



**PASSWORD  
DEPOT**  
BY AceBIT

# Password Depot für Linux

---

## Quick Start Guide – Linux

Stand: 26.01.2026

Dieser Leitfaden zeigt Ihnen die wichtigsten Schritte, um Password Depot auf Linux sicher zu nutzen – ohne technisches Vorwissen.

## Inhaltsverzeichnis

Inhaltsverzeichnis .....	2
Einführung .....	3
So sieht die App aus (Kurzüberblick) .....	3
Wichtige Begriffe .....	4
Erste Schritte .....	5
Datenbank-Manager öffnen .....	5
Neue Datenbank erstellen (lokal oder in der Cloud) .....	6
Schlüsseldatei auswählen oder erstellen .....	7
Datenbank öffnen und entsperren .....	8
Cloud-Speicher verbinden (Dropbox, Google Drive, OneDrive, HiDrive, Box) .....	9
Enterprise Server (Unternehmen) .....	10
Orientierung in der Hauptansicht .....	11
Kernfunktionen .....	12
Einträge anlegen .....	12
Passwort-Eintrag: Wichtigste Felder .....	13
Passwort-Generator nutzen .....	14
URLs und Vorlagen verwalten .....	15
Erweiterte Einstellungen für einen Eintrag .....	16
TOTP (2FA) verwenden .....	17
Benutzerdefinierte Felder .....	17
Zweites Passwort für kontrollierten Zugriff .....	18
Bedingter Zugriff (Warnmeldung beim Zugriff) .....	19
TANs verwalten .....	20
Schnellaktionen in der Detailansicht .....	21
Tipps .....	22
Sicher arbeiten .....	22
Zwischenablage automatisch löschen .....	22
Automatisch speichern und Backups nutzen .....	23
Sprache ändern .....	23
Verschlüsselte Verbindung (SSL/TLS) für Enterprise Server .....	24
Wenn etwas nicht funktioniert .....	24
Hilfe und Support .....	24

## Einführung

Password Depot speichert Zugangsdaten, Dokumente und weitere vertrauliche Informationen in einer verschlüsselten Datenbank. Diese Datenbank wird mit einem Master-Passwort (und optional einer Schlüsseldatei) geöffnet.

**WICHTIG:** Ohne Ihr Master-Passwort für Ihre Datenbank können Ihre Daten nicht wiederhergestellt werden. Wählen Sie ein starkes Passwort, das Sie sicher behalten.

### So sieht die App aus (Kurzüberblick)

- **Startbildschirm:** Über den Startbildschirm erhalten Sie Zugriff auf den Datenbank-Manager.
- **Datenbank-Manager:** Im Datenbank-Manager können Sie Datenbanken erstellen, auswählen und öffnen (lokal gespeicherte Datenbanken, in der Cloud, Datenbanken vom Enterprise Server oder Backups/Sicherungsdateien).
- **Hauptansicht:** Auf der linken Seite sehen Sie die Navigation, in der Mitte die Liste der Einträge der aktuell geöffneten Datenbank, rechts finden Sie Details und Schnellaktionen.



### Password Depot 19 (alpha)

 Datenbankmanager  
Öffnet eine bestehende oder erstellt eine neue Datenbank

 Ausfahrt  
Beendet das Programm

## Wichtige Begriffe

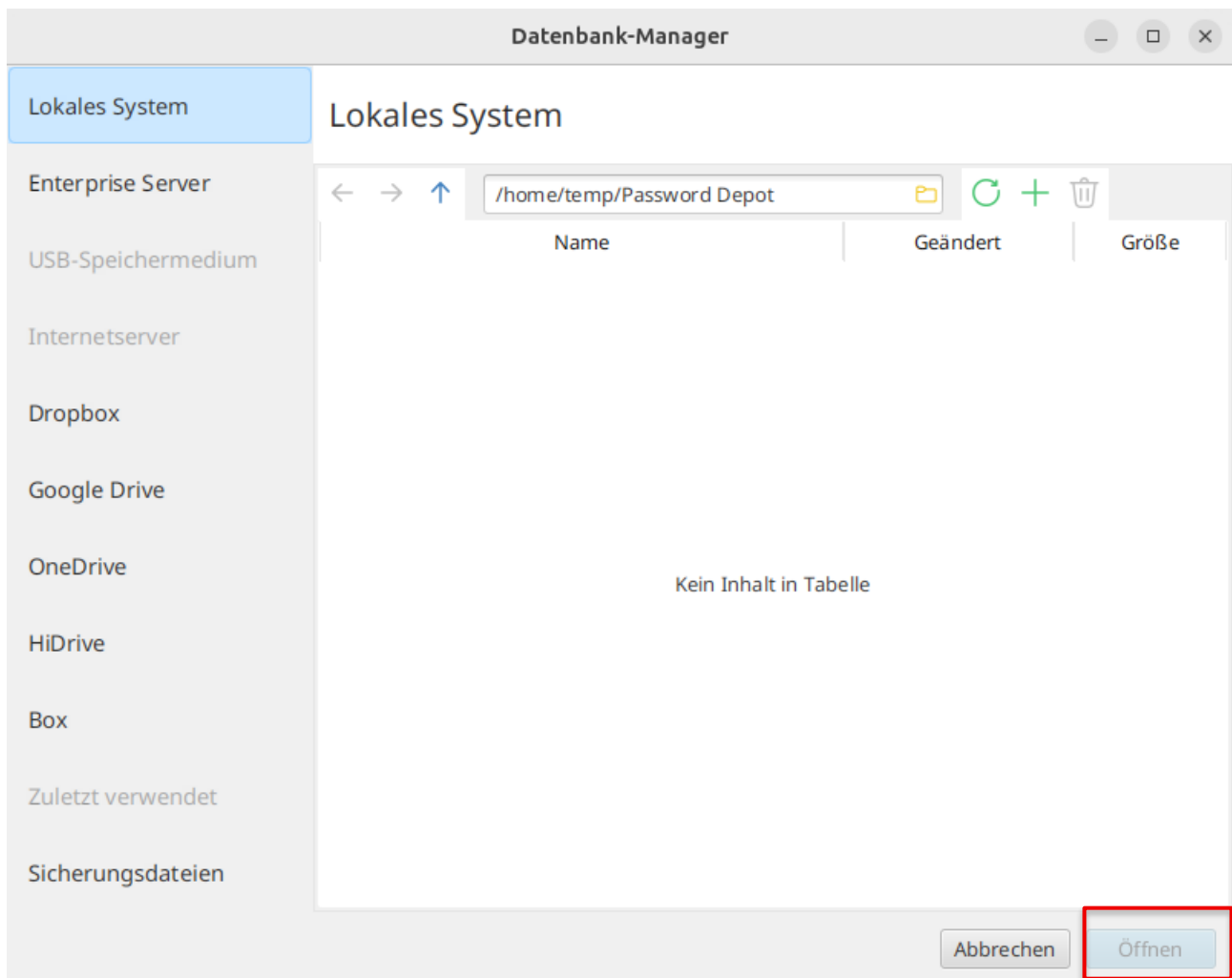
- **Datenbank:** Dies ist Ihre verschlüsselte Datei mit allen Einträgen (z. B. "Privat.psw").
- **Master-Passwort:** Dabei handelt es sich um das Hauptkennwort zum Öffnen der Datenbank.
- **Schlüsseldatei:** Dies ist eine zusätzliche Datei, welche als zweiter Faktor zum Öffnen der Datenbank dient (2FA = Zwei-Faktor-Authentifizierung).
- **Eintrag:** Ein Eintrag bezeichnet ein gespeichertes Objekt, z. B. Passwort, Kreditkarte oder Identität.
- **TOTP:** Dabei handelt es sich um einen zeitbasierten Einmalcode für 2FA-Logins.

## Erste Schritte

### Datenbank-Manager öffnen

Der **Datenbank-Manager** ist der zentrale Verwaltungsbereich von Password Depot für Linux und bietet eine Übersicht über die vorhandenen Speicherorte und Datenbanken.

- Klicken Sie im Startbildschirm auf **Datenbank-Manager**.
- Wählen Sie links den gewünschten Speicherort (**Lokales System**, **Enterprise Server**, **Dropbox**, **Google Drive**, **OneDrive**, **HiDrive**, **Box** oder **Sicherungsdateien**).
- Wählen Sie aus der Liste die gewünschte Datenbank aus und klicken Sie auf **Öffnen**.




## Neue Datenbank erstellen (lokal oder in der Cloud)

Um eine neue Datenbank zu erstellen, gehen Sie wie folgt vor:

- Öffnen Sie im **Datenbank-Manager** einen Speicherort (z. B. **Lokales System** oder ein Cloud-Dienst).
- Klicken Sie auf **Neu** (Plus-Symbol).
- Geben Sie einen Datenbanknamen ein.
- Wählen Sie die gewünschte Authentifizierung: **Master-Passwort**, **Master-Passwort und Schlüsseldatei** oder nur **Schlüsseldatei**.
- Geben Sie ein Master-Passwort ein und wiederholen Sie es. Falls eine Schlüsseldatei zusätzlich oder alternativ als Authentifizierungsmethode gewählt wurde, geben Sie diese ebenfalls an.
- Optional: Prüfen Sie das Master-Passwort gegen bekannte Passwort-Leaks (**Überprüfen Sie gehackte Passwörter**).
- Klicken Sie auf **OK**, um die Erstellung Ihrer Datenbank abzuschließen.

**WICHTIG:** Wählen Sie ein starkes Master-Passwort: Idealerweise besteht dieses aus mindestens 12 Zeichen und wird nur einmal verwendet.

**Neue Datenbank**



### Festlegen der Einstellungen für die neue Datenbank

Datenbankname:	Authentifizierung durch:
<input type="text"/>	Master-Passwort
Kommentar:	Master-Passwort:
<input type="text"/>	<input type="password"/>
Hinweis zum Master-Passwort:	Master-Passwort erneut eingeben:
<input type="text"/>	<input type="password"/>
	Schlüsseldatei:
	<input type="text"/>

## Schlüsseldatei auswählen oder erstellen

Wenn Sie die Authentifizierungsmethode **Master-Passwort und Schlüsseldatei** oder nur **Schlüsseldatei** verwenden, benötigen Sie eine Datei mit der Endung `.key`. Sie können hierfür eine bereits vorhandene Datei auswählen oder eine neue erzeugen.

- Klicken Sie bei **Schlüsseldatei** auf **Auswählen**, um eine vorhandene Datei zu selektieren.
- Alternativ klicken Sie auf **Generieren**, um eine neue Schlüsseldatei zu erstellen und zu speichern.

**WICHTIG:** Bewahren Sie die Schlüsseldatei getrennt vom Master-Passwort auf. Verlieren Sie die Schlüsseldatei, verlieren Sie auch den Zugriff auf die Datenbank, die damit geschützt ist.

Schlüsseldateigenerator

Bewegen Sie die Maus über diesen Bereich, um zufällige Daten zu generieren:

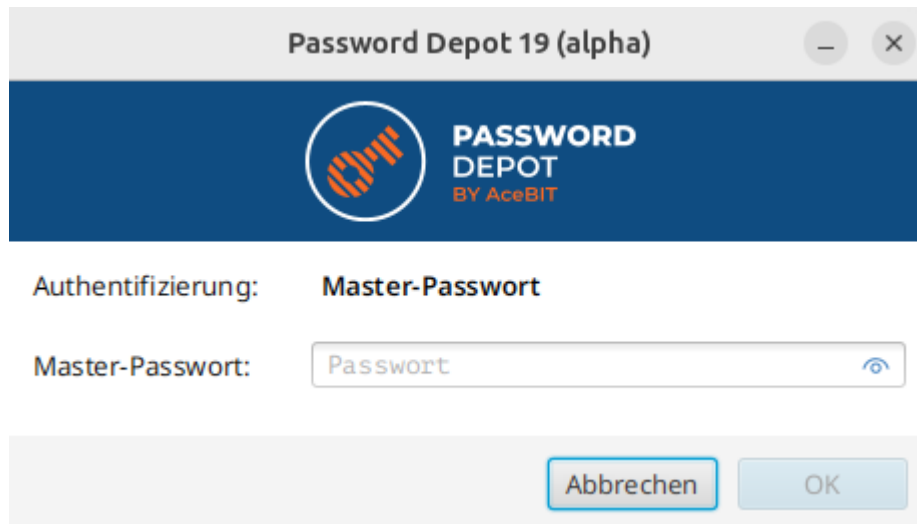
Eckdaten:

Schlüssel in Datei speichern:

Abbrechen Speichern

## Datenbank öffnen und entsperren

- Wählen Sie im **Datenbank-Manager** eine Datenbank aus.
- Klicken Sie auf **Öffnen** oder doppelklicken Sie die entsprechende Datei.
- Geben Sie im Entsperr-Dialog das Master-Passwort ein und wählen Sie ggf. die zugehörige Schlüsseldatei.
- Klicken Sie abschließend auf **OK**, um die Datenbank zu öffnen.

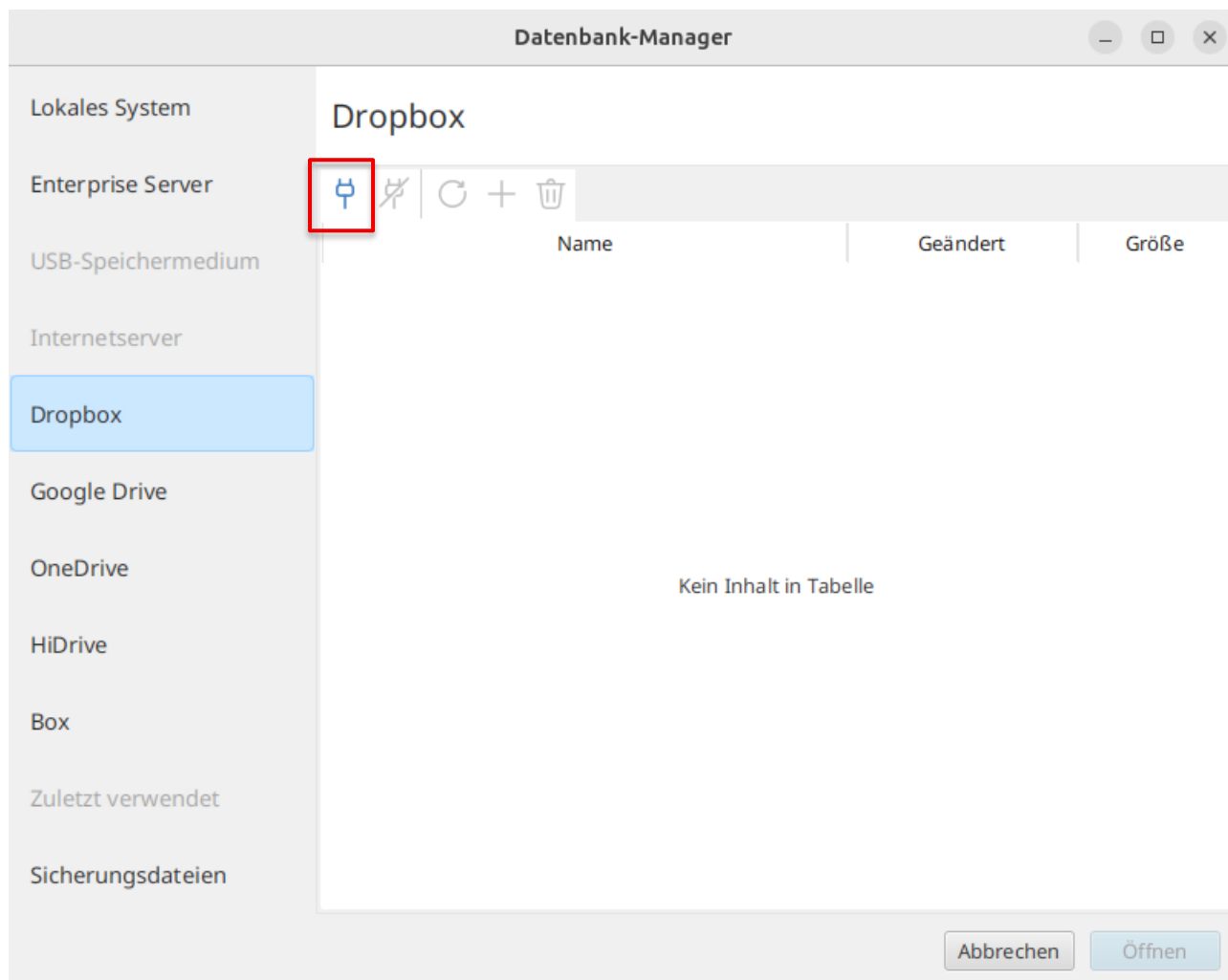


The image shows a screenshot of a software dialog box titled "Password Depot 19 (alpha)". The dialog has a dark blue header with the "PASSWORD DEPOT BY AceBIT" logo. Below the header, the text "Authentifizierung: Master-Passwort" is displayed. Underneath, there is a text input field labeled "Master-Passwort:" containing the placeholder text "Passwort" and a small eye icon to toggle visibility. At the bottom right, there are two buttons: "Abbrechen" (highlighted with a blue border) and "OK".

## Cloud-Speicher verbinden (Dropbox, Google Drive, OneDrive, HiDrive, Box)

Für Cloud-Speicher müssen Sie Password Depot einmalig in Ihrem Standardbrowser freischalten.

- Wählen Sie im **Datenbank-Manager** den gewünschten Cloud-Speicher.
- Klicken Sie auf **Verbinden** (Stecker-Symbol).
- Folgen Sie den Anweisungen im Browser und erlauben Sie den Zugriff.
- Kehren Sie in die App zurück und klicken Sie auf **Aktualisieren**, falls nötig.



## Enterprise Server (Unternehmen)

Wenn Ihre Organisation einen Password Depot Enterprise Server nutzt, erhalten Sie die Zugangsdaten von Ihrem Administrator.

- Wählen Sie im Datenbank-Manager **Enterprise Server**.
- Klicken Sie auf **Verbinden** (Stecker-Symbol) und geben Sie Serveradresse, Port, Serverversion, Benutzername und Passwort ein. Falls von Ihrem Unternehmen eingerichtet, steht Ihnen neben der Standard-Authentifizierung noch die Authentifizierung via Azure AD zur Verfügung.
- Öffnen Sie eine freigegebene Datenbank aus der Liste.

**ACHTUNG:** Die Erzeugung von Datenbanken auf dem Enterprise Server findet ausschließlich über den Server-Manager des Servers statt. Datenbanken auf dem Server können Sie nur öffnen, wenn Sie zugriffsberechtigt sind. Zugriffsrechte werden Ihnen von Ihrem Serveradministrator gewährt.



The image shows a screenshot of a login dialog box titled "Password Depot Enterprise Server-Login". The dialog has a dark blue header with the Password Depot logo and the text "PASSWORD DEPOT BY AceBIT". Below the header, there are several input fields and dropdown menus:

- A text input field for the server address, followed by a port field containing "25019".
- A dropdown menu currently showing "Enterprise Server 19".
- A dropdown menu currently showing "Standardauthentifizierung".
- A text input field for the username, labeled "Benutzername".
- A text input field for the password, labeled "Passwort", with a visibility toggle icon on the right.

At the bottom of the dialog, there are two buttons: "Abbrechen" (Cancel) and "OK".

## Orientierung in der Hauptansicht

- Links sehen Sie die Navigation (z. B. Datenbank, Papierkorb, Kategorien).
- In der Mitte befindet sich die Liste der Einträge. Doppelklicken Sie einen (Unter-)Ordner, um ihn zu öffnen.
- Auf der rechten Seite werden Details zum ausgewählten Eintrag sowie Schnellaktionen (Kopieren, URL öffnen) angezeigt.
- Oben befinden sich die Symbolleisten-Buttons (Datenbank-Manager, Neuer Eintrag, Bearbeiten, Navigation zurück/vor etc.).

The screenshot shows the Password Depot 19 (alpha) interface. The main window displays a file browser view for the folder 'AceBIT-GmbH\_EN.p...'. The interface includes a menu bar with options like 'Datenbank', 'Bearbeiten', 'Suchen', 'Sicht', 'Ordner', 'Eintrag', 'Werkzeuge', and 'Helfen'. A search bar is located at the top right. The main content area shows a table of folders with the following columns: 'Beschreibung', 'URL', 'Benutzername', and 'Geändert'.

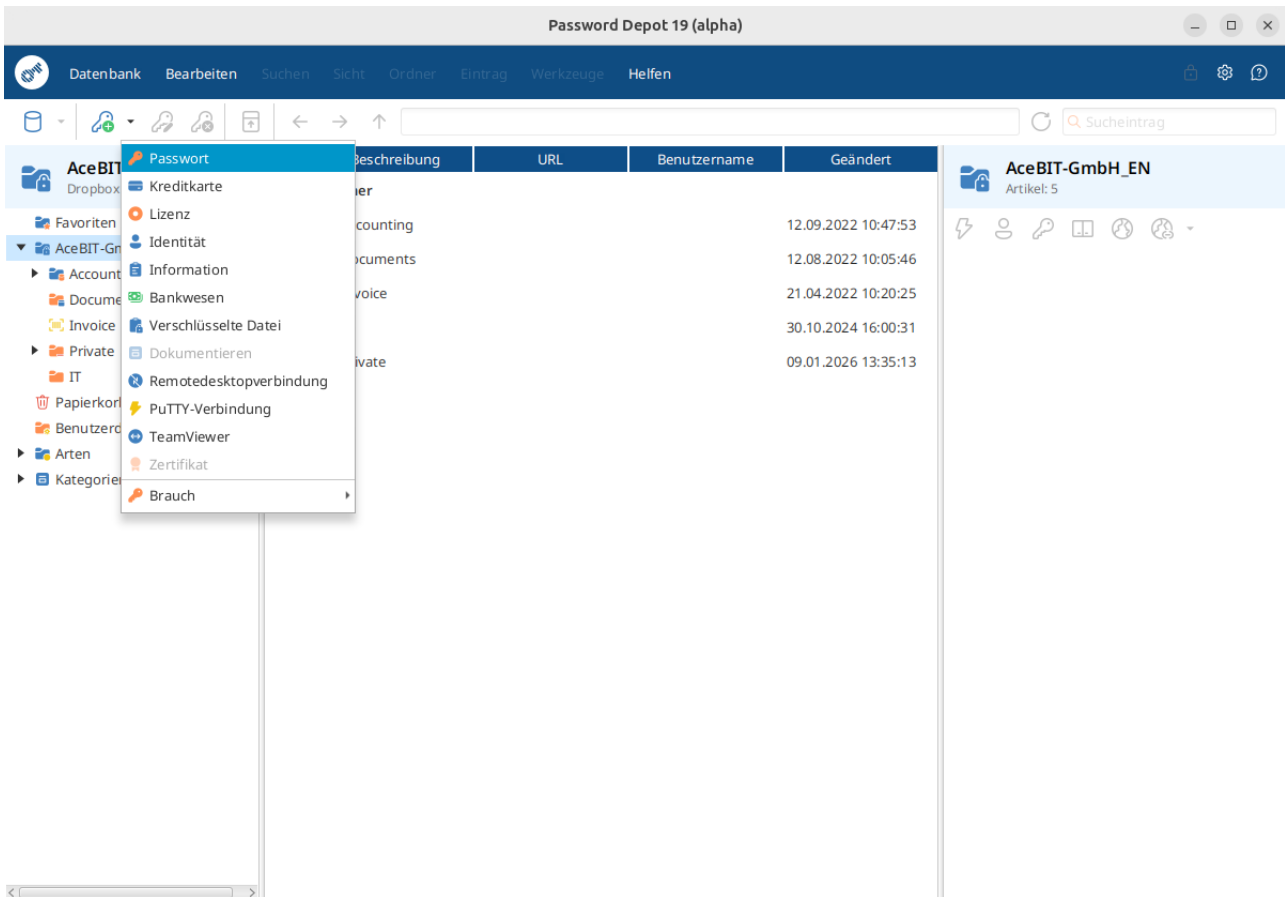
Beschreibung	URL	Benutzername	Geändert
Ordner			
Accounting			12.09.2022 10:47:53
Documents			12.08.2022 10:05:46
Invoice			21.04.2022 10:20:25
IT			30.10.2024 16:00:31
Private			09.01.2026 13:35:13

On the right side, there is a panel for 'AceBIT-GmbH\_EN' showing 'Artikel: 5' and several action icons (copy, paste, delete, etc.). The left sidebar shows a navigation tree with folders like 'Favoriten', 'AceBIT-GmbH\_EN', 'Accounting', 'Documents', 'Invoice', 'Private', 'IT', 'Papierkorb', 'Benutzerdefinierte Eintragstyp.', 'Arten', and 'Kategorien'.

# Kernfunktionen

## Einträge anlegen

- Klicken Sie oben auf **Neuer Eintrag** (Schlüssel mit Plus-Symbol). Dadurch legen Sie einen Eintrag vom Typ **Passwort** an.
- Für andere Eintragstypen klicken Sie auf das kleine Dreieck neben **Neuer Eintrag**.
- Wählen Sie den gewünschten Typ (z. B. Kreditkarte, Identität usw.).
- Füllen Sie die benötigten Felder aus und klicken Sie auf **OK**, um den Eintrag abzuspeichern.




## Passwort-Eintrag: Wichtigste Felder

Je nach Eintragstyp stehen Ihnen verschiedene Felder zur Verfügung. Bis auf das Feld **Beschreibung** sind diese je nach Eintragstyp optional. Zu den wichtigsten Feldern gehören:



- **Beschreibung:** Name des Eintrags (z. B. "E-Mail – privat").
- **Benutzername** und **Passwort**.
- **Kategorie** und Stichworte (**Tags**): Dies erlaubt Ihnen eine bessere Sortierung bzw. ein leichteres Ausfindigmachen wichtiger Einträge.
- **Ablaufdatum** (definiertes Gültigkeitsdatum für einen Eintrag) sowie zusätzliche **Kommentare**.

**Eigenschaften von Passwort Depot**


Allgemein | URLs | Zusätzlich | Benutzerdefinierte Felder | TANs | Anlagen | Versionen


Beschreibung:  

Benutzer:

Passwort:     
Sehr stark (Länge: 24 Zeichen; Entropie: 157 Bits)

Kategorie:

Bedeutung:  

Läuft ab:   

Stichworte:

Kommentare:

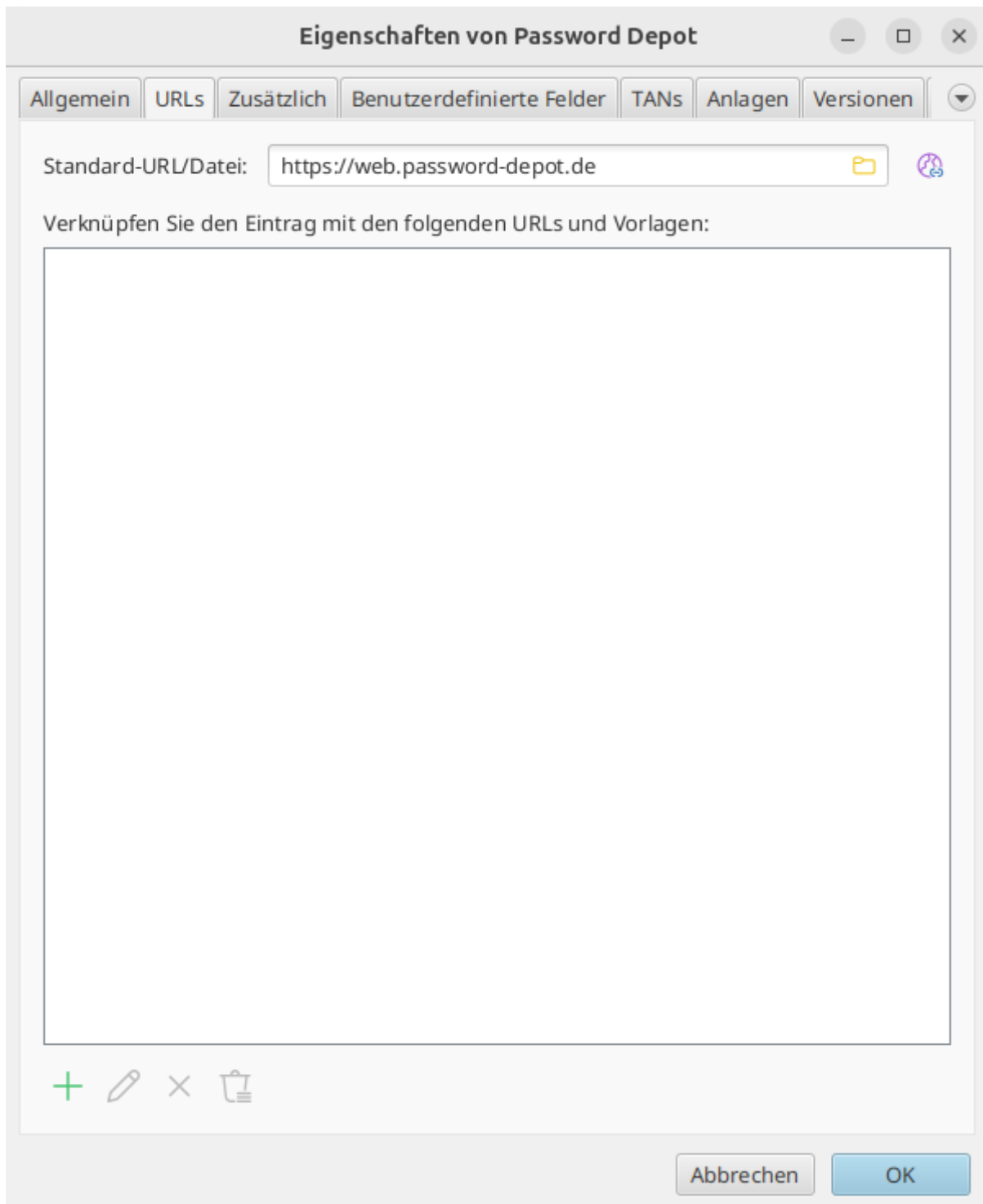
Abbrechen OK



## URLs und Vorlagen verwalten

Speichern Sie eine Standard-URL und bei Bedarf weitere URLs/Vorlagen für denselben Eintrag.

- Öffnen Sie den Eintrag und wechseln Sie zur Registerkarte **URLs**.
- Tragen Sie die Standard-URL ein und öffnen Sie diese bei Bedarf direkt über den entsprechenden Button.
- Fügen Sie ggf. weitere URLs/Vorlagen hinzu über das Plus-Symbol.
- Bearbeiten oder löschen Sie Einträge per Auswahl und Schaltfläche oder per Doppelklick.



## Erweiterte Einstellungen für einen Eintrag

Im Tab **Zusätzlich** können Sie weitere Konfigurationen vornehmen, wie ein Eintrag verwendet werden soll.

- **Autovervollständigungssequenz:** Legen Sie fest, welche Reihenfolge beim automatischen Ausfüllen verwendet werden soll (Benutzername, Tab, Passwort, TOTP).
- **Auto-Vervollständigungsmethode:** Wählen Sie die verwendete Methode für das automatische Ausfüllen aus (beispielsweise **Simulation von Tastatureingaben** oder **Zwischenablage**).
- **Bevorzugter Browser:** Legen Sie einen bevorzugten Browser fest. Falls gewünscht, wählen Sie zusätzlich die Option **URL im privaten Browsermodus öffnen**.

The screenshot shows the 'Eigenschaften von Passwort Depot' dialog box with the 'Zusätzlich' tab selected. The 'Autovervollständigungssequenz' section is highlighted with a red box. Below this section, there are three checkboxes: 'URL im privaten Browsermodus öffnen' (unchecked), 'Eintrag mit Browser-Add-ons nutzen' (checked), and 'Keine Kennwortrichtlinien für diesen Eintrag' (unchecked). At the bottom, there are fields for '2FA-Geheimnis' (masked with dots) and 'TOTP' (743636), and 'Abbrechen' and 'OK' buttons.

**Eigenschaften von Passwort Depot**

Allgemein | URLs | **Zusätzlich** | Benutzerdefinierte Felder | TANs | Anlagen | Versionen

Fenstertitel:  
[ ]

Befehlszeilenparameter:  
Geben Sie die Parameterzeichenfolge ein, die zum Öffnen einer lokalen Datei verwendet

**Autovervollständigungssequenz:**  
<USER><TAB><PASS><ENTER> [ ] **Komponieren**

Auto-Vervollständigungsmethode:  
Globale Einstellungen verwenden [ ]

Bevorzugter Browser:  
<Default Browser> [ ]

URL im privaten Browsermodus öffnen

Eintrag mit Browser-Add-ons nutzen

Keine Kennwortrichtlinien für diesen Eintrag

2FA-Geheimnis: [ ] TOTP: 743636 [ ]

**Abbrechen** **OK**

## TOTP (2FA) verwenden

- Öffnen Sie den Eintrag und wechseln Sie zur Registerkarte **Zusätzlich**.
- Tragen Sie das **2FA-Geheimnis** (Secret) ein.
- Kopieren Sie bei Bedarf den aktuellen TOTP-Code über das Kopier-Symbol rechts im Feld.

**ACHTUNG:** Behandeln Sie das 2FA-Geheimnis wie ein Passwort. Geben Sie den Code nur ein, wenn Sie der jeweiligen Website/App vertrauen.

## Benutzerdefinierte Felder

Für zusätzliche Informationen zu einem Eintrag, die nicht von den vorhandenen Feldern abgedeckt werden, können Sie benutzerdefinierte Felder anlegen (z. B. Sicherheitsfrage, Kundennummer, Recovery-Codes).

- Öffnen Sie den Eintrag und wechseln Sie zur Registerkarte **Benutzerdefinierte Felder**.
- Klicken Sie auf das Plus-Symbol, um ein Feld hinzuzufügen.
- Wählen Sie Typ und Wert. Markieren Sie vertrauliche Werte als geschützt.
- Blenden Sie geschützte Werte bei Bedarf ein/aus (Augen-Symbol).

Eigenschaften von Passwort Depot

Allgemein | URLs | Zusätzlich | **Benutzerdefinierte Felder** | TANs | Anlagen | Versionen

Name	Typ	Wert
Kein Inhalt in Tabelle		

+ ✎ ✕ ↑ ↓ 👁

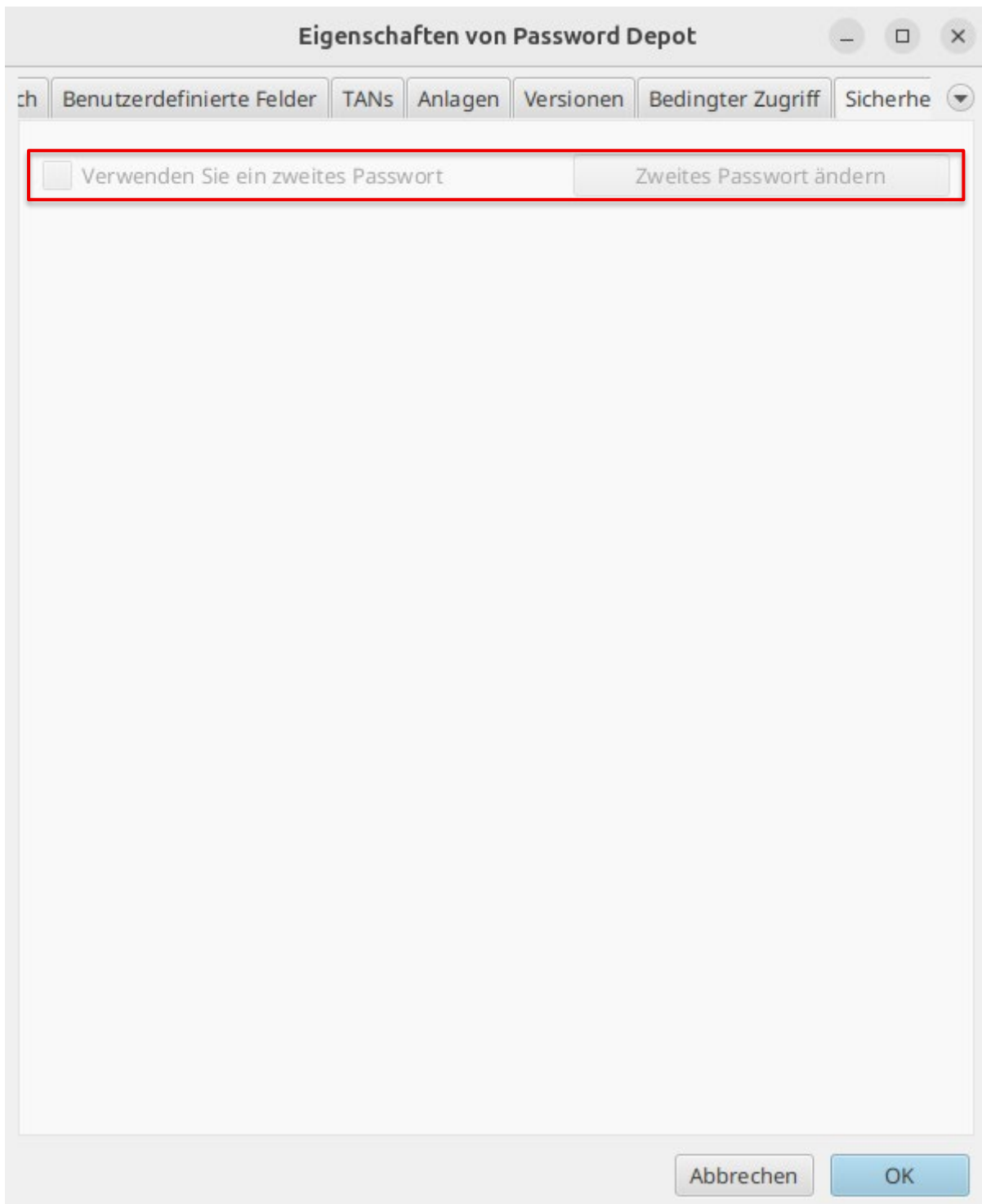
Abbrechen OK

## Zweites Passwort für kontrollierten Zugriff

Schützen Sie besonders sensible Einträge zusätzlich mit einem zweiten Passwort (separates Passwort pro Eintrag/Ordner).

- Öffnen Sie den entsprechenden Eintrag und wechseln Sie zur Registerkarte **Sicherheit**.
- Aktivieren Sie die Option **Verwenden Sie ein zweites Passwort**.
- Legen Sie das zweite Passwort fest und speichern Sie den Eintrag.
- Beim Öffnen eines Eintrags wird nun zusätzlich das zweite Kennwort abgefragt.

**WICHTIG:** Merken Sie sich auch das Zweitpasswort zuverlässig. Ohne Zweitpasswort bleiben geschützte Inhalte gesperrt.



## Bedingter Zugriff (Warnmeldung beim Zugriff)

Lassen Sie beim Zugriff auf einen Eintrag eine Warnmeldung anzeigen – optional mit Bestätigungstext.

- Öffnen Sie den Eintrag und wechseln Sie zur Registerkarte **Bedingter Zugriff**.
- Aktivieren Sie die Option **Beim Zugriff die Warnmeldung anzeigen**.
- Geben Sie den Warntext ein und wählen Sie einen Wichtigkeitsgrad aus.
- Wenn **Kritisch** ausgewählt ist: Definieren Sie zusätzlich einen Bestätigungstext, den Sie beim Zugriff eingeben müssen.

The screenshot shows the 'Eigenschaften von Password Depot' dialog box with the 'Bedingter Zugriff' tab selected. The dialog has a title bar with standard window controls (minimize, maximize, close) and a tabbed interface with tabs for 'Benutzerdefinierte Felder', 'TANs', 'Anlagen', 'Versionen', 'Bedingter Zugriff', and 'Sicherheit'. The 'Bedingter Zugriff' tab is active and contains the following sections:

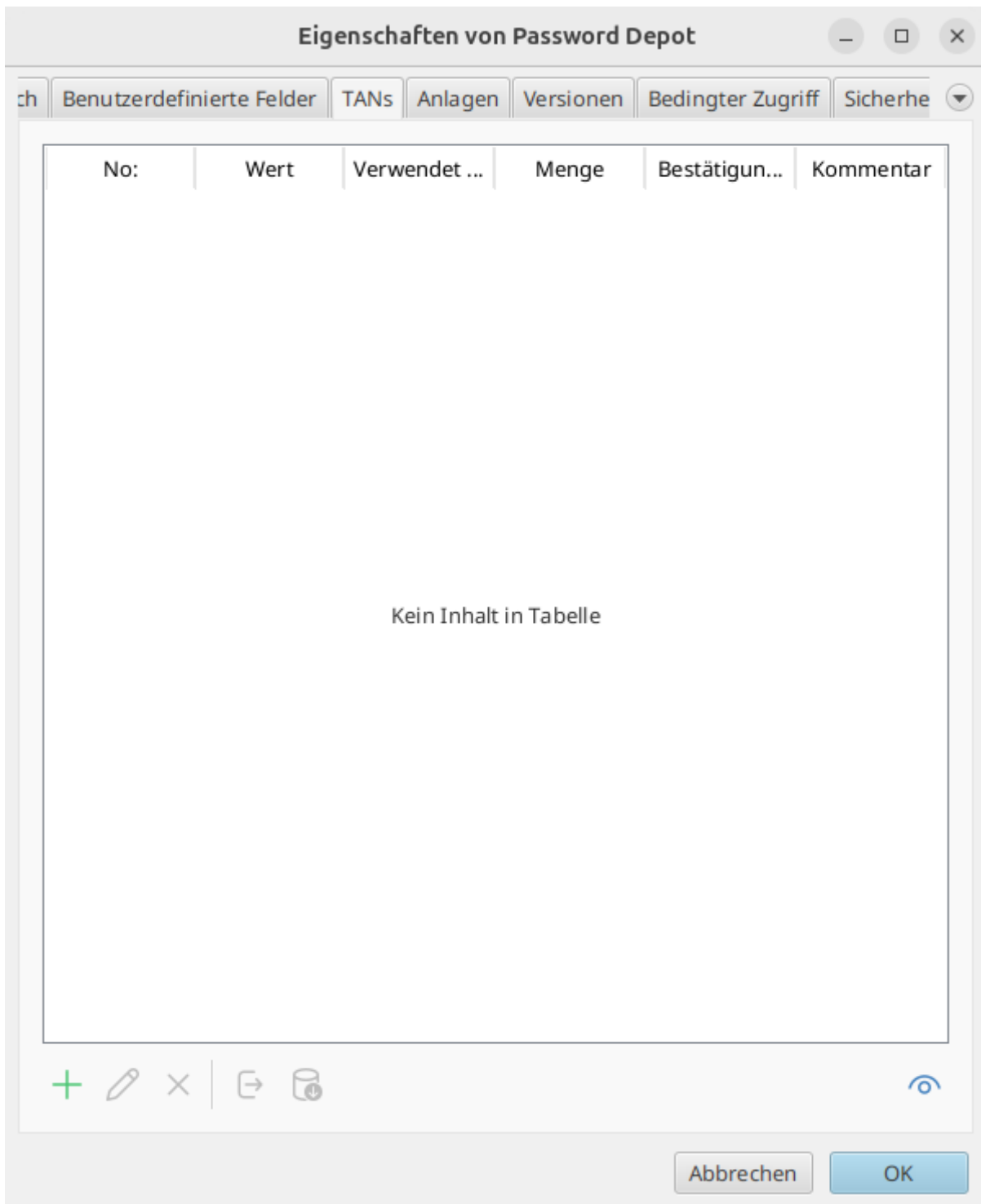
- Warnmeldung**: A section with a checkbox labeled 'Beim Zugriff die Warnmeldung anzeigen:'. Below the checkbox is a large empty text area for entering the warning message.
- Schweregrad:**: A section with three radio button options: 'Informationen (Popup-Benachrichtigung)' (selected), 'Major (modales Meldungsfeld)', and 'Kritisch (modales Dialogfeld mit dem Überprüfungstext):'. Below the 'Kritisch' option is a text input field for a confirmation message.
- Beschränken Sie den Zugriff auf den Eintrag**: A section with a checkbox labeled 'Aktive Verbindung zum Password Depot Server erforderlich'.

At the bottom right of the dialog are two buttons: 'Abbrechen' and 'OK'.

## TANs verwalten

Wenn Sie TANs verwenden, können Sie diese pro Eintrag speichern und als "verwendet" dokumentieren.

- Öffnen Sie den Eintrag und wechseln Sie zur Registerkarte **TANs**.
- Klicken Sie auf das Plus-Symbol, um eine TAN hinzuzufügen.
- Bearbeiten Sie TANs wenn nötig per Doppelklick.
- Blenden Sie TAN-Werte bei Bedarf ein/aus (Augen-Symbol).



## Schnellaktionen in der Detailansicht

In der Detailansicht rechts finden Sie über die Symbole verschiedene Schnellaktion, um wichtige Elemente direkt zu übertragen. Zur Verfügung stehen unter anderem:

- **Benutzername kopieren.**
- **Passwort kopieren.**
- **URL kopieren oder URL öffnen.**

The screenshot displays the Password Depot 19 (alpha) application. The main window is titled 'Password Depot 19 (alpha)' and shows a list of entries under the folder 'AceBIT-GmbH\_EN.p...'. The entry 'Password Depot' is selected, and its details are shown on the right. A red box highlights the action icons above the details panel: a lightning bolt (copy), a person (copy username), a key (copy password), a document (copy URL), a globe (open URL), and a refresh icon.

Beschreibung	URL	Benutzername	Geändert
Ordner			
Bank			20.12.2022 09:26:51
Credit cards			18.08.2023 14:46:40
Email accounts			30.10.2024 14:50:44
Passwort			
AceBIT Support	https://support.aceb...	Admin	18.08.2023 14:44:22
Password Depot	https://web.passwor...	AceBIT	15.05.2025 14:54:39
Kreditkarte			
Mastercard			15.05.2025 10:59:31
Visa			26.01.2026 15:21:01
Lizenz			
Password Depot 19			26.01.2026 15:15:00
Remotedesktopver...			
Windows Server	192.168.1.182		21.04.2022 11:24:13
TeamViewer			
TeamViewer PC1			21.04.2022 11:25:25

Details for 'Password Depot':

Benutzername	AceBIT
Passwort	*****
URL	https://web.password...
TOTP	630187 [26]
Bedeutung	Medium
Autor	UserA
Zuletzt geändert	15.05.2025 14:54:39

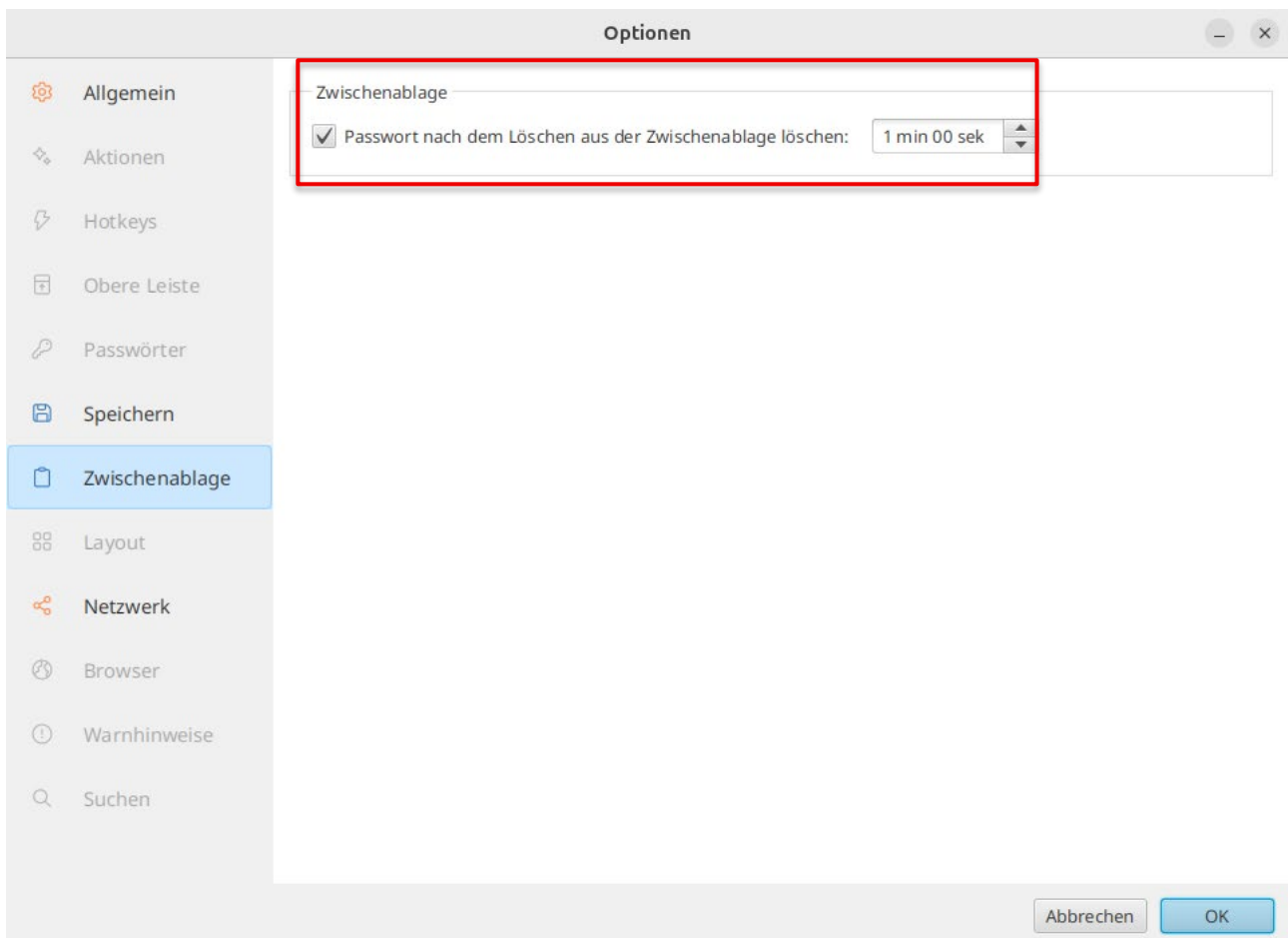
## Tipps

### Sicher arbeiten

- Wählen Sie ein langes, einzigartiges Master-Passwort und verwenden Sie es nur für Password Depot.
- Aktivieren Sie das automatische Löschen der Zwischenablage, wenn Sie häufig Passwörter kopieren.
- Nutzen Sie ein Ablaufdatum für zeitkritische Passwörter und überprüfen Sie abgelaufene Einträge regelmäßig.
- Schützen Sie wichtige Einträge mit einem zweiten Passwort oder mit bedingtem Zugriff.

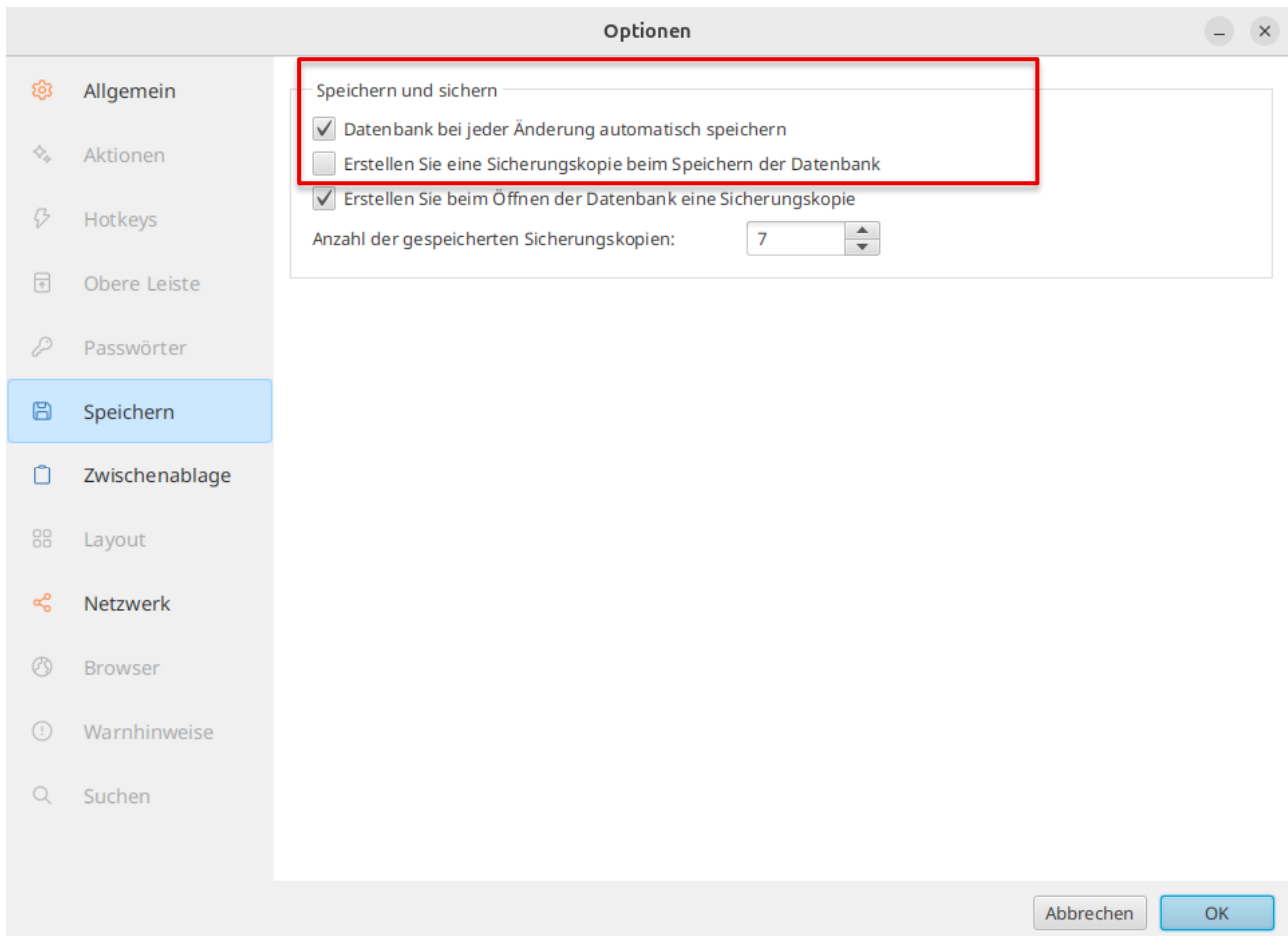
### Zwischenablage automatisch löschen

- Öffnen Sie **Bearbeiten** → **Optionen**.
- Wählen Sie links den Menüpunkt **Zwischenablage**.
- Aktivieren Sie die Option zum automatischen Löschen des Kennworts aus der Zwischenablage und stellen Sie die gewünschte Zeit ein.



## Automatisch speichern und Backups nutzen

- Navigieren Sie zu **Bearbeiten** → **Optionen**.
- Wählen Sie links den Menüpunkt **Speichern**.
- Aktivieren Sie **Automatisch speichern** und Backups beim Öffnen/Speichern.
- Legen Sie fest, wie viele Sicherungskopien aufbewahrt werden.



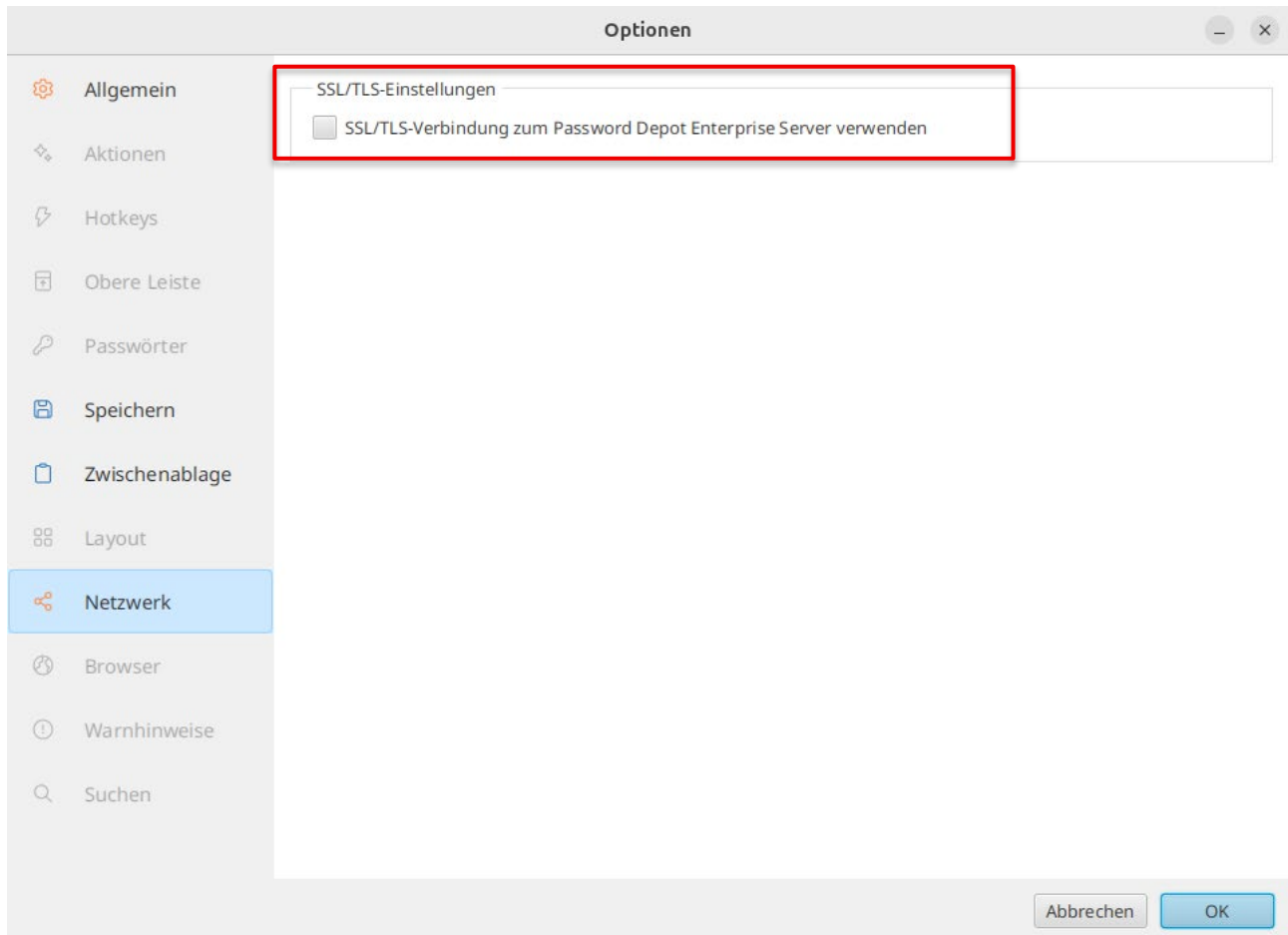
## Sprache ändern

- Öffnen Sie **Bearbeiten** → **Optionen** → **Allgemein**.
- Wählen Sie die gewünschte Sprache aus.
- Starten Sie die App neu, damit die Sprache vollständig übernommen wird.

## Verschlüsselte Verbindung (SSL/TLS) für Enterprise Server

Wenn Sie den Password Depot Enterprise Server nutzen, können Sie eine verschlüsselte Verbindung (SSL/TLS) aktivieren.

- Navigieren Sie zu Sie **Bearbeiten** → **Optionen** → **Netzwerk**.
- Aktivieren Sie **SSL/TLS-Verbindung zum Password Depot Enterprise Server verwenden**.



## Wenn etwas nicht funktioniert

- Falsches Master-Passwort/Schlüsseldatei: Prüfen Sie Groß-/Kleinschreibung und wählen Sie die korrekte Schlüsseldatei.
- Referenzeintrag nicht gefunden: Der verknüpfte Eintrag wurde gelöscht oder verschoben. Öffnen Sie den Originaleintrag oder korrigieren Sie die Verknüpfung.
- Eintrag verlangt Server-Verbindung: Öffnen Sie die Datenbank über **Enterprise Server** und stellen Sie eine aktive Verbindung her.

## Hilfe und Support

Beachten Sie, dass es sich beim Password Depot-Client für Linux um eine frühe Version handelt und noch nicht alle Funktionen auswählbar sind.

Wählen Sie bei weiterem Unterstützungsbedarf **Hilfe** → **Online-Support**. Dort finden Sie Antworten auf häufige Fragen und können uns zusätzlich über die bereitgestellten Formulare direkt kontaktieren.