Password DEPOT

User Manual

Password Depot 17

Last Updated: 13.12.22

AceBIT
Every Bit an Ace!

Welcome to Password Depot!

Congratulations on your decision to manage your passwords and login credentials with a password manager. You are in good company: Password Depot is used worldwide by thousands of businesses, banks, government agencies and private users.

Would you like to start immediately, without having to read the entire user manual? Our quick start instructions will help you. You may find our video tutorials helpful, too!

What is special about Password Depot?

Password Depot is an efficient and, most importantly, secure program for managing your passwords and login credentials. Password Depot uses sophisticated security mechanisms and offers a wide range of functions. It was developed for the use in a professional environment with strict safety standards.

Security

Password Depot guarantees a high security standard in multiple ways:

- AES-256 encryption: The software encrypts your data with the Rijndael 256 algorithm, also known as AES-256 (*Advanced Encryption Standard*). This is currently the most secure method of encrypting data on a computer. For instance, AES is used for US government documents of the highest confidentiality level. One advantage of the AES security algorithm is that the master password for encrypting your password database is not saved on your computer and thus cannot be found by third parties.
- Protection against keylogging: All password fields have an integrated protection against various keylogging types.
- Clipboard protection: Password Depot automatically recognizes active clipboard viewers and hides changes to the clipboard. After automatically filling in data, all sensitive data is automatically deleted from the clipboard. As of Windows 10 Update 1809 and higher, Password Depot prevents the logging of data copied to the clipboard.
- Program protection: Various options allow for the protection of Password Depot itself: Whenever the program enters locked mode, all sensitive data is cleared from the memory. The program is able to auto-lock, for example whenever the computer switches to standby or hibernation mode or whenever the current session changes.
- Highly secure shredding method: Temporary program data is shredded using a method conforming to the DOD 5220.22-M standard of the US Department of Defense. The definite, irrevocable deletion of temporary files is very important, because they can contain data that could be extracted and used by third parties. Simply deleting files in Windows Explorer is not secure, since only the filename will be deleted this way. To destroy a file beyond recovery, it must be rewritten before deleting it.
- Lock function: The internal lock function prevents unauthorized persons from accessing Password Depot. Thus, you can keep the program running on your computer without unauthorized persons being able to see your passwords.

Functionality

Password Depot protects your confidential passwords and login credentials from external access while offering maximum user-friendliness and a comprehensive range of functions.

- The integrated password generator creates randomized, impossible-to-crack passwords. These can be entered by drag & drop afterwards. Password Depot generates true-random data that cannot be predicted, whereas other, more conventional generators create random data based on system time, which can be predicted or reproduced.
- The auto-complete function allows for automatically completing fields on a website with user name and password. You can also generate individual auto-complete sequences using the integrated editor.
- The top bar mode simplifies navigation on the Internet. You can minimize the program to a small bar at the top of the screen, which can easily be moved at will.
- USB flash drive support allows for installing Password Depot on a USB storage device. This way, you can access your passwords from any PC.
- You can also save your encrypted databases on the Internet and enjoy access to all of them, no matter your location.
- The Enterprise Server allows for the shared use of password databases in teams and businesses.
- Free mobile apps allow for the use of the software on mobile devices. The operating systems iOS and Android are supported.

Tips on the user manual

In this user manual, you can find explanations on all functions of Password Depot.

If you need help with a specific topic, you can enter a keyword either on the tab *Index* or on the tab *Search.* All topics containing this keyword will then be displayed.

If you need help with an action you just performed, you can open the help topic by pressing the F1 key or the *Help* button in the dialog window.

In case you are missing a topic in the manual, please contact our support.

In order to make navigating the manual easier, different contents are visually differentiated by their design:

Tips

Examples

Notes

Warnings

What's new in Password Depot?

Password Depot is continually developed, updated and improved. In order to see what makes the current version better than the previous ones, please visit our website.

See also: Update Manager

Quick start

Would you like to start immediately, without having to read the entire user manual? The following instructions will help you:

- Install Password Depot.
  In order for passwords to be added directly from your browser and data on websites to be filled in automatically later on, install the browser add-ons as well. Without the add-ons, passwords can only be added or filled in manually. However, they can also be installed retroactively.
- Launch Password Depot.
- Add a new database by clicking *Database* → *Database Manager* → *Local system* → *New database*.
- Open the database by authenticating according to the method chosen in the previous step.
- Add your passwords by clicking *Edit* → *New* → *Password*. If you have installed and activated the add-ons, you can use your credentials directly in the browser. Password Depot will offer to save them in the open database.
- Organize your passwords in folders. You can create a folder by right-clicking on the area on the left and selecting *New*.
- If necessary, edit an entry by selecting it and clicking *Properties*.
- Next time you load the URL in your browser, the add-on will fill in the stored information automatically. All that remains to be done is clicking on the login button.

See also: Auto-complete Function

Installation

In order to install Password Depot on your computer, please follow these steps:

- On the Password Depot Website, select the desired version of Password Depot under *Download*.
- Click the download link.
- Select the folder where you want to save the file or execute it directly.
- Follow the instructions of the installation wizard.
- For passwords to be filled in automatically in the browser, you will need the Password Depot add-ons. Make sure to set a checkmark on the relevant options in the installation wizard.
- After a successful installation, always open the update manager first (*Help → Search for updates*). This way, you can ensure that you always use the latest version of Password Depot.
- Via *Help → Unlock*, you can unlock the full version of Password Depot with your license keys/unlock codes.

Installing add-ons retroactively

If, for whatever reason, the add-ons were not installed during the initial setup of Password Depot, you can always install them retroactively here:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge
- Internet Explorer: Can only be installed with the installation wizard.

Unlocking the full version of Password Depot

In order to work with the full version of Password Depot, activate the program. For using the trial or freeware version of Password Depot, this is not necessary.

The activation will be carried out in the program itself. To do so, click *Help → Unlock*. If Password Depot is already unlocked, you will not see this menu. A dialog window with two options will open:

- If you do not have a license key/unlock code yet, *Step 1 - Purchase a License Key online* will take you to the website where you can order a license key.
- If you already have a license key, select *Step 2 - Unlock Password Depot*.

NOTE: You need to be connected to the internet in order to activate the software. If, for whatever reason, you do not have an internet connection, please send an email to info@acebit.de and request a license file.

Enter License Key (Unlock Code)

After selecting one of the options above, enter your license key in the appropriate field. The wizard will show you whether the unlocking process was successful. If so, you can now work with the full version of the program.

NOTE: You can see whether the program is activated under *Help → Abaout Password Depot.* If you can see a license key under *Installed License Key*, the software has been activated successfully.

Upgrading from previous versions

If you already possess a previous version of Password Depot, you can upgrade it to the latest version.

- First, order the upgrade from your version to the latest one. An upgrade is less expensive than purchasing new full versions.
- After placing your order, you will receive a license key/unlock code for the latest version.
- Install the new version. If the old version is still installed on the PC, you do not necessarily have to uninstall it. If you do uninstall the old version afterwards, however, we recommend reinstalling the latest version as well in order to avoid errors.
- Open the downloaded latest version.
- Click *Help → Unlock* and select *Step 2 - Unlock Password Depot*.
- Enter the license key you received with your order.
- When the new version has been unlocked, you can open your databases from the old version here. To do so, open the database manager. Click *Browse* and select the path to your file. By default, your file is found in *My documents* (XP) or *Documents* (Vista, Windows 7, 8 and 10). Confirm your selection by clicking *OK* and authenticate with your master password and/or your key file.

NOTE: For very old versions, it may be helpful to open the database in the old version, convert it to the XML format and import the XML file in a new database in the new version.

Update Manager

The update manager allows you to always keep your program up to date with just a few clicks.

Go to *Help → Search for updates*. The program connects to the AceBIT server and informs you whether an update is available. If so, you can download this new version and install it on your PC.

Open the update manager regularly to keep your software up to date.

NOTE: The update manager only installs free updates, for examples from version 14.0.4 to version 14.0.5. Chargeable upgrades, such as from version 14.0.4 to version 15.0.0 for example, are not included.

USB installation

You can run Password Depot on a USB device. This may be helpful if you would like to carry your passwords or other confidential data you manage in Password Depot with you at all times.

If you would like to use Password Depot on a USB device, install it using the function *USB Installation*, not the standard installer. You can find the USB installation wizard by going to *Tools* → *USB Installation*. Here, you can install Password Depot on a USB device such as a flash drive, upgrade older versions of Password Depot or update databases on the device. To do so, follow these instructions:

- Removable drive: Select the device on which you would like to install Password Depot.
- Copy/Update databases: After choosing your device, select the databases you want to copy or upgrade.
- **Update Password Depot configuration file on the target medium:** If selected, your settings for the program will be transferred to the device as well.
- Update Autorun.inf to launch Password Depot automatically: If checked, the file autorun.inf will be installed on the device as well. This will automatically launch Password Depot as soon as you use the device.
- Next: Click on this button to run the installation or to upgrade automatically.

NOTE: Certain functions that require a local installation, such as browser add-ons, cannot be used with the USB installation.

NOTE: Before you upgrade Password Depot on a USB device, you will need to upgrade it on your local system.

User interface

The user interface is divided into five areas: The password area, the navigation area, the status bar, the toolbar and the details. Except for the password area and the toolbar, these areas can be shown or hidden via the menu *View*.

Password area

The password area is the main area of Password Depot. Therefore, it is in the middle of the screen and cannot be hidden.

This area allows for access to your passwords. It displays the description of your passwords as well as, if desired, further information. In *Edit → Options → Layout,* you can customize your view. In order to change the view of the password list, click on the tab *Display*.

You can move entries into another group with drag & drop from the password area. To do so, the navigation area needs to be opened.

Navigation area

This area offers a tree structure of the folders in the open database, similar to the one found in the Windows Explorer. Additionally, you can access your favorites and the recycle bin here as well.

Types

Here, you can view a list of all entry types. By double-clicking a type, you can see a list of all entries of that type in the current database.

Categories

Here, you can view a list of all categories, both built-in and custom ones. Just as you can with entry types, you can double-click a category to see a list of all entries of that category in the current database.

Status bar

On the bottom border, you can find a blue bar with information on your version, license status/remaining days in trial mode, number of objects, local system or network, and statistics.

Toolbar

The toolbar is above the navigation and password areas. It allows for quick access to important functions of Password Depot. On the right, you can see a field for a file path and the search function.

Details

This area is on the right of the window. Here, you can see detailed information on selected keywords. Additionally, the following actions are available:

- Auto-Complete (F6)
- Copy user name (F3)
- Copy password (F2)
- Custom fields/Global custom fields
- Copy URL (F4)
- Open URL in browser (F5)

Sort by

Choose here how to sort your entries. If you have selected the option *Custom View*, you can sort your entries by drag & drop. Furthermore, you can display your entries in descending or ascending order.

Group by

Choose here if you would like to group your entries. They can be grouped either by type or by category.

Mode

Here, you can choose whether to use Password Depot in Expert, Beginner or Custom Mode.

Top Bar

The top bar is a useful and unique feature of Password Depot. You can change into this mode either via the button in the toolbar or via *Ctrl* + *T*.

This button minimizes Password Depot to a small bar positioned above the other programs on your computer. This ensures constant access to the passwords saved in Password Depot. It can be moved by pressing the left mouse button and dragging it around.

The top bar allows for the selection of a specific password:

- Select a group in the field *Folders*. Afterwards, all passwords in this group will be displayed in the field *Entry*.
- Select a password in the field *Entry*.

To the right of the *Entry* field, you can search for entries.

In the right half of the top bar, you can see a number of symbols, with which you can carry out various program functions. To customize these symbols, right-click the top bar and click *Customize*. The following symbols can be displayed in the top bar:

- Search
- Program options
- Open Database Manager
- Save database
- New password
- Copy global fields to clipboard
- Select a favorites item
- URL
- Partial password
- TOTP
- Password Generator
- Modify password
- User name
- Password
- Copy custom fields to Clipboard
- TAN
- Insert data to an input box
- Suggest password for URL
- Open URL
- Auto-complete form (F6)
- Restore (CTRl +T): Restores the main view of the client.
- Lock Password Depot (Ctrl+ L)
- Minimize
- Exit: Closes Password Depot.

Database Manager

In the database manager (*Database → Database manager*), you can create new databases and open existing ones. Databases can be created or saved in the following locations, each of which has its own tab in the database manager:

- Local System
- Enterprise Server
- USB Storage Device
- Internet Server
- Dropbox
- Google Drive
- OneDrive
- HiDrive
- Box
- Recent Files
- Backups

Database Manager - Local System

In Password Depot, you can open and save databases in your local system. To do so, open the Database Manager (*Database → Database Manager*) and click on the *Local System* tab. The following options are available now:

- Back: If you changed folders in the browser, you can jump back to the previous folder with this button.
- Forward: If you jumped back previously, you can jump forward again with this button.
- Level up: Changes over to the next higher-order folder/directory.
- Refresh: Updates the list of databases in your local system.
- New database: Allows you to create a new database in your local system. A detailed description of that process can be found here.
- Delete: Deletes a selected database from the list.
- Browse: Allows you to search the local system for a specific database.
- **Open:** Opens a selected database.

Database Manager - Enterprise Server

In Password Depot, you can open and save databases on the Enterprise Server module. To do so, open the Database Manager (*Database → Database Manager*) and click on the tab Enterprise Server. The following options are now available:

- Sign in: Takes you to the login site of the Enterprise Server. Enter the required data and authenticate via username and password, the integrated Windows Authentication or Azure AD. Since version 12.0.7, you can optionally activate a Two-Factor Authentication for logging in on the Enterprise Server. After signing in, you can see all databases you have access to.
- Sign out: Logs you out of the Enterprise Server.
- Refresh: Updates the list of databases available on the Enterprise Server.
- Change password: Allows you to change the password for the Enterprise Server.
- View Certificate: If a certificate was installed earlier, you can see its details here.
- Offline Mode: Allows you to edit databases without being connected to the server. Upon reconnecting to the server, the database will be synchronized automatically.
- Open: Opens a selected database.

NOTE: Creating databases on the Enterprise Server is only possible with the Server Manager. If you would like to share a database from your local system with others, send it to your system administrator.

NOTE: Once you have opened a database on Enterprise Server, you can easily switch between available databases by using the *Databases from Server* window in the navigation area to the left without needing to re-open the Database Manager.

Enterprise Server: Login

To sign in, you will need to enter the following information on the server:

- Server Address: Enter the address under which the Enterprise Server runs. Usually, this is an address like 90.0.0.1.
- Port: Enter a port number with which the server can be reached. Each main version has its own default port.
- **Authentication Method:** Select the correct authentication method (Integrated Windows Authentication, standard authentication with username and password, or Azure AD authentication).

Lastly, click *OK*.

NOTE: You can only open files in the *Enterprise Server* tab that you have the necessary permissions to. Permissions are granted to you by your server administrator. If you successfully sign in on the server and receive the message that you have not been assigned a database yet, please contact your server administrator because working on the server will not be possible otherwise.

Authentication methods on the Enterprise Server

Generally, the server administrator decides how users are to log in on the Enterprise Server. Thus, it is only required for users to select the correct authentication mode to establish a secure client to server connection.

Integrated Windows Authentication

To sign in on the Enterprise Server using the Integrated Windows Authentication, also known as Single Sign-On, you will need to be a member of Active Directory. Furthermore, the server administrator needs to run an Active Directory synchronization to add you as a server user. If these requirements are met, select the correct option in the window *Database Manager - Enterprise Server Login* and make sure you use the correct address and port. Your Windows NT credentials will be used to log in. If all settings are correct, you can see your login name and your domain in the next window already. Click *OK* to sign in on the server.

Standard authentication

If your server administrator added you as a local user and assigned you a username and a password, you can use the standard authentication to sign in on the Enterprise Server. Enter your assigned credentials and make sure to use the correct server address and port.

Azure AD Authentication

To sign in on the Enterprise Server using the Azure AD Authentication, you will need to be a member of Azure Active Directory. Furthermore, the server administrator needs to run an Azure AD synchronization to add you as a server user. If these requirements are met, select the correct option in the window *Database Manager - Enterprise Server Login* and make sure you use the correct address and port.

You will receive a message that Password Depot wants to use *microsoftonline.com* to sign in. Confirm this to continue. You will be forwarded to your browser. Select the desired Microsoft account and enter your email address and password. Afterwards, you will need to allow Password Depot access to your Microsoft account again. As soon as all necessary steps have been carried out, a connection to the Enterprise Server will be launched.

NOTE: Next to the *Sign in* button (plug symbol), you can see a little arrow. If you click it, a drop down menu will open. Here, you can select an authentication method so that you will be forwared to the *Password Depot Enterprise Server - Login* window, in which this authentication method is already preselected.

Database Manager - USB Storage Device

In Password Depot, you can open and save databases on a mobile storage device, e.g. a USB stick. To do so, open the Database Manager (*Database → Database Manager*) and click on the tab *USB Storage Device*. The following options are now available:

- Back: If you changed folders in the browser, you can jump back to the previous folder with this button.
- Forward: If you jumped back previously, you can jump forward again with this button.
- Level up: Changes over to the next higher-order folder/directory.
- Drive: Allows you to select a USB storage device.
- Refresh: Updates the list of databases on your USB storage device.
- New database: Allows you to create a new database on your USB storage device. A detailed description of that process can be found here.
- Delete: Deletes a selected database from the list.
- Browse: Allows you to search the USB storage device for a specific database.
- **Open:** Opens a selected database.

TIP: To save databases onto a USB stick, you can use the function USB Installation on the tab *Tools*.

Database Manager - Internet Server

In Password Depot, you can open and save databases on an Internet server. To do so, open the Database Manager (*Database → Database Manager*) and click on the tab *Internet Server*. A new dialog window will open. Click on the icon *Manage servers*. Afterwards, click *+ New* in order to choose from one of the offered services:

- Custom Server
- GMX MediaCenter
- WEB.DE Online-Speicher
- MagentaCLOUD
- freenet Cloud
- Strato HiDrive
- Yandex Disk
- pCloud
- wölkli

Since version 14, Password Depot supports the above cloud servers via the WebDAV protocol. After selecting one of these services, you will need to enter some information in the next window. You can read in the section Manage Databases on Internet Servers which data is required in order to establish a connection.

After selecting a cloud service, the following options are available:

- Refresh: Updates the list of available databases on the Internet server.
- Manage Servers: Allows you to create or add a new server on which you then can create databases.
- New database: Allows you to create a new database on your Internet Server. A detailed description of that process can be found here.
- Open: Opens a selected database from the list.

NOTE: The function *New database* is only active if the Internet Server protocol is set to FTP or SFTP. New files cannot be uploaded to HTTP or HTTPS servers. Find out more in the Manage Internet Server section.

Manage Internet Servers

With Password Depot, you can save databases or backup files on Internet servers. The function *Manage Internet Servers* allows for the central management of these servers. To do so, click *Edit → Internet Server.* A new window with the following options will open:

- +New: Here, you can add a new Internet server.
- Edit: Allows you to modify an already added server in a new window.
- Delete: Removes an already added server from the list.

Adding/editing an Internet server

If you click *+New*, a drop down menu will open from which you can choose from the offered cloud servers. Since version 14, Password Depot supports various cloud servers via the WebDAV protocol. After selecting a service, you will need to enter the following information before you can use it:

- Protocol: Here, you can choose between FTP, HTTP, SFTP, HTTPS, FTPS and FTPES, WebDAV and WebDAV (SSL).
- Address: Enter the server address here. Please do not enter a path or storage location here!
- Port: By default, *Auto* will be entered here. In this case, the program will automatically search for the correct port.
- Path: Enter the complete path here. Do not enter any file names! To access the root directory, this field should contain only one slash (/). When using one of the cloud servers, the complete path is already entered here.
- User name: Enter your user name here. This is required for FTP servers.
- Password: Enter your password here. This is required for FTP servers.
- Passive: Allows to switch between active and passive transfer mode when using the FTP protocol.

"Active" and "Passive" refer to the server behavior when transmitting data to a client. In passive mode, the client initiates the transfer. In active mode, however, the server asks the client which port should be used for the transfer. If a firewall is active on the client, it may interrupt the connection. In this case, the passive mode is recommended.

TIP: We generally recommend using the SFTP protocol since it allows for both reading and writing access while being more secure than the FTP protocol. However, if you only require reading access to a file on an Internet server, the HTTP protocol suffices.

Database Manager - Dropbox, Google Drive, OneDrive, HiDrive, Box

In Password Depot, you can save and open databases in Dropbox, Google Drive, Microsoft OneDrive, HiDrive or Box. To do so, open the Database Manager (*Database → Database Manager*) and click on the tab of one of the listed cloud services. The following options are now available:

- Sign in: Directs you to the cloud service login website.
- Sign out: Allows you to log out from the cloud service.
- Refresh: Refreshes the list of available databases saved in your cloud.
- New database: Enables you to create a new database in your cloud. A detailed description of this process is provided here.
- Delete: Deletes a selected database from the list.
- Open: Opens a database selected in the list.

WARNING: We highly recommend against manually creating paths to the database directories. Instead, sign in to your cloud service with Password Depot and allow the Program to create a path, provided it does not exist yet. After Password Depot has created the directory, you can upload your databases with the Windows Explorer or your browser.

NOTE: When saving your databases in a cloud, your confidential data only ever "touches" the cloud in AES 256-BIT encrypted form, never unencrypted. Your databases are always and only decrypted locally.

Database Manager - Recent Files

On the *Recent Files* tab in the Database Manager (*Database → Database Manager*), you can see all the files you have been accessing recently. This applies both to local files as well as files that were opened on e.g. an Internet Server or via Enterprise Server.

Simply select the desired database and click *OK* to get to the authentication window.

You can remove an entry by selecting it and clicking *Remove*. This only removes it from the list, but does not delete the database. Invalid entries can be removed with the button *Remove invalid*.

NOTE: The tab *Recent Files* is only available if you have activated the option *Store lists of used databases and key files* via *Edit → Options → General*.

Database Manager - Backups

This tab contains a list of all backups from the backups folder. The folder paths can be changed in *Edit → Options (F10) → Save*.

If a database is corrupted, or was deleted by mistake, you can open a backup file of the database here.

Once you have opened a backup file, you should save it again in its original format by clicking on *Database → Save as (Ctrl+Alt+S)*.

New Database

To create a new database, proceed as follows:

- Open the Database Manager by clicking *Database → Database Manager.*
- Select a storage location on the left.
- Click *New database*.
- Name the new database. If desired, add a description.
- Select an authentication method. You can choose from a master password, a key file or a combination of master password and key file.
    - When choosing an authentication method that uses a master password, enter a desired master password or generate one with the master password generator by clicking the star symbol. Repeat the master password. Its quality will be displayed below. Enter a hint for your master password, if desired. Additionally, you can check if your master password is found in Pwned databases, which contain credentials that are known to have been breached.
    - When choosing an authentication method that uses a key file, you can either search for an existing key file by clicking the folder symbol or generate a new key file by clicking the star symbol.
- Click *OK* when you are done.

WARNING: If you forget your master password and have not entered a hint that might help you, there is no way to access your database!

NOTE: If you only use a key file to authenticate, always be sure to keep it in a secure location. Otherwise, anyone who has access to your key file will have access to your database.

Master Password Generator

The master password generator helps you create a particularly secure password that you can still remember. You can open it in two situations:

- when creating a new database
- when editing the authentication method of an existing database

The basis of your master password is a sentence of your choice. The master password generator selects the initials and transforms some of them into other characters. Since version 16.0.3, a master password has to be at least 15 characters long, which have to cover at least three out of four character types, i.e. uppercase letters, lowercase letters, numbers or special characters.

- Please enter below an easy-to-remember phrase of at least 8 words: Here, you enter a phrase that should contain at least eight words. You can invent the phrase yourself, but should be sure to be able to remember it! Having entered your phrase into this field, click on button *Generate Password* to make the generator create a password.
- Generated password: Shows the password that the password generator has created from the phrase you had entered above.
- Password quality: Shows how secure your master password is.
- Convert phrase using: You can chose from a number of options regarding lowercase and uppercase letters and the conversion table being used. You also have the possibility to keep the original uppercase/lowercase letters of your sentence.
- Template used: Here, you can see how the initial letters of your original phrase were changed. To understand the meaning of each template element, please refer to the *Template Legend* at the bottom of the window.

On the *Leetspeak Conversion Table* tab, you can see and edit which letters are transformed to which other characters.

Lastly, click *OK* to use the generated master password for your database.

NOTE: Please make absolutely sure you can remember the generated master password!

Key File Generator

You can open the key file generator in two situations:

- when creating a new database
- when editing the authentication method of an existing database

To open the key file generator, select an authentication method with a key file. Click on the star symbol next to the field *Key file*.

To create a key file in the key file generator, move your mouse over the field in the generator. The randomly chosen characters make up a key. After it has been generated, click *Save*.

WARNING: Always store your key file in a secure location and create backup files. We strongly recommend against using only a key file to protect your passwords. If you protect your database with a key file only and store this key file together with the database, any third party could gain access to your file.

Open Databases

- Open the database manager by clicking on *Database → Database Manager.*
- Select the desired storage location in the left panel.
- Select a database and click on *Open*.

If the desired database is not listed, click on *Browse* and look for its storage location.

Save Databases

To save an open database manually, click on *Database* → *Save* or *Save as*.

Save

This function saves the current database. This way, the currently opened database will be overwritten with all the changes that have been made in the current session until that point in time.

Save as

The function *Save as* saves the current database as well. Here, however, you have the opportunity to save the current database as a copy of the original file under a different name.

TIP: You can set Password Depot to automatically save the database after every change in the *Save* tab of the Options.

Database Properties

The properties of each database can be defined individually. To view and edit the properties of your database, click *Database properties (Ctrl + I)* on the *Database* tab or right-click on the database in the navigation area and select *Properties*.

The *Properties* window contains the following six tabs:

- General: Displays general information on the database.
- Content: Here, you can see the content of your database.
- Advanced: Allows for defining password policies.
- Notes: Allows for editing the notes and the hint on the master password.
- Backup: Allows for creating and saving backup files on internet or other remote servers and setting intervals for these backups, independent from regular backup files which are defined through the program options.
- Entries: Here, you can choose from different types of entries and deactivate those which are not necessary to you.
- Security: Allows you to set a second password for additional security of your database and to edit an existing second password.

Properties - General

In the *General* tab, you can view and partly edit some basic information on your database.

In the very top, you can see the name of the database, which cannot be changed here. Below, you can see the following information:

- Location: Shows you where this database is saved. This cannot be changed here. In order to modify the name or the location of the database, either go to *Database* → *Save as* or carry out the change in the Windows Explorer.
- Size: Shows you the size of the database.
- Last modified: Shows you when the database was last modified.
- Contains: Shows you how many folders and entries the database contains.
- Authentication: Shows you which authentication method is currently used and allows to edit it by clicking *Change*.
- Use compression to reduce the Database size: Makes the database smaller by compressing it.

NOTE: Make sure to keep your database up to date and avoid unnecessary baggage. To find and delete attachments and symbols, use the Clean-up function in the menu *Tools* → *Clean-up.*

Change Authentication Method

To change the authentication method of an open database, click *Properties (Ctrl + I)* in the toolbar. In the *General* tab, go to *Change* in the *Authentication* area.

First, authenticate with your current credentials and click *Next*. Then, choose a new authentication method via *Authentication by* or set a new master password.

- Master password: Protects the database with a master password. Enter a master password of your choice here, either in plain text or hidden, or generate a secure master password with the master password generator. Below, you can see how secure your password is.
- Master password and key file: Protects your database with a master password and a key file.
- Key file: Protects the database with a key file. Via the star symbol, you can generate a key file. Via the folder symbol, you can search for an existing one. Please note that persons who have access to your key file also have access to your database. Therefore, please store your key file in a secure location.

NOTE: If you have added a hint for your authentication, remember to change it as well.

Properties - Content

In the *Content* tab of the Database Properties, you can find more options about the database content.

Database Objects

- Custom icons: Shows you how many custom icons you have in your database. To remove them, click *Delete icons*.
- Attachments: Shows you how many attachments your entries have as well as their total size. To remove them, click *Delete attachments*.
- Ignored URLs: Shows you how many URLs are ignored by the browser add-ons. You can modify these URLs by clicking *Edit URLs*.
- Update icons and window titles: This option allows you to automatically update the custom icons and window titles of your entries.

History

Here, you can choose to save a history of password changes. If so, you can define the maximum number of saved changes. To clear the password change history, click *Delete history*.

Recycle bin

Here, you can choose whether to permanently delete entries immediately or to move them to the Recycle Bin, from which they can be restored. If you have chosen the latter, you can define the maximum number of entries in the Recycle Bin. To clear the Recycle Bin and permanently delete its contents, click *Empty Recycle Bin*.

TIP: You can also open the recycle bin settings by right-clicking the recycle bin in the navigation area. This way, you will also get to the options *Empty recycle bin* and *Restore all*.

Learn more about the Recycle Bin here.

Properties - Advanced

On the *Advanced* tab of the database properties, you can define different settings for the password policy.

Password policy

- Passwords hidden by default: If this option is checked, passwords are hidden and will be shown as asterisks (***). If it is unchecked, passwords will be shown in plain text. However, this is not recommended for security reasons.
- Check password resistance to dictionary attacks: If you activate this option, the software will check every password for character strings which may be part of a dictionary, and warn you in case it finds any.
- Force new/edited passwords to comply with the following policies: If you select this option, all new or modified passwords will be checked for compliance with the parameters defined below. When a password does not meet the defined policy, you will be prompted to modify the password.
    - Minimum length: Define how many characters a password must contain at minimum.
    - Password must include: Define which characters a password must contain and how they must be distributed.

Second password

Activating this option forces authorized users to protect the database with a scond password. This way, Enterprise Server databases can be protected from access by the super-admin.

Properties - Notes

In the *Notes* tab of the database properties, you can change the comment on the database and the hint for your master password.

- Hint: Here, you can enter a hint to help you remember your master password, should you ever forget it. Please do not enter your actual master password.
- Comment: Here, you can enter a description of your database, which may be helpful if you work with multiple databases.

NOTE: Do not enter any information that could help a third party guess your master password. A hint should serve as a helpful reminder to you and no one else.

Properties - Backup

In the *Backup* tab of the database properties, you can set up additional backups. This should not be confused with the standard backup file, which is set via *Edit → Options (F10) → Save*.

Remote backup locations

Choose whether you want to save your backup locally and/or on an Internet server. You can edit your available servers by clicking Manage Servers. If choosing to save backups locally, you manually enter a path or select one via *Browse*.

Remote backup settings

If you have set up remote backups, you can choose to create automatic backups here, as well as the interval in which backups are created. By clicking *Create backup*, you can manually create a remote backup.

Properties - Entries

In the *Entries* tab of the database properties, you can view and choose from all entry types available in Password Depot.

You can remove the checkmark on entry types that you do not use. This way, an entry type will not be displayed when you create a new entry, allowing you to structure your database according to your individual needs.

Properties - Security

In the *Security* tab of the database properties, you can set a second password to ensure controlled access to important database records, and edit an existing second password. If you use a second password, please make sure to use one that you can remember easily, because there will be no way to restore it if you forget it.

Backup Files

In Password Depot, you can manually and/or automatically create backup files of your databases.

Backup files increase the security standard of your database. For instance, you can re-create the content of a database that was accidentally deleted by using a backup file.

Backup files are, on principle, identical with regular databases. The only difference is the file name extension ".bckd".

NOTE: The use of backup files is highly recommended.

Backup location

By default, backup files are saved in the following directory:

C:\Users\\Documents\Password Depot\Backup

You can view this backup location via *Edit → Options (F10) → Save → Working directories → Backups*.

How to Create Backup Files

Backup files can be created in two different ways: manually by the user and/or automatically by Password Depot.

Creating backup files manually

You can manually create backup files of your current database. To do so, open the tab *Database* and click on *Backup (Ctrl+B)*.

Creating backup files automatically

You can set Password Depot to regularly create automatic backups. For this purpose, the following options are available:

- Automatic, remote: In *Database → Properties (Ctrl + I) → Backup*, you can set up automatic remote backups and the intervals in which they are created.
- Automatic, local: In *Edit → Options (F10) → Save → Save and Backup*, you can set up automatic local backups and choose when they should be created.
    - Create a backup copy on database saving
    - Create a backup copy on database opening
    - Additionally, you can define how many backup copies should be saved at maximum. Outdated backups will be deleted automatically.

How to Open Backup Files

The backup files generated by Password Depot have the file extension ".bckd" and are stored, by default, in the following folder:

C:\Users\\Documents\Password Depot\Backup

To open a backup file, please follow these steps:

- Open Password Depot.
- Click on *Database → Database Manager.*
- Click on *Backups*.
- Select a backup of your file from the desired date and click *Open*.
- Authenticate with your master password and/or key file.
- Click on *Database → Save as (Ctrl + Alt + S)* to save the file in its original .pswd or .pswe format.

Add Entries

To add new entries, click on *Edit → New* or use the Password button on the toolbar (Ctrl+Ins). By clicking on the button directly, you can add a password entry. By clicking on the arrow on the right, you can choose an entry type from a drop down menu. The following types are available:

- Password
- Remote Desktop Connection
- TeamViewer
- PuTTY Connection
- Credit Card
- Banking
- Software License
- Identity
- Information
- Encrypted File
- Document
- Certificate
- Custom

All entry types, save for the document, allow for the use of the virtual keyboard. It can be found in the bottom left of each window.

NOTE: If a desired entry type is not shown, it may have been deactivated in the database properties. You can activate it in *Database → Database properties (Ctrl + I) → Entries*.

Modify Entries

To edit existing password entries, open the *Properties* window. There are five methods to open it:

- Select an entry and click *Properties* in the toolbar.
- Select an entry and press Ctrl + M.
- Right-click an entry and select the option *Properties*.
- Select an entry and use the tab *Edit → Properties.*
- Select an entry and double-click it.

Add/Modify Entry - Password

To add new password entries, click on *Edit* → *New* → *Password* or use the Password button on the toolbar *(Ctrl+Ins)*.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- User: Enter the user name.
- Password: Enter the password. In the bar below, you can see how secure your password is. By clicking the eye symbol, you can hide or display your password in plain text. Clicking the star symbol opens the password generator.
- Category: Assign a category to the entry to help structure your database.
- Importance: Select the level of importance for this entry.
- Expires: If you would like your entry to be valid for a limited time, you can check this option and define an expiration date. By clicking *Extend*, you can extend its validity. Note that expired passwords can still be used. This function only serves as a reminder to change passwords regularly.
- Tags: Here, you can add tags to allow for better filtering of your entries.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- URL
- Additional
- Custom Fields
- TANs
- Attachments
- Versions
- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - Remote Desktop Connection

You can manage your Remote Desktop Connections in Password Depot to establish a connection to the server with one click. To add new remote desktop connection entries, click on *Edit* → *New* → *Remote Desktop Connection* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Computer: Enter the address of the computer.
- User: Enter the user name.
- Password: Enter the password. In the bar below, you can see how secure your password is. By clicking the eye symbol, you can hide or display your password in plain text. Clicking the star symbol opens the password generator.
- Category: Assign a category to the entry to help structure your database.
- Importance: Select the level of importance for this entry.
- Expires: If you would like your entry to be valid for a limited time, you can check this option and define an expiration date. By clicking *Extend*, you can extend its validity. Note that expired passwords can still be used. This function only serves as a reminder to change passwords regularly.
- Tags: Here, you can add tags to allow for better filtering of your entries.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- Versions
- Conditional Access
- Security

Add/Modify Entry - TeamViewer

To add new TeamViewer entries, click on *Edit* → *New* → *TeamViewer* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Partner ID: Add the partner ID you would like to connect to.
- Password: Enter the TeamViewer password of your partner to establish a connection.
- Mode: Here, you can choose whether you want to connect via remote control or carry out a file transfer.
- Category: Assign a category to the entry to help structure your database.
- Importance: Select the level of importance for this entry.
- Expires: If you would like your entry to be valid for a limited time, you can check this option and define an expiration date. By clicking *Extend*, you can extend its validity. Note that expired passwords can still be used. This function only serves as a reminder to change passwords regularly.
- Tags: Here, you can add tags to allow for better filtering of your entries.
- Comments: You can add further notes here.

Additionally, the following tabs are available here:

- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - PuTTY Connection

You can manage your PuTTY connections in Password Depot to establish a connection to the server with one click. To add new PuTTY connection entries, click on *Edit* → *New* → *PuTTY Connection* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Protocol: Select the connection protocol. Ssh, telnet, rlogin or raw are available here.
- Host: Enter the address of the host.
- Port: Enter the port number of the server through which you want to communicate.
- Password: Enter the password. By clicking the eye symbol, you can hide or display your password in plain text.
- Key file: Enter the path of the key file, either manually or by clicking the folder icon.
- Key password: Enter the password of your key file. By clicking the eye symbol, you can hide or display your password in plain text.
- Category: Assign a category to the entry to help structure your database.
- Importance: Select the level of importance for this entry.
- Expires: If you would like your entry to be valid for a limited time, you can check this option and define an expiration date. By clicking *Extend*, you can extend its validity. Note that expired passwords can still be used. This function only serves as a reminder to change passwords regularly.
- Tags: Here, you can add tags to allow for better filtering of your entries.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - Credit Card

To add new credit card entries, click on *Edit* → *New* → *Credit Card* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Card: Select a credit card type.
- Card Holder: Enter the name of the credit card owner.
- Card Number: Enter the credit card number.
- Expires on: Enter the expiry date of the credit card.
- Security Code: Enter the security code of the credit card. By clicking the eye symbol, you can hide or display it in plain text.
- Service Phone: Enter the telephone number of the credit card company.
- Service URL: Enter the URL of the bank manually, by browsing your folders or by opening your standard browser.
- Additional code: Enter a supplementary code if needed.
- PIN: If applicable, enter the PIN of your credit card. By clicking the eye symbol, you can hide or display it in plain text.
- Comments: You can add further notes here.

Additionally, the following tabs are available here:

- URLs
- Additional
- Versions
- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - Banking

To add new banking entries, click on *Edit* → *New* → *Banking* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- User: Enter the user name.
- Password: Enter the password. In the bar below, you can see how secure your password is. By clicking the eye symbol, you can hide or display your password in plain text. Clicking the star symbol opens the password generator.
- Card Holder: Enter the name of the EC card holder.
- IBAN: Enter the IBAN code.
- BIC: Enter the BIC.
- Bank name: Enter the name of your bank.
- Account number: Enter the number of your bank account.
- Bank code number: Enter the code to identify your bank.
- Card number: Enter the number of your EC card.
- Service phone: Enter the service telephone number of your bank.
- Legitimacy ID: Enter an additional ID code, if applicable.
- PIN: Enter your PIN.
- Expires on: Enter the expiry date of your EC card.
- Category: Assign a category to the entry to help structure your database.
- Comments: You can add further notes here.

Additionally, the following tabs are available here:

- URLs
- Additional
- TANs
- Versions
- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - Software License

To add new software license entries, click on *Edit* → *New* → *Software License* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Product: Enter the name of the product.
- Version: Enter the version number.
- Registered Name: Enter the name of the person the software is licensed to.
- Email Address: Enter the email address used for the purchase of the license.
- License Key: Enter the product's license key.
- Additional Key: Enter an additional key, if needed.
- Download URL: Enter the URL where the product can be downloaded manually, by browsing your folders or in your standard browser.
- User: Enter the user name.
- Password: Enter the password. By clicking the eye symbol, you can hide or display your password in plain text.
- Purchase Date: Select the date on which you bought the product.
- Expires: Indicate the software expiry date of the license key, if applicable.
- Order Number: Enter the order number of the product.
- Category: Assign a category to the entry to help structure your database.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- Additional
- Attachments
- Versions
- Conditional Access
- Security

Add/Modify Entry - Identity

To add new identity entries, click on *Edit* → *New* → *Identity* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Account Name/ID: Enter an account name or another form of ID here.
- First/Last Name: Enter the name of the person here.
- Email Address: Enter the email address here.
- Web Site: Enter the URL of a website connected to the person, either manually, by browsing through your folders or in your standard browser.
- Birth Date: Enter the birth date of the person.
- **Company:** Enter the company name here.
- Street/House number: Enter postal address information here.
- Address 2: Enter further address information here, if applicable.
- City: Enter the name of the city here.
- State (Province): Enter a state, province, or district here.
- ZIP: Enter the postal code of the city here.
- Country: Enter the country here.
- Phone/Mobile/Fax: Enter the telephone, mobile, and fax numbers here.
- Category: Assign the entry a category to help structure your database.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- Attachments
- Versions
- Conditional Access
- Security

Add/Modify Entry - Information

To add new identity entries, click on *Edit* → *New* → *Information* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Category: Assign the entry a category to help structure your database.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- Attachments
- Versions
- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - Encrypted File

Password Depot allows to securely encrypt external files with a password. The password you need for decryption can be saved in your database.

The following options are available for creating an encrypted file:

- In the menu *Edit* → *New* → *Encrypted File*
- In the menu *Tools* → *Encrypt external files*
- By selecting *Password* → *Arrow button* → *Encrypted File* in the toolbar
- By right-clicking the file in the Windows Explorer and selecting *Password Depot* → *Encrypt*. The password can be entered into Password Depot automatically.

If you encrypt a file via *Edit* → *New* or the toolbar, the following information can be entered in the *General* tab:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- Password: Enter the password. By clicking the eye symbol, you can hide or display your password in plain text.
- Category: Assign a category to the entry to help structure your database.
- Comments: You can add further notes here.

In the *Files* tab, you have the following options:

- Files: Shows a list of encrypted files belonging to the selected entry. They can be ordered by Name, Path on Disk, Last modified, and Size.
- Add file: Allows you to add an encrypted file (*.pwde) to the list.
- Delete file: Removes no longer needed files from the list.
- Decrypt file: Select a file from the list and click on Decrypt file to decrypt the file with a saved password.

Additionally, the following tabs are available:

- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: Encrypted files are always located on your storage medium. Only the password and the link to the encrypted file are saved in Password Depot. If you delete the file from your computer, you cannot access it anymore. In contrast, the Document type always saves your file as a part of the database.

Add/Modify Entry - Document

Password Depot allows the inclusion of documents in your encrypted database. To add new documents, click on *Edit* → *New* → *Document* or use the arrow on the *Password* button on the toolbar.

First, choose a file. The following information will be entered automatically and cannot be edited:

- Document: The name of the file.
- Type: The type (i.e. file name extension) of the file.
- Size: The size of of the file.
- Modified: Date and time of the last change.

In addition, the following fields are available:

- Original path: The original path of the file. With *Erase*, you can permanently delete the original file from your hard drive.
- Default folder: The default folder for actions with this file. It can be added manually or by clicking the folder symbol.
- Category: Assign the entry a category to help structure your database.
- Comments: You can add further notes here.

Below, the following functions are available:

- View: Displays the file with the application linked in Windows.
- Edit: Opens the file with the application linked in Windows.
- Import: Import the file again, e.g. from another source.
- Export: Save the file on a storage medium.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: The *Document* type saves a file directly in a Password Depot database, meaning that documents are a component of your database. In contrast, encrypted files are always saved to your storage medium.

Add/Modify Entry - Certificate

To add new certificates, click on *Edit* → *New* → *Certificate* or use the arrow on the *Password* button on the toolbar.

On the *General* tab, you can enter the following information:

- Description: Enter a description for the new entry. The description is the name that will be displayed in the password area, and is therefore the only field that is not optional.
- Change icon: By clicking on the icon of an entry, you can change it. By right-clicking the symbol, you can choose between the options *Select Icon*, *Load from URL* and *Reset Icon*.
- **Public key:** Here, you can select a certificate by clicking the folder symbol, view it by clickng the magnifier symbol or save it by clicking the floppy disk symbol.
- Private key: Here, you can select a certificate by clicking the folder symbol, view it by clickng the magnifier symbol or save it by clicking the floppy disk symbol as well.
- Password: Enter the password. By clicking the eye symbol, you can hide or display your password in plain text.
- Category: Assign a category to the entry to help structure your database.
- Importance: Select the level of importance for this entry.
- Expires: If your certificate is valid for a limited time, you can add an expiration date here. By clicking *Extend*, you can extend its validity.
- Tags: Here, you can add tags to allow for better filtering of your entries.
- Comments: You can add further notes here.

Additionally, the following tabs are available:

- Conditional Access
- Security

Click *OK* to save changes or *Cancel* to close the window without saving changes.

Add/Modify Entry - Custom

Password Depot 17 allows you to use custom templates for entries. To add a custom entry, click on *Edit* → *New* → *Custom* or use the arrow on the *Password* button on the toolbar. If you have not created any custom templates yet, you can do so here. Otherwise, a list of available templates will be displayed here.

To create a new template, go to *Edit* → *New template*. Here, you can name the new template and change its icon. Below, you can edit the components of your template. The following components are available:

- Custom
- User name
- Password
- URL
- Comments
- Importance
- Expiry date
- Category
- Tags

New components can be added by clicking the plus symbol. By selecting a component and double-clicking it or clicking the pencil symbol, you can edit it. You can delete a component by selecting it and clicking the folder symbol with the red cross. The arrow buttons move a selected component up or down. The eye symbol hides or displays the values of password components in plain text.

Custom entries are created on the basis of these templates.

Additionally, the following tabs are available both while creating new templates and while creating new custom entries:

- Additional
- Versions
- Conditional Access
- Security

Click *OK* to save changes to the template or entry, or *Cancel* to close the window without saving changes.

Add/Modify Entries - URLs Tab

The *URLs* tab is available for various entry types. Here, you can link an entry to a URL, which is required for working with the browser add-ons, for instance.

Default URL

Enter the URL of a website or the path of a file that this entry should be used with.

NOTE: The *Default URL* field cannot contain wildcards (*). To add masks with wildcards, please use the list below.

Associate the entry with following URLs and Templates

Here, you can link the selected entry to other URLs that use the same login credentials. This way, you do not have to create a new entry for each deviating URL.

You can add a new URL by clicking the plus symbol. By clicking the folder symbol with the cross, you can remove a selected URL. The recycle bin icon deletes all URLs from this list.

When adding a new URL, you can enter either exact URLs or masks. In such masks, characters can be replaced with a specific placeholder character. In Password Depot, this character is an asterisk (*) that you can place before or after the URL.

EXAMPLE: http://www.example-url.com/* includes both http://www.example-url.com/forum/ as well as http://www.example-url.com/login.php.
example-url.com includes all possible sites of this domain.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entries - Additional Tab

The *Additional* tab is available for various entry types. Here, you can edit various settings concerning, among others, the auto-complete function or browser add-ons.

Window Title

The title of the linked application or browser window will be displayed here.

Command line parameters

Here, you can enter the parameters with which you would like to open a local application or document.

EXAMPLE: If you would like to open an encrypted Word document, select the path to Winword (e.g. C: \Programs\Microsoft Office\OFFICE11\WINWORD.EXE) in *General/URL/Local Document* and indicate the path of the document that is to be opened (e.g. C: \mydocument.doc).

If the program you would like to open with command line parameters is password-protected and opened via a DOS command line parameter (for example PuTTY or MySQL), you can use the *Insert* button to the right to add the user name and password to the command.

EXAMPLE: The correct way of indicating a command for PuTTY is as follows: Create a new password entry. Enter your log-in credentials into the "password" and "user name" fields as usual. Select the path to PuTTY: either enter it into the field *Default URL/File* on the tab *URLs*, or select it by clicking the icon next to the input field. Switch to the tab Additional. In the field *Open local file with command line parameters*, you need to enter the following: @ -pw . If you now select the new entry in Password Depot and click F5, PuTTY will open and you will automatically be logged in with your account.

Auto-complete sequence

Select an auto-complete sequence from the list. If a desired auto-complete sequence is not listed, you can create custom sequences by clicking *Compose*.

Auto-complete method

Select one of the following methods to use for the auto-complete mode:

- Use global settings: With this method, data will, if possible, be inserted based on global settings.

- Clipboard I: With this method, data is first copied to the clipboard and then entered into the target field by simulating the key combination *SHIFT + INS*.
- **Clipboard II:** With this method, data is first copied to the clipboard and then entered into the target field by simulating the key combination *CTRL +V.*
- Keyboard input simulation: With this method, data is entered into the target field by simulating keyboard typing.
- Multi-Channel Obfuscation: This method offers particular protection from keyloggers as the password is not entered all at once but by a random mix of entry methods.
- **Windows Messaging I:** This method sends passwords directly to the target input field.

Usually, you will not need to change this option. Each of the methods above works correctly in the majority of the cases. For testing purposes, you can open Notepad.exe and check the auto-completion of a dummy password. There are, however, some exceptions in which one or more of these methods does not work. In this case, we recommend trying each method.

Preferred browser

If you have multiple browsers installed on your computer, you can assign a specific browser to an entry here. This may be helpful if certain websites can only be displayed correctly in a specific browser.

Open URL in private browsing mode

If you allow Password Depot to open URLs, the browser will be opened in private browsing mode.

Use entry with browser add-ons

Here, you can determine whether or not the selected login credentials are automatically filled out by the browser add-ons.

Update web form data

You can manually update the web form data associated with a password here. This can be useful if the auto-completion via the add-ons does not work correctly.

No password policies for this entry

Here, you can define whether or not the password policy compliance of an entry should be assessed. This way, you can avoid warnings regarding the security of the entry. This option is only recommended if a password is weak but you cannot change it.

2FA Secret

Entries can save 2FA keys to generate TOTP codes and make two-factor authentication easier. If, for example, two-factor authentication is necessary for logging in on a website, you can save the secret key on the *Additional* tab. Password Depot uses it to generate a TOTP code that you can use for logging in on this website.

You can use a button on the top bar to copy TOTP codes. Find out more here.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entry - Custom Fields Tab

Custom fields allow you to add your own fields to an entry and to define their value.
Here, you can see a list of the existing custom fields. The columns of the list are:

- Name
- Value

Below, you can find six buttons for working with custom fields:

- Add field: Creates a new field. Name it and enter a value.
- Edit field: Here, you can edit the name or value of an existing field.
- Delete field: Removes a custom field from your list.
- Up/Down: Changes the order of the custom fields.
- Hide: Activate or deactivate this option to show the values of password-type fields in plain text or hide them respectively.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

See also: Global custom fields

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entries - TAN Tab

Here, you can add TANs for your password. The columns are *No.*, *Value, Used on, Amount, Confirmation Code*, and *Comment*. The buttons below offer the following options:

- Add TAN: Allows you to enter a new TAN.
- Edit TAN: Allows you to edit existing TANs.
- Delete TAN: Allows you to delete TANs from the list.
- Import TANs: Allows you to import TANs from a CSV file, XML file or TAN list. The format TAN list requires a text file that contains exactly one TAN per line. Since banks usually issue printed TAN lists, you may need an OCR software.
- Export TANs: Allows you to export TANs into a CSV, XML or TXT file.
- Hide: Activate or deactivate this option to hide your TANs or display them in plain text respectively.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entries - Attachments Tab

Here, you can add attachments to an entry. The following options are available:

- Add attachments: Allows you to select a file from its location to add it to the list of attachments. On the right, you can see its path.
- **Delete attachments:** Removes a selected attachment.
- **Delete from Disk:** Deletes the attachment from its original location while keeping it saved in Password Depot.
- **Extract to Disk:** Saves the selected attachment to a location of your choice.
- Open with internal viewer: Opens the selected attachment.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

WARNING: Using attachments is not recommended. In fact, they are not available on the Enterprise Server. Please use the Document type instead.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entries - Security Tab

On the *Security* tab, the options *Use a second password* and *Change second password* are available.

A second password is used to ensure controlled access to important database entries, databases or folders.

By clicking *Change second password*, you can define a second password or change an existing one.

WARNING: Please make absolutely sure that you will not forget your second password. Otherwise, you will not be able to access the data you protected with it.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entries - Versions Tab

On the *History* tab, you can see the changes made to a password. This may be helpful in case your data was lost or you have accidentally overwritten an entry.

- View Differences: Displays all differences between two versions of an entry.
- Delete: Removes an item from the history list.
- Restore: Restores an entry to the selected state.
- Changes history: Allows you to select whether you want to use global settings, not save any changes or keep a history of the changes to this entry.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Add/Modify Entries - Conditional Access Tab

All entry types available in Password Depot have the *Conditional Access* tab. This tab is particularly helpful if multiple users have access to the same server database.

Warning message

Activate this option and enter an individual text in the field below if you would like users to receive a warning when accessing this entry. How this warning is displayed depends on the severity level selected.

Severity level

- Informational (popup notification): Displays the warning message in a Windows popup notification.
- **Major (modal message box):** Accessing the entry opens a new dialog window that contains the warning message. The entry can only be opened by clicking *OK*.
- Critical **(modal dialog box with the verification text):** Accessing the entry opens a new dialog window that contains the warning message and a custom text that users will have to confirm before being able to open the entry. This custom verification text can be entered into the field below.

Limit access to the entry

You can only activate this option when working with Enterprise Server databases. In this case, you can check the option and allow accessing the entry only when connected to Password Depot Enterprise Server.

Click *OK* to save changes or *Cancel* to close the window without saving changes.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Import & Export Entries

The *Import* and *Export* functions allow you to import passwords from an external file or to export the current database to an external file. These functions are especially useful for interactions between Password Depot and other password managers.

NOTE: Your database is a highly confidential document. Please make sure that no unauthorized persons gain access to it and store the document in a secure location.

WARNING: If you export your database, it will be saved in unencrypted form on your hard drive!

Exporting entries

Databases and database entries can be exported into another file format via *Tools → Export.*

Supported Formats for Export

Databases can be exported into one of the following file formats:

- XML (Extensible Markup Language)
- CSV (file with entries separated by comma)
- TXT (text file)
- HTML (Hyper Text Markup Language)

WARNING: These file formats do not support encryption. Anyone with access to these files can read their content.

NOTE: Every CSV file contains one password per line. Up to nine fields are assigned to each password in turn, separated by semicolon: *Description*, *Importance*, *Password*, *Last modified*, *Expiry Date*, *User Name*, *URL*, *Comments*, and *Category*.

How to Export

Before exporting the content of your file, you need to authenticate correctly first.
Afterwards, you can define the following:

- Export format: Select the format into which you want to export the content.
- Target file: Choose a name for your export target file. Click on *Browse* to define the location for storing it.

Click *Next* to continue. Choose what data you would like to export:

- All entries in the database
- Entries in the active view
- Selected entries in: Here, you can select entire folders with their sub-folders in addition to individual entries.

Click *Next* again to continue. If you are exporting your database to a CSV file, you can define the export parameters now. Afterwards, the wizard will display the results of the export.

TIP: If you select *Show the exported file in Windows Explorer*, you will be forwarded to the Windows Explorer directory in which your exported file is saved afterwards.

NOTE: The virtual keyboard can be used in this window. It can be found in the bottom left.

Importing entries

Password Depot allows to import passwords from external files, including from other password managers. To do so, go to *Tools* → *Import*.

Supported import formats

The software supports the following file formats for importing passwords:

- XML (Extensible Markup Language)
- CSV (file with entries separated by comma)
- Password Depot Format (.pswe and .pswd as well as older versions and backups)
- TXT (text file)

If you would like to import passwords from other password managers, you will need to export these passwords as a CSV or XML file first. Afterwards, you can import this file into Password Depot with the help of the import wizard.

Import process

To launch the import wizard, authenticate first. Then, enter the following information:

- Import format: Format of the file you wish to import.
- Source file: Click the button Browse to select a source file that should be imported.
- Target folder: In the drop-down list, select a target folder into which the passwords are to be imported.

Click *Next* to continue and *Finish* to complete the process.

NOTE ON THE ENTERPRISE SERVER: This function cannot be used when you are connected to the Enterprise Server. If you would like to import passwords on the Enterprise Server, contact your administrator. They have to open the database into which passwords should be imported as a local database. Only then, the *Import* button will be available. The administrator can then import the desired passwords, save the file and add it to the server again afterwards.

NOTE: The virtual keyboard can be used on this tab. It can be found in the bottom left.

Import Wizard - Importing CSV files

This page of the import wizard is used to adjust parameters for importing passwords from a CSV file.

If the source file was created using the same version of Password Depot, you can adopt the standard values of the wizard. If the source file was created using another version or another software altogether, you have to check or define the following field assignments:

- Delimiter: This is a character used in CSV files to separate values, the most frequently used symbols being ';', ',' or ' ' (blank).
- Text qualifier: This is a symbol used to group complex strings; the most often used symbol is '"' (double quotation marks).
- Available Fields: If the source file is not empty and the delimiter and text qualifier are specified correctly, this list contains values from the first row of the source file.
- Assign target and source fields: This list is used to establish correspondence between values in the source file and the relevant fields used by Password Depot. To assign a source field to a target field in Password Depot, select a value from the *Available Fields* list on the left and the relevant target field from the list on the right and click the >> button. To remove a relation, select an item from the list on the right and click the << button.

If the first line of the CSV file contains field descriptions, please check the *First line contains field names* box to exclude the first line from the import process.

Click *Next* to continue.

Clean-Up Entries

Using the Clean-up function on the Tools tab, you can see rarely used or expired entries at a glance and, if desired, delete those entries.

The following filter options are available:

- Show entries expired before: Shows all passwords which have expired before the day you have selected.
- With attachments, bigger than (KB): Shows all passwords which have an attachment bigger than the size you entered. This option allows you to quickly find big attachments that might slow down your database.
- Entries not used after: Shows all passwords which have not been used since the day you have selected.
- Never used entries: Shows all passwords that you have never used since you created them.
- With History: Shows all passwords for which "Keep change history" has been set previously.
- With custom icon: Shows all passwords which have been customized by the user.

After setting your filter options, you will see a list of all passwords that meet your criteria with additional information, such as expiry date or frequency of use. For the clean-up of the displayed passwords, the following options are available:

- Delete History: Deletes Change history of the selected passwords.
- Delete Attachments: Deletes attachments of the selected passwords.
- Reset Icon: Resets the standard icons of the selected passwords.
- Delete: Deletes all passwords which you have selected in the list.
- Export: Click the *Export* button to export the clean-up results into an external CSV file and save it to your local system.

Click *Close* to finish.

NOTE: Deleted passwords will be moved to the Recycle Bin, from which they can be restored.

Delete Entries

The *Delete* function on the toolbar (Ctrl + Del, or *Edit* → *Delete*) deletes both passwords and subgroups of the active group. Please note that all subgroups and entries of a group will be deleted as well if you delete a group.

NOTE: Deleted entries will be moved to the Recycle Bin, from which they can be restored.

Recycle Bin

Password Depot features a recycle bin into which deleted password entries are moved.

You can find the bin in the main view in the navigation area, which can be found on the left.

Clicking on the recycle bin symbol, the Recycle Bin tab will open in the main view. Here, you can see a list of all deleted entries with the following options:

- Empty recycle bin: Permanently deletes all entries contained in the bin. In order to delete only a single entry, right-click this item and choose *Delete*.
- Restore all: Restores all deleted entries to their original places.
- Restore: Restores only those entries that are selected from the list.
- Settings

NOTE: If you have mistakenly deleted an entry, quit the program without saving the file. The next time you open the program, the entry in question will be in the recycle bin again, where you can restore it. If you have activated the option to automatically save the database upon quitting Password Depot, you may need to refer to backup copies of your file.

Search Entries

The search function (Ctrl + F) can be found on the right in the toolbar, above the list of entries. It allows for searching entries in the currently opened database. Alternatively, you can select the tab *Search → Search*.

Note that the search function only scans entries that you can read. Entries protected by a second password that has not been entered yet are ignored.

In order to search an entry, enter a search term into the search field. The following attributes of an entry are scanned:

- Description
- Username
- URL
- Comments
- Category
- Tags
- Content (in information entries only)

You can refine your search with the following logical operators:

Keyword/Symbol	Examples	Function
NOT	social NOT security	Finds items that contain *social*, but not *security*.
	social security	Finds items that contain *social, security* or both.
OR	social OR security	Finds items that contain *social, security* or both.
Quotation marks	"social security"	Finds items that contain the exact phrase *social security*.
>	date:>11.05.2020 size:>500	Finds items with a modification date after 11.05.2020. Finds items with attachments whose size exceeds 500 bytes.
<	date:<11.05.2020 size:<500	Finds items with a modification date after 11.05.2020. Finds items with attachments whose size is less than 500 bytes.
..	date:11.05.2020..11.10.2020	Finds items with a date beginning on 11.05.2020 and ending on 11.10.2020.

Note that the operators are not localizable. Even if the program has a user interface language other than English, *AND/OR/NOT* should be used anyway.

Furthermore, the following filters are available:

- Entry type (type:): Currently, Password Depot supports the strings "Password", "CreditCard", "License", "Identity", "Information", "Banking", "EncryptedFile", "Document", "RDP", "PuTTy", "TeamViewer", "Certificate",

and "Custom". Note that these strings are not localizable; you will need to use the English terms regardless of the language of your user interface.

- Modify date (date:): Returns entries edited before or after a certain date, depending on the operator used. Password Depot supports the DD.MM.YYYY format for dates.
- Expiry date (edate:): Returns entries that expire before or after a certain date, depending on the operator used. Password Depot supports the DD.MM.YYYY format for dates.
- Attachments size (size:): Returns entries with attachments bigger or smaller than the specified size, depending on the operator used. The size is measured in bytes.

Advanced Search

The advanced search function (Ctrl + Alt + F) can be opened via *Search → Advanced.* It allows you to specify your search further with the use of various criteria. These criteria are:

- Description
- User name
- URL
- Comments
- Tags
- Modified before/after
- Expired before/after
- Category
- Importance
- Attachment size
- Entry type

Click *Start search* to launch the search. Entries matching your criteria will then be displayed at the bottom of the window. To work with one of the entries, right-click it and choose an action.

By clicking *New search,* you can clear the entries and launch a new search. Click *Close* to exit the window.

Search and Replace

The *Search and replace* function (Ctrl + R) can be found under *Search → Search and replace*. It allows you to search your entire database for a string of characters and to replace it with another.

- Search for: Enter the character string you are searching for.
- Replace with: Enter the new string.
- Folder: Select the directory from which the search should start.
- Search in: Restrict the fields in which you want to search.

WARNING: This operation cannot be undone.

Print Entries

To print entries, click *Database* → *Print*.

After authenticating correctly, you can see a print preview of your entries. With the arrow buttons, you can flip the pages, With the plus and minus symbols, you can change the scale of the page. Furthermore, you can export your entries to a PDF file.

Content

Here, you can define what you would like to print. You can print all or only selected entries. Additionally, you can define in which order passwords should be printed.

You can furthermore define which fields of the selected entries should be printed. Please note that the *Descriptions* field is always required and cannot be deselected. By default, the number of attachments is printed as well, but not the attachments themselves.

Layout

Here, you can adjust the layout of the pages you would like to print. If desired, you can give the document a title. Additionally, you can choose to print it either in portrait or landscape orientation and define the margins and the fonts of the title, folders and entries.

Click *Print* to finish.

NOTE: The printout of your passwords is a highly confidential document. Please make sure that no unauthorized persons gain access, and store it in a secure location.

Synchronize Entries

The *Synchronize databases* function in the Tools tab can be used to compare two databases and update them.

First, select the file with which you would like to compare the currently opened file and click Open. Next, authenticate for the second file.

You will now see an overview of all differences. On the left-hand side, you will see the file with which you are synchronizing your current file ("External File"). On the right-hand side, you will see your current database ("Current File"). To help you compare the two databases, the size and the date of the last modification will be displayed for each of the two.

The entries are sorted into three categories:

- Not existing entries
- Different entries
- Identical entries

The modification date will be displayed next to each modified entry to help you decide which version to use in which database in the future. To view the differences in more detail, right-click an entry and select *View differences*.

In the middle, you can define what to do with the entries. To do so, click on the action field and select an option from the drop-down menu. Here, you can adopt changes from either database in the other. Furthermore, you can delete entries. In the bottom left, you can see *Recommended actions*.

Lastly, click *Synchronize* to finish.

Organizing Entries in Folders

Password Depot allows you to create folders to better organize your entries. To do so, right-click the root folder in the navigation area, select *New*, and name the folder.

Repeat this process to create sub-folders.

Entries can be moved to a folder by drag&drop.

Folder Properties

Right-click a folder and select *Properties* in order to view and edit its properties.

In the *General* tab, you have the following options:

- Name: Here, you can change the name of the folder.
- Change icon: You can choose between standard or custom icons. *Reset icons* allows you to restore the default icon.
- Category: Assign a category to this folder.
- Comments: Add further information, if desired.

Furthermore, you can see the type and the location of the folder here. If the folder is the root directory, this field will be empty. Additionally, you can see further information on the contents of the folder here.

In the *Security* tab, you can protect the folder with a second password.

Sharing Entries and Folders

When working with databases on the Enterprise Server, users can grant access to individual entries or entire folders with other users or groups on the server. If sharing entries is permitted on the server, users or groups that would normally not have access to certain data can get temporary access without having to involve an administrator.

Right-click the object you would like to share and select *Grant access (Shift + Ctrl + G)*. Select a user or group you would like to grant access. With the options *Valid from* and *Valid to*, you can set a time limit. If you do not want to set a time limit, simply remove the checkmark from *Valid to*. Under *Access level*, you can define what permissions the user or group will have. The following options are available:

- Use: The user/group can use the entry/folder.
- Read: The user/group can open the entry/folder and view it in plain text.
- Modify: The user/group can make changes to the entry/folder.
- Delete: The user/group can delete the entry/folder.

Click *Next*. If desired, you can seal the entry. Find out more about sealed entries here. Lastly, click *Finish.*

Shared entries

Under *Tools → Shared entries*, Enterprise Server users that are allowed to share entries with other users or groups can see which entries or folders they have shared with whom. The following information is available:

- Description
- Path
- Shared with
- Valid from
- Valid to
- Permissions

Under *Revoke permissions*, you can retract granted permissions at any time.

Sealed Access

When sharing an entry or folder with another user, you have the option to seal the access. In this case, approval by an authorized person is necessary to open a shared entry or folder for the first time.

If you would like to seal an object, select the option *Seal access to the object*. Next, name one or more authorized people to grant approval. When you have entered all required information, click *Finish*.

NOTE: Only users with admin rights can grant approval for sealed entries or folders.

The user who has been granted sealed access can then sign in on the Enterprise Server with their login credentials. They will see the database containing the entry or folder they have been granted sealed access to. By double-clicking on that entry or folder, the user can request approval. To do so, they will have to give a reason for accessing the data and click *Request approval*.

An authorized person will have to grant approval in the Server Manager. You can find more information on that in our Enterprise Server Manual.

If approval has been granted, the user can double-click the shared entry or folder again. By clicking *Break seal*, the seal can be broken and the entry can be used according to the granted permissions.

NOTE: The seal status can always be changed by an authorized person. For instance, a broken seal can be reset, thus re-sealing the entry. In this case, the user has to request approval again.

Change Entry Type

When you select an entry, you have the option to convert it to another entry type by clicking *Entry → Change Type (Shift + Ctrl + T)*.

In the *Change entry type* window, you can see the following:

- Current type
- Convert to: Choose the new entry type for the selected entry.
- **Associate field names:** Here, you can define how to treat the fields of the current entry type during conversion.

WARNING: If you do not assign any fields, only the information that is present in the new entry type will be converted. To avoid data loss, make sure to assign fields during conversion since each entry type uses a different template.

Click *Convert* to finish.

TIP: You may select multiple entries of the same type and convert them into another type simultaneously, provided these entries are converted into the same target entry type.

Browser Add-Ons

Password Depot can fill in web forms with user names, passwords and other login data for you. There are two methods in which this can be done:

- The *Auto-Complete* function (lightning symbol)
- The browser add-ons

In this section, the browser add-ons will be explained in detail. Not only can they fill in logins on websites automatically for you, they can also adopt new login credentials directly into Password Depot. The browser add-ons are automatically launched along with the browser and always activate when you open a website with a login. Currently, we offer add-ons for the following browsers:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

If you do not want to use the add-ons, you can remove their checkmarks when installing the program. They can be deactivated retroactively in the respective browser.

NOTE: The add-ons do not work if a dialog window is open in Password Depot or if Password Depot is locked or closed.

Automatic Completion of Log-ins

If an entry has already been created for a website URL, user name, password and other data will be entered automatically.

TIP: The add-on symbol in the login fields of a website tells you if the add-on is available here.

If multiple entries are saved for an opened URL, the fields are not filled in automatically. Instead, click on the add-on symbol and select the desired login.

If you never want the browser add-ons to fill in your login credentials, remove the checkmark on the option *Auto-fill web forms using add-ons* under *Edit → Options (F10) → Browsers*.

If you do not want the browser add-ons to fill in your login credentials on specific websites, you can add those URLs to the list of ignored URLS under *Database → Database properties (Ctrl + I) → Content*. Alternatively, you can go to *Edit → Properties (Ctrl + M) → Additional* on each entry and deactivate the automatic completion there.

Add New Passwords from Web Browsers

If you log in on a website that has not been saved in Password Depot yet, you can allow the program to automatically ask you if a new entry with the credentials you just entered should be created. You can activate or deactivate this option in *Edit → Options → Browser*.

When the program asks you whether it should create a new entry, you can see its description, user name, password, URL and the folder in which the entry will be saved. You can continue by clicking *Add.* Clicking *Cancel* will end the process without saving the new entry.

TIP: You can pick a different folder within the database than the one you have currently opened for the new entry. However, no other database can be selected.

Update existing entries

In case you need to change your login credentials and do so directly on the website in the browser, Password Depot will ask if you would like to update the already existing entry. Click *Update* to save the changes in Password Depot.

Additional options

On the login site

If you click on the add-on symbol, you can copy the user name, the password and/or the URL to your clipboard. With the pen symbol, you can open the properties of the entry in Password Depot to edit it.

In the browser

If you click on the add-on symbol in the browser itself, the following options will be available:

- Search your depot: Search for an entry in your open database. With the respective symbols, you can copy data, edit the entry or open it in a new tab. Please note that the search currently only works with character strings present in the URL.
- Open native client: Opens the desktop client.
- Settings: Here, you can change the WebSocket port. Additionally, you can find the option *Auto-Fill when domain matches*. By default, this option is deactivated to avoid errors when filling in fields.
- Generate secure password: Opens the password generator.
- How secure is my password?: When creating a new password without the help of the generator, you can check how secure it is here. Please note that this is only an estimate.
- Visit Password Depot Website
- Rate us: We would be very happy if you could rate our add-on and its features!

TIP: If you have trouble with your add-on, please visit the Add-On section in our support center.

Auto-Complete

Password Depot can fill in web forms with user names, passwords and other login data for you. There are two methods in which this can be done:

- The *Auto-Complete* function (lightning symbol)
- The browser add-ons

In this section, the *Auto-Complete* function will be explained in detail. This function is available both in the client and in the top-bar. To fill out a website automatically with this function, follow these steps:

- Select an entry in the client or the top-bar.
- Click on the *Auto-Complete* button (lightning symbol).
- In the upper right, a window informing you of the *Auto-Complete* mode will open.
- Click the first field of the login that you want to be filled out. The fields in this window will then be filled in automatically.
- If you change your mind and do not want your login credentials to be filled in automatically, simply click *Cancel auto-complete* in the window that opened in the upper right when you clicked the lightning symbol.

NOTE: The order in which the data of an entry is entered can be defined in the *Auto-complete sequence* window. Such an auto-complete sequence is required for the auto-complete function to be used with an entry.

Auto-complete Sequences

An auto-complete sequence is the order in which fields in a website are filled with your user name, password and other data.

The *Auto-complete sequences* options can be opened with two methods:

- by going to *Edit → Auto-complete sequences (Ctrl + Q)*
- In the *Password* or *Properties* windows on the *Additional* tab

The *Auto-complete sequences* window includes the default auto-complete sequence of Password Depot. The following options are available here:

- Add: Add a new sequence.
- Edit: Allows for modifying an existing sequence.
- Delete: Removes a selected sequence.
- Delete all: Deletes all sequences except for the default sequence.

Adding or editing auto-complete sequences

When creating a new sequence or editing an existing one, the following options are available:

- USER: Adds a user name.
- TAB: Jumps to the next input element.
- PASS: Adds a password.
- Custom: You can also use your defined custom fields for auto-completion. For more information, see here.
- CLEAR: Clears content of target edit box.
- ENTER: Emulates the key "Enter".
- SPACE: Emulates the key "Space".
- Additional: Allows the addition of arrow keys, the keys *Home, Del, End, Backspace*, or a delay.

For the added elements, the following options are available:

- Up/Down: Moves elements in the sequence.
- Delete: Removes elements from the sequence.
- Delete all: Removes the entire sequence.

After creating the desired sequence, click *OK*.

Program Options

In the *Edit → Options* window (F10), you can configure important program features. The following tabs are available here:

- General
- Actions
- Hotkeys
- Top Bar
- Passwords
- Save
- Clipboard
- Layout
- Network
- Browsers
- Warnings

On the bottom left of each tab, you can reset any changes by clicking *Restore default settings*.

Certain security-related functions are not saved in the program options but in the database itself. You can find them in the database properties.

Options - General

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *General* tab:

User Interface

Here, you can set the language for the user interface.

Program start

- Start mode: Choose whether Password Depot should start in a normal window, minimized, in top-bar mode or in the last state it was used.
- Start in locked mode
- Launch application with Windows startup: If activated, Password Depot automatically starts when Windows starts. By clicking *Delay start*, you can define by how many seconds the Password Depot launch should be delayed.
- Open last used database at program start
- Store lists of used databases and key files: If you save a list of recently used databases and key files, you can see it on the *Recent Files* tab in the main menu and when opening a database.

Update settings

Here, you can decide if new updates should be automatically downloaded and prompt you to install them, if Password Depot should look for updates but only send you a notification, or if new updates should be ignored. Additionally, you can define an interval in which Password Depot looks for new updates.

Options - Actions

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Actions* tab:

Auto-Complete

- Open the password's URL first: If you select this option, the URL/local file which you have defined for this password will be opened before the auto-complete function starts.
- Window position
- Auto-complete delay: Determine a value for the delay with which the program enters data. This may increase the accuracy of the auto-complete function on slower computers.

NOTE: These options refer to the auto-complete function (F6, lightning symbol), not the browser add-ons.

Double-click actions

- Action # 1: Select the option which you want to be taken if you double-click on a password in your database.
- Action # 2: If it makes sense with your first action, you can select another option here that will be taken after the first one.

Minimize program

- Automatically minimize when the program is inactive for: Here, you can define after which period of not using Password Depot the program should minimize automatically.
- Minimize when the Close button is clicked: If you select this option, the program is minimized instead of closed when you click the *Close* button.
- Minimize to system tray: With this option, you can set the program to be minimized into the system tray.

Close database and lock program

Here, you can define if and when Password Depot should automatically close the currently opened database and lock itself.

- When the computer is idle for: Here, you can define after which period of not using the computer the program should minimize and lock automatically.
- When the current user (session) changes: The program is automatically minimized and locked when the active desktop user or terminal session changes.

- When the computer enters standby/hibernate mode: The program is automatically minimized and locked when the computer goes into standby or hibernate mode.
- When the program is auto-minimized: If you select this option, the program is locked automatically when it is auto-minimized.
- Always when program is minimized: If you select this option, the program is locked automatically when it is minimized.

Options - Hotkeys

Password Depot uses a number of hotkeys that work both inside and outside of the program. You can view and edit them under *Options → Hotkeys*.

The following system-wide hotkeys are pre-defined by default:

Main window/Minimize	CTRL + ALT + R
Top bar/Minimize	CTRL + ALT + T
Find and insert username	CTRL + ALT + U
Find and insert password	CTRL + ALT + P
Find and auto-complete	CTRL + ALT + A
Insert selected username	CTRL + SHIFT + ALT + U
Insert selected password	CTRL + SHIFT + ALT + P
Auto-complete selected	CTRL + SHIFT + ALT + A

Additionally, you can dock Password Depot on the respective side of the screen by pressing WinKey + ← or →, minimize Password Depot by pressing WinKey + ↓, or maximize it by pressing WinKey + ↑.

Options - Top Bar

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Top bar* tab:

Position

- Floating: Allows you to move the top bar freely. If you select *Always top left*, the top bar will always open there initially, but can still be moved.
- Top screen edge: The top bar is always displayed on the upper edge of the screen. You can define whether it should always be on top of other programs and if it should be hidden automatically when you work with another program.
- Bottom screen edge: The top bar is always displayed on the lower edge of the screen. You can define whether it should always be on top of other programs and if it should be hidden automatically when you work with another program.
- Monitor: If you are working with multiple monitors, you can choose which one to display the top bar on.

Appearance

- Use theme colors: If activated, the top bar uses the same color scheme as the client.
- Custom colors: If you activate this option, you can determine the background color and the font color of the top bar yourself.
- Show bar captions: If this option is selected, you will see explanatory texts when you move your mouse over the symbols in the top bar.
- Show server database selector: When working with the enterprise server, you can use this drop-down menu to select any database on the server that you have access to.
- Show search box
- Transparency of bar
- Length of drop-down lists
- Width of Folder field
- Width of Password field
- Width of Search field
- Customize Top Bar: Allows you to define the functions of the top bar. More information can be found below.
- Large/Small icons

Customize Top Bar

Here, you can add functions to the top bar or remove functions that you do not need. In the *Customize top bar* window, you will see two lists. The one on the left lists available functions. The one on the right lists functions currently on your top bar. The following options are available:

- Add: Select a function and click *Add* to add it to your top bar.
- **Remove:** Select a function and click *Remove* to remove it from your top bar.
- Reset: Restores the default settings.

- Move up/down: Allows you to define the order of the functions on the top bar.
- User name as text button/Password as text button: Displays user names or passwords in plain text on the top bar. The option *Max. text length* allows you to define how many characters should be displayed at maximum.

Options - Passwords

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Password* tab:

Editing:

- Default auto-complete method: Here, you can define which auto-complete method is used by default.
- **Default auto-complete sequence:** Here, you can define which auto-complete sequence is used by default.
- Default expiration period for entries
- Show warning for expired entries: If you check this option, you will receive a warning by the program if entries have expired. The option *Days to warn before expiry* allows you to define how many days you will receive a warning before entries expire.

Master Password Policy:

Here, you can define global default settings for the passwords you create with the Password Generator. The following options are available:

- Minimum length
- Password must include: Allows you to define what character types passwords will be made up of.
- Enforce password history
- Password expires in: Allows you to define for how many days a password is valid. Note that expired passwords can still be used. This function merely serves as a reminder to change your passwords regularly.
- Minimum password age: Allows you to define how many days a password should be old before it can be changed.

Options - Save

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Save* tab:

Save and backup

- Auto save database on every change: If you activate this option, any change to your database will be saved automatically.
- Create a backup copy on database saving: If you select this option, a backup file of your database will be created each time you select *Save* or *Save As* from the *Database* menu, or *Save* on the tool bar.
- **Create a backup copy on database opening:** If you select this option, you can create backups via *Database → Backup*.
- Number of stored backup copies: Allows you to define how many backup files you would like to keep at maximum.

Remote databases

Here, you can define if local copies of databases from Internet servers should be saved or deleted after signing out, if local copies of Enterprise Server databases should be saved, and if Enterprise Server databases that were edited in the offline mode should be synchronized automatically next time you connect to the server. Please note that you need permission from an administrator for the latter two options.

Working directories

Here, you can see and edit the default directories for databases and backup files.

Options - Clipboard

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Clipboard* tab:

Clipboard

- Delete password from clipboard after: Here, you can define after how many seconds Password Depot automatically clears copied data from the clipboard.
- Hide clipboard changes from external viewers: With this function, Password Depot hides changes made to the clipboard for increased security.

NOTE: Password Depot only recognizes particular clipboard viewers. Therefore, it does not replace a full-featured anti-spyware program. Learn what to do when Password Depot recognizes a clipboard viewer here.

Options - Layout

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Layout* tab:

Entries font

Allows you to change the font used for your entries.

Display

Here, you can select what information on your entries will be displayed in the main view. The following options are available:

- ! (Importance)
- Description
- # (Entry ID)
- URL
- Username
- Password
- Type
- Modified
- Expiry date
- Category
- Comments
- Last accessed

TIP: If you click one of these layout categories in the main view, your entries will be sorted accordingly.

Expired entries

Here, you can define what to do with expired entries:

- Hide expired entries from the list
- Hide expired entries from the search results

Options - Network

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Network* tab:

Enterprise Server

- Default authentication mode: Here, you can select a default authentication method for signing in on the Enterprise Server. This method will be pre-selected in the login window of the Enterprise Server. You can choose from *Integrated Windows Authentication (SSO)*, *Sign in with user name and password* or *Azure AD Authentication*.
- **Internet Protocol version:** Choose between IPv4 and IPv6.
- Automatically reconnect on network errors: If you activate this option, you can define under *Reconnect interval* after how many seconds Password Depot should attempt to reconnect. Under *Reconnect attempts*, you can define how many times Password Depot should attempt to reconnect at maximum.

SSL/TLS options

If your administrator has installed a certificate for the Enterprise Server, activate the option to use an SSL/TSL connection here, and decide if the server certificate should be verified.

Options - Browsers

In the program options (*Edit → Options (F10)* or the gear symbol), you can change the following settings in the *Browsers* tab:

Internet Browsers:

Here, you can define which browser Password Depot should use by default to open URLs. It can be opened via F5. You can either select a browser from the list of browsers recognized by Password Depot or add a custom browser by clicking *Custom browsers...* To do so, follow these steps:

- Click *Add*.
- Enter a description of the browser.
- Enter a path to the .exe file of the browser, either manually or by clicking *Browse*.
- Optionally, define additional parameters.
- Lastly, click *OK*.

Browser add-ons

- Auto-fill web forms using add-ons
- Automatically select passwords in top bar: If the program is set to the top bar mode and you manually enter an URL into the browser, the program automatically selects the matching password, provided there is one saved with the current URL. For this function to work, the browser add-ons must be activated.
- Add new passwords from web browsers
- Warn about identical passwords for different URLs
- **WebSockets port:** Here, you can define or change the WebSockets for Password Depot. By default, Password Depot 17 uses 25109.
- Protect access with a password: If this option is activated, you will have to enter an additional password before working with the add-ons. When activating this option, a window will open, in which you can set your password. You can edit this password by clicking *Change*. If you would like to deactivate this option, you will have to enter the password again before you can do so.

NOTE: All browser add-on options refer to Mozilla Firefox, Google Chrome, Microsoft Edge and Internet Explorer since we currently offer add-ons for these browsers only.

Add-ons online:

Here, you can retroactively install the add-ons in the respective browsers.

Options - Warnings

In the *Warnings* tab of the program options (*Edit → Options (F10)* or the gear symbol), you can define which warnings Password Depot should send you. The following options are available:

- Weak master password.
- Recommendation to use secure FTP protocol.
- Extraction of encrypted data on disk.
- Too many entries in the root folder.
- The database is too large.
- Data copied to the Clipboard.
- Password Depot is running in locked state.
- Disconnected from Password Depot Enterprise Server.
- Moving of non-empty folders.
- Switch to offline mode.

Select all options by clicking *Check all.* Deselect all options by clicking *Uncheck all*.

Virtual Keyboard

The virtual keyboard allows you to enter characters without using your physical keyboard when creating or editing entries. It does not simulate keyboard typing so that neither hardware nor software loggers can intercept any input.

Click the desired keys with your mouse to enter them.

By clicking on *Settings*, you have the following options:

- Emulate fake cursors: If activated, multiple fake cursors will be emulated to protect you from other persons who might be watching your screen.
- Disable press effect: If activated, the keys you click on will not be highlighted.

Global Custom Fields

Global custom fields, which can be accessed via the menu *Edit*, provide frequently used custom information without having to add an individual custom field for each new entry.

- Add field: Creates a new field. Name it and enter a value.
- Edit field: Here, you can edit the name or value of an existing field.
- Delete field: Removes a custom field from your list.
- Up/Down: Changes the order of the custom fields.
- Hide: Activate or deactivate this option to show the values of password-type fields in plain text or hide them respectively.

Creating a new Global Custom Field

If you click the plus in the *Global Custom Fields* window, you will need to enter the following information:

- Name: Enter a name for the field or choose one from the list.
- Type: Select a type for this field.
- Value: Enter a value for the field.
- **Input element:** Here, you can enter the name of an appropriate HTML input element.

Key Shortcuts

To quickly access the most important functions of Password Depot, use the following key shortcuts:

Function	Shortcut
Favorites	ALT + C
Save Database	CTRL + S
Save Database As	CTRL + ALT + S
Print Database	CTRL + P
Close Database	CTRL + W
Backup Now	CTRL + B
Lock	CTRL + L
Exit	ALT + F4
Add Password	CTRL + Ins
Modify Password ("Properties")	CTRL + M
Delete	CTRL + Del
Database Properties	CTRL + I
Copy password to clipboard	F2
Copy user name to clipboard	F3
Copy URL to clipboard	F4
Open URL in standard browser	F5
Auto-complete	F6
Select all	CTRL + A
Auto-complete sequences	CTRL + Q
Search	CTRL + F
Advanced search	CTRL + ALT + F
Search and replace	CTRL + R
Options	F10
Program help	CTRL + H
Program help for specific functions	F1

NOTE: The shortcuts listed above are fixed and cannot be edited by users. Password Depot additionally uses customizable system-wide shortcuts that work both inside and outside of Password Depot. Learn more in the Hotkeys section.

Password Generator

The Password Generator is a tool for creating random passwords. It can be opened in different ways:

- in the dialog windows for adding (*Edit → New*) or modifying (*Edit → Properties*) entries, via the star symbol
- in the top bar by clicking on the star symbol
- with the browser add-ons

When generating a new password, you can choose between the *Standard* and the *Advanced* generator.

Standard

On the *Standard* tab, you have the following options:

- Character types to include in the password
- Length: Allows you to define the maximum length of a generated password. The upper limit is 256 characters.
- Exclude characters: Allows you to define characters that the password should not include. By default, a number of similar-looking characters is listed here. You can edit this list however you like.
- Password policy: Here, you can choose whether the new password should adhere to existing global policies.

To generate a password with the standard password generator, move your cursor over the green field with random data. Your mouse movement will select random characters, which make up the password. It will be displayed in the *Password* field. The *Clear* button empties the password field, allowing you to generate a new password. By clicking *Show/Hide*, you can display it in plain text or hide it. By clicking *Copy*, you can copy it to your clipboard.

Click *OK* to copy the password to the clipboard or save it in the window for adding or modifying entries. If you want to end the process without saving the password, click *Cancel.*

Advanced

The advanced password generator allows you to generate secure, random passwords while defining precisely what characters it should contain. These settings can be saved as templates for future entries.

The following options are available:

Template

- Custom template: Select this option to create your own template. You can save it by clicking *Save*. Templates that you do not need can be removed by clicking *Delete*.
- Default settings for new passwords: Automatically adopts global default settings.
- Deduce settings from current password: This setting will be automatically selected if you already have a password for an entry. In this case, the settings from the old password will be adopted for the new password.

Password settings

- Password length
- Use only following characters: If this option is activated, the password can only consist of the characters you have defined here.
- Use following character types with relative frequencies: Allows you to define what character types the password should consist of and what percentage of the password each character type should make up. By clicking *Custom*, you can add your own characters. Please note that only the first 256 ASCII characters are supported.
- Use at least one character of each type selected above
- Exclude characters: Allows you to define characters that the password should not include. By default, a number of similar-looking characters is listed here. You can edit this list however you like.
- Exclude consecutive identical characters
- **Exclude strings from dictionaries:** Select this option to avoid strings of characters that can be found in dictionaries to increase security.

Generator

- Generate: Creates a random password based on your settings. With the arrow button, you can define how many passwords the generator tries out in order to find the best result.
- Password: The generated password will be displayed here. Below, you can see its quality. The bluer and fuller the bar is and the higher the estimate on how long it would take to crack the password is, the more secure your password is.
- Hide/Show: Shows the password in plain text or hides it.
- Copy: Copies the password to the clipboard.

Click *OK* to copy the password to the clipboard or save it in the window for adding or modifying entries. If you want to end the process without saving the password, click *Cancel.*

Partial Password Builder

You can open the partial password builder

- by right-clicking an entry
- via *Entry → Partial password*
- in the top bar by clicking the table icon

The partial password method is an authentication method for passwords that increases protection from password theft. It prompts users to only enter a number of characters of a password instead of the entire password. This way, key loggers are prevented from recording the password.

In the partial password builder, you can see the following lines:

- Position: Each character is assigned a number.
- Password: Lists the characters of the password.
- Select: Allows you to select individual characters by checking the boxes.
- Partial password: Generates the partial password based on your selection.

When creating a partial password, you have the following options:

- Hide Password: Allows you to show the password in plain text or hide it.
- Always on top: If activated, the *Partial Password Builder* will always be visible in the foreground.
- **Copy to clipboard:** Copies the partial password to the clipboard.
- Close: Closes the partial password builder.

Security check

You can check the quality of your passwords by going to *Tools* → *Security Check*.

In the wizard, you can select which entries should be assessed. You have the following options:

- All entries in the database
- Entries in the active view
- Selected entries in: Allows you to select a folder whose contents should be checked. If desired, you can include sub-folders as well.

Furthermore, you can select or deselect individual entries.

Via *Check in Pwned passwords*, you can check if your credentials are known to have fallen victim to security breaches.

Click *Next* to analyze the selected entries. The results will show you the following information:

- !: Shows you the importance of an entry.
- Description
- Entropy: Shows you the security of an entry in bit. The higher the number, the more secure the password.
- Dictionary: Shows you how similar the password is to words or other character strings that can be found in dictionaries. The lower the percentage, the more secure the password.
- Quality: Shows the quality of the password as a colorful bar. The fuller and bluer the bar, the more secure your password.
- Strength: Tells you how secure your password is in words.

If you click on the title of a column, the entries will be sorted accordingly. The option *Display only vulnerable entries* allows you to only display entries that Password Depot deems unsafe.

To improve the quality of a password, select it and click *Edit*.

Lock Password Depot

This function is one of the most important local security features of Password Depot. It guarantees that unauthorized persons cannot view your database while the program runs on your computer. Please note that you cannot carry out any actions or use the browser add-ons while the program is locked.

Lock Password Depot

You can use the lock function in multiple ways:

- via *Database → Lock (Ctrl + L)*
- via the lock symbol on the right in the client or on the top bar

Moreover, in the Options on the *Actions* tab, you can set Password Depot to lock itself automatically after a period of inactivity.

Unlock Password Depot

To unlock Password Depot, click the Password Depot icon in the tray bar and authenticate correctly for the current database.

Encrypt, Decrypt and Erase External Files

Password Depot allows you to encrypt, decrypt or erase external files, regardless of their format. The encryption uses the AES 256-Bit algorithm.

You can find the functions *Encrypt external files*, *Decrypt external files* and *Erase external files* in the *Tools* menu.

Encrypt external files

- Select *Tools* → *Encrypt external files.*
- Select the file(s) you want to encrypt and click *Open*.
- Enter your desired password in the dialog field *Password Depot - Encrypt* and repeat it. By clicking *Generate*, you can generate a password. By clicking *Show/Hide*, you can display the password in plain text or hide it. The quality of the password will be displayed as a bar.
- If desired, select the following options:
  - Delete original file(s) after encryption: Permanently deletes the original file.
  - Create a self-extracting archive: Allows users who have not installed Password Depot to open the file.
  - Store password with Password Depot: Saves the password in Password Depot.
- Click *Encrypt* to finish.

Decrypt external files

- Select *Tools* → *Decrypt external files*.
- Select the encrypted (.pwde) file you want to decrypt, and click *Open*.
- Enter the password of the file in the *Password Depot - Decrypt* window.
- If desired, you can select *Delete encrypted files after decryption* if you no longer need the decrypted file.
- Click *Decrypt* to finish.

Erase external files

With Password Depot, you can permanently delete files from your hard drive. These erased files cannot be restored, not even by specialized programs, since they are overwritten multiple times during their deletion. To erase files, follow these steps:

- Select *Tools* → *Erase external file.*
- Select the file(s) you would like to delete and click *Open*.
- Password Depot will warn you that the selected file(s) will be deleted. If you want to permanently delete them, click *Erase.*

Search Duplicates

The function *Tools → Search for duplicates* allows you to search for duplicated user names, passwords and URLs. While multiple entries may use the same user name or URL, passwords should never be identical.

It is possible to combine the analysis by selecting multiple categories. Here, the operators AND and OR are available.

Click *Find Duplicates* to launch the search. The results will be listed according to your selected categories.

If you right-click on the list of the results, the following functions are available:

- Edit: Opens the entry for editing.
- Delete: Deletes the entry from the database.
- Open URL: Opens the URL of the entry in the browser.
- Select all: Selects all entries in the list of the results.

By clicking the *Export* button, you can export the list of possible duplicates into an external CSV file.

Mode

Password Depot can be run in three different modes. The selected mode defines what functions are available. In order to change modes, click *View → Mode*.

Expert Mode

In the expert mode, all functions of the program are available. Thus, it is best suited for users who are already familiar with the program and want to use all of its features.

This mode is only available in the trial version and the full version.

Beginner mode

In beginner mode, only the simplest and most basic functions are available. Due to its limited range of features, it is best suited for users who are not familiar with Password Depot yet and/or only want to work with its basic features.

This mode is available in all versions. In the freeware version, it is the only mode that can be used.

Options

The following options can be found in *Edit → Options (F10)* or the gear icon in the upper right:

User Interface

Here, you can set the language for the user interface.

Internet Browser

Here, you can define which browser Password Depot should use by default to open URLs. It can be opened via F5. You can either select a browser from the list of browsers recognized by Password Depot or add a custom browser by clicking *Custom browsers...*

Browser add-ons

- Auto-fill web forms using add-ons
- Automatically select passwords in top bar: If the program is set to the top bar mode and you manually enter an URL into the browser, the program automatically selects the matching password, provided there is one saved with the current URL. For this function to work, the browser add-ons must be activated.
- Add new passwords from web browsers
- Warn about identical passwords for different URLs

- **WebSockets port:** Here, you can define or change the WebSockets for Password Depot. By default, Password Depot 17 uses 25109.
- Protect access with a password: If this option is activated, you will have to enter an additional password before working with the add-ons. When activating this option, a window will open, in which you can set your password. You can edit this password by clicking *Change*. If you would like to deactivate this option, you will have to enter the password again before you can do so.

NOTE: All browser add-on options refer to Mozilla Firefox, Google Chrome, Microsoft Edge and Internet Explorer since we currently offer add-ons for these browsers only.

Custom mode

The custom mode allows you to define which of Password Depot's features you would like to work with and which ones should be hidden. Of course, only features that are not required for Password Depot to work properly can be deactivated.

This mode is only available in the trial version and the full version.

Edit Custom mode

Clicking *Edit Custom mode* opens the *Custom Mode Editor* window. On the left, you will see a list of available categories. If you click a category, the commands (i.e. functions) included in it will be displayed on the right, where you can select the functions that you would like to work with. The following categories are available:

- Edit including the commands *Auto-complete sequences*, *Duplicate*, *Categories*, *Internet server* and *Global custom fields*
- Entry including the commands *Copy TAN N/A to clipboard*, *Create Shell link*, *Print*, *Generate Password*, *Partial password builder*, *Edit TAN N/A*, *Mark TAN N/A as used*, and *Regenerate password*
- File including *Save as* and *Backup*
- Folder including *Properties*
- Search including *Advanced search* and *Search and Replace*
- Tools including *Import*, *Export*, *Encrypt external files*, *Decrypt external files*, *Security check*, *USB installation*, *Erase external files*, *Synchronize databases*, *Clean-up* and *Search for duplicates*

Click *OK* after making all desired adjustments.

Clipboard Monitor Alert

This dialog window opens when Password Depot attempts to copy sensitive data to the clipboard and detects an unknown application that monitors changes made to the clipboard.

NOTE: This alert does not necessarily mean that you are dealing with a genuine threat or an infection. It is primarily a notification that you should investigate.

If this window is displayed, you have the following options:

- Protect: Hides changes made to the clipboard.
- Ignore: Ignores the application. Select this option if you are sure that the application does not pose any threat.
- Cancel: Closes the window without carrying out an action.
- Save selection: If this option is activated, Password Depot will apply the selected option to future processes as well.

NOTE: Password Depot cannot guarantee that there are no clipboard viewers on your PC. It only recognizes certain kinds of clipboard viewers and therefore does not replace a full-featured anti-spyware program.

Technical Support and FAQs

We are happy to offer you the best support possible when it comes to questions and problems regarding Password Depot.

Please visit our website to view all available support options.

In addition to our technical support, you can also find an overview of frequently asked questions about Password Depot as well as their answers here. Please click here to find the FAQs in our knowledge base.

If your question was not answered in the FAQs and you need a quick solution, please visit our community.

License Agreement

The license agreement for Password Depot can be found in the installation wizard and on our website.

Contacting AceBIT GmbH

Would you like to order Password Depot? Please click here to get to the order page for Password Depot Version 17.

If you have technical queries or problems regarding one of our software products, please visit our Help Desk.

Address: AceBIT GmbH
Holzhofallee 15
64295 Darmstadt
- Germany -

Phone: +49 61 51 136 50-0

Fax: +49 61 51 136 50-20

Email: info@acebit.de

You can reach us between 9:00AM and 5:00PM on business days. Please note that we do not offer a support hotline. Support inquiries will only be answered via our Help Desk or our Community.

Inquiries will usually be answered within 48 hours on business days.