



Quick Start Guide

Password Depot for macOS



Last Updated: 14.10.22

Table of Contents

Installation	1
Upgrade from Previous Versions	1
Home Screen	2
User Interface	3
Menu Bar	4
Database Manager	6
Local System	6
Enterprise Server	7
How Can I Authenticate on the Enterprise Server?	9
Cloud	12
Recent Files	14
Databases	15
Create a New Database	15
Authentication	17
Open Database	21
Close Database	22
Lock Database	22
Delete Database	23
Folders	23
Recycle Bin	25
Export	26
Import	28
Database Properties	30
Topbar	32
Entries	34
Create New Entry	34
Arrangement of Entries	37
Edit Entry	39
Delete Entry	39
Actions	40
Search	43
Advanced Search	43
Search and Replace	44
Analyze Entries	46
Clean-up Entries	47

Search for Duplicates.....	50
Password Generator	52
Password Generator – Settings	53
Auto-Complete	55
Using the Feature “Auto-Complete (F6)”	55
Using the Browser Add-ons.....	56
Autofill Access Data.....	58
Add New Passwords from Web Browsers.....	60
Update an Existing Password Entry.....	61
Additional Features	62
Available on the Corresponding Login Page.....	62
Available in Your Browser	63
Preferences	67
Useful Links	69

Installation

The Password Depot macOS edition can be used **free of charge**. You do not need a license to work with it. You can download the macOS edition from our [download page](#). After the download, you can install it on your system. It will **not** be required to unlock the macOS edition afterwards, that is, after installation you can start working with the program immediately.

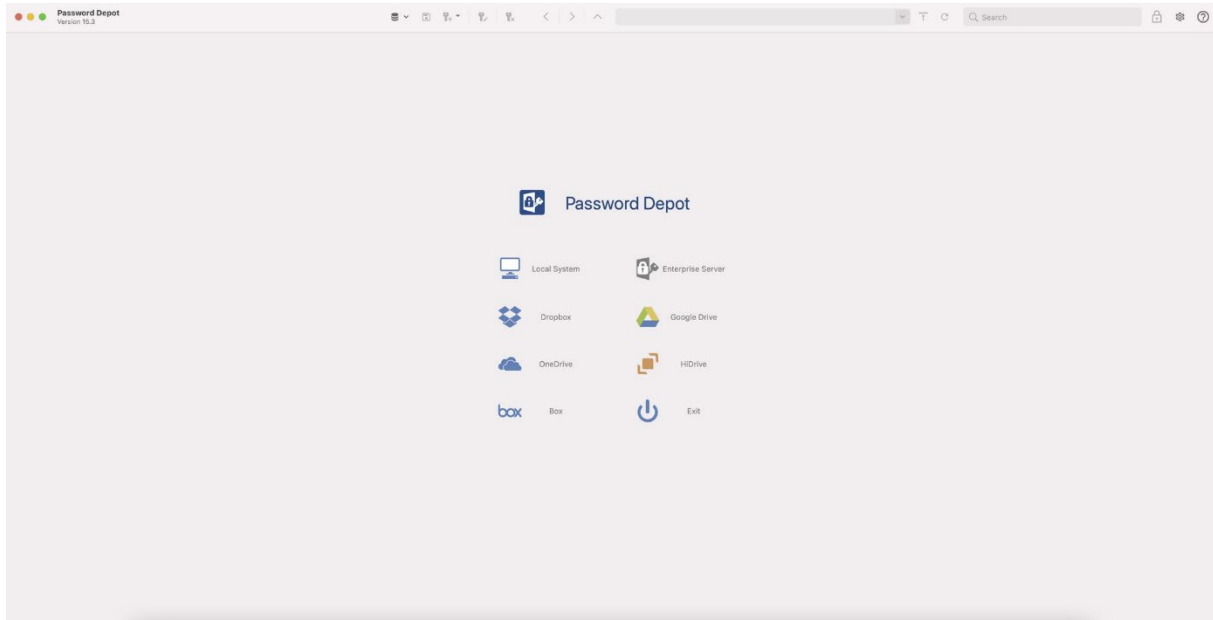
The latest version of Password Depot for macOS can always be downloaded [here](#). You can also find further details as well as the checksums on our website. From build 12.0.3 onwards the Password Depot edition for macOS is a **64-bit app**.

Upgrade from Previous Versions

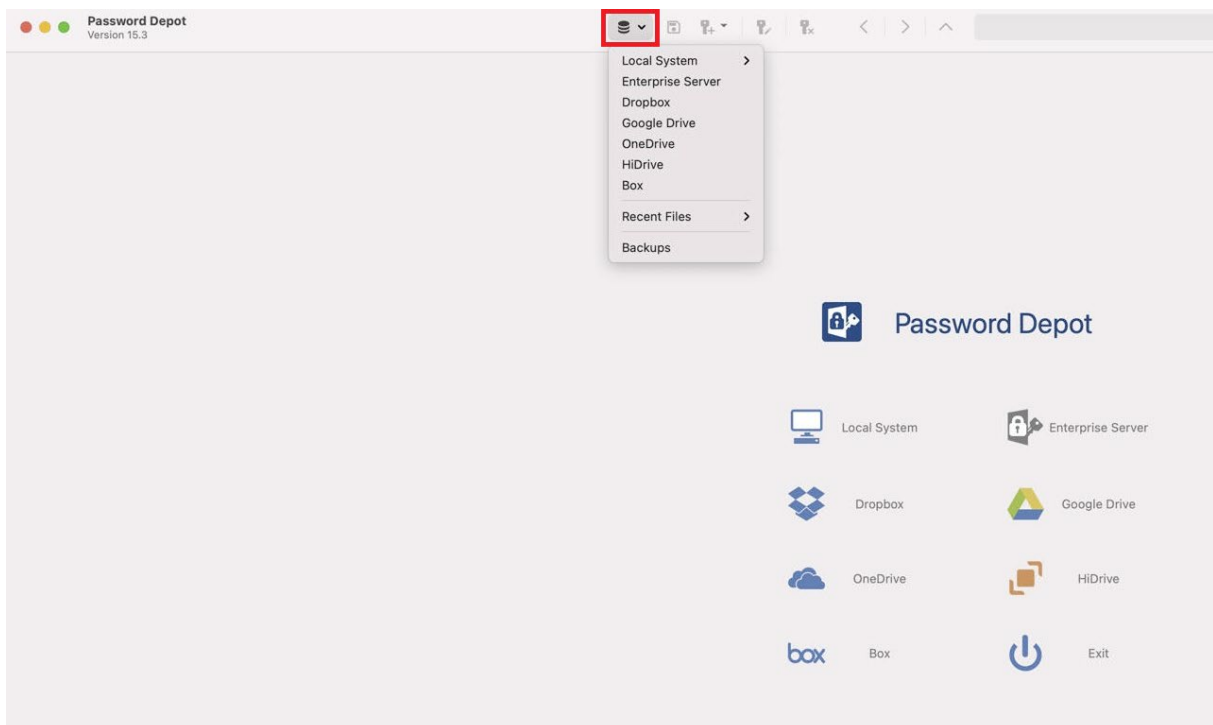
We recommend always working with the latest version of Password Depot and keeping your software updated. You can install both minor updates and upgrades to the next main version without purchasing a license. Furthermore, there is no need to follow a special upgrade process. Simply visit our homepage and select the macOS edition you would like to [download](#) and install (update or upgrade). Your previous password files will not be affected by an update or upgrade. Once the update or upgrade is completed, you can continue working with the new version and your existing databases.

Home Screen

After installation, you can launch Password Depot for the first time on your Mac. When launching the program, you can see the home screen, which is also the Database Manager:

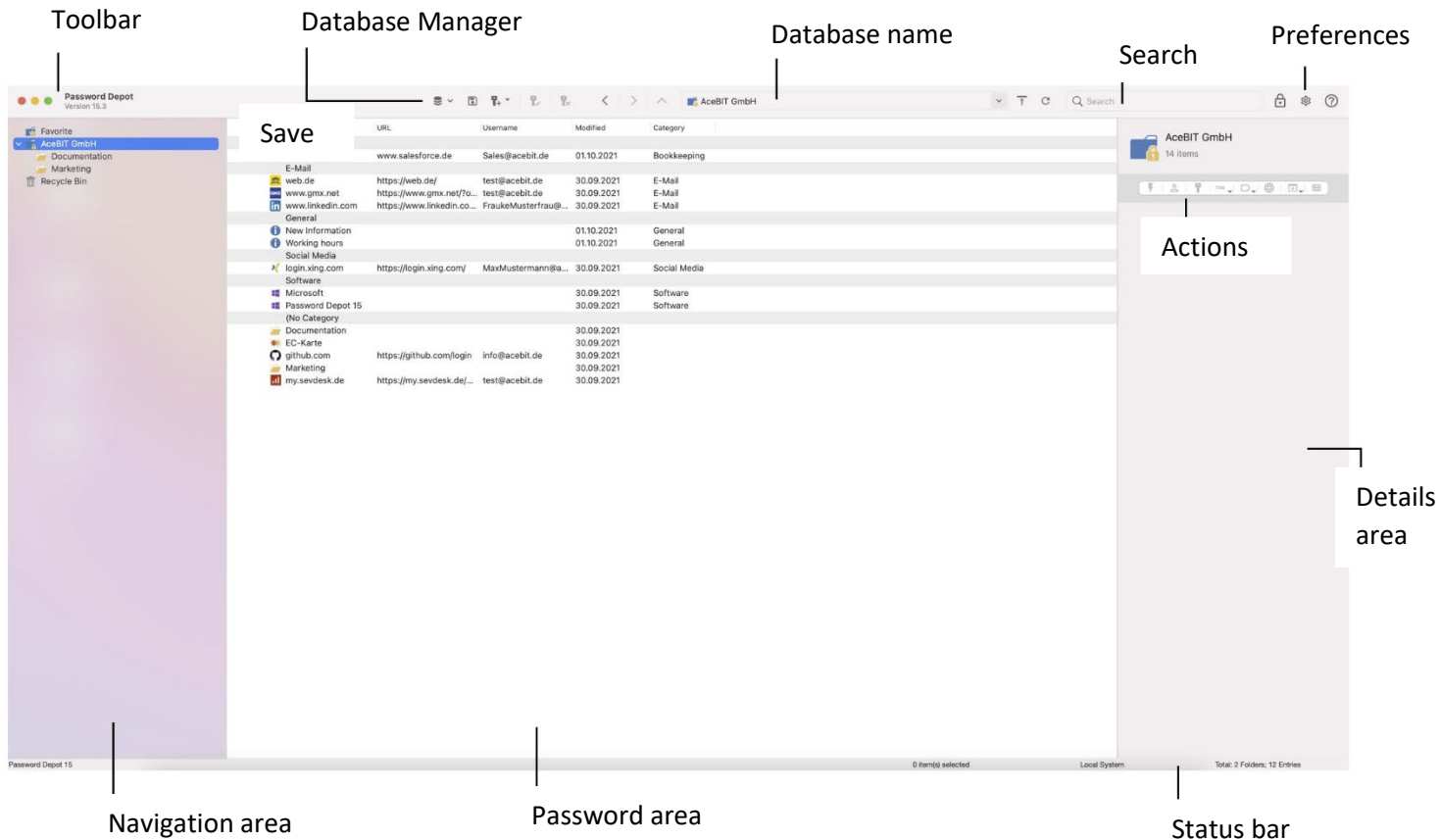


You can select the location for storing your databases. This applies for both newly created databases as well as existing ones. As an alternative, you can also open the Database Manager by left clicking with your mouse on the icon in the toolbar:



User Interface

The user interface of Password Depot is structured logically for intuitive usage.



Toolbar: Above the navigation and password areas, you will find the toolbar providing quick access to Password Depot's most important functions, such as the Database Manager, creating a new entry or editing an existing one, locking the database or refreshing the current view or changing into top bar mode etc.

Database Manager: You can select the location for storing your databases here. This applies for both new databases and existing password files. Furthermore, you can also access backup and recently opened files very quickly by using the Database Manager.

Database name: You can see the name/description of your database that you selected during creation here.

Search: You can perform a global search here, that is, you can search for single objects within your entire database.

Preferences: Opens the preferences to change the language of the user interface, for example.

Actions: If you select an entry from the password area you can perform different actions with it, such as copying the username or password to the clipboard or opening the URL in your browser etc.

Details area: This area is situated on the right of the screen. Its purpose is to display the most important information of a selected entry. This way, it will be easier to access more quickly the most important information of an element and it will also be easier to identify it in your password list.

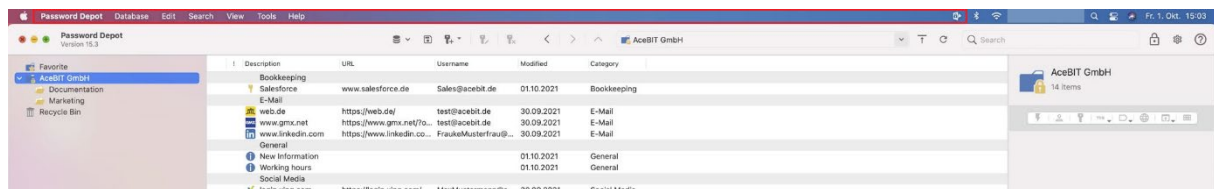
Status bar: Here, you can see which version of Password Depot for macOS you are currently working with, how many folders and entries are included and if you are working on your local system or connected to the Enterprise Server, for example. In addition to that, you can also check here if you have selected any elements from your list of passwords and if so, how many you have selected.

Password area: This is the main window, which is therefore placed in the center of the screen and cannot be closed or hidden. The password area provides access to all passwords within the currently opened database. You will be able to see the description of an entry here, the corresponding URL, if added, the username, the last access, and the category.

Navigation area: The navigation area of Password Depot is structured like the one of the Windows Explorer. You can see the name of your database as well as all folders here. In addition to that, you can also access the recycle bin of this database as well as the folder **Favorite**.

Menu Bar

When you launch Password Depot, you can see the menu bar at the top of the screen which gives you access to additional features:



Password Depot: Select the menu item **About Password Depot** to check the version of the program. You can also access the preferences, hide, or quit Password Depot.

Database: You can get to the Database Manager, save, lock, close or print your database. In addition to that, you can open the Database properties.

Edit: Create a new entry or perform different actions with a previously selected element. Actions include deleting, cutting, copying, pasting, or duplicating an entry. You can also choose an entry from the password list and open its properties (**Edit -> Properties**) or create new categories and global custom fields as well as editing existing ones.

Search: This menu item includes normal and **advanced search** as well as the option **Search and Replace**.

View: You can select here different views for your database. There are several areas which can be shown or hidden, depending on a user's needs: **Navigation area, Databases on the Server, Details,**

Status bar. Additionally, you can also decide according to which grouping the entries should be arranged within your database and you can update the status of your database by choosing **Refresh**.

Tools: Additional tools such as import and export, synchronization and analyzation of databases or the database clean-up can be found here.

Help: Choose this option if you want to open the Password Depot homepage or if you need online support. You can also install add-ons for Google Chrome and Firefox here.

Password Depot icon: You can find the blue Password Depot icon in the menu bar at the top on the right. By clicking on it, you can either lock, unlock or close a database, quit Password Depot, or open the Password Depot homepage by choosing the option **About Password Depot**.

Database Manager

Using the **Database Manager**, you can create new databases and open existing ones.

With Password Depot for macOS you can choose from one of the following locations for storing your password files:

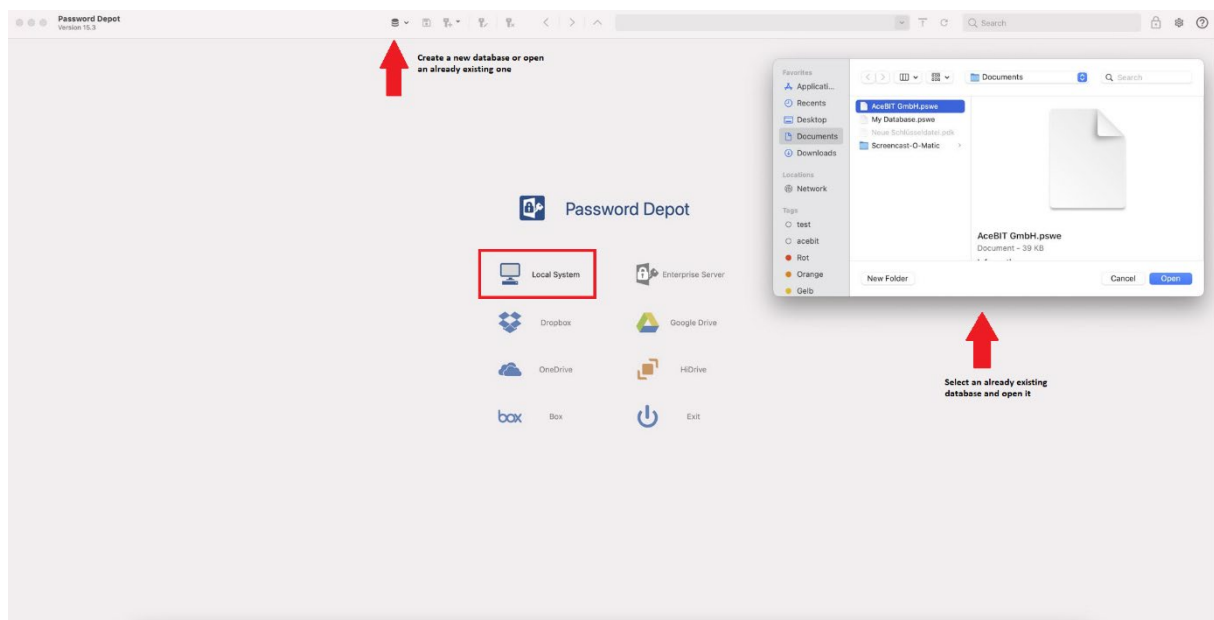
- **Local system**
- **Enterprise Server**
- **Cloud**

The Database Manager includes a single tab for every location. In addition to that, you can also find the options

- **Recent Files**
- and
- **Backups**

in the Database Manager, too. Using these options, you can easily either access files you were previously working with or open backup files of your databases, if necessary.

Local System



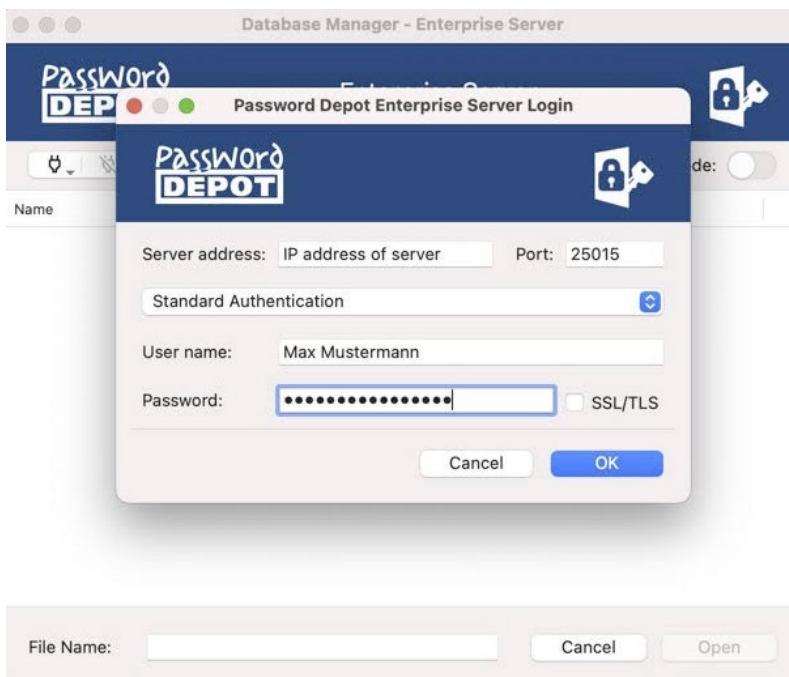
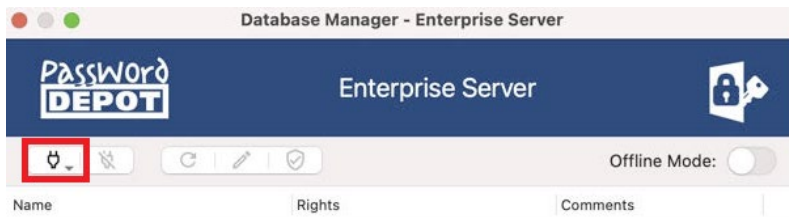
If you have chosen the local system, by default, your password files will be stored to the directory `\Users\\Documents\Password Depot\`

On your local system, you can create a new database and open or delete an existing one. You can learn more about these processes in the chapter [Databases](#).

Enterprise Server

As is the case with all editions of Password Depot, you can connect to **Password Depot Enterprise Server** with your Mac also and thus can access shared databases and entries on your private or company's server.

To connect to the Enterprise Server, choose this option in the Database Manager. Click on the **plug symbol** next and enter the credentials your server administrator gave you.



NOTE: Creating databases on the Enterprise Server can be done in the Server Manager **only**.



You can either access the server of the **latest version 16** or you can also connect to the Enterprise Server version **15**. To connect to an older Enterprise Server version, change the port according to the main version (port 25015 for version 15). No other changes or settings are required.

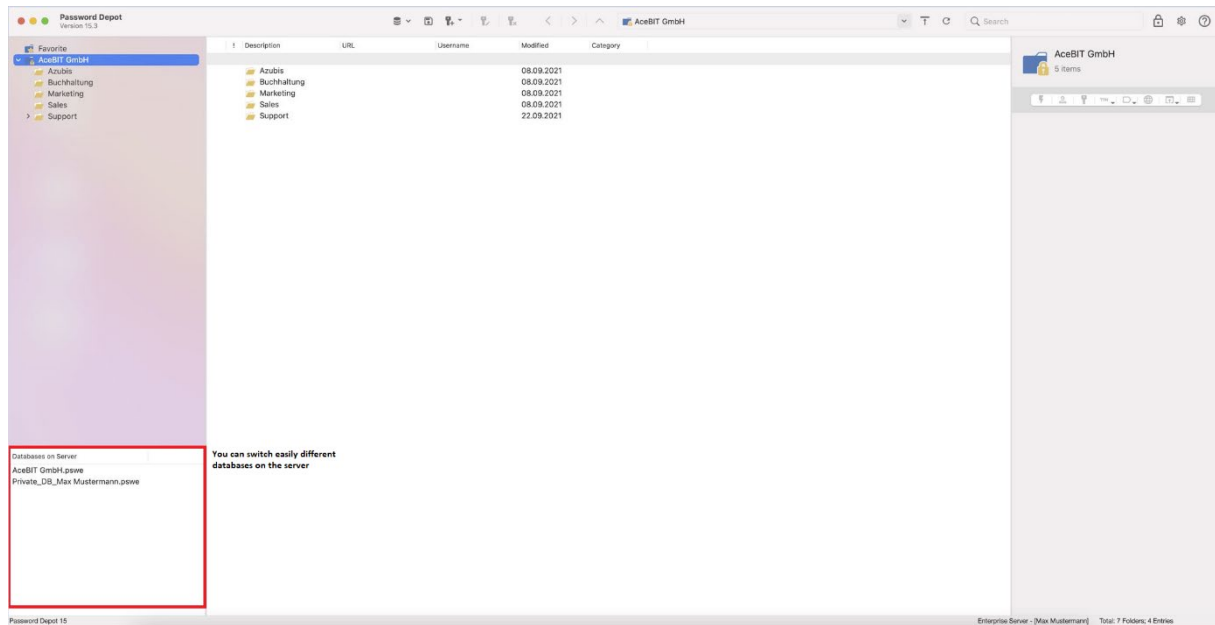
Login to the Enterprise Server not only requires your credentials but, apart from that, also special server data. Below you can find a list of the data required:

- **Server:** Type in the address the Enterprise Server is executed from. In general, it is a local address, for example 90.0.0.1.
- **Port:** Enter the port number Password Depot Enterprise Server can be accessed through. In Password Depot version 16, it is port 25016 by default.
- **Username:** Enter the username assigned by your database administrator.
- **Password:** Enter the password assigned by your database administrator.
- **Use SSL/TLS:** Decide whether you want to use SSL/TLS. We recommend activating this option if you wish to connect your Mac to the Enterprise Server outside a local network.

Afterwards, select **OK** to finish the login process. If the login was successful, you can see all databases on the server you can access. Select one of them and lastly click **Open**.



NOTE: You can only open databases on the server if you **can access them**. Permissions on databases, folders and entries are assigned to users by the system administrator. As soon as you open a database on the Enterprise Server, you can see this database in a small window called **Databases on server** located in the navigation area at the bottom on the left. You can easily switch between different databases on the server without opening the Database Manager every time you want to access another database.



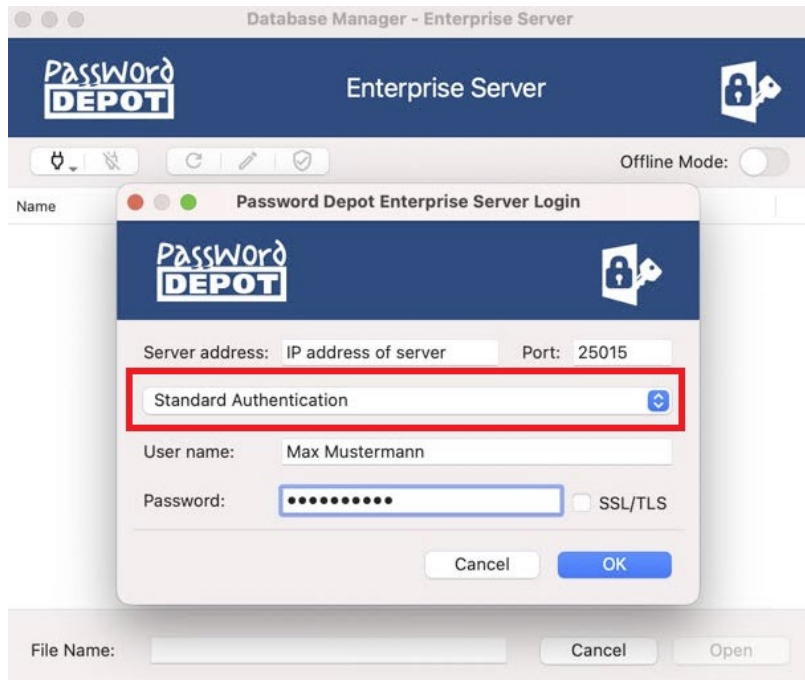
NOTE: You can use **Two-Factor Authentication (2FA)** when connecting to the Enterprise Server with the macOS client. For more information, please click [here](#).

How Can I Authenticate on the Enterprise Server?

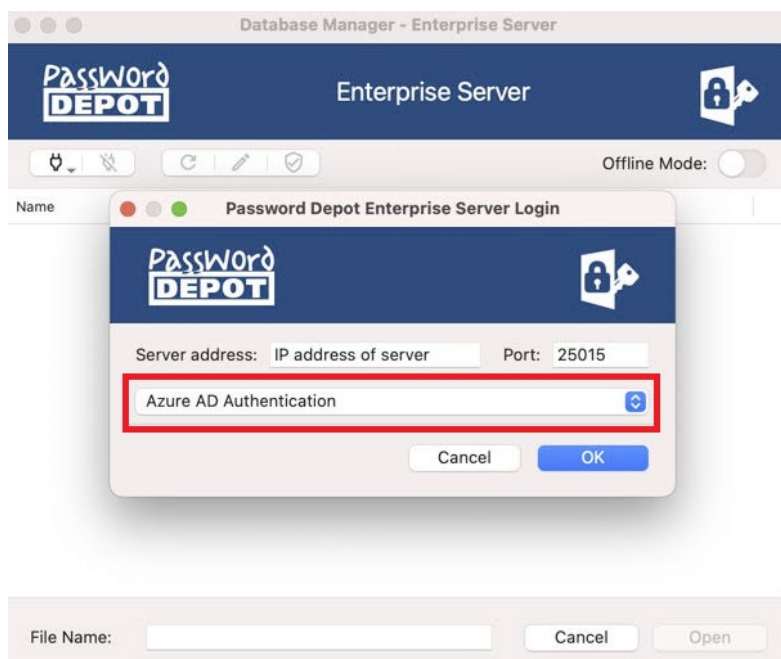
In general, the server administrator decides how users should authenticate on the Enterprise Server. Thus, when connecting to the Enterprise Server, it is only required for users to select the correct authentication mode to establish a client to server connection.

1. **Standard Authentication:** Select this option if you want to login with your username and password.
2. **Azure AD Authentication:** Select this option if you want to login with your Azure AD access data.

Standard Authentication: You can use the Standard Authentication to connect to the Enterprise Server if your Password Depot Server administrator has created local users and assigned usernames and passwords to single users:



Azure AD Authentication: If you want to use Azure AD Authentication, it is required that you are a member of Azure Active Directory. Besides, your server administrator must perform Azure AD synchronization in the Server Manager (prior to the user login) to add Azure AD users to the Password Depot server. If this is the case, please select the Azure AD Authentication in the **Password Depot Enterprise Server Login** window:



Afterwards, a new dialog window will be displayed saying that Password Depot would like to use “microsoftonline.com” for authentication. Please confirm to proceed. You are forwarded to your browser next. Select the correct Microsoft account, enter your email address and password. Lastly, you must enable Password Depot one more time to access your Microsoft account.

A connection to the Enterprise Server will be established once you have completed all the required steps. Afterwards, you can select the desired database and open it.

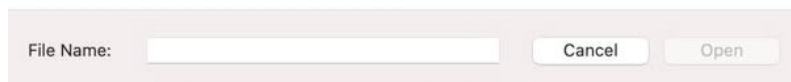
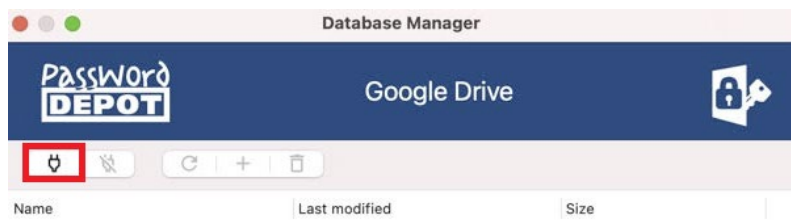
Cloud

The Database Manager of Password Depot for macOS offers different cloud services for storing databases:

- **Dropbox**
- **Google Drive**
- **Microsoft OneDrive**
- **Box**
- **HiDrive**

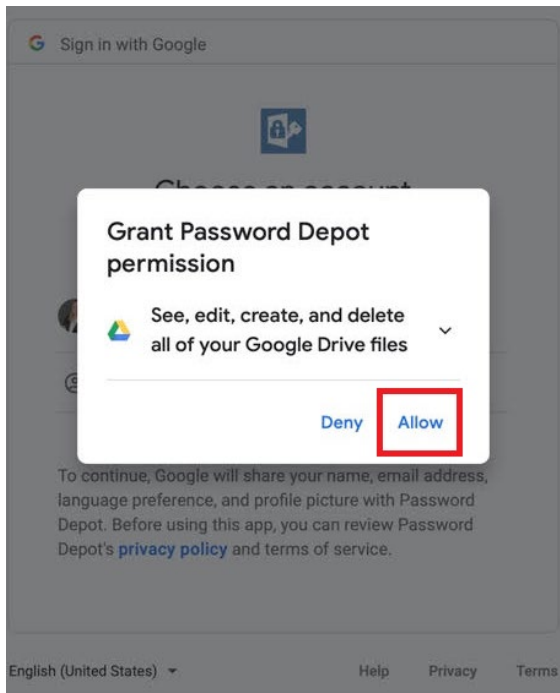
Using a cloud service, you can create a new database and open or delete already existing ones. If you want to create a new database and store it to one of the offered cloud services directly or if you wish to work with a database already stored to the cloud, please proceed as follows:

1. Open the **Database Manager** and select the desired cloud service.
2. Connect to the cloud. To do so, click on the **plug symbol**.

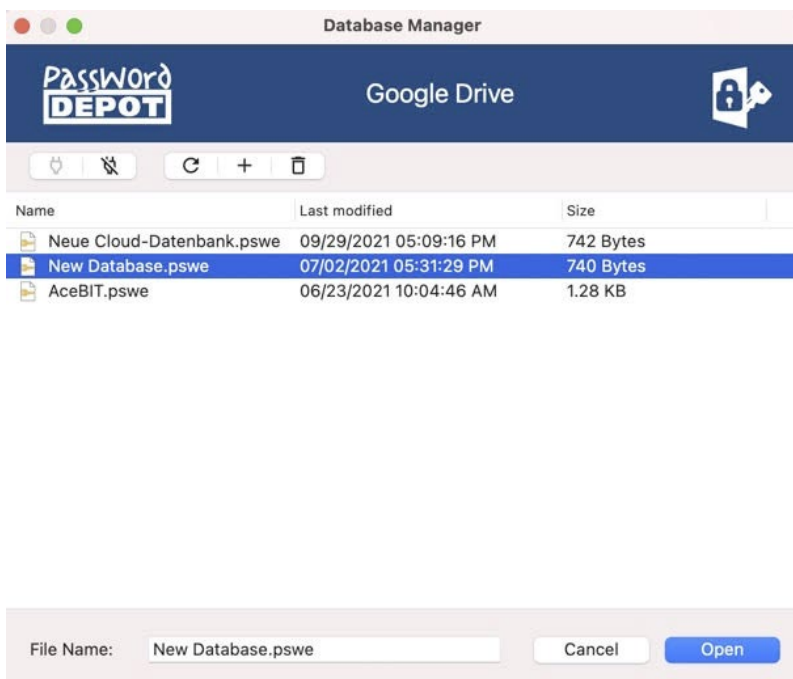




3. A new dialog window will open, and you will be asked to authenticate. Please **enter your credentials** and connect.

NOTE: You must enable Password Depot **to access** the cloud. Otherwise storing databases to the cloud will not be possible at all. Therefore, after authentication, you will be asked **to confirm** first before you can continue.



4. After the login, you can see existing databases that have been stored to the cloud earlier. If you want to open a database, double click on the desired password file, and **authenticate**. Your database will be downloaded from the cloud, and you can start working with it.
5. If you want to create a new database and store it to the cloud directly, please click on **+**. The new database will then be stored to the cloud automatically:



6. Use the  icon to delete a password file from your cloud, or the  icon to update the view. If you want to disconnect, please use the crossed-out plug symbol.

Recent Files

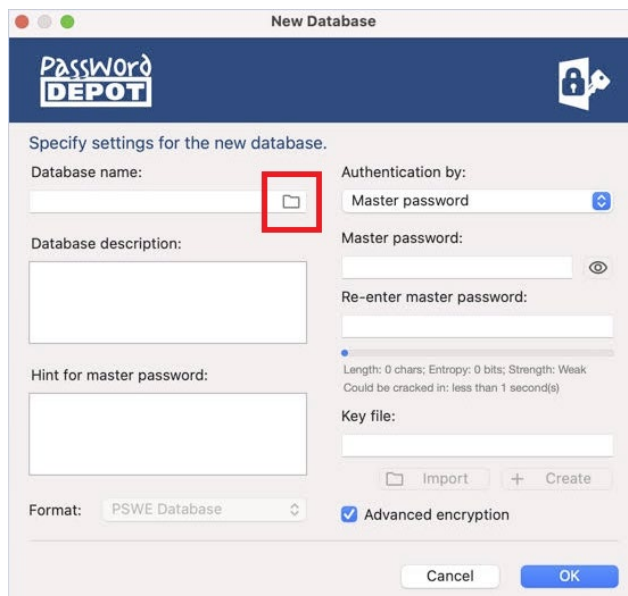
In the Database Manager, you can see the option **Recent files** in the drop-down menu. You can find all databases that have been opened recently here. This applies to all databases, such as databases stored to the local system or stored to your own server or the Enterprise Server, for example. Select the desired database and authenticate.

Databases

Create a New Database

First, select a location in the **Database Manager** for storing your new database. Next, please proceed as follows:

1. Select **+** if you want to create a new database and store it to the cloud or select the option **Create a new database** for adding a new password file to your local system.
2. Enter a database name. The name is mandatory. For local databases, please click on the folder first and then enter the database name in the new dialog window, which will be displayed immediately. You can also change the path for storing your databases to the local system:



3. Select the desired **authentication**. You can choose from **master password**, **master password and key file** and **key file** only. Fill in all necessary fields depending on the selected authentication. Learn more about the different authentications in the chapter [Authentication](#).
4. You can add additional information describing your database in the field **Database description**.
5. If desired, you can add a **hint** referring to your master password in the corresponding field. This hint will be displayed when you click on the corresponding button in case you have forgotten your master password.
6. Finally, select **OK** to create the new database. Authenticate next and the new password file will open.

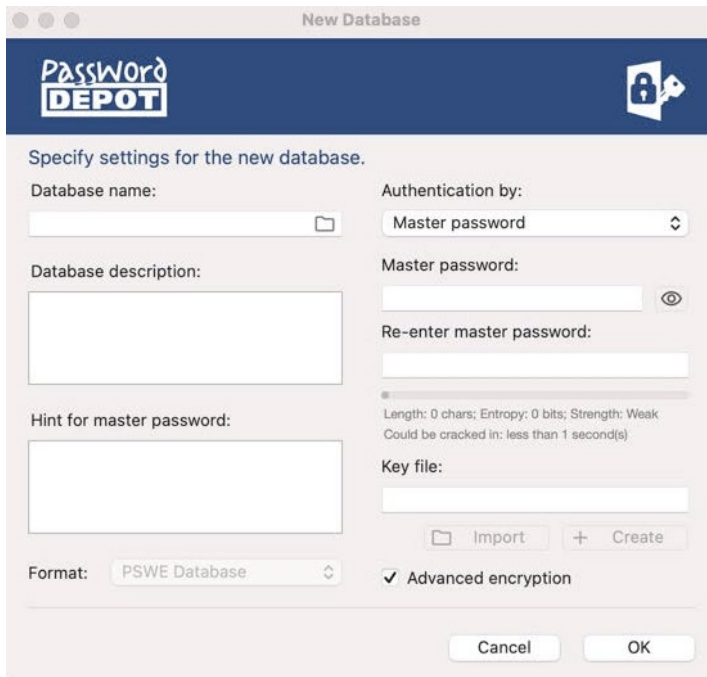
NOTE: When adding a hint, please do **not** enter any information about your master password which could help third parties guess it. Any information added to the hint field should help *you* to remember your master password, but it should be useless to other people.

WARNING: You cannot open your database without entering the **correct** master password. Therefore, please choose a strong master password but also one you will remember!

Authentication

If you create a new database as described above, you will be asked to choose an **authentication**. Three options are available:

- **Master password**
- **Master password and key file**
- **Key file**



New Database

Specify settings for the new database.

Database name:

Database description:

Hint for master password:

Format:

Authentication by:

Master password:

Re-enter master password:

Length: 0 chars; Entropy: 0 bits; Strength: Weak
Could be cracked in: less than 1 second(s)

Key file:

Advanced encryption



New Database

Specify settings for the new database.

Database name:

Database description:

Hint for master password:

Format:

Authentication by:

- Master password
- Master password and key file
- Key file

Re-enter master password:


Length: 0 chars; Entropy: 0 bits; Strength: Weak
Could be cracked in: less than 1 second(s)

Key file:

Advanced encryption

Master password


We recommend always creating a secure master password for encrypting your password files. For your security, the master password policy requires the master password to consist of at least 15 characters and include at least three out of the four following character types: uppercase letters, lowercase letters, numbers, and special characters. Furthermore, you can check whether your master password is present in pwned databases. Such databases contain login data that have been subject to data breaches and are therefore not safe to use anymore. By selecting the corresponding option, you can check whether this is the case for your master password.

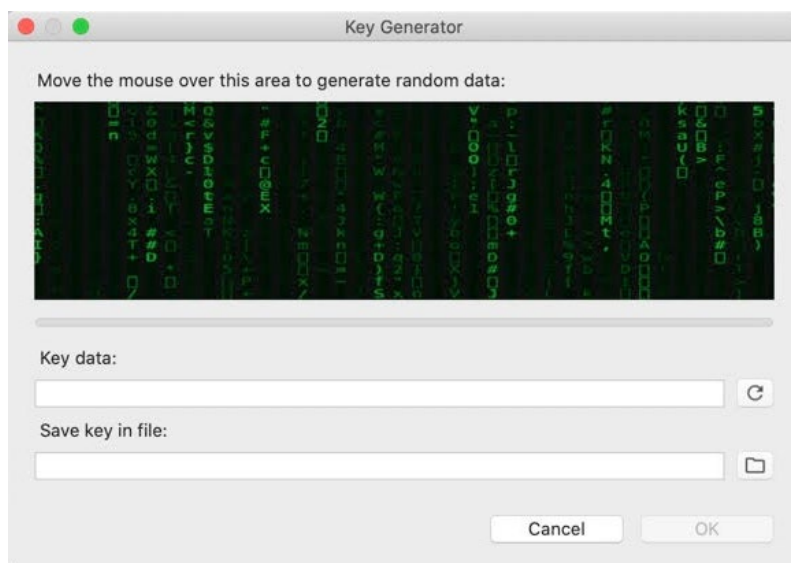
Re-enter your master password in the corresponding field. You can display your master password in clear text for a short time by clicking on the  icon.

ATTENTION: In general, we recommend only using this option if necessary because, in case of doubt, third parties could read your master password and thus be able to access your passwords and sensitive data without permission!

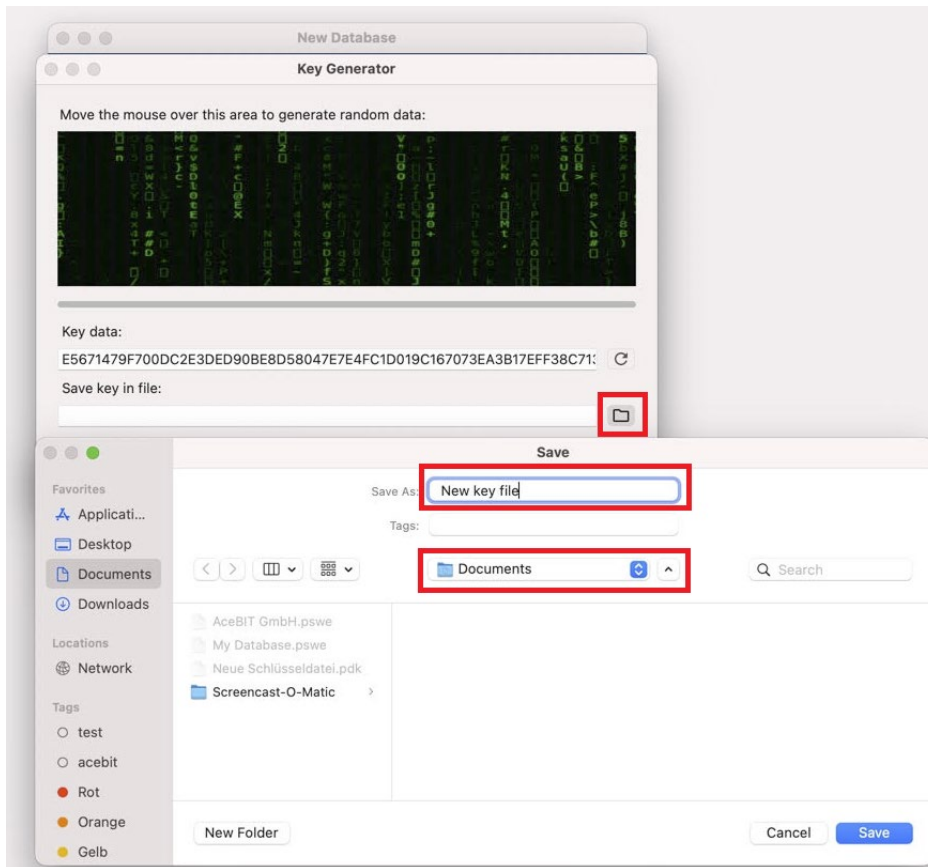
Master password and key file

If you encrypt your database with a **master password** and a **key file**, you are using **Two-Factor Authentication**. In this case, you can only open your database if both the master password and the key file are correct. Choose this authentication from the drop-down menu, if desired.

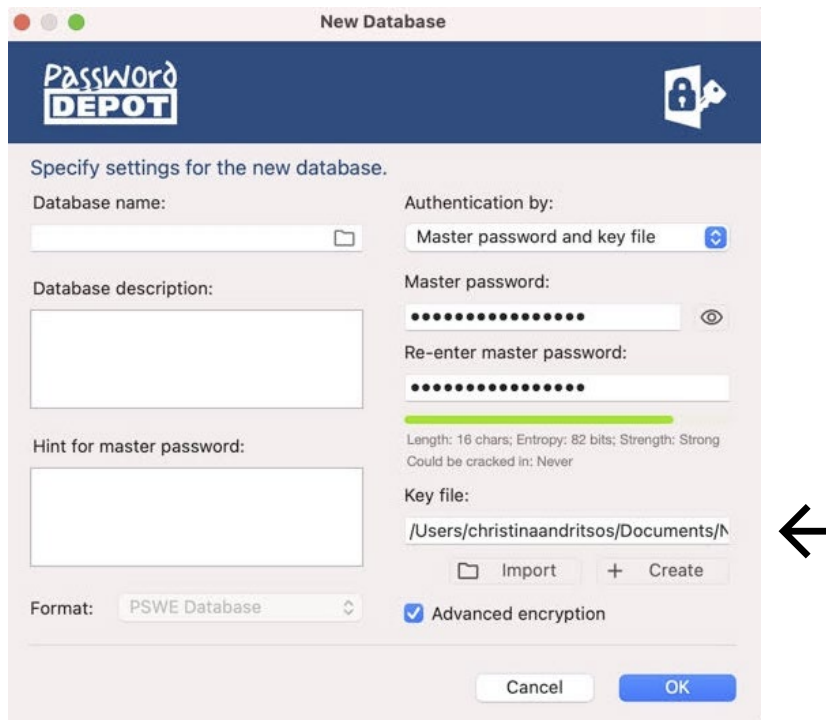
Next, please enter a master password first and repeat it in the field below. Then, generate a new key file. To do so, click on  **Create**. A new dialog window will open as follows:



Move the mouse over the area to generate random data and create a new key file. The process will be completed as soon as the bar below the area turns blue and you can see the key data in the corresponding field. You can specify the location for storing the key file using the option **Save key in file**. To do so, enter a name first and select the desired location next:



Lastly, click **Save**. The selected location will now be displayed in the field **Save key in file**. Click **OK** and you will get back to the window for creating a new database. You can see the recently created key file in the corresponding field:



You can also use the browse button **Import** if you want to use any already existing key file for encrypting your new database. Search for it on your Mac and select **Open**. Afterwards, you will get back to the above window and the previously selected key file will now be displayed in the corresponding field.


Key file:

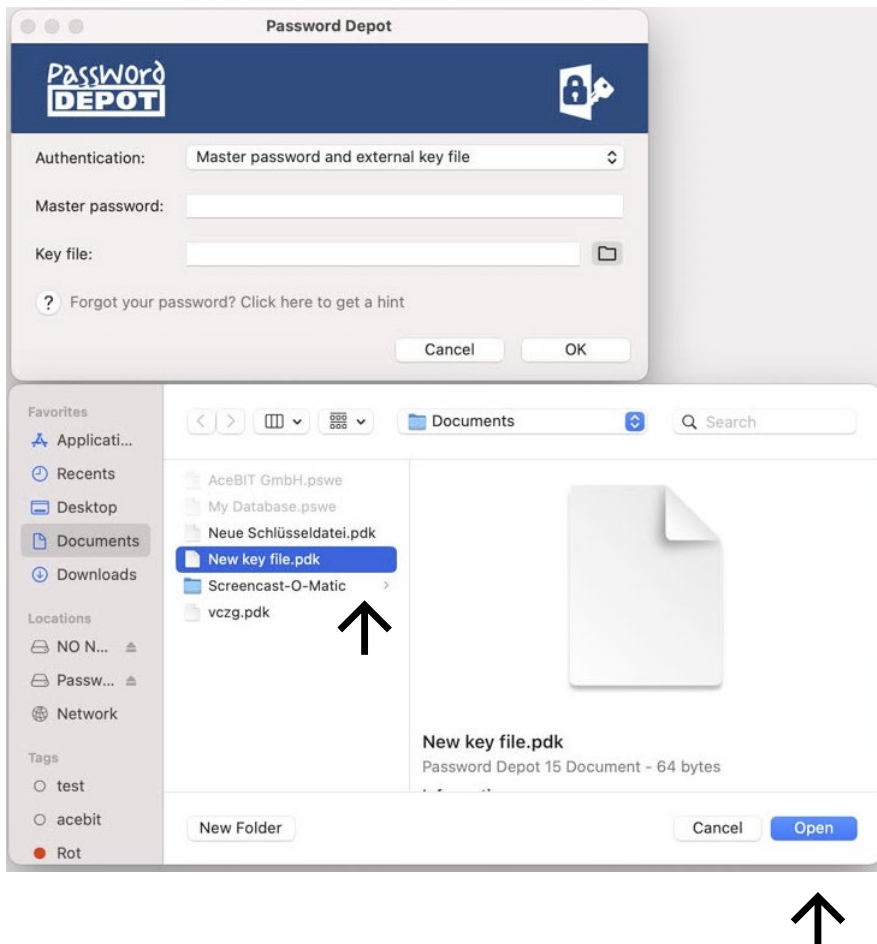
Your password file will be encrypted with a key file **only** using this method of authentication. To generate a new key file or to choose an existing one, please proceed as mentioned above. However, in this case, please take the following into consideration:

WARNING: We **do not** recommend using only a key file for encrypting your database since it will be easy for third parties to get access to your file if you only encrypt it with a key file and have stored both your password and key file in the same location.

Open Database

1. Open Password Depot and select the **location**.
2. Select the desired database and click **Open** at the bottom on the right or **double click** on the corresponding file.
3. **Authenticate** by entering your master password and/or key file and finally click **OK**. The database will open if authentication was successful. Please make sure to select the correct authentication type.

NOTE: To enter the corresponding key file, click on  first. A new dialog window will open where you can search for your key file. Finally, click **Open** and the requested file will be pasted into the authentication window.



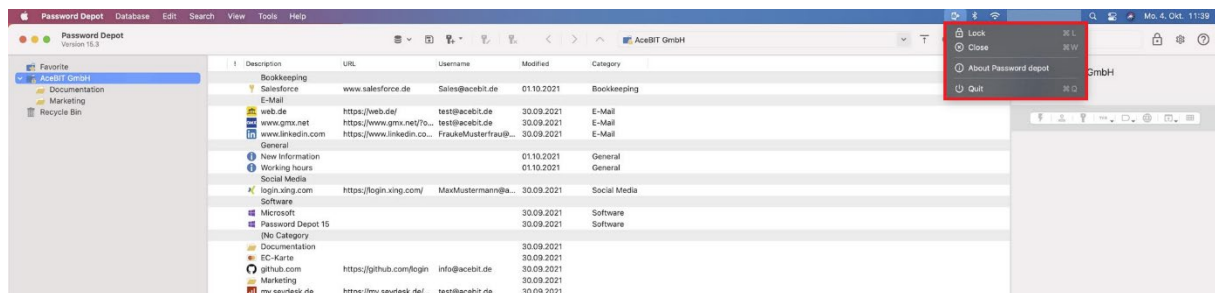
Password Depot for macOS – Quickstart guide

As soon as the key file has been added successfully, the authentication window will be displayed as follows:




Close Database


If you want to close your database, go to your Mac's menu bar and click the **blue Password Depot icon** -> **Close**. You will get back to the Database Manager. More options are available here such as locking your database or quitting Password Depot. You can find the same options by clicking **Database** in the menu bar.



Lock Database

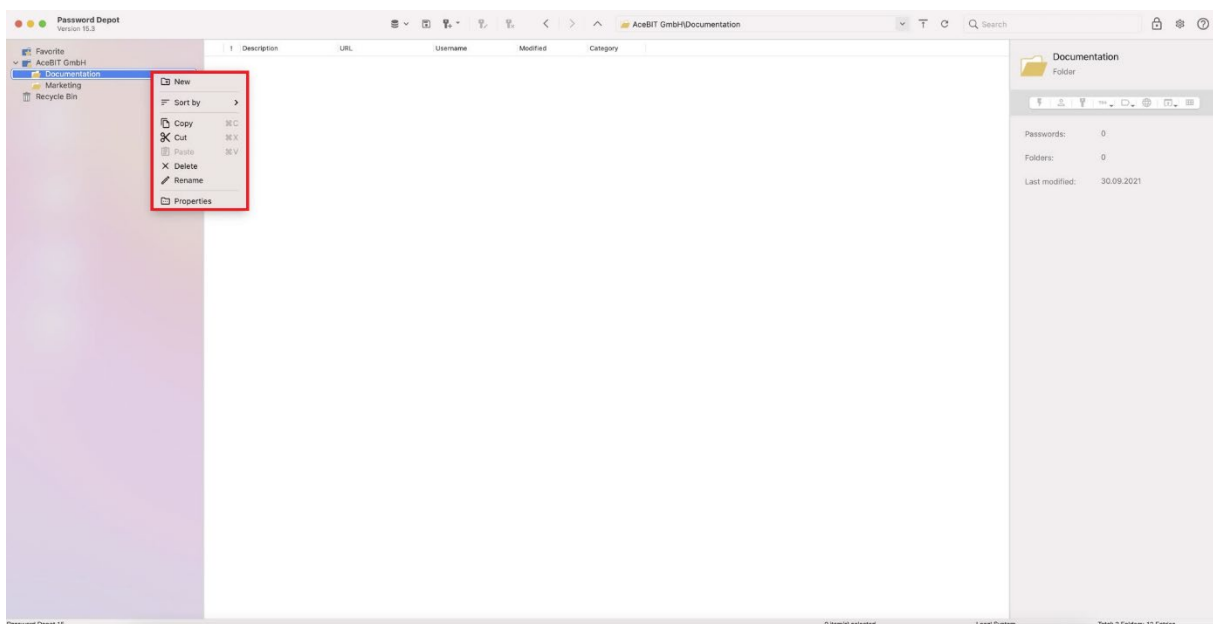
You can lock your Password Depot database if you need to leave your desk and do not want to shut down the program or computer, for example. To do so, go to the toolbar and select the icon . Your database will be locked, and Password Depot will be minimized. The blue Password Depot icon will now be visible in the Dock with an additional yellow lock. If you want to continue working with the program, click the icon in the Dock and authenticate.

Delete Database

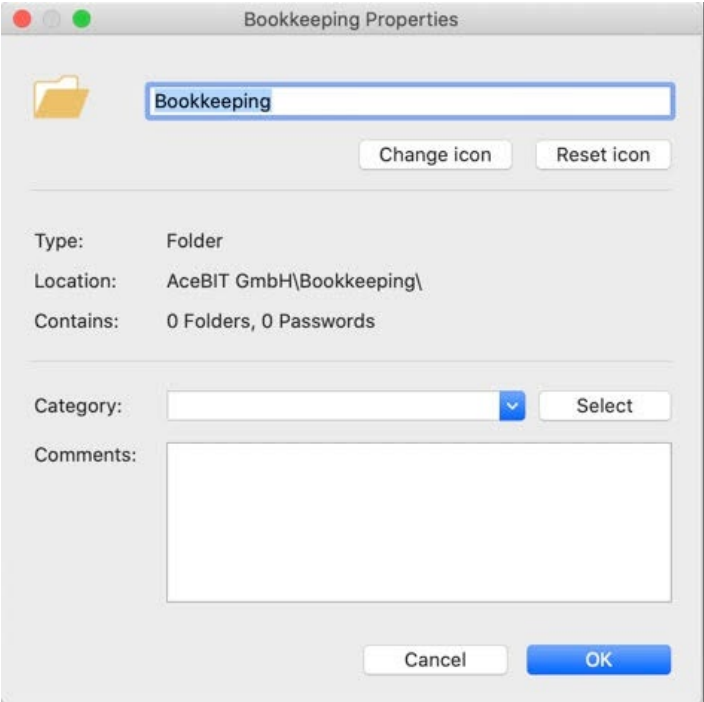
1. Open Password Depot.
2. Select the location of the database you would like to delete.
 - **Cloud:** First, login to the desired cloud service. After authentication, you can see all databases stored to this cloud service. Choose the desired database and afterwards, click . You will be asked to confirm the database's permanent deletion. Choose **OK** to confirm or select **Cancel** to stop the process.
 - **Local system:** Click this option in the Database Manager and afterwards, select the correct database. Right click on the desired object and use the option **Move to Trash**. The database will then be moved to the recycle bin. You can restore it from the recycle bin later in case you need to access it again.
 - **Enterprise Server:** Deleting databases on the Enterprise Server can only be done by the server administrator.

Folders

You can add individual **folders** and **subfolders** to the root directory of your database. To do so, either right click on the root folder or any other folder within your database and choose the option **New**:



This way, you can also delete existing folders and subfolders or rename them. Furthermore, you can also open a folder's properties to edit them:

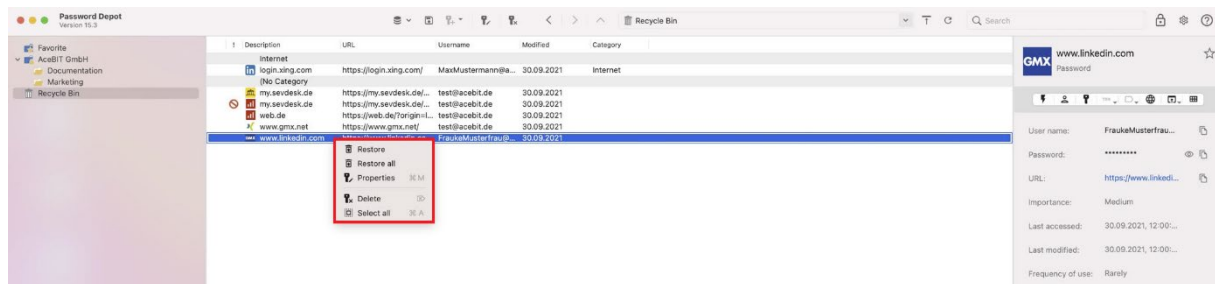


Recycle Bin

The recycle bin is located in the navigation area on the left below your database tree. You can adjust the recycle bin settings in the [Database properties](#).

If you select objects from the recycle bin and right click them with the mouse, different options will be available:

- **Restore**
- **Restore all**
- **Properties**
- **Delete**
- **Select all**



Objects which have been moved to the recycle bin can be restored again, if necessary. If you want to delete an object from the recycle bin permanently, please select **Delete** from the options above. Subsequently, Password Depot will ask you if the selected object should really be deleted permanently. Click **OK** if you want to continue or choose **Cancel** if you do not want to proceed.

If you want to delete or restore all objects located in the recycle bin at the same time, right click with your mouse on the recycle bin in the navigation area and either select “Empty Recycle Bin” or “Restore all”.

Database Import/Export

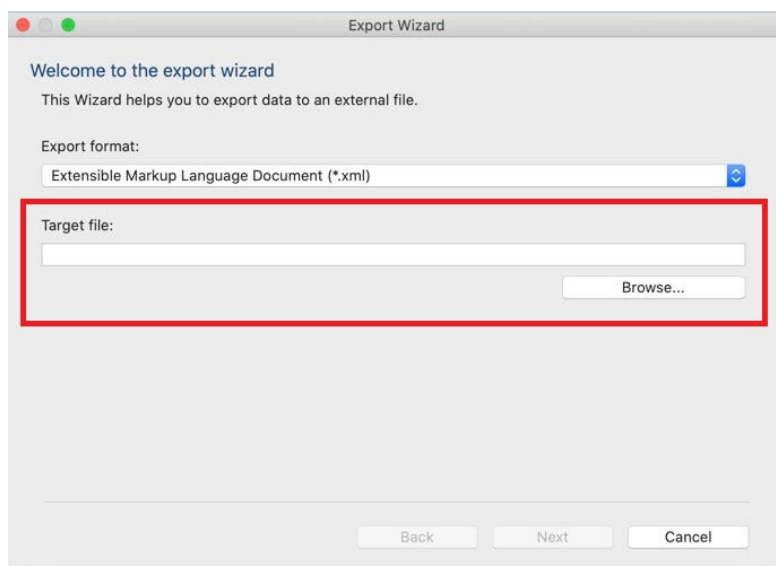
The menu item **Tools** includes options for exporting and importing whole databases as well as single entries or folders only. You can import data from an external file into Password Depot or export data from Password Depot into another file. Exporting and importing data is very useful, for example, if you would like to move entries from one database to another. Additionally, these options can also be helpful with regards to the interaction between Password Depot and other password managers.

Export

Go to **Tools -> Export** to start the export wizard.

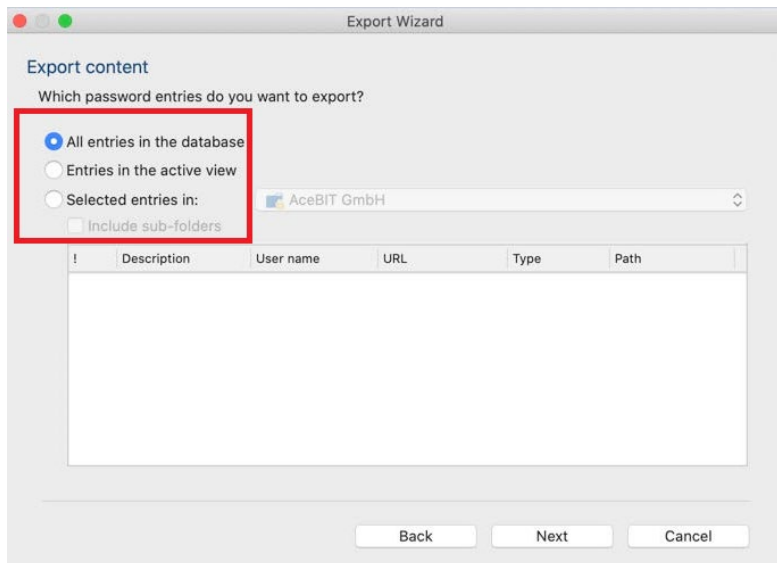
NOTE: It is only possible to use the **XML format** (Extensible Markup Language) for exporting your data as of the latest Password Depot macOS edition.

2. Next, you can see the **export format (XML)** first. Below that, it is required to enter a file name which you can do by using the **Browse** button. Additionally, you can also determine the location for storing the exported data:



WARNING: During export, your database will be saved unencrypted on your hard drive! Thus, it is highly recommended to delete the exported file from your hard drive permanently once the process has been completed.

3. Select **Next** to continue. You can determine the export content now:



TIP: If you choose the option **All entries in the database** you can select individual folders within your database for export and you can also determine further whether sub-folders should also be included.

4. Again, select **Next** to continue. The export wizard will now display the export result.

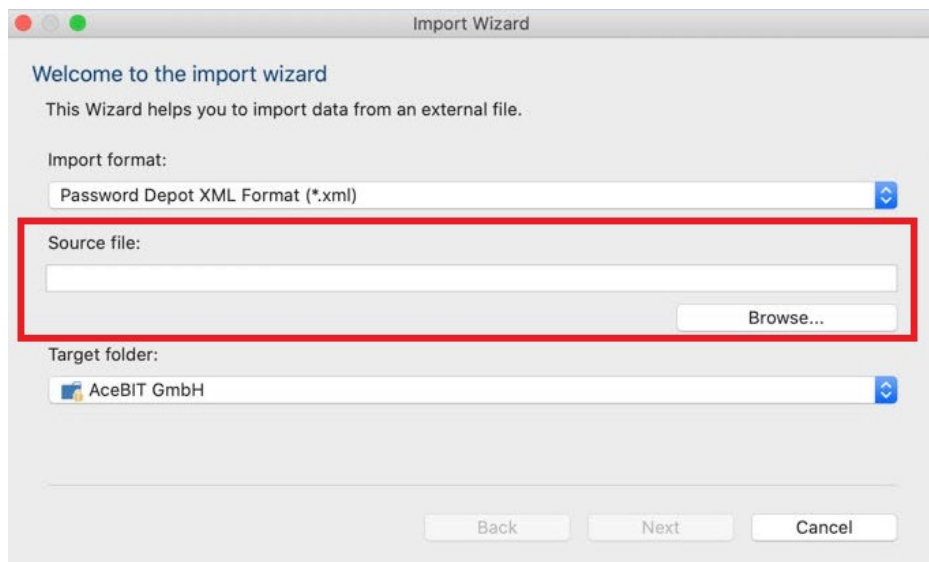
5. Lastly, select **Finish** to complete the process and close the export wizard.

Import

As mentioned above, the menu item **Tools** also includes the option for importing data that has previously been exported with Password Depot. This may be helpful if you would like to move entries from one database to another, for example.

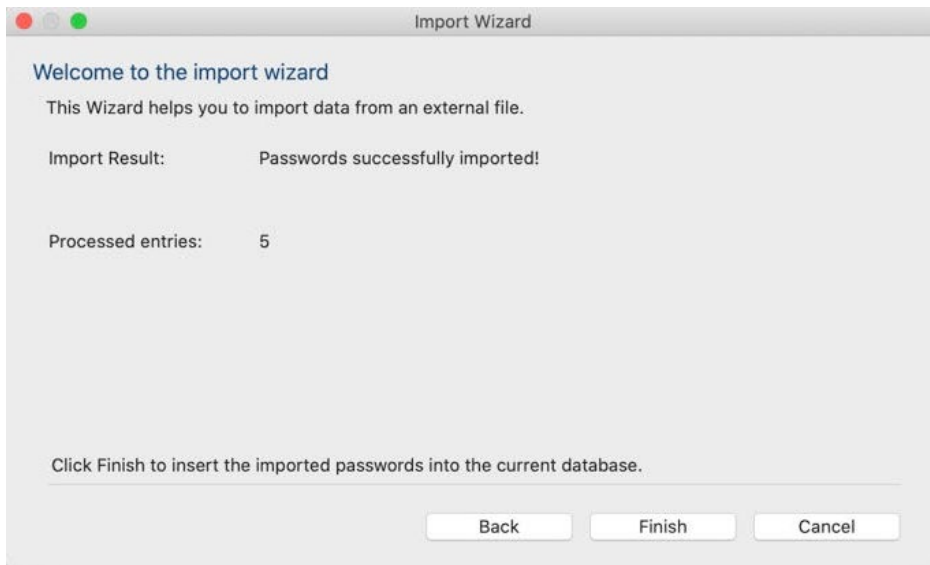
NOTE: As of the latest Password Depot macOS edition, you can only use the **XML format** (Extensible Markup Language) for importing your data.

1. Please go to **Tools -> Import** to start the import wizard.
2. Next, you can see the **import format (XML)** first. Use the **Browse** button below to enter the source file which should be used for importing your data:



In the **Target folder** area, you can select the corresponding folder within your database from the drop-down menu for importing the entries. By default, the database's **root directory** is preselected.

3. Select **Next** to continue. The import wizard will now display the import result:



4. Finally, select **Finish** to complete the process and close the import wizard. The new entries have been added to your database.

Database Properties

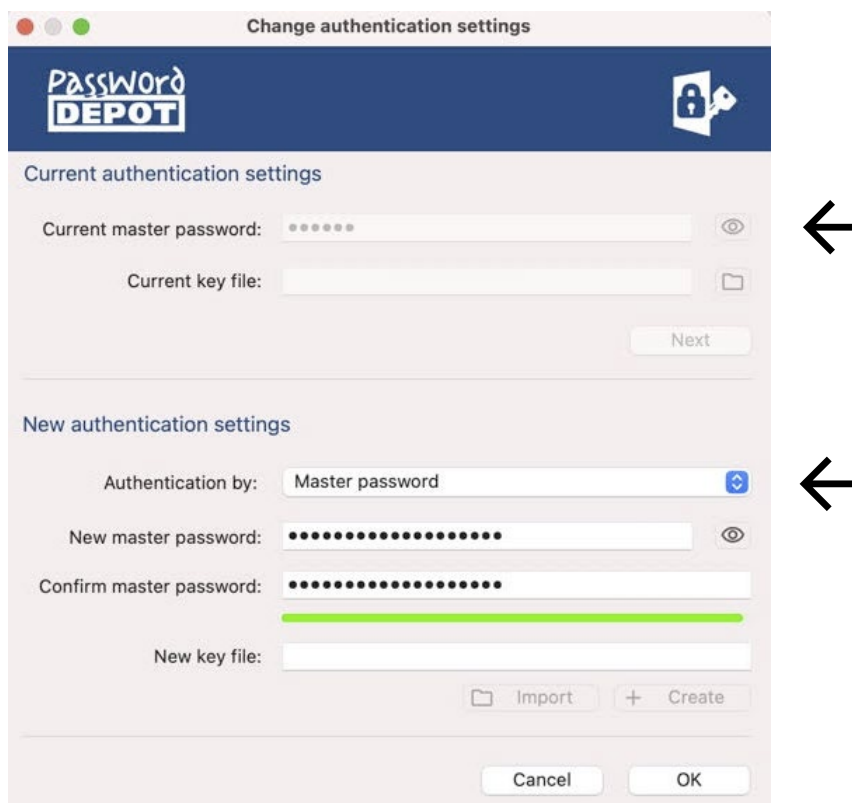
You can open the **Database Properties** by clicking **Database -> Database properties**. However, this is only possible if your database is open.

The database properties include the following:

- **File name**
- **Location**
- **Size**
- **Contains (number of folders and entries)**
- **Last modified**
- **Authentication**
- **Recycle bin settings**
- **Comments**
- **Hint**

In the database properties window, you can set the following options:

Authentication: You can see here the current authentication which has been selected for your database. If you want, you can change it here. To do so, click **Change**. Before selecting a new authentication and entering new data, you will be asked about your current authentication first. After entering the correct data, you can determine new authentication settings next:



Recycle Bin settings: Here, you can adjust the settings for deleting entries and decide whether you want them to be deleted immediately or if such entries should be moved to the recycle bin first before deleting them permanently. Entries from the recycle bin can be restored again if necessary. Furthermore, you can also define the maximum number of objects in the recycle bin here. By default, the number is set to 1000.

Comments and Hint: In the **Comments** field, you can add any additional information referring to your database or edit existing comments. In the **Hint** field, you can see whether you have stored a hint about your master password of this particular database. In case you forget your master password, a hint can help you remember it so that you will still be able to open your database. You can edit the hint field here, too.

- **Starts the auto-completion process (F6):** Select the lightning icon if you want to automatically insert your data on a website. You can learn more about this feature in the chapter [Auto Complete](#).
- **Restore:** Switch back to full-screen mode.
- **Lock:** Lock Password Depot. Your database will be locked immediately, and Password Depot will be minimized. If you want to access your data again, first you will have to authenticate correctly.
- **Minimize:** You can minimize Password Depot to the Dock, for example, if you do not need it but also do not want to close it. Click on the minimized Password Depot in the Dock again to switch back to topbar mode.
- **Exit:** Exit Password Depot. Both your database and the application will be closed subsequently.

NOTE: You can also move the topbar on your screen. To do so, place the mouse on the topbar and drag it to the desired position on your screen.

Entries

Create New Entry

As soon as you have created a new database or opened an existing one, you can add **new entries**. To do so, please proceed as follows:

1. Click on the **key icon** with a **plus** in the database's toolbar or click on the small arrow next to it.
2. Now, select the desired **type of entry**. Apart from the common password entry you can also choose from other types of entries, such as **credit card, software license, identity, information, TeamViewer, Remote Desktop Connection** etc.


NOTE: If you short click on the icon for creating new entries, the program will automatically choose the entry type **Password**. If you press the button for longer, a drop-down menu will open, and you can choose the desired type of entry.

3. Fill in all necessary/desired fields. The **Description** field is mandatory, and you need to enter some data. All other fields are optional. This applies to **all** types of entries.
4. Next, select **OK** to save and add this new entry to your database. Select **Cancel** if you do not want to save anything.

Depending on the type of entry selected, different tabs are available for entering additional information, if required:

General: You can add **general information** about the corresponding entry here, for example its description, the matching URL, category, expiration date and importance etc. Additionally, you can enter your **username** and determine the **password** for this entry. The options username and password are included in **Password, Remote Desktop Connection, TeamViewer, and PuTTY Connection**.




URLs: Here, you can add the URL of a website which you would like to use for login with your username and password.

- **Default URL/File:** Please enter the correct and exact address of the corresponding URL. Apart from that, you can refer to a certain file by using the **browse button**. Select the option **Open URL in browser**  to open the corresponding URL in your browser directly or to directly open a file.

- **Associate the entry with following URLs and Templates:** Here, you can add individual forms with placeholders (*).




Additional: In this tab, you can adjust the settings regarding auto fill of your data on websites. Specify the parameters to be used when opening a local executable file or saved document. Compose an auto-complete sequence which should be used for this special entry to fill in your credentials on the corresponding website. By default, this sequence is **<USER><TAB><PASS><ENTER>**. Furthermore, you can also use this tab to encrypt the corresponding entry with a second password. This may be useful when working with the Enterprise Server since it gives you the possibility to encrypt important passwords or entries with an additional second password.

Custom Fields: Custom fields allow you to create your own customized fields for entries and define their values:

- + Create a new custom field. Both fields “Name” and “Value” are mandatory.
-  Edit/Modify an existing custom field.
-  Delete a custom field.
-  Select a custom field from the list and change its current position by using the up and down arrows. This way, you can create a custom sorting for your list of custom fields.

TIP: By clicking on the eye icon at the bottom on the right, you can reveal a custom field’s value and see it in clear text. By default, a custom field’s value is hidden.

TANs: You can deposit TAN numbers associated with a password. For example, if you store your bank details in Password Depot, you can enter TAN numbers which you have received by your bank for certain transactions here.

- + Enter a new TAN number.
-  Edit an existing TAN number.
-  Delete an existing TAN number.
-  Select a TAN number from the list and change its current position by using the up and down arrows. This way, you can create a custom sorting for your list of custom fields.

TIP: By clicking on the eye icon at the bottom on the right, you can reveal a TAN value and see it in clear text. By default, a TAN value is hidden.

Attachments: Using this option, you can attach external documents to your database's entries, in case you want to store such external files with Password Depot.

+ Upload a new file.

× The attached document will be deleted.

↓ Extract the attached file to store it to your local system (or any other location of your choice outside Password Depot).

WARNING: We recommend not to attach too many files/documents to your database or password entries because this may reduce the performance of the program. Therefore, please use the entry type **Document** instead if you wish to add external files to your database.

TIP: Have a look at our latest [user manual for Password Depot 16](#) (Windows) and learn more about the above tabs, which have the same uses in the Windows version.

Arrangement of Entries

Regarding the arrangement of entries in the password area, go to the toolbar and select

View -> Group by

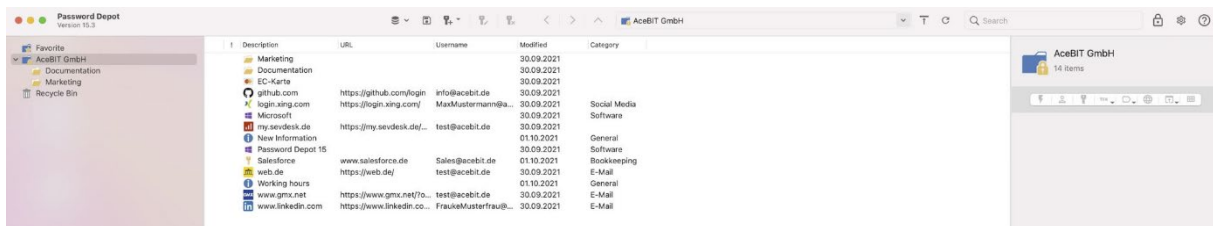
You can choose between the following options:

- **(None)**
- **Type**
- **Category**

Depending on the selected grouping the arrangement of entries will be as follows:

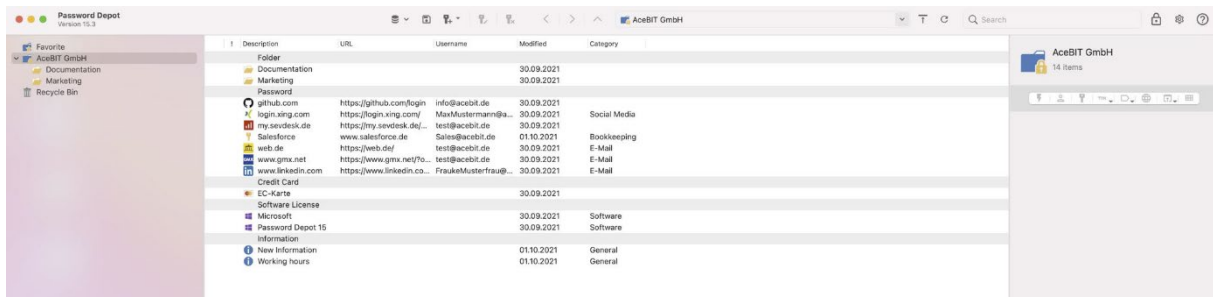
(None)

Your entries will be listed in the main view without grouping:



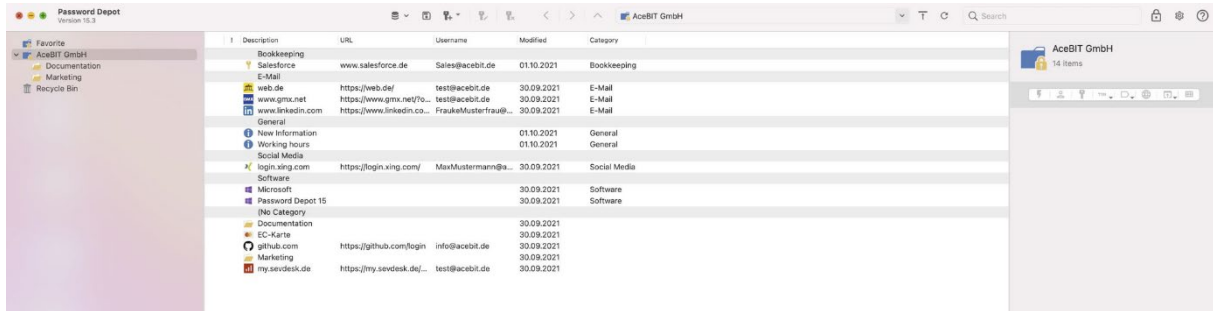
Type

With this grouping, the different types of entries and folders are divided into individual groups. In the password area, you can see that those individual groups are separated by a title describing which type of entry or folder is represented:



Category

Here, grouping depends on categories, which means that entries will be grouped by the categories you have assigned them to. For example, if you have assigned a piece of information and a password to the category **Internet**, those entries will be displayed together with the title **Internet** in your password list. Entries that do not contain a category will be listed with the title **(No Category)**:



Edit Entry

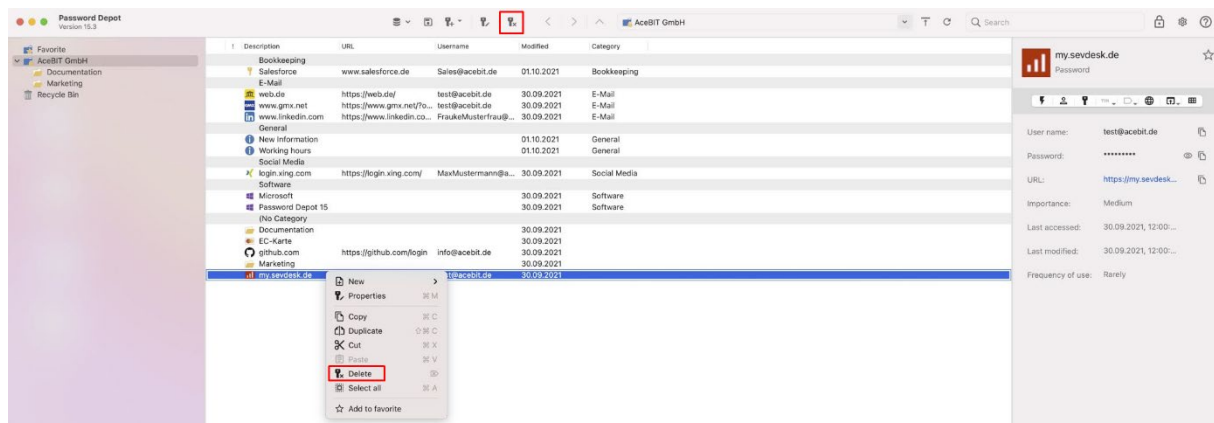
You can edit existing entries in your database at any time. To do so, please proceed as follows:

1. Open the **entry's properties** by double clicking on it.
2. Modify the entry.
3. Click **OK** to finish or **Cancel** if you do not want to save changes.

TIP: Alternatively, choose an entry from the list, select the key icon with the pen in the toolbar and modify the entry.

Delete Entry

1. Select an **existing entry** from the password area of your database.
2. In the database's toolbar, select the key icon for deleting entries or right click with your mouse on the desired entry and select **Delete** afterwards:

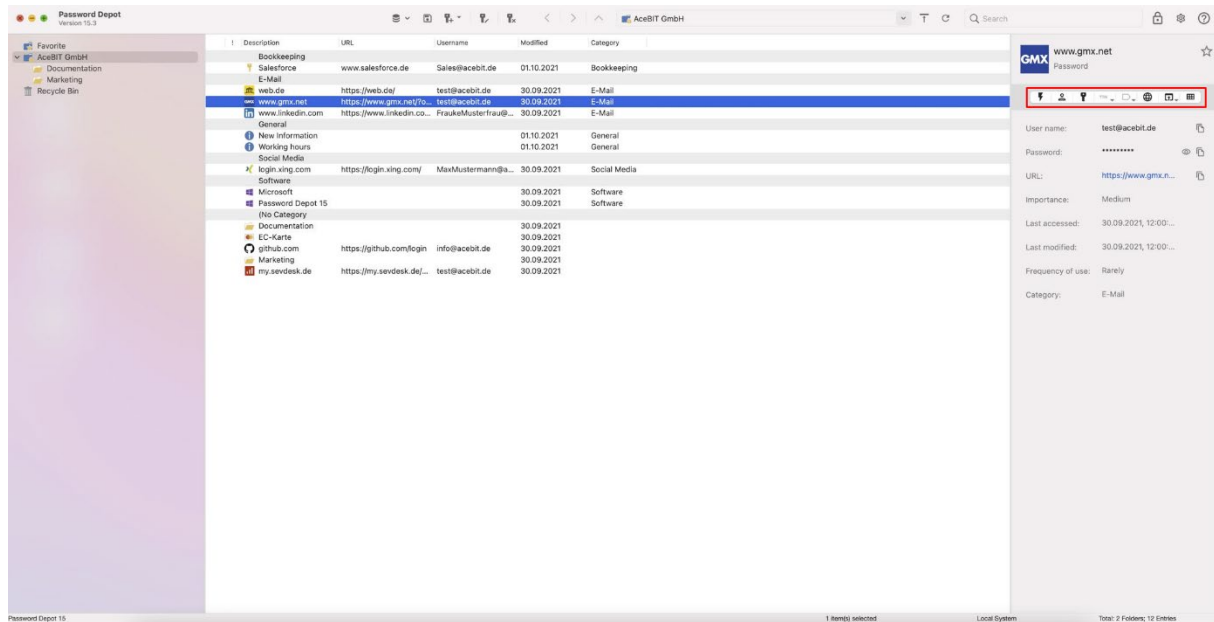


3. Depending on the recycle bin settings, the selected entry will either be deleted permanently or moved to the recycle bin. If the latter is activated, you can restore objects that have been moved to the recycle bin before. However, if this option is not activated, you will be asked to confirm before permanently deleting the selected object.

WARNING: If you have selected the option **Delete entries immediately** in the recycle bin settings, entries will be deleted permanently after confirming. In this case, it will **NOT** be possible to restore deleted objects, or any information connected to them.

Actions

Different actions are available for existing entries. In our Password Depot macOS edition, these actions are displayed in the **details area** on the right:



1. Open your database and select the desired entry.
2. Next, choose an action from the available ones:



Starts the auto completion process (F6): Open a URL in your browser first and click this icon next to automatically insert your login data on the website. Learn more about this feature in the chapter [Auto Complete](#).

Copy username: Copy the entry's username to the clipboard.

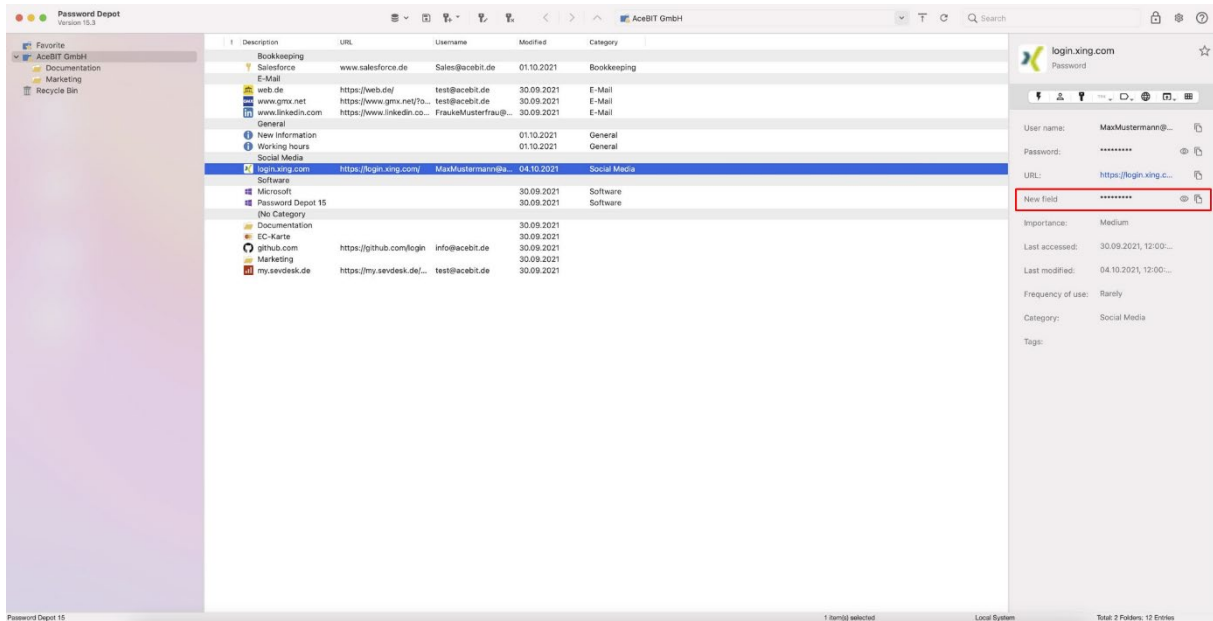
Copy password: Copy the entry's password to the clipboard.

TAN: Copy a TAN number to the clipboard.

Copy Custom Fields: Copy a custom field's value to the clipboard.

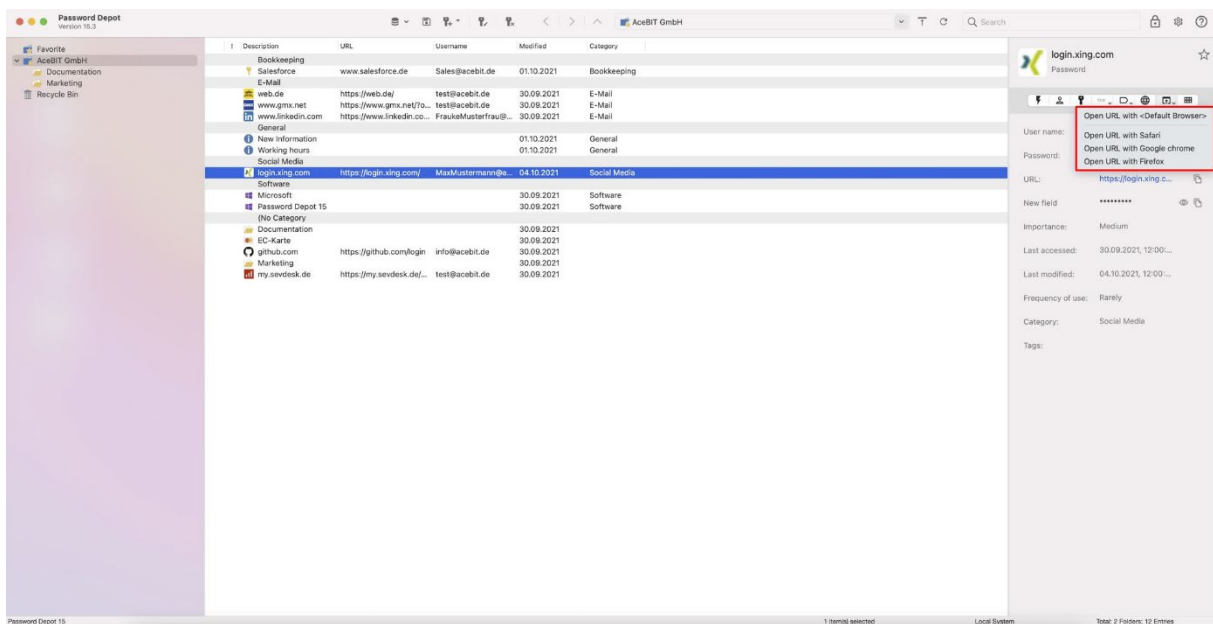
TIP: Custom fields are also displayed in the details area. Use the icon  to copy a custom field's value to the clipboard. When long pressing the icon , a custom field's value will be revealed, and you can see it in clear text.

Password Depot for macOS – Quickstart guide



Copy URL: Copy the entry's URL to the clipboard.

Open URL: Open the entry's URL in your browser directly. To do so, please select the desired browser from the drop down-menu:

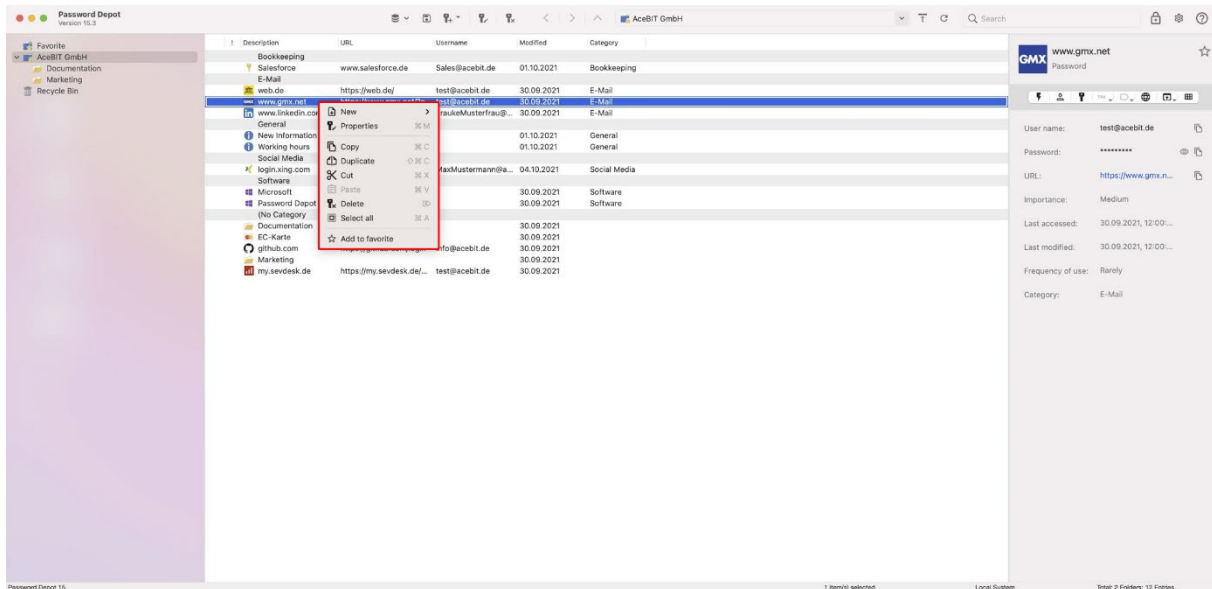


Partial Password: The method of using a partial password describes a way of authentication used for protection from stealing passwords. Users are asked to enter a few characters of a password only, that is, a segment rather than entering the complete password. This makes it difficult to retrieve a password using common hacking techniques such as keylogging.

Password Depot for macOS – Quickstart guide

NOTE: If one of these actions cannot be selected, you probably did not add any information/data for the desired action to the entry's properties. For example, if the action **Open URL** cannot be selected here, no URL has been stored for the corresponding entry.

TIP: You can call up additional actions by right clicking on the desired entry with your mouse:



New: Create a new entry and add it to your database.

Properties: Open the properties of the selected entry.

Copy: Copy the selected entry to the clipboard. Any information connected to it will also be copied.

Duplicate: Duplicate the highlighted entry. The duplicate will be added to your database immediately.

Cut: Cut the selected entry and any information connected to it.

Paste: Paste an object that has been cut before to your database.

Delete: Delete the selected entry. Any information connected to it will also be deleted.

Select all: All objects/entries within your database will be selected. By right clicking again, you can carry out further actions, for example deleting or copying all selected objects.

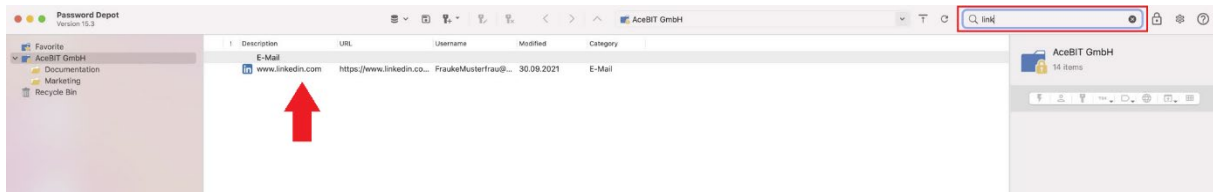
Add to favorite: Add the selected object/entry to the **favorites** folder which is located in the navigation area at the top (above your database's root directory).

HINT: If you add an entry to the favorites folder, it will be displayed with a red flag in the password area.

Search

The **search box** is available in the toolbar right above the details area. You can also use the keyboard shortcut **command + F**. Additionally, search is also available in the menu bar under **Search**. You can use this option to search for entries within your database.

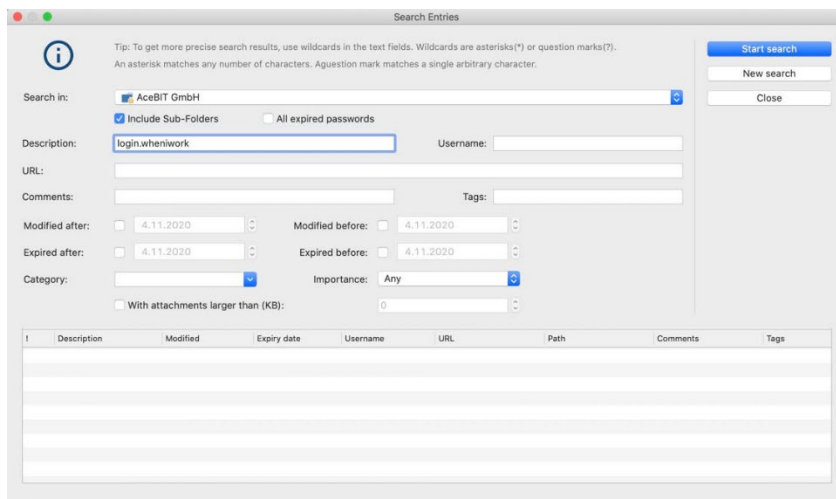
To start a search, please enter a search term or keyword into the search box. Password Depot will start the search while you type and display the results subsequently:



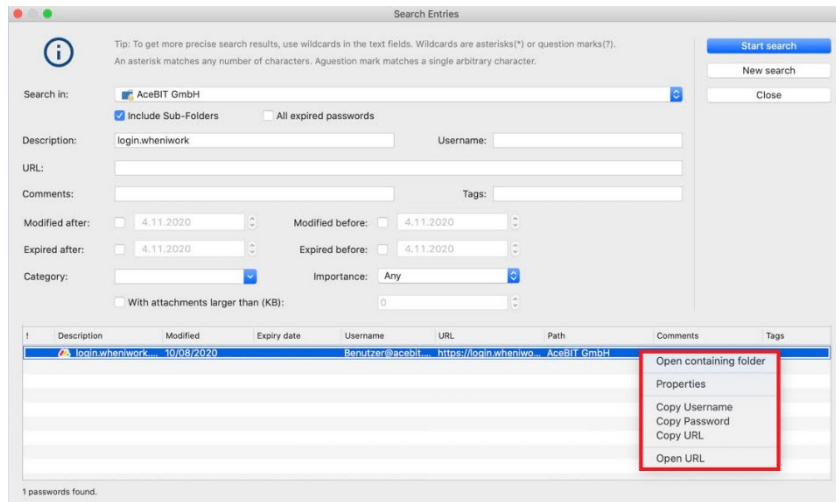
Once you have found the desired entry, double click on it and you will be forwarded to its corresponding folder or sub-folder. If you double click on it again, you can open its properties and edit it.

Advanced Search

With the **Advanced Search** (keyboard shortcut: **command + Shift + F**) you can specify the search in your database based on various criteria (description, username, URL, tags, date of modification and expiration, category, importance etc.). Once you have set all necessary criteria, select **Start search** to start the process:



The search results will be displayed at the bottom of the dialog box. If the desired entry was found during advanced search, you can carry out further actions by right-clicking on the corresponding entry in the list of results:



You can choose from the following actions:

- **Open containing folder**
- **Properties**
- **Copy Username**
- **Copy Password**
- **Copy URL**
- **Open URL**

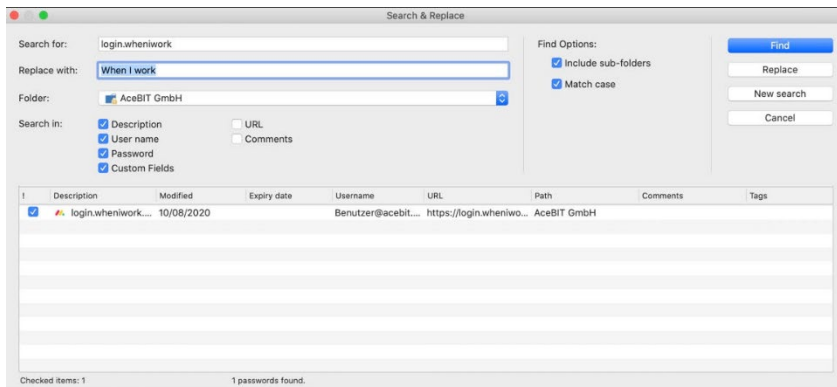
Search and Replace

Using the option **Search and Replace** (keyboard shortcut: **command + R**), you can search for a specific sequence of characters within your database and immediately replace it with another string of characters. To do so, please proceed as follows:

- **Search for:** Enter the string of characters you would like to replace.
- **Replace with:** Enter the new sequence of characters you would like to use in the future.
- **Folder:** Select the correct folder or sub-folder where search should be performed.
- **Search in:** Specify the fields which should be included during search.

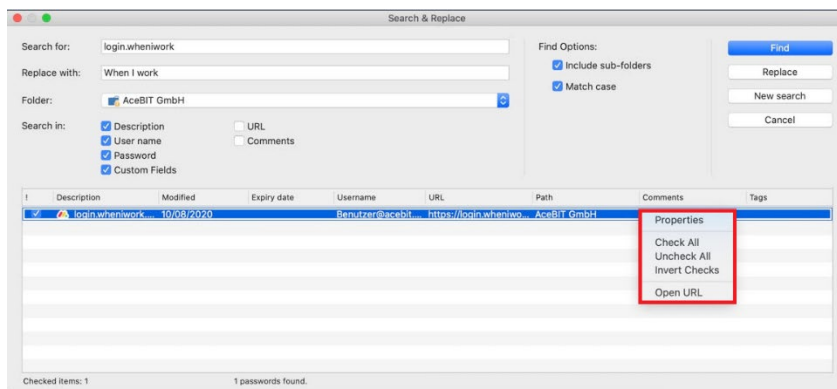
You can specify the search even more by selecting **further options** such as **Include sub-folders** or **Match case** which can be found next to the above-mentioned criteria.

Once you have set all necessary criteria, click **Find** to start the search. Select **Replace** to replace the old sequence of characters with the new one you entered into the field **Replace with**:



WARNING: The process of replacing a specific sequence of characters **cannot** be undone once performed. Thus, before starting the process, we recommend always checking carefully whether to replace a string of characters in your database.

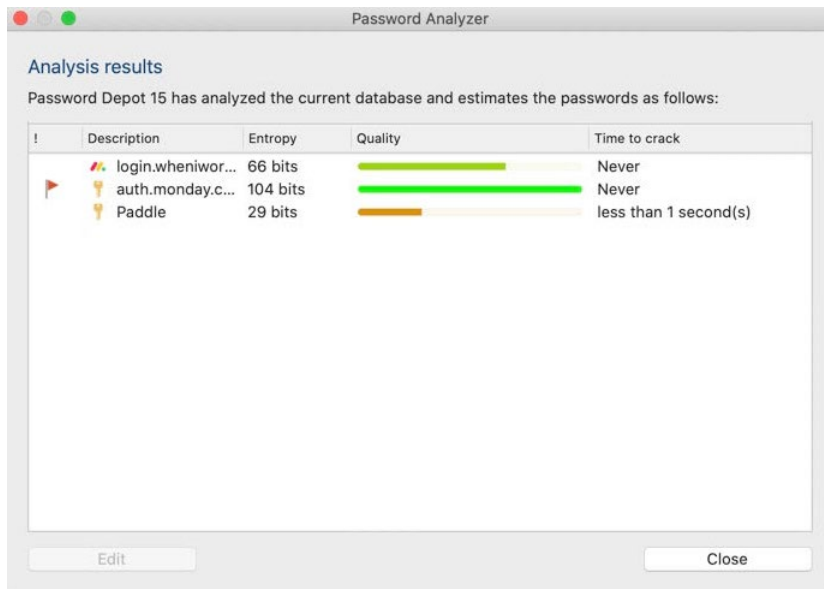
You can also right-click on a desired entry displayed in the list of results to perform further actions:



- **Properties:** Open the properties of the selected entry to modify it.
- **Check All:** Select all entries from the list of results.
- **Uncheck All:** Uncheck all the entries from the result list that have been selected before.
- **Invert Checks:** Uncheck all the selected entries and select all unchecked entries from the list.
- **Open URL:** Open the entry's URL in the browser.

Analyze Entries

This option is available for **analyzing passwords** and their quality. It can be found in the menu bar under **Tools -> Analyze**. Once the process of analyzing passwords has started, a new dialog window will be displayed showing the analysis result:



The password analyzer dialog window includes five different columns:

- **!** Shows a password's importance.
- **Description:** Here, you can see a password's description assigned by you when creating this entry.
- **Entropy:** Shows your passwords' strength in bits (unit). The higher the number of bits, the stronger the password.
- **Quality:** This column contains a colored bar indicating the passwords' quality by using different colors. The longer and greener or bluer the bar, the higher a password's quality. The latter depends on both a password's length as well as the different types of characters included. You can achieve highest quality and a maximum of security if your passwords consist of different types of characters as follows: lowercase and uppercase characters, numbers as well as special characters.
- **Time to crack:** Indicates how long it would approximately take to crack a password if a professional hacker attempted to do so (during brute-force or dictionary attacks). Please note that the time displayed is only an approximate value which, nevertheless, is calculated with specific algorithms and thus more accurate than many other methods found on the internet.

To improve a password's quality immediately, if desired, please select the corresponding entry from the list first and the button **Edit** next. Subsequently, the entry's properties will open, and you can

change the password accordingly. As an alternative, you can also double click on the desired entry being displayed in the list. The entry's properties will open, and you can edit it afterwards.

Clean-up Entries

The **Clean-up** feature can also be found in the menu bar under **Tools**. You can use it to check if your database contains entries which have not been used for a long time or have already expired.

NOTE: Please make sure to always keep your database updated since unused and/or expired entries can overload the program and thus lead to problems concerning the database's runtime behavior.

You can set different filters to find the required entries for clean-up:

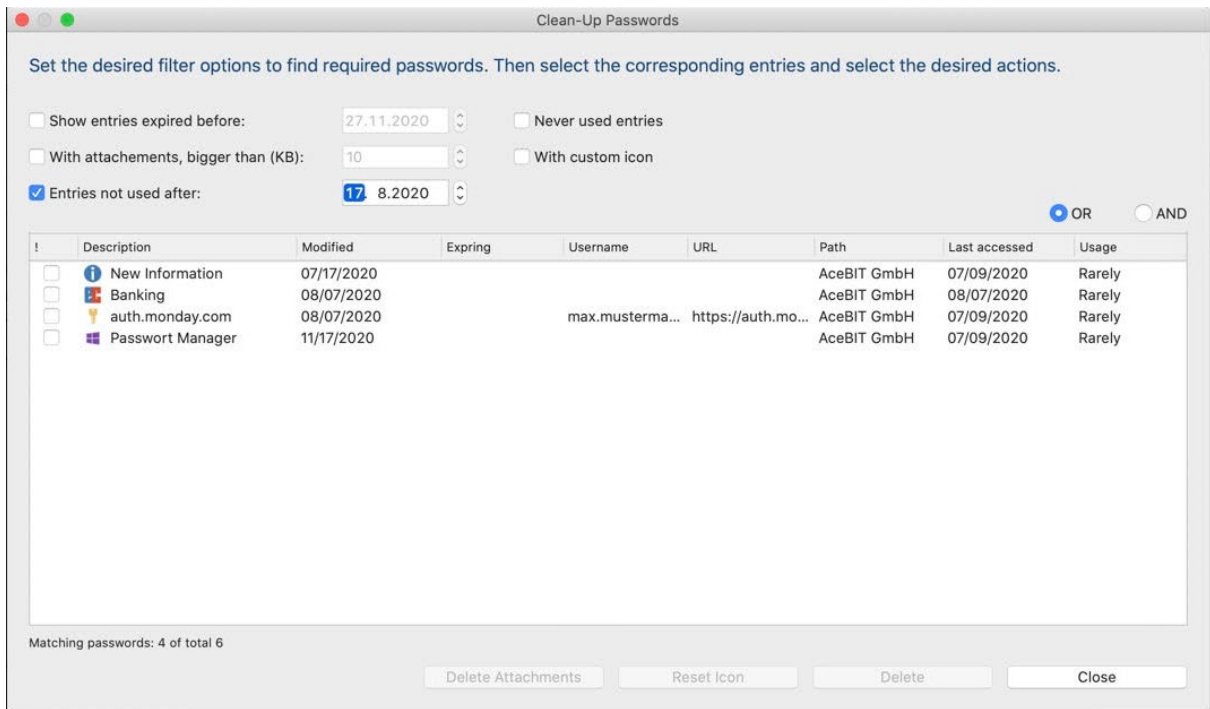
- **Show entries expired before:** Shows all entries which have already expired before a specific date.
- **With attachments, bigger than (KB):** Shows all entries with an attachment bigger than the number of KB entered. This option is helpful to quickly find entries with large attachments which might cause a delay when loading your database.
- **Entries not used after:** Shows all entries which have not been used since the day entered.
- **Never used entries:** Shows all entries which have never been used since creating them.
- **With custom icon:** Shows all entries containing a custom icon which have been assigned by the user himself.

NOTE: Additionally, you can also use the options OR/AND to either start the search for entries according to the filter options separately or to consider every single filter option set for each entry.

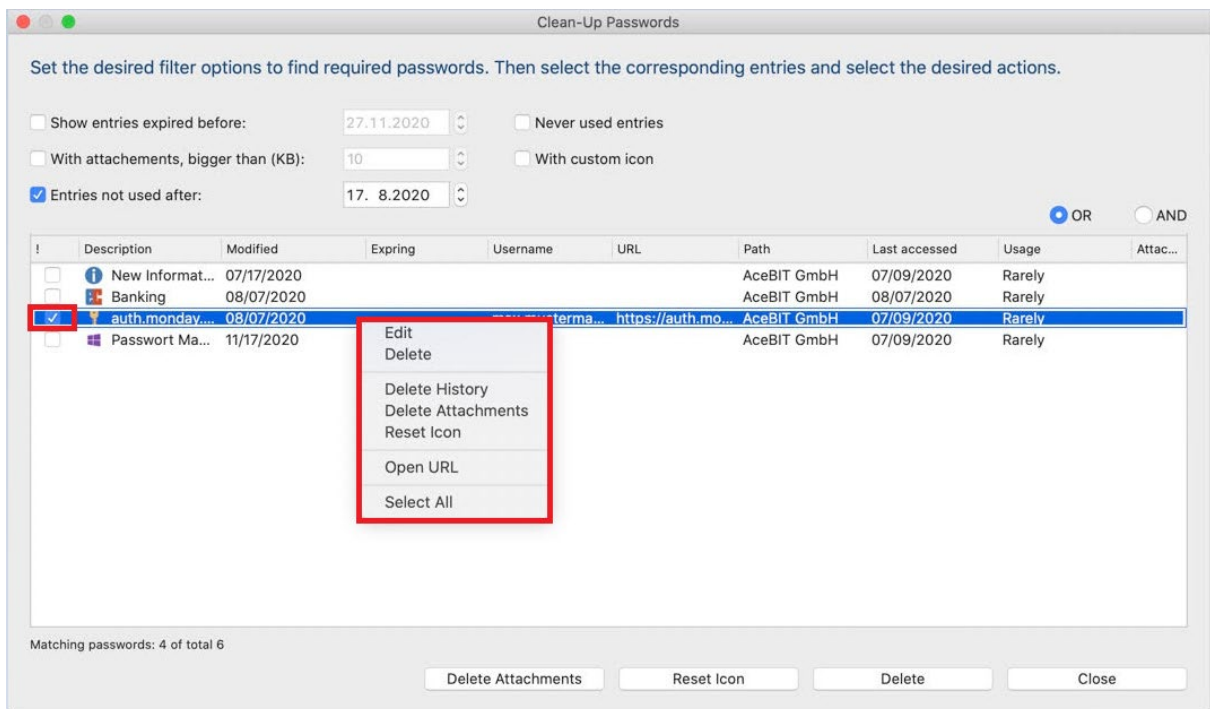
Once all filter options have been set and search has been started, all entries which meet the criteria entered will be displayed in a list of results. In addition to that, further information about each entry is available as follows:

- **Importance**
- **Description**
- **Modified**
- **Expiring**
- **Username**
- **URL**
- **Path**
- **Last accessed**
- **Usage**
- **Attachments**

Password Depot for macOS – Quickstart guide



You can now check the desired entry and right click it with your mouse. The following actions will be available next:



- **Edit:** You can open the entry's properties to edit it.
- **Delete:** Delete the selected entry if you do not need it anymore, for example. Depending on the recycle bin settings, the corresponding entry will either be moved to the recycle bin first or deleted permanently.

- **Delete History:** Delete the entry's history.
- **Delete Attachments:** Delete all attachments of the entry selected.
- **Reset Icon:** Reset the entry's custom icon to the default one (e.g., the key symbol for passwords).
- **Open URL:** Open the entry's URL in your browser.
- **Select All:** Check all entries displayed in the list of results. This may be helpful if you would like to perform the same action with several entries at the same time, for example, deleting those entries in one step if you do not need them anymore.

Finally, select **Close** to finish the clean-up process.

Search for Duplicates

This option is also available in the menu bar under **Tools**. You can use it to check if your database contains duplicated entries. You can search for duplicates using the following criteria:

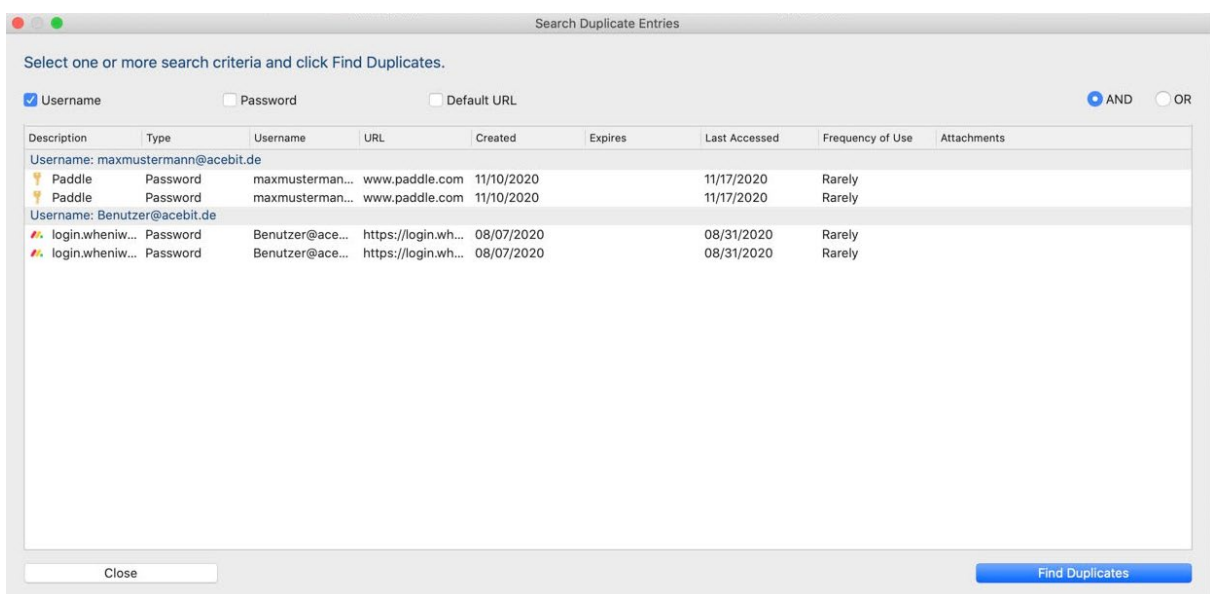
- **Username**
- **Password**
- **Default URL**

Whereas the same username is often used for more than one entry (e.g., because it is your email address) and the same URL may also be used twice (e.g., if you have several accounts on one website), we strongly recommended not using the same password for different accounts. Thus, the **Search for Duplicates** feature is very helpful to find out about entries within your database using the same password.

You can use different filters when searching for duplicates within your database. In addition to that, you can also check OR/AND if you want to either consider the selected filters separately or all together.

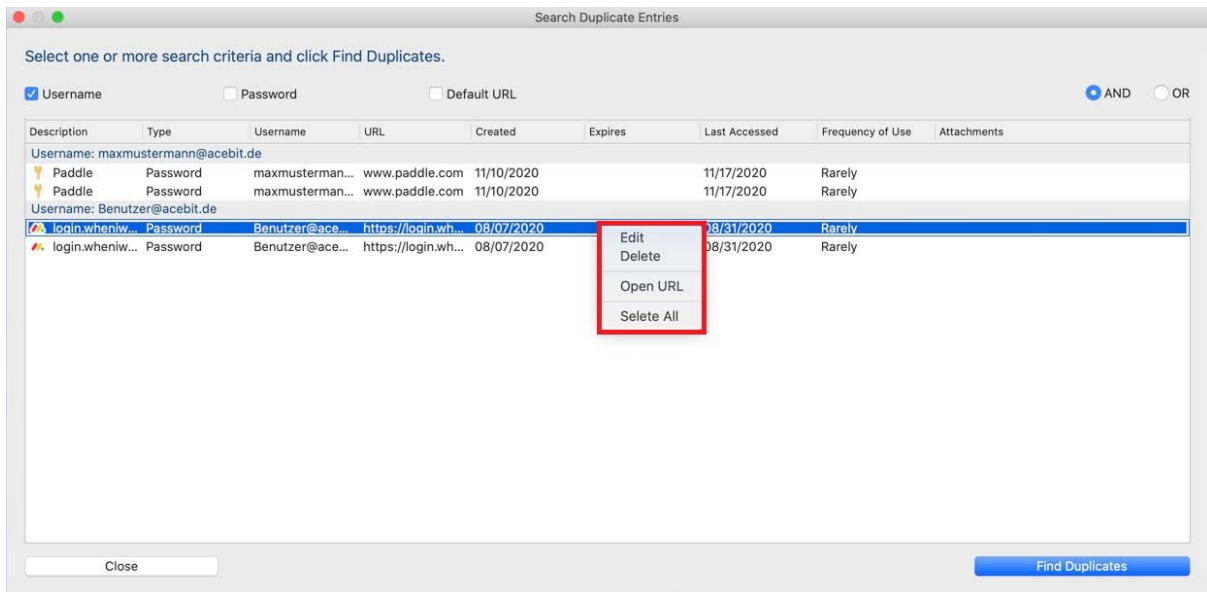
Click **Find Duplicates** to start.

The results will be displayed and grouped together according to the previously selected criteria and operator:



Password Depot for macOS – Quickstart guide

If you want to proceed further, you can right click with your mouse on the desired entry displayed in the list of results. Choose from the following actions:



- **Edit:** Open the entry's properties to modify them.
- **Delete:** Delete the selected entry from your database. Depending on the recycle bin settings, the corresponding entry will either be moved to the recycle bin first or deleted permanently.
- **Open URL:** Open the entry's URL in your browser.
- **Select All:** Check all entries displayed in the list of results. This may be helpful if you would like to perform the same action with several entries at the same time, for example, deleting those entries if you do not need them anymore.

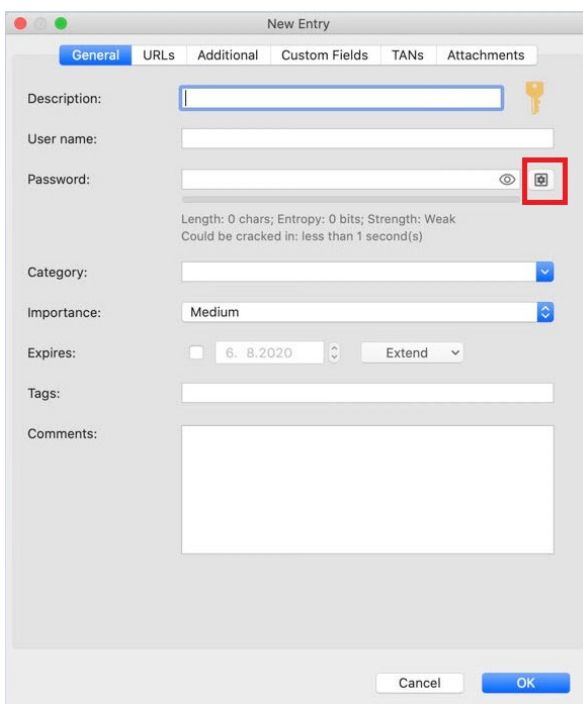
Password Generator

Like all other editions of Password Depot, the macOS edition also includes an integrated **Password Generator** which can be used for creating **secure passwords**. For example, you can generate a secure password when first adding it to your database. Alternatively, you can also benefit from the password generator if you want to change an existing password within your database and wish to add a secure one. To use the password generator, please proceed as follows:

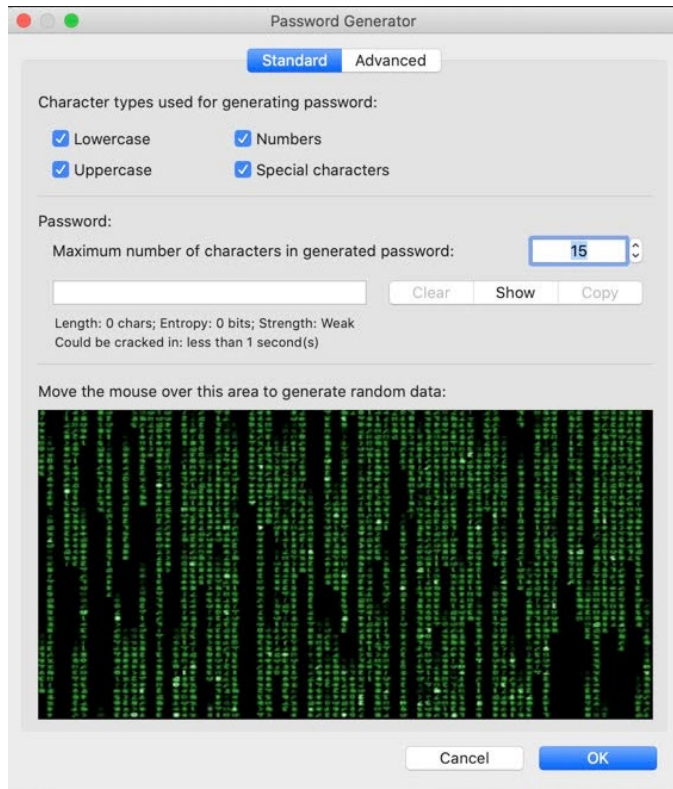
1. In the database's toolbar, select the key icon for creating a new entry and choose the type of entry **Password**. Alternatively, double click on an existing password entry in the password area. The entry's properties will open.

NOTE: The password generator is also available for the following types of entries: **Remote Desktop Connection** and **TeamViewer**.

2. Next to the password field, you can see the following icon:



3. Click the icon and the **Password Generator** will open.



4. Move the mouse over the area to generate random data. You can see how data is entered into the corresponding field subsequently.
5. If you want to save the generated password, select **OK**. Next, the newly created password will be entered in the corresponding field in the password's properties. Select **Cancel** if you do not want to save it. You will be forwarded to the entry's properties and the generated password will not be saved or entered here.

Password Generator – Settings

The Password Generator includes two tabs:

- **Standard**
- **Advanced**

In these two tabs the settings can be adjusted as follows:

Standard

Character types used for generating passwords: Here, you can determine the character types which should be included in every generated password by default. To create secure passwords, it is recommended to use all offered character types.

Maximum number of characters in generated password: Determine how many characters a generated password should have at most.

Clear/Show/Copy: Using this button, you can either delete or copy the generated password or show it in clear text.

NOTE: Below the password field, you can see additional details regarding the length and strength of the password. Please note that this is only supposed to be a guideline helping you to create strong passwords.

Advanced

You can further specify the password generator's settings in this tab. This may be helpful, for example, if you need to set up special password policies for individual entries that should only refer to these. Thus, you can create special password policies for specific entries only which may be different from the database's default password policies.

Use following characters: Here, you can enter any characters you want and thus determine that only those characters will be used by the program when generating new passwords.

Use following character types with relative frequencies: By default, all character types are checked, and the password generator uses all selected types of characters with relative frequencies when creating new passwords.

Custom: Add more character types to be used by the password generator when generating new passwords (apart from the default character types).

Password length: Determine the length of generated passwords.

Password Generator: You can also create a new password using the separate **Password Generator** at the bottom of the **Advanced** tab. This generated password will correspond to the settings/policies you defined in the same tab before. Using the buttons **Copy** and **Show**, you can either copy this password to the clipboard or show it in clear text.

If you generate a new password in the **Advanced** tab, click **OK** and the new password will be entered into the password field. You will be forwarded to the password's properties next.

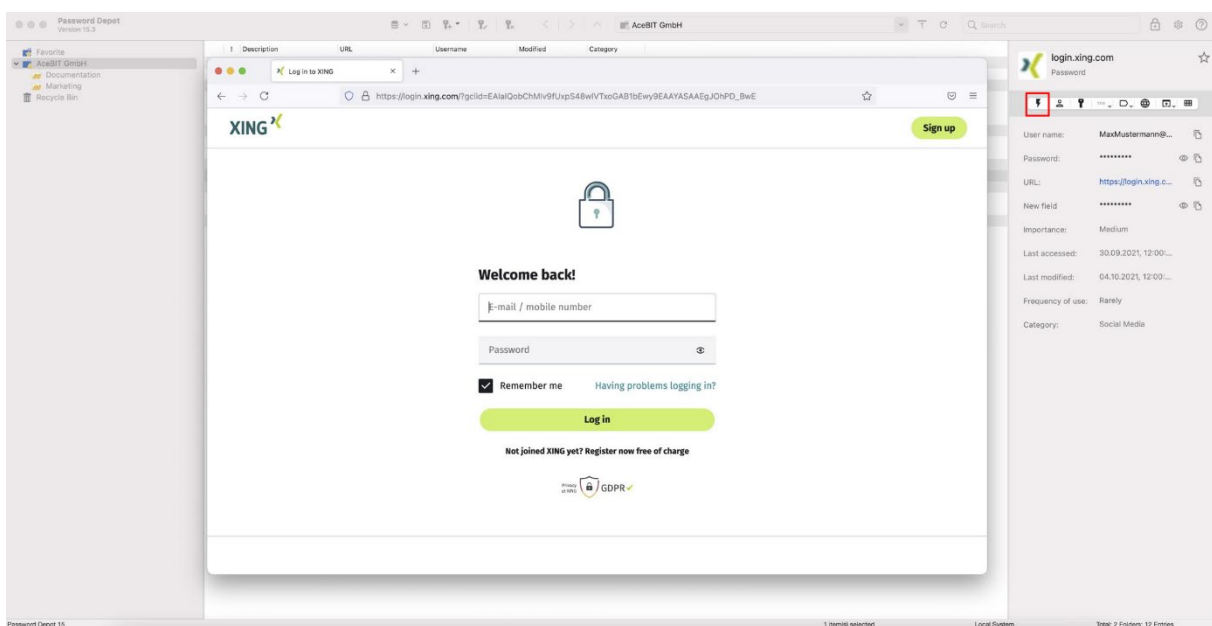
NOTE: Normally, the additional settings in the **Advanced** tab for generating new passwords are not necessary. However, they may be helpful if special policies, deviating from the database's default password policies, are required for individual entries. Thus, you can change the database's default password policies temporarily without the need of changing them permanently.

Auto-Complete

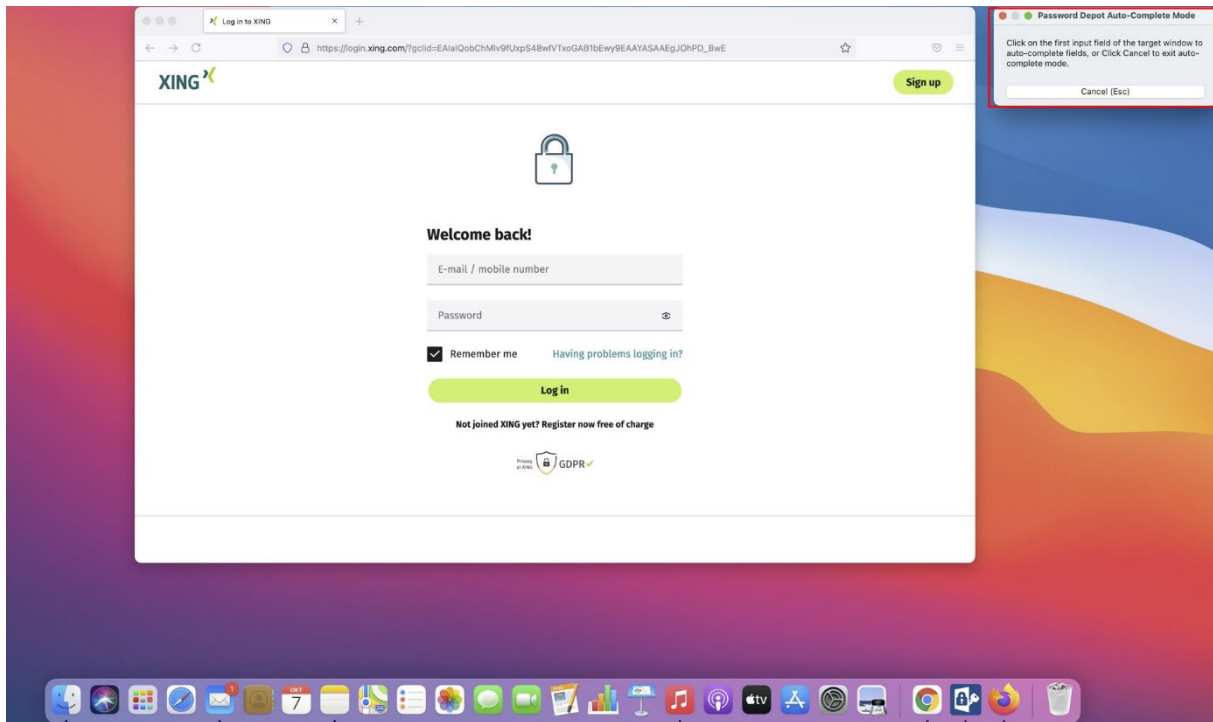
Using the Feature “Auto-Complete (F6)”

If you open a URL in your browser which you have also stored to Password Depot and assigned to a specific entry within your database, you can use the **Auto-Complete (F6)** feature, the so-called “lightning icon”, to automatically enter your access data on the corresponding website. The login will then happen automatically. Thus, you do not have to enter your data manually and you can make sure to transfer your username and password safely using Password Depot. To start the auto-complete process, please proceed as follows:

1. Open the corresponding URL in your browser.
2. Go back to Password Depot afterwards and search for the correct entry.
3. Select the entry, go to the details area on the right and click the lightning icon:



4. Password Depot will minimize, and you will see a small dialog window called **Password Depot Auto-Complete Mode** at the top on the right of your screen:



5. Left click with your mouse on the website's first login field (usually the field for the username). Password Depot will then insert your data and you will be signed in automatically.
6. Select **Cancel** if you do not want to proceed and insert your data automatically.

Using the Browser Add-ons

With Password Depot for macOS, you can also use the browser add-ons to insert your access data on websites automatically. The browser add-ons can transfer your data to a webform automatically. It is also possible to add new credentials to your database from a website automatically. Thus, you do not have to enter your credentials manually every time you want to log in, which saves time. In addition to that, using the Password Depot add-on for login does not put your data at risk. The browser add-ons are activated as soon as you launch the browser, and they start working as soon as you open a website which has been stored to your password file and connected to an entry.

However, you can only work with the browser add-on if it has been installed correctly in your browser. The Password Depot add-on currently supports the following browsers in macOS:

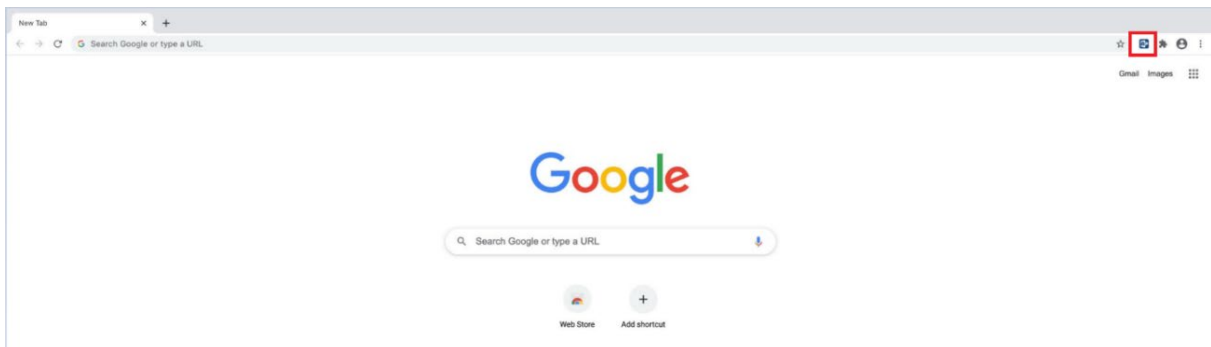
- [Google Chrome](#)
- [Mozilla Firefox](#)

Please note that the add-on is currently **not** available in Safari.

For installation, please choose one of the browsers listed above.

NOTE: For correct installation, it is required to open the link in the corresponding browser, that is, if you want to use and install the add-on in Google Chrome, you need to open the above link in Google Chrome, too. Otherwise, the installation will not work.

Once installation has been completed, the blue Password Depot icon will be displayed in your browser:



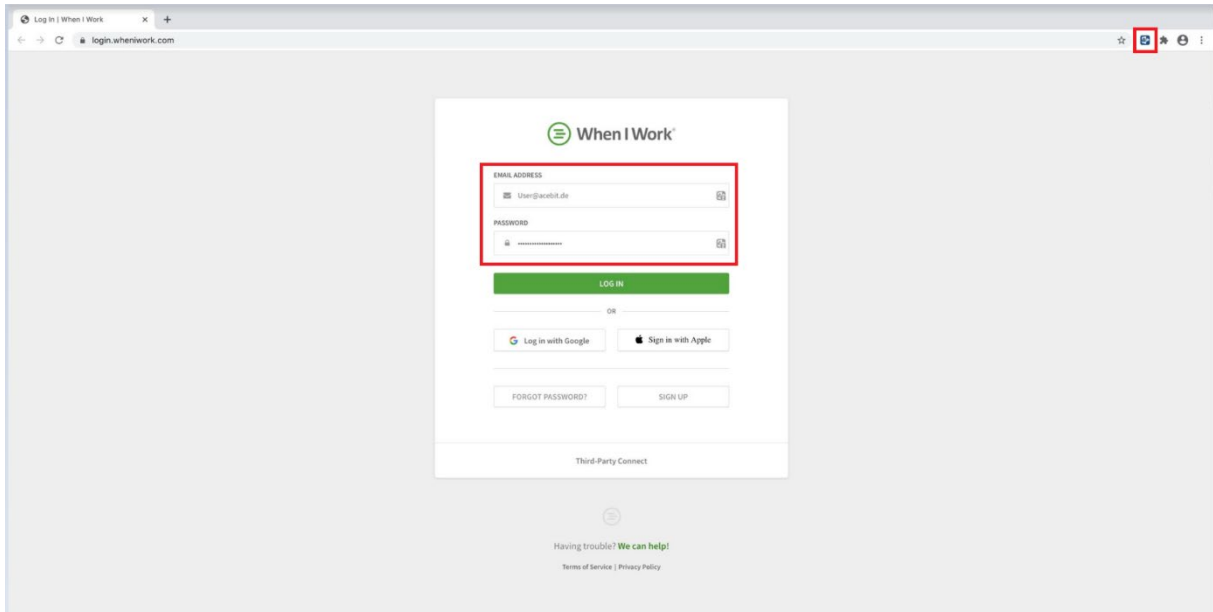
Example: The above picture shows the add-on in Google Chrome after the installation.

NOTE: Due to security reasons, it is required that Password Depot is working in the background if you want to use the add-ons.

Please also note that using the browser add-ons must be enabled in the preferences in the **Browser** tab. If you work with the Enterprise Server, auto-complete using the add-ons must also be enabled in the Server Manager by your server administrator.

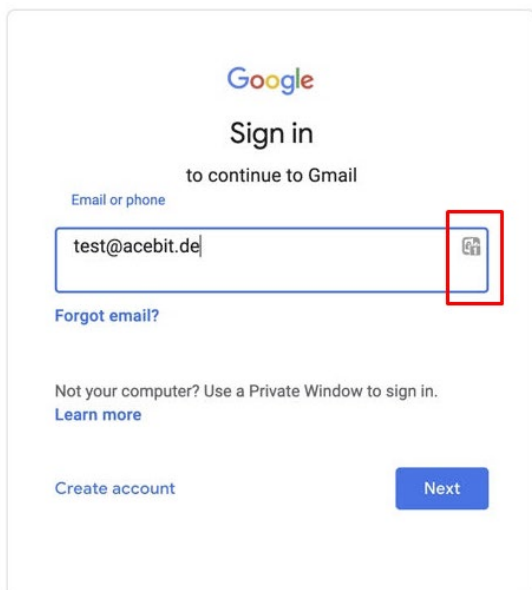
Autofill Access Data

If you have already added access data to your database and connected a specific URL to it, you can open the latter in your browser by using the option **Open URL**. The add-on will then insert your data automatically on the website:



Finally, select **Login** to finish and sign in.

TIP: To check if the add-on is working on a website, please have a look at the login boxes and see if the add-on icon is displayed there:

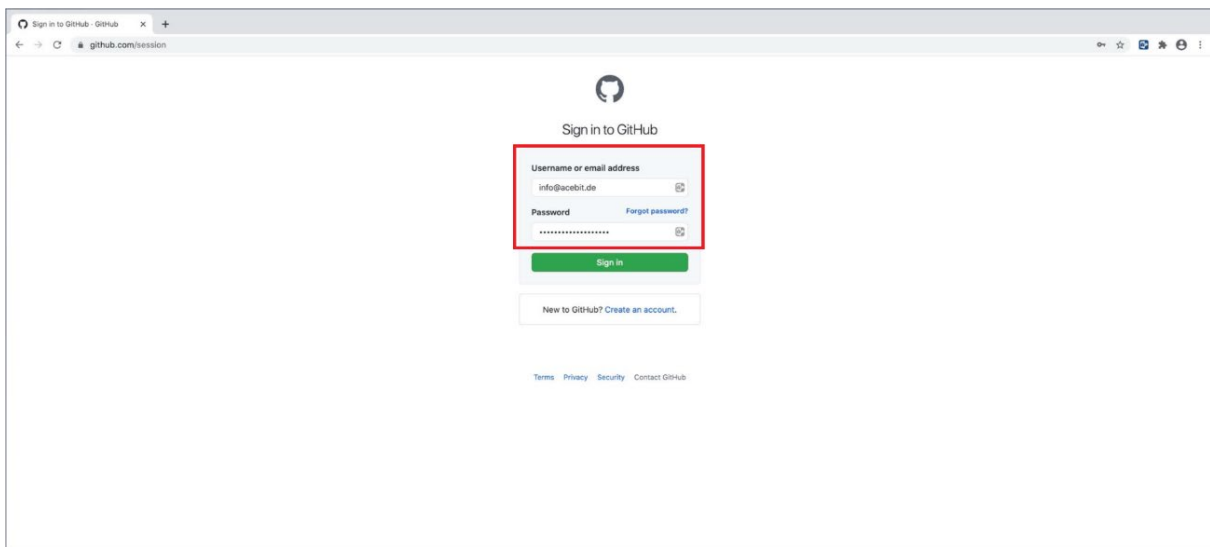


Password Depot for macOS – Quickstart guide

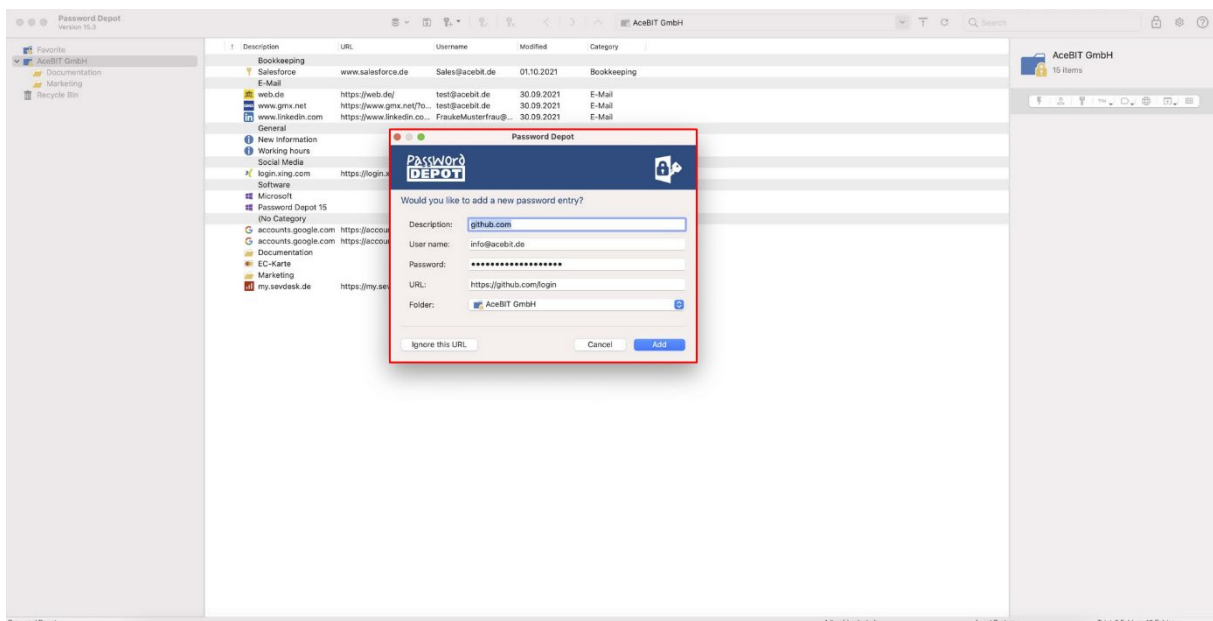
Add New Passwords from Web Browsers

You can also enter new login credentials on a new website manually and let Password Depot create a new entry within your database subsequently. This is a useful option since Password Depot adds the **username, password, and URL** for this new entry to your database automatically so that you do not need to create this new database entry yourself.

1. Open the corresponding URL in the browser and enter your access data:



2. Password Depot will recognize the credentials and ask if you would like to create a new entry and add it to your database:

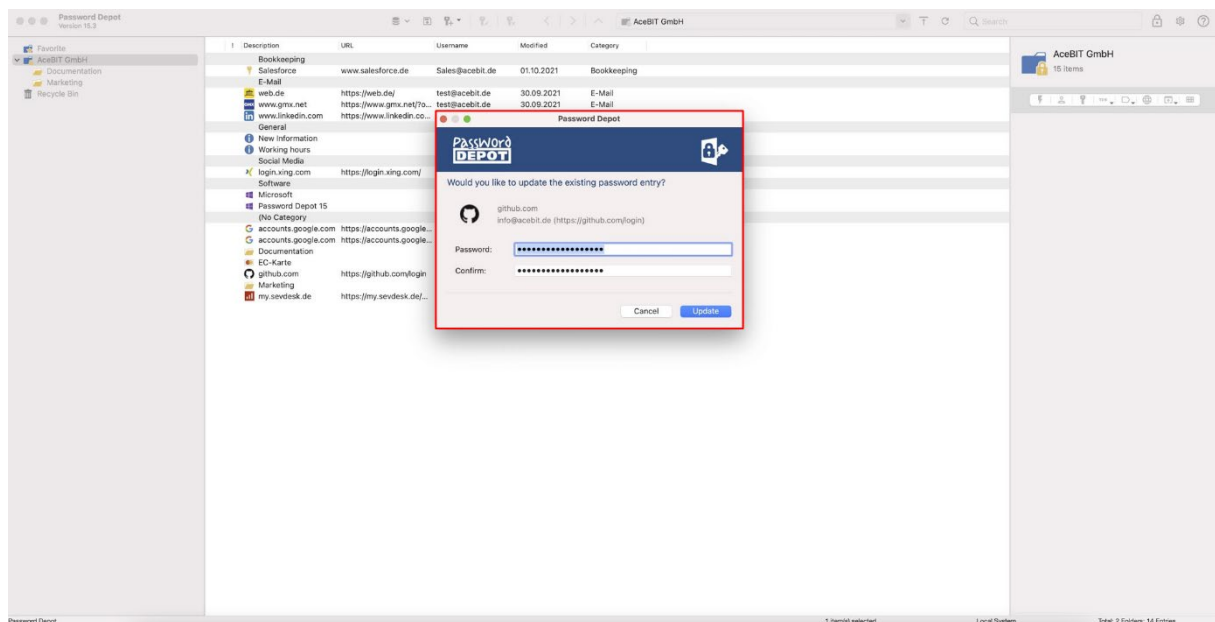


3. Select **Add** to confirm and add this new entry to your database. Select **Cancel** if you do not want to add a new entry.

TIP: By clicking the button **Ignore this URL**, the browser add-on will ignore this specific URL onwards and thus, auto-complete will not be carried out any longer when the website is accessed in your browser.

Update an Existing Password Entry

In case you need to update your login credentials and thus change them in your browser directly, you can add those changes to Password Depot immediately. The program recognizes that your database already contains an entry with similar data and will ask if you would like to update it as requested:



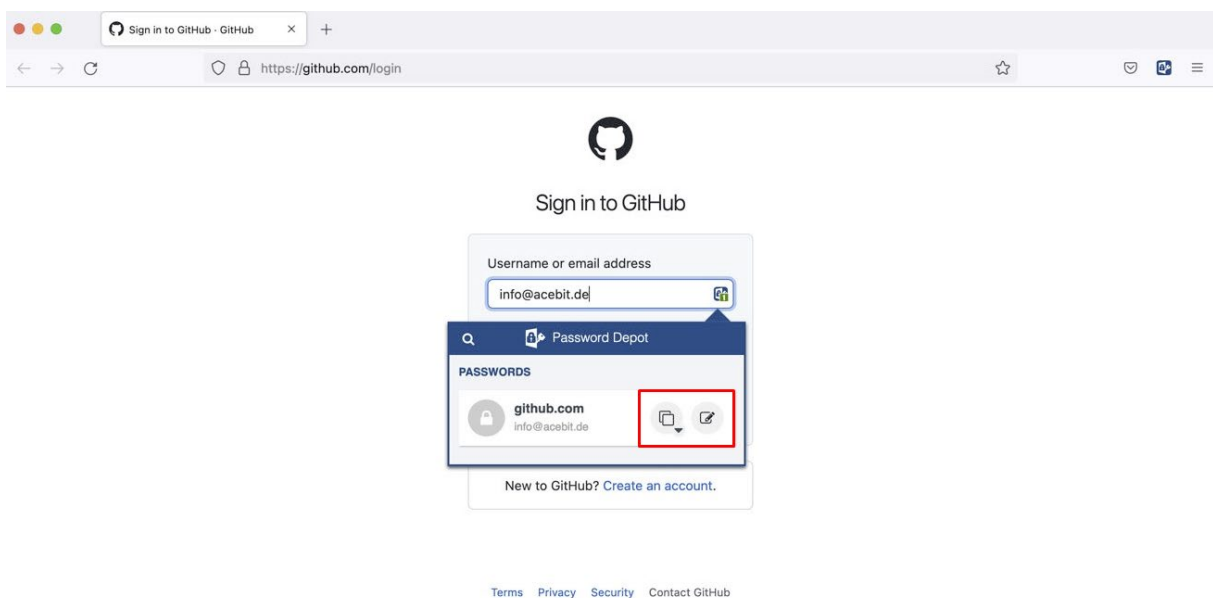
Select **Update** if you want to update the corresponding entry as requested or select **Cancel** if you do not want to save changes.



Additional Features

The current add-on provides even more options. Please read the information below carefully if you would like to learn more about them.

Available on the Corresponding Login Page

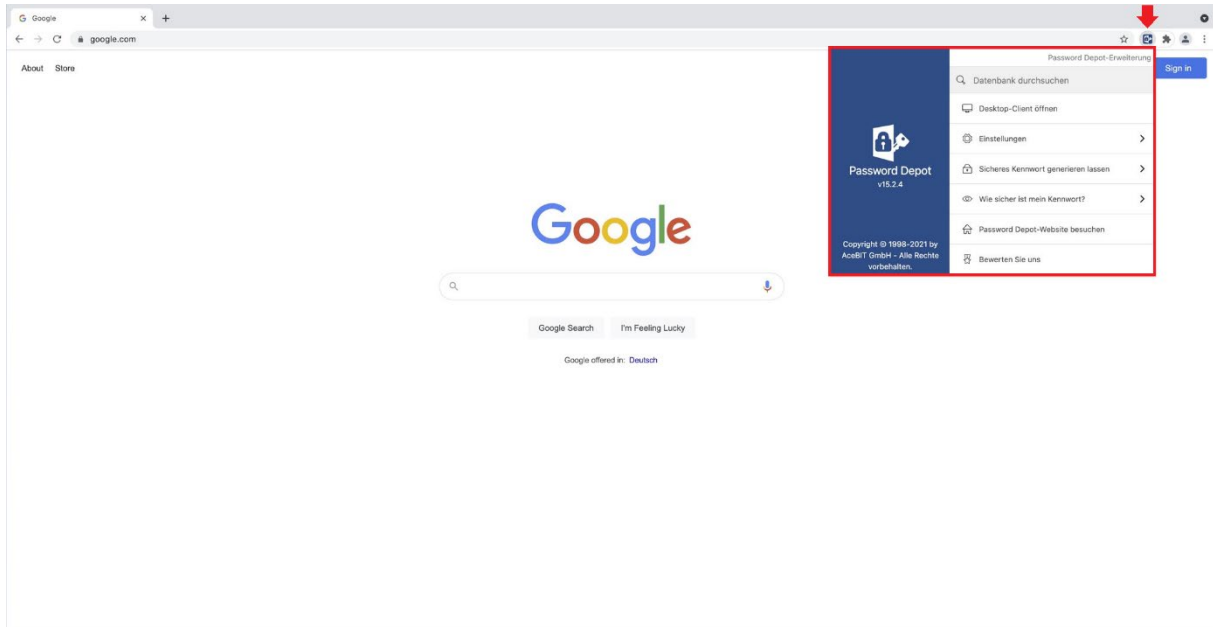
If you click on the add-on icon displayed in the corresponding login boxes of a website, you can see a new dialog window:



Select  for copying the **username** and/or **password/URL** to the clipboard. You can paste the copied information to other applications afterwards, if required. Select  if you want to edit the corresponding entry immediately. You will get back to Password Depot and the entry's properties.

Available in Your Browser

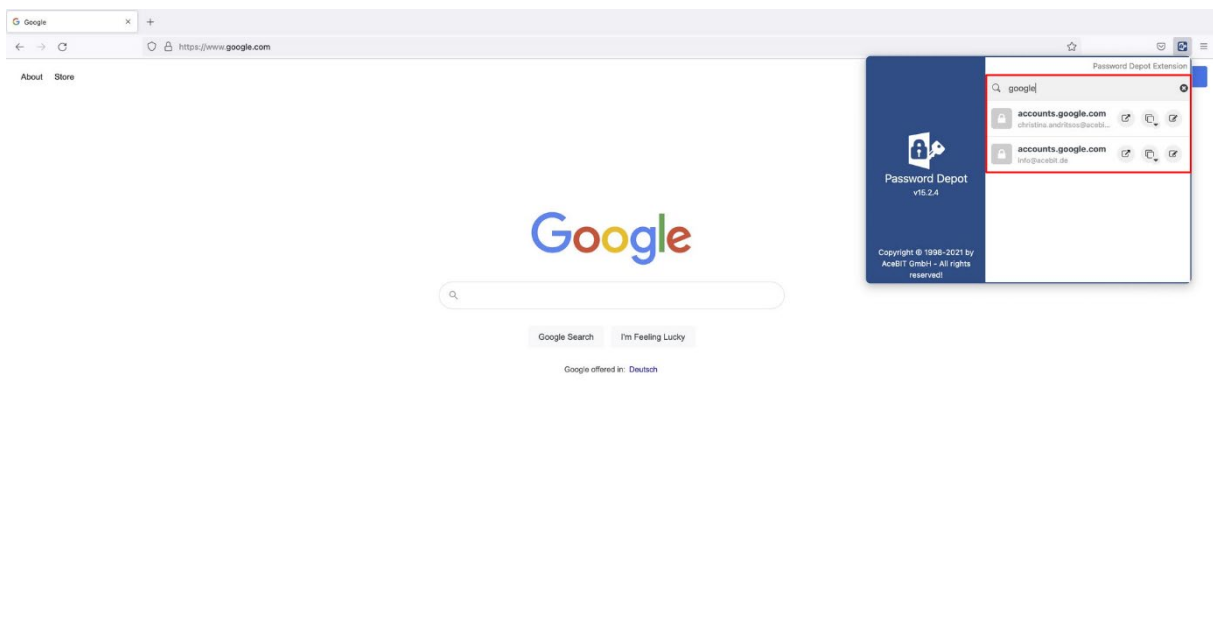
If you click on the add-on icon in your browser (it is always displayed at the top right corner), a new dialog window will open:




The following features are available here:

Search your depot:

You can start searching for an entry within your database. Any entries found will be displayed subsequently below the search box:



You can either copy the corresponding access data and/or URL to the clipboard or edit the requested entry in Password Depot immediately by clicking the corresponding icons. Furthermore, you can also select  to open the desired entry found during search in a new tab. This way, you can call up an entry and open it in your browser afterwards without going back to the client at all.

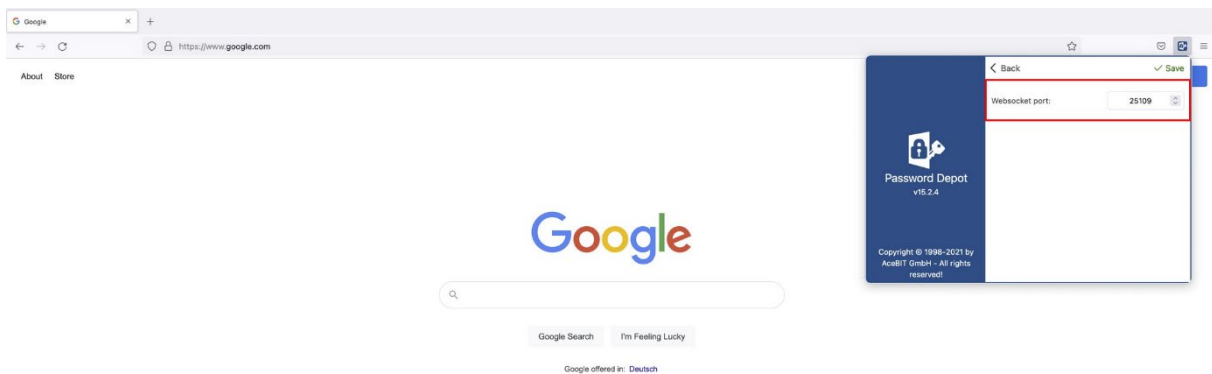
Open Native Client:

Go back to the native client.

NOTE: Searching for an entry in your browser will only display results if your entries include **specific URLs**. Therefore, entries within your database that do not have a specific URL will not be taken into account in this case. Those entries can only be found during search in the native macOS client.

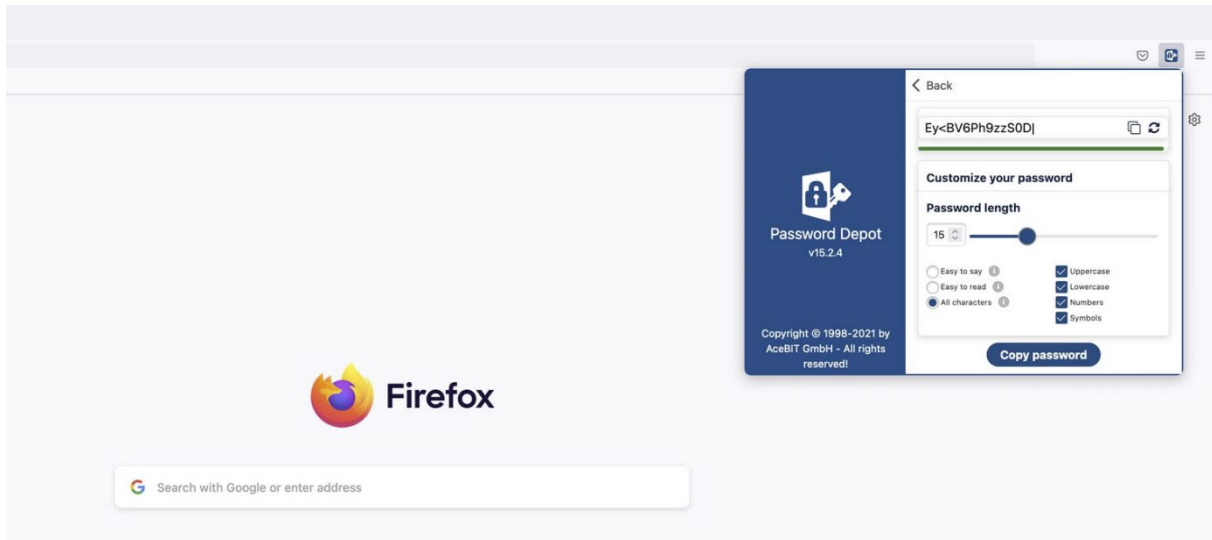
Settings:



You can change the WebSocket port here (e.g., if you work on a terminal server).



Generate Secure Password:

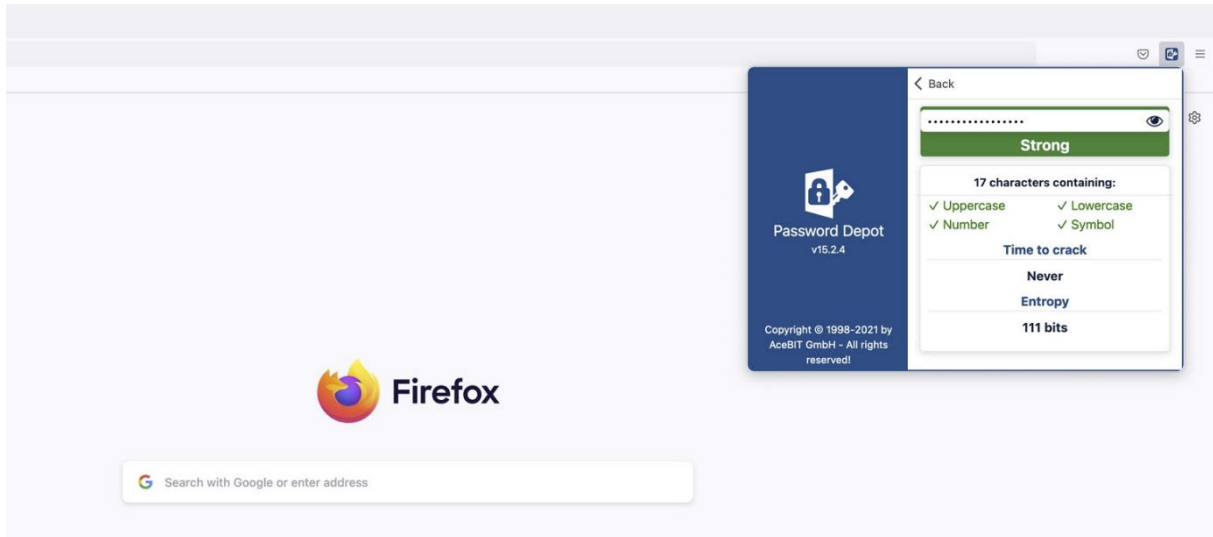
You can generate new and secure passwords using the Password Depot add-on in your browser and use such passwords immediately, e.g., if you want to create a new account and need a new password. This is useful since you can create secure passwords in your browser directly and use them for the login immediately. Returning to the native client is not necessary anymore.



- You can see the generated password in the corresponding box at the top. Select  to copy it, select  to create a new password.
- **Password Length:** Define the length of all newly created passwords.
- **Easy to say:** Choose this option if you want to avoid numbers and special characters in newly created passwords.
- **Easy to read:** Choose this option if you want to avoid ambiguous characters (e.g., O & 0) in newly created passwords.
- **All characters:** Choose this option if you want to include all kinds of character combinations.
- In addition to that, you can also define which characters should be included in general when generating a new password with the browser's password generator: **Uppercase, Lowercase, Numbers, Symbols.**

How Secure is my Password?

If you want to create new passwords on your own and do not want to use the password generator, you can use this option to check whether such passwords are secure. To do so, enter the password into the corresponding box. Next, you can see if the password is weak, medium, fair, or strong, which characters have been included, its entropy and the time that it would take to crack it.



NOTE: This is only a guideline which should help and support you in generating secure and strong passwords.

Visit Password Depot Website:

Choose this option if you want to visit the Password Depot website.

Rate Us

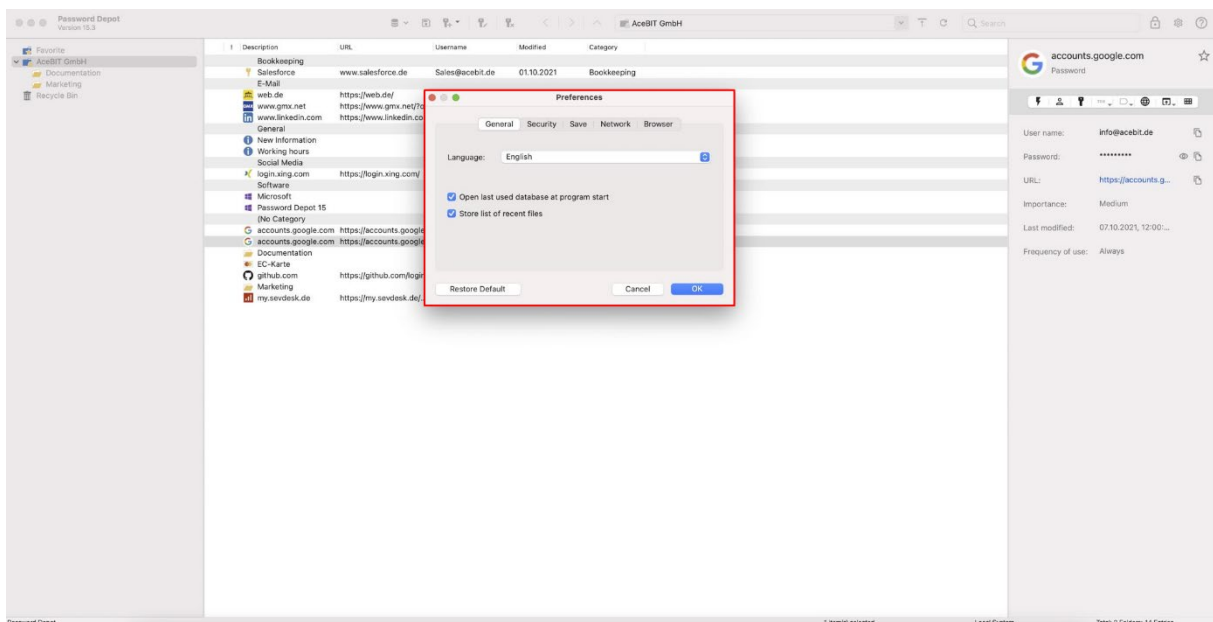
We would be very happy if you could rate our new add-on and its new features!

NOTE: Should you notice any problems when using the add-on, please visit the [Add-on area](#) in our Support Center for further help or send an email to info@acebit.de.

Preferences

When working with a database, you can see the icon  in the toolbar. By clicking on this icon, you can open the program options/preferences. A new dialog window will open. This dialog window includes the following tabs:

- **General**
- **Security**
- **Save**
- **Network**
- **Browser**



These tabs and the options included will be explained in detail:

General: You can change the language of the program here. Password Depot for macOS is currently available in German and English. The option **Automatic** means that the program will automatically choose the language selected during installation of Password Depot. Furthermore, you can determine here whether you want the program to open the last used password file at program start and whether the software should store a list of recent files.

Security: Here, you can define the settings concerning the clipboard and automatic locking of the program. Determine a specific time after which passwords copied to the clipboard with Password Depot should be deleted completely by activating the option **Delete password from clipboard after**. You can also activate the option **Automatically lock when the program is inactive for** and set up a

time after which Password Depot should automatically lock if the program is inactive and currently not being used.

Save: This tab deals with saving password files and creating backups files. For example, you can determine whether your password file should be saved on every change automatically and if a backup file should be created every time on file saving/opening. In addition to that, you can also define the maximum number of stored backup copies individually.

By default, the working directories of your Password Depot databases (local system) are the following in macOS:

Databases

`\Users\<Username>\Documents\Password Depot\`

Backup files

`\Users\<Username>\Documents\Password Depot\Backup`

Network: Here, you can determine whether you want to use SSL/TLS connection to **Password Depot Enterprise Server**. We recommend using this option if you want your Mac to connect to the Enterprise Server outside a local network.

Browser: Here, you can set any options regarding the usage of browser add-ons. For example, you can define whether you want the add-on to auto-fill web forms in general and if new passwords from web browsers should be added to your database automatically. Additionally, you can also adjust the port number for communication with the browser add-ons and activate or deactivate the option **Protect access with a password**. If this option is chosen, a separate password is required for successful communication with the browser add-ons. Learn more about this feature in our [Support Center](#).

TIP: Every tab contains the button **Restore Default** at the bottom on the left. Use this option if you would like to restore the default settings for any settings that you made changes to.

Useful Links

[Tips for creating strong passwords](#)

[AES 256-bit encryption](#)

[Download the current Password Depot desktop edition](#)

[Password Depot manuals](#)

[What's new](#)

[AceBIT Community](#)

[Support Center](#)

[Subscribe to our Password Depot newsletter](#)