

# Password Guard<sup>v4</sup>

## Benutzerhandbuch



# Password Guard<sup>v4</sup>

Benutzerhandbuch



# Inhalt

<b>Einführung</b>	<b>9</b>
Übersicht	9
Sicherheitsmerkmale	10
Hinweise zum Systemschutz	11
Installation	12
<b>Kennwörter verwalten</b>	<b>15</b>
Kennwortliste anlegen	15
Kennwortliste zum Bearbeiten öffnen	17
Listeneinträge hinzufügen	17
Symbol und Formularsteuerung	19
Listenansicht und Navigation	20
Kategorien verwalten	20
Masterpasswort ändern	20
Statusbericht	21
Kennwortliste drucken	22
Datenaustausch	22
GoMobile!	22
Anmeldedaten auf Webseiten einfügen	23
Sicherheit von Kennwörtern verbessern	24
<b>Kennwortgenerator</b>	<b>27</b>
<b>Kennwortanalyse</b>	<b>29</b>

<b>Softwarelizenzen verwalten</b>	<b>31</b>
Übersicht	31
Listeneinträge hinzufügen	32
Listenansicht und Navigation	33
Lizenzliste drucken	34
<b>Express Cleaner</b>	<b>37</b>
<b>Datenshredder</b>	<b>39</b>
<b>Programmooptionen</b>	<b>41</b>
Allgemeine Einstellungen	41
Sicherheitseinstellungen	42
Datei-Sicherungskopien	43







# Einführung

## Übersicht

Viel Geld und Nerven kosten Anwendern ausspionierte PINs, gehackte E-Mail- oder Benutzerkonten. Die Hauptursache dabei ist, dass mit Zugangsdaten entweder einfach zu gedankenlos umgegangen wird oder entsprechende Passwörter zu einfach gewählt werden.

Natürlich sind solche Verhaltensweisen verständlich, denn wer kann sich schon wirklich sicherere Kennwörter merken, also beispielsweise einen kryptischen Zeichensalat, der zwar jedem Angriff eines Hackers Stand hält aber extrem abstrakt auf den Betrachter wirkt.

Hier kann Ihnen Password Guard v4 jetzt seine unschätzbaren Dienste anbieten: Endlich können Sie wirklich sichere Kennwörter generieren, anwenden, verwalten, pflegen und auch vor Hackern geschützt aufbewahren und durch die entsprechende Autorisation jeder Zeit immer wieder ganz einfach abrufen.

Zusätzlich bietet Ihnen Password Guard v4 folgende nützliche Funktionen, die das Leistungsspektrum abrunden:

- Kennwortgenerator zum Generieren von individuellen Passwörtern
- Kennwortanalyse zur Überprüfung der Qualität von Passwörtern
- Lizenzverwaltung für erworbene Softwarelizenzen und Product Keys
- Datenshredder zum sicheren und unwiderruflichen Löschen von Dateien
- Express Cleaner zum schnellen Bereinigen sensibler Systemdaten
- Automatische Erstellung von Sicherheitskopien von Programmdateien

Eine wichtige Neuerung in dieser Programmversion sind die verbesserten und mehr personalisierbaren Sicherheitsfunktionen, die jeder Zeit sicherstellen, dass diese Kennwortverwaltung allen Angriffsversuchen von außen Stand hält. Das hier gebotene Sicherheitsnetz ist einzigartig und in seiner Komplexität all umfassend.

## Sicherheitsmerkmale

Password Guard v4 weist eine Vielzahl von Sicherheitsfunktionen auf, die Ihre sensiblen Daten effektiv vor unbefugtem Zugriff schützen und Sie als Anwender hilfreich unterstützen.

Als primäre Sicherheitsfunktionen wären hierbei zu nennen:

- Blowfish 448 bit-Datenverschlüsselung
- Brute Force-Schutz für alle Autorisationsdialoge
- Proaktiver Schutz vor schädlicher Software
- Warnung vor Prozessen mit Zwischenablagezugriff

Als sekundäre Sicherheitsfunktionen wären zu nennen:

- Verschlüsselte Datenbanken und Transferdateien
- Schutz des Masterpasswortes vor externem Zugriff
- Verschlüsselter Speicher für Programmoptionen
- Laufzeitverschlüsselung für sensible Daten

Folgende Funktionen runden das Sicherheitspaket ab:

- Überprüfung von sensiblem Zwischenablageinhalt
- Meldung fehlgeschlagener Autorisationsversuche
- Optionales Gültigkeitsdatum für Zugangsdaten
- Protokollierung von Systemereignissen

Als Anwender werden Sie zusätzlich durch folgende Funktionen unterstützt:

- Automatisches Schließen geöffneter Kennwortlisten
- Kennwortgenerator mit statistischer Streuung
- Kennwortanalysefunktion für sichere Kennwörter
- Hinweis auf unsichere Zugangsdaten

Die Anzeige des Systemprotokolls, in dem alle relevanten Ereignisse und Aktionen aufgeführt werden, erreichen Sie übrigens über den Menüpunkt „Optionen“ in den Sicherheitseinstellungen und den dort verfügbaren Link „Systemprotokoll anzeigen“.

## Hinweise zum Systemschutz

Während Ihrer Arbeit mit Password Guard kann es vorkommen, dass Ihnen der integrierte Systemschutz Warnmeldungen oder Fragen zur Legitimation von ausgeführten Prozessen stellt. Prüfen Sie bei jeder Warnmeldung bzw. der zu erfolgenden Autorisation genau, ob Sie dem Herausgeber des betroffenen Programmes vertrauen oder ob der Systemschutz ggf. sogar ein unerwünschtes schädliches Programm auf Ihrem Computer entdeckt hat.

Bei jeder Systemschutz-Benachrichtigung haben Sie zum Zwecke der Prüfung die Möglichkeit, den Speicherort und den Eigenschaftsdialog des betroffenen Programmes zu betrachten. Der Link „Welche Gefahren bestehen hier?“ erläutert Ihnen zudem immer genau, um welche potentielle Gefahr es sich handelt, die dem betroffenen Programm zuzuordnen wäre.

Wenn Sie einen Prozess bzw. Programm autorisiert haben, wird für dieses Programm keine weitere Warnmeldung mehr eingeblendet. Programme, die über ein extremes Bedrohungspotenzial für sensible Daten verfügen, können aus Sicherheitsgründen nicht autorisiert werden; solche Programme werden automatisch beendet, um die verarbeiteten Kennwortdaten vor unbefugtem Zugriff zu schützen.

## Installation

1. Starten Sie Ihren Computer und legen Sie die Password Guard-Programm-CD-ROM in das Laufwerk ein. Wenn Sie das Programm als Download erworben haben, fahren Sie bitte mit Schritt 5 fort.
2. Für den Fall, dass die automatische Benachrichtigung beim Wechsel aktiviert ist, wird die Installationsroutine kurze Zeit nach Einlegen der CD ohne weitere Anwenderinterventionen gestartet.
3. Sollte die Installations-Routine nicht selbstständig gestartet sein, öffnen Sie bitte das Arbeitsplatz-Verzeichnis auf Ihrem Desktop durch einen Doppelklick und markieren Sie im darauffin erscheinenden Fenster das Laufwerk, in dem die Password Guard-CD-ROM eingelegt worden ist.
4. Doppelklicken Sie anschließend auf das markierte CD-ROM-Laufwerk-symbol.
5. Starten Sie die Installation mit einem Doppelklick auf die Datei setup.exe
6. Nach Abschluss der Installation rufen Sie „Password Guard“ aus dem Startmenü aus auf, um das Programm zu starten.





# Kennwörter verwalten

## Kennwortlisten anlegen

Nach der Installation des Programmes sind, wenn Sie nicht schon bereits die Vorgängerversion auf Ihrem Computer genutzt haben, noch keine gültigen Kennwortlisten vorhanden bzw. abrufbar. Wenn Sie im Menü eine der Kennwortlisten aufrufen („Meine Kennwörter“, „Geschäftlich“ oder „Gemeinsame Kennwörter“), gelangen Sie automatisch zum Assistenten zum Anlegen einer Kennwortliste. Hier geben Sie dann Ihr Masterpasswort und einen Kennworthinweis als Gedankenstütze ein, um die entsprechende Kennwortliste zu erstellen.

Unterstützt werden Sie dabei von der Möglichkeit, den Kennwortgenerator zur Erstellung zu verwenden sowie eingeblendeten Informationen, die das von Ihnen verwendete Masterpasswort bewerten, also konkret seine Qualität und eventuell vorhandene Schwachstellen.

Ihre Kennwortdaten werden von Password Guard in einer verschlüsselten und extrem sicheren Datenbank gespeichert. Der zu Grunde liegende Verschlüsselungsalgorithmus ist dabei der 448bit starke Blowfish-Algorithmus und verwendet als Hauptschlüssel Ihr Kennwortlisten-Masterpasswort.

Das Kennwortlisten-Masterpasswort ist Ihr einziger Schlüssel zu den gespeicherten Daten einer Kennwortliste. Der Vorteil des Masterpasswort-Verfahrens ist, dass Sie sich in Zukunft nur noch ein einziges Kennwort merken müssen, egal wie viele Kennwörter Sie zu verwalten haben. Mit dem Masterpasswort Ihrer Kennwortliste haben Sie Zugriff auf alle mit Password Guard gespeicherten Kennwörter. Auch dient das Masterpasswort gleichzeitig als Autorisation beim Ausfüllen von Anmeldeinformationen auf Webseiten.

Aus diesem Grund sollten Sie

- Ihr Masterpasswort nicht zu einfach wählen, um durch simples Erraten des Kennwortes den Zugang zu Ihren Daten zu ermöglichen
- Ihr Masterpasswort nie vergessen, da Sie ansonsten nie wieder Zugriff auf die gespeicherten Kennwortdaten erhalten können

Ein sicheres Kennwort sollte für einen Angreifer nur eine zufällige Zeichenfolge sein. Die folgenden Kriterien sollten Sie bei der Wahl Ihres Masterpasswortes beachten:

**Wählen Sie ein langes Kennwort.** Jedes Zeichen, das Sie Ihrem Kennwort hinzufügen, erhöht den Schutz um ein Vielfaches. Ihr Kennwort sollte mindestens 8 Zeichen enthalten, 14 oder mehr sind ideal.

**Kombinieren Sie Buchstaben, Ziffern und Symbole.** Je mehr verschiedene Zeichenarten Ihr Kennwort enthält, desto schwerer ist es zu erraten. Weitere wichtige Besonderheiten:

**Je weniger verschiedene Zeichenarten Ihr Kennwort enthält, desto länger muss es sein.** Ein Kennwort mit 15 Zeichen, das nur aus willkürlich ausgewählten Buchstaben und Ziffern besteht, ist 33.000 Mal sicherer als ein Kennwort, das 8 Zeichen der gesamten Tastatur enthält. Wenn Sie kein Kennwort mit Symbolen erstellen können, müssen Sie ein erheblich längeres Kennwort wählen, um denselben Schutz zu erzielen. Ein ideales Kennwort ist lang und besteht aus verschiedenen Symbolen.

**Nutzen Sie die gesamte Tastatur** und nicht nur die am häufigsten verwendeten Zeichen. Symbole, die Sie durch Drücken der Umschalttaste und Eingeben einer Zahl erstellen können, werden häufig in Kennwörtern verwendet. Ihr Kennwort ist sicherer, wenn Sie aus allen Symbolen der Tastatur wählen.

**Verwenden Sie Wörter und Sätze, die Sie sich leicht merken können, für andere jedoch nur schwer zu erraten sind.** Am einfachsten können Sie sich Ihre Kennwörter und Kennsätze merken, indem Sie sie notieren. Im Gegensatz zur weit verbreiteten Meinung spricht nichts dagegen, Kennwörter zu notieren. Sie müssen jedoch ausreichend geschützt werden, damit sie sicher und effektiv bleiben.

Wählen Sie auf jeden Fall kein Kennwort, bei dem auch die Gefahr besteht, dass Sie es vergessen und sich somit eine eigene Falle stellen, die Ihnen letzten Endes den Zugriff auf Ihre eigenen Daten verwehrt.

Achten Sie bei der Eingabe von Kennwörtern auch stets darauf, dass Ihnen niemand über die Schulter schaut und so Ihr Kennwort erfährt. Wenn Sie die Bildschirmtastatur zur Eingabe Ihres Masterpasswortes verwenden, bedenken Sie, dass jede unmittelbar in der Nähe Ihres Monitors befindliche Person Ihre Eingabe noch deutlicher verfolgen kann, als bei der Eingabe durch die Computertastatur.



## Kennwortlisten zum Bearbeiten öffnen

Wählen Sie zum Öffnen einer Kennwortliste die gewünschte Liste im Startmenü des Programms aus, also entweder „Meine Kennwörter“, „Geschäftlich“ oder „Gemeinsame Kennwörter“. Anschließend gelangen Sie zur Eingabe des Masterpasswortes. Wenn dieses Passwort korrekt eingegeben wurde, gelangen Sie zur Listenansicht der angeforderten Kennwortliste.

Zur Eingabe des Masterpasswortes können Sie eine Bildschirmtastatur verwenden, die sich auch an einigen anderen Stellen im Programm verwenden lässt. Die Bildschirmtastatur rufen Sie über den entsprechenden Link am unteren Fensterrand auf. Die Bildschirmtastatur funktioniert wie Ihre Computertastatur: Klicken Sie einfach mit der Maus auf die gewünschten Buchstaben oder verwenden Sie die entsprechenden Umschalttasten zum Ändern der Tastaturbelegung. Durch Anklicken der Eingabetaste schließen Sie Ihre Eingabe ab.

## Listeneinträge hinzufügen

Nach der erfolgten Autorisation zum Öffnen einer Kennwortliste gelangen Sie sofort in die entsprechende Listenansicht. Am unteren Fensterrand finden Sie den Link „Neuer Eintrag“, der Sie zur Eingabe der Daten eines Listeneintrages führt.

Mit Password Guard können Sie hier dann folgende Daten zu einem Kennworteintrag speichern und bearbeiten:

**Kategorie:** Zuerst wählen Sie aus, in welche Kategorie dieser Eintrag fällt. Dies ermöglicht zum Einen das Verwalten von Kennwörtern in verschiedenen Rubriken und zum Anderen werden die Beschriftungen und somit die Funktion entsprechender Eingabefelder sinngemäß angepasst.

**Bezeichnung:** Hier geben Sie einen Namen für den Eintrag ein, der das leichte Wiederauffinden ermöglicht.

**URL für Login:** Hier geben Sie die Internetadresse der verbundenen Webseite ein, auf der ein Anmeldedialog zur Eingabe von Zugangsdaten vorhanden ist. Wenn Sie später diese Webseite besuchen, und die entsprechende Programmoption zum Ausfüllen von Zugangsdaten auf Webseiten aktiviert ist, können Sie nach Autorisation durch Ihr Masterpasswort die Zugangsdaten (Benutzername und Kennwort) bequem eintragen lassen.

**Benutzername:** Hier geben Sie den Benutzernamen der Zugangskennung ein.

**Kennwort:** Hier geben Sie das Kennwort der Zugangskennung ein. Die Sterneskala unten verrät Ihnen immer, wie stark dieses Passwort gegen Angriffe von Hackern ist. Die Schaltfläche „Einblenden“ aktiviert die Anzeige des Passwortes im Klartext. Beim Klicken auf die Schaltfläche „Extras“ rufen Sie ein Menü mit speziellen Funktionen auf. Dieses Menü enthält je nach Status folgende Funktionen:

- Sichereres Kennwort generieren
- Benutzername generieren
- Kennwortgenerator verwenden
- Kennwortqualität analysieren
- Browseradresse als URL einfügen
- Symbol und Formularsteuerung
- Benutzerdefinierte Felder
- TAN-Listenverwaltung
- Zugangsdaten-Änderungsassistent

**Notizen:** Hier können Sie weitere Daten zu diesem Eintrag eingeben, in der Kategorie „E-Mail“ beispielsweise die Daten der E-Mailservers.

**Anlagen:** Über die Schaltfläche „Anlagen“ können Sie beliebige Dateien als Anhang zu einem Listeneintrag hinzufügen.

**Optionen:** Hier können Sie ein Ablaufdatum für die Zugangsdaten speichern und konfigurieren, ob eine Verknüpfung im Favoritenmenü von Password Guard angezeigt wird sowie, ob der Text im Notizfeld nach erfolgtem Login auf einer Webseite als Memo-Fenster eingeblendet werden soll. Dies kann hilfreich sein, wenn die aufgerufene Website beispielweise weitere Autorisationen erfordert und Sie diese Angaben im Notizfeld eingegeben haben und in solchen Fällen zusätzlich benötigen.

Den Eintrag speichern Sie durch Klicken auf den Link „Eintrag speichern“ am unteren Fensterrand. Wenn Sie die Escape-Taste drücken oder den Pfeil links oben anklicken, werden Ihre Eingaben nicht gespeichert und Sie gelangen wieder umgehend zurück zur Listenansicht.

Durch Anklicken des Links „Eintrag löschen“ können Sie den aktuell angezeigten Eintrag löschen. Alternativ können Sie in der Listenansicht auch diesen Eintrag selektieren und dann die Entfernen-Taste drücken.

Wenn Sie die Programmoption „Geöffnete Kennwortlisten im Leerlauf automatisch schließen“ aktiviert haben, finden Sie rechts unten im Eingabedialog ein Stecknadel-symbol, mit dem Sie das automatische Schließen der gerade bearbeiteten Liste temporär deaktivieren können und so verhindern, dass bei eventuell längeren Bearbeitungszeiten der Eingabedialog automatisch geschlossen wird und Daten verloren gehen würden.

## **Symbol und Formularsteuerung**

Die Symbolauswahl und Formularsteuerung für einen Listeneintrag rufen Sie über die Schaltfläche „Extras“ neben dem Eingabefeld für das Kennwort auf.

Hier können Sie das Listensymbol für einen Eintrag anpassen und vorgeben, ob beim Besuch der im Adressfeld (Login-URL) angegebenen Webseite im Browser die Automatik zum Ausfüllen der Zugangsdaten eingeblendet werden soll oder der manuelle Abruf vorbereitet werden soll, falls es beim automatischen Ausfüllen permanent zu Problemen kommen sollte.

Der manuelle Abruf steht Ihnen dann jeweils ganz komfortabel zur Verfügung: Wenn Sie die entsprechende Webseite besuchen, ändert sich das Password Guard-Symbol im Infobereich in einen blauen Pfeil. Zusätzlich wird ein Info-Fenster eingeblendet, dass Sie darauf hinweist, dass Sie die Daten der Benutzeranmeldung manuell abrufen und einfügen können.

Sollte der Aufbau des Anmeldeformulars auf der zu diesem Kennwortlisteneintrag gehörenden Webseite vom Standard abweichen, also das Eingabefeld für das Benutzerkennwort nicht direkt nach dem Eingabefeld des Benutzernamens folgen, können Sie zusätzlich angeben, wie das Anmeldeformular genau aufgebaut ist und so die automatische Ausfüllsequenz bequem anpassen.

Zum Abschluss bietet Ihnen der Dialog für die Formularsteuerung noch die Option, ob das Anmeldeformular stets nach dem Ausfüllen automatisch abgesendet werden soll. Verlangt die entsprechende Webseite mehr Eingaben als nur den Benutzernamen und das Kennwort, können Sie so sicherstellen, dass nach dem automatischen Einfügen dieser Daten noch die Gelegenheit für zusätzliche Eingaben besteht.

Die Optionen für den Aufbau des Anmeldeformulars und das automatische Absenden haben natürlich keine Wirkung, wenn Sie die Anmeldeinformationen manuell einfügen. Diese Optionen steuern jeweils nur den automatischen Ablauf.

## Listenansicht und Navigation

Am oberen Rand der Kennwortlistenansicht finden Sie die Kategorieauswahl. Wenn Sie eine Kennwortliste geöffnet haben, ist noch keine Kategorie ausgewählt und alle gespeicherten Listeneinträge werden ungefiltert angezeigt und sind somit auch schnell zu erreichen.

Wünschen Sie eine Filterung von Einträgen einer bestimmten Kategorie, dann klicken Sie auf den gewünschten Kategorienamen in dieser Leiste. Durch erneutes Klicken, wird diese Filterung wieder aufgehoben und alle Elemente werden angezeigt. Mit der STRG-Taste und den Cursor-rechts/links-Tasten können Sie durch die Kategorien blättern.

Wenn Sie nach einem Listenelement suchen möchten, geben Sie den entsprechenden Suchbegriff in das Suchfeld rechts oben ein.

Zum Navigieren durch die Liste können Sie hier das Mausrad oder die Cursortasten verwenden. Um einen Eintrag mit einem bestimmten Anfangsbuchstaben schnell zu selektieren, tippen Sie einfach diesen Buchstaben ein. Selbstverständlich sind auch die Bild aufwärts/abwärts, Pos1 und Ende-Tasten verfügbar, um schnell innerhalb einer Listenansicht navigieren zu können.

Sind in einer Listenansicht mehr als 18 Elemente enthalten, weist Sie ein Pfeilsymbol beim Einblenden kurz darauf hin, dass Sie durch Scrollen der Liste nach unten zu weiteren Elementen gelangen können.

Rechts unten finden Sie in der Listenansicht stets zur Information noch die Anzahl der enthaltenen Einträge.

Das jeweils selektierte Element einer Liste erkennen Sie durch die vergrößerte Darstellung. Wenn Sie ein solches Element anklicken oder die Eingabetaste drücken, gelangen Sie stets zum Eingabedialog für den Datensatz dieses Eintrages.

## **Kategorien verwalten**

Um die Kategorien Ihrer Kennwortliste zu erweitern oder individuell anzupassen, klicken Sie bitte in der Kategorieauswahlleiste oben auf den kleinen Pfeil links. Hier öffnet sich ein Menü, mit dem Sie schnell eine neue Kategorie erstellen können oder alle Kategorien Ihrer Kennwortliste bearbeiten können.

Für jede Kategorie können Sie eine individuelle Bezeichnung, den Datentyp, eine Beschreibung und ein Standard-Symbol festlegen.

Um Kategorien in der Kategorieauswahlleiste selbst umzusortieren, halten Sie bitte die Umschalttaste gedrückt und ziehen Sie den entsprechenden Eintrag mit der Maus an die gewünschte neue Position.

Wenn Sie einen Listeneintrag in eine andere Kategorie einsortieren möchten, können Sie in der neuen Programmversion den entsprechend markierten Eintrag auf die Kategorieauswahlleiste oben ziehen.

## **Masterpasswort ändern**

Um das Masterpasswort einer Kennwortliste von Zeit zu Zeit ändern zu können, klicken Sie in der Listenansicht auf den entsprechenden Link unten am Fensterrand. Anschließend geben Sie das aktuelle Kennwort zur Autorisation sowie das neue Kennwort und den neuen Kennworthinweis ein.

## **Statusbericht**

Password Guard bietet Ihnen mit dem Statusbericht die Möglichkeit, die gespeicherten Kennwortdaten in Bezug auf die Sicherheit der Daten zu prüfen. Den Statusbericht für eine Kennwortliste rufen Sie über den entsprechenden Link in der Kennwortlistenansicht auf.

Die hier einsehbare Sicherheitsbewertung der einzelnen Listeneinträge gibt die Kennwortstärke und eventuelle Sicherheitsrisiken übersichtlich wieder.

## **Kennwortliste drucken**

Auf der Seite „Statusbericht“ finden Sie einen Link, mit dem Sie die aktuell geöffnete Kennwortliste auf einen Drucker ausgeben können. Bewahren Sie solche gedruckten Listen unbedingt an einem sicheren Ort auf, um sich selbst vor Schaden durch Missbrauch dieser Daten zu bewahren.

Nicht mehr benötigte oder veraltete Ausdrücke sollten Sie zudem stets gewissenhaft vernichten, um keinen unbefugten Dritten ungewollt Auskunft über die dort offenbarten Daten zu geben.

## **Datenaustausch**

Um Daten zwischen verschiedenen Kennwortlisten auszutauschen, klicken Sie einfach auf den Link „Datenaustausch“ in der Kennwortlistenansicht. Wählen Sie dann die entsprechende Aufgabe aus und geben Sie dann den damit verbundenen Dateinamen und einen Transfercode an.

Klicken Sie anschließend auf die Schaltfläche „Transferelemente auswählen“, um die zu transferierenden Einträge auszuwählen und die Aufgabe abzuschließen.

## **GoMobile!**

Um die Daten Ihrer persönlichen Kennwortliste extern bzw. mobil nutzen zu können, rufen Sie die GoMobile!-Funktion in der Kennwortlistenansicht auf. Wählen Sie dort den zu verwendenden USB-Stick aus und starten Sie den Datentransfer. Nach Abschluss der Datenübertragung können Sie mit dem USB-Stick die Automatikfunktionen mobil nutzen und so bequem auf Ihre Kennwörter zugreifen.

## Anmeldedaten auf Webseiten einfügen

Wenn Sie die Option zum Ausfüllen von Zugangsdaten auf Webseiten aktiviert haben und entsprechende Daten wie Internet-Adresse (URL), Benutzername und Kennwort in Ihrer Kennwortliste für diese Funktion hinterlegt sind, können Sie mit Password Guard diese komfortable Funktion verwenden, um sich ganz einfach auf entsprechenden Webseiten, wie z. B. einem Online-Shop, der Homepage Ihres Online-Bankings usw., anzumelden.

Wenn Sie eine Webseite besuchen, für die eine entsprechende Adresse (URL) in der Kennwortliste gespeichert ist, blendet das Programm ein Fenster ein, in dem Sie diesen Vorgang durch das entsprechende Masterpasswort autorisieren können. Zusätzlich können Sie hier, wenn mehrere Einträge auf diese Internetadresse verweisen, die entsprechende Kennwortliste bzw. den zu verwendenden Kennworteintrag auswählen.

Nach erfolgter Autorisation durch das entsprechende Masterpasswort blendet das Programm ein Info-Fenster ein, das Ihnen den nächsten Schritt erläutert: Zum automatischen Einfügen der hinterlegten Zugangsdaten müssen Sie nur noch in das 1. Eingabefeld auf der entsprechenden Webseite klicken, um das automatische Ausfüllen zu starten. Das Programm emuliert in diesem Falle Ihre manuelle Eingabe und sendet das entsprechende Zugangsdatenformular an den Webseitenserver, um den Vorgang der Anmeldung auf dieser Website vorzunehmen.

Sie von hier aus auch die Funktion zum manuellen Einfügen der Daten starten. Klicken Sie dafür einfach auf den Link „Manuell einfügen“. Anschließend können Sie die URL (Internetadresse), Benutzername und Kennwort einfach per Drag&Drop oder über die Zwischenablage in das als Ziel vorgesehene Eingabefeld einfügen.

Wenn Sie überhaupt keine Automatikfunktion wünschen, steht Ihnen in der neuen Programmversion der schnelle Abruf Ihrer Kennwortdaten zur Verfügung. Betätigen Sie hierfür die im Optionsdialog vorgegebene Tastenkombination (also z. B. STRG+ALT+P), um den Dialog zum Abruf Ihrer Kennwortdaten aufzurufen. Nach erfolgter Legitimation durch Ihr Masterpasswort können Sie von hier aus die Daten per Drag&Drop oder über die Zwischenablage in das als Ziel vorgesehene Eingabefeld einfügen.

Beachten Sie bitte, dass das Ziel von Drag&Drop-Operationen nur einzeilige und dafür vorgesehene Eingabefelder sein dürfen, da die ausgeführten Tastatursequenzen immer zuvor den dort enthaltenen Textpuffer leeren!

## **Sicherheit von Kennwörtern verbessern**

Die folgende Anleitung beschreibt, wie Sie mit Password Guard v4 schwache und somit unsichere Kennwörter verbessern können.

Rufen Sie zum Verbessern der Sicherheit Ihrer Zugangsdaten als ersten Schritt den Statusbericht der entsprechenden Kennwortliste auf. Prüfen Sie dann in der Spalte „Sicherheitsrisiken“, welche Ihre Zugangsdaten über ein sehr schwaches Kennwort verfügen. Öffnen Sie diese Listeneinträge nacheinander zum Bearbeiten und rufen Sie über die Schaltfläche „Extras“ den Befehl „Zugangsdaten-Änderungsassistent“ auf. Folgen Sie den Anweisungen auf der Assistentenseite, um die Sicherheit der Zugangsdaten zu erhöhen.







# Kennwortgenerator

Über das Startmenü des Programmes sowie an diversen Stellen des Programmes (Anlegen einer Kennwortliste, Ändern des Masterpasswortes, Kennwortlisteneintrag editieren) erreichen Sie einen separaten Kennwortgenerator, mit dem Sie schnell und bequem sichere Kennwörter erstellen lassen können. Zur Auswahl stehen hierbei 3 mögliche Varianten:

- Sehr sicher und für die Speicherung im Programm vorgesehen
- Relativ einfach zu merken (dadurch aber eher unsicher)
- Benutzerdefinierte Anzahl Zeichen, Zeichenauswahl usw.

Durch Klicken auf die Schaltfläche „Generieren“ starten Sie den Vorgang. Im Eingabefeld erscheint dann das entsprechende Resultat. Sie können hier auch noch eigene Variationen hinzufügen, da das Eingabefeld entsprechende Eingaben zulässt.

Durch Klicken auf die Schaltfläche „Kopieren“ wird der Text mit dem generierten Kennwort in die Zwischenablage kopiert und steht somit bei Einfügeoperationen an beliebiger Stelle zur Verfügung.

Wenn der Kennwortgenerator über eine andere Seite im Programm aufgerufen wurde, dann ist unter der Schaltfläche „Generieren“ jeweils eine Schaltfläche „Übernehmen“ verfügbar, die den Kennworttext in den aufrufenden Dialog überträgt.



# Kennwortanalyse

Über das Startmenü des Programmes erreichen Sie die Kennwortanalysefunktion. Geben Sie im ersten Schritt das zu überprüfende Kennwort ein und klicken Sie dann auf die Schaltfläche „Jetzt analysieren“. Anschließend werden die jeweils gültigen Indikatoren eingeblendet und Sie können so genau entnehmen, welche Faktoren das überprüfte Kennwort sicher oder unsicher machen.

Die Gesamtbewertung der gegebenen Kennwortqualität wird dann in der Bewertungsskala sichtbar, die mit Werten von 0 bis 100 arbeitet. Eine volle Punktzahl entspricht im Übrigen 5 Sternen des an anderer Stelle im Programm verwendeten Darstellungssystems. 80 Punkte würden 4 Sternen, 60 Punkte würden 3 Sternen entsprechen usw.

Die Kennwortanalysefunktion, die Sie auch aus dem Bearbeitungsdialog eines Kennworteintrages aufrufen können, erklärt also stets genau, warum ein Zugangskennwort z. B. als mangelhaft oder sehr gut bewertet wurde.



# Softwarelizenzen verwalten

## Übersicht

Immer mehr Computersoftware wird ausschließlich über das Internet vertrieben oder der Bezug einer Lizenz als Download stellt die erste Wahl da, da die Vorteile gegenüber dem Erwerb einer physischen Vertriebsform, also Packung mit CD und gedrucktem Handbuch, überwiegen.

Ein Nebeneffekt ist aber meistens, dass so lizenzierte Software ungenügend verwaltet oder entsprechende Lizenzschlüssel zum Freischalten mit der Zeit verloren gehen. Auch hier kann Ihnen Password Guard v4 seine hilfreichen Dienste anbieten. Sie erhalten die Möglichkeit, Softwarelizenzen komfortabel zu verwalten, um

- dem Verlust von Lizenzinformationen (Product Key usw.) vorzubeugen
- Softwarelizenzen stets entsprechend dem Lizenzvertrag zu verwenden
- die Herkunftsquelle und andere Daten (Hersteller, Rechnungs-Nummer usw.) immer schnell zur Hand zu haben
- zu dokumentieren, auf welchem Computer welcher Lizenzschlüssel verwendet wurde, um z. B. Probleme bei erneut zu erfolgreicher Software-Produktaktivierungen zu umgehen

Die Lizenzverwaltung von Password Guard ist also eine zentrale Stelle, an der Sie alle diese Informationen komfortabel verwalten können und diese Daten nicht mehr beispielsweise in Ihrem E-Mail-Programm zusammensuchen müssen.

Bedenken Sie, dass der Verlust von lizenzbezogenen Daten (Product Key usw.) sich immer als mehr oder weniger großer finanzieller Schaden herausstellen kann, wenn Sie ein Produkt, für das Sie die entsprechenden Lizenzkosten getragen haben, aus diesem Grund nicht mehr verwenden können und Sie auch keine Möglichkeit mehr haben, die Rechtmäßigkeit oder Bezugsquelle einer Softwarelizenz nachweisen zu können.

## Listeneinträge hinzufügen

Nach dem Aufruf der Lizenzverwaltung im Startmenü gelangen Sie direkt in die entsprechende Listenansicht. Am unteren Fensterrand finden Sie den Link „Neuer Eintrag“, der Sie zur Eingabe der Daten eines Listeneintrages führt.

Mit Password Guard können Sie folgende Daten zu einer Softwarelizenz speichern und bearbeiten:

**Produktname:** Hier geben Sie einen Namen für den Eintrag ein, der das leichte Wiederauffinden ermöglicht.

**Kategorie:** Hier geben Sie eine Kategorie für die Art der Software an, also z. B. AntiVirus, Betriebssystem, Utility usw.

**Lizenzschlüssel:** Hier geben Sie den Lizenzschlüssel (Product Key, CD-Key o.ä.) ein, den Sie mit dieser Softwarelizenz erworben haben und der Sie zur Nutzung dieses Produktes berechtigt.

**Lizenzform:** Hier geben Sie an, ob es sich bei der Softwarelizenz um eine Einzelplatzlizenz oder um eine Multivolumenlizenz handelt. In der Regel sind erworbene Softwarelizenzen immer Einzelplatzlizenzen, dürfen also nur auf einem Computer installiert und genutzt werden.

**Installations-PC:** Hier geben Sie den Namen des Computers an, auf dem Sie die Software installiert haben. Diese Angabe hilft Ihnen zu vermeiden, bei Einsatz von mehreren Softwarelizenzen bei einer erneuten Installation und Software-Produktaktivierung versehentlich einen falschen Lizenzschlüssel zu verwenden, also einen Product Key der bereits bei der Aktivierung auf einem anderen Computer verwendet wurde. So stellen Sie sicher, dass Sie stets für ein und selben Rechner auch den ursprünglichen Product Key verwenden.

**Händler-Website:** Hier geben Sie die Internet-Adresse des Händlers an, bei dem Sie die Softwarelizenz erworben haben.

**Rechnungs-Nr.:** Hier geben Sie die Rechnungsnummer oder andere Referenzdaten zur Bestellung der Softwarelizenz an.

**Rechnungs-Datum:** Hier geben Sie das Datum der Rechnung an.

**Setup-Medium:** Hier geben Sie an, auf welchem Medium Sie die Installationsdateien erhalten haben: Als Download oder als beispielsweise CD-ROM.



**Download-URL:** Wenn Sie die Softwarelizenz als elektronischen Download lizenziert haben, können Sie hier die Adresse für den Download des Setup-Programms eingeben..

**Hersteller-Website:** Um Produktsupport oder andere Informationen direkt vom Hersteller der Software zu erhalten, geben Sie hier die entsprechende Internetadresse an, um bei Bedarf die Website des Unternehmens bei Bedarf besuchen zu können.

**Notizen:** Hier können Sie zusätzliche Informationen zu diesem Eintrag eingeben.

**Anlagen:** Über die Schaltfläche „Anlagen“ können Sie beliebige Dateien als Anhang zu einem Listeneintrag hinzufügen, also z. B. eine Rechnung im PDF-Format.

Den Eintrag speichern Sie durch Klicken auf den Link „Eintrag speichern“ am unteren Fensterrand. Wenn Sie die Escape-Taste drücken oder den Pfeil links oben anklicken, werden Ihre Eingaben nicht gespeichert und Sie gelangen wieder zurück zur Listenansicht.

Durch Anklicken des Links „Eintrag löschen“ können Sie den aktuell angezeigten Eintrag löschen. Alternativ können Sie in der Listenansicht auch diesen Eintrag selektieren und dann die Entfernen-Taste drücken.

## Listenansicht und Navigation

Am oberen Rand der Lizenzverwaltungsansicht finden Sie die Registerauswahl (Buchstaben A-Z, 0-9). Wenn Sie die Lizenzverwaltung geöffnet haben, ist noch kein Register ausgewählt und alle Einträge werden ungefiltert angezeigt und sind somit schnell zu erreichen.

Wünschen Sie eine Filterung von Einträgen eines bestimmten Registers, dann klicken Sie auf den gewünschten Kategorienamen in dieser Leiste. Durch erneutes Klicken, wird diese Filterung wieder aufgehoben und alle Elemente angezeigt. Mit der STRG-Taste und den Cursor-rechts/links-Tasten können Sie durch die Register blättern.

Wenn Sie nach einem Listenelement suchen möchten, geben Sie den entsprechenden Suchbegriff in das Suchfeld rechts oben ein.

Zum Navigieren durch die Liste können Sie hier das Mausrad oder die Cursorstasten verwenden. Um einen Eintrag mit einem bestimmten Anfangsbuchstaben schnell zu selektieren, tippen Sie einfach diesen Buchstaben ein. Selbstverständlich sind auch

die Bild aufwärts/abwärts, Pos1 und Ende-Tasten verfügbar, um schnell innerhalb einer Listenansicht navigieren zu können.

Sind in einer Listenansicht mehr als 18 Elemente enthalten, weist Sie ein Pfeilsymbol beim Einblenden kurz darauf hin, dass Sie durch Scrollen der Liste nach unten zu weiteren Elementen gelangen können.

Rechts unten finden Sie in der Listenansicht stets zur Information noch die Anzahl der enthaltenen Einträge.

Das jeweils selektierte Element einer Liste erkennen Sie durch die vergrößerte Darstellung. Wenn Sie ein solches Element anklicken oder die Eingabetaste drücken, gelangen Sie stets zum Eingabedialog für den Datensatz dieses Eintrages.

## **Lizenzliste drucken**

Unter der Listenansicht finden Sie einen Link, mit dem Sie die Lizenzverwaltungsliste auf einen Drucker ausgeben können. Bewahren Sie auch solche gedruckten Listen unbedingt an einem sicheren Ort auf, um sich selbst vor Schaden durch Missbrauch dieser Daten zu bewahren.

Nicht mehr benötigte oder veraltete Ausdrücke sollten Sie gewissenhaft vernichten, um keinen unbefugten Dritten ungewollt Auskunft über die dort abgedruckten Daten zu geben.





# Express Cleaner

Eine weitere nützliche Funktion von Password Guard ist der Express Cleaner, mit dem Sie sensible Daten mit einem Klick bereinigen können. Zur Auswahl steht Ihnen dabei die Bereinigung der folgenden Systemdaten:

- Dateien und Ordner im Papierkorb
- Menü „Zuletzt verwendete Dokumente“
- Gespeicherte Suchvorgänge (Windows Explorer)
- Temporäre Dateien
- Inhalt der Zwischenablage

Nutzer des Internet Explorers können mit dem Express Cleaner zusätzlich folgende sensible Daten bereinigen lassen:

- Gespeicherte Cookies
- Temporäre Internetdateien
- Einträge im Ordner „Verlauf“
- (Manuell) eingegebene Internet-Adressen
- Standard-Speicherordner für „Ziel speichern unter“-Operationen

Den Express Cleaner können Sie zusätzlich jederzeit auch über das Kontextmenü des Programms im Infobereich starten und so im Handumdrehen die Bereinigung der sensiblen Systemdaten ausführen.

Auf der Seite „Express Cleaner“ finden Sie unten einen Link für den Aufruf des „Datenshredders“, mit dem Sie Dateien sicher löschen können.



# Datenshreder

Werden Dateien über den Windows-Explorer gelöscht oder in den Papierkorb verschoben, sind diese Dateien nur wieder dem freiem Speicherplatz auf der Festplatte zugeordnet. Wann eine so markierte Datei wirklich gelöscht bzw. überschrieben und somit nicht rekonstruierbar wird, entzieht sich dem Einfluss des Anwenders.

Wenn nicht autorisierte Personen Zugriff auf Ihre Festplatte erhalten oder zum Beispiel ein PC-Notdienst oder hilfreicher Nachbar Ihnen beim "Wiederbeleben" Ihres Computers nach einem Systemcrash hilft, können Daten, die streng vertraulich waren und die Sie bereits für gelöscht hielten, wie durch Geisterhand wieder auf Ihrem Computer sichtbar werden.

Ab diesem Zeitpunkt haben unbefugte Personen Einblick in Ihre vertraulichen, vermeintlich gelöschten Daten. Seien es Daten privater Natur, brisante geschäftliche Korrespondenz oder Personal- und Kundendaten, deren fahrlässige Zugänglichkeit sogar rechtliche Konsequenzen für Sie haben kann.

Mit dem in Password Guard integrierten Datenshreder können Sie jetzt ganz einfach und schnell sensible Dateien spurlos löschen. Dabei kommen u. a. empfohlene Algorithmen der National Security Agency (NSA) bzw. des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Anwendung, um Daten unwiderruflich und nicht rekonstruierbar zu löschen.

Den integrierten Datenshreder erreichen Sie durch Aufruf des Express Cleaners im Hauptmenü. Auf der Express Cleaner-Seite klicken Sie bitte unten auf den Link „Datashredder“, um Dateien sicher zu löschen.

Auf der entsprechenden Programmseite wählen Sie dann einfach die zu löschenden Dateien und Ordner aus und können auch die anzuwendende Löschmethode auswählen.





# Programmoptionen

Über das Startmenü erreichen Sie das Optionsmenü des Programms. Dort stehen Ihnen diverse Einstellungen zum Anpassen des Programms zur Verfügung.

## Allgemeine Einstellungen

### **Password Guard beim Systemstart automatisch laden und Systemschutz aktivieren:**

Um alle Funktionen des Programmes sinnvoll zu nutzen und auch die integrierten Schutzmaßnahmen gegen Spyware zu aktivieren, sollten Sie diese Option aktivieren.

### **Akustische Signale bei Animationen, Popups und Aktionen wiedergeben:**

Wenn diese Option deaktiviert ist, werden keine entsprechenden Sounds während der Programmausführung ausgegeben.

### **Nachfragen, ob neu installierte Software in die Lizenzverwaltung eingetragen werden soll:**

Wenn diese Option aktiviert ist, überwacht Password Guard die Installationsvorgänge auf Ihrem System um zu ermitteln, ob neue Software installiert wurde und eine Nachfrage zu stellen, ob Sie den entsprechenden Lizenzschlüssel in Ihrer Datenbank speichern möchten.

### **Infobereich-Symbol zum Aufheben aller automatischen Autorisationen einblenden:**

Wenn Sie in den Sicherheitseinstellungen die Funktion aktiviert haben, dass Masterpasswörter nur einmal täglich abgefragt werden sollen, können Sie mit dieser Option ein Symbol im Infobereich einblenden lassen, mit dessen Hilfe Sie alle bereits erteilten Autorisationen bei Bedarf schnell wieder aufheben können.

### **Webseitenanmeldungen nach Autorisation automatisch mit hinterlegten Zugangsdaten ausfüllen:**

Wenn diese Option gewählt ist, wird beim Öffnen einer hinterlegten Internetadresse in Ihrem Browser der Dialog zum automatischen Ausfüllen eingeblendet. Ist diese Option deaktiviert, können Sie trotzdem stets über den manuellen Datenabruf Zugriff auf die entsprechenden Daten erhalten und z. B. Formulare für die Benutzeranmeldung per Drag&Drop ausfüllen.

**Überwachte Browser:** Wählen Sie hier die von Ihnen genutzten Internet-Browser aus, für die die Funktion zum Ausfüllen von Zugangsdaten aktiviert werden soll.

**System- und sicherheitsrelevante Ereignisse protokollieren:** Diese Option aktiviert die Protokollierung von entsprechenden Ereignissen im Systemprotokoll von Password Guard.

**Globale Tastenkombination für manuellen Kennwortdatenabruf aktivieren:** Wählen Sie diese Option, um den manuellen Kennwortdatenabruf mit Hilfe einer systemweiten Tastaturkombination aufzurufen.

**Speicherordner für Programmdateien:** Um festzulegen, wo die Kennwortdateien und Daten der Lizenzverwaltung gespeichert werden sollen, können Sie die hierfür vorgesehenen Speicherordner anpassen.

## Sicherheitseinstellungen

Über die Schaltfläche „Sicherheitseinstellungen“ im Optionsdialog rufen Sie die Einstellungen für die Sicherheitsfunktionen von Password Guard auf.

Die Sicherheitseinstellungen sind in 4 Gruppen eingeteilt. Die Skala rechts gibt an, wie hoch die Sicherheit insgesamt entsprechend der gewählten Optionen ist.

**Password Guard Systemschutz:** In dieser Gruppe wählen Sie die Optionen für den Systemschutz aus. Der Systemschutz überwacht und meldet auf Wunsch verdächtige Programme, die Zugriff auf sensible Daten nehmen können.

**Primäre Sicherheitsoptionen:** In dieser Gruppe wählen Sie alle primären Sicherheitsoptionen aus, die die Sicherheit für Ihre Kennwortdaten erhöhen.

**Sekundäre Sicherheitsoptionen:** In dieser Gruppe wählen Sie alle sekundären Sicherheitsoptionen aus, die die Sicherheit Ihrer Kennwortdaten erhöhen.

**Masterpasswort-Autorisation:** In dieser Gruppe können Sie auswählen, ob der Zugang zum Optionsdialog und zur Lizenzverwaltung zusätzlich durch die Abfrage des Masterpasswortes der Kennwortliste „Meine Kennwörter“ geschützt werden soll. Desweiteren können Sie hier festlegen, ob jedes Masterpasswort der einzelnen Kennwortlisten nur einmal täglich abgefragt werden soll. Dies erhöht ggf. den Komfort, lässt aber gleichzeitig das Risiko steigen, dass eine Person, die Zugang zu Ihrem Computer hat, somit auch Zugang zu allen sensiblen Kennwortdaten erhalten kann.

## **Datei-Sicherungskopien**

Über die Schaltfläche „Datei-Sicherungskopien“ im Optionsdialog rufen Sie die Einstellungen für die automatische Backup-Funktion auf.

Auf der Seite „Sicherungskopien“ wählen Sie zum Einrichten der Backup-Funktion aus, ob automatisch Kopien der Dateien erstellt werden sollen, wo diese gespeichert werden sollen und in welchem Modus die Datensicherung erfolgen soll.

Wenn Sie eine Sicherungskopie wiederherstellen möchten, wählen Sie einfach die entsprechende Sicherungskopie sowie die wiederherzustellenden Datenelemente aus, also z. B. ob Sie nur die Datei mit Ihren persönlichen Kennwörtern oder die Datei mit den Daten der Lizenzverwaltung wiederherstellen möchten.

Wenn Sie das Programm später auf einem neuen Computer nutzen, sollten Sie, wenn Sie die Wiederherstellungsfunktion auch für alte Sicherungen nutzen möchten, vom alten Computer die Sicherungskopien in das ausgewählte Sicherungsverzeichnis kopieren, um diese auf dem neuen Computer bei Bedarf wiederherstellen zu können.









**Password Guard v4 Benutzerhandbuch**  
©2010 SYDATEC. Alle Rechte vorbehalten.

[www.sydatec.com](http://www.sydatec.com)