



**PASSWORD
DEPOT**
BY AceBIT

Password Depot for Linux

Quick Start Guide – Linux

As of: January 26, 2026

This guide shows you the most important steps for using Password Depot on Linux securely—no technical knowledge required.

Table of Contents

Table of Contents	2
Introduction.....	3
What the app looks like (quick overview)	3
Key terms.....	4
Getting started	5
Open the Database Manager	5
Create a new database (local or cloud).....	6
Select or create a key file	7
Open and unlock a database	8
Connect cloud storage (Dropbox, Google Drive, OneDrive, HiDrive, Box).....	9
Enterprise Server (company).....	10
Getting oriented in the main view	11
Core features.....	12
Create entries	12
Password entry: most important fields.....	13
Use the password generator	14
Manage URLs and templates.....	15
Additional settings for an entry.....	16
Use TOTP (2FA).....	17
Custom fields	17
Second password for controlled access	18
Conditional access (warning on access)	19
Manage TANs.....	20
Quick actions in the details view	21
Tips	22
Work securely.....	22
Automatically clear the clipboard	22
Auto-save and use backups.....	23
Change language	23
Encrypted connection (SSL/TLS) for Enterprise Server	24
If something does not work.....	24
Help and support.....	24

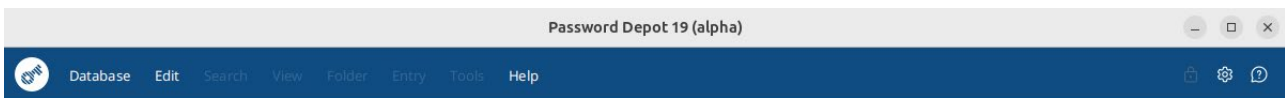
Introduction

Password Depot stores credentials, documents, and other confidential information in an encrypted database. This database is opened with a master password (and optionally a key file).

IMPORTANT: Without your database master password, your data cannot be recovered. Choose a strong password that you can keep safe.

What the app looks like (quick overview)

- **Start screen:** From the start screen, you can access the Database Manager.
- **Database Manager:** In the Database Manager, you can create, select, and open databases (databases stored locally, in the cloud, databases from the Enterprise Server, or backups/backup files).
- **Main view:** On the left you see the navigation, in the middle the list of entries in the currently opened database, and on the right you will find details and quick actions.



Password Depot 19 (alpha)

 Database Manager
Open an existing or creates a new database

 Exit
Exits the program

Key terms

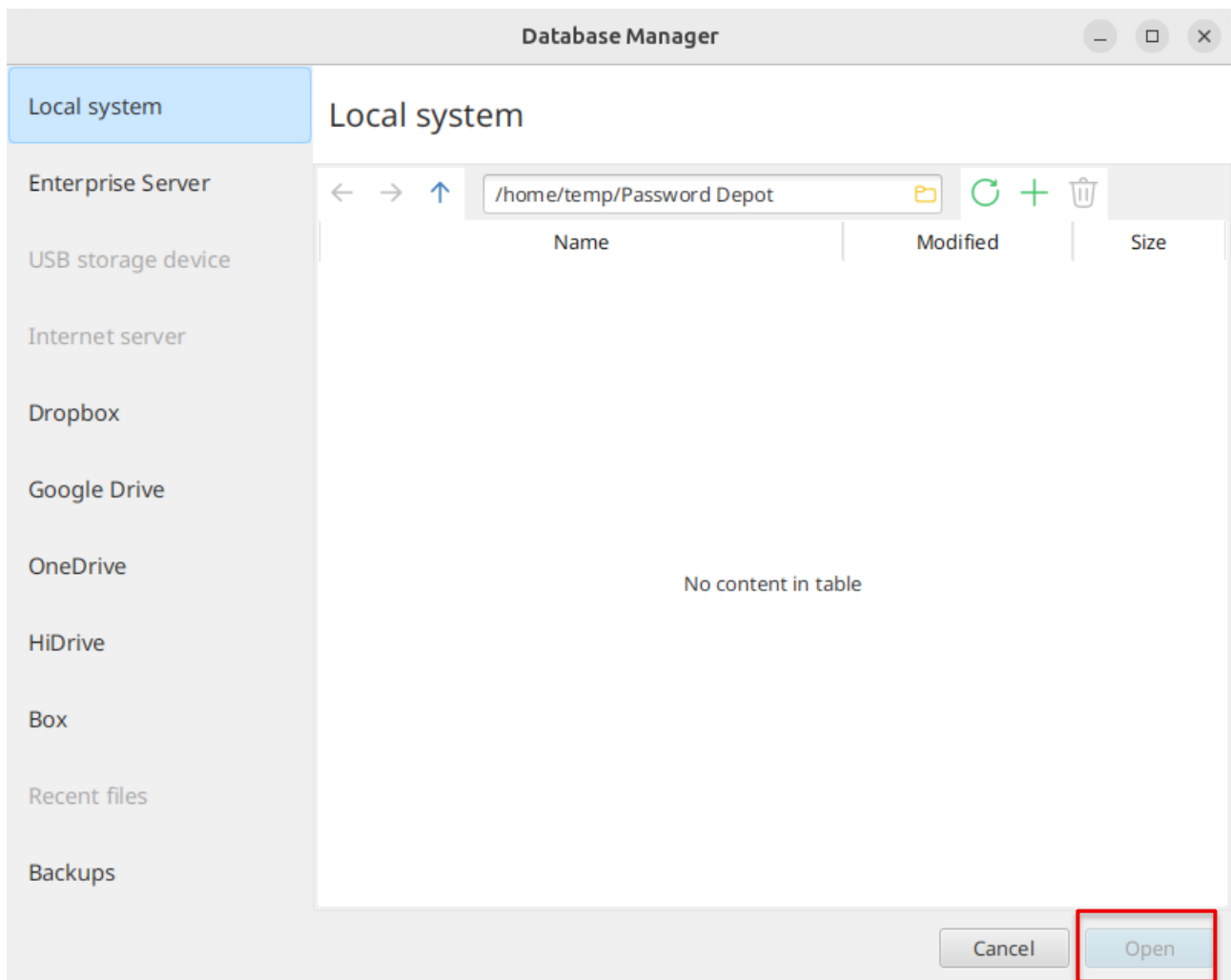
- **Database:** This is your encrypted file containing all entries (e.g., "Private.psw").
- **Master password:** This is the main password used to open the database.
- **Key file:** This is an additional file that acts as a second factor for opening the database (2FA = two-factor authentication).
- **Entry:** An entry is a stored item, e.g., a password, credit card, or identity.
- **TOTP:** This is a time-based one-time code for 2FA logins.

Getting started

Open the Database Manager

The **Database Manager** is the central administration area of Password Depot for Linux and provides an overview of the available storage locations and databases.

- On the start screen, click **Database Manager**.
- On the left, select the desired storage location (**Local system**, **Enterprise Server**, **Dropbox**, **Google Drive**, **OneDrive**, **HiDrive**, **Box**, or **Backups**).
- Select the desired database from the list and click **Open**.




Create a new database (local or cloud)

To create a new database, proceed as follows:

- In the **Database Manager**, open a storage location (e.g., **Local system** or a cloud service).
- Click **New** (plus icon).
- Enter a database name.
- Select the desired authentication: **master password**, **master password and key file**, or **key file** only.
- Enter a master password and repeat it. If a key file was selected in addition to or instead of the master password as an authentication method, specify it as well.
- Optional: Check the master password against known password leaks (**Check in Pwned Passwords**).
- Click OK to complete creating your database.

IMPORTANT: Choose a strong master password: ideally it is at least 12 characters long and is used only once.

New Database



Specify settings for the new database

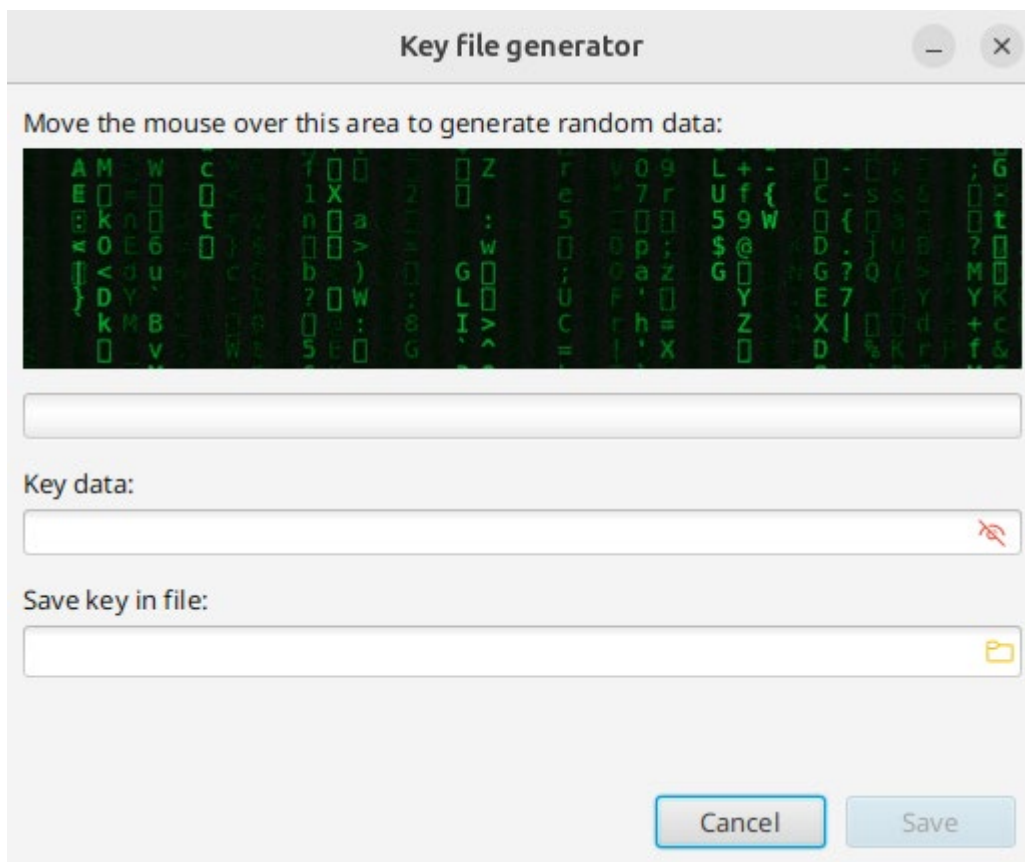
Database name: <input type="text"/>	Authentication by: <input type="text" value="Master password"/>
Comment: <input type="text"/>	Master password: <input type="password"/>
Hint for master password: <input type="text"/>	Re-enter master password: <input type="password"/>
	Key file: <input type="text"/>

Select or create a key file

If you use the authentication method **master password and key file** or **key file** only, you need a file with the .key extension. You can select an existing file or generate a new one.

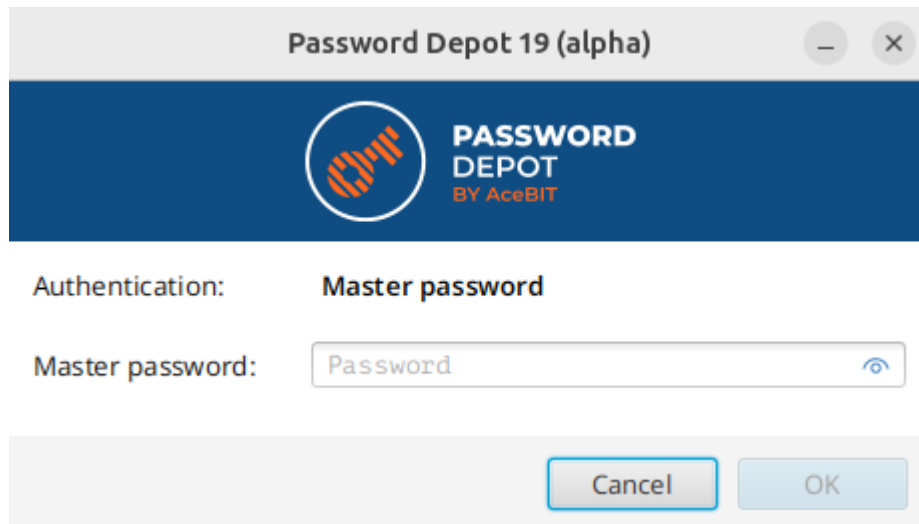
- For **Key file**, click **Select** to choose an existing file.
- Alternatively, click **Generate** to create and save a new key file.

IMPORTANT: Store the key file separately from the master password. If you lose the key file, you also lose access to the database protected by it.



Open and unlock a database

- Select a database in the **Database Manager**.
- Click **Open** or double-click the corresponding file.
- In the unlock dialog, enter the master password and, if applicable, select the corresponding key file.
- Finally, click **OK** to open the database.

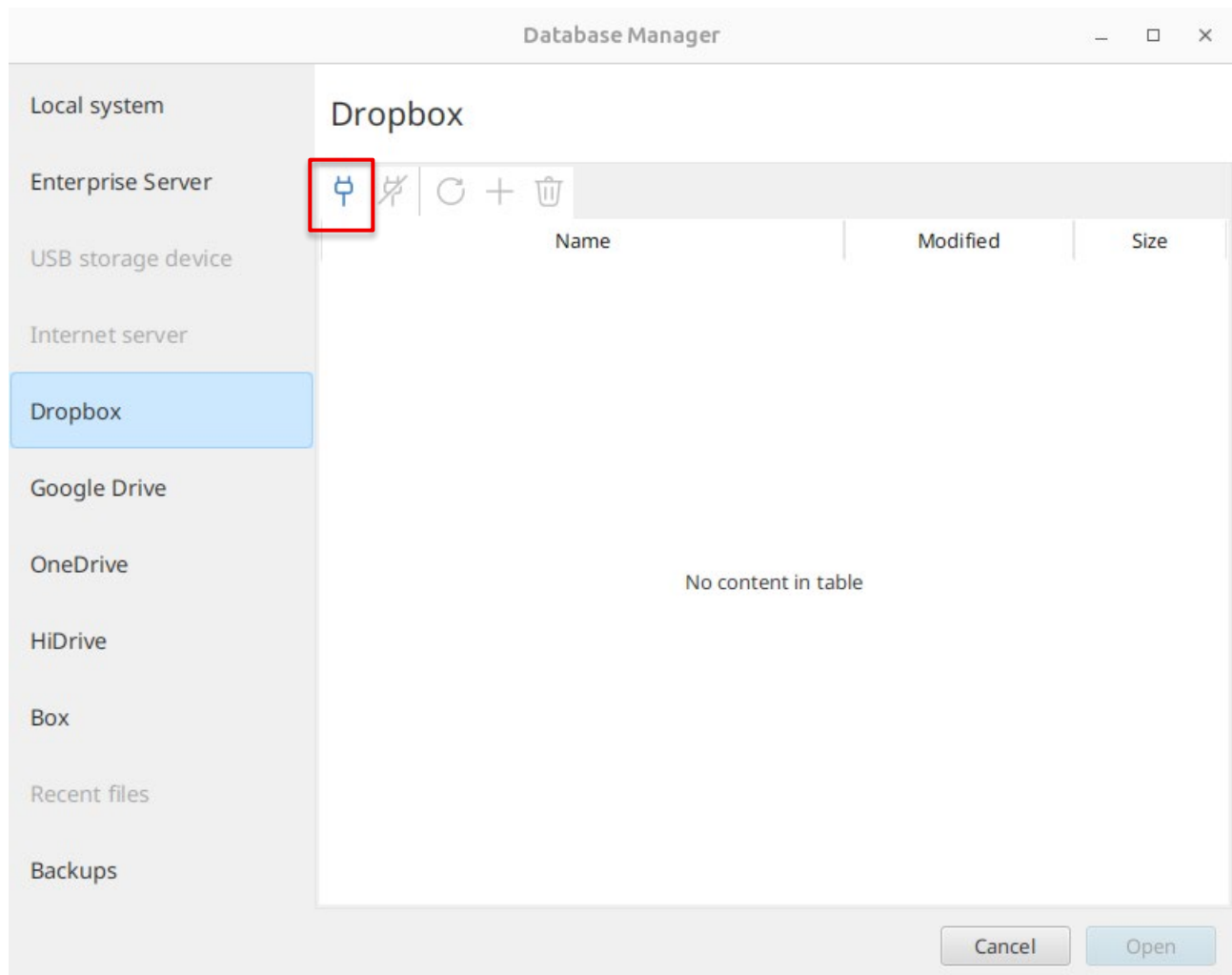


The screenshot shows a dialog box titled "Password Depot 19 (alpha)". The dialog has a dark blue header with the Password Depot logo and the text "PASSWORD DEPOT BY AceBIT". Below the header, the "Authentication:" label is followed by "Master password". Underneath, the "Master password:" label is followed by a text input field containing the word "Password" and a small eye icon to toggle visibility. At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

Connect cloud storage (Dropbox, Google Drive, OneDrive, HiDrive, Box)

For cloud storage, you must authorize Password Depot once in your default browser.

- In the **Database Manager**, select the desired cloud storage.
- Click **Connect** (plug icon).
- Follow the instructions in the browser and allow access.
- Return to the app and click **Refresh** if necessary.



Enterprise Server (company)

If your organization uses a Password Depot Enterprise Server, you will receive the login details from your administrator.

- In the Database Manager, select **Enterprise Server**.
- Click **Connect** (plug icon) and enter the server address, port, server version, username, and password. If set up by your company, Azure AD authentication is also available in addition to standard authentication.
- Open a shared database from the list.

WARNING: Databases on the Enterprise Server can only be created using the server's Server Manager. You can only open databases on the server if you are authorized. Access rights are granted by your server administrator.



The screenshot shows a 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 number field containing "25019".
- A dropdown menu currently showing "Enterprise Server 19".
- A dropdown menu currently showing "Standard Authentication".
- A text input field labeled "User name" with a user icon on the left.
- A text input field labeled "Password" with a key icon on the left and an eye icon on the right to toggle visibility.

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

Getting oriented in the main view

- On the left you see the navigation (e.g., Database, Recycle Bin, Categories).
- In the middle is the list of entries. Double-click a (sub)folder to open it.
- On the right, details for the selected entry and quick actions (Copy, open URL) are shown.
- At the top are the toolbar buttons (Database Manager, New Entry, Edit, back/forward navigation, etc.).

The screenshot displays the main interface of Password Depot 19 (alpha). The window title is "Password Depot 19 (alpha)". The interface is divided into several sections:

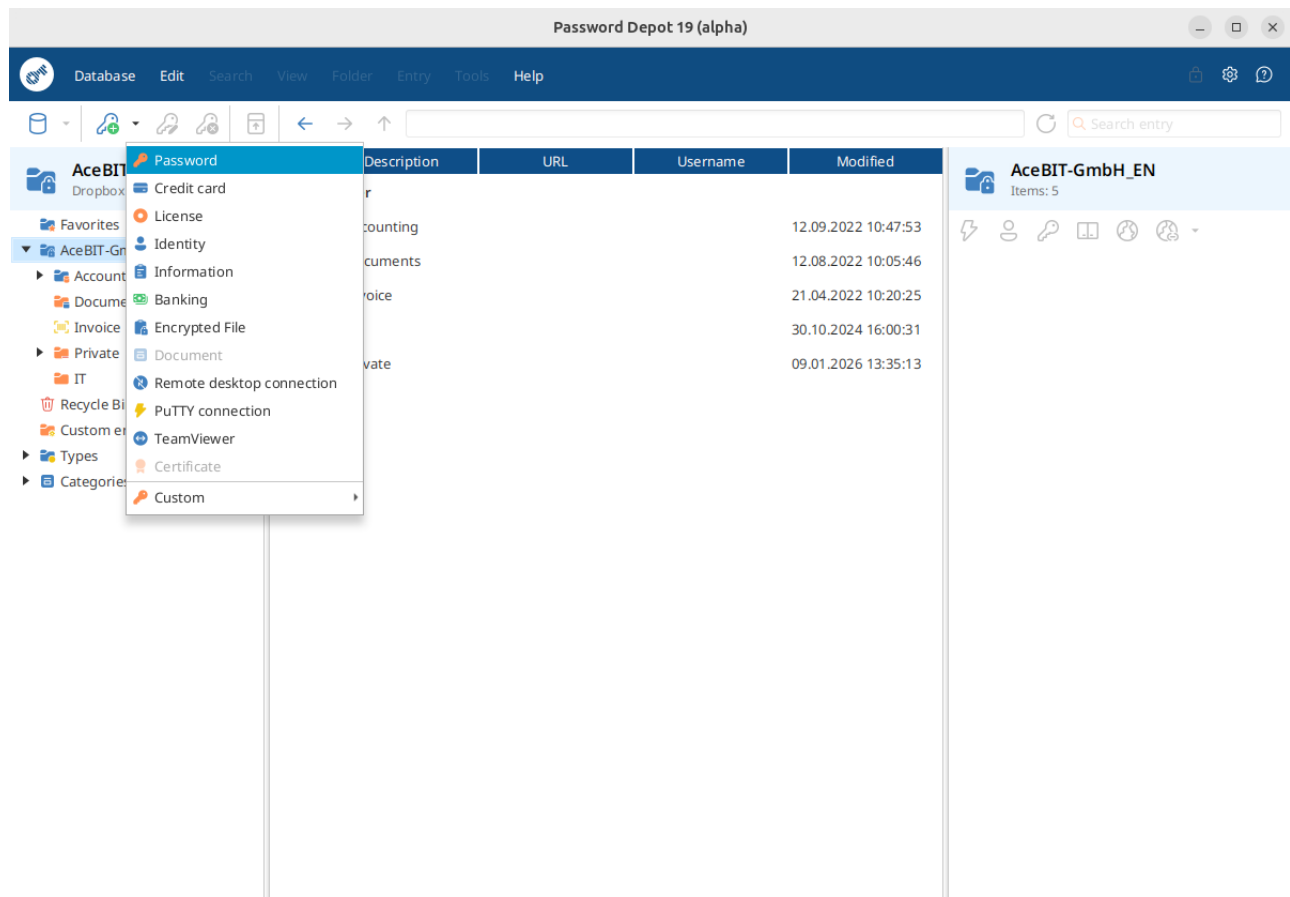
- Top Menu:** Database, Edit, Search, View, Folder, Entry, Tools, Help.
- Toolbar:** Includes navigation icons (back, forward, up), a search bar labeled "Search entry", and other utility icons.
- Left Panel:** A navigation tree showing the current location: "AceBIT-GmbH_EN.p..." (Dropbox) > "AceBIT-GmbH_EN". Below it are "Favorites" and a list of folders: Accounting, Documents, Invoice, Private, IT, Recycle Bin, Custom entry types, Types, and Categories.
- Center Panel:** A table listing the contents of the "AceBIT-GmbH_EN" folder. The table has columns for "Description", "URL", "Username", and "Modified".
- Right Panel:** A summary for the selected folder "AceBIT-GmbH_EN" showing "Items: 5" and a set of quick action icons (copy, paste, etc.).

Description	URL	Username	Modified
Folder			
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

Core features

Create entries

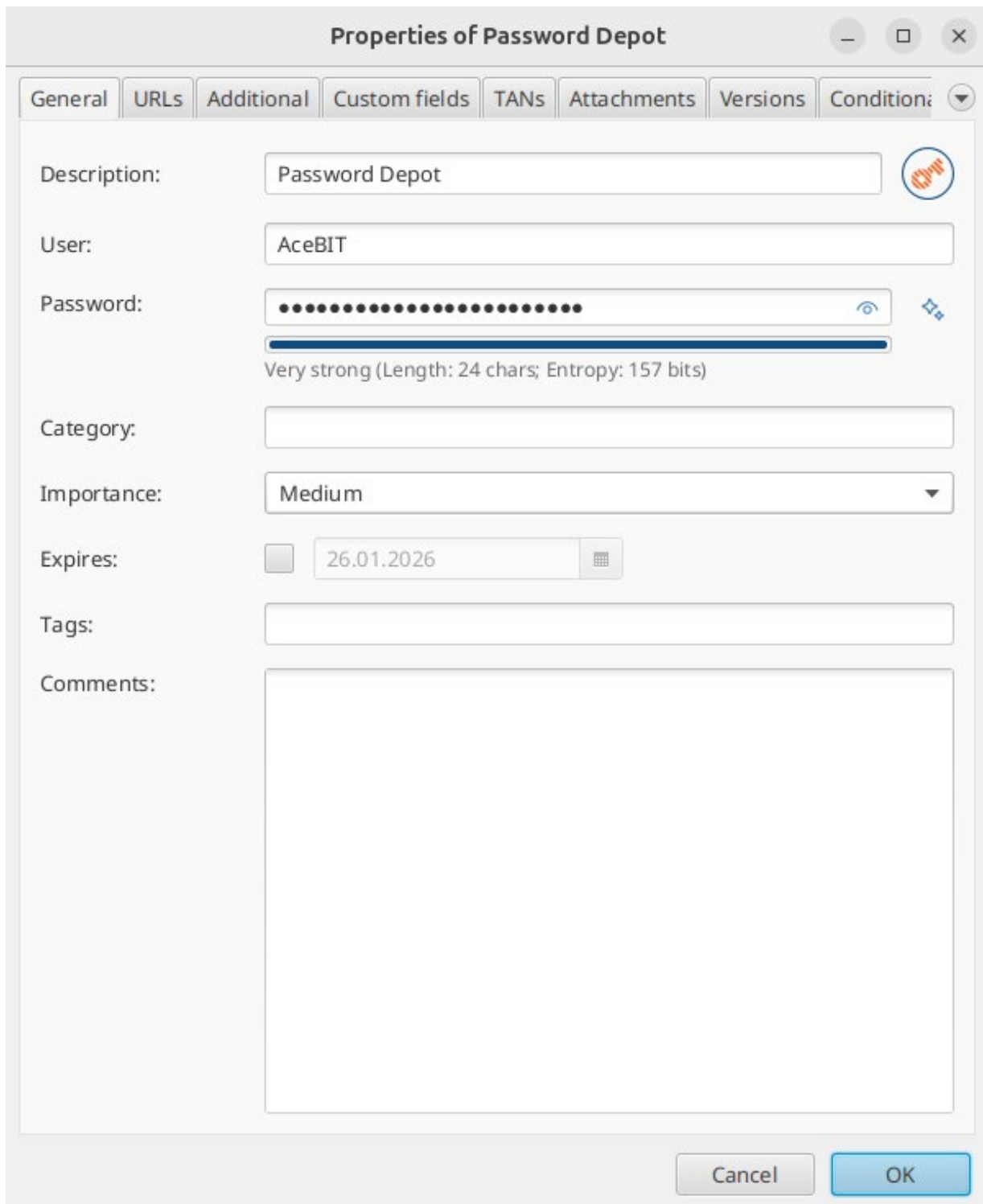
- At the top, click **New Entry** (key with plus icon). This creates an entry of type **Password**.
- For other entry types, click the small triangle next to **New Entry**.
- Select the desired type (e.g., credit card, identity, etc.).
- Fill in the required fields and click **OK** to save the entry.



Password entry: most important fields

Depending on the entry type, different fields are available. Except for the **Description** field, these are optional depending on the type. The most important fields include:

- **Description:** Name of the entry (e.g., "Email – personal").
- **Username and password.**
- **Category and keywords (tags):** This allows better organization and makes it easier to find important entries.
- **Expiration date** (defined validity date for an entry) and additional **comments**.



The screenshot shows a window titled "Properties of Password Depot" with several tabs: General, URLs, Additional, Custom fields, TANs, Attachments, Versions, and Condition. The "General" tab is active. The fields are as follows:

- Description:** Password Depot
- User:** AceBIT
- Password:** A field containing 24 dots, with a strength indicator below it showing "Very strong (Length: 24 chars; Entropy: 157 bits)".
- Category:** (Empty)
- Importance:** Medium
- Expires:** A checkbox is unchecked, and the date is 26.01.2026.
- Tags:** (Empty)
- Comments:** (Empty text area)

At the bottom right, there are "Cancel" and "OK" buttons.

Use the password generator

- Open a password entry (create a new one or edit an existing one).
- In the password field, click **Generate (password generator)**.
- In addition to the standard variant, the **Advanced** or **Passphrase** tabs provide additional configuration options for the password generator.
- Adjust length/options as desired and confirm the result with **OK**.

Password Generator

Standard | **Advanced** | Passphrase

Options:

- Lowercase
- Numbers
- Uppercase
- Special
- Exclude characters: o00LlI1,\'\"/>

Length: 10

Password policy

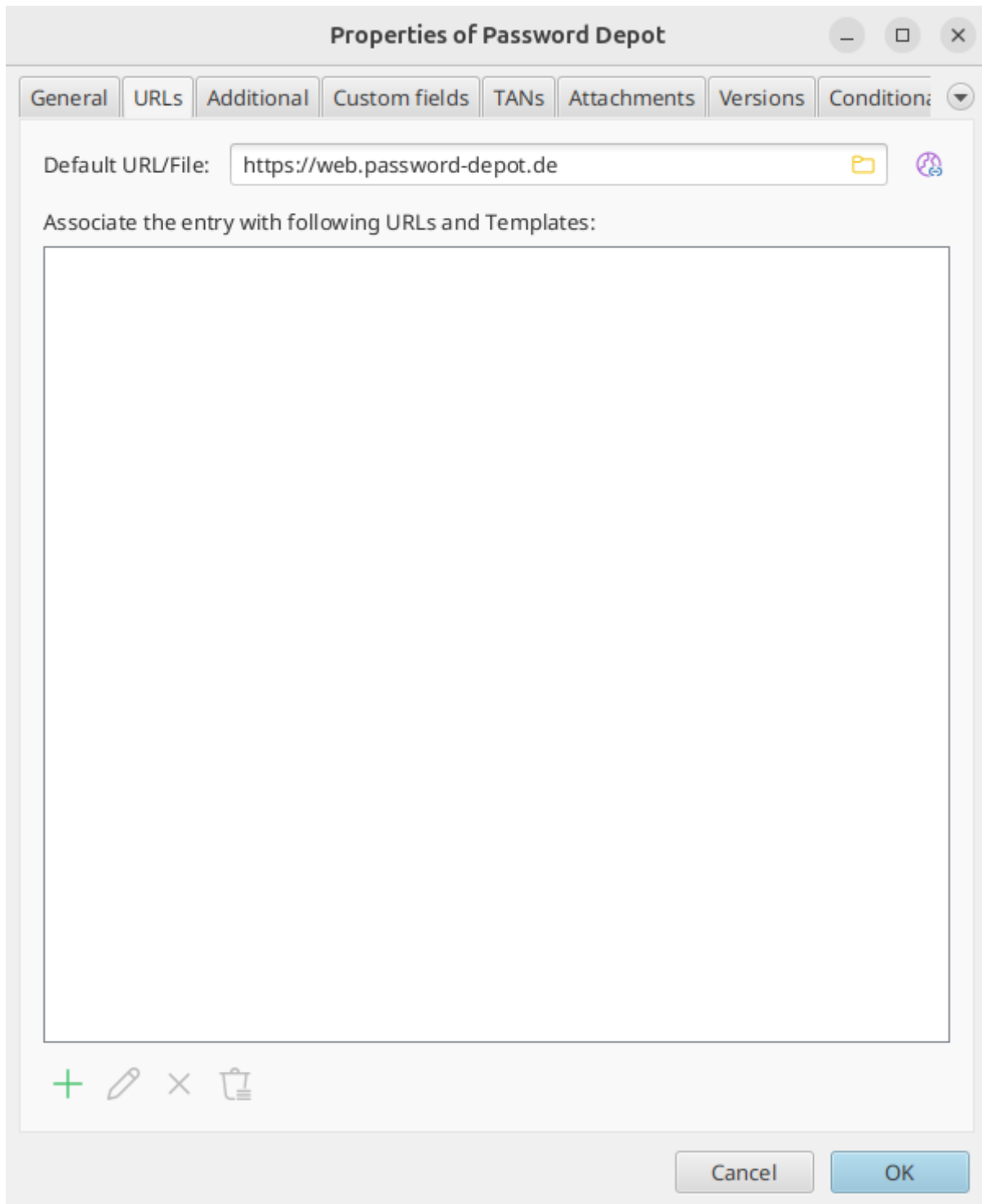
Move the mouse over this area to generate random data:

Password:

Manage URLs and templates

Save a default URL and, if needed, additional URLs/templates for the same entry.

- Open the entry and switch to the **URLs** tab.
- Enter the default URL and, if needed, open it directly using the corresponding button.
- If necessary, add additional URLs/templates using the plus icon.
- Edit or delete items by selecting them and using the button, or by double-clicking.



Additional settings for an entry

On the **Additional** tab, you can configure additional options for how an entry should be used.

- **Auto-complete sequence:** Define the order used for auto-fill (username, Tab, password, TOTP).
- **Auto-complete method:** Select the method used for auto-fill (for example, **simulating keystrokes** or using the **clipboard**).
- **Preferred browser:** Set a preferred browser. If desired, also select the option to **Open URL in private browsing mode**.

The screenshot shows the 'Properties of Password Depot' dialog box with the 'Additional' tab selected. The 'Auto-complete sequence' is set to '<USER><TAB><PASS><ENTER>' with a 'Compose' button. The 'Auto-complete method' is set to 'Use global settings'. The 'Preferred browser' is set to '<Default Browser>'. Other settings include 'Open URL in private browsing mode' (unchecked), 'Use entry with browser add-ons' (checked), and 'No password policies for this entry' (unchecked). The '2FA Secret' is masked with dots and the 'TOTP' is set to '718907'. 'Cancel' and 'OK' buttons are at the bottom.

Field	Value
Window title	
Command line parameters	Enter the parameters string used to open a local file
Auto-complete sequence	<USER><TAB><PASS><ENTER>
Auto-complete method	Use global settings
Preferred browser	<Default Browser>
Open URL in private browsing mode	<input type="checkbox"/>
Use entry with browser add-ons	<input checked="" type="checkbox"/>
No password policies for this entry	<input type="checkbox"/>
2FA Secret	•••••
TOTP	718907

Use TOTP (2FA)

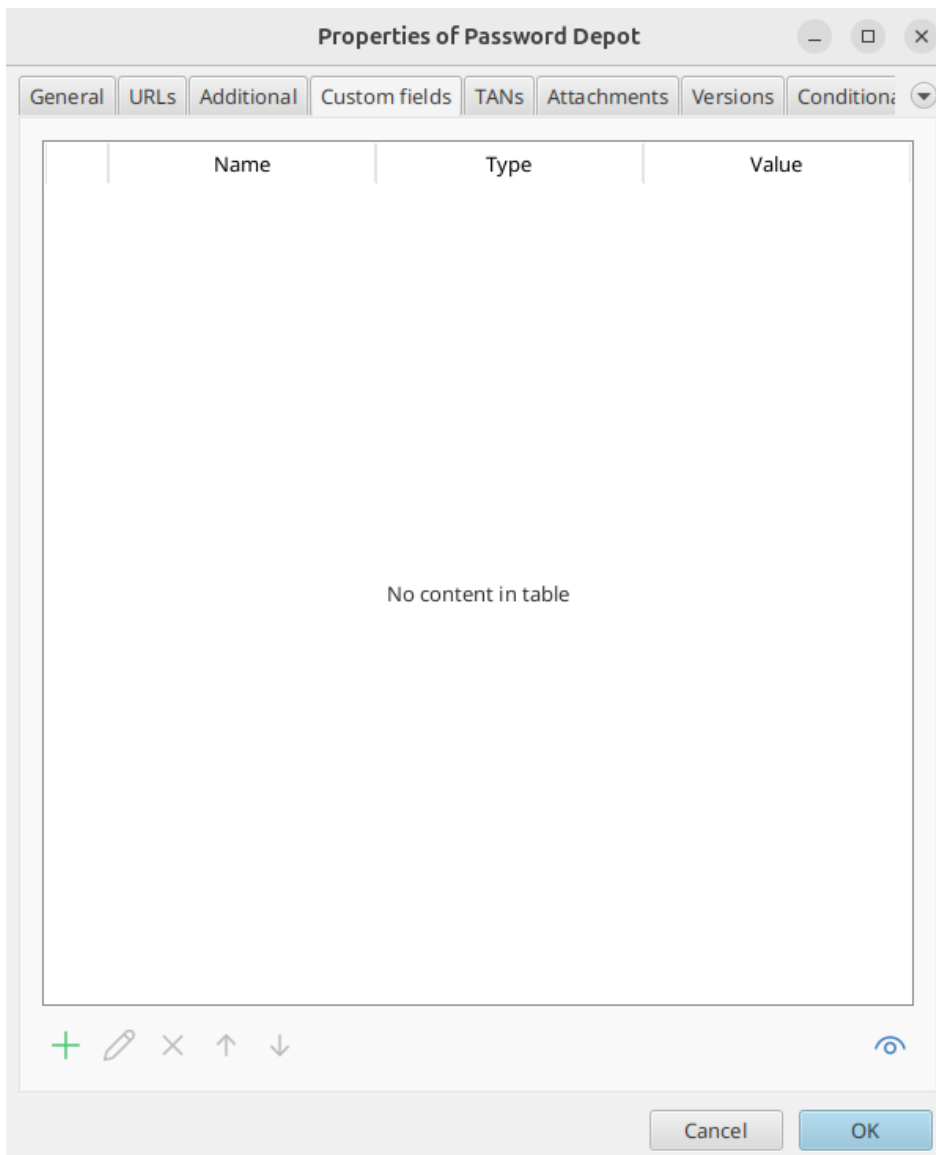
- Open the entry and switch to the **Additional** tab.
- Enter the **2FA Secret**.
- If needed, copy the current TOTP code using the copy icon on the right side of the field.

WARNING: Treat the 2FA secret like a password. Only enter the code if you trust the respective website/app.

Custom fields

For additional information about an entry that is not covered by the existing fields, you can create custom fields (e.g., security question, customer number, recovery codes).

- Open the entry and switch to the **Custom fields** tab.
- Click the plus icon to add a field.
- Select type and value. Mark confidential values as protected.
- Show/hide protected values as needed (eye icon).



The screenshot shows a dialog box titled "Properties of Password Depot" with several tabs: General, URLs, Additional, Custom fields, TANS, Attachments, Versions, and Conditions. The "Custom fields" tab is selected. It contains a table with three columns: Name, Type, and Value. The table is currently empty, displaying "No content in table". At the bottom of the table area, there are icons for adding (+), editing (pencil), deleting (X), moving up (↑), and moving down (↓). A blue eye icon is also present. At the bottom of the dialog, there are "Cancel" and "OK" buttons.

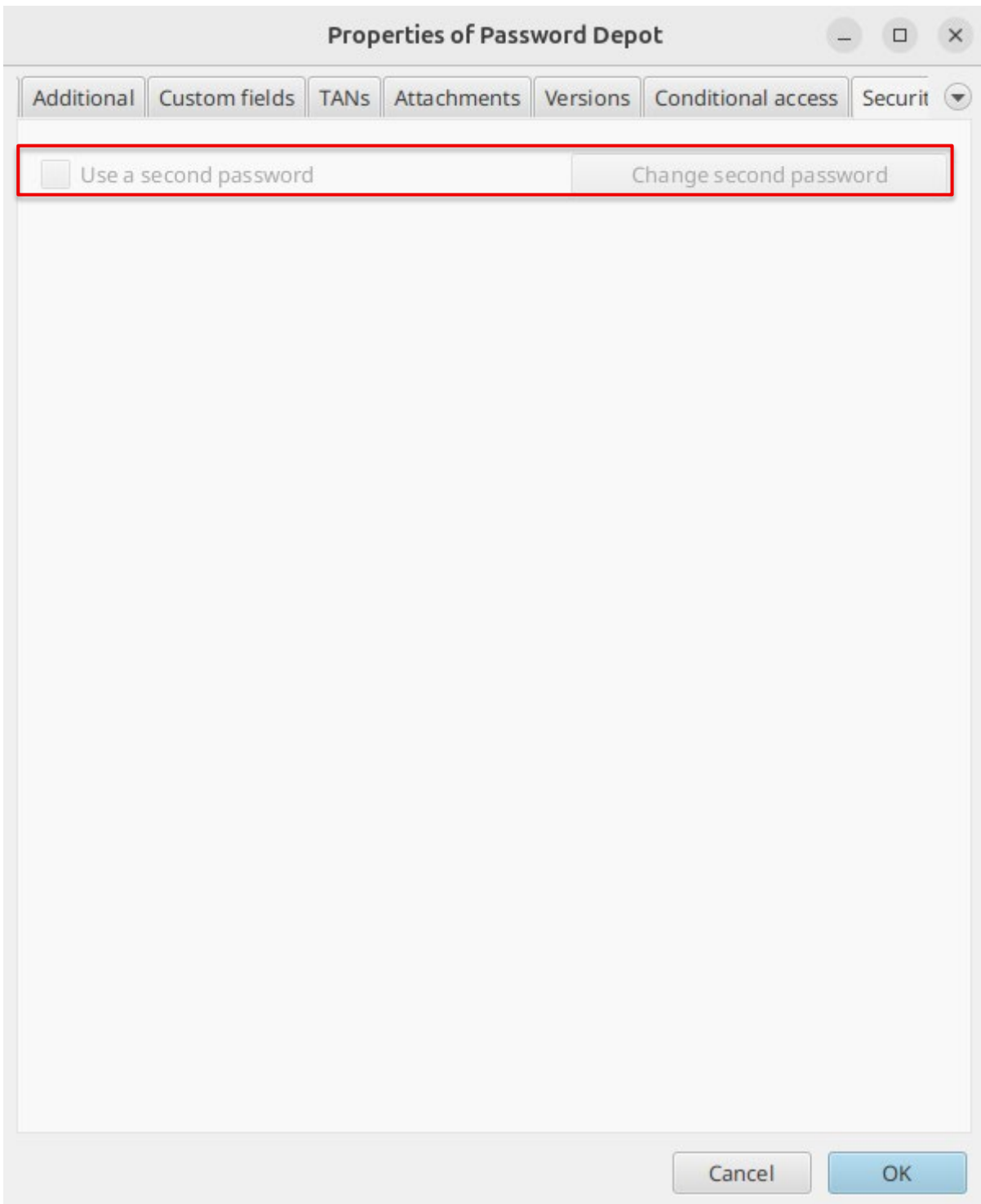
Name	Type	Value
No content in table		

Second password for controlled access

Protect especially sensitive entries with an additional second password (a separate password per entry/folder).

- Open the relevant entry and switch to the **Security** tab.
- Enable the option **Use a second password**.
- Set the second password and save the entry.
- When opening an entry, the second password will now be requested as well.

IMPORTANT: Make sure you also remember the second password. Without it, protected content will remain locked.



Conditional access (warning on access)

Display a warning message when accessing an entry – optionally with a confirmation text.

- Open the entry and switch to the **Conditional access** tab.
- Enable the option **Show the warning message on access**.
- Enter the warning text and select an importance level.
- If **Critical** is selected: also define a confirmation text that you must enter when accessing the entry.

The screenshot shows the 'Properties of Password Depot' dialog box with the 'Conditional access' tab selected. The dialog has a title bar with standard window controls (minimize, maximize, close) and a tabbed interface with tabs for 'Additional', 'Custom fields', 'TANs', 'Attachments', 'Versions', 'Conditional access', and 'Security'. The 'Conditional access' tab is active and contains the following sections:

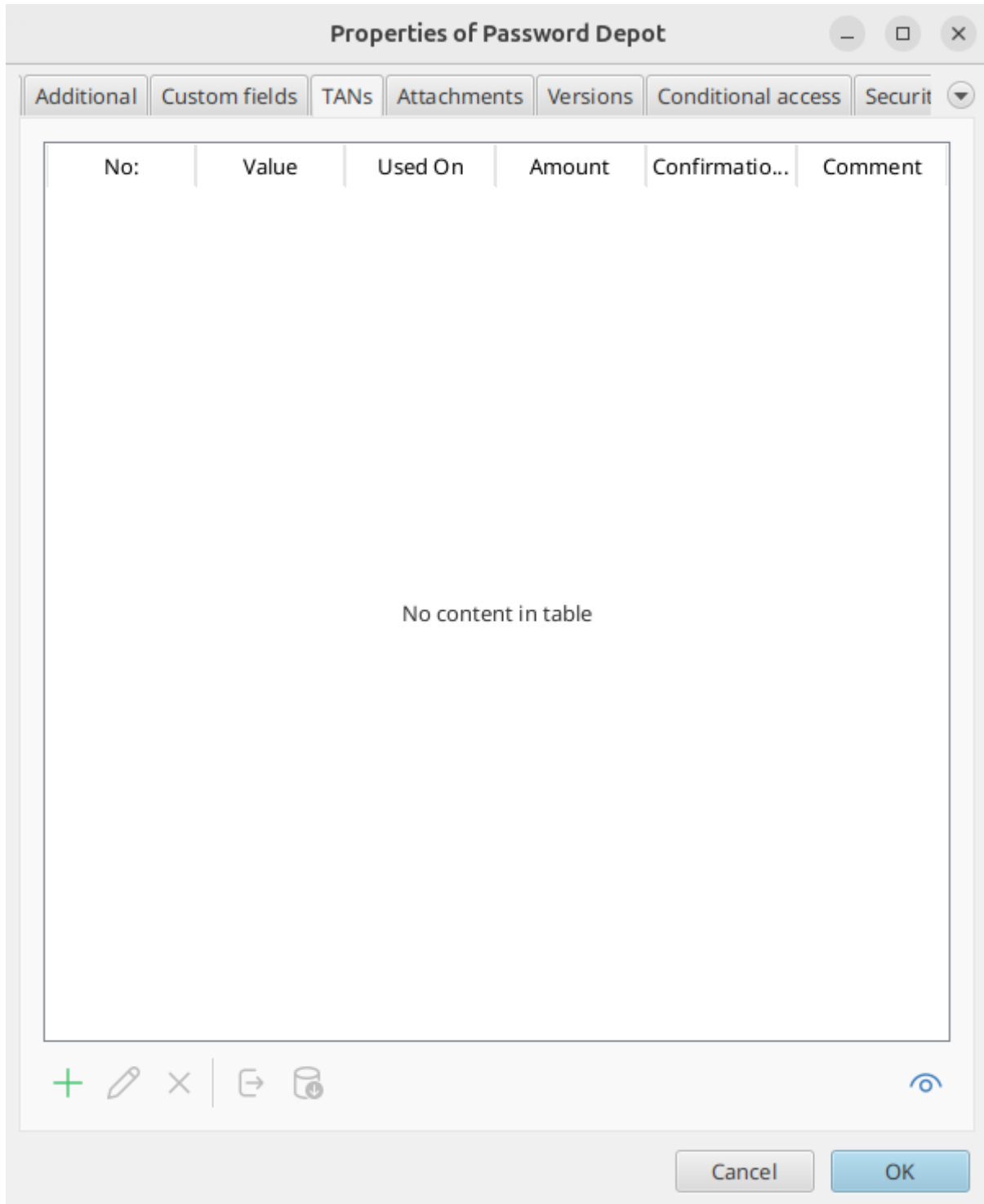
- Warning message**:
 - A checkbox labeled 'Show the warning message on access:' is currently unchecked.
 - Below the checkbox is a large empty text area for entering the warning message.
- Severity level:**
 - Three radio buttons are present:
 - 'Information (popup notification)' is selected.
 - 'Major (modal message box)' is unselected.
 - 'Critical (modal dialog box with the verification text):' is unselected.
 - Below the radio buttons is a text input field for verification text, which is currently empty.
- Limit access to the entry**:
 - A checkbox labeled 'Active connection to Password Depot Server is required' is currently unchecked.

At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

Manage TANs

If you use TANs, you can store them per entry and mark them as "used".

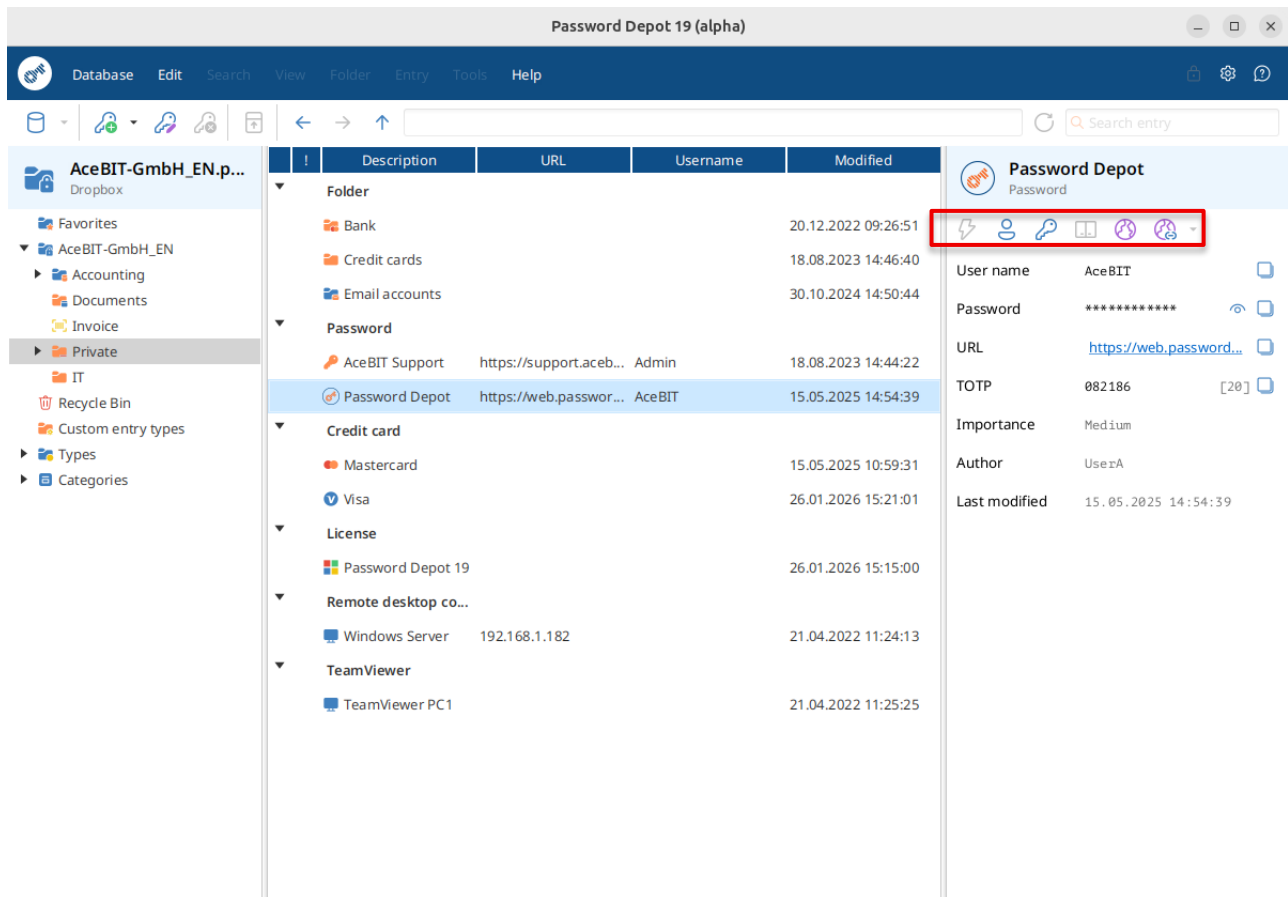
- Open the entry and switch to the **TANs** tab.
- Click the plus icon to add a TAN.
- Edit TANs by double-clicking if necessary.
- Show/hide TAN values as needed (eye icon).



Quick actions in the details view

In the details view on the right, the icons provide various quick actions to transfer important elements directly. Available actions include, among others:

- **Copy username.**
- **Copy password.**
- **Copy URL or Open URL.**



The screenshot displays the Password Depot 19 (alpha) application interface. The main window shows a list of entries with columns for Description, URL, Username, and Modified. The 'Password Depot' entry is selected, and its details are shown in a right-hand pane. A red box highlights the quick action icons in the details view, which include a lightning bolt (copy), a person (copy username), a key (copy password), a link (copy URL), a globe (open URL), and a refresh (refresh).

Description	URL	Username	Modified
Folder			
Bank			20.12.2022 09:26:51
Credit cards			18.08.2023 14:46:40
Email accounts			30.10.2024 14:50:44
Password			
AceBIT Support	https://support.aceb...	Admin	18.08.2023 14:44:22
Password Depot	https://web.passwor...	AceBIT	15.05.2025 14:54:39
Credit card			
Mastercard			15.05.2025 10:59:31
Visa			26.01.2026 15:21:01
License			
Password Depot 19			26.01.2026 15:15:00
Remote desktop co...			
Windows Server	192.168.1.182		21.04.2022 11:24:13
TeamViewer			
TeamViewer PC1			21.04.2022 11:25:25

Password Depot
Password

User name: AceBIT

Password: *****

URL: https://web.password...

TOTP: 082186 [20]

Importance: Medium

Author: UserA

Last modified: 15.05.2025 14:54:39

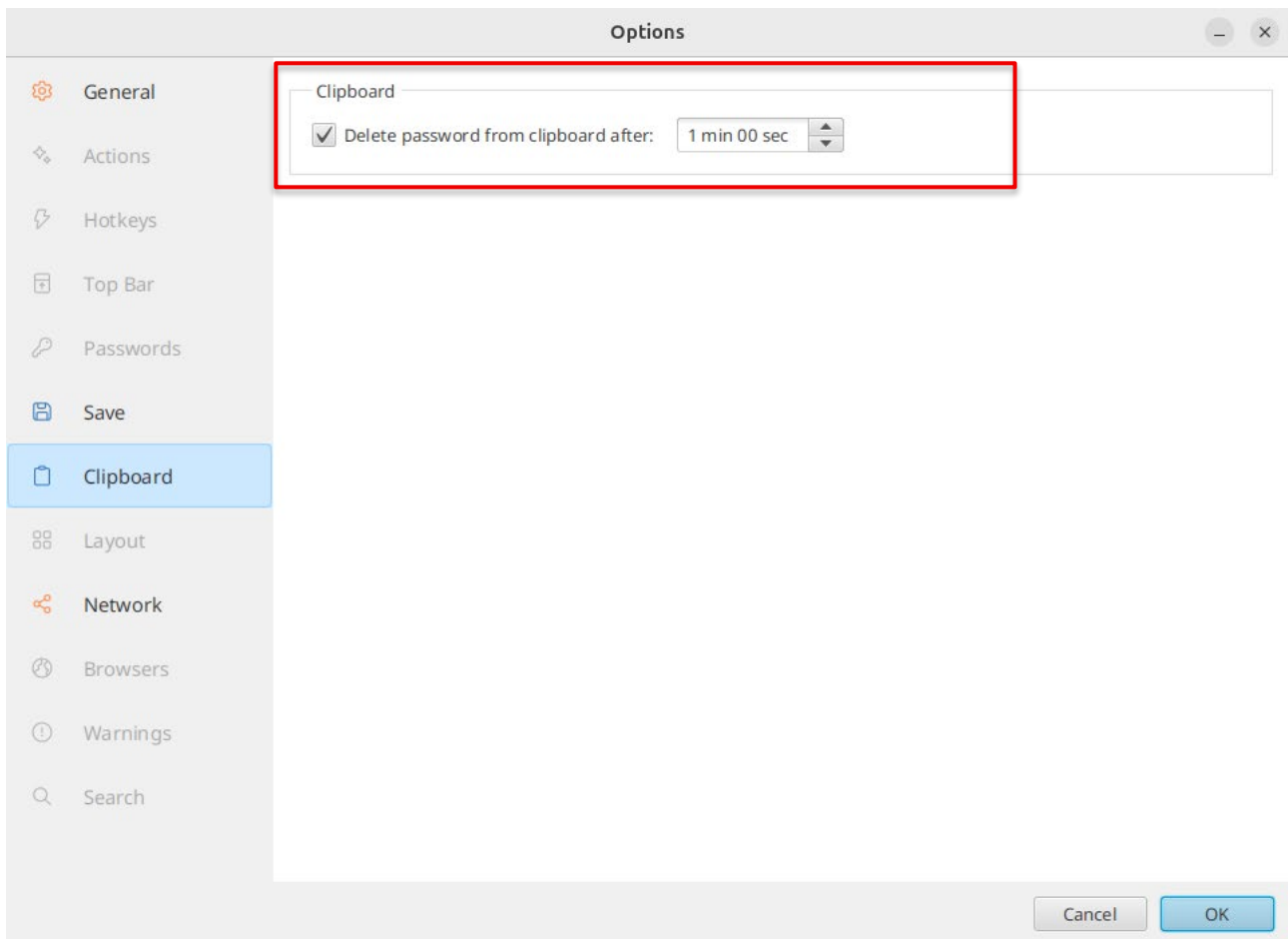
Tips

Work securely

- Choose a long, unique master password and use it only for Password Depot.
- Enable automatic clipboard clearing if you frequently copy passwords.
- Use an expiration date for time-critical passwords and review expired entries regularly.
- Protect important entries with a second password or with conditional access.

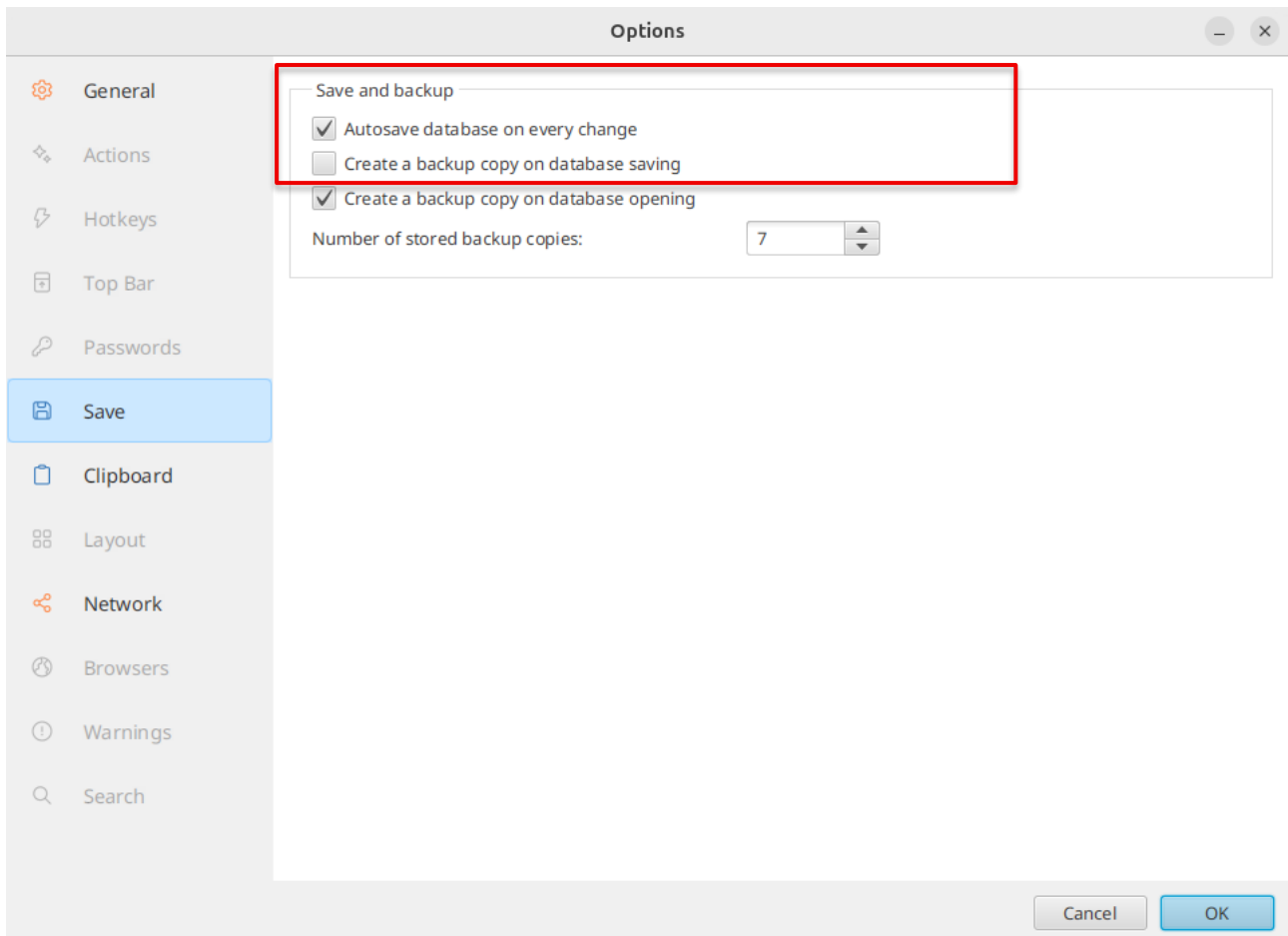
Automatically clear the clipboard

- Open **Edit** → **Options**.
- On the left, select **Clipboard**.
- Enable the option to automatically delete the password from the clipboard and set the desired time.



Auto-save and use backups

- Go to **Edit** → **Options**.
- On the left, select **Save**.
- Enable **Autosave** and Backups on open/save.
- Specify how many backup copies are kept.



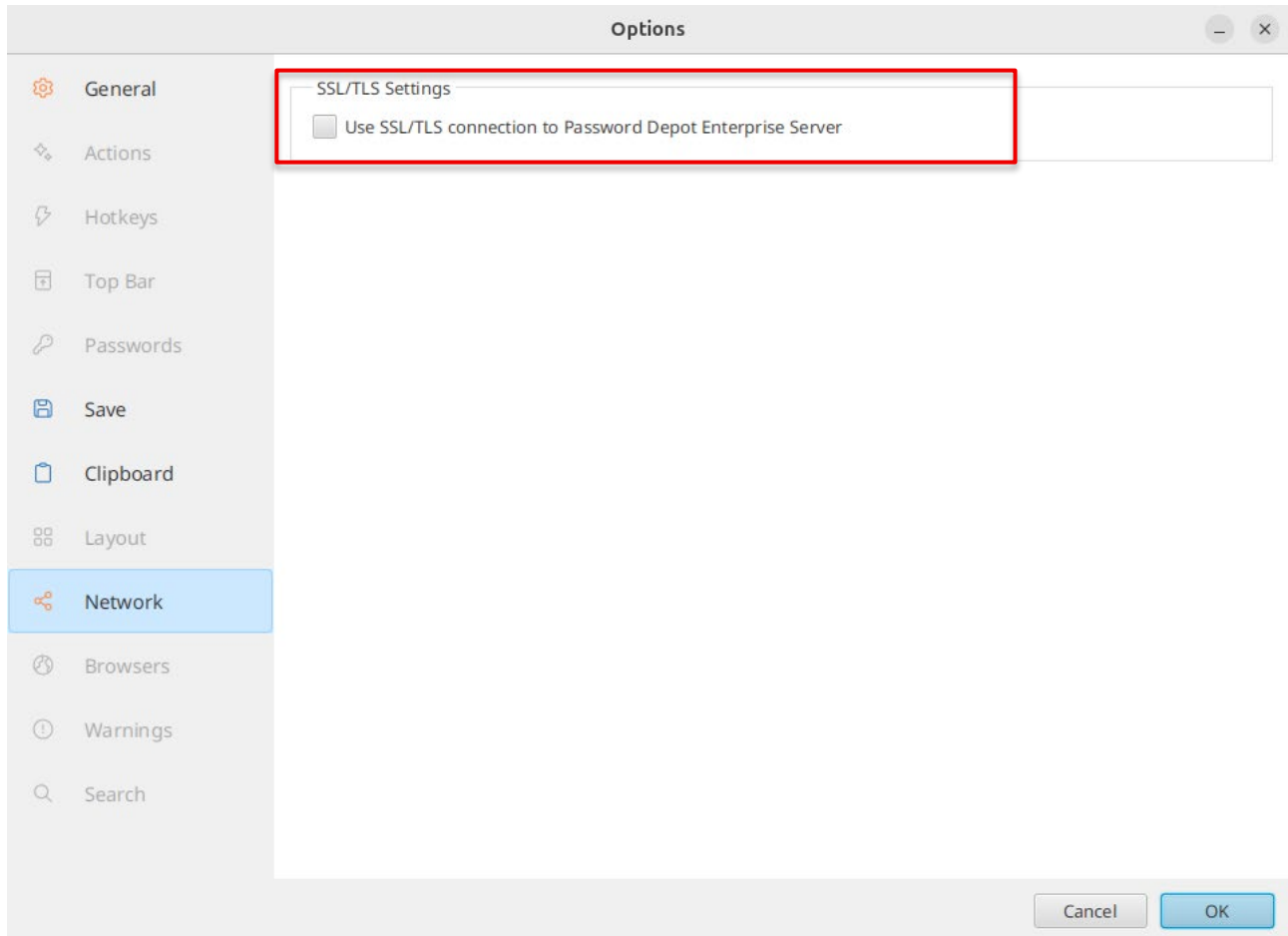
Change language

- Open **Edit** → **Options** → **General**.
- Select the desired language.
- Restart the app so the language is applied fully.

Encrypted connection (SSL/TLS) for Enterprise Server

If you use the Password Depot Enterprise Server, you can enable an encrypted connection (SSL/TLS).

- Go to **Edit** → **Options** → **Network**.
- Enable **Use SSL/TLS connection to the Password Depot Enterprise Server**.



If something does not work

- Wrong master password/key file: Check upper/lower case and select the correct key file.
- Reference entry not found: The linked entry was deleted or moved. Open the original entry or correct the link.
- Entry requires a server connection: Open the database via **Enterprise Server** and ensure there is an active connection.

Help and support

Please note that the Password Depot client for Linux is an early version and not all features are available yet.

If you need further assistance, choose **Help** → **Support**. There you will find answers to frequently asked questions and you can also contact us directly using the provided forms.