

ALPEG SYSTEMS

GUARDIAN PRO

Benutzerhandbuch Pro-Version 1.3.0



Sicher verwahren. Bewusst verwalten.

Installation · Tresor · Passwörter · Pro-Verwaltung · Lizenz

Für Windows x64 | Build 1.3.0-pro.monitoring.1

Dokumentstand 17. Oktober 2026

Orientierung und Geltungsbereich

Dieses Handbuch beschreibt ALPEG Guardian Pro **Pro-Version 1.3.0** mit dem Build **1.3.0-pro.monitoring.1**. Es umfasst die belegten gemeinsamen Free-Funktionen und die zusätzlichen Pro-Funktionen dieses Stands.

Die Anleitung wurde mit dem Chat „Zahlungsarchitektur integrieren“, den Projektquellen und den Releaseunterlagen abgeglichen. Dort ist die Veröffentlichung von 1.3.0 am 17.10.2026 dokumentiert. Der lokale Installer stimmt in Größe und SHA-256 mit dem Veröffentlichungsnachweis überein. Eine neue vollständige Bedienprüfung des installierten Builds wurde für dieses Handbuch nicht durchgeführt. Verbleibende offene Punkte sind im letzten Kapitel als **zu verifizieren** ausgewiesen.

So lesen Sie die Anleitung

„Datei → Backup“ bezeichnet eine Folge von Menüpunkten. Die deutschsprachige Oberfläche verwendet teilweise englische Begriffe wie Secret Inventory, Credential Lifecycle und Quick View. „Tresor“ und „Vault“ bezeichnen dieselbe verschlüsselte Datei. Tastenkombinationen beziehen sich auf das aktive Guardian-Fenster.

Kapitel	Seite
01 Orientierung und Geltungsbereich	2
02 Funktionsumfang Free und Pro	3
03 Installation und erster Start	4
04 Ersten Tresor einrichten	5
05 Einträge und tägliche Bedienung	6
06 Passwörter, TOTP und Sicherheitsprüfung	7
07 Import und Migration	8
08 Backup, Recovery und Export	9
09 Pro-Lizenz freischalten	10
10 Secret Inventory und Credential Lifecycle	11
11 Websites prüfen und gesammelt bereinigen	12
12 Dependency Mapping: Umstellungen verfolgen	13
13 Kontinuierliche Leak-Warnungen einrichten	14
14 Hinweise und Datenquellen verstehen	15
15 Einstellungen, Updates und Deinstallation	16
16 Fehlerbehebung und Tastenkürzel	17
17 Quellen, Prüfstatus und Versionshistorie	18

Funktionsumfang Free und Pro

Bereich	Bestätigter Umfang in diesem Handbuch
Gemeinsame Basis Free und Pro	Lokaler verschlüsselter .agv-Tresor; Masterpasswort; Einträge für Website/Login, API-Key, Secure Note, Server und WiFi; Suche, Kategorien, Tags, Favoriten und zuletzt verwendete Einträge.
Passwörter und Schutz	Generator, lokale Stärkeanzeige, Sicherheitsprüfung, freiwillige Onlineprüfung kompromittierter Passwörter, TOTP, bewusste Kopieraktionen, automatische Sperre und Zwischenablagebereinigung.
Daten übernehmen und sichern	Import über KDBX, XML, CSV und unterstütztes JSON; Zusatzfelder, Anhänge und Verlauf; verschlüsselte Backups, Recovery sowie KDBX- und CSV-Export.
Bedienung	Quick View, Detailpanel, Auto-Type, Darstellungs- und Akzentwahl, Tray-Verhalten sowie Updateprüfung.
Pro zusätzlich	Lizenzfreischaltung; Website-Prüfung mit Rückmeldung; Sammelbereinigung; Secret Inventory und Credential Lifecycle mit lokalen Verwaltungsdaten und Hinweisen; Dependency Mapping; freiwilliges Leak-Monitoring mit Hintergrundbetrieb.

In diesem Build nicht als nutzbar beschrieben

Browserintegration und AutoFill: Für beide Editionen in Planung und in diesem Release nicht freigegeben. Ältere Hilfetexte oder mitgelieferte Browserdateien belegen keine verfügbare Funktion. Die CSV-Migration von Browserpasswörtern ist davon unabhängig.

Grenzen des Monitorings: Öffentliche Dienstmeldungen lassen sich optional abgleichen. Persönliche Identitätstreffer benötigen eine eigene lokale Leakdatei. Ein persönlicher Leakdatenbestand, eine vollständige Dark-Web-Suche sowie die geplante zentrale Vorfalldatenbank und API werden nicht mitgeliefert. Passwörter werden beim Anbieter nicht automatisch geändert.

Was die Lizenz schützt

Eine gültige Pro-Berechtigung schaltet Pro-Zusatzaktionen frei. Ein Lizenzfehler sperrt nicht den lokalen Basistresor, dessen Bearbeitung, Backup und Export. Bereits gespeicherte Verwaltungsdaten bleiben lesbar. Geräteanzahl, Laufzeit und Kaufbedingungen ergeben sich aus Ihrer erworbenen Lizenz; das Titelbild ist eine Produktabbildung.

Installation und erster Start

Vorbereiten

Verwenden Sie den Installer **ALPEG-Guardian-Pro-1.3.0-pro.monitoring.1-Setup-x64.exe** aus Ihrer vertrauenswürdigen Bereitstellung. Die vorliegende Setup-Konfiguration richtet sich an Windows x64 und verlangt mindestens Windows 10 Build 17763. Die vollständige Installations- und Upgradeprüfung dieses konkreten Setups unter Ihrer Windows-Version ist zu verifizieren. Eine gesonderte .NET-Installation ist laut Projektdokumentation nicht erforderlich.

1. Sichern Sie bei vorhandener Nutzung den Tresor verschlüsselt auf einem anderen Datenträger. Notieren Sie, welches Masterpasswort zur Sicherung gehört.
2. Beenden Sie Guardian über **Datei** → **Beenden**. Arbeiten Sie während Installation oder Upgrade nicht parallel am selben Tresor.
3. Starten Sie die Setup-Datei. Prüfen Sie Dateiname und Herkunft, bevor Sie die von Windows angeforderten Administratorrechte gewähren.
4. Folgen Sie dem Assistenten und lesen Sie die Lizenzbedingungen. Der vorgesehene Pro-Standardpfad lautet **Program Files\ALPEG-SYSTEMS\GuardianPro**. Eine Desktop-Verknüpfung ist optional.
5. Starten Sie Guardian Pro. Prüfen Sie unter **Hilfe** → **Über Guardian**, dass der installierte Stand zur Pro-Version 1.3.0 gehört.
6. Legen Sie einen neuen Tresor an oder öffnen Sie Ihre vorhandene .agv-Datei. Für Pro-Aktionen führen Sie die Lizenzfreischaltung aus Kapitel 09 durch.

Programmdateien und persönliche Daten

Speichern Sie Tresore außerhalb des Programmverzeichnisses. Der in der Hilfebibliothek genannte Standard für Tresordaten ist **%LOCALAPPDATA%\ALPEG-SYSTEMS\Guardian**; Sie können einen eigenen lokalen Pfad wählen. Pro-Einstellungen und Lizenzidentität sind von der Tresordatei getrennt. Kopieren oder löschen Sie diese Identitätsdateien nicht zur Fehlerbehebung.

Free und Pro

Guardian Pro besitzt einen separaten Programmpfad. Verwenden Sie beim Wechsel eine gesicherte Kopie des Tresors und prüfen Sie die übernommenen Daten. Öffnen Sie dieselbe Datei nicht gleichzeitig in Free und Pro. Erweiterte Tresore nicht mit einem alten Guardian-Programm bearbeiten, das das Dateiformat nicht unterstützt.

Ersten Tresor einrichten

1. Öffnen Sie **Datei** → **Neuer Vault....** In erläuternden Texten kann „Neuer Tresor“ stehen.
2. Wählen Sie einen lokalen Speicherort und einen aussagekräftigen Dateinamen für die .agv-Datei.
3. Legen Sie ein einzigartiges Masterpasswort mit mindestens **12 Zeichen** fest. Eine lange, nicht vorhersehbare Passphrase ist sinnvoll.
4. Geben Sie das Passwort zur Bestätigung erneut ein und schließen Sie die Tresorerstellung ab. Bei abweichenden Eingaben prüfen Sie beide Felder und das Tastaturlayout.
5. Erstellen Sie einen ersten Testeintrag über **Strg+N**, speichern Sie ihn und prüfen Sie seine Anzeige.
6. Sperren Sie den Tresor mit **Strg+L**. Öffnen Sie ihn über **Datei** → **Vault öffnen...** und testen Sie das Masterpasswort.
7. Erstellen Sie über **Datei** → **Backup...** eine verschlüsselte Sicherung auf einem anderen Datenträger.

Masterpasswort sicher aufbewahren

Es gibt keinen Passwortreset und keine Hintertür für einen vergessenen Tresorschlüssel. Bewahren Sie Ihr Masterpasswort sicher außerhalb des Tresors auf. Ein Aktivierungscode für Pro ersetzt das Masterpasswort nicht. Auch eine gültige Lizenz kann einen nicht entschlüsselbaren Tresor nicht öffnen.

Verschlüsselung und Schutzgrenzen

Die gemeinsame Tresorbasis verwendet **Argon2id** zur Schlüsselableitung und **AES-256-GCM** zur authentisierten Verschlüsselung. Laut Dokumentation sind für Argon2id 64 MiB Speicher, drei Durchläufe und zwei parallele Spuren vorgesehen. Die verschlüsselte Datei schützt gespeicherte Daten; ein entsperrter Tresor hält Daten im Arbeitsspeicher.

Sperren Sie Guardian vor Pausen. Schadsoftware, ein kompromittiertes Windows-Konto oder Zugriff auf eine entsperrte Sitzung können den Schutz umgehen. Eine Stärkeanzeige ist keine Garantie. Ein unabhängiges Sicherheitsaudit ist durch die vorliegenden Quellen nicht nachgewiesen.

Einträge und tägliche Bedienung

Eintrag erstellen und ändern

1. Öffnen Sie den Tresor und drücken Sie **Strg+N**. Wählen Sie den passenden Eintragstyp.
2. Tragen Sie Titel, Website, Benutzername und Passwort ein, soweit sie für den gewählten Typ relevant sind. Hinterlegen Sie Notizen sowie Kategorien und Tags nach Bedarf.
3. Nutzen Sie im Editor **Passwort generieren**. Erst **Übernehmen** setzt den erzeugten Wert in das Passwortfeld.
4. Speichern Sie. Zum späteren Ändern wählen Sie den Eintrag und drücken **Strg+E**. Abbrechen verwirft die laufende Eingabe.

Wichtig: Ein geändertes Passwort in Guardian ändert kein Konto beim Anbieter. Ändern Sie das Passwort auf der offiziellen Website, speichern Sie den neuen Wert in Guardian und testen Sie anschließend die Anmeldung.

Finden, ordnen und anzeigen

Mit **Strg+F** suchen Sie nach Titel, Website oder Benutzername. Die Navigation bietet alle Einträge, Favoriten, Recently Used sowie die Eintragstypen und Kategorien/Tags. Kategorien ordnen Einträge; Tags erlauben mehrere Zuordnungen. Markieren Sie häufig benötigte Einträge als Favoriten.

Leertaste öffnet Quick View ohne Passwortausgabe. **Strg+Alt+D** schaltet das Detailpanel um. Das Rechtsklickmenü bietet unter anderem Kopieren, Website öffnen, Bearbeiten, Duplizieren, Favorit, History, Tags und Löschen. Passwörter und TOTP bleiben in der Liste verborgen.

Zusatzfelder, Anhänge und Verlauf

Unter **Eintrag bearbeiten** → **Zusatzfelder und Anhänge** können die übernommenen Zusatzdaten und der Verlauf geprüft werden. Änderungen an Passwort, Benutzername oder Notizen bewahren bisherige Werte in der History. Der Verlauf enthält sensible Daten. KDBX-Export und verschlüsselte Backups erhalten erweiterte Daten; CSV nicht.

Kopieren, Auto-Type und Löschen

Strg+C kopiert den Benutzernamen, **Strg+Umschalt+C** das Passwort. Prüfen Sie das Ziel, bevor Sie einfügen. Auto-Type sendet nach Warnung und fünf Sekunden Benutzername, Tab und Passwort an das aktive Fenster. Es authentisiert das Ziel nicht; zunächst mit Testwerten prüfen. Eine Sperre während des Countdowns verhindert die Ausgabe. **Entf** löscht nach Bestätigung. Alte Backups können den Eintrag weiter enthalten.

Passwörter, TOTP und Sicherheitsprüfung

Passwortgenerator

Öffnen Sie **Werkzeuge** → **Passwortgenerator**. Der Generator erzeugt sofort ein maskiertes Zufallspasswort. Standard sind 24 Zeichen; wählbar sind 14 bis 128 Zeichen. **Neu generieren** erzeugt einen weiteren Wert, **Kopieren** überträgt ihn in die Zwischenablage. Im Eintragseditor übernimmt **Übernehmen** den Wert. Verwenden Sie für jedes Konto ein eigenes Passwort und beachten Sie die Regeln des Anbieters.

Lokale Sicherheitsprüfung

1. Öffnen Sie **Werkzeuge** → **Sicherheitsprüfung**.
2. Wählen Sie einen Eintrag mit Hinweis. Prüfen Sie die rechts angezeigte Ursache und die vorgeschlagenen Schritte.
3. Bei schwachen oder wiederverwendeten Passwörtern ändern Sie den Wert beim Anbieter. Verwenden Sie für jedes betroffene Konto ein eigenes Passwort.
4. Bei HTTP oder fehlender Website prüfen Sie die offizielle HTTPS-Adresse und korrigieren den Eintrag. Ein Altershinweis verlangt eine Prüfung und beweist allein keine Unsicherheit.
5. Speichern Sie den aktualisierten Eintrag. Die Prüfung wird erneut ausgewertet; erledigte Hinweise verschwinden.

Freiwillige Onlineprüfung

Werkzeuge → **Kompromittierte Passwörter prüfen (Online)**... benötigt Internet und Ihre Zustimmung. Der Client überträgt die ersten fünf Zeichen des SHA-1-Passworthashes an Have I Been Pwned, nicht das Passwort. Der Anbieter sieht Ihre IP-Adresse. Ein Treffer betrifft den Passwortwert und beweist nicht, welches Konto betroffen ist. Nach einer Änderung erneut prüfen. Keine Treffer sind keine Sicherheitsgarantie. Diese Einzelprüfung ist keine laufende Leak-Überwachung.

TOTP als zweiten Faktor verwenden

Hinterlegen Sie ein unterstütztes Base32-Secret oder eine passende otpauth-URI im Eintrag. Unterstützt sind **sechs Stellen, SHA1 und 30 Sekunden**; andere Parameter werden nicht zugesagt. Vergleichen Sie den Code beim Einrichten mit einem unabhängigen Authenticator. **Strg+Umschalt+O** kopiert TOTP. Bei Abweichungen Windows-Uhrzeit, Secret und Anbieterparameter prüfen.

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

Import und Migration

Gemeinsamer Ablauf

1. Sichern Sie Ihren vorhandenen Ziel-Tresor. Erstellen Sie beim bisherigen Passwortmanager die passende Exportdatei.
2. Öffnen Sie den Ziel-Tresor und **Datei** → **Import / Migration....** Gehen Sie über Weiter zur Dateiauswahl.
3. Wählen Sie die Datei. Prüfen Sie Format, Feldzuordnung und Vorschau. Passen Sie falsch zugeordnete Spalten an und aktualisieren Sie die Vorschau.
4. Lassen Sie das standardmäßige Überspringen identischer Loginidentitäten bzw. Konflikte bei der ersten Migration aktiv. Prüfen Sie Warnungen und übersprungene Daten.
5. Bestätigen Sie den Import. Vergleichen Sie Anzahl und Stichproben, testen Sie wichtige Logins und sichern Sie den übernommenen Bestand.

Quelle	Bestätigter Übernahmeweg
KeePass	KDBX 3.1, 4.0 und 4.1 oder KeePass-XML; KDBX mit Passwort und optional zusätzlicher Schlüsseldatei.
Chrome, Edge, Brave, Firefox	Vorher im jeweiligen Browser erstellter Passwort-CSV-Export. Kein direktes Auslesen der Browserprofile.
Bitwarden	JSON oder CSV.
1Password, Proton Pass, NordPass	CSV. Native 1PUX- und andere proprietäre Archive werden nicht vollständig unterstützt.
Eigene CSV	Feldzuordnung für die angebotenen Standardfelder kontrollieren.

Besonderheiten bei KeePass

Geben Sie für KDBX das KeePass-Masterpasswort ein. Die Frage nach einer zusätzlichen Schlüsseldatei beantworten Sie nur dann mit Ja, wenn diese tatsächlich verwendet wurde. Windows-Kontobindung und Plugin-Schlüssel werden nicht unterstützt. AGTE übernimmt Anhänge, Zusatzfelder und vollständige ältere Eintragsstände. Auto-Type-Konfigurationen, Plugin-Einstellungen und datenbankweite Metadaten werden nicht übernommen. Die Quelldatei bleibt unverändert.

Klartextdateien und Formaterweiterung

CSV und XML können Zugangsdaten unverschlüsselt enthalten. Schützen Sie Exportdateien und geben Sie sie nicht weiter. Eine normale Löschung garantiert auf SSDs keine physische Entfernung. Tresore mit Anhängen, Zusatzfeldern oder vollständigen Verläufen verwenden AGV-Hüllversion 2; dieser Guardian liest Version 1 und 2. Ältere Programme können Version 2 ablehnen.

Backup, Recovery und Export

Verschlüsseltes Backup erstellen

1. Öffnen Sie den Tresor und **Datei** → **Backup...**
2. Wählen Sie einen neuen Dateinamen auf einem anderen Datenträger. Die Sicherung bleibt verschlüsselt. **Datei** → **Export verschlüsselt...** verwendet dieselbe Backup-Funktion.
3. Bewahren Sie mehrere Stände auf und testen Sie die Wiederherstellung. Für eine manuelle Dateikopie schließen Sie den Tresor vorher.

Aus einer Sicherung wiederherstellen

1. Wählen Sie **Datei** → **Recovery aus Backup...** und die Backupdatei.
2. Geben Sie das Masterpasswort ein, das zum Zeitpunkt dieser Sicherung galt.
3. Wählen Sie einen neuen Zieldateinamen. Die Recovery prüft das Backup und überschreibt keinen bestehenden Tresor.
4. Öffnen Sie den wiederhergestellten Tresor und kontrollieren Sie Einträge, Zusatzdaten und wichtige Zugangsdaten.

Was .bak und .lock bedeuten

Zu einer Datei wie Personal.agv kann Personal.agv.bak den vorherigen verschlüsselten Speicherstand enthalten. Diese Datei bleibt nach dem Schließen erhalten und wird beim nächsten Speichern ersetzt. Sie ist kein externes Backup und hilft nicht bei Verlust desselben Datenträgers. Die .lock-Datei schützt gegen gleichzeitige Schreibzugriffe; löschen Sie sie nicht während einer geöffneten Sitzung.

KDBX und CSV exportieren

Öffnen Sie **Datei** → **Export KDBX / CSV...** und wählen Sie das gewünschte Format. Für KDBX vergeben Sie ein Passwort für den verschlüsselten Export. Der KDBX-Export bewahrt Zusatzfelder, Anhänge und Verlauf einschließlich der Pro-Verwaltungsdaten. CSV enthält Klartextzugangsdaten einschließlich TOTP, aber keine Anhänge, Zusatzfelder oder Verläufe. Bestätigen Sie die Klartextwarnung nur, wenn Sie dieses Format bewusst benötigen.

Masterpasswort ändern

Öffnen Sie **Werkzeuge** → **Master-Passwort ändern...** und geben Sie das neue Passwort zweimal ein. Die Mindestlänge beträgt 12 Zeichen. Guardian verschlüsselt den aktuellen Tresor mit einem neu abgeleiteten Schlüssel. Testen Sie das Wiederöffnen und erstellen Sie ein neues externes Backup. **Ältere Backups bleiben mit dem früheren Passwort geschützt.** Eine Änderung vernichtet diese Kopien nicht.

Pro-Lizenz freischalten

Voraussetzungen

Sie benötigen eine für Guardian Pro gültige Lizenz, einen frischen eigenen Aktivierungscode und für die Erstaktivierung eine Verbindung zum Lizenzdienst. Die Lizenz und das Masterpasswort erfüllen getrennte Aufgaben. Der lokale Tresor benötigt kein Cloudkonto; die Pro-Aktivierung kommuniziert mit dem Lizenzdienst.

1. Starten Sie Guardian Pro. Öffnen Sie **Werkzeuge** → **Pro-Lizenz...**; die Hilfebibliothek nennt alternativ **Einstellungen** → **Pro-Lizenz**.
2. Geben Sie Ihren Aktivierungscode direkt in das maskierte Feld ein. Teilen Sie den Code nicht im Chat, in Screenshots oder Supportprotokollen. Laut Projektdokumentation wird der Code nicht gespeichert.
3. Betätigen Sie **Aktivieren** einmal und warten Sie das Ergebnis ab. Bei einem unklaren Ausgang nicht wiederholt neu registrieren und keine Installationsidentität löschen.
4. Prüfen Sie, ob der Dialog einen aktiven Status und freigegebene Pro-Funktionen meldet. Bei späteren Problemen verwenden Sie **Erneut prüfen**.
5. Öffnen Sie einen Tresor und testen Sie eine Pro-Aktion, beispielsweise das Bearbeiten der Verwaltungsdaten im Secret Inventory.

Wenn die Lizenzprüfung scheitert

Prüfen Sie Internetverbindung, Windows-Datum und -Uhrzeit sowie die angezeigte Fehlermeldung. Verwenden Sie Erneut prüfen. Besteht das Problem weiter, wenden Sie sich über Ihren Kauf- oder den offiziellen ALPEG-Supportkanal an den Anbieter. Übermitteln Sie nur bereinigte Fehlertexte, Versionsangaben und gegebenenfalls öffentliche Lizenz-/Installationskennungen, keine Geheimnisse.

Die Pro-Freigabe wird anhand der signierten Produktberechtigung, Installationsbindung und Zeitfristen geprüft. Bei gültigem lokalen Berechtigungsnachweis kann eine Offline-Nutzung möglich sein; eine unbegrenzte Offline-Freigabe wird nicht zugesagt. Dauer und Erneuerungsfristen dieses Builds sind **zu verifizieren**.

Ihre Daten bleiben zugänglich

Bei Lizenzfehlern bleiben Öffnen und Bearbeiten des Basistresors, Lesen, Backup und Export möglich. Vorhandene Secret-Inventory- und Lifecycle-Daten werden nicht erzwungen gelöscht. Änderungen an diesen Pro-Verwaltungsdaten benötigen eine gültige Pro-Lizenz.

Kauf, Gerätezahl und Wechsel

Die genauen Schritte zum Erhalt eines Aktivierungscodes nach dem Kauf, Gerätewechsel, Übertragung und Freigabe belegter Geräte sind für den konkreten Shopablauf **zu verifizieren**. Die Produktabbildung auf dem Titelblatt zeigt ein Angebot mit fünf Geräten; maßgeblich sind die Bedingungen Ihrer tatsächlich erworbenen Lizenz.

Secret Inventory und Credential Lifecycle

Zugangsdaten mit Verwaltungsdaten ergänzen

1. Öffnen Sie einen Tresor und **Werkzeuge** → **Secret Inventory...**
2. Wählen Sie den gewünschten Zugang. Klicken Sie auf **Verwaltungsdaten bearbeiten...**; ein Doppelklick öffnet ebenfalls den Editor.
3. Erfassen Sie **Zweck, System, Verantwortlich und Umgebung**. Wählen Sie Risiko: Niedrig, Mittel oder Hoch.
4. Tragen Sie bei Bedarf ein Ablaufdatum im Format **JJJJ-MM-TT** ein oder lassen Sie das Feld leer. Wählen Sie den dokumentierten Status.
5. Speichern Sie. Die aktive Pro-Berechtigung wird vor dem Öffnen des Editors und vor dem Speichern geprüft.

Die Übersicht zeigt Titel, System, Verantwortlichkeit, Umgebung, Risiko, Status, Ablaufdatum, Handlungsbedarf und letzte lokal erfasste Nutzung. „Nicht verwaltet“ bedeutet, dass noch kein entsprechendes Verwaltungsprofil vorliegt. Eine fehlende Nutzung wird nicht geraten.

Erneuerungen bearbeiten

Werkzeuge → **Credential Lifecycle...** öffnet die Übersicht mit aktiviertem Filter **Nur Handlungsbedarf**. Hinweise entstehen ab 30 Tagen vor dem lokalen Ablaufdatum, bei abgelaufenen Einträgen oder bei manuell dokumentierter Erneuerungsfälligkeit. Zähler im Werkzeugmenü und in der Statusleiste erscheinen nur bei geöffnetem Tresor. Es gibt in diesem Stand keine Hintergrundjobs und keine automatische Passwortrotation.

Status	Bedeutung und mögliche Folgeschritte
Aktiv / Erneuerung fällig	Wechsel in beide Richtungen möglich; außerdem Ersetzt, Widerrufen oder Archiviert dokumentierbar.
Ersetzt / Widerrufen	Dokumentierter Zustand; anschließend Archiviert möglich. Keine stille Reaktivierung.
Archiviert	Abgeschlossener dokumentierter Zustand. Der Eintrag bleibt erhalten.

Ändern oder widerrufen Sie den Zugang zuerst beim Anbieter. Dokumentieren Sie danach den Zustand in Guardian. Ein Statuswechsel ändert keine externen Zugangsdaten und löscht keinen Eintrag. Der lokale Statusverlauf hält Zeitpunkt sowie Ausgangs- und Zielzustand fest, ist aber kein manipulationssicheres Auditprotokoll.

Speicherung und Datenerhalt

Die Verwaltungsdaten liegen verschlüsselt als Zusatzfeld im Tresor. Backups und KDBX erhalten diese Daten; CSV nicht. Vor Änderungen wird ein Eintragsstand im Verlauf bewahrt. Bei nicht lesbaren oder unbekannten Datenversionen werden vorhandene Daten nicht durch Standardwerte überschrieben. Sichern Sie den Tresor und klären Sie die Meldung mit dem Support.

Websites prüfen und gesammelt bereinigen

Freiwillige Website-Prüfung starten

1. Öffnen Sie den Tresor und **Werkzeuge** → **Website-Bereinigung....**
2. Lesen Sie den Hinweis und aktivieren Sie **Prüfung erlauben**. Zielseiten sehen Ihre Verbindung/IP; keine Website-Liste geht an das LMS.
3. Klicken Sie auf **Alte Websites prüfen**. Für die Onlineprüfung ist die Pro-Freigabe erforderlich.
4. Lesen Sie Fortschritt und Abschlussmeldung: bearbeitete Einträge, online geprüfte Ziele sowie übersprungene Kategorien. Mit **Prüfung abbrechen** oder durch Entziehen der Einwilligung stoppen Sie weitere Anfragen.

Die Prüfung berücksichtigt Login-Einträge mit bekannter letzter Nutzung vor mehr als zwei Jahren. Importierte Einträge ohne Nutzungsdatum werden nicht als alt eingestuft. Geprüft werden öffentliche HTTPS-Origins ohne Anmeldung, Pfad oder URL-Geheimnisse. Eine 24-Stunden-Pause und gemeinsame Websites können weitere Anfragen verhindern. Die Prüfung ist keine Anmeldung und prüft nicht, ob Ihr Konto noch besteht.

Ergebnisse richtig verstehen

Die Liste zeigt unter anderem Erreichbar, Problem beobachtet, Ziel geändert, Nicht sicher prüfbar oder Prüfung unklar. „Nutzung unbekannt“ und „Nicht älter als zwei Jahre“ erklären übersprungene Einträge. Ein einzelner Netzwerkfehler beweist keine dauerhaft verschwundene Website. Erst mindestens fünf verteilte 404-/410-Belege über mehr als 30 Tage können „Bereinigung prüfen“ ergeben. Erfolg oder eine Lücke über sieben Tage unterbrechen die Serie.

Mehrere Einträge bewusst entfernen

1. Prüfen Sie die ausgewählten Konten unabhängig. Mit **Website öffnen** oder **Bearbeiten** prüfen Sie einen einzelnen Eintrag.
2. Wählen Sie mehrere Zeilen mit Strg/Umschalt oder **Alle auswählen**. Klicken Sie **Ausgewählte löschen....** Die Auswahl kann auch Einträge ohne Bereinigungsempfehlung enthalten.
3. Kontrollieren Sie die vollständige Liste im Bestätigungsdialog. Belassen Sie die empfohlene **gemeinsame verschlüsselte Sicherung** und wählen Sie deren Ziel. Sie enthält den gesamten Tresor vor der Sammelaktion.
4. Bestätigen Sie mit **Auswahl entfernen**. Eine einzige Sicherung wird angelegt und die Sammeländerung einmal gespeichert. Ein Sicherheitsfehler verhindert die Löschung.

Ohne zusätzliche Sicherung ist eine ausdrückliche weitere Bestätigung erforderlich. Vorhandene Backups und .bak werden nicht vernichtet. Entfernen aus Guardian löscht kein Konto beim Anbieter. Prüfmetadaten sind an das Windows-Benutzerkonto gebunden und nicht Teil der portablen Tresordaten.

Dependency Mapping: Umstellungen verfolgen

Wo wird derselbe Zugang verwendet?

Dependency Mapping dokumentiert Anwendungen und Dienste, in denen ein Zugang verwendet wird. Nach einer Passwort- oder Schlüsseländerung können Sie jede erforderliche Umstellung einzeln verfolgen. Guardian erkennt diese Abhängigkeiten nicht automatisch und prüft die tatsächliche Anmeldung beim Anbieter nicht.

1. Öffnen Sie **Werkzeuge** → **Secret Inventory...** oder **Credential Lifecycle...**. Wählen Sie einen Zugang und anschließend **Abhängigkeiten...**
2. Klicken Sie **Abhängigkeit hinzufügen...**. Tragen Sie Anwendung / Dienst, Umgebung, Verantwortlich und einen Hinweis zur Umstellung ein. Eine Anwendung oder ein Dienst muss angegeben sein.
3. Speichern Sie die Zuordnung. Ergänzen Sie bei Bedarf weitere Anwendungen oder Dienste. Die Übersicht zeigt offene und bestätigte Umstellungen für den aktuellen Durchlauf.
4. Führen Sie die Änderung außerhalb von Guardian durch und testen Sie den jeweiligen Zugang. Wählen Sie die betreffende Zuordnung und **Umstellung bestätigen**.

Ein Beispiel

Ein API-Key wird in einer Anwendung und in einem geplanten Auftrag verwendet. Erneuern Sie den Schlüssel beim Anbieter, hinterlegen Sie den neuen Wert in Guardian und stellen Sie beide Verwendungen um. Bestätigen Sie jede Zuordnung erst nach eigener Prüfung. Eine Bestätigung ist Ihre Dokumentation und keine automatische Funktionsprüfung durch Guardian.

Aktion	Wirkung
Bearbeiten	Ändert die dokumentierte Zuordnung. Ein Doppelklick öffnet ebenfalls den Editor.
Wieder offen setzen	Nimmt die Bestätigung dieser Zuordnung im aktuellen Durchlauf zurück.
Zuordnung entfernen	Entfernt nur die Zuordnung. Zugang und frühere Eintragsversionen bleiben erhalten.
Neuer Umstellungsdurchlauf...	Setzt nach Bestätigung alle Zuordnungen wieder offen. Für jede weitere Erneuerung ausdrücklich neu starten.

Die Übersicht zeigt Anwendung / Dienst, Umgebung, Verantwortlich, Umstellungsstatus und Bestätigungszeitpunkt. Offene Umstellungen ergänzen den Handlungsbedarf in den Verwaltungsübersichten. Änderungen benötigen eine gültige Pro-Berechtigung. Die Daten liegen verschlüsselt im Tresor; frühere Bestätigungen bleiben in der Eintragshistorie. Verschlüsselte Backups und KDBX erhalten die Zusatzdaten; CSV nicht.

Kontinuierliche Leak-Warnungen einrichten

Bewusst aktivieren

Das optionale Leak-Monitoring arbeitet nach Aktivierung in einem separaten Hintergrundmodus im angemeldeten Windows-Konto. Es prüft etwa alle sechs Stunden und kann bei geschlossenem Hauptprogramm und gesperrtem Tresor weiterarbeiten. Es speichert kein Masterpasswort und entsperrt den Tresor nicht. Der Browserbaustein wird dafür nicht benötigt.

1. Öffnen und entsperren Sie den Tresor. Wählen Sie **Werkzeuge** → **Sicherheitsprüfung** und dort **Leak-Monitoring...**
2. Im Reiter **Überwachung einrichten** wählen Sie eine Quelle: den kostenlosen öffentlichen HIBP-Katalog oder über **Eigene Leakdatei...** einen eigenen zulässigen lokalen JSON-Datenbestand. Mindestens eine Quelle ist erforderlich.
3. Markieren Sie nur Ihre eigenen Konten in der Auswahlliste. Optional aktivieren Sie **Eigene E-Mail-Adressen für lokale Identitätstreffer einbeziehen**. Diese Option allein liefert noch keinen persönlichen Leakdatenbestand.
4. Klicken Sie **Auswahl übernehmen**. Guardian speichert die bewusst registrierten Bezeichnungen, Domains und optional E-Mail-Fingerabdrücke außerhalb des Tresors mit Windows-DPAPI geschützt. Passwörter werden nicht übernommen.
5. Klicken Sie **Aktivieren / Übernehmen**. Lesen und bestätigen Sie den Hinweis zu Hintergrundbetrieb und Start bei der Windows-Anmeldung. Dafür wird eine gültige Pro-Lizenz geprüft.
6. Verwenden Sie **Jetzt prüfen** und kontrollieren Sie den Status, die Zeitpunkte der letzten Prüfungen und gegebenenfalls die Hinweise.

Auswahl aktuell halten

Änderungen an Eintrag, Domain oder E-Mail-Adresse aktualisieren die Watchliste nicht automatisch. Übernehmen Sie die gewünschte Auswahl ausdrücklich erneut. Zum Abmelden markieren Sie Einträge in der Überwachungsliste und wählen **Überwachung entfernen**. Damit entfernen Sie die Monitoringregistrierung, nicht den Tresoreintrag.

Abschalten und vorübergehend beenden

Deaktivieren schaltet die Überwachung aus und entfernt ihren Autostart. Das Abschalten und Entfernen von Registrierungen ist auch ohne aktive Pro-Lizenz möglich. Über das separate Monitor-Symbol im Windows-Infobereich können Sie den Hintergrundmodus **Bis zur nächsten Anmeldung beenden**. Das ist keine dauerhafte Deaktivierung.

Ein ausgeschalteter oder abgemeldeter PC kann keine lokale Prüfung oder Sofortmeldung ausführen. Beim nächsten Start wird nachgeholt; bei Fehlern werden weitere Versuche verzögert. Windows-Einstellungen können Meldungen unterdrücken. Die vollständige Liveprüfung dieser Fälle ist noch offen.

Hinweise und Datenquellen verstehen

Prüfung	Was ein Treffer aussagt
Manuelle Passwort-Leakprüfung	Ein gespeicherter Passwortwert ist in bekannten Passwort-Leakdaten enthalten. Kein Nachweis eines Einbruchs in das zugeordnete Konto.
Öffentlicher Dienstkatalog	Eine Meldung passt zum registrierten Dienst / zur Domain. Keine persönliche Zuordnung Ihrer E-Mail-Adresse und kein Nachweis zur Offenlegung Ihres aktuellen Passworts.
Eigene lokale Leakdatei	Ein registrierter E-Mail-Fingerabdruck stimmt mit einem Datensatz in Ihrer eigenen Datei überein. Aussagekraft und Abdeckung hängen von dieser Quelle ab. Guardian verifiziert deren Herkunft oder Richtigkeit nicht.

Hinweise lesen und bearbeiten

1. Öffnen Sie das Leak-Monitoring und den Reiter **Hinweise**. Wählen Sie eine Meldung.
2. Lesen Sie Quelle, Vorfalldatum und Erkennungszeitpunkt. Prüfen Sie die offiziellen Hinweise des betroffenen Anbieters. Ein später entdeckter Hinweis kann einen lange zurückliegenden Vorfall betreffen.
3. Ändern Sie bei Betroffenheit das Passwort beim Anbieter, vermeiden Sie Wiederverwendung und aktivieren Sie einen zweiten Faktor. Aktualisieren Sie Guardian danach.
4. Dokumentieren Sie erforderliche Erneuerungen im Credential Lifecycle und prüfen Sie betroffene Verwendungen im Dependency Mapping.
5. Mit **Als gelesen** markieren Sie die Meldung als gelesen. Das bestätigt weder eine Passwortänderung noch die fachliche Erledigung.

Benachrichtigungen im Hintergrund sind neutral und enthalten keine Kontodetails. Details lesen Sie in Guardian. Die Pro-Berechtigung wird vor der Abfrage und vor der Ergebnisübernahme geprüft. Ein Quellen- oder Lizenzfehler ist kein Ergebnis „keine Leaks“. Beachten Sie die letzte vollständige Prüfung und die getrennten Zeitangaben je Quelle.

Eigene Leakdatei: optional, nicht mitgeliefert

Erforderlich ist eine UTF-8-JSON-Datei im dokumentierten Guardian-Feedformat Version 1 auf einem lokalen festen Laufwerk, maximal 16 MiB. PublishedAt muss innerhalb der letzten sieben Tage liegen und darf höchstens fünf Minuten in der Zukunft liegen. Veraltete, ungültige oder doppelte Vorfallkennungen werden abgewiesen. Mit **Datei lösen** entfernen Sie die gewählte Quelle; übernehmen Sie die Änderung anschließend.

Die Datei enthält Vorfallkennungen, Titel, Vorfalldatum und E-Mail-Fingerabdrücke, keine Rohpasswörter, Tokens oder Cookies. Fingerabdrücke werden aus getrimmten, NFC-normalisierten, kleingeschriebenen E-Mail-Adressen als SHA-256 gebildet und bleiben rückführbar. Für die technische Bereitstellung dient die Projektdokumentation `monitoring-feed-format.md`. Schützen Sie Datei und Quellbestand.

Ohne eigenen aktuellen Datenbestand sind persönliche Dark-Web-/Leakdaten nicht abgedeckt. Guardian liefert keine vollständige Dark-Web-Suche und beschafft keine persönlichen Leakdaten. Keine Treffer sind keine Sicherheitsgarantie. Eine zentrale Vorfalldatenbank und eine angebotene API sind spätere Planungen.

Einstellungen, Updates und Deinstallation

Sicherheit und Bedienung einstellen

Öffnen Sie **Werkzeuge** → **Einstellungen**. Auto-Lock sperrt bei Inaktivität auch im Hintergrund. Clipboard Auto-Clear entfernt nach der gewählten Zeit die eigene noch aktuelle Kopie. Zwischenzeitlich von Ihnen kopierter fremder Inhalt bleibt erhalten. Windows-Zwischenablageverlauf und Drittprogramme können zusätzliche Kopien besitzen.

Für Doppelklicks können unter anderem Quick View, Passwort kopieren, Website öffnen und Bearbeiten gewählt werden. Eine aufgeführte AutoFill-Option macht die geplante Browserintegration noch nicht verfügbar. Beim Schließen über X wählen Sie zwischen Hintergrundbetrieb und vollständigem Beenden. Im Hintergrund bleibt Guardian im Infobereich erreichbar; Auto-Lock läuft weiter. **Datei** → **Beenden** beendet das Hauptprogramm unabhängig von der X-Einstellung. Ein ausdrücklich aktivierter Leak-Monitor läuft separat weiter (Kapitel 13/14).

Darstellung

Die dokumentierte Darstellungswahl umfasst ALPEG Dunkel, Windows Hell und Systemeinstellung folgen sowie zusätzliche Farbschemata. Die Akzentwahl umfasst ALPEG Blau, Petrol, Salbeigrün, Violett, Graphit, Mattgold und Systemfarbe. Prüfen Sie die Vorschau und klicken Sie Speichern. Abbrechen behält die bisherigen Einstellungen. **Ansicht** → **Compact Mode** verkleinert das Fenster; das Detailpanel lässt sich gesondert umschalten.

Updates prüfen und installieren

1. Erstellen Sie vor jeder Aktualisierung ein externes verschlüsseltes Backup.
2. Öffnen Sie **Hilfe** → **Nach Updates suchen....** Unter **Hilfe** → **Update-Einstellungen...** können Sie die automatische tägliche Suche einstellen.
3. Ein Update wird nur angeboten, wenn der Editionskanal ein passendes neueres freigegebenes Paket bereitstellt. Eine neuere Website-Version muss deshalb nicht automatisch im Programm erscheinen.
4. Wenn ein Angebot vorliegt, lesen Sie die Hinweise und stimmen Sie dem Download zu. Der Client prüft Manifest/Download und fragt vor der Installation nochmals nach.
5. Nach der Installation prüfen Sie die Version unter Hilfe → Über Guardian und testen das Öffnen Ihres Tresors.

Die Updateprüfung verbindet sich laut Quellcode mit www.alpeg-systems.com; dabei werden keine Tresorinhalte, Lizenzdaten oder Geräteerkennung übertragen. Ohne Verbindung bleibt Guardian nutzbar. Der Veröffentlichungsnachweis für 1.3.0 bestätigt: Die Bereitstellung erfolgt über Shop und manuellen Download; der programminterne Updatekanal bietet diese Version derzeit nicht an.

Deinstallieren

Sichern Sie Tresore extern, beenden Sie Guardian und verwenden Sie die reguläre Windows-App-Deinstallation. Laut Projektdokumentation bleiben Tresore und Nutzerdaten standardmäßig erhalten; eine optionale Datenlöschung verlangt zusätzliche Bestätigung. Prüfen Sie die tatsächlich angezeigten Optionen. Extern gespeicherte Tresore bleiben erhalten. Eine Deinstallation ist kein Nachweis forensischer Datenvernichtung.

Fehlerbehebung und Tastenkürzel

Situation	Vorgehen
Passwort falsch / Datei beschädigt	Tastaturlayout, Dateiauswahl und Eingabe prüfen. Bekannte Sicherung mit dem damals gültigen Passwort testen. Beide Ursachen werden absichtlich nicht sicher unterschieden.
Tresor bereits geöffnet	Andere Sitzung regulär schließen. Nicht gleichzeitig dieselbe Datei bearbeiten und keine aktive .lock-Datei löschen.
Import leer / unvollständig	Exportformat, Feldzuordnung und Warnungen prüfen. Für KDBX Passwort und nur bei tatsächlicher Nutzung zusätzliche Schlüsseldatei angeben.
Login nach Änderung fehlerhaft	Prüfen, ob das Passwort beim Anbieter geändert wurde. Eine Änderung nur in Guardian genügt nicht.
Generator wirkt nicht	Ergebnis ist maskiert. Im Editor Übernehmen wählen; Kopieren setzt nur die Zwischenablage.
Pro-Aktion gesperrt	Pro-Lizenz öffnen, Internet und Uhrzeit prüfen, Erneut prüfen verwenden. Basistresor, Backup und Export bleiben nutzbar.
Website-Scan ohne Onlineprüfungen	Abschlussmeldung lesen: unbekannte/jüngere Nutzung, Pause, gleiches Ziel oder unsichere Adresse können die Ursache sein.
Guardian bleibt nach X aktiv	Hintergrundbetrieb des Hauptprogramms prüfen. Ein aktivierter Leak-Monitor läuft separat; über Leak-Monitoring → Deaktivieren ausschalten.

Tastenkombinationen

Tasten	Aktion
Strg+F / Strg+N / Strg+E	Suchen / Neuer Eintrag / Bearbeiten
Strg+D / Strg+Umschalt+S	Duplizieren / Favorit umschalten
Strg+L / Leertaste / Strg+Alt+D	Sperren / Quick View / Detailpanel
Strg+C / Strg+Umschalt+C	Benutzername kopieren / Passwort kopieren
Strg+Umschalt+O / Strg+Enter	TOTP kopieren / Website öffnen
Strg+Umschalt+T / Entf	Auto-Type / Löschen mit Bestätigung

Für Supportfälle notieren Sie Pro-Version, Build, Windows-Version, Fehlertext und die betroffene Aktion. Entfernen Sie Passwörter, TOTP-Secrets, Aktivierungscodes und ungeschützte Tresorinhalte aus allen Unterlagen.

Quellen, Prüfstatus und Versionshistorie

Versionshistorie des Handbuchs

Pro-Version	Dokumentstand und Umfang
1.3.0	17.10.2026 · Aktualisierte Ausgabe für 1.3.0-pro.monitoring.1. Einschließlich Dependency Mapping und kontinuierlicher Leak-Warnungen. Ersetzt die zuvor erstellte Ausgabe 1.1.0.
1.1.0	17.10.2026 · Frühere Handbuchausgabe für management.2; durch diese Ausgabe abgelöst.

Geprüfter Release

Abgleich mit dem Chat „Zahlungsarchitektur integrieren“: Guardian Pro 1.3.0 wurde am 17.10.2026 veröffentlicht. Der Veröffentlichungsbericht bestätigt Shopbereitstellung und manuellen Download. Der lokale Installer stimmt mit den dort dokumentierten 69.878.731 Bytes und der SHA-256-Prüfsumme überein. Die Programmdatei nennt 1.3.0-pro.monitoring.1 und Quellrevision 6a81ab394ec60909cb6fbd8a3f1003ad369eeedd. [1]

Installer: ALPEG-Guardian-Pro-1.3.0-pro.monitoring.1-Setup-x64.exe
SHA-256:
64e666a4861aef255613f40d67bc6221ba585ea9984720e3f25d19932ef8948a

Quellen und Einordnung

[1] Lokales Projekt guardian-pro-management / Pro: VEROEFFENTLICHUNG-2026-10-17.md; PRO-MANAGEMENT-v1.md; CHECKER-CLEANUP-v2.md; ABNAHME-DEPENDENCIES-2026-10-17.md; MONITORING-INTEGRATIONSPLAN-2026-10-17.md; Hilfebibliothek und monitoring-feed-format.md. Menü-, Lizenz-, Management-, Dependency-, Monitoring-, Setup- und Updatequellen wurden ergänzend gelesen. Der historische Kandidatenstatus einzelner Dokumente wird durch den späteren Veröffentlichungsnachweis eingeordnet. Prüfstand: 17.10.2026.

[2] Chat „Zahlungsarchitektur integrieren“: Veröffentlichung von 1.3.0, manueller Updateweg, Abdeckungsgrenze des Monitorings und Darstellung der Browserintegration als in Planung. Die Produktseite war in dieser Sitzung nicht direkt abrufbar; der dort dokumentierte frühere Onlineabgleich wird nicht als neuer Liveabruf ausgegeben.

Offizielle Produktseite: www.alpeg-systems.com/produkte/guardian. Produktabbildung vom Auftraggeber. Gestaltung nach Auftrag: dunkel/gold.

Noch zu verifizieren

Die Veröffentlichung ist bestätigt. Sie ersetzt keine vollständige Betriebsprüfung: Installation/Upgrade/Deinstallation, Windows-Neuanmeldung, Sperrbildschirm, Benachrichtigungsunterdrückung und alle sichtbaren Beschriftungen sind für das konkrete Setup weiter zu prüfen. Dokumentierte synthetische Tests sind kein Nachweis dieser Liveabläufe.

Der genaue Shopweg zum Aktivierungscode, Gerätewechsel und -freigabe, vertragliche Gerätegrenzen und konkrete Offline-Lizenzfristen sind vor einer verbindlichen Anleitung zu verifizieren. Persönliche Leak-/Dark-Web-Treffer bleiben ohne eigenen aktuellen Datenbestand nicht abgedeckt. Die geplante zentrale Vorfalldatenbank und API sind keine enthaltenen Funktionen.