Password Depot for macOS

Quick Start Guide – macOS

As of: January 26, 2026

This guide shows the most important steps to use Password Depot on macOS securely—without any technical prior knowledge.

Table of Contents

Table of Contents 2

Introduction 4

How the app is structured 4

Key terms 5

Getting started 6

Database Manager 6

Create a new database 7

Open an existing database 8

Preferences 9

Core functions 11

Create folders 11

Create, edit and organize entries 12

Favorites and Recycle Bin 13

Create secure passwords: Password Generator 14

Use credentials: Copy, open URL, auto-complete 14

Customize the auto-complete sequence (auto-fill) 16

Store and copy a 2FA code 17

Versions 18

Browser add-ons: Fill web forms 20

Install add-ons (Chrome/Firefox/Edge) 20

Enable add-ons in Password Depot 21

Use add-ons in the browser 22

Manage ignored websites 24

Search, Filter and Replace 25

Import and Export (XML) 26

Analysis, duplicates and cleanup 28

Analyze 28

Search for duplicates 29

Clean-up 30

Backups and restore 31

Database properties 32

Lock and unlock the database 33

Storage locations and synchronization 34
Cloud storage 34
Enterprise Server (company) 35
Offline Mode 36
Share and seal entries (if available) 37
Tips 38
Work securely 38
Organize the database 38
Create a partial password 38
Solve common problems 39
Help and Support 39

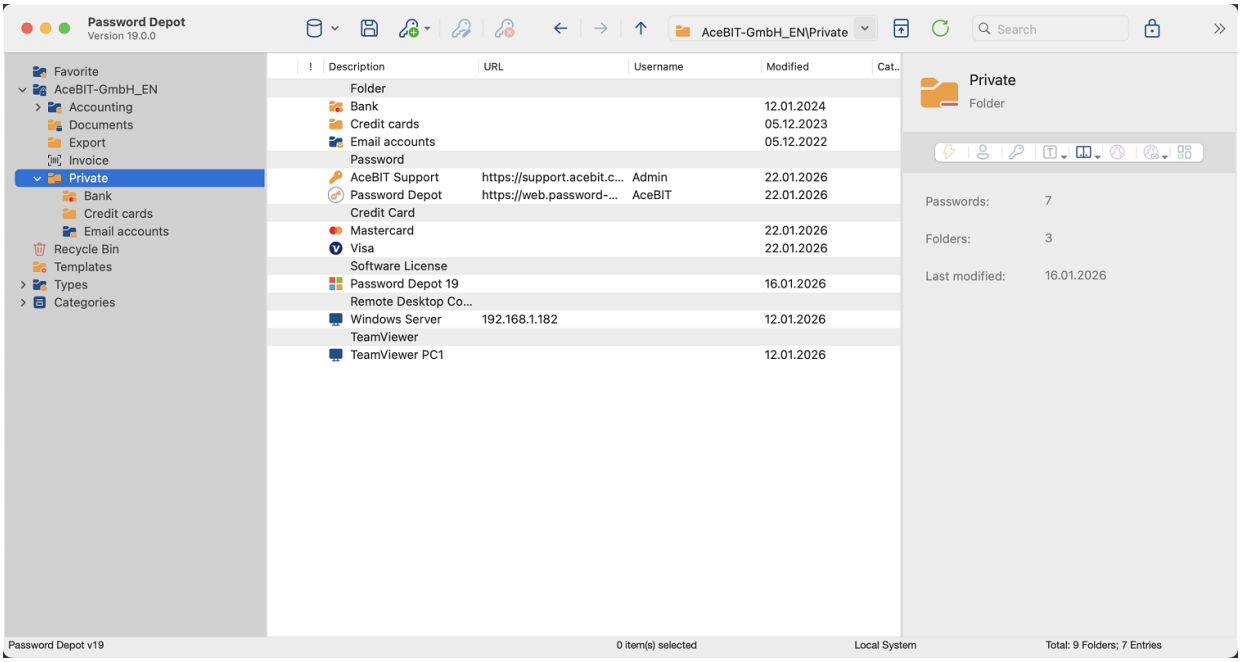
Introduction

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.

How the app is structured

- **Navigation panel on the left**: folders, favorites, recycle bin and (optionally) templates.
- **List in the middle**: entries in the currently selected folder.
- **Details panel on the right**: contents and quick actions (e.g., copy username/password, open URL, auto-complete).



Key terms

- **Database**: Your encrypted file with all entries (e.g., "Private.pswe").
- **Master password**: The primary password used to open the database.
- **Key file**: An additional file used as a second factor to open the database (2FA = two-factor authentication).
- **Entry**: A stored item, e.g., password, credit card or identity.
- **Folder**: Allows you to group entries (e.g., "Work", "Private").
- **Favorites**: Quick access to frequently used entries.
- **TOTP**: A time-based one-time code for 2FA logins.

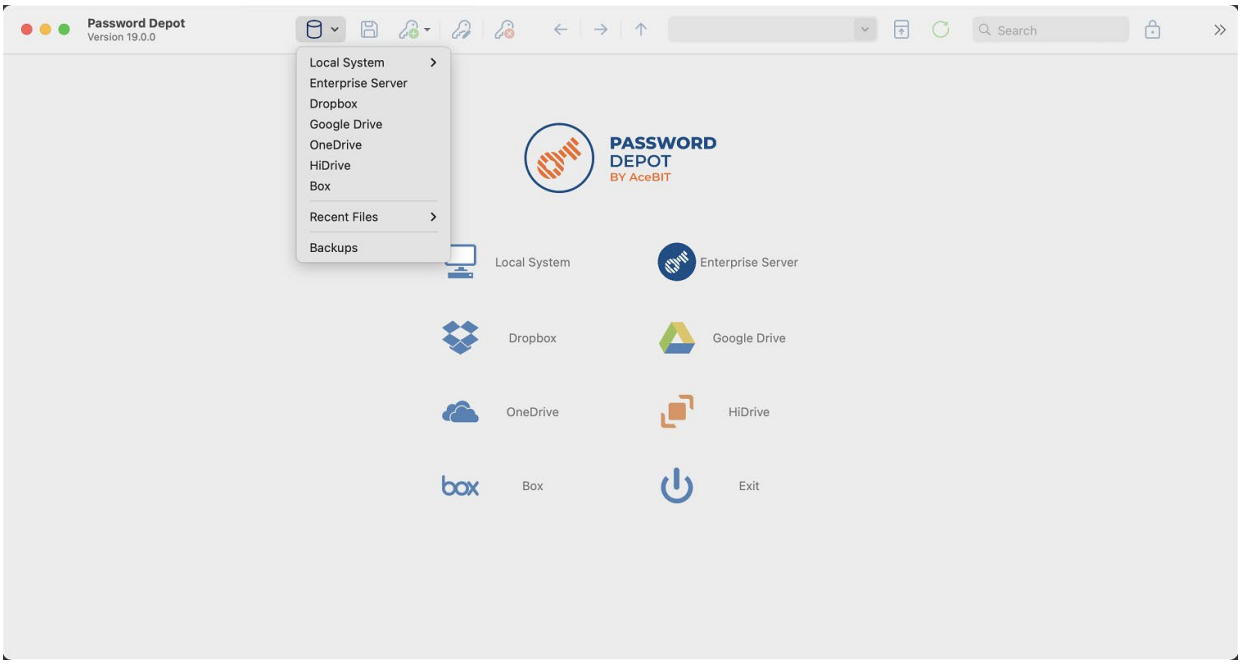
Getting started

Database Manager

The **Database Manager** is the central administration area of Password Depot for macOS and provides an overview of available storage locations and databases. Open it via **Database** → **Database Manager**.

The following options are available:

- **Local system** – databases stored on your device.
- **Dropbox / Google Drive / OneDrive / HiDrive / Box** – databases in the selected cloud.
- **Enterprise Server** – if your company uses Password Depot, databases can be stored centrally on the Enterprise Server. From there you can access databases shared with you.
- **Exit** – exits Password Depot.

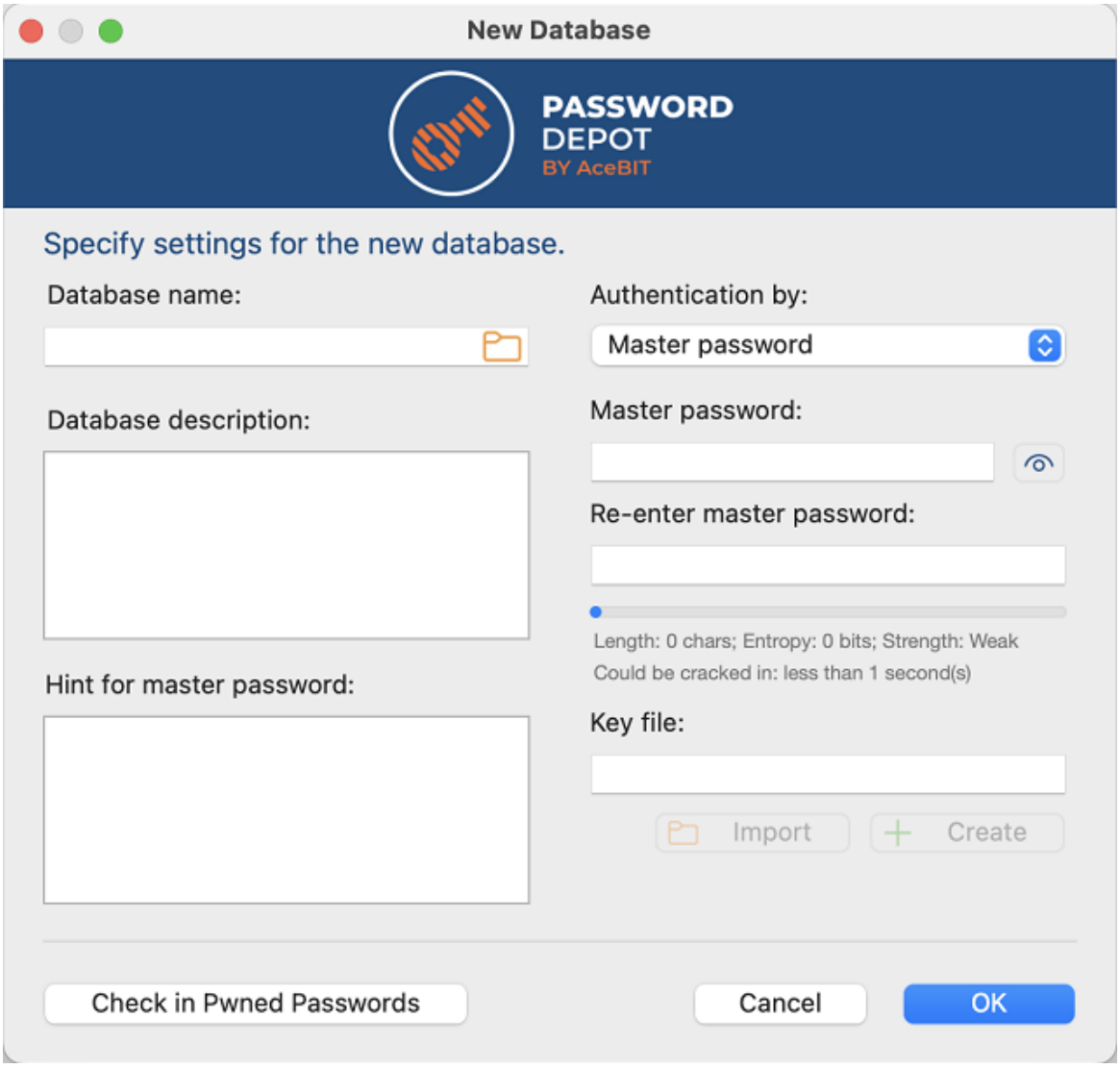


Create a new database

To create a new database, proceed as follows:

- In the **Database Manager**, select the desired storage location, e.g., Local system.
- Select **Create new database**. (If you use a cloud service, you must connect to it first.)
- Enter a name for the database and select the authentication method: **master password**, **master password and key file**, or **key file** only. For higher security, store key files separately from the database (e.g., on a USB stick).
- Set a strong master password and confirm it.
- Click **OK** to create the database.

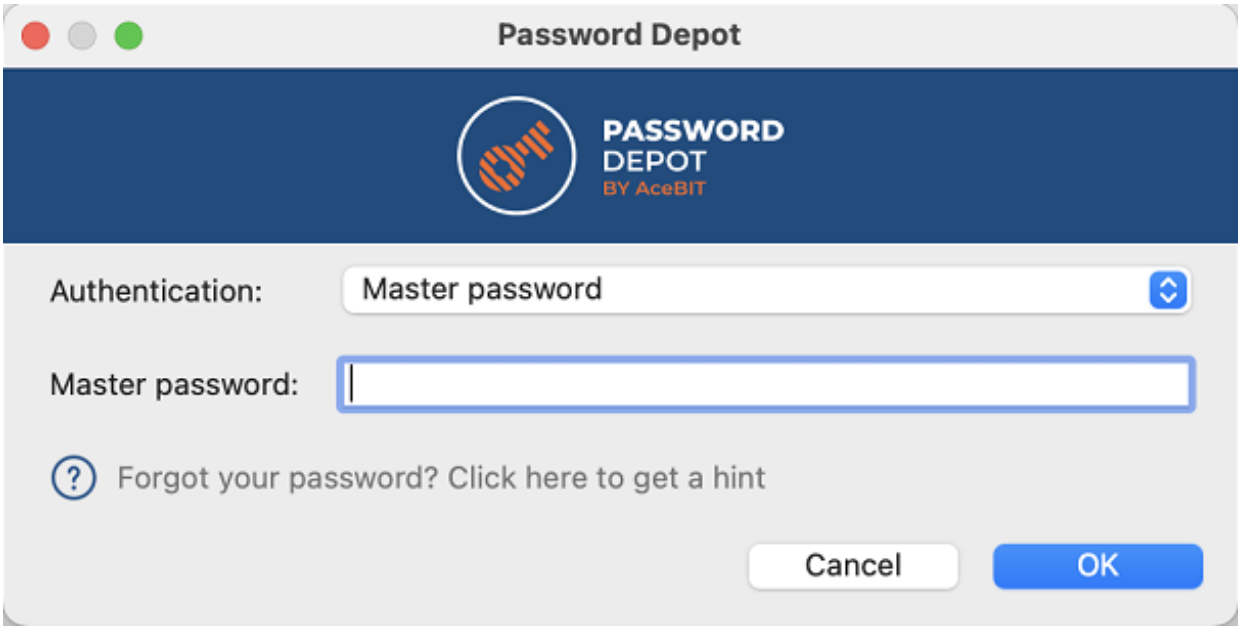
IMPORTANT: Choose a strong master password. Ideally it should be at least 12 characters long and used only once. If needed, use the **Check in Pwned Passwords** button. This allows you to automatically check whether your chosen password appears in known data leaks.



Open an existing database

To open an existing database, use the **Database Manager** again.

- Select the storage location where the database you want to open is stored.
- Select the desired database from the list of displayed databases.
- Authenticate by entering the master password and/or selecting the key file.
- If **Open last used database at program start** is enabled in **Preferences**, the database you last used will automatically be offered for opening when Password Depot starts.

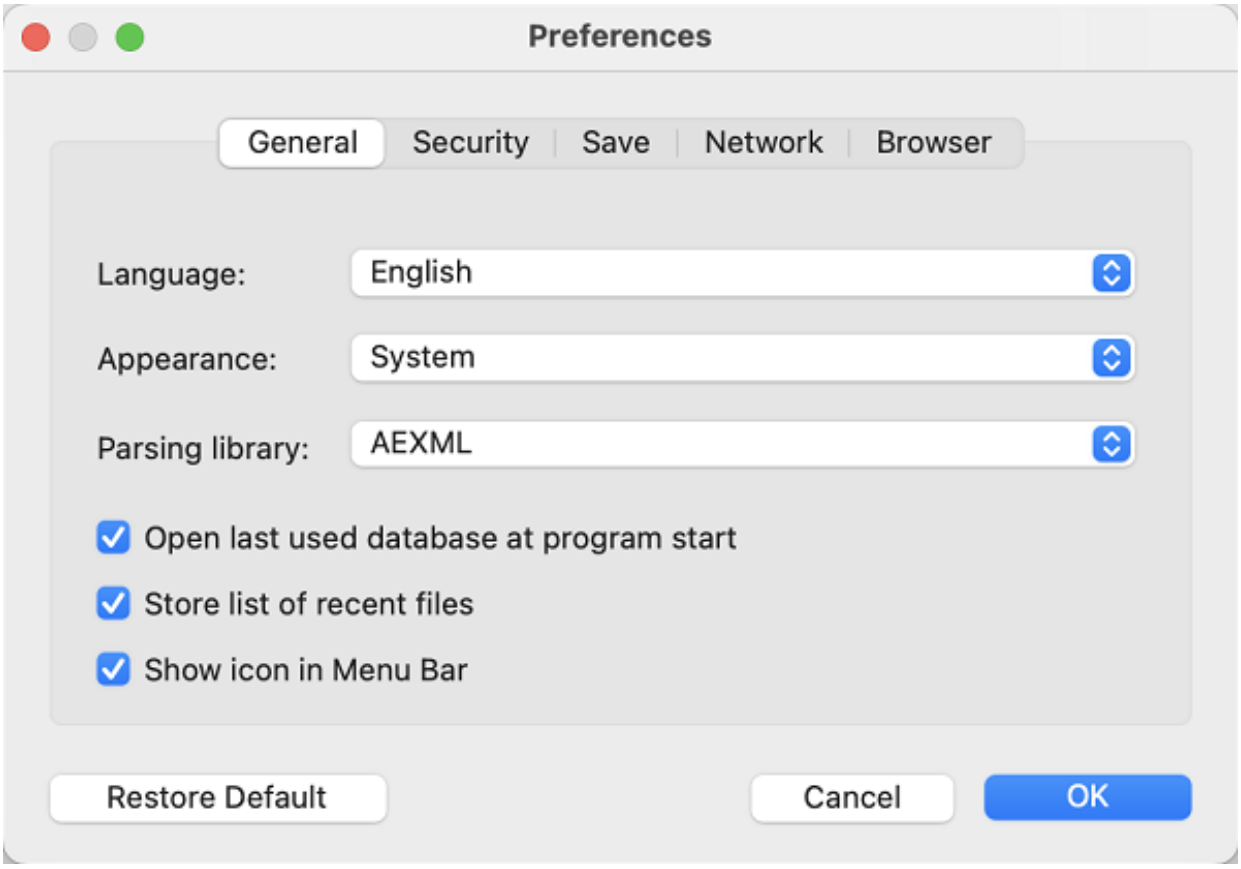


Preferences

- Open the **Preferences** via the gear icon on the right side of the top bar. Various configuration options are available.

General

- **Language**: Select the application language. By default, German, English, Spanish, Dutch and French are available.
- **Appearance**: Choose between System, Light and Dark mode.
- **Parsing library**: Change the XML library used. This can help if you experience memory issues. Options: Fuzi and AEXML.
- **Open last used database at program start**: If enabled, the database you last used is automatically selected at startup.
- **Store list of recent files**: Saves recently used databases and shows them for quick selection.
- **Show icon in Menu Bar**: Choose whether to show the icon in the macOS menu bar.



Security

- **Clear password from clipboard after**: Enable automatic clipboard clearing after a set time. Recommended: a short value such as 30-60 seconds.

IMPORTANT: Only copy passwords when you will paste them immediately. Avoid unnecessary clipboard usage.

- **Auto-lock after program inactivity**: Your database is locked automatically after the configured time if the program is inactive. For security, use a short value such as 3–5 minutes.

Save

- **Automatically save database after every change**: If enabled, the database is saved after every change.
- **Create backup file when saving a database**: Creates a backup file each time the database is saved.
- **Create backup file when opening a database**: Creates a backup file each time the database is opened.
- **Number of saved backup files**: Define how many backup files are kept.
- **Remote database: Automatically delete local copy when closing**: Locally created copies of remote databases are deleted after closing the database.
- **Database from Enterprise Server: Save local copy**: Enable this option for Enterprise Server offline mode.

Network

- **Use SSL/TLS connection to Password Depot Enterprise Server 17**: Only relevant for Enterprise Server users of version 17.

Browser

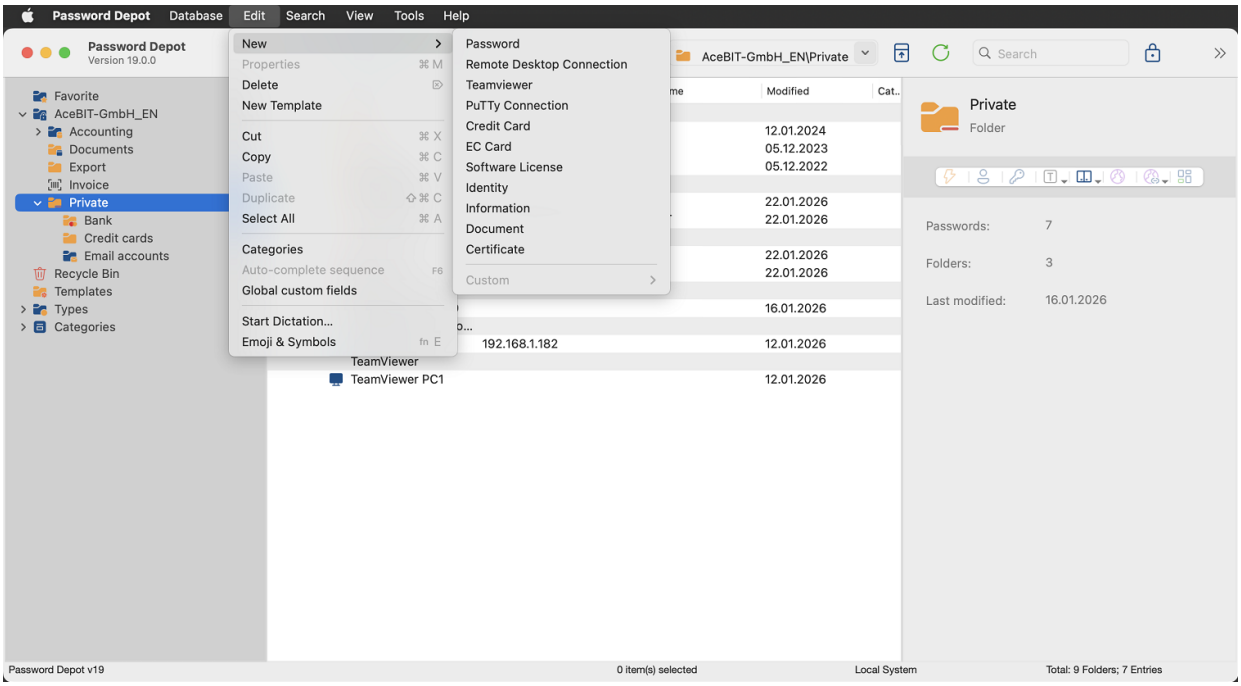
- **Auto-fill web forms using add-ons**: If enabled, you can use add-ons to auto-fill your login data.
- **Add new passwords from web browsers:** If enabled, a corresponding entry is created automatically when you enter new login data that does not yet exist.
- **Protect access with a password**: For higher security, you can additionally protect access with a password.

Core functions

Create folders

Folders help you structure your entries and keep everything organized. To create a folder:

- Open the database you want to work with.
- Create a folder in the navigation panel. Choose a suitable name (e.g., "Private" or "Work").

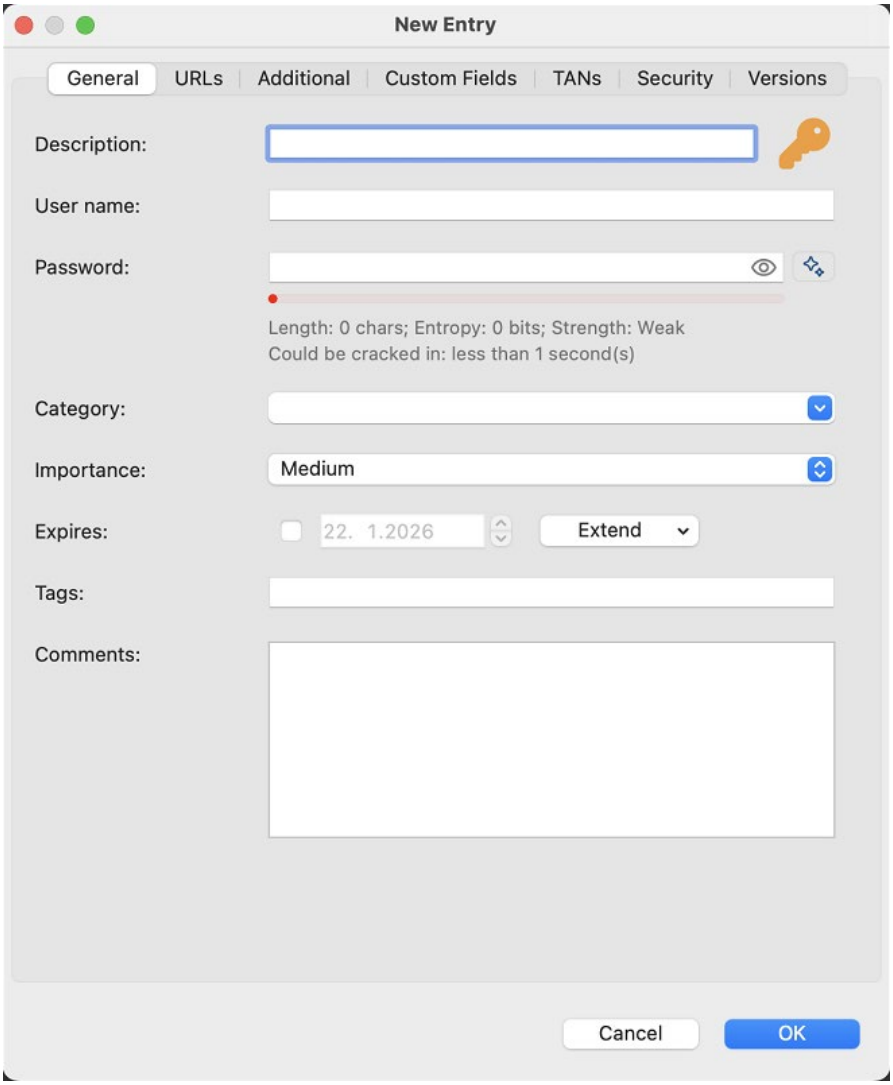


Create, edit and organize entries

Entries are your stored information - e.g., passwords, website logins, credit cards or licenses.

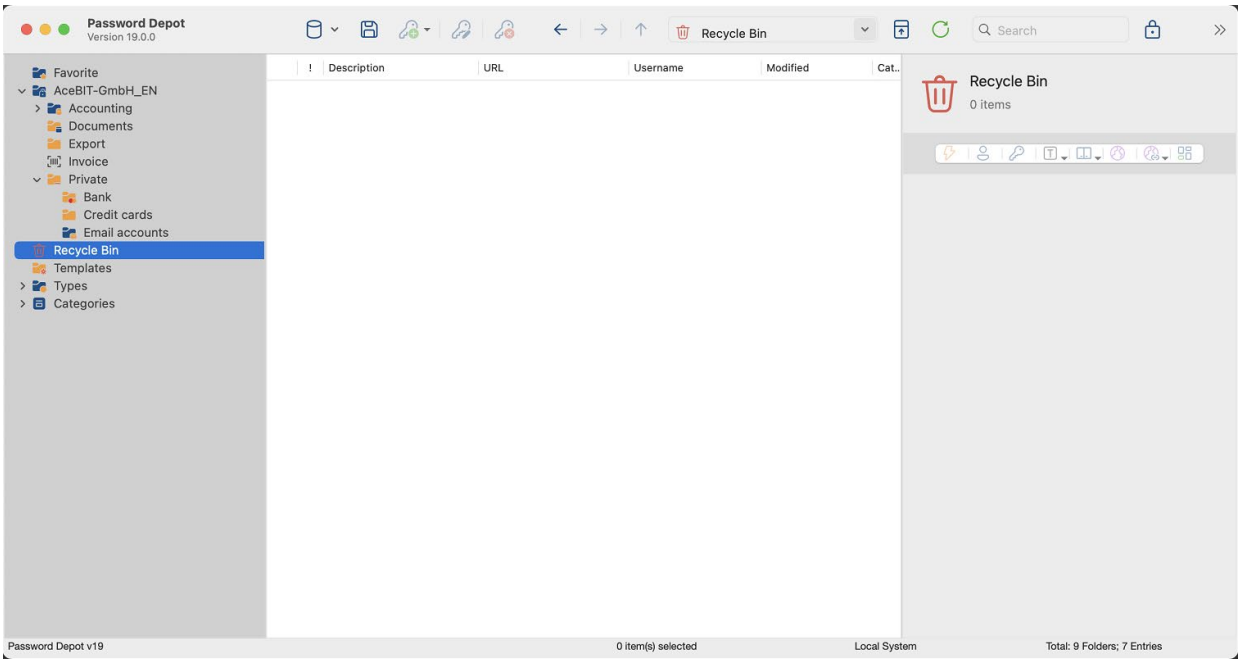
To create a new entry:

- Select **Create new password** (key icon with a white plus on a green background) or choose **Edit** → **New** and select the desired entry type. In addition to the default entry type **Password**, the following entry types are available: **Remote Desktop connection**, **TeamViewer**, **PuTTY connection, Credit card**, **Debit card**, **Software license, Identity**, **Information**, **Document**, **Certificate**, and **Custom**.
- Fill in at least the **Description**. Depending on the entry type, you can add user name, password, URL and other fields.
- For faster retrieval, assign the entry to a category and add tags.
- Click **OK** to create the entry. To edit an existing entry or add information later, double-click it or select **Edit selected entry** (key icon with a pen) in the top bar. Alternatively, right-click the entry and select **Properties**.
- You can mark important entries as favorites (star icon).



Favorites and Recycle Bin

- Select **Favorites** in the left panel to display entries you marked with a star. This helps you find important entries faster.
- **Recycle Bin**: Deleted entries are moved to the recycle bin (depending on the database setting) and may be restored.

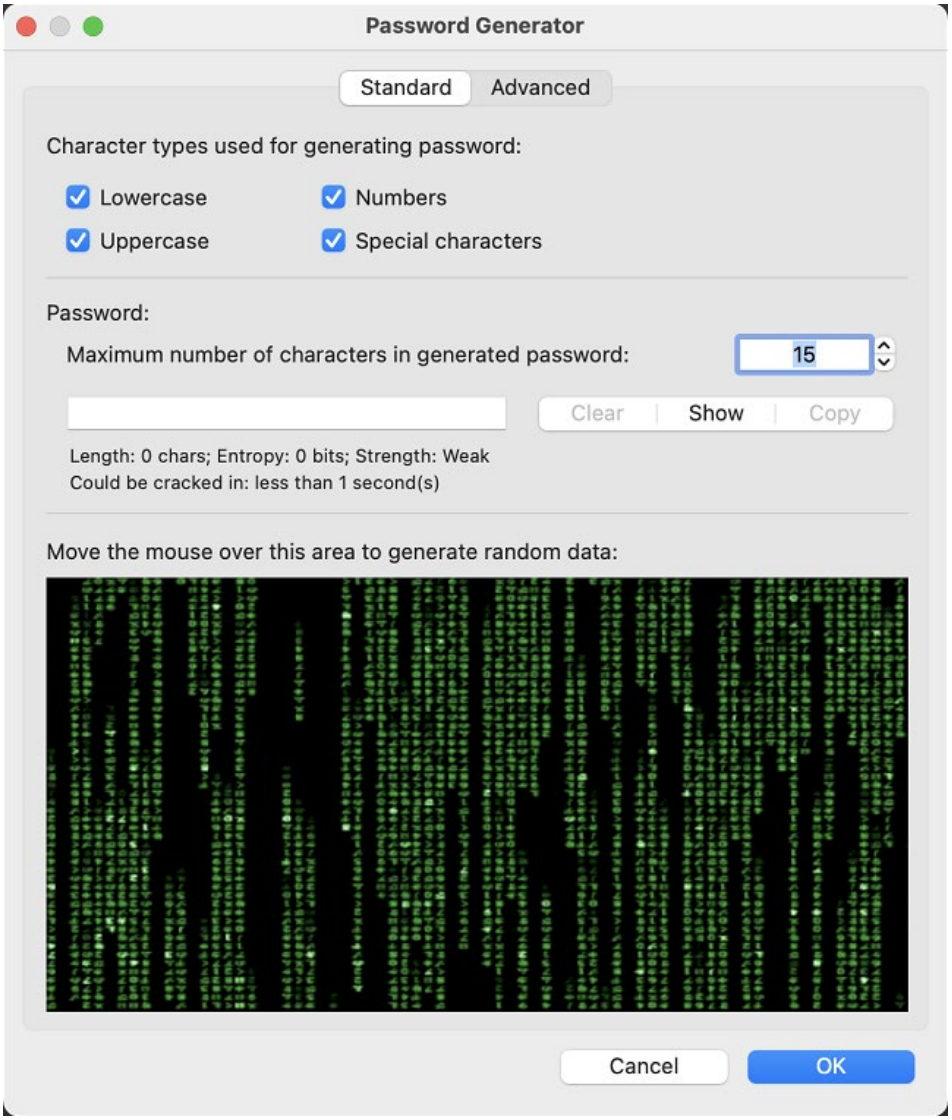


Create secure passwords: Password Generator

Instead of creating passwords yourself, you can use the **Password Generator**, which automatically creates secure passwords.

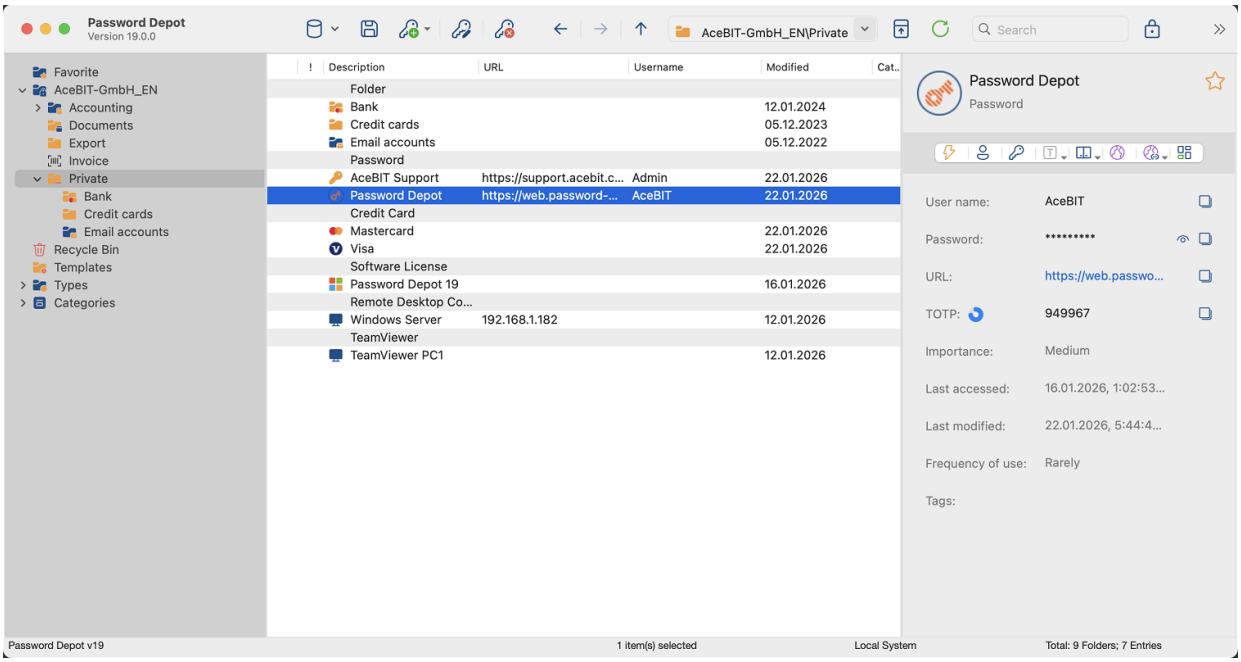
- Open an entry by double-clicking it or selecting **Edit selected entry** (key icon with a pen) in the top bar. Alternatively, right-click the entry and select **Properties**.
- Click the star icon to the right of the Password field to open the **Password Generator**.
- Choose between **Standard** and **Advanced** and set rules the generated password must meet (e.g., length or character types).
- Move the mouse over the field to generate a random password.
- Click **OK** to save the password. It will be adopted automatically.

TIP: Use a separate random password per account, created via the generator.



Use credentials: Copy, open URL, auto-complete

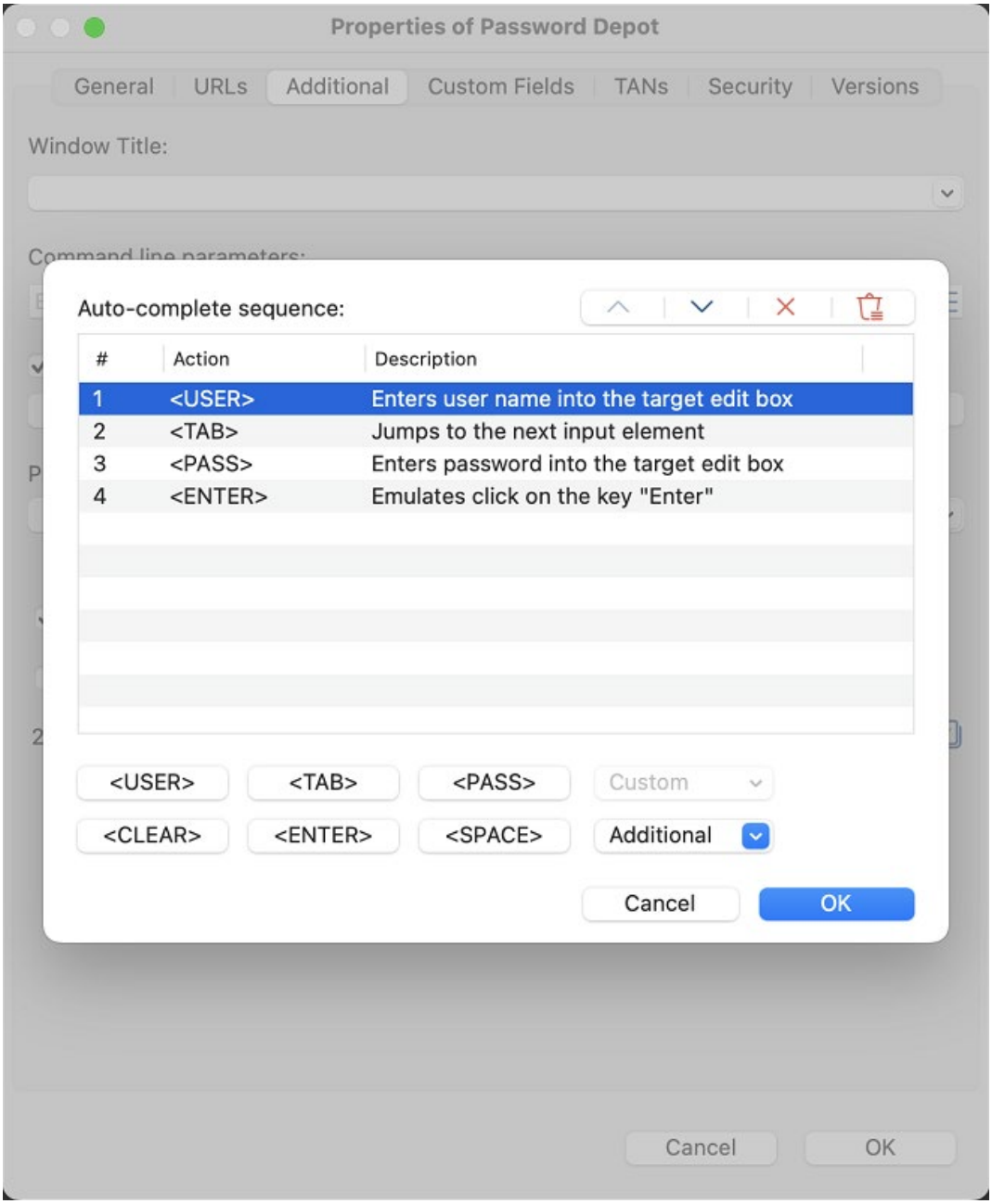
- **Copy:** In the details panel, use the functions to copy username and password. Clicking the respective icons copies them to your clipboard.
- **Open URL**: If a URL is stored for an entry, you can open it directly in your default browser or another browser.
- Using the lightning icon in the details panel on the right, you can enab**le Auto-Complete** for an entry. You can then automatically fill username, password and, if applicable, additional elements.



Customize the auto-complete sequence (auto-fill)

In an entry's properties, besides the **General** tab (and depending on the entry type), additional tabs are available to store more information or define advanced settings. To customize the auto-complete sequence, select the **Additional** tab in the entry properties. Customizing can be helpful if you want to extend your sequence or if you experience problems with auto-fill.

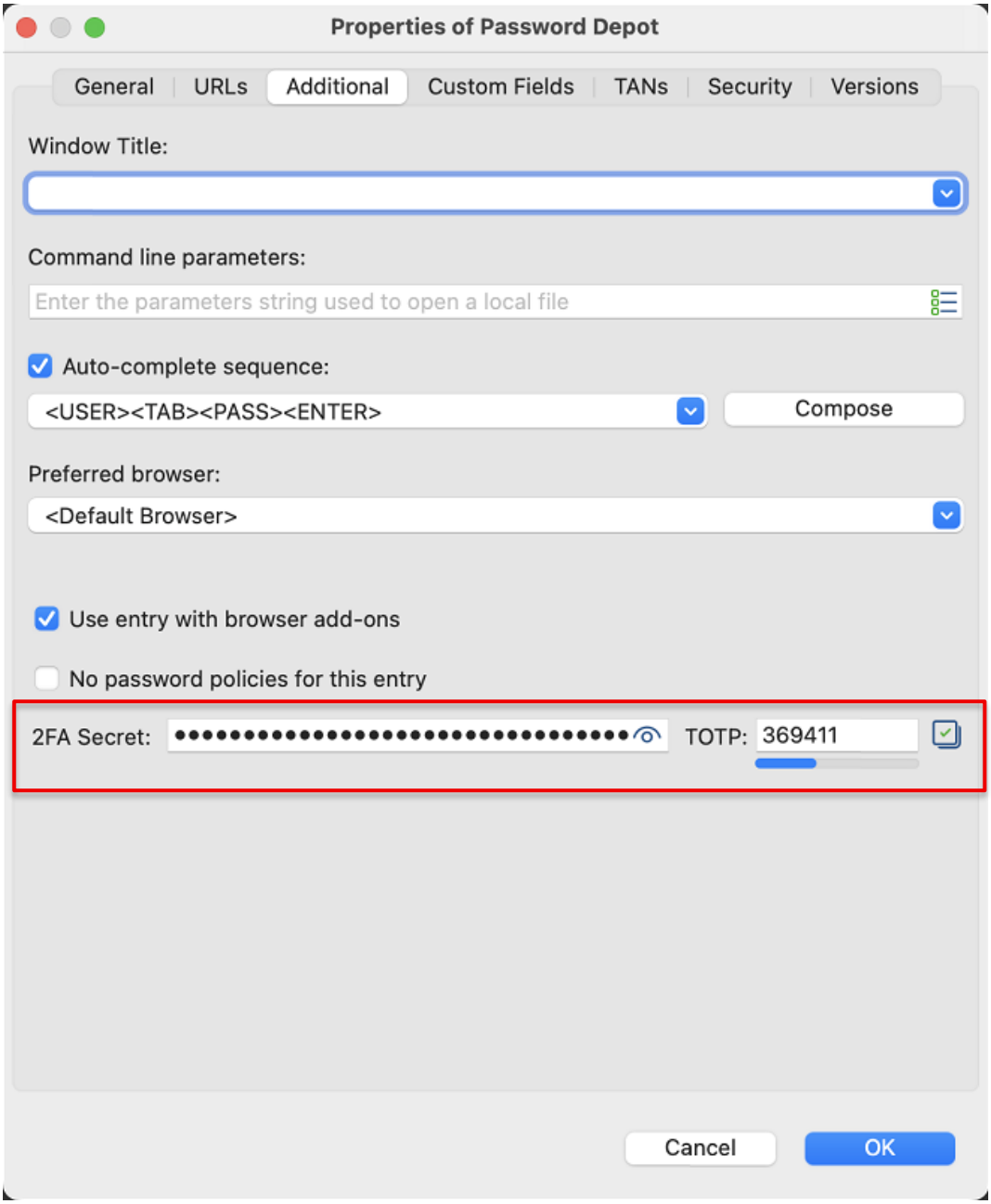
- Enable **Auto-complete sequence**.
- Edit the sequence if necessary via the **Compose** button.
- Assemble the sequence building blocks as desired (e.g., <USER><TAB><PASS><ENTER>).



Store and copy a 2FA code

Many services use a one-time code (TOTP) in addition to the password**.** Password Depot supports these codes.

- Open the desired entry for editing.
- Select the **Additional** tab.
- Enter the corresponding key under **2FA Secret**. Password Depot will automatically generate a TOTP from it.
- Copy the TOTP using **Copy to clipboard** to paste it into the corresponding field.



Versions

If version history is enabled, you can record changes to an entry and review earlier states.

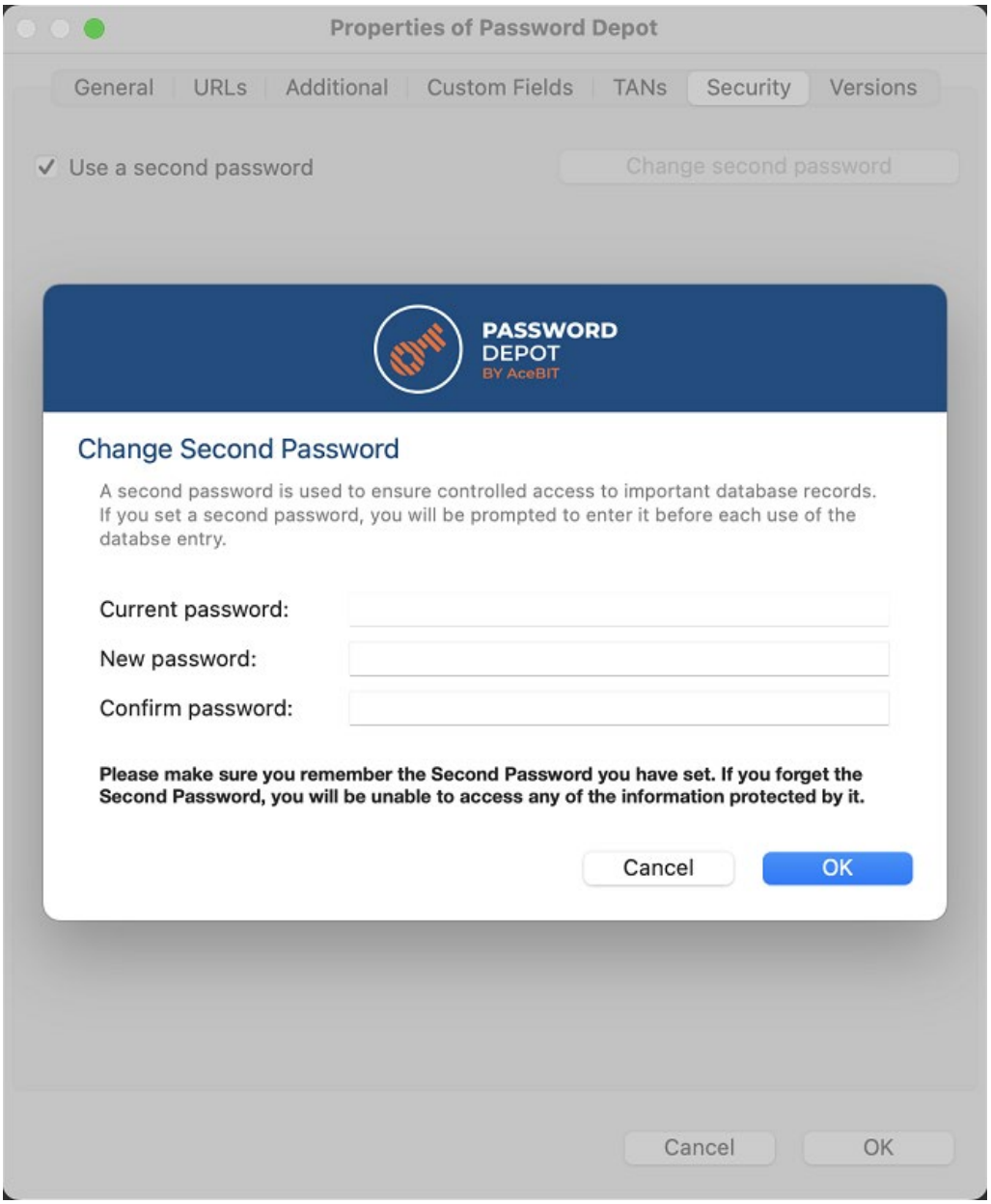
- Open an entry for editing and select the Versions tab.
- In the bottom-right under Versions, configure the desired settings. Available options: **Keep no versions**, **Keep versions**, and **Use global settings**.

Set a second password

A second password protects particularly sensitive areas. When accessing them, you must enter this second password in addition to the master password.

- Open an entry for editing and select the **Security** tab.
- Enable **Use a second password**.
- Choose a secure second password and enter it.

IMPORTANT: Make sure you reliably remember the second password as well. Without it, protected contents remain locked.



Browser add-ons: Fill web forms

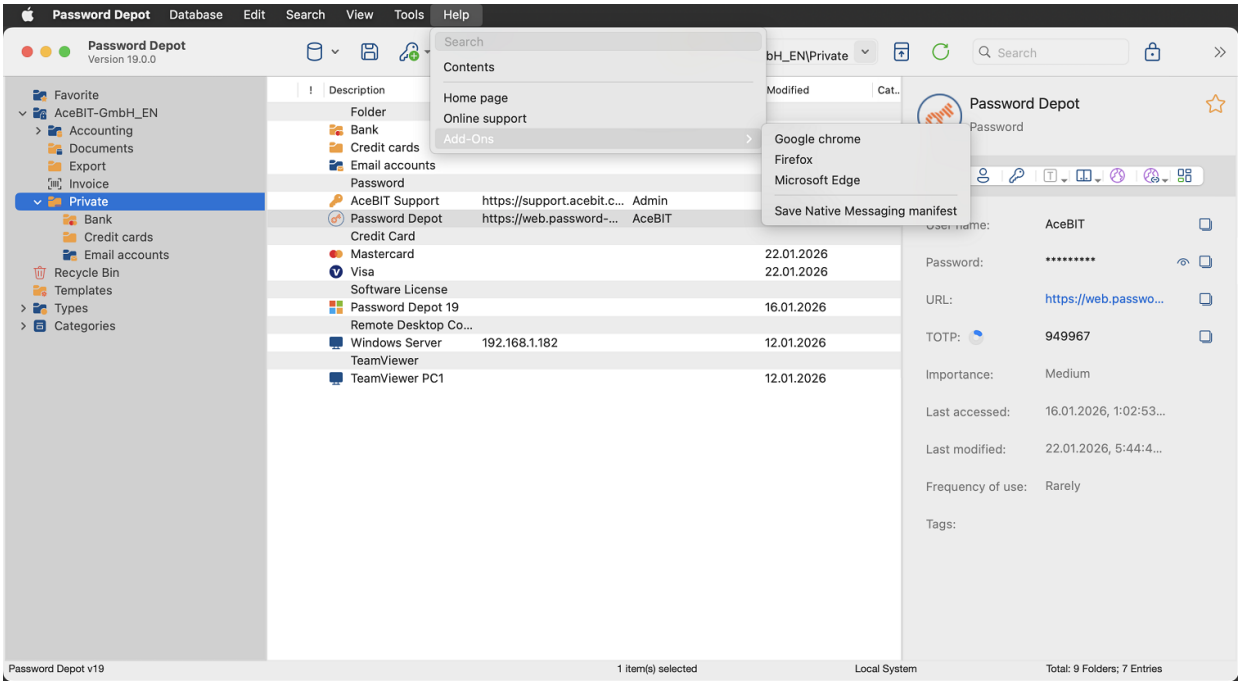
With Password Depot add-ons (browser extensions), logins can be detected directly in the browser, filled, and new entries can be created.

Install add-ons (Chrome/Firefox/Edge)

- Open **Help** → **Add-Ons** and select the desired browser (Google Chrome, Firefox or Microsoft Edge).
- If the add-on requires a connection to the app, select **Help** → **Add-Ons** → **Save Native Messaging manifest**.
- Select the browser, accept the suggested extension ID and save the file to the suggested folder.

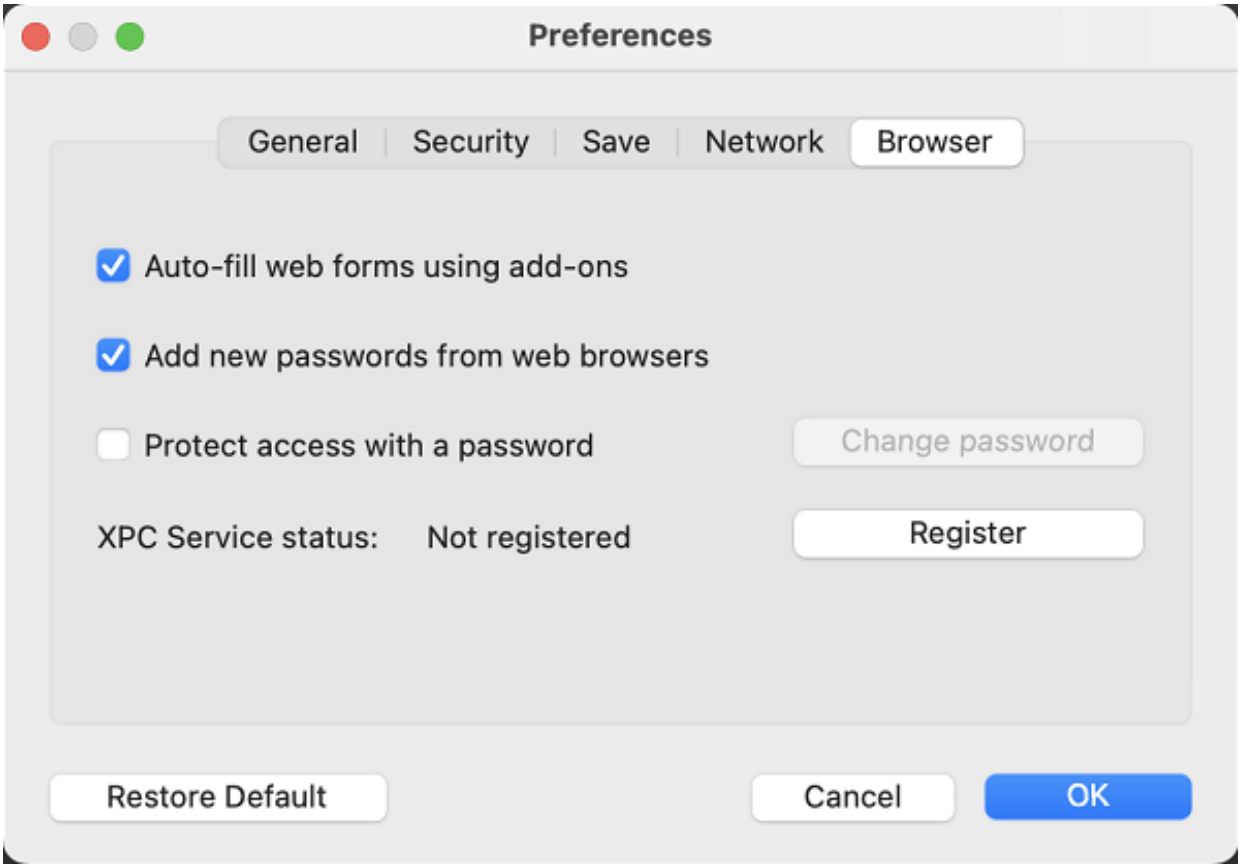
Then restart the browser.

- The restart the browser.



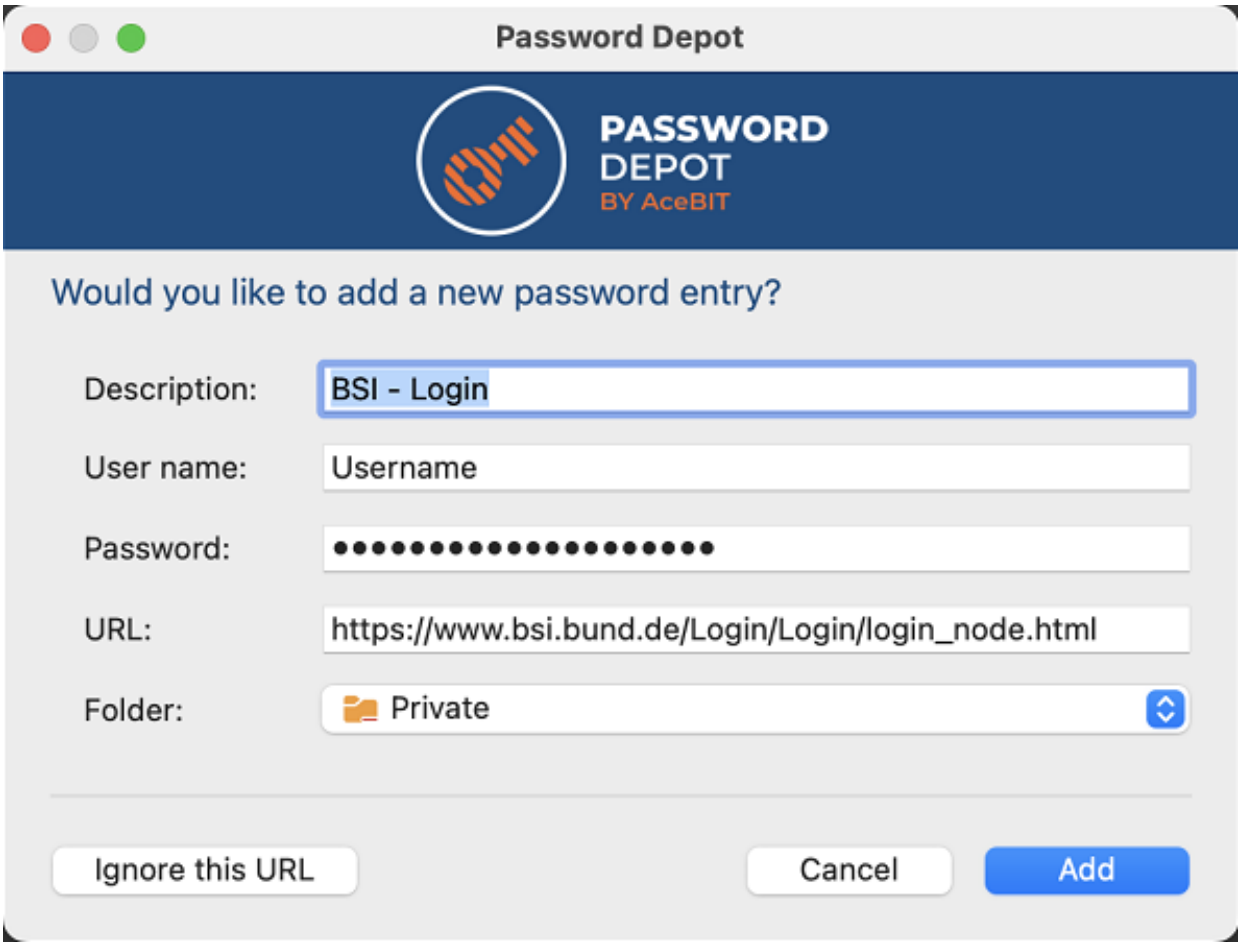
Enable add-ons in Password Depot

- Open **Preferences**.
- Select the **Browser** tab.
- Enable **Auto-fill web forms using add-ons**. This allows the add-on to auto-fill entries in the browser.
- If **Add new passwords from web browsers** is enabled, Password Depot can automatically create entries for login data that does not yet exist.
- Optionally enable **Protect access with a password**. This is recommended in shared environments.

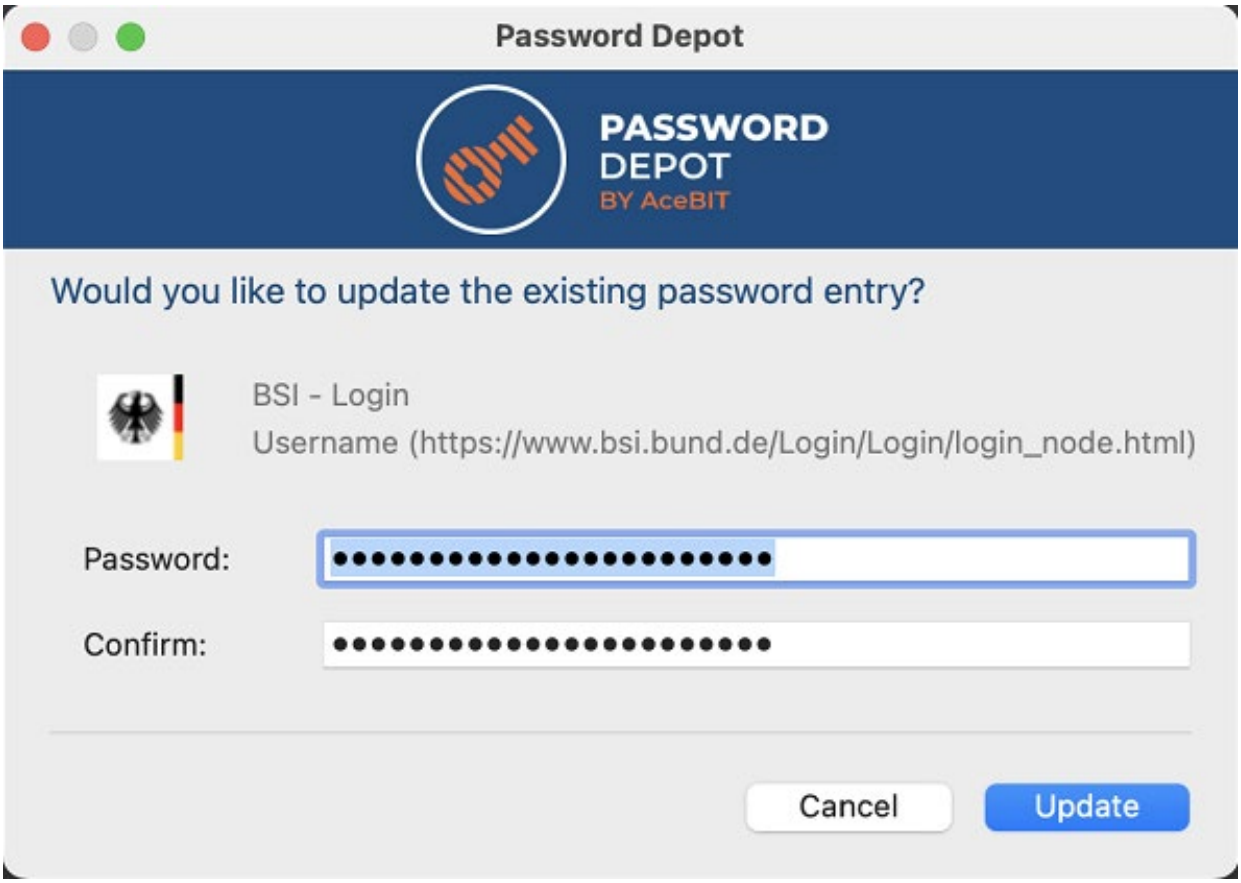


Use add-ons in the browser

- **Auto-fill**: Select the matching entry in the add-on so that the corresponding field is filled.
- If no entry exists yet, Password Depot can offer to create one automatically (see **Enable add-ons in Password Depot**).



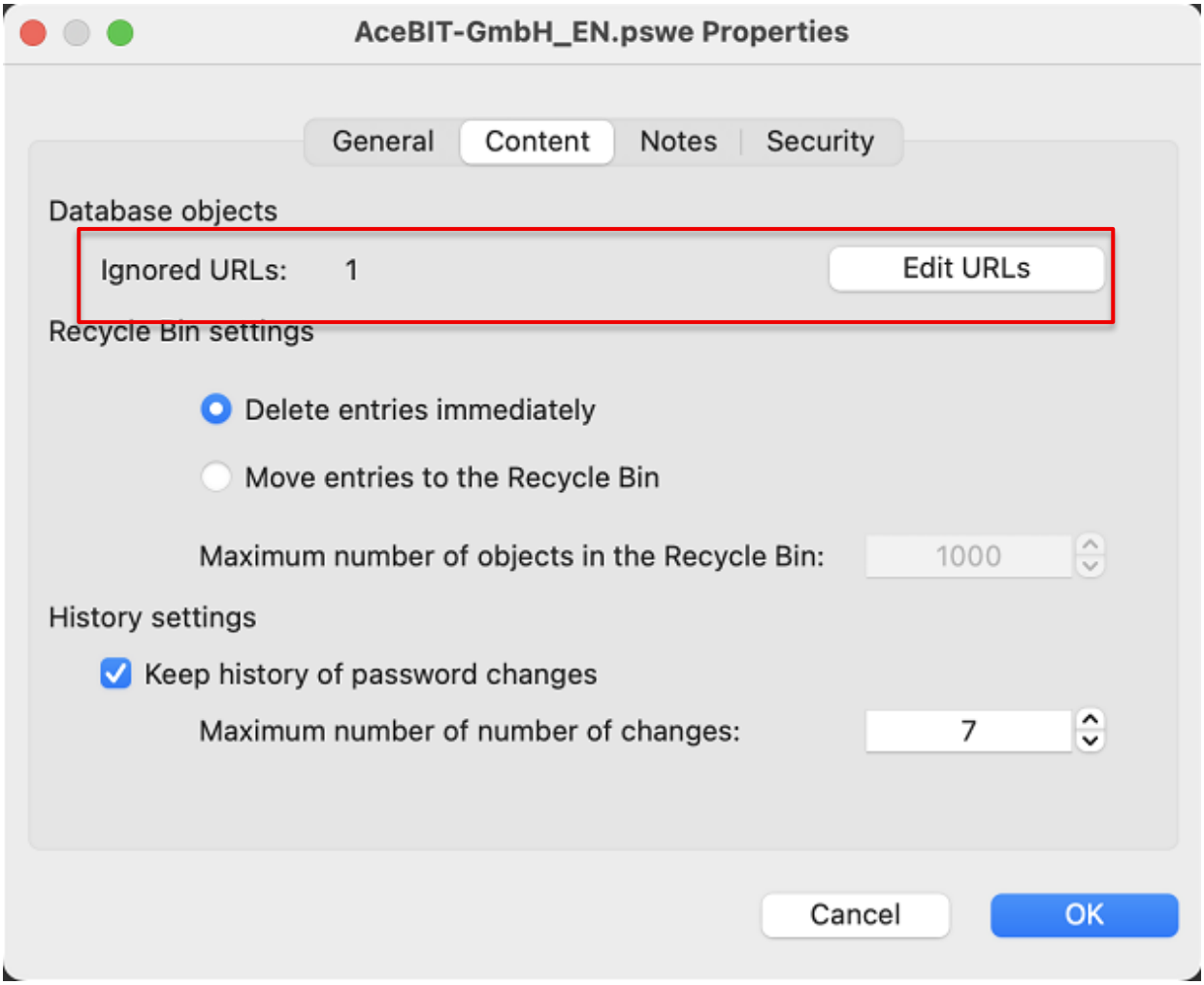
- **Update**: If a password is changed in the browser, Password Depot can offer to update the entry.



- **Ignore**: If the website should not be saved, select Ignore this URL.

Manage ignored websites

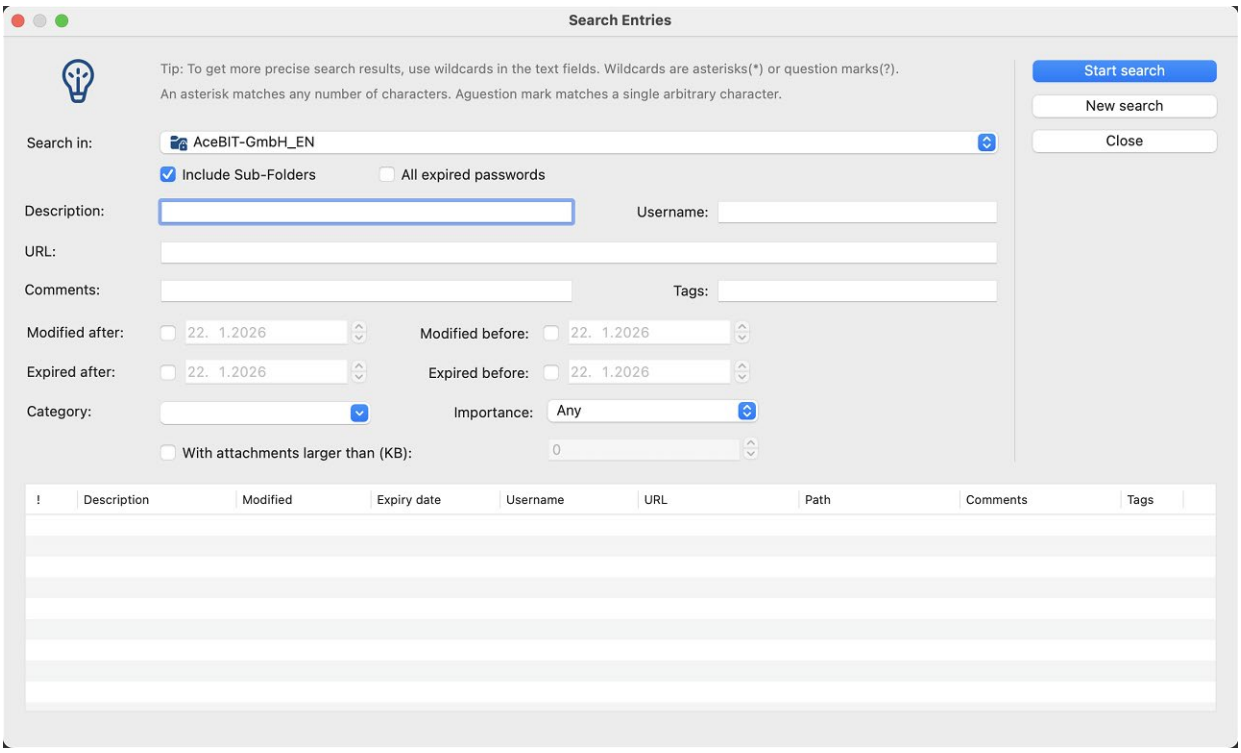
- Open **Database** → **Database properties**.
- Select **Content** tab.
- Next to **Ignored URLs**, click **Edit URLs**.
- Here you can add or remove ignored URLs. Finally, click **OK** to save your changes.



Search, Filter and Replace

To quickly find required entries, Password Depot provides various search functions.

- Click into the search field (magnifying glass) or select **Search** → **Search** for a normal search.
- For complex queries, select **Search** → **Advanced search**. Here you can search for elements such as tags, expiration date or category.

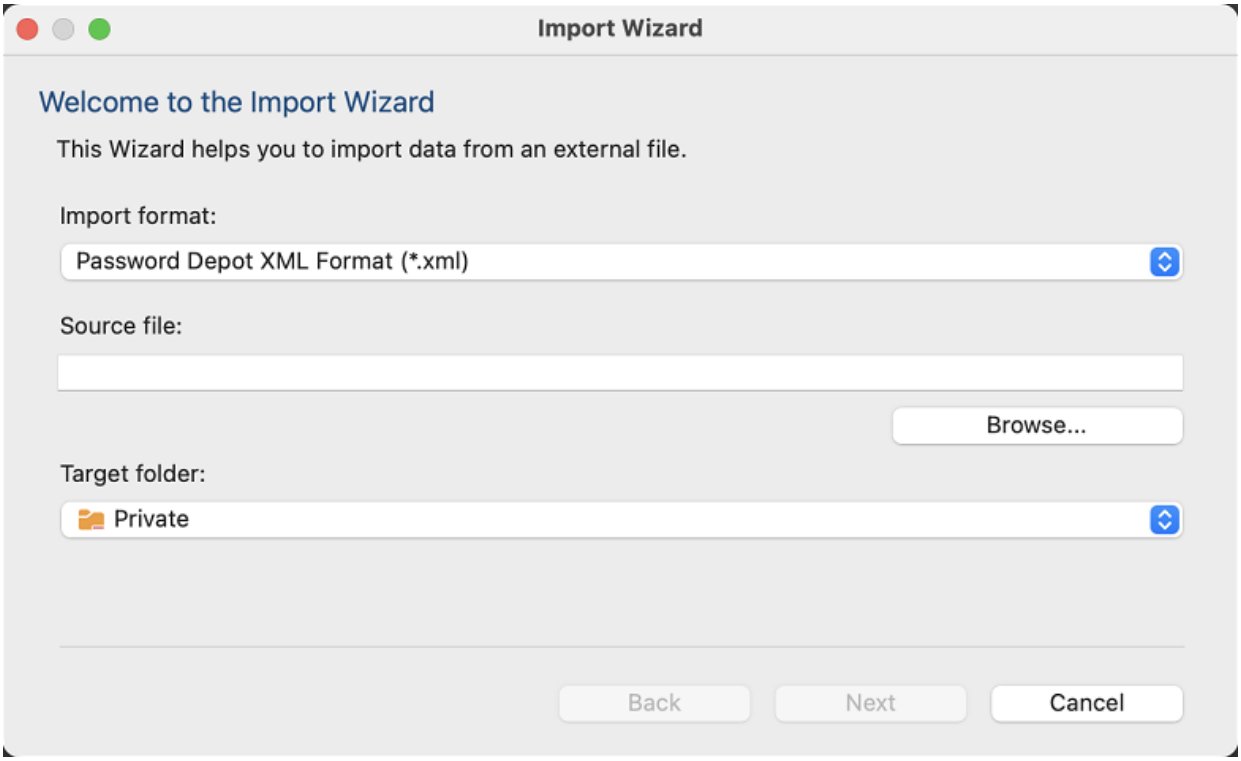


- To make many changes at once (e.g., a new domain), select **Search** → **Search and replace**.

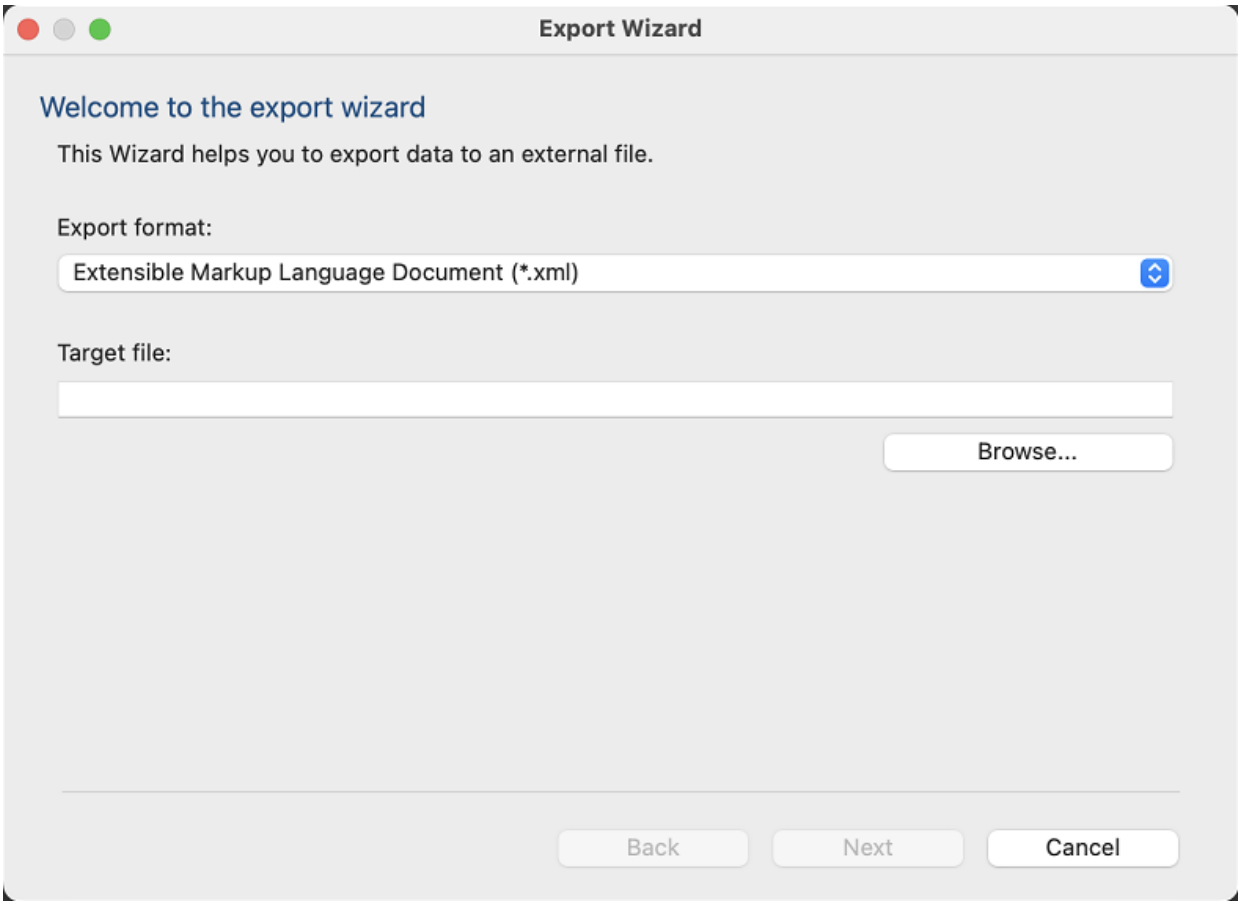
Import and Export (XML)

For further processing, you can import or export data from/to an XML file.

- Click **Tools** → **Import**, select an XML file and the desired destination folder. Follow the wizard to import your data.



- To export your data as an XML file, select **Tools** → **Export**. You must enter your master password again. Choose the target file and whether to export all entries or only a specific view.



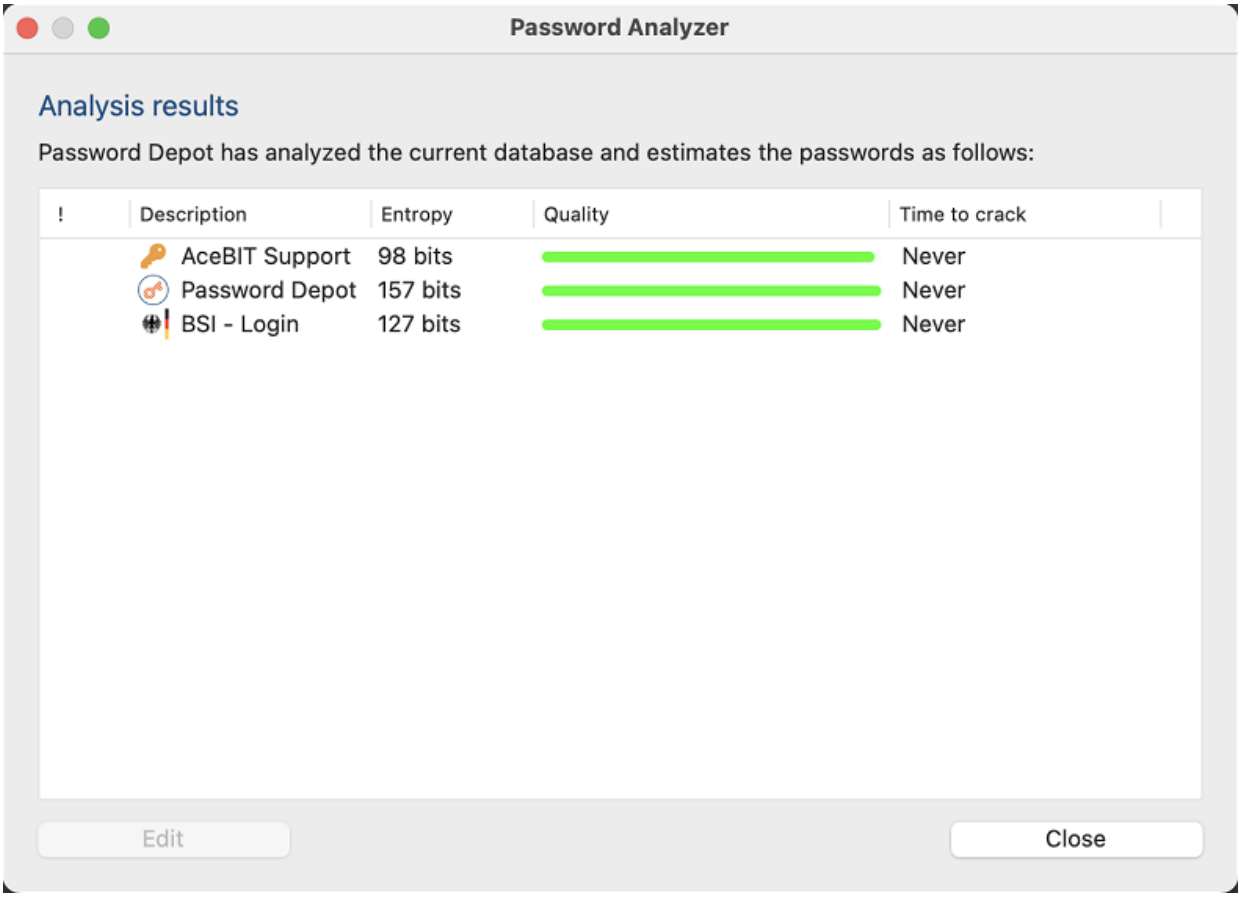
WARNING: Export files contain your data unencrypted. Store export files only briefly and delete them afterward.

Analysis, duplicates and cleanup

Password Depot provides several tools to help you keep your database and entries at high quality over time.

Analyze

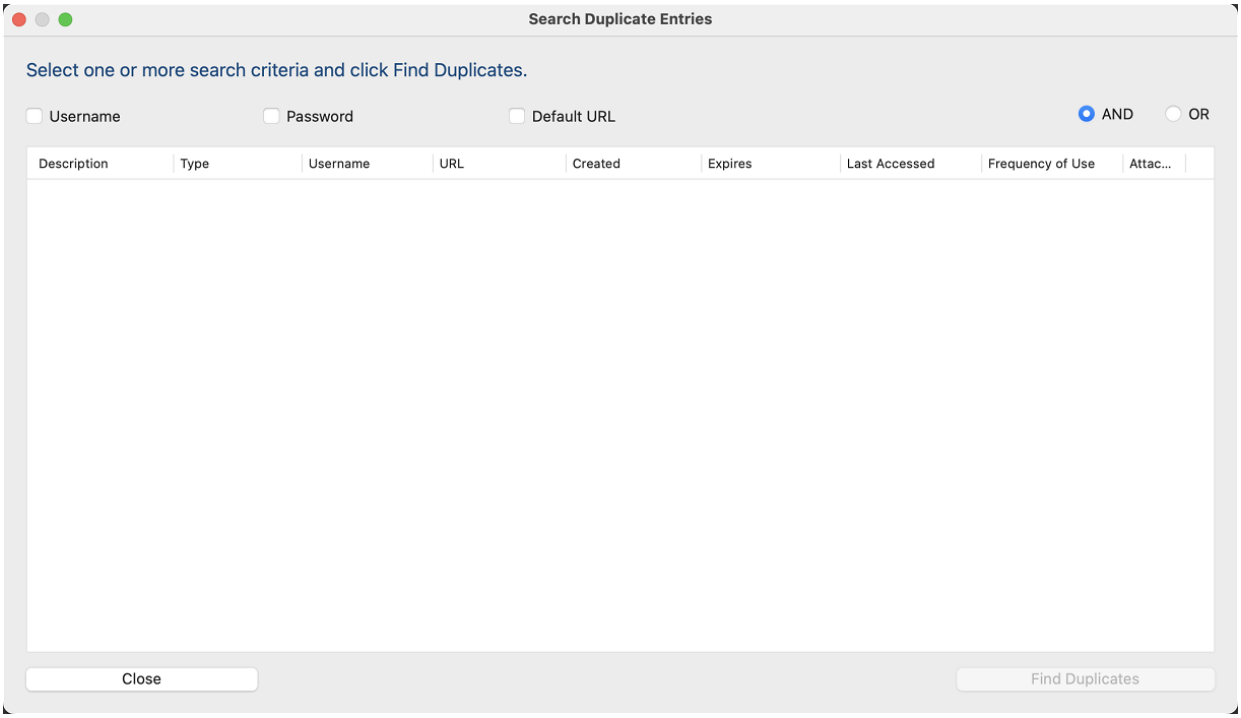
- Select **Tools→ Analyze**.
- Password Depot analyzes the strength of your passwords (by entropy, quality and estimated cracking time).
- Open an entry if necessary to improve it.



Search for duplicates

Password Depot provides a dedicated function to identify duplicates in your entries.

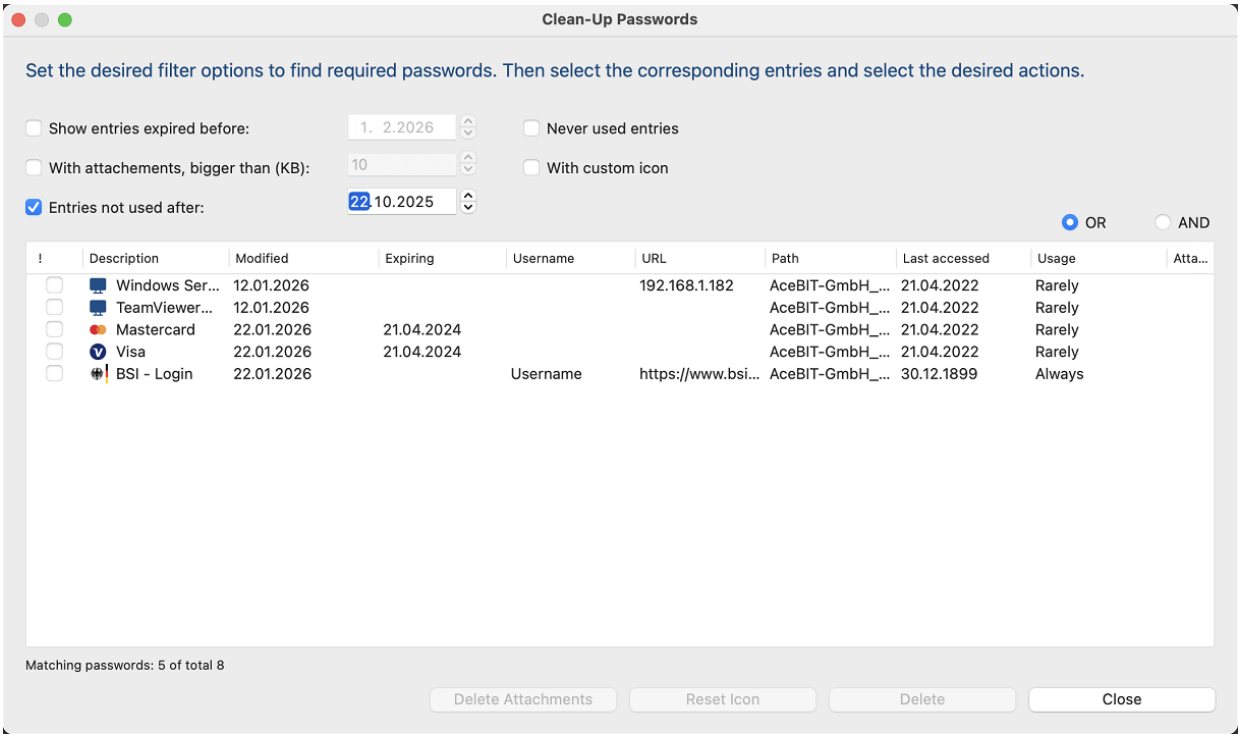
- Select **Tools→ Search for duplicates**.
- Choose whether to search by username, password and/or default URL.
- You can open results directly by double-clicking them and edit if needed.



Clean-up

Keep your database up to date and efficient. Use Password Depot's cleanup tool.

- Select **Tools**→ **Clean-up**.
- Filter entries by expiration date, size of attachments, or last use date.
- Remove attachments if needed or delete entries you no longer require.

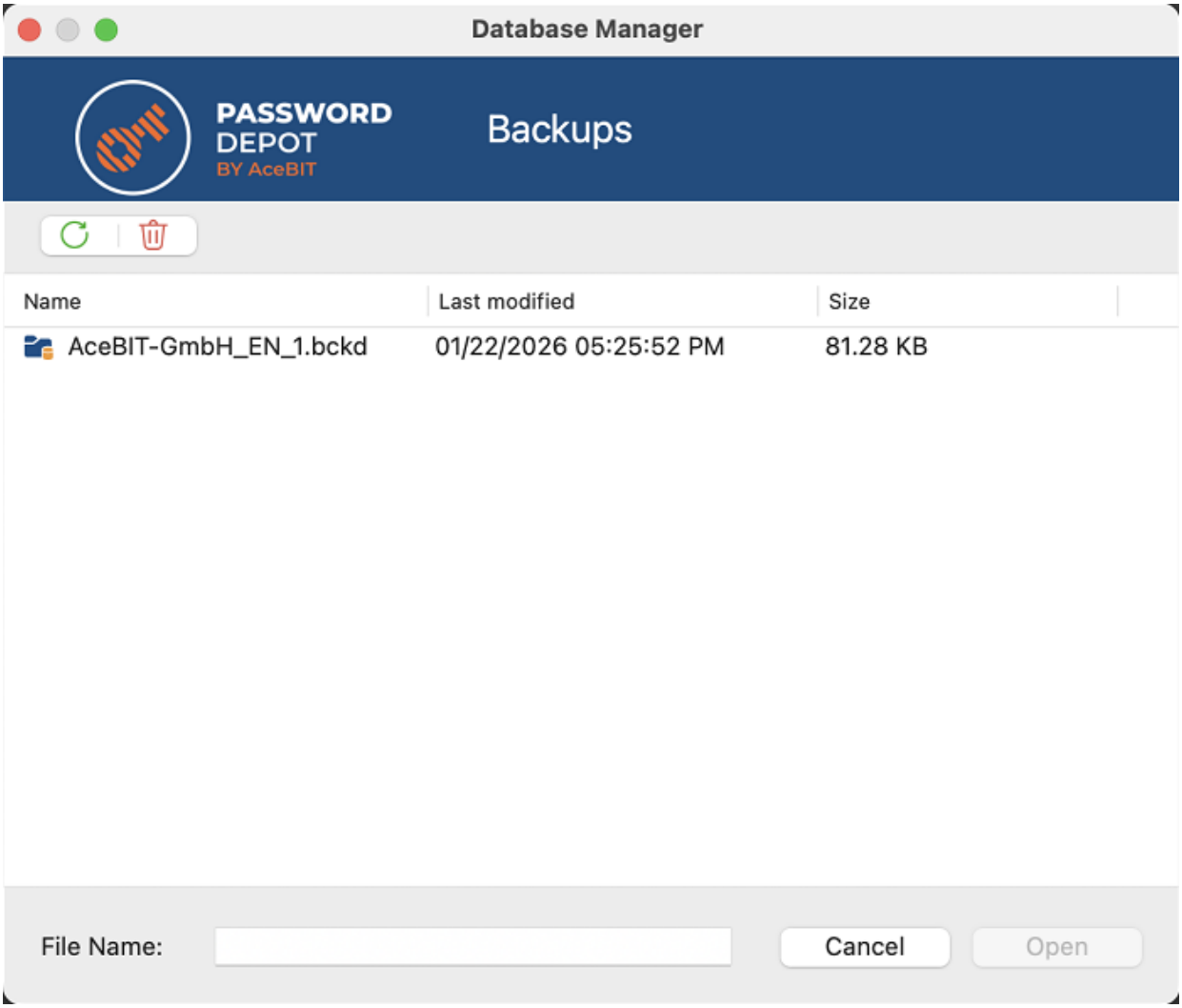


Backups and restore

Backup files help you retain access to your data if you make accidental changes or files become corrupted.

- In **Preferences** under **Save**, enable automatic creation of backup files when opening and/or saving your database.
- To open a backup, open the **Database Manager** and select **Backup files**.
- Select the desired backup database from the list.

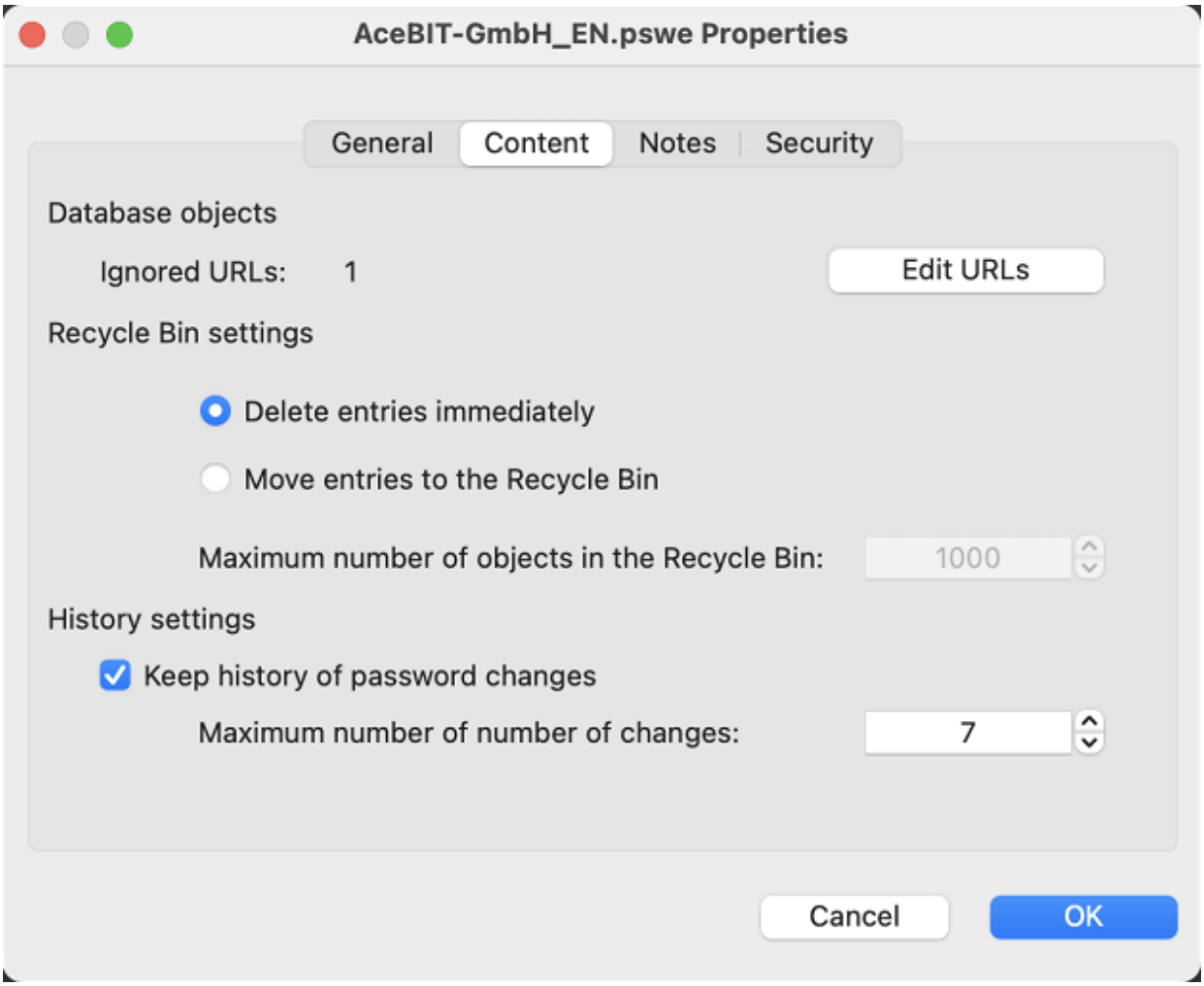
IMPORTANT: Only delete backup files if you are sure you no longer need them.



Database properties

In Database properties you can configure additional settings. Available tabs include **General**, **Content**, **Notes** and **Security**.

- Select **Database** → **Database Properties**.
- To define how deleted entries are handled (delete immediately or move to the recycle bin first), select the option in the **Content** tab under **Recycle Bin settings**.
- In the **Content** tab you will also find history settings. If **Save password change history** is enabled, Password Depot stores the maximum number of versions defined in Properties. This helps you track changes and, if necessary, return to the original password after accidental changes.
- In the **Security tab** of **Database properties** you can also enable **Use a second password**. This allows you to add extra protection to particularly sensitive entries.



Lock and unlock the database

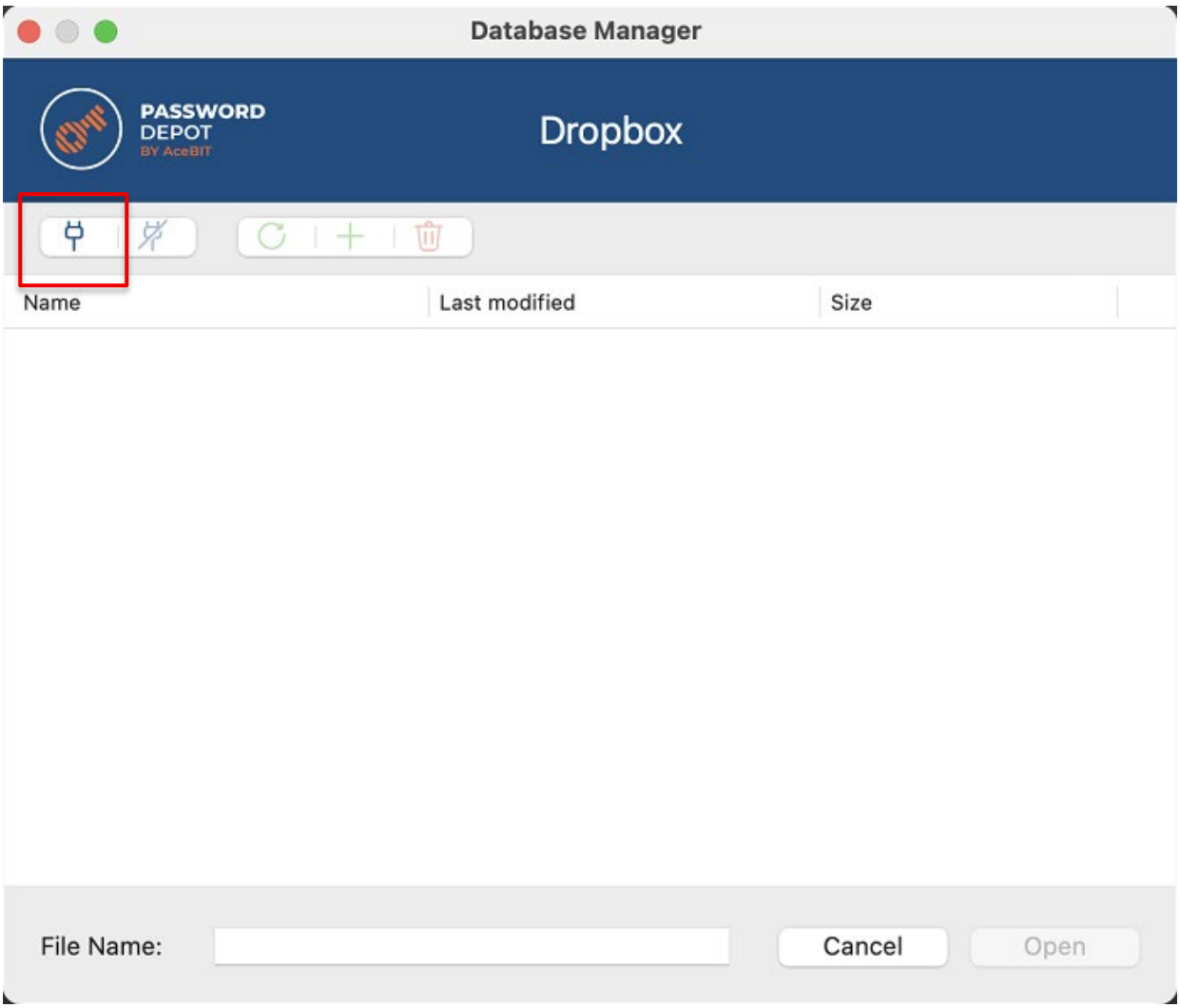
- Click **Lock** or use the menu to close the current database without quitting the app.
- To open the database again later, authenticate again with your master password and/or key file.
- For higher security, configure an automatic lock in the preferences.

Storage locations and synchronization

If you use the same database on multiple devices, store the database in a central location (cloud for private use or Enterprise Server for company customers). This ensures you always work with the latest version.

Cloud storage

- Open the **Database Manager** and select your desired cloud provider (Dropbox, Google Drive, OneDrive, HiDrive or Box).
- Click **Sign In** (Plug symbol) and follow the dialog.
- Once cloud storage is successfully set up, selecting the storage location will list all databases stored there and you can open them or create a new one.

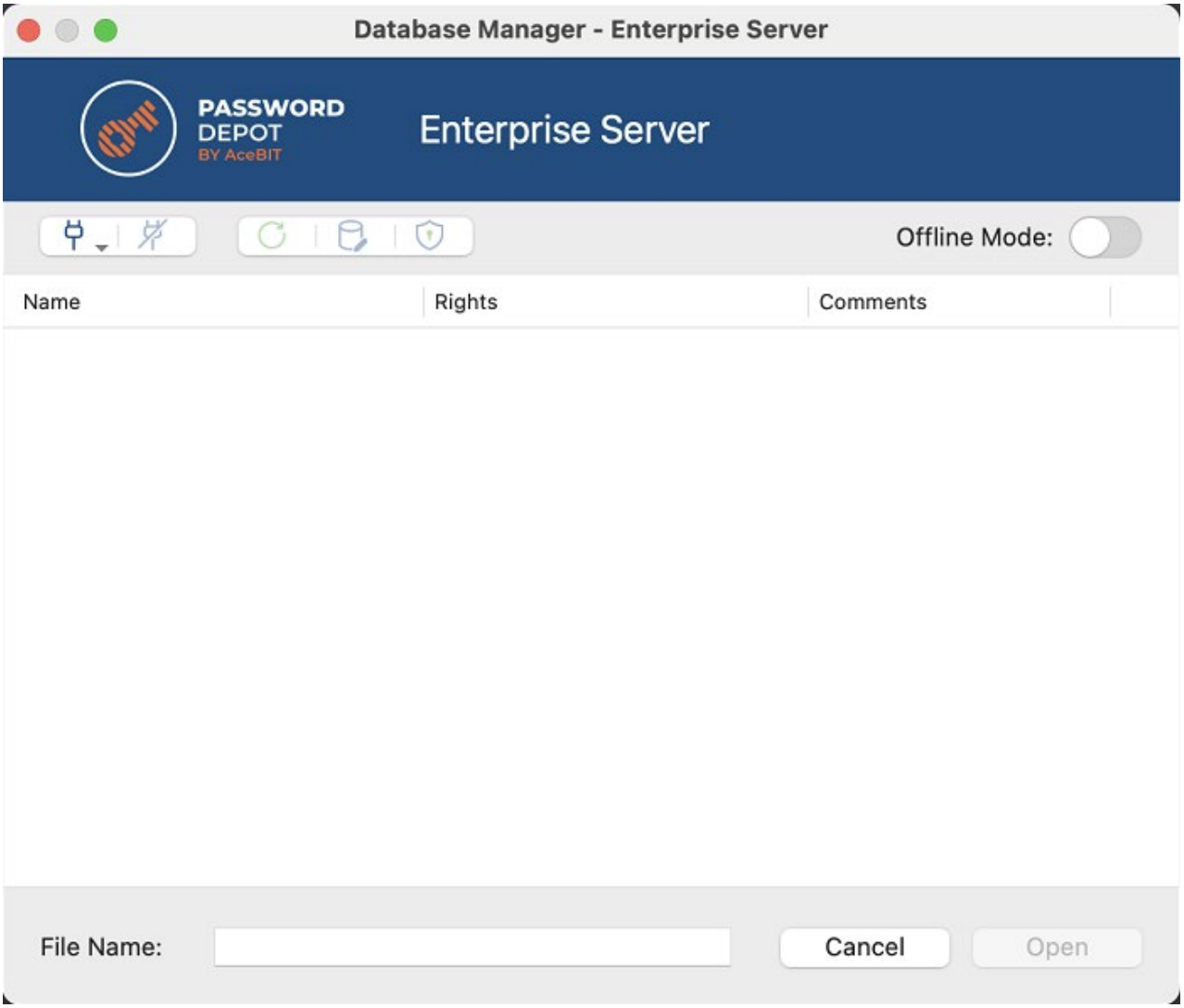


Enterprise Server (company)

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

- Open the **Database Manager** and select **Enterprise Server**.
- Click **Connect to Enterprise Server** and enter server address, port, server version, username and password. In addition to standard authentication, Azure AD authentication and OpenID Connect may also be available if configured by your company.
- Open a shared database from the list.

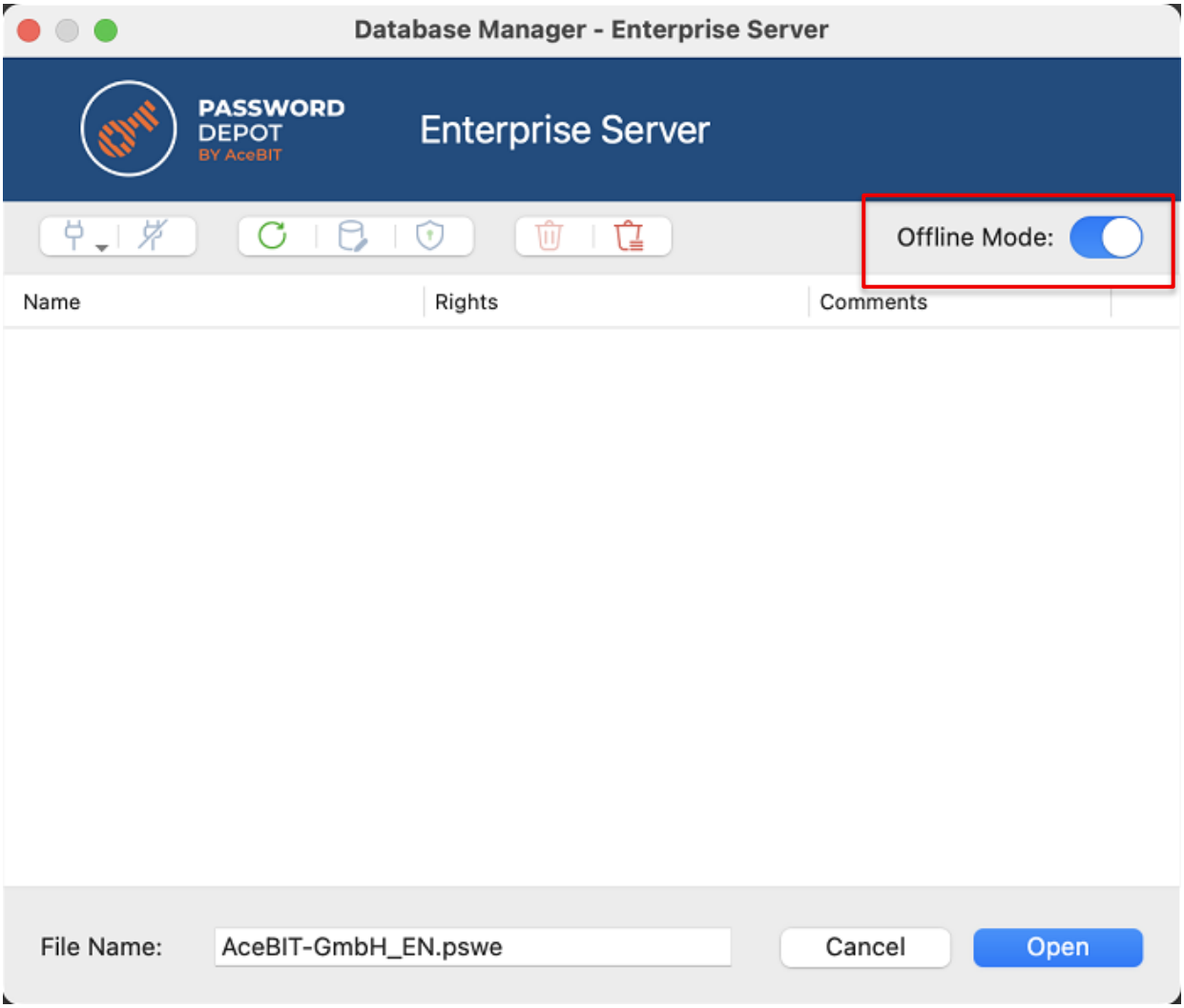
WARNING: Creating databases on the Enterprise Server is done exclusively via the server's Server Manager. You can only open server databases if you have access rights. Access rights are granted by your server administrator.



Offline Mode

If your administrator has granted the required permissions and **Database from Enterprise Server: Save local copy** is enabled in **Preferences**, you can also use Enterprise Server databases offline. This ensures you still have access to your data if you are offline or a server connection is not possible.

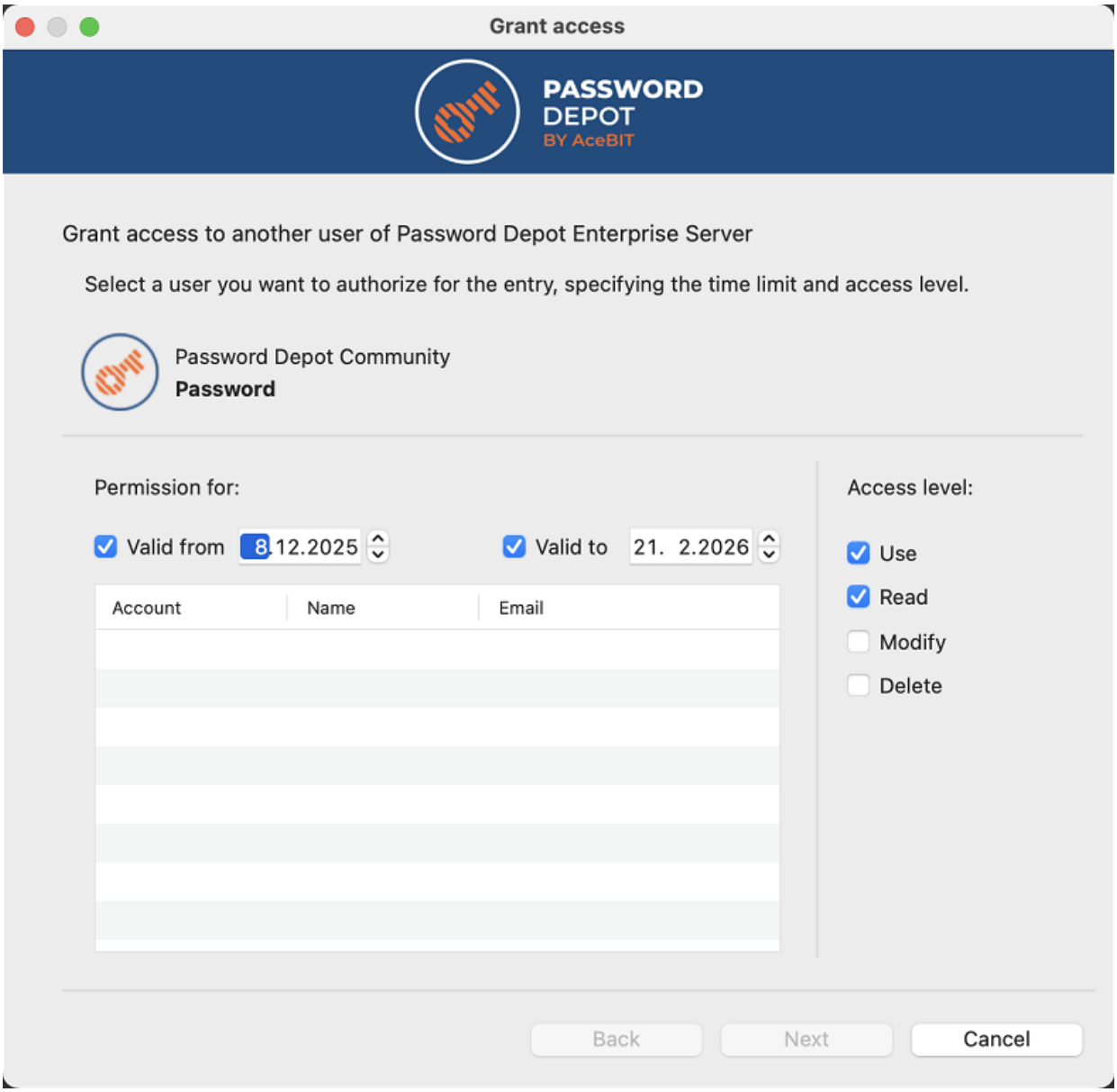
- Enable the **Offline Mode** switch.
- Open the offline database and work with it as usual.
- Once you are online again, follow any prompts that appear for uploading/synchronizing.



Share and seal entries (if available)

If your administrator has granted the appropriate permissions on the Enterprise Server, you can share specific entries with other Enterprise Server users. This allows them to access those entries without full access to the entire database.

- Select the desired entry and choose **Grant access**.
- Select the user to share the entry with. Optionally define access rights (Access/Read/Edit/Delete) and a validity period.
- If **sealing** is configured/allowed, actions can only be permitted after approval by defined reviewers.
- You can find an overview of entries you shared under **Tools** → **Shared entries**.



Tips

Work securely

- Use a strong master password and never share it.
- Consistently lock the database when you are not using it.
- Create regular backups and store them in a secure location.
- Use a unique random password per account, which can be created via the generator.
- Set a second password only for particularly sensitive entries (e.g., admin access).

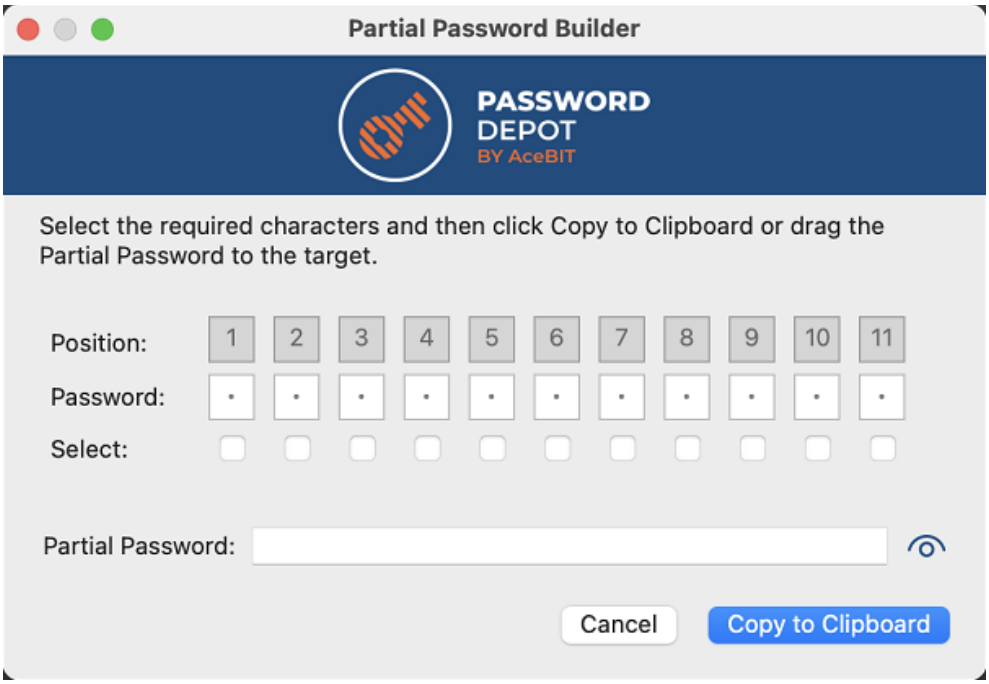
Organize the database

- Use folders for clear structures (e.g., "Private", "Work", "Banking").
- Assign categories and tags (keywords) to find entries faster later.
- Mark important entries as favorites.

Create a partial password

Some systems ask only for specific characters of a password. In such cases, it can be helpful to compile a partial password.

- Select the desired entry.
- Select **Partial password** (available as an action in the details panel). The **Partial Password Builder** opens.
- Mark the required positions and copy the result.



Solve common problems

- **The master password/key file is not accepted**: Check capitalization and the keyboard layout you are using. Also check that you selected the correct database file (.pswe) and, if applicable, the matching key file (.pdk).
- **The add-on did not fill the login data**: Check in **Preferences** whether auto-fill is enabled. If necessary, reinstall the Native Messaging manifest.

Help and Support

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