Der stille Prozess läuft unabhängig vom geschlossenen Guardian und gesperrten Tresor im angemeldeten Windows-Konto. PC ausgeschaltet oder Windows abgemeldet: Nachholen beim nächsten Anmelden. Windows darf Mitteilungen unterdrücken; Hinweise bleiben im Dialog gespeichert. Keine Kontodetails auf dem Sperrbildschirm.

> Die Aufnahme zeigt bewusst deaktiviertes Monitoring und keine eingerichtete persönliche Datenquelle. „Nicht abgedeckt“ ist keine Entwarnung.

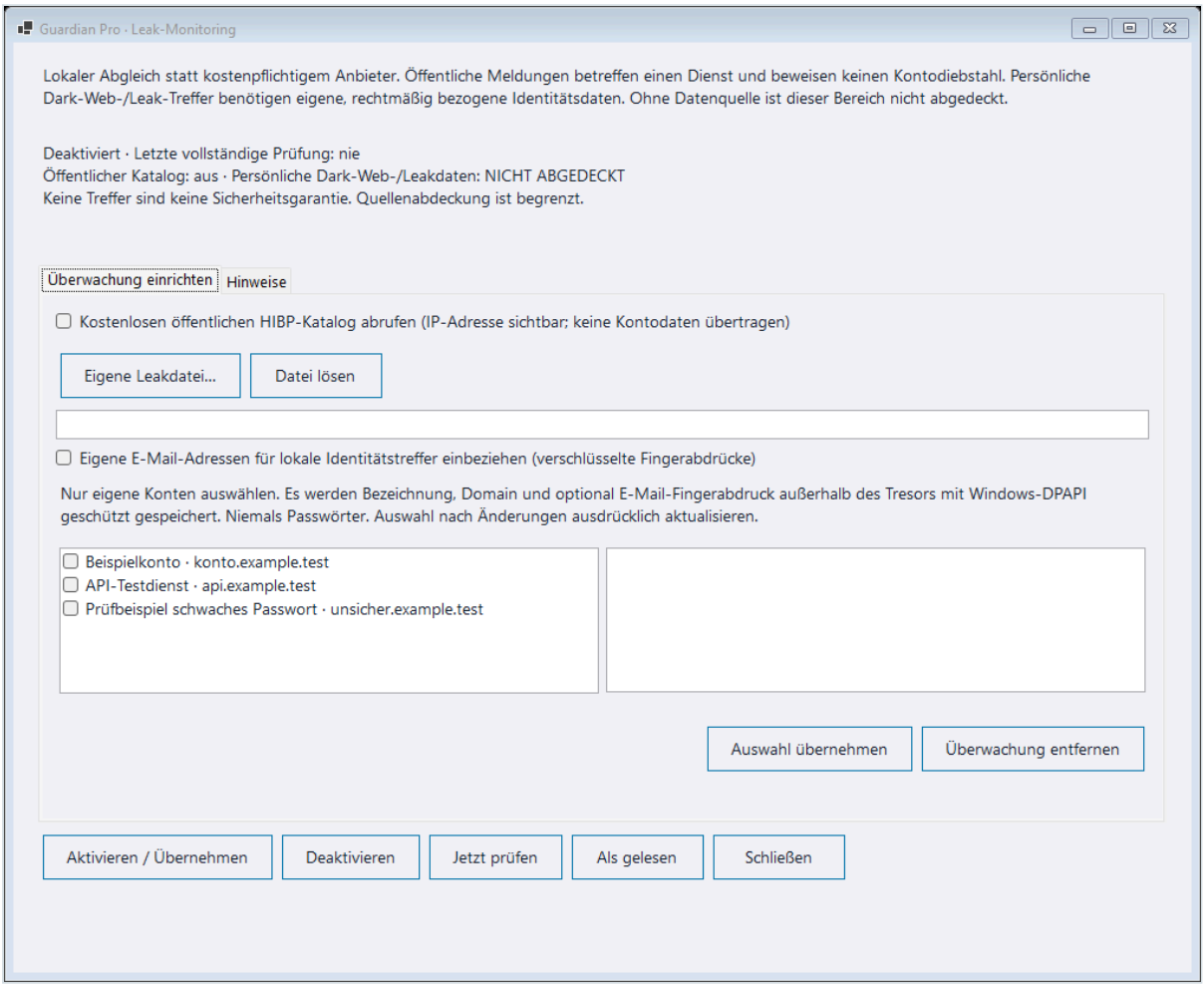


Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Monitoring im Hintergrund

Nach Kontoänderungen Auswahl ausdrücklich aktualisieren. Einträge rechts entfernen löscht die zusätzliche Überwachungsregistrierung und zugehörige Hinweise; der Tresoreintrag bleibt erhalten. Deaktivieren stoppt Prüfungen und entfernt den Autostart. Bereits gespeicherte Hinweise bleiben lesbar, auch ohne aktive Pro-Lizenz. Lizenzfehler pausieren nur neue Monitoringprüfungen. Die vorhandene manuelle Passwortprüfung bleibt unverändert. Keine Treffer sind keine Sicherheitsgarantie. Keine Passwörter werden automatisch geändert und keine Webseiten oder Browseragenten gestartet.

> Dieses freiwillig aktivierte Monitoring ist vom normalen Lifecycle zu unterscheiden: Lifecycle-Erinnerungen arbeiten nur bei geöffnetem Tresor. Monitoring führt keine automatischen Anbieteränderungen aus.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Persönliche Quellen und Abdeckung

Persönliches Monitoring braucht eigene rechtmäßig bezogene Quellen. Öffentliche Vorfallmeldungen belegen betroffene Dienste, keine persönliche Betroffenheit. Guardian enthält keine vollständige Datenbank fremder Zugangsdaten.

Die lokale Quelldatei muss der mitgelieferten Beschreibung `docs/help/monitoring-feed-format.md` entsprechen. Die Daten müssen aktuell sein; spätestens nach sieben Tagen ist eine Aktualisierung nötig. Ein veralteter oder unlesbarer Bestand ist kein erfolgreicher negativer Test.

Ausdrücklich gewählte Domains und optionale SHA-256-Fingerabdrücke der eigenen Identitäten werden Windows-geschützt registriert. Keine Passwörter und kein vollständiger Tresor werden für diese Registrierung gespeichert.

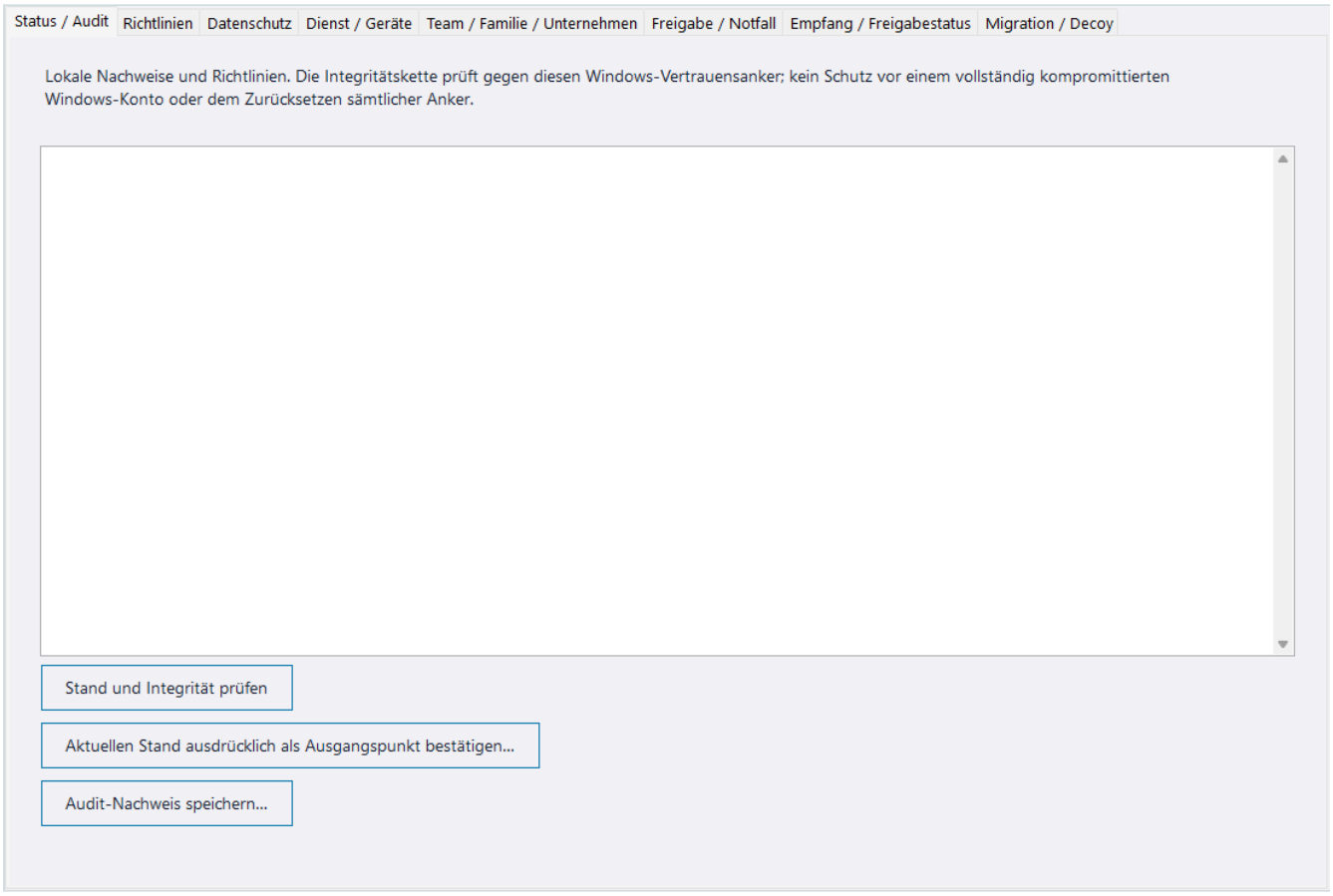
> Nach Kontoänderungen die Auswahl ausdrücklich aktualisieren. Fingerabdrücke bleiben schutzwürdige personenbezogene Daten. Keine Treffer und fehlende Abdeckung sind unterschiedliche Zustände.

Sicherheitszentrale: Status und Integrität

Öffnen Sie Secret Inventory oder Credential Lifecycle und dort „Pro-Sicherheitszentrale…“. Status / Audit prüft die verschlüsselte Tresordatei gegen einen ausdrücklich bestätigten lokalen Vertrauensanker. Ohne Ausgangspunkt wird keine verifizierte Integrität behauptet. Bestätigen Sie nur einen zuvor geprüften Stand als Ausgangspunkt.

Nachfolgende Speichervorgänge werden mit einer authentifizierten Ereigniskette verknüpft. Eine abweichende Datei bleibt als Abweichung sichtbar. Der exportierbare Nachweis enthält Kennungen und Status, keine Passwörter. Ein vorhandener Geräteschlüssel signiert den Export; dessen Fingerabdruck ist unabhängig zu prüfen. Vollständiges Zurücksetzen aller lokalen Anker oder ein kompromittiertes Windows-Konto wird damit nicht ausgeschlossen.

Unter Richtlinien legen Sie Mindestlänge neuer Zugänge und einen Erneuerungshinweis fest. Die Vorgaben ändern keine Zugänge beim Anbieter. Datenschutz erklärt die Übertragungszwecke und zeigt maximal 1000 aufgezeichnete Netzwerkaufrufe ohne deren Inhalte. Fehlende Protokolle sind kein Beweis, dass nichts übertragen wurde.

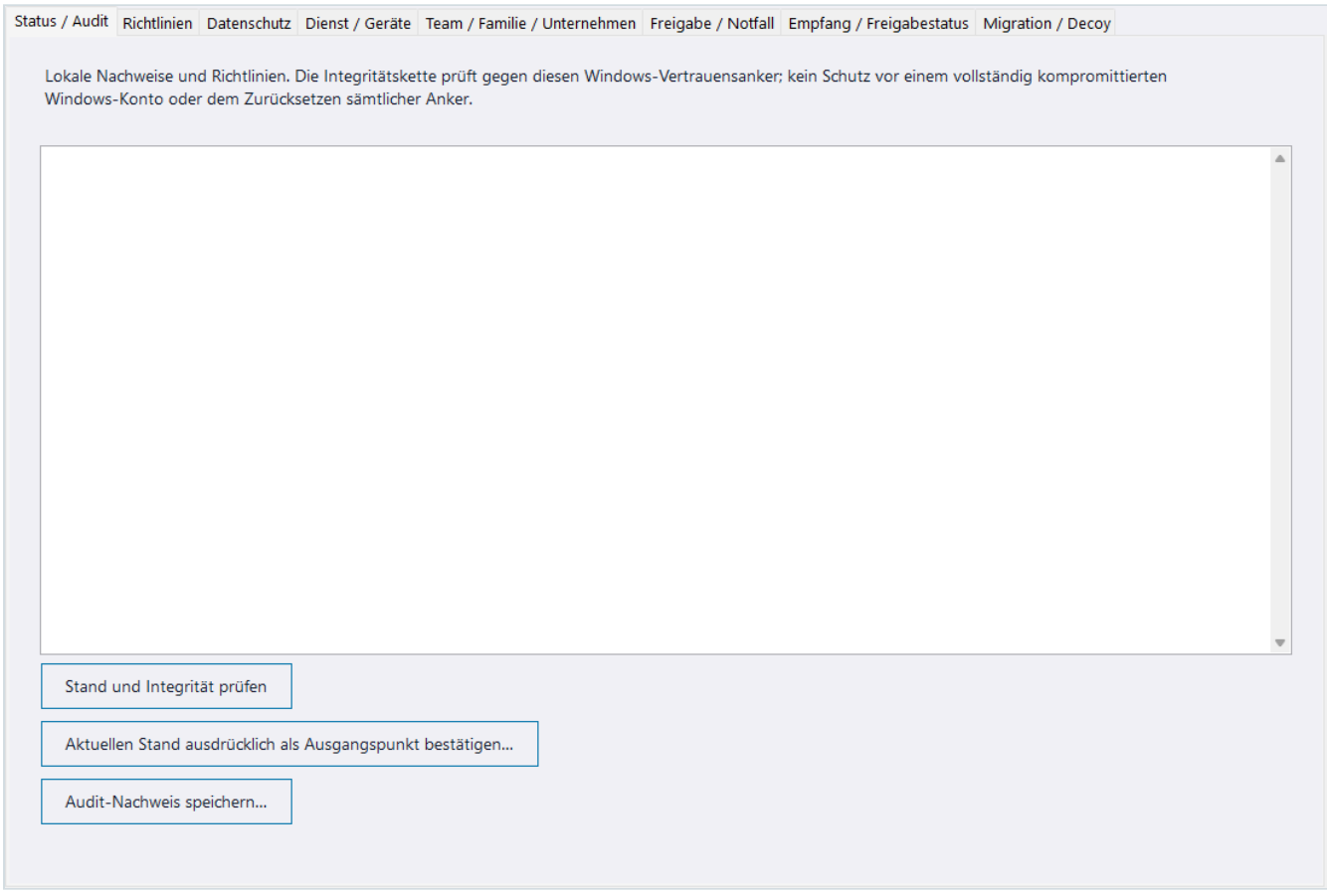


Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Audit-Nachweise ausgeben

1. Nur einen zuvor geprüften Tresorstand ausdrücklich als Ausgangspunkt bestätigen.
2. Stand und Integrität gegen diesen lokalen Anker prüfen.
3. „Audit-Nachweis speichern“ und eine neue JSON-Datei wählen.
4. Kennungen und Status vor Weitergabe prüfen; bei vorhandenem Geräteschlüssel den Fingerabdruck unabhängig vergleichen.
5. Frühere Nachweise nach einem Vorfall erhalten. Eine spätere neue Ausgangspunktbestätigung erklärt frühere Abweichungen nicht für ungeschehen.

> Lokale authentifizierte Ereignisketten sind keine zugesagte rechtliche Revisionssicherheit. Ein kompromittiertes Windows-Konto oder vollständiges Zurücksetzen aller lokalen Anker wird nicht ausgeschlossen.

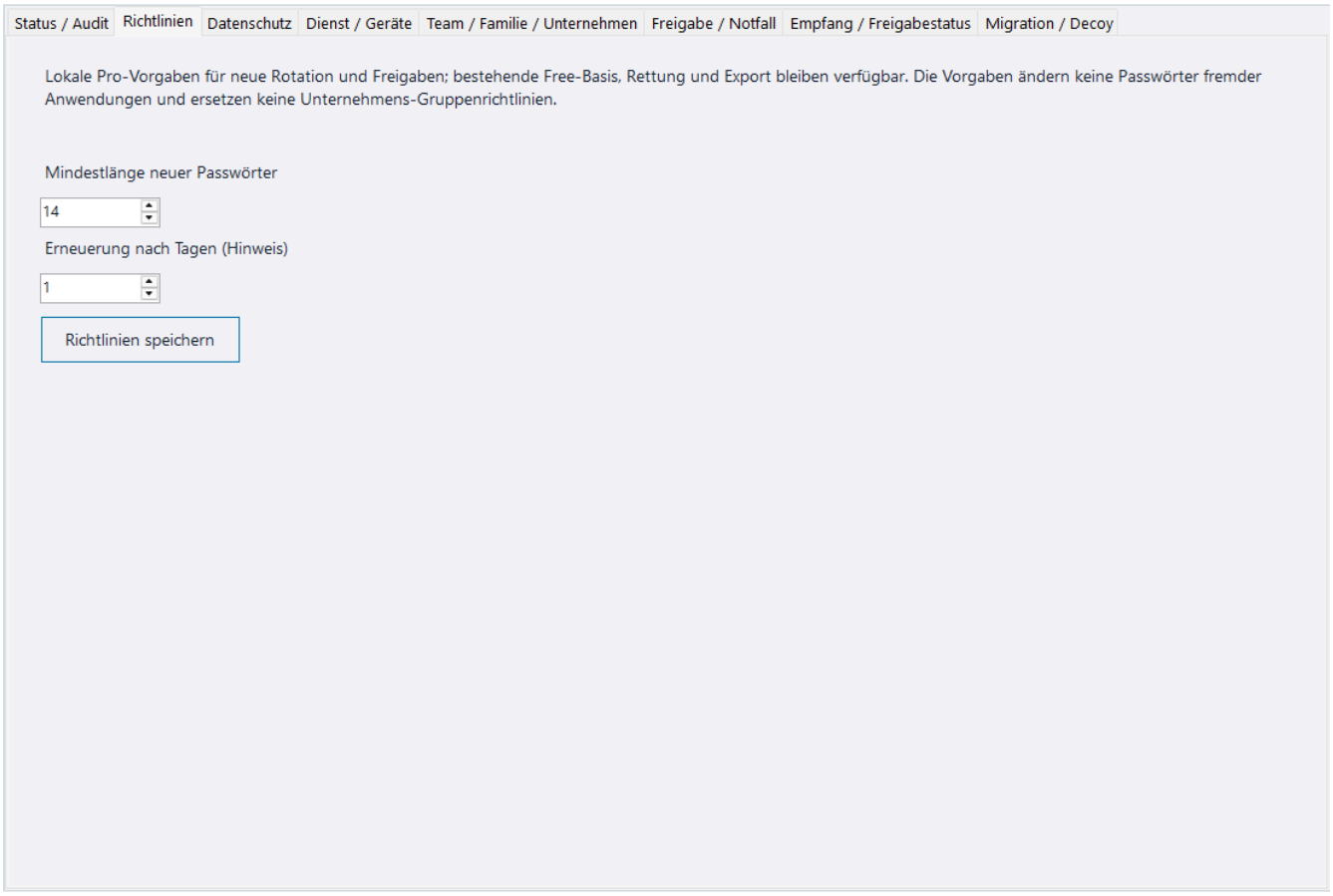


Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Lokale Pro-Richtlinien

1. In der Sicherheitszentrale das Register Richtlinien wählen.
2. Mindestlänge neu vorbereiteter Passwörter und Erneuerungshinweis in Tagen festlegen.
3. „Richtlinien speichern“ bestätigen.
4. Bei neuen Rotationen und Freigaben die Vorgaben beachten; vorhandene externe Zugänge bei Bedarf manuell ändern.

> Dies sind lokale Vorgaben, keine zentralen Unternehmens-Gruppenrichtlinien. Die Einstellung ändert keine Passwörter beim Anbieter und ersetzt keinen Funktionstest.



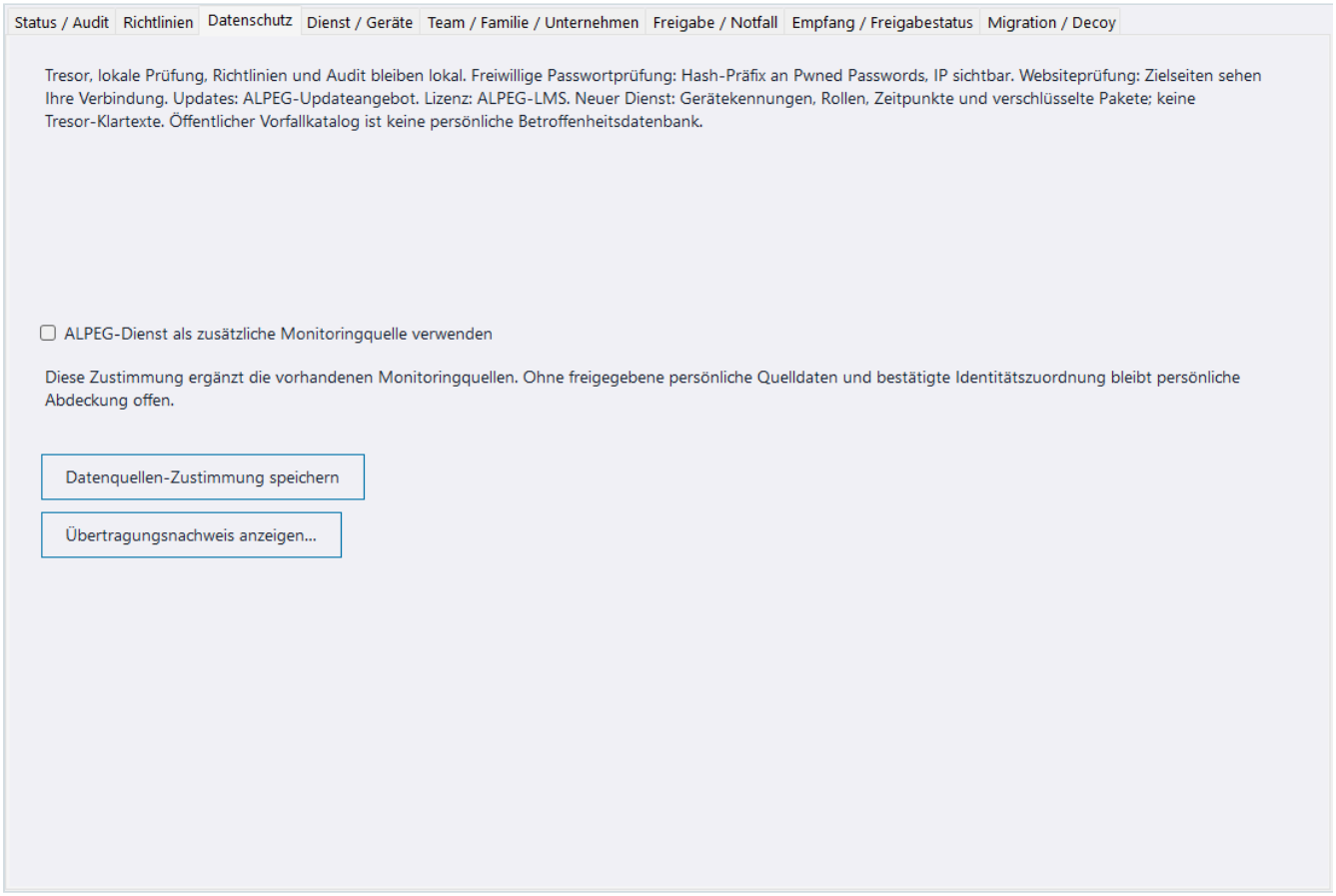
Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Datenschutz und Übertragungen

Funktion	Übertragungszweck
Lokaler Tresor	Verschlüsselte lokale Daten; kein automatischer Tresorupload.
Passwortprüfung	Fünf Hashpräfix-Zeichen an Pwned Passwords; IP sichtbar.
Websiteprüfung	Verbindungen zu geeigneten öffentlichen HTTPS-Zielen.
Update / Lizenz	ALPEG-Updateangebot bzw. LMS-Anmeldung und Lizenznachweis.
Koordinationsdienst	Geräte, Rollen, Zeitpunkte und verschlüsselte Pakete.
Zusätzliches Monitoring	Nach Einwilligung ausgewählte Domains und Identitätsfingerabdrücke.

Der Übertragungsnachweis zeigt die letzten maximal 1.000 aufgezeichneten Aufrufe dieser Pro-Funktionen ohne Inhalte oder Zugangsdaten. Extern im Browser geöffnete Seiten werden nicht erfasst.

> HTTP-Antwort bedeutet nicht automatisch fachlichen Erfolg. Ein fehlender Eintrag beweist nicht, dass keine Übertragung stattgefunden hat.



Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

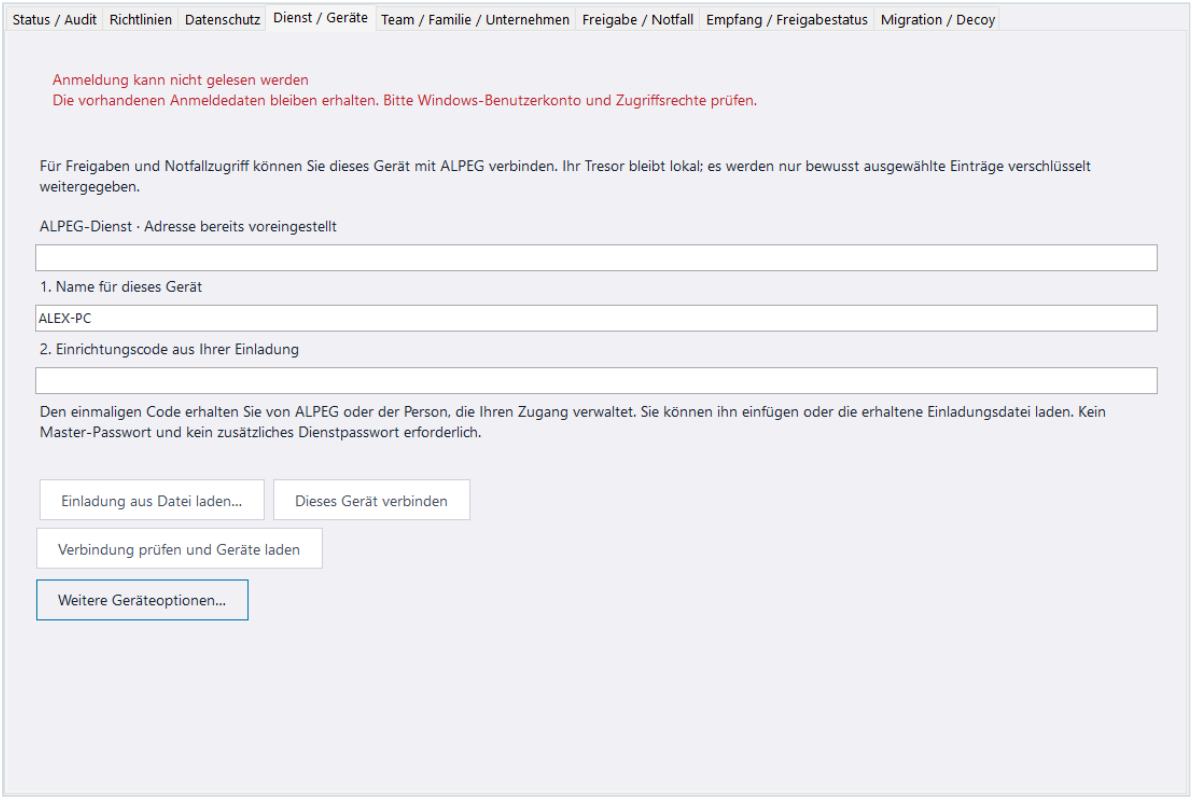
Koordinationsdienst und Geräte

Der eigene ALPEG-Dienst koordiniert Geräte, Rollen, Freigaben und Notfallfristen. Der Tresor bleibt lokal. Ein lokal gestarteter Testdienst ist kein öffentlich verfügbarer Produktivdienst. Für entfernten Betrieb ist eine vom Betreiber eingerichtete HTTPS-Adresse erforderlich. Tragen Sie unter Dienst / Geräte Adresse, Gerätebezeichnung und eine einmalige Einladung des Betreibers ein.

Privater Geräteschlüssel und Zugangstoken werden mit Windows-Datenschutz geschützt. Exportieren Sie ausschließlich das öffentliche Geräteprofil. Vergleichen Sie Gerätekennung und Schlüsselfingerabdruck über einen unabhängigen Kontakt, bevor Sie einem Gerät vertrauen. Ein Betreiber kann bis fünf aktive Geräte je Teilnehmer einladen. Gerätewiderruf sperrt den Dienstzugang und zugehörige zukünftige Paketabrufe, löscht jedoch keine lokalen Tresore.

1. Unter Dienst / Geräte freigegebene HTTPS-Adresse und Gerätebezeichnung prüfen.
2. Einmaligen Einrichtungscode aus der Einladung eingeben oder laden und Gerät verbinden.
3. Anschließend „Verbindung prüfen und Geräte laden“ verwenden. Bei bestehender Verbindung keinen neuen Einladungscode wiederholt benutzen.
4. Bei Bedarf ausschließlich das öffentliche Geräteprofil exportieren.

> LMS-Lizenzkonto und Koordinationsdienst sind getrennt. Die vorbelegte Adresse beweist keine erfolgreiche Verbindung. Die Beispielregister zeigen keinen produktiv verbundenen Dienst.



Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

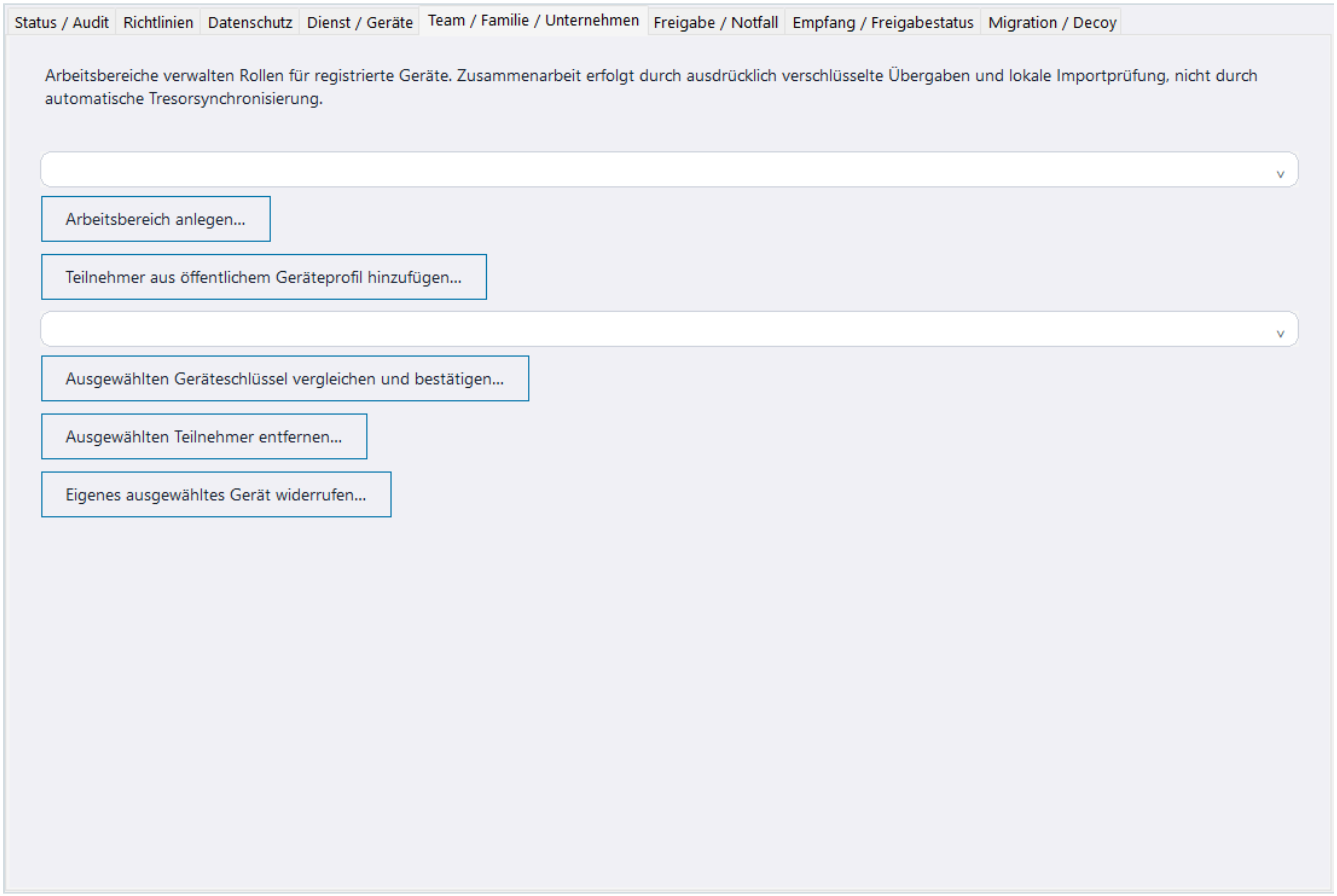
Gerätevertrauen und Widerruf

Vergleichen Sie Gerätekennung und Schlüsselfingerabdruck über einen unabhängigen Kontakt. Bestätigen Sie erst danach einen Empfängerschlüssel.

Gerätewiderruf sperrt den Dienstzugang und zukünftige Paketabrufe. Lokale Tresore und bereits entschlüsselte Kopien werden dadurch nicht gelöscht.

Lizenzplätze im LMS und Geräteeinladungen im Koordinationsdienst gehören zu unterschiedlichen Verwaltungsbereichen. Abmelden oder ein Dienstwiderruf gibt nicht automatisch einen Lizenzplatz frei.

> Bei unklarer Identität keine Freigabe erzwingen. Private Geräteschlüssel und Token nie als öffentliches Geräteprofil weitergeben.



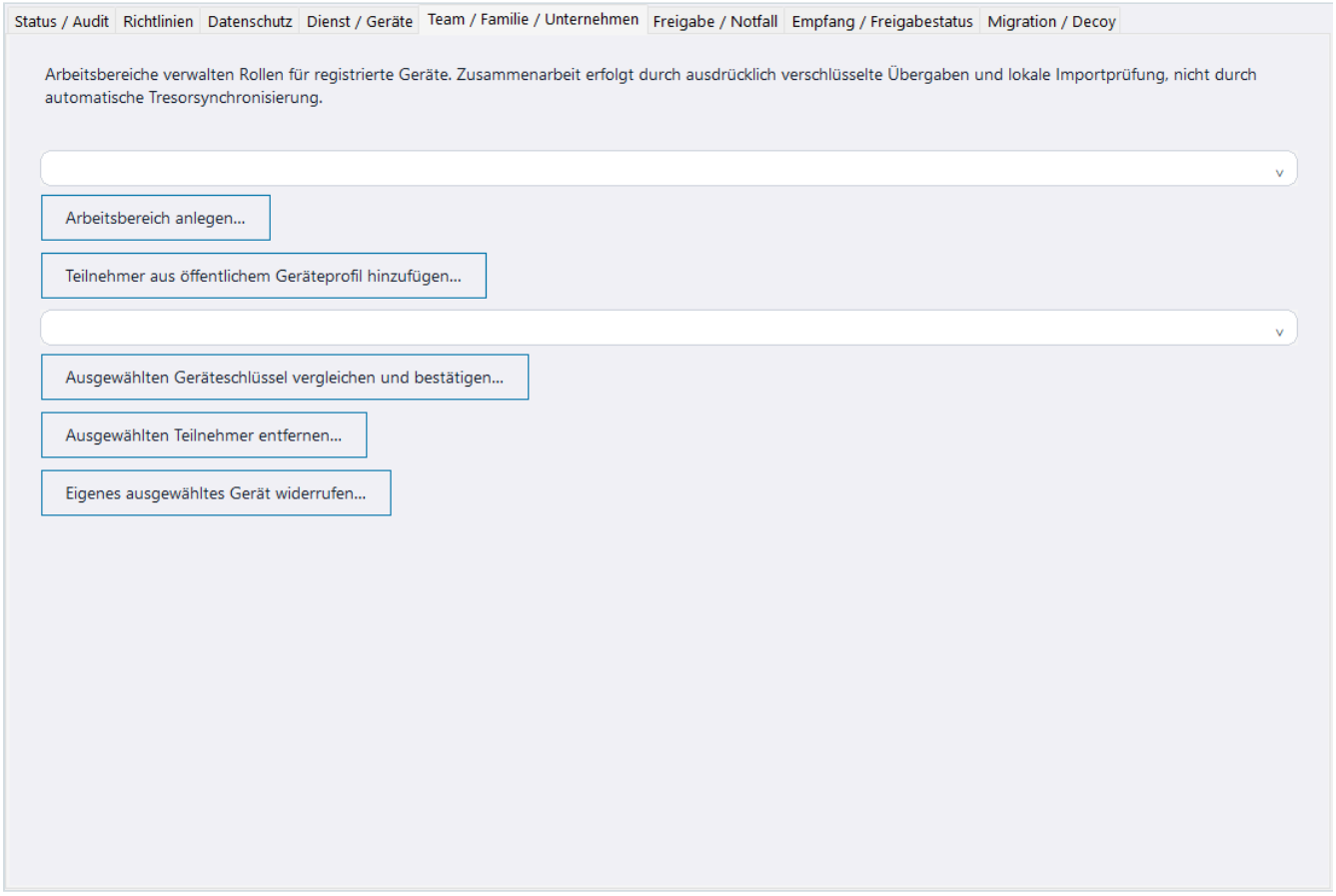
Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Arbeitsbereiche und Rollen

Rolle	Befugnis im Koordinationsdienst
viewer	Freigegebene Inhalte empfangen.
editor	Zusätzlich Inhalte freigeben.
admin	Teilnehmer und Freigaben verwalten.
owner	Zusätzlich Administratoren verwalten.

1. Arbeitsbereich auswählen oder anlegen.
2. Teilnehmer über ihr öffentliches Geräteprofil hinzufügen.
3. Geräteschlüssel unabhängig vergleichen und bestätigen.
4. Nicht mehr benötigte Teilnehmer und eigene alte Geräte bewusst entfernen bzw. widerrufen.

> Keine automatische gemeinsame Tresorsynchronisierung und keine vollständige zentrale Unternehmensverwaltung. Zusammenarbeit erfolgt durch ausdrücklich verschlüsselte Übergaben.



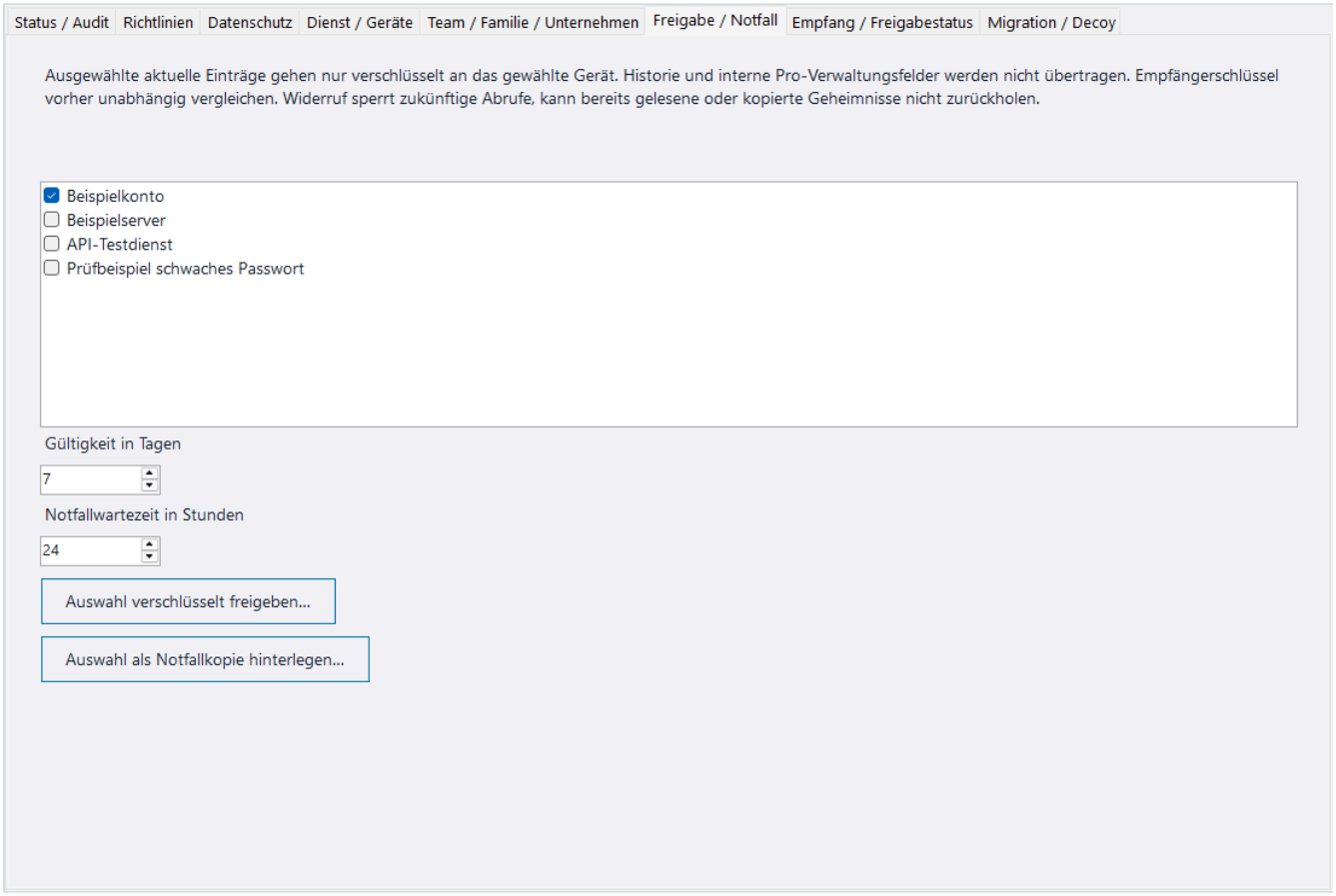
Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Verschlüsselte Einträge freigeben

1. Arbeitsbereich und unabhängig bestätigtes Empfängergerät wählen.
2. Unter Freigabe / Notfall nur benötigte aktuelle Einträge markieren.
3. Gültigkeit festlegen und „Auswahl verschlüsselt freigeben“ bestätigen.
4. Der Empfänger entschlüsselt lokal und prüft vor der Übernahme die Vorschau.
5. Nicht mehr benötigte Freigaben widerrufen.

Aktuelle Einträge, Anhänge und gewöhnliche Zusatzfelder werden Ende zu Ende verschlüsselt. Historien und interne Pro-Verwaltungsfelder bleiben von der Übertragung ausgeschlossen.

> Widerruf verhindert neue Abrufe, holt aber gelesene oder kopierte Geheimnisse nicht zurück. Bei Bedarf Zugangsdaten beim Anbieter ändern.

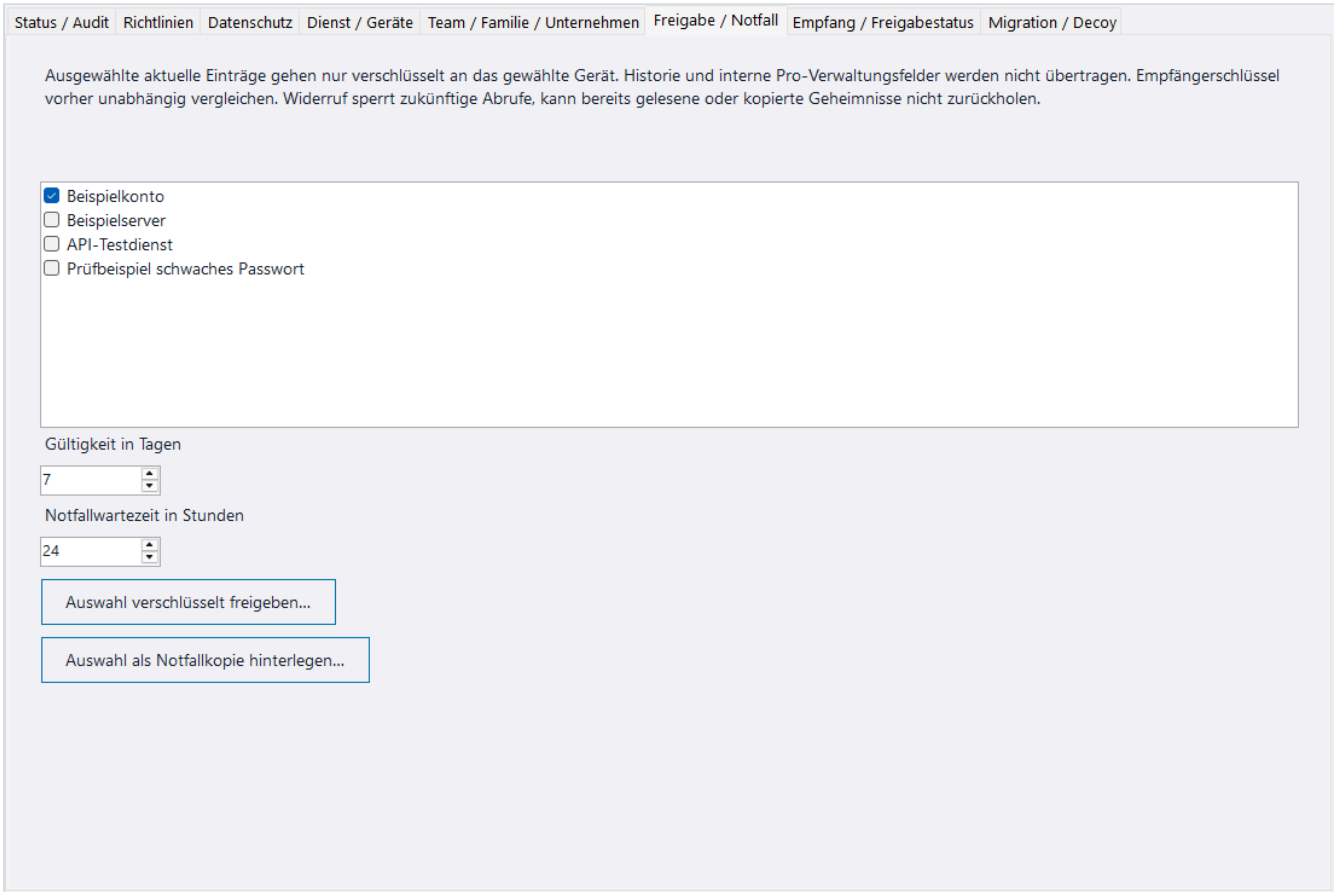


Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Notfallkopien und Wartefristen

1. Empfängergerät bestätigen, Einträge auswählen und Gültigkeit sowie Notfallwartezeit sinnvoll abstimmen.
2. „Auswahl als Notfallkopie hinterlegen“ bewusst bestätigen.
3. Der Empfänger fordert den Notfallzugriff an; die Wartefrist wird serverseitig kontrolliert.
4. Während der Frist kann der Absender widerrufen.
5. Nach Änderungen einen passenden neuen Stand hinterlegen und frühere Freigaben prüfen.

> Eine Notfallkopie ist ein ausdrücklich hinterlegter Stand, kein automatisch aktueller Tresor und keine Masterpasswort-Wiederherstellung. Fristen und Zugriffssteuerung benötigen einen korrekt betriebenen Dienst.

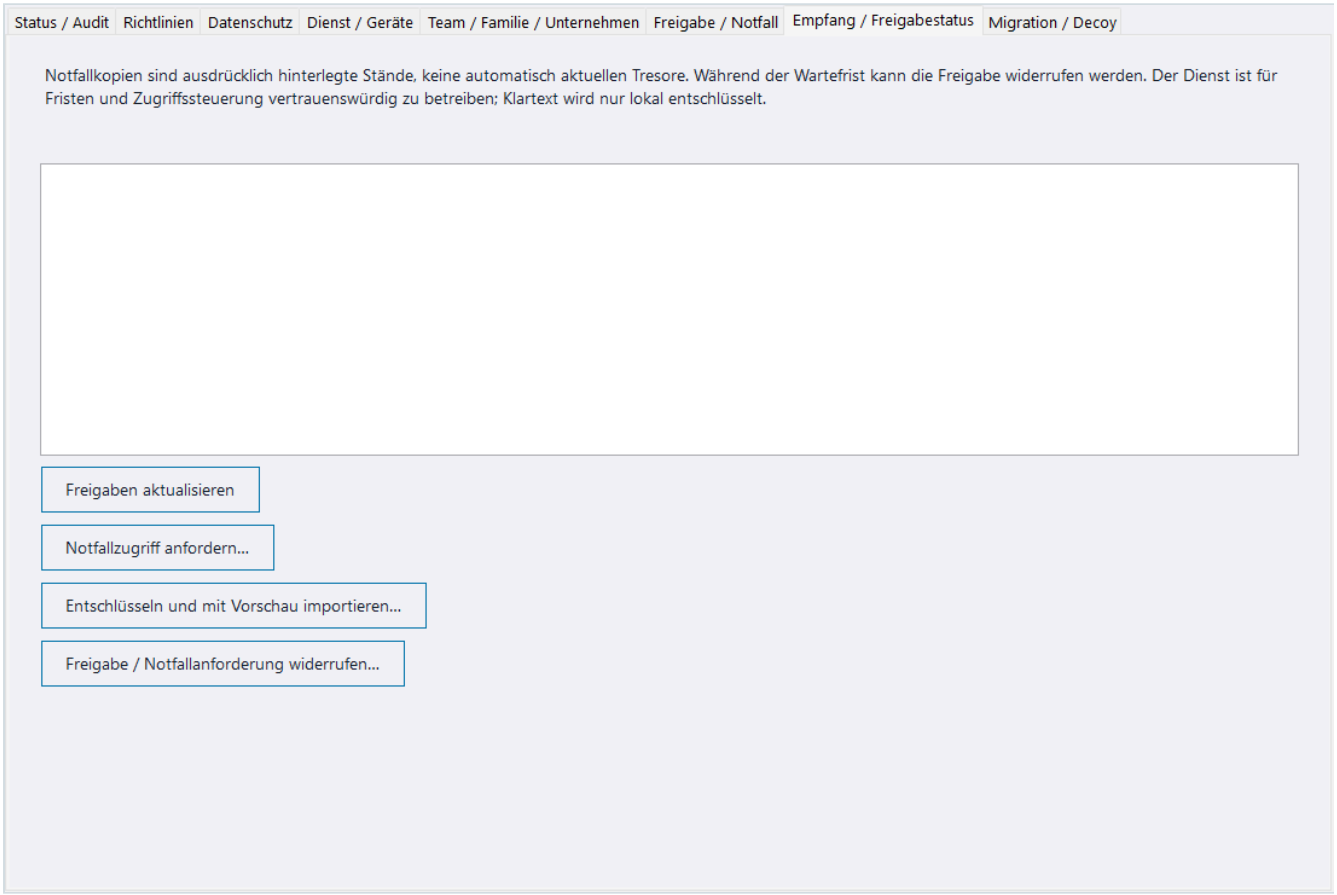


Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Empfang und Freigabestatus

1. Freigaben aktualisieren und bekannte Absenderidentität prüfen.
2. Bei Notfallkopien zunächst Zugriff anfordern und Wartefrist beachten.
3. „Entschlüsseln und mit Vorschau importieren“ wählen.
4. Zusätzliche verschlüsselte Sicherung anlegen, Vorschau und Konflikte prüfen.
5. Tatsächlich übernommene Inhalte im lokalen Tresor kontrollieren.

> Konflikte werden übersprungen. Empfangene Inhalte sind lokale Kopien und werden bei späteren Anbieteränderungen oder Widerrufen nicht automatisch aktualisiert.



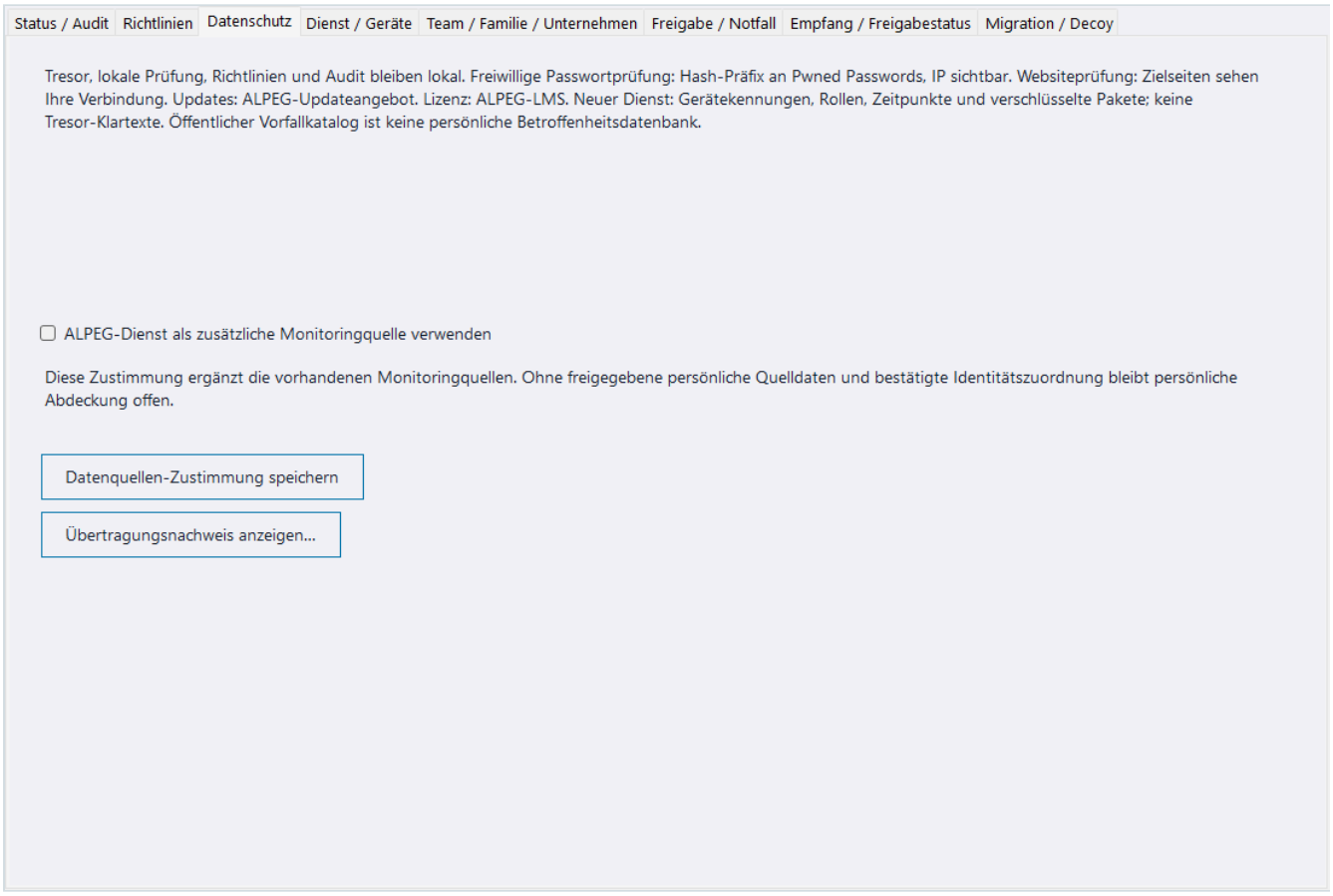
Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Zusätzliche Dienst-Monitoringquelle

Unter Datenschutz kann der ALPEG-Dienst zusätzlich als Monitoringquelle freigegeben werden. Das bestehende Leak-Monitoring muss ebenfalls aktiviert sein und ausdrücklich gewählte Konten überwachen. An den Dienst gehen Domains und SHA-256-Fingerabdrücke ausgewählter Identitäten, niemals deren Passwörter oder der gesamte Tresor. Fingerabdrücke sind weiterhin schutzwürdige personenbezogene Daten.

Der Betreiber führt eine eigene Vorfalldatenbank mit nachvollziehbaren Quellen und Importen. Öffentliche HIBP-Vorfallmeldungen belegen betroffene Dienste, aber keine persönliche Betroffenheit. Persönliche Daten dürfen nur aus entsprechend autorisierten Quellen importiert werden. Identitätsbesitz muss unabhängig geprüft und dem Teilnehmer ausdrücklich zugeordnet werden.

Ohne persönliche Quelldaten und bestätigte Zuordnung bleibt die persönliche Abdeckung ausdrücklich offen. Ein leerer Trefferbestand bedeutet keine Entwarnung. Der Entwicklungsbestand enthält öffentliche Vorfallmetadaten und keine persönlichen Leakzuordnungen. Bereits vorhandene Hinweise bleiben erhalten; zurückgezogene Quellen liefern keine neuen Treffer.



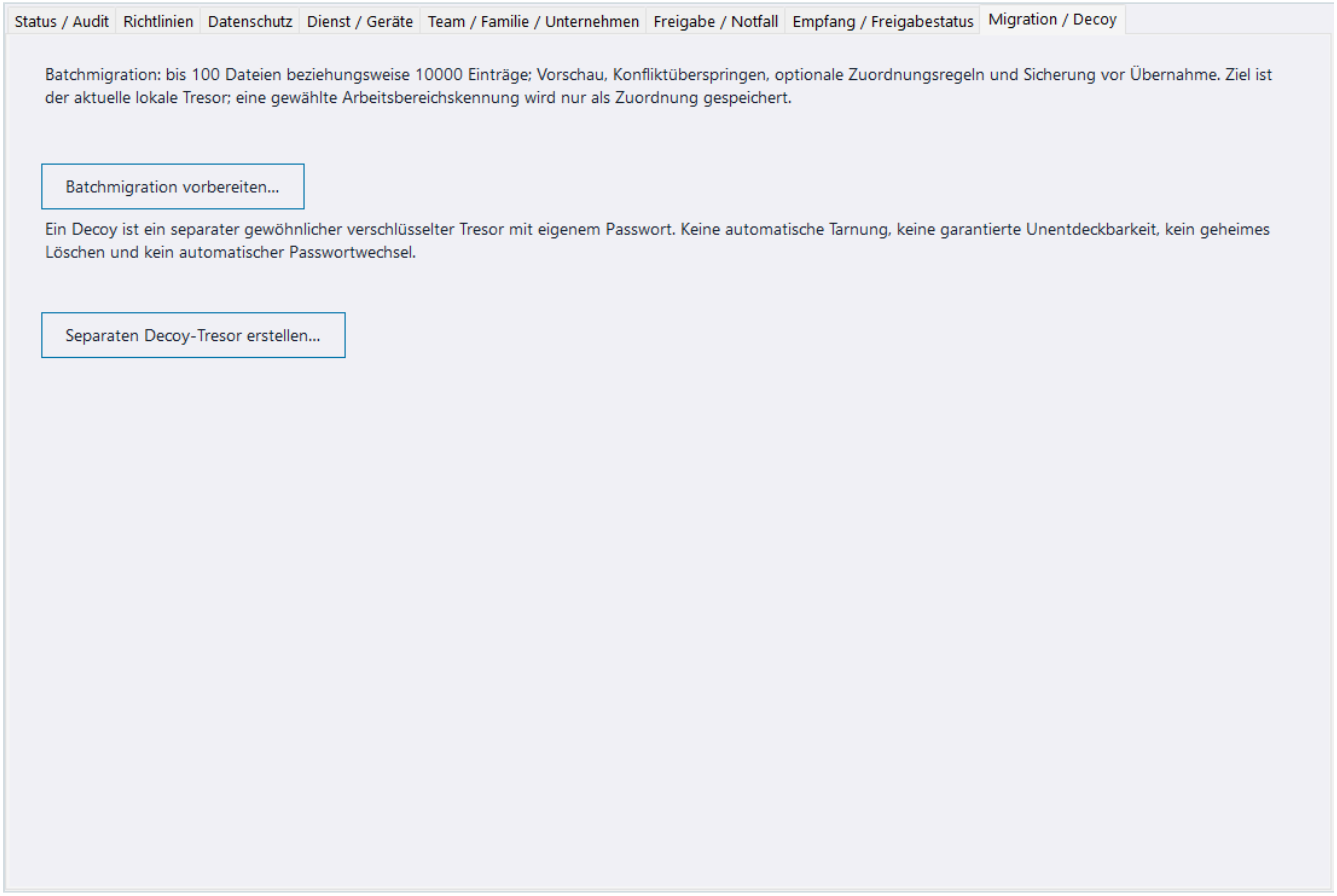
Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Separater Decoy-Tresor (Pro)

1. Unter Migration / Decoy „Separaten Decoy-Tresor erstellen“ wählen.
2. Eigenen neuen Dateipfad und eigenes starkes Masterpasswort verwenden.
3. Den erzeugten Tresor und seine separate Ablage prüfen.
4. Bei Bedarf über den normalen Öffnen-Weg dorthin wechseln.

Ein Decoy ist ein gewöhnlicher verschlüsselter Tresor. Er wird nicht automatisch verborgen oder anstelle des echten Tresors geöffnet.

> Keine garantierte Unentdeckbarkeit, kein heimliches Löschen und kein automatischer Passwortwechsel. Dies ist keine zugesagte Absicherung gegen Zwang oder kompromittierte Endgeräte.



Registeransicht ohne eingerichteten Dienst · synthetische Beispielumgebung

Konto und Pro-Lizenz aktivieren

1. Werkzeuge → Pro-Lizenz oder die Lizenzaktion in den Einstellungen öffnen.
2. „Anmelden / Registrieren“ wählen. Im Browser mit dem verifizierten Konto der E-Mail-Adresse anmelden, an die Ihre Lizenz zugestellt wurde.
3. Zurück in Guardian „Meine Lizenzen laden“ wählen. Bei mehreren Seiten die passende weitere Lizenzseite laden.
4. Eigene Guardian-Lizenz auswählen und „Pro aktivieren“ bestätigen.
5. Status prüfen. „Erneut prüfen“ aktualisiert den Nachweis online; eine begonnene Anmeldung kann abgebrochen werden.

> Der frühere Aktivierungscode-Dialog ist nicht der aktuelle Freischaltweg. Die abgebildeten Konten und Lizenzkennungen sind synthetische Testdaten. Die Anmeldung entschlüsselt keinen Tresor.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Geräteplätze und Offlinefrist

Eine Pro-Lizenz erlaubt bis zu **fünf aktive Geräte**. Im LMS-Kundenportal können Sie alte Geräteplätze freigeben. Abmelden allein gibt keinen Platz frei.

Pro-Rechte werden regulär täglich online erneuert. Bei Nichterreichbarkeit gilt der letzte bestätigte Nachweis höchstens **72 Stunden** und niemals über das bezahlte Ende hinaus. Eine online bestätigte Sperre beendet Pro sofort.

Ohne gültigen Nachweis werden zusätzliche Pro-Aktionen eingeschränkt. Lokaler Tresor, Basisbearbeitung, Backup und Export bleiben zugänglich; Archive oder Zugangsdaten werden nicht gelöscht und es ist kein zweiter Free-Installer nötig.

> Das Abmelden ist keine Vertragskündigung. Laufzeit und Kündigung verwalten Sie im Kundenkonto. Koordinationsdienst-Registrierungen sind getrennt von der LMS-Geräteplatzverwaltung.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

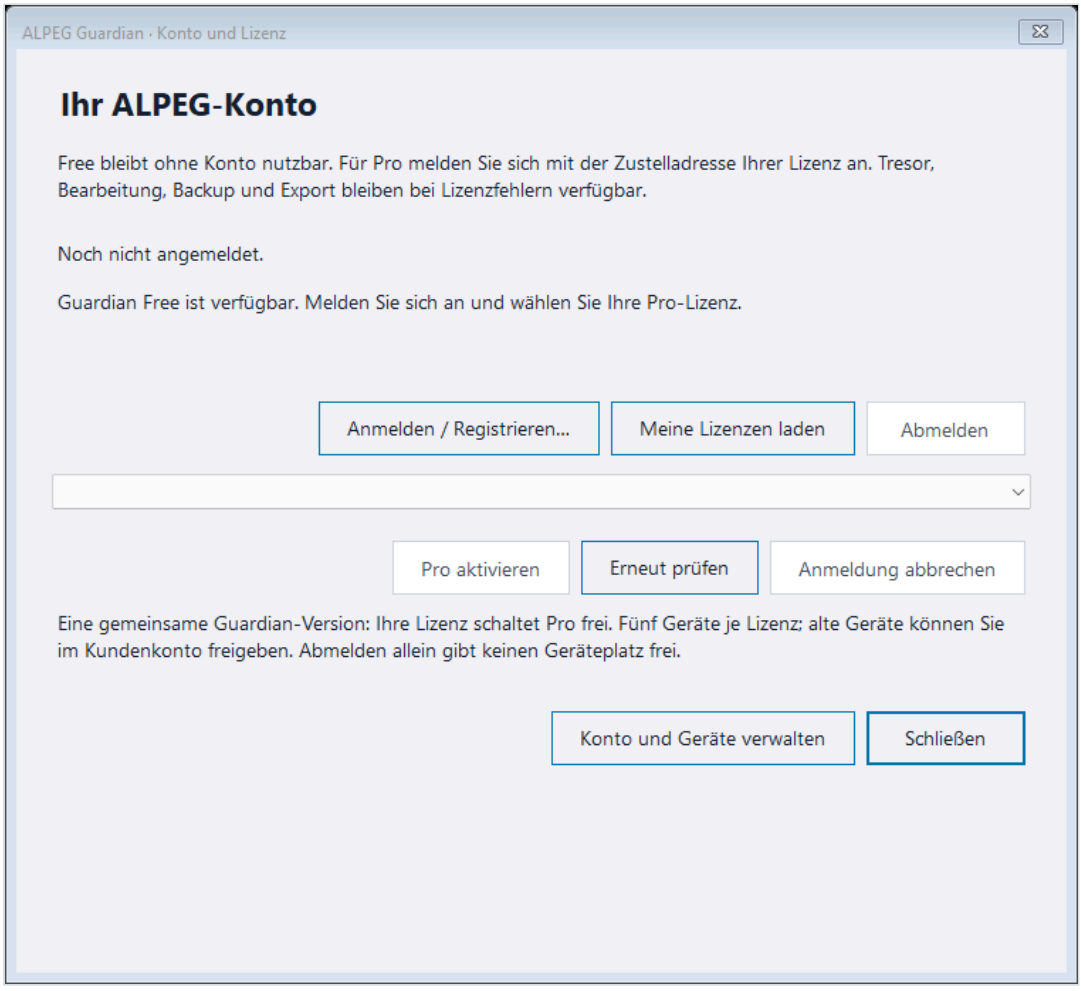
Konto verloren oder Anmeldung fehlerhaft

Prüfen Sie verifizierte Zustelladresse, Produkt, ausgewählte Lizenz, Laufzeit und freie Geräteplätze. Eine bloße Browseranmeldung aktiviert Pro noch nicht; die Lizenz muss im Programm ausgewählt und aktiviert werden.

Bei abgebrochener Anmeldung im Dialog erneut beginnen, statt mehrere parallele Aktivierungen zu starten. Ein Netzwerkfehler ist nicht automatisch eine bestätigte Sperre. Die vorhandene Offlinefrist endet dennoch verbindlich.

Ohne Zugriff auf die bisherige Zustelladresse wenden Sie sich mit ursprünglichem Kaufnachweis an den Support. Eine bekannte UUID oder Lizenznummer allein reicht nicht als Identitätsnachweis.

> Lizenzkonto, Dienstkonto und Masterpasswort lösen verschiedene Aufgaben. Ein wiederhergestelltes Lizenzkonto kann ein vergessenes Tresor-Masterpasswort nicht zurücksetzen.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Einstellungen und Bedienverhalten

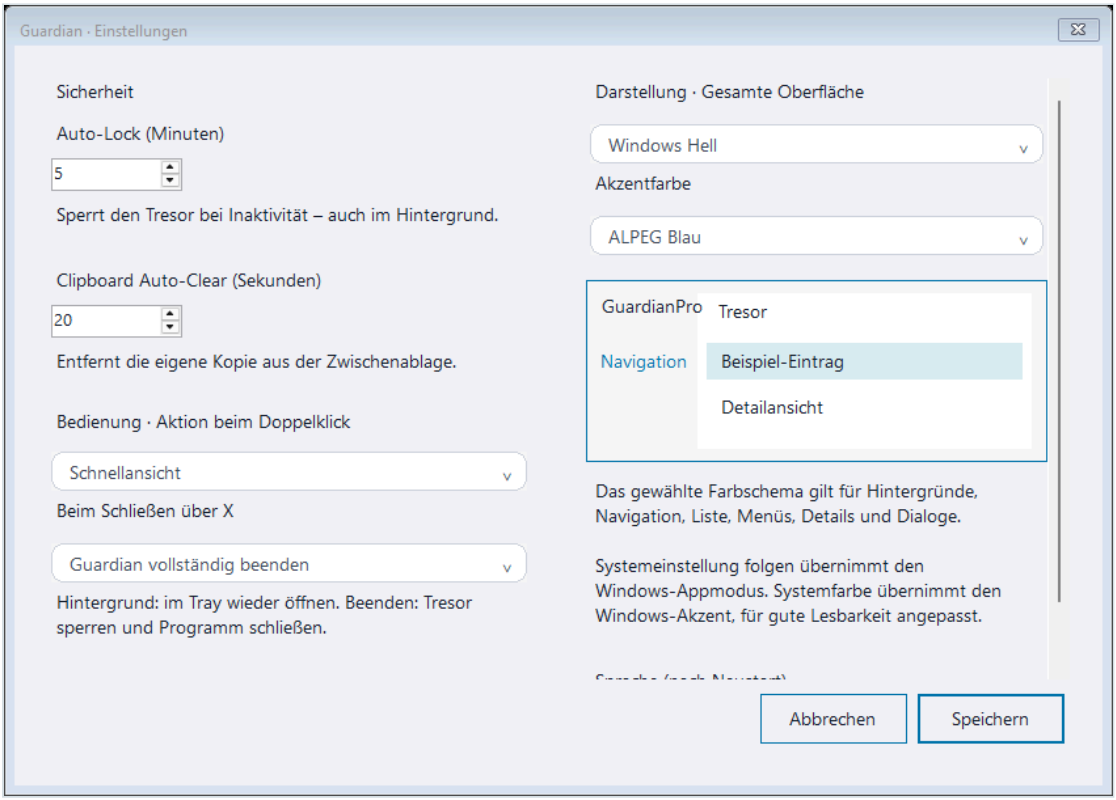
Sicherheit: Auto-Lock in Minuten sperrt den Tresor bei Inaktivität, auch im Hintergrund. Clipboard Auto-Clear entfernt nach der eingestellten Zeit die eigene aktuelle Kopie. Fremder Text, den Sie danach kopiert haben, bleibt erhalten.

Bedienung: Doppelklick kann Quick View, Copy Password, Open Website, Edit oder AutoFill auslösen. Bei „Beim Schließen über X“ wählen Sie zwischen Im Hintergrund weiterlaufen und Guardian vollständig beenden. Im Hintergrund bleibt Guardian im Tray erreichbar; Auto-Lock läuft weiter. Vollständig beenden sperrt den Tresor, entfernt die eigene Zwischenablagekopie und beendet das Programm. Datei → Beenden beendet unabhängig von der X-Auswahl.

Darstellung: ALPEG Dunkel, Windows Hell, Systemeinstellung folgen sowie ALPEG Blau, Petrol, Salbeigrün, Violett, Graphit, Mattgold und Grau-Schwarz gestalten die gesamte Oberfläche einschließlich Liste, Navigation, Details, Menüs und Dialogen. Bei Systemeinstellung folgen übernimmt Guardian den Windows-Appmodus und reagiert auf dessen Änderungen. Die separate Akzentwahl bietet ALPEG Blau, Petrol, Salbeigrün, Violett, Graphit, Mattgold und Systemfarbe. Systemfarbe folgt dem Windows-Akzent. Farbtöne werden für gut lesbaren Kontrast angepasst.

Die Vorschau zeigt Ihre Auswahl. Erst Speichern übernimmt sie und merkt sie für den nächsten Start. Abbrechen behält die bisherigen Einstellungen. Layout und Branding bleiben gleich.

View → Compact Mode verkleinert das Fenster und klappt Details ein. Ctrl+Alt+D schaltet das Detailpanel um. Die Fensterbuttons oben rechts sind Minimieren, Maximieren/Wiederherstellen und das rote X.



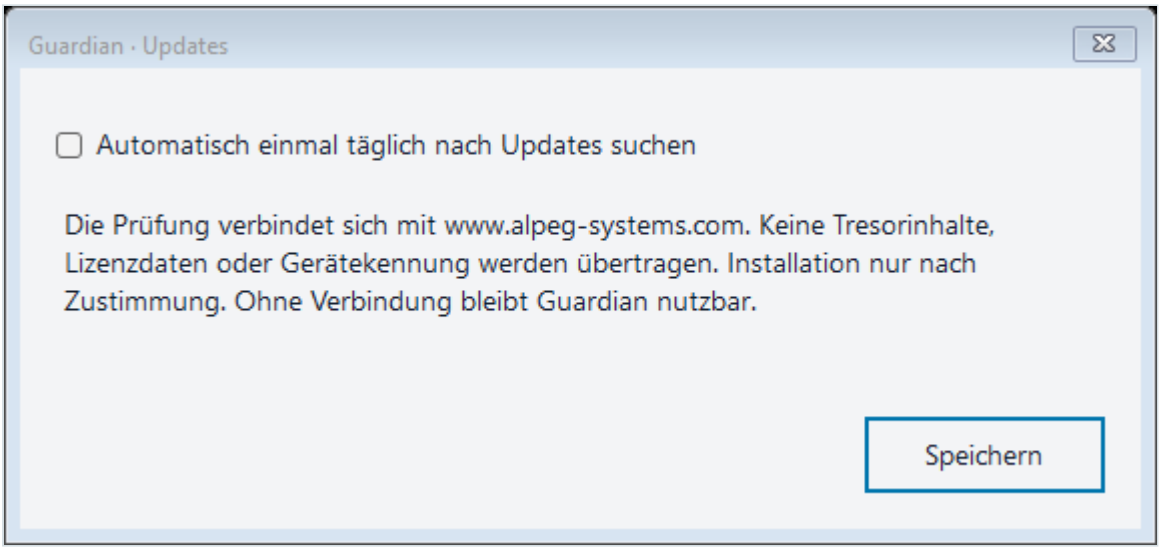
Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Updates und vollständiges Beenden

1. Über Hilfe → Nach Updates suchen eine manuelle Prüfung starten. Die automatische tägliche Suche kann in den Update-Einstellungen abgeschaltet werden.
2. Nur das offizielle Updateangebot verwenden. Signierte Updateinformationen und der Paketnachweis werden geprüft.
3. Vor Installation den lokalen Tresor verschlüsselt sichern und Guardian über Datei → Beenden vollständig schließen.
4. Windows-Abfragen und Installation selbst bestätigen. Nach Abschluss Versionsanzeige und Datenbestand prüfen.

Das rote X kann je nach Einstellung in den Infobereich wechseln. Datei → Beenden beendet das normale Hauptprogramm zuverlässig. Ein gesondert bewusst aktiviertes Monitoring hat seinen eigenen Deaktivierungsweg.

> Die Updateprüfung überträgt keine Tresorinhalte oder Masterpasswörter. Sie ist von der LMS-Lizenzprüfung getrennt. Ein Ende der Pro-Rechte erfordert keine besondere Neuinstallation.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

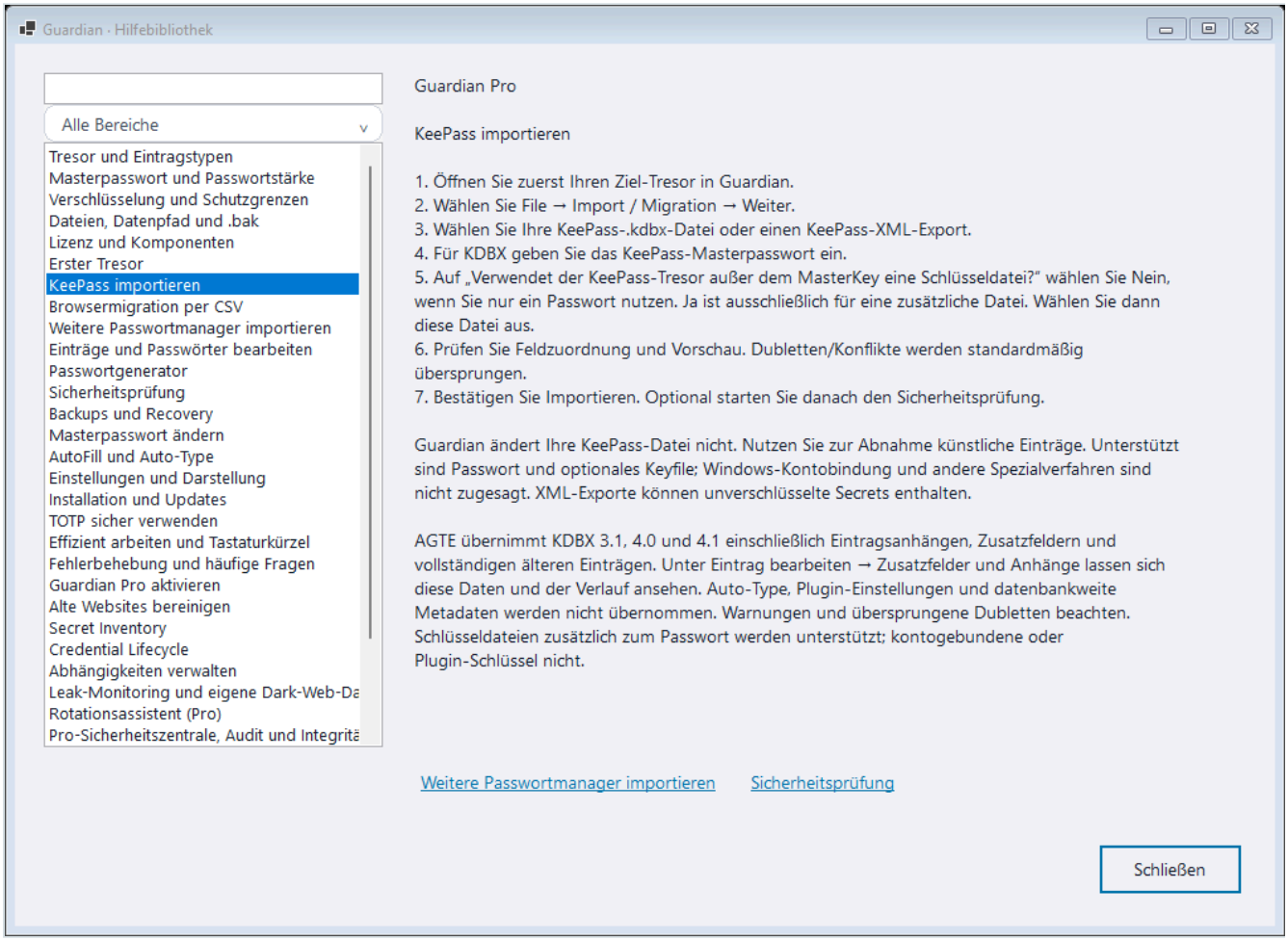
Hilfebibliothek und historische Hinweise

Hilfe → Hilfebibliothek öffnet die eingebauten Artikel. Suchen Sie nach Begriffen wie KeePass, Backup oder TOTP. Hinweise und Komponenten-Lizenzen sind dort ebenfalls zugänglich.

Einzelne eingebaute Texte stammen aus früheren Entwicklungsständen. Für den aktuellen Lizenzweg gelten die Kontoanmeldung und Lizenzwahl dieses Handbuchs. Die in älteren Artikeln beschriebene Browserintegration ist in 1.6.0 deaktiviert.

Das frühere PDF zu 1.3.0 bleibt ein historisches Dokument und beschreibt weder die aktuelle Pro-Kontoaktivierung noch alle neuen Verwaltungsfunktionen.

> Bei abweichenden historischen Anleitungen nicht alte Kandidaten nachinstallieren oder Schutzmaßnahmen umgehen. Programmversion und aktuellen veröffentlichten Dokumentationsstand vergleichen.



Echte Programmaufnahme · ausschließlich synthetische Beispieldaten

Kommandozeile: Voraussetzungen

Zum Paket gehört die separate **GuardianPro.Cli.exe**. Die Befehle sind auf Status, Integrität, Auditexport und Dienstabfragen begrenzt. Es gibt keine allgemeine Geheimnis-API und keine automatische Ausgabe von Tresorpasswörtern an andere Programme.

Bis auf die Hilfe benötigen Aktionen die gültige Pro-Berechtigung des aktuellen Windows-Profils. Für entfernte Geräte-, Arbeitsbereichs- und Freigabelisten ist außerdem eine passende Dienstanmeldung nötig.

```
.\GuardianPro.Cli.exe help
.\GuardianPro.Cli.exe status
.\GuardianPro.Cli.exe integrity "D:\Tresore\Beispiel.agv"
.\GuardianPro.Cli.exe audit-export "D:\Nachweise\Guardian-Audit.json"
```

> In PowerShell im Verzeichnis der CLI arbeiten oder ihren vollständigen Pfad angeben. Kennungen und Zeitangaben sind schutzwürdig. Die CLI nutzt das bestehende Benutzerprofil; keinen Masterpasswortwert in Befehlsargumente schreiben.

Kommandozeile: Befehle und Ergebnisse

Befehl	Wirkung
help / --help	Hilfe ohne Lizenzaktion anzeigen.
status	Version, Dienstverbindung, Ereigniszahl und Monitoring-Abdeckung als JSON.
integrity <Tresor.agv>	Dateistand gegen vorhandenen lokalen Integritätsanker prüfen. Kein Entschlüsseln des Tresors.
audit-export <neue Datei.json>	Auditnachweis in eine neue Datei schreiben; vorhandene Ziele werden nicht überschrieben.
devices	Geräteliste vom eingerichteten Dienst abfragen.
workspaces	Arbeitsbereiche vom Dienst abfragen.
grants	Freigabestatus vom Dienst abfragen.

Rückgabewerte: 0 bei regulärem Abschluss; 3 bei fehlender Pro-Berechtigung; 2 bei ungültigen Argumenten oder fehlgeschlagener Datei-/Dienstaktion. Inhalt des Ergebnisses zusätzlich lesen: Ein Integritätsbefund kann eine fachliche Warnung enthalten.

```
.\GuardianPro.Cli.exe devices
.\GuardianPro.Cli.exe workspaces
.\GuardianPro.Cli.exe grants
```

> Keine allgemeine Entwickler-API und keine automatische Secretübergabe zugesagt. Dienstabfragen benötigen Verbindung und passende Rollen; fehlende Verbindung nicht durch wiederholte Neuregistrierung beheben.

Tastaturkürzel

Taste	Aktion
Strg+F	Suche
Strg+N / Strg+E	Neuer Eintrag / Bearbeiten
Strg+D	Duplizieren
Strg+Umschalt+S	Favorit umschalten
Strg+L	Tresor sperren
Leertaste	Quick View
Strg+Alt+D	Detailpanel ein-/ausblenden
Entf	Löschen mit Bestätigung
Strg+C	Benutzername kopieren
Strg+Umschalt+C	Passwort kopieren
Strg+Umschalt+O	TOTP kopieren
Strg+Eingabe	HTTPS-Website öffnen
Strg+Umschalt+T	Auto-Type nach Warnung und Wartezeit

> Historisches Strg+Umschalt+F steht für Browser-Autofill, dessen Integration in dieser Version deaktiviert ist. Andere Anwendungen können dieselben Tasten verwenden; das richtige Fenster muss den Fokus haben.

Fehler gezielt eingrenzen

Passwort falsch oder Tresor beschädigt: Tastaturlayout und Dateiauswahl prüfen. Öffnen Sie eine bekannte Backupkopie mit dem dazugehörigen damaligen Passwort. Guardian kann diese beiden Fehler absichtlich nicht sicher unterscheiden.

Tresor bereits geöffnet: Schließen Sie die andere Sitzung regulär; nicht gleichzeitig dieselbe Datei bearbeiten.

Import zeigt keine Einträge: Dateiformat und Exportart prüfen. CSV-Feldzuordnung kontrollieren. KDBX benötigt das KeePass-Passwort und nur dann eine Schlüsseldatei, wenn tatsächlich eine benutzt wurde.

Login nach Bearbeiten falsch: Wurde das Passwort auch beim Anbieter geändert? Guardian speichert lokal und führt keinen automatischen Kontowechsel aus.

Generator scheinbar ohne Wirkung: Der neue Dialog zeigt den erzeugten Wert maskiert. Kopieren bestätigt die Zwischenablageaktion; im Editor Übernehmen verwenden.

Warum bleibt .bak nach Beenden? Sie ist die verschlüsselte Sicherung des vorherigen Stands. Warum bleibt Guardian im Tray? Diese Option ist in Einstellungen aktiv.

Keine Datenlecktreffer? Das ist keine Garantie; neue Lecks oder nicht erfasste Passwörter können fehlen. Supportunterlagen immer ohne Passwörter, TOTP-Secrets oder ungeschützte Tresorinhalte teilen.

Notfallplan für Ihren Tresor

Masterpasswort vergessen

Guardian kann es nicht zurücksetzen. Eine ältere Sicherung kann nur helfen, wenn deren damaliges Kennwort bekannt ist. Das Lizenzkonto und Notfall-Freigaben ersetzen diesen Nachweis nicht.

Rechner oder Windows-Profil verloren

Eine unabhängige verschlüsselte AGV-Sicherung mit bekanntem Masterpasswort ist der wichtigste Wiederherstellungsweg. Windows-gebundene Pro-Metadaten, Geräteidentitäten oder Monitoringzustände sind nicht durch bloßes Kopieren ihres Datenordners garantiert übertragbar.

Unerwartete Integritätsabweichung

Original und Nachweise unverändert kopieren, Ursache prüfen und eine bekannte gute Sicherung verwenden. Den aktuellen Zustand nicht ungeprüft zum neuen vertrauenswürdigen Ausgangspunkt erklären.

> Regelmäßig einen vollständigen Wiederherstellungsversuch mit einer Kopie durchführen. Eine .bak auf demselben Datenträger schützt nicht vor dessen vollständigem Verlust.

Gute Arbeitsabläufe

Neuer Anbieterzugang

1. Einen eindeutigen starken Wert generieren und beim Anbieter selbst einrichten.
2. Passendes Konto in Guardian speichern, HTTPS-Adresse prüfen und tatsächlichen Login testen.
3. Gegebenenfalls TOTP gegen unabhängigen Authenticator prüfen und Wiederherstellungscodes getrennt aufbewahren.

Migration

Ziel sichern, Quelle unverändert behalten, Vorschau und Konflikte prüfen, Stichproben testen. Klartextexporte anschließend geschützt behandeln.

Pro-Freigabe

Empfängerschlüssel unabhängig vergleichen, minimal benötigte Einträge wählen und begrenzte Gültigkeit setzen. Widerruf kann bereits entschlüsselte Kopien nicht zurückholen.

> Eine unabhängige Datensicherung und ein geschütztes Windows-Konto bleiben nötig. Dieses Programm ersetzt weder alle Sicherheitsmaßnahmen noch eine rechtliche Aufbewahrungslösung.

Funktionsvergleich · 1

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Für Free und Pro verfügbar		
Verfügbarkeit	✓ Jetzt verfügbar	✓ Jetzt verfügbar
Private und gewerbliche Nutzung	✓ Kostenlos nutzbar	✓ Mit Pro-Lizenz
Lokaler Tresor ohne Cloudpflicht	✓ Lokal nutzbar	✓ Gemeinsame Basis
AES-256-GCM-Verschlüsselung	✓ Verschlüsselte Daten	✓ Gemeinsame Basis
Argon2id-Schlüsselableitung	✓ Masterpasswort geschützt	✓ Gemeinsame Basis
Logins und Website-Zugänge	✓ Enthalten	✓ Gemeinsame Basis

Funktionsvergleich · 2

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
API-Schlüssel	✓ Enthalten	✓ Gemeinsame Basis
Sichere Notizen	✓ Enthalten	✓ Gemeinsame Basis
Server- und WLAN-Zugänge	✓ Enthalten	✓ Gemeinsame Basis
Mehrere Tresordateien	✓ Getrennte Dateien	✓ Gemeinsame Basis
Passwortgenerator	✓ Enthalten	✓ Gemeinsame Basis
Passwortstärkeanzeige	✓ Enthalten	✓ Gemeinsame Basis
Prüfung schwacher Passwörter	✓ Enthalten	✓ Gemeinsame Basis

Funktionsvergleich · 3

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Prüfung wiederverwendeter Passwörter	✓ Enthalten	✓ Gemeinsame Basis
Alte Zugangsdaten und HTTP-Hinweise	✓ Sicherheitsprüfung	✓ Gemeinsame Basis
Manuelle Passwortleckprüfung	✓ Nur mit Zustimmung	✓ Gemeinsame Basis
TOTP-Einmalcodes	✓ SHA1 / 6 Stellen	✓ Gemeinsame Basis
Automatische Tresorsperre	✓ Enthalten	✓ Gemeinsame Basis
Zeitgesteuertes Zwischenablageleeren	✓ Enthalten	✓ Gemeinsame Basis
Suche und Filter	✓ Enthalten	✓ Gemeinsame Basis

Funktionsvergleich · 4

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Kategorien und Tags	✓ Enthalten	✓ Gemeinsame Basis
Favoriten und zuletzt verwendet	✓ Enthalten	✓ Gemeinsame Basis
Eintragshistorie	✓ Enthalten	✓ Gemeinsame Basis
Zusatzfelder und Anhänge	✓ AGTE-Datenübernahme	✓ Gemeinsame Basis
KDBX 3.1 / 4.0 / 4.1 importieren	✓ Eigene AGTE	✓ Gemeinsame Basis
KDBX-Schlüsseldateien	✓ Passwort plus Datei	✓ Gemeinsame Basis
KeePass-XML importieren	✓ Exportdatei einlesen	✓ Gemeinsame Basis

Funktionsvergleich · 5

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Bitwarden-JSON importieren	✓ items-Format	✓ Gemeinsame Basis
1Password / Proton Pass / NordPass importieren	✓ Über CSV-Export	✓ Gemeinsame Basis
Chrome / Edge / Firefox importieren	✓ Über CSV-Export	✓ Gemeinsame Basis
Allgemeiner CSV-Import	✓ Felder zuordnen	✓ Gemeinsame Basis
Importvorschau und Dublettenprüfung	✓ Vor Übernahme	✓ Gemeinsame Basis
Verschlüsselter KDBX-Export	✓ Eigene AGTE	✓ Gemeinsame Basis
CSV-Export	✓ Klartext mit Warnung	✓ Gemeinsame Basis

Funktionsvergleich · 6

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Verschlüsselte Backups	✓ Enthalten	✓ Gemeinsame Basis
Wiederherstellung	✓ Enthalten	✓ Gemeinsame Basis
Auto-Type	✓ Aktives Fenster prüfen	✓ Gemeinsame Basis
Kontextmenü und Tastaturkürzel	✓ Enthalten	✓ Gemeinsame Basis
Kompaktansicht und Schnellansicht	✓ Enthalten	✓ Gemeinsame Basis
Tray- und Hintergrundbetrieb	✓ Enthalten	✓ Gemeinsame Basis
Farbschemata und Akzente	✓ Wählbar	✓ Gemeinsame Basis

Funktionsvergleich · 7

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Deutsch und US-Englisch	✓ Wählbar	✓ Gemeinsame Basis
Offline-Hilfebibliothek	✓ Enthalten	✓ Gemeinsame Basis
Manuelle Updateprüfung	✓ Signierte Informationen	✓ Gemeinsame Basis
Tägliche Updateprüfung	✓ Abschaltbar	✓ Gemeinsame Basis
Updateinstallation nach Zustimmung	✓ Daten bleiben erhalten	✓ Gemeinsame Basis
Sauberer Installer / Uninstaller	✓ Nutzerdaten bleiben	✓ Gemeinsame Basis
Für Free und Pro in Planung		

Funktionsvergleich · 8

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Browserintegration / Browser-AutoFill	In Planung Spätere Nachrüstung	In Planung Spätere Nachrüstung
Passkey-Zugriff über Browserhelfer	In Planung Gemeinsamer Baustein	In Planung Gemeinsamer Baustein
In Pro verfügbar		
Website-Bereinigungschecker	× Nicht enthalten	✓ Enthalten; Sammelbereinigung
Dark-Web-Monitoring	× Nicht enthalten	Bedingt Lokaler Identitätsabgleich; eigener aktueller Datenbestand erforderlich, nicht mitgeliefert
Kontinuierliche Leak-Warnungen	× Nicht enthalten	✓ Nach Aktivierung alle sechs Stunden; auch bei geschlossenem Guardian
Credential Lifecycle	× Nicht enthalten	✓ Zustände und fällige Erneuerungen

Funktionsvergleich · 9

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Secret Inventory	✗ Nicht enthalten	✓ Zweck, System, Verantwortung und Risiko
Dependency Mapping	✗ Nicht enthalten	✓ Manuelle Abhängigkeiten und Umstellungszyklen
Erweiterte Verwaltungs-Historie	✗ Nicht enthalten	✓ Verwaltungsänderungen im verschlüsselten Eintragsverlauf; kein manipulationssicherer Audit Trail
Geräteverwaltung	✗ Nicht enthalten	✓ Im LMS-Kundenportal; bis zu fünf aktive Geräte, Abmelden gibt keinen Platz frei
Pro-Lizenzaktivierung und Erneuerung	– Keine Aktivierung	✓ Verifiziertes Lizenzkonto; täglich erneuern, maximal 72 Stunden offline innerhalb bezahlter Rechte
Rotationsregeln	✗ Nicht enthalten	✓ Lokale Passwort-Mindestlänge und Erneuerungshinweise
Safe Rotation	✗ Nicht enthalten	✓ Geführter Wechsel mit Bestätigung der Anbieteränderung und abhängiger Dienste; kein automatischer Fremdsystemwechsel

Funktionsvergleich · 10

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Audit Trail	× Nicht enthalten	✓ Lokales verkettetes Journal mit Export; kein unabhängiger manipulationssicherer Auditdienst
Vault Integrity Chain	× Nicht enthalten	✓ Lokaler Vertrauensanker und Integritätsprüfung nach Einrichtung; kein Schutz bei vollständiger Übernahme des Windows-Kontos
Emergency Access	× Nicht enthalten	Dienst erforderlich Verschlüsselte Notfallkopie mit Wartezeit und registriertem Empfängergerät
Decoy Vault	× Nicht enthalten	✓ Separater gewöhnlicher Tresor; manuell öffnen, keine automatische Tarnung
Privacy Dashboard	× Nicht enthalten	✓ Datenquellen-Zustimmung und Nachweis der letzten maximal 1000 Programm-Netzwerkaufrufe; keine Browserhistorie
Erweiterte Richtlinien / Policies	× Nicht enthalten	✓ Lokale Pro-Vorgaben; keine zentrale Unternehmens-Gruppenrichtlinie
Sichere Freigaben	× Nicht enthalten	Dienst erforderlich Verschlüsselte Übergabe nach Geräteschlüsselprüfung; Widerruf verhindert keine Nutzung bereits gelesener Kopien

Funktionsvergleich · 11

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Team- und Familienfunktionen	✕ Nicht enthalten	Dienst erforderlich Arbeitsbereiche, registrierte Geräte und Rollen; keine automatische Tresorsynchronisierung
Unternehmensverwaltung	✕ Nicht enthalten	Begrenzt verfügbar Geräte-/Arbeitsbereichsrollen mit Koordinationsdienst; keine vollständige Unternehmensverwaltung
Erweiterte Migrationsanalyse	✕ Nicht enthalten	✓ Stapelvorschau und übersprungene Konflikte vor Übernahme
Historische Migrationsbereinigung	✕ Nicht enthalten	✓ Optional nur Verlauf neu importierter Einträge entfernen; Quellen und bestehende Einträge bleiben erhalten
Große Unternehmensimporte	✕ Nicht enthalten	✓ Bis 100 Dateien und insgesamt 10000 Einträge je Stapel; keine unbegrenzten Massenimporte
Migrations-Mapping-Regeln	✕ Nicht enthalten	✓ Eigene JSON-Zuordnung für die unterstützten Zielfelder
Batch-Migration	✕ Nicht enthalten	✓ Stapelweise Übernahme nach Vorschau und zusätzlicher verschlüsselter Sicherung

Funktionsvergleich · 12

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Team- und Tresorzuordnung	× Nicht enthalten	Begrenzt verfügbar Import in den geöffneten lokalen Tresor; Arbeitsbereichskennung als Zuordnung, keine automatische Verteilung
Detaillierte Migrationsberichte	× Nicht enthalten	✓ JSON-Stapelbericht mit Mengen, Konflikten und Zuordnung; ohne Geheimnisse
CLI und Entwickleranbindungen	× Nicht enthalten	CLI verfügbar Pro-Status, Integritätsprüfung, Auditexport sowie Dienstabfragen; keine allgemeine Entwickler-API-Zusage
Weitere geplante Erweiterungen		
Erweiterte Passkey-Funktionen	× Nicht enthalten	In Planung Umfang noch festlegen
Eigene Vorfalldatenbank und externe API	– Nicht Bestandteil	In Planung Späterer Ausbau; derzeit nicht verfügbar
Konto für kostenlose Funktionen	– Keine Anmeldung erforderlich	– Free bleibt ohne Konto nutzbar

Funktionsvergleich · 13

Stand Guardian 1.6.0. „Dienst erforderlich“ oder „Begrenzt verfügbar“ sind Voraussetzungen bzw. Einschränkungen und keine Zusage einer automatisch vorhandenen Infrastruktur.

Funktion	Guardian Free · 1.6.0	Guardian Pro · 1.6.0
Konto für Pro-Freischaltung	– Keine Pro-Freischaltung	✓ Verifizierte Zustelladresse und bestehende Lizenz auswählen
Geräte und Offlinefrist	✓ Kostenlose Funktionen lokal nutzbar	Bis fünf Geräte; tägliche Erneuerung, höchstens 72 Stunden offline und nie über das bezahlte Ende hinaus

Begriffe und Kontakt

Begriff	Bedeutung
AGV	Verschlüsselter Guardian-Tresor.
Masterpasswort	Geheimnis zum Entschlüsseln des lokalen Tresors.
LMS-Lizenzkonto	Verifiziertes Konto zur Pro-Freischaltung und Lizenzverwaltung.
Koordinationsdienst	Getrennter Dienst für Geräte, Rollen und verschlüsselte Übergaben.
TOTP	Zeitabhängiger Einmalcode; unterstützte Parameter beachten.
Integritätsanker	Bewusst bestätigter lokaler Vergleichsstand.
Notfallkopie	Ausdrücklich hinterlegter Eintragsstand, keine laufende Synchronisierung.

Guardian-Produktseite
ALPEG-Systems Shop
LMS-Kundenportal
Allgemein: info@alpeg-systems.com
Lizenzzustellung: lizenzen@alpeg-systems.com

Bei Supportfragen Version, Windows-Version, Aktion und genaue Fehlermeldung nennen. Keine Kennwörter, TOTP-Secrets oder unverschlüsselten Tresorinhalte senden.

Lizenzen und Dokumentstand

ALPEG-Anwendungscode ist proprietär. Mitgelieferte Komponenten behalten ihre eigenen Lizenzbedingungen. Hinweise und vollständige zugehörige Texte sind in der Installation und Hilfebibliothek enthalten.

Die reguläre 1.6.0-Auslieferung enthält die erforderliche .NET-Laufzeit. Kryptografie und Import verwenden die mitgelieferten Drittanbieterkomponenten; KeePassLib gehört nicht als allgemeiner Produktbestandteil zum Laufzeitpaket.

Dieses Handbuch dokumentiert den vorhandenen Stand. Es behauptet keine unabhängige Sicherheitszertifizierung, keine garantierte Rechts-/Revisionssicherheit und keine bereits aktive persönliche Leakdaten-Abdeckung.

Für die Aufnahmen wurden ausschließlich ein neuer synthetischer Tresor und eine lokale signierende Testgegenstelle verwendet. Die Registerbilder dienstgebundener Funktionen zeigen die Oberfläche ohne eingerichtete Dienstanmeldung.

> Ausgabe 1.0 · Guardian 1.6.0 · 22. November 2026. Das frühere Handbuch 1.3.0 bleibt ausschließlich historisch. Bei späteren Funktionsänderungen benötigen Programm und Dokumentation einen neuen abgestimmten Stand.