



**PASSWORD
DEPOT**
BY AceBIT

User Manual Password Depot 19

Welcome to Password Depot	10
What is special about Password Depot?	10
Security	10
High Functionality	11
What's new?	13
Getting Started	14
Quick Start	14
Installation	16
Installing Add-Ons	17
Unlocking Password Depot to the full version	18
Enter License Key (Unlock Code)	18
Upgrade from Previous Versions	19
Update Manager	20
Introduction	21
How to Use this Manual	21
Professional Version Benefits	22
Know-how on Password Security	23
User Interface	24
General Description	24
Password area	24
Navigation area	24
Types	24
Categories	25
Status bar	25
Tool bar	25
Tab bar	25
Details	25
Customize View	27
Password Area	27
Navigation Area	28
Types	28
Categories	28

Statusbar.....	28
Toolbar	29
Tab bar	29
Details.....	29
Sort by.....	30
Direction.....	30
Group by	30
Virtual Keyboard	31
Topbar Mode	32
Databases	34
Add Databases	34
Open Databases	36
Save Databases	37
Save	37
Save as.....	37
Home	38
Home.....	38
Home - New Database	42
Home - Local System	44
Home - Enterprise Server	45
Enterprise Server: Login.....	46
How to authenticate on the Enterprise Server?	46
Home - Internet Server	50
Examples for entering an Internet server	52
Home - Dropbox	54
Home - Google Drive.....	56
Database Manager - OneDrive	58
Home - HiDrive Cloud	60
Home - Box Cloud	62
Home - Local backups.....	64
Database Properties.....	65
Database Properties	65
Properties - General	66
Properties - Content.....	67

Database objects	67
History	67
Recycle bin.....	68
Properties - Advanced	69
Passwords policy	69
Second password.....	69
Properties - Notes.....	70
Properties - Backup	71
Remote backup locations	71
Remote backup settings.....	71
Properties - Entries	72
Properties - Security	73
Database Authentication.....	74
Enter Master Password.....	74
Forgot your (Master) Password?	74
Entering a wrong Master Password.....	74
Change Master Password	74
Change Authentication	75
Key File Generator	76
Backup Copies of Database	77
Backups.....	77
Backup location.....	77
Create Backup Files.....	78
Creating backup files manually	78
Creating backup files automatically	78
Open Backup Files	79
Entries	80
Adding & Modifying Entries.....	80
Basic Entry Operations.....	80
Add Entry.....	80
Modify Entry	82
Entry Type: Password	83
Add/Modify Entry - Remote Desktop Connection.....	85
Add/Modify Entry - TeamViewer	87
Entry Type: PuTTY Connection.....	89
Entry Type: Credit Card	91

Add/Modify Entry - Banking.....	93
Entry Type: Software License	95
Add/Modify Entry - Identity.....	97
Entry Type: Information.....	99
Entry Type: Encrypted File.....	100
Add/Modify Entry - Document.....	102
Entry Type: Certificate.....	104
Entry Type: Custom	106
Entry Type: Linked Entry	108
Advanced Entry Operations	109
Add/Modify Entry - Tab URLs.....	109
Add/Modify Entry - Tab Additional.....	110
Add/Modify Entry - Tab Custom Fields.....	114
Add/Modify Entry - Tab TANs.....	115
Add/Modify Entry - Tab Attachments.....	116
Add/Modify Entry - Tab Versions.....	117
Add/Modify Entry - Tab Conditional Access.....	118
Add/Modify Entry - Security Tab	119
Importing & Exporting Entries.....	120
Importing and Exporting Passwords	120
Exporting Entries.....	121
Supported Formats for Export	121
How to Export	121
Import Wizard	123
Supported Import Formats	123
Import process	123
Import Wizard - CSV File Import	125
Import Wizard - Import from other password managers.....	127
Import Wizard - Import Completed.....	129
Cleaning-up & Deleting Password Entries.....	130
Clean up Password Entries.....	130
Delete Passwords.....	132
Recycle Bin	133
Program-internal Password Entry Functions.....	134
Search Password Entry.....	134
Advanced Search.....	137

Search and Replace.....	138
Sort Password Entries.....	139
Print Password Entries.....	140
Content.....	140
Layout.....	141
Synchronize Password Entries.....	142
Compare Entries.....	143
Organize Entries in Folders.....	144
Categorize Password Entries.....	145
Grant Access to Entries.....	146
Seal Entries.....	148
Change type.....	150
Using Password Entries on the Internet.....	151
Key Shortcuts.....	151
Open URL.....	153
Open URL with.....	154
Copy Information to Clipboard.....	155
Auto-completion of Web Forms.....	156
Browser Add-Ons.....	156
Ignored URLs.....	159
Auto Completion.....	160
Auto-complete Sequences.....	161
Clipboard Monitor Alert.....	163
Passwords.....	164
Security Check.....	164
Generating Passwords.....	167
Password Generator.....	167
Standard.....	167
Advanced.....	168
Passphrase.....	169
Advanced Password Generator.....	171
Template.....	171
Password settings.....	171
Generator.....	172
Partial Password Builder.....	174

Master Password Generator	175
Password Depot Operations	177
Lock Password Depot.....	177
Lock Password Depot.....	177
Unlock Password Depot.....	177
USB Installation.....	179
Mobile Versions	180
Operating System Android	180
Operating System iOS.....	180
Command Line Parameters.....	181
PasswordDepot.exe.....	181
pdFileTools.exe	181
Encrypt & Decrypt External Files.....	182
Encrypt external files	182
Decrypt external files.....	182
Erase external files.....	183
Erase External Files	184
Global Custom Fields	185
Creating a new Global Custom Field.....	185
Search Duplicates.....	186
Offline Mode.....	187
Required settings on Password Depot Enterprise Server.....	187
Required settings in Password Depot Client.....	187
How to use the offline mode.....	188
Offline mode access conditions.....	188
Offline Access with Standard Authentication (Password Depot user credentials)	189
Offline Access with Integrated Windows Authentication.....	190
Offline Access with OpenID Connect.....	192
Customize Password Depot.....	195
Customize Browsers.....	195
Customize Icons.....	196
Standard	196
Custom.....	196

Customize Appearance	198
Password Area.....	198
Navigation Area.....	199
Types.....	199
Categories.....	199
Statusbar.....	199
Toolbar.....	200
Tab bar.....	200
Details.....	200
Sort by.....	201
Direction.....	201
Group by.....	201
Program Options	202
Program Options.....	202
Options - General.....	203
User interface.....	203
Program start.....	203
Update settings.....	204
.....	204
Options - Actions.....	205
Auto-complete.....	205
Double-click actions.....	205
Minimize program.....	205
Close database and lock program.....	206
Options - Hotkeys.....	207
Options - Topbar.....	208
Position.....	208
Appearance.....	208
Options - Customize Top Bar.....	210
Options - Passwords.....	211
Editing.....	211
Master Password Policy.....	211
Options - Save.....	213
Save and backup.....	213
Remote databases / Databases from Enterprise Server.....	213
Working directories.....	213

Options - Clipboard.....	214
Clipboard.....	214
Options - Layout.....	215
Options - Network.....	216
Enterprise Server.....	216
SSL/TLS Settings.....	217
Options - Browsers.....	218
Internet browsers.....	218
Browser add-ons.....	218
Add-ons online.....	218
.....	218
Options - Warnings.....	219
Options - Search.....	220
User Modes.....	221
User Modes.....	221
Expert Mode.....	222
Beginner Mode.....	223
Options.....	223
Custom Mode.....	226
Edit Custom Mode.....	227
Support.....	229
Technical Support / Frequently Asked Questions (FAQs).....	229
Personal and Business customers:.....	229
Business customers:.....	229
License Agreement.....	230

Welcome to Password Depot

Congratulations for choosing **Password Depot** for the administration and protection of your passwords and access data! You are in good company: **Password Depot** is used by several thousands of businesses, banks, government agencies, and private users.

You want to start immediately, without having to read the entire user manual? Our [quick start instructions](#) will help you in this regard.

Moreover, for a quick start, you may find our [video tutorials](#) helpful, too!

What is special about Password Depot?

Password Depot is a **powerful, technically mature**, and, most importantly, **secure** application for managing your passwords and access data. Unlike conventional freeware and shareware utilities, **Password Depot** provides sophisticated security mechanisms and a well-conceived, wide range of functions. It was developed for operation in professional environments with strict security standards.

Security

Password Depot provides extremely high security standards in multiple ways:

- **Encryption with AES-256:** The software encrypts databases using the Rijndael 256 algorithm, also known as AES-256 (**Advanced Encryption Standard**). According to the state of the art, currently this is certainly the most secure method of encrypting data on a computer. In the United States of America, AES is accepted for national documents with the highest level of security clearance! One advantage of this security algorithm is that the **master password** for encrypting a database is not stored on your computer. Therefore, nobody can possibly find the **master password** on your computer. You are the only person who knows this password.

- **Anti-keylogging protection:** All passwords have an internal protection against various types of keylogging.
- **Clipboard protection:** **Password Depot** automatically detects active clipboard viewers and hides any changes to the clipboard that it makes; after auto-completion, all sensitive data is automatically removed from the clipboard. Furthermore, Password Depot prevents recording of data copied to the Clipboard history on Windows 10 Release 1809 or higher.
- **Program protection:** Several new options optimize the protection of **Password Depot** itself: Whenever the program enters the locked mode, all sensitive data is cleared from the memory. The program is able to auto-minimize/auto-lock whenever the computer switches to standby or hibernation mode, whenever the current session changes, etc.
- **Highly secure shredding method:** **Password Depot** uses a shredder conforming to the DOD 5220.22-M specification of the US Department of Defense to delete temporary program files. The definite, irrevocable deletion of temporary files is also 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, because in fact only the filename will be deleted this way. To destroy a file beyond recovery, you must overwrite the file before deleting it.
- **Lock function:** You can restrict other users' unauthorized access to **Password Depot** using the program's lock function. This way, you can leave the software running on your computer without risking someone else looking through your passwords.

High Functionality

Password Depot protects your important and confidential passwords and access data from external access – whilst offering maximum user-friendliness and a comprehensive range of functions!

- The integrated **Password Generator** creates virtually uncrackable randomized passwords. These can be inserted into the corresponding website field by using drag & drop. **Password Depot** generates true-random data, which cannot be predicted. Many conventional generators create random data based on system time and thus 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 through 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 place your encrypted databases on the **Internet** and enjoy access to all of them, no matter your location!
- The **tab bar** allows working with multiple databases simultaneously, significantly simplifying remote management.
- The **Server Module** allows for simultaneous shared access to databases on a network by several clients in teams and companies. The system or network administrator assigns certain rights to the clients. For example, they can determine whether files may only be opened in read-only mode or may be modified.
- Furthermore, free **apps for smartphones** allow for using the software on mobile devices. iOS and Android are our currently supported operating systems.

We hope that this brief introduction to the main features of **Password Depot** has given you a good overview and made it easier for you to get started with the program. If you have any questions or suggestions, please do not hesitate to contact us. Our [Technical Support / FAQs](#) team is happy to help you.

We wish you great success and enjoyment in using **Password Depot**!

What's new?

Our software is continuously developed, updated, and enhanced to ensure optimal performance. In order to see what makes this current version better than the previous versions, please visit our [website](#).

See also: [Update Manager](#)

Getting Started

Quick Start

You want to start immediately, without having to read the entire user manual? The following instructions will help you in this regard:

1. [Installing Password Depot](#).

In order to be able to add passwords directly from the browser and for information to be filled in automatically on websites, you need to install the browser add-ons. If these add-ons are not installed, passwords can only be added manually and the completion process needs to be started manually. (The add-ons can also be [installed subsequently](#).)

2. Starting [Password Depot](#).

3. Creating a [new database](#), by clicking on [Home](#) → [Local system](#) → [New Database](#).

4. [Opening](#) a database by authenticating yourself with the method defined in step 3.

5. Adding passwords by clicking on [Edit](#) → [New](#) → [Password](#). If add-ons are installed and activated, you can simply log in to the browser directly and [Password Depot](#) will offer you to save this information in the opened database.

6. Creating folders to better organize your entries. To create a folder, right-click on the left navigation panel (similar to Windows Explorer) and select [New](#).

7. If necessary, make [changes](#) to the entry, by clicking on [Properties](#).

HINT: To ensure the password is filled in on every page of the website, add a URL ([URLs](#) tab) mask to the entry. E.g. [*domain.com*](#)

8. 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-completion](#).

Installation

To install **Password Depot** on your computer, please follow these steps:

1. Go to the **Password Depot** [website](#) and select the **Download** menu.
2. Click on the indicated download link for your desired version.
3. Then select the folder where you wish to save the file or **execute** the file directly.
4. Follow the instructions of the installation wizard.
5. To ensure passwords are filled in automatically in browsers, you need to install add-ons (e.g. for Google Chrome, Microsoft Edge or Mozilla Firefox). Tick the relevant boxes in the installation wizard.
6. After successful installation, always go to the **Update Manager (Help → Search for Updates)**. This way, you always ensure using the latest version of **Password Depot**.
7. Go to **Help → Unlock** to enter your valid license key (unlock code) you received by e-mail to [unlock the program](#).

Installing Add-Ons

To enhance the user experience, Password Depot also offers add-ons for various web browsers such as Chrome, Edge, and Firefox. These add-ons enable seamless integration of Password Depot into the respective browser, making it easier to access stored passwords.

However, the installer for Password Depot cannot automatically install the add-ons. Web browsers have strict security policies to protect user privacy and system integrity. As a result, they typically do not allow automatic installations of add-ons or extensions from third parties, as this could pose a security risk.

To install an add-on for Password Depot on your preferred web browser, simply visit the corresponding web store:

- [Firefox](#)
- [Chrome](#)
- [Microsoft Edge](#)

Alternatively you are able to download the add-on by clicking onto [Help](#) → [Add-Ons](#) and choosing the browser add-on of your choice.

Unlocking Password Depot to the full version

To use **Password Depot** in its full version you must first activate the software. If you prefer to use the trial version, you can do so without activation.

The software activation is executed within the program itself. To do so, please click on **Help → Unlock** (if your version of Password Depot has already been activated, you won't see this option). A new dialog window should open, offering two options:

- If you have already purchased a license key (an unlock code), select **Step 2 – Unlock Password Depot**.
- Alternatively, by selecting **Step 1 – Purchase a License Key online**, you get to the website, where you can order a license key (an unlock code).

Enter License Key (Unlock Code)

After having selected one of the two options mentioned above, you will now possess a valid license key. Now, please enter it in the corresponding field. You will receive the license key always when **ordering the software**.

The wizard will show you whether the unlocking process has been successful or not. If so, you will now be able to work with the program as full version.

NOTE: You can check if your activation of the program has been successful if you go to **Help → About Password Depot**. If you can see here below **installed license key** an actual license key, you have unlocked the software successfully.

See also: [Professional version benefits](#); [Upgrade from previous versions](#)

Upgrade from Previous Versions

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

1. First, you will have to **order** the relevant upgrade for your version. The purchase of upgrades is less expensive than purchasing new full versions.
2. Having completed your order, you will receive a **license key** (an unlock code) for the current version.
3. Now **install** the current version. If your old version is no longer installed on your PC, you do not need to re-install it. If it is already/still installed, however, you do not need to uninstall it. Yet, we would recommend an uninstallation as this enables a better overview and, in case of uninstallation, installing Password Depot's current version again.
4. **Open** the newly downloaded current version.
5. Go to **Help → Unlock** and select **Step 2 – Unlock Password Depot**.
6. Follow the wizard's instructions. Afterwards, enter the **license key** (unlock code) you received when ordering the license.
7. Finally, you can open your database from the old version in the new, activated version: In the main menu, go to **Home → Local system** and select the path to your file. By default, your file is to be found at "Documents". Confirm your choice with **Open** and authenticate yourself for the file by using your master password and/or key file.

NOTE: For very old versions, it may be helpful to open your database in the old version first, followed by conversion to XML. Subsequently, create a new, empty database in Password Depot and import your XML file.

Update Manager

The **Update Manager** enables you to keep your software always up-to-date.

To open the Update Manager, click on **Help → Search for Updates**.

After you have launched the Update Manager, the program connects to the AceBIT server and checks if newer versions of **Password Depot** are **available**. If this is the case, the new version will be downloaded and installed on your PC.

Use this function regularly to find out whether a new version is available.

NOTE: The **Update Manager** only installs updates that are **free of charge** (e.g. from version 18.0.4 to 18.0.5), not however fee-based upgrades from one version to a higher one (e.g. from version 17.0.5 to 18.0.0).

Introduction

How to Use this Manual

This guide offers explanations for all functions of [Password Depot](#) .

If you need help on a certain topic, you can enter the corresponding keyword into the [Index](#) tab or into the [Search](#) tab. In the latter case, all topics using the keyword you entered will be displayed.

Whenever you need assistance for an action you are carrying out at that moment, you can call up the corresponding help topic by pressing either the **F1** key or the [Help buttons](#) within the respective dialog boxes.

If a topic is missing in the manual, please contact our technical [support](#).

In order to facilitate working with the user help guide, different text contents are differentiated from one another by their design:

- [Hints](#) are highlighted in blue.
- [Examples](#) are highlighted in yellow.
- [Notes](#) are highlighted in green.
- [Warnings](#) are highlighted in red.

Professional Version Benefits

These are the advantages of the [licensed professional version](#) of **Password Depot**:

- **No restrictions on the number of databases:** In the licensed version (and the 30-day trial), you can create and use an unlimited number of databases, whereas the freeware version allows you to manage one database file only.
- **No restrictions on the number of passwords:** In the licensed version (and the 30-day trial), you can manage an unlimited number of passwords, whereas the freeware version allows you to manage 20 passwords only.
- Free usage of the **Password Depot Enterprise Server** for up to 3 users: The licensed version of **Password Depot** allows you to use the Enterprise Server with up to three users for free. A separate server license is only required for greater numbers of users.
- Registered users can request help from our [technical support](#) via email whenever they have questions or problems (usually within 72 hours during work days).
- **Notification about upgrades** and other products via email.
- The integrated **Update Manager** automatically keeps your software up-to-date.

Click here to go to the [online ordering page](#).

See also: [Activation](#)

Know-how on Password Security

Our [website](#) offers important know-how on the notion of password security:

- [Tips for Strong Passwords](#): Get to know some basic rules for creating safe passwords.
- [How Does The Encryption Algorithm Rijndael Work?](#): This page explains how the Rijndael encryption algorithm works and why it is regarded as particularly secure.
- [More Security With The Use Of Password Depot](#): Learn how to store all your passwords securely and how to delete confidential data irrevocably.
- [Brute-Force Attacks](#): Find out more about brute-force attacks and how you can protect yourself against them.
- [Secure Password Management In Companies](#): Advice for how to improve your team's or company's security.
- [Identical Passwords](#): This article explains why using identical passwords is a bad idea and the risks involved.

User Interface

General Description

The user interface is divided into the following areas: The password area, the navigation area, the status bar, the toolbar, the tab bar 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 displays the credentials for your passwords. It displays the description of your passwords and additional 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 hierarchic 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

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

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 bar with information on your version, license status/remaining days in trial mode, number of objects, local system or network, and statistics.

Tool bar

The tool bar is above the navigation and password area. 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.

Tab bar

The tab bar is positioned above the toolbar and displays all currently open databases. This layout facilitates efficient management and operation when working with multiple databases. To open additional databases, click the **Start** button.

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**)

If you have added a URL to the entry, you can open it by clicking on the **blue-highlighted link**.

Below the icons in the details section, the **entry and its associated data** — such as the username and password—are displayed. If the entry includes a **TOTP code**, it will also be shown along with the remaining validity time in [seconds].

Customize View

The user interface consists of a maximum of five simultaneous windows or areas: **Password area**, **Navigation area**, **Statusbar**, **Toolbar**, **Tab bar** and **Details**.

Password Area

This is the main window. It is therefore placed in the center of the screen and cannot be closed or hidden.

This window provides access to your passwords.

A password's description and additional **information** can be displayed such as last modified, user name, URL, and category. Go to **Edit → Options → Layout** and change the layout according to your personal needs.

If the details view is enabled, you can select the details that should be displayed by right clicking on the details bar.

- You can select a different view for the list of passwords in the **View** tab.
- To edit password entries, switch to the **Edit** tab or **right-click on an entry**. This way, you can add, modify, delete, and print entries.

By right-clicking on an entry, you open the **password menu**. The menu's functions can only be used, however, if the information needed for this function – e.g. a TAN – is existent.

With this menu, you can:

- **modify ("Properties")**, **delete** or **print** the selected password(s), similar to the functions in the **Database** and **Edit** tabs.
- **cut**, **copy**, **insert** and **duplicate** the entry or add it to your list of favorites.
- copy the password's information to the **clipboard**.
- create a **Windows Shell Link**. This is a shortcut to a password that you can save anywhere on your system (e.g. on your desktop) and that allows you to access the password quickly.

From within the **Password Area window**, you can also move passwords from one group to another. Just select the passwords you want to move in the navigation area to the left of

Password Depot (which means this feature needs to be activated) and then drag & drop them into the desired group.

Navigation Area

This area displays a hierarchic structure of the folders inside the opened database, similar to Windows Explorer. Additionally, it also displays the [Favorites](#), the [Recycle Bin](#) and the [Search Results](#) after a search for quick access.

Types

In the navigation area, you can display the list of all types of entries available in Password Depot no matter if you have already used those entries or not. In general, you will see all entry types here. Double click a specific type of entry to display all entries of the same type currently available in your database in the main view. This will temporarily hide all other types of entries within the database in the main view and might be helpful, for example, if you would like to work with "Password" or "Information" entries only for some time.

Categories

You can do the same with the categories of your database. In the navigation area, all available categories will be displayed, that is both the built-in ones as well as the categories you created yourself. If your entries have been assigned to specific categories, you can double-click on a specific category in the navigation area to call up all entries that belong to the corresponding category (all types of entries included). Those entries will then be displayed in the main view. This way, you can search for entries using the categories they have been assigned to and display them in the main view.

If you are using the [Enterprise Server](#), you can quickly access the files from the server. To display the files in this area, click on [View](#) and activate the option [Databases on Server](#). The files on the server are only displayed if you are connected and logged in to the server.

Statusbar

If you have set the [Statusbar](#) function under [View](#), you will find a blue bar at the bottom edge of Password Depot, including information for version, license status (or remaining days for the trial mode), number of objects, "local system" (or network), and overall statistics (number of folders and passwords/entries).

Toolbar

Above the navigation and password areas, you will always find the **Toolbar**, offering quick access to Password Depot's important core functions, e.g. **Password** (create new password, second symbol from the left). Further to the right, there is a box/field for a file **path** as well as the basic **search function** ("Search entry").

Tab bar

The tab bar is positioned above the toolbar and displays all currently opened databases. This layout facilitates efficient management and operation when working with multiple databases. To open additional databases, click the **Home** button.

Details

This window is situated on the right side of the screen.

Its purpose is to display the information of a selected password in a more compact manner, so that required entries can be identified more quickly.

Furthermore, different actions are available in the details area which can be useful for your entries:

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

With these actions you can easily access any data stored in Password Depot and further use it.

HINT: If you have added custom fields to an entry, you will also see them in the details area on the right. However, information will not be displayed in clear text but hidden. If you want to read it, click on the eye icon. The information will be shown in clear text for

a short time. Next to it you can use the corresponding icon for pasting the information of a custom field to the clipboard.

NOTE: If you select the icon for **Custom Fields** in the details area, both custom fields referring to this entry and global custom fields which you may have added under **Edit** → **Global custom fields** will be displayed here. Thus, you can select the required information.

You can also see a star in the details area on the right. A yellow star means that this entry is one of your favorites.

Sort by

Here, you can choose how password entries are sorted, e.g. by their **Description** or **Importance**. When choosing the option **Custom sort**, you can change the arrangement of entries in the password area via **Drag & Drop** accordingly. To do so, select an entry from the list, and drag & drop it to the correct position.

Direction

Decide whether the sort order should be in **Ascending** or **Descending** order.

Group by

Choose if and how the entries should be grouped. They can be grouped either by their **Type** or **Category**.

Virtual Keyboard

The **virtual** (on-screen) **keyboard** allows you to insert keystrokes directly into password fields or whenever creating/modifying entries – without using the physical keyboard. The virtual keyboard does not emulate keyboard events, so no hardware or software keyloggers can intercept entered keystrokes.



Use the mouse to dial the strings for a target edit box.

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

- **Emulate fake cursors:** When enabled, multiple fake cursors will appear on your screen to help protect your activity from prying eyes.
- **Disable press effect:** When enabled, the keys you click on will not be highlighted.

Topbar Mode

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

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](#)
- [Database Manager](#) (Home screen)
- [Save Database](#)
- [New Password](#)
- Copy [Global custom fields](#) to clipboard
- [Favorites](#)
- [Copy URL](#)
- [Partial Password](#)
- [TOTP](#)
- [Password Generator](#)
- [Modify Password](#)

- Username
- Password
- **Custom fields:** Copies the content of custom fields to the clipboard.
- TAN
- Insert Data
- Suggest
- Open URL
- Auto-complete (**F6**)
- Restore (**Ctrl** + **T**): Restores the main view of the client.
- Lock (**Ctrl** + **L**)
- Minimize
- **Exit:** Closes Password Depot.

Databases

Add Databases

To create a new database, proceed as follows:

- Open the Home section by clicking on [Home](#).
- Click [New database](#).
- Name the new database.
- Choose the storage location by clicking on the drop-down menu or on [+ New](#) if the storage location should not yet be displayed. You can choose from the following:
 - Internet Server (FTP / WebDav / HTTP)
 - Dropbox
 - Google Drive
 - Microsoft OneDrive
 - Microsoft OneDrive for Business
 - Box Cloud
 - HiDrive Cloud
- Click on [Next >](#), to proceed with the creation of the database.
- **Encryption options:** Choose a [primary password](#), a [primary password](#) and a [key file](#) or only a [key file](#).
 - When choosing an authentication method that uses a primary password, enter a desired primary password or generate one with the [master password generator](#) by clicking the star symbol. Re-enter the primary password. Its quality will be displayed below. Enter a hint for your primary 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 **Next >** when you are done.
- Lastly, you are able to enter any **Comments** or **Decryption hints** to the database description which may help you remember your primary password if it may have been forgotten.
- Click on **Finish** to finalize the creation of the database.

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.

Open Databases

1. Open the database manager by clicking on [Home](#).
2. Select the desired storage location of the database.
3. Select a database and click on [Open](#).
4. Enter your credentials to authenticate.

If you should not find your database in the list, click on [Search](#) and search for the respective database.

Save Databases

To save the opened database manually, click on **Database → Save** or **Save as**.

Save

This function saves the current database. During this process, the currently opened file is overwritten with the changes that were made during the active session.

Save as

The **Save as** function basically fulfills the same purpose as the **Save** function, with the single difference that you can specify another name for the file, so you do not overwrite the old original file.

HINT: Go to **Options → Save** and check the option **Autosave database on every change**.

Home

Home

With the release of **Password Depot 18**, a new **home screen** was introduced. This screen simplifies navigation and provides an improved overview of your databases and their storage locations.

The **Home** screen serves as central interface and replaces the database manager. It displays all available storage locations – for faster and more intuitive access.

The global navigation (**Home**, **Local system**, **PD Enterprise Server**, **Add location storage**, **Local backup**) offers the possibility of saving and illustrating the exact storage location, as well as displaying previously used databases.

Databases can be created and saved in the following locations (each of which has its own tab within the **Home section**):

- [Local system](#)
- [PD Enterprise Server](#)
- [Internet Server \(FTP / WebDav / HTTP\)](#)
- [Dropbox](#)
- [Google Drive](#)
- [Microsoft OneDrive / Microsoft OneDrive for Business](#)
- [Box Cloud](#)
- [HiDrive Cloud](#)
- [Local backup](#)

Global Navigation

On the **left side** of the start screen, there is a global navigation panel that provides access to all available storage locations.

Home Tab

When opening the start page, the [Home tab](#) is displayed by default.

Getting Started

In the [Getting Started](#) section, the following options are available:

- Connect to [Enterprise Server](#)
- [Create a new database](#)
- [Open an existing database](#)

Databases

The [Databases](#) section displays a list of the [most recently used databases](#). By clicking on [Favorites](#), you can directly access your preferred databases.

The list includes the following information:

- Name of the database file
- Storage location
- Opened
- File size

Location storage

Also within the [Home](#) tab, you will find the [Location Storage](#) section. Here, you can access:

- [Local databases](#) (local system)
- The [Password Depot Enterprise Server](#)
- [Additional storage locations](#), such as OneDrive

You can also add new storage locations from this section by clicking on [Add location storage](#).

HINT: After adding a new storage location, you can modify its name and properties by right-clicking the entry, as long as the storage type allows such changes.

Local System

Via the **toolbar**, you can:

- Open databases
- Create new databases
- Delete existing databases
- Navigate between folders
- Specify paths
- Refresh the view
- Filter results
- Search for databases

PD Enterprise Server

Clicking on **PD Enterprise Server** opens the login dialog for connecting to the Enterprise Server.

Add location storage

To add a new storage location, select a provider from the list (e.g., OneDrive) to store your database there. After you have authorized the desired provider, it will be listed in the list by default.

Backups

In the **local backup** tab, all locally stored **backup files** of your databases are displayed.

Using the **toolbar** in the tab **local backup**, you can:

- Open

- Delete
- Move
- Refresh
- Filter
- Search

these backup files.

Home - New Database

In **Password Depot**, you have different options to create a new database.

- 1. Click on **Database → New database**.
- 2. Click on **Home →** button **New database**.
- 3. Click on **Home → Local system → New database**.

The dialog box **New database** contains the following elements:

- **Database name:** Enter a valid file name without path and file extension, e.g. "My passwords". The database will be saved under the name specified here with the file name extension ".pswe" or ".pswd" , so that you can easily find it again later.
- **Storage location:** Select the storage location for the database. By clicking on **+ New**, additional options are available.

Then click **Next >**, to continue with the following encryption options fields:

- **Protect with:** Here you can choose from three different methods to protect the database:
 - **Primary password:** The conventional and – depending on the complexity of the master password – secure method for encrypting a database with a primary password.
 - **Primary password and key file:** The database is protected with a primary password and, in addition, a key file.
 - **Key file:** The database is protected with a key file. Key files contain complex keys that are very secure and cannot be cracked even by brute-force attacks. However, keep in mind that anyone who has access to both your key file and your database can access your passwords! Therefore, you should treat the key file like a real "safe key" and always keep it in a secure place (e.g. on a USB stick).
- **Master password:** You use the master password to open your database. If you forget this password, there is no way to open your database anymore! If you have chosen authentication via primary password, enter your desired main password here or open the [master password generator](#) (the second asterisk icon to the right of the input field) to have a particularly secure master password generated. Using the eye

icon next to the input field, you can hide your password entry or display it in plain text.

WARNING: If you forget your main password and you have not specified a hint, or the hint does not help you, there is NO way to view the passwords in the affected database anymore! Therefore, use a password that you can easily remember.

- **Re-enter password:** Repeat the master password you entered previously. Both entries must be identical, otherwise the password will not be accepted!
- **Quality of the password:** Indicates how secure your main password is. The larger the bar becomes, the more secure your password is. Never use passwords for which the bar is shown in red – stick to green or blue bars. You will also be shown approximately how long it would take a professional hacker to crack the password. Using the **pwneD?** button, you can check whether similar passwords have been compromised in the past.
- **Key file:** If you have chosen authentication via key file, enter the path to an existing key file here by clicking the first button to the right of the input field to select an existing key file. Click the second button to open the [Key File Generator](#) and create a new key file.

Then click **Next >**, to continue creating the database. In the final step of creation, add **comments** or **decryption hints** that could serve as a reminder if you forget your password.

Finally, click **Finish** to complete the creation of the database.

Home - Local System

In **Password Depot**, you can open and save databases on your local system. To do so, please open the [Home](#) screen and click on the tab **Local system**. The following options are now available:

- **Open:** Opens a database selected in the list. Select the database from the list and click on **Open**.
- **New database:** Enables you to create a new database on your local system. A detailed description of this process is provided [here](#).
- **Delete database:** Deletes a selected database from the list.
- **Back:** If you changed folders in the browser, with this button, you can jump back to the previous folder.
- **Forward:** If you jumped back/changed a folder previously, with this button, you can jump forward again.
- **Level up:** Changes over to the next higher-order folder/directory.
- **Refresh:** Refreshes the list of databases on your local system, e.g., after you have made changes to the files.
- **Filter:** Filter the current overview of your databases as desired.
- **Search:** Allows you to search the local system for a specific database and then to load it.

The list shows all recently used Password Depot databases that are stored **locally**.

Home - Enterprise Server

In **Password Depot**, you can open and save databases on the Enterprise Server module. To do so, please open the [Home](#) screen and click on the tab **PD Enterprise Server**. The following options are now available:

- **Sign in:** Directs you to the login site of the Enterprise Server. Here, you enter all of the information indicated below this list. After login, all databases that you can access will be listed. Alternatively, you can also use the integrated Windows authentication, if available – for this purpose, click on the right arrow button. Further, since version 12.0.7, optional Two-Factor Authentication has been implemented when connecting to the Enterprise Server. The administrator is able to activate Two-Factor Authentication for the client's server login. If this option is selected, clients need to enter both user name and password (if standard authentication is used) as well as a particular code they will receive during login process. You can read more about Two-Factor Authentication [here](#).
- **Sign out:** Logs you out of the Enterprise Server.
- **Open:** Opens a database selected in the list. For this purpose, select the desired database in the view and then click on **Open**.
- **Refresh:** Refreshes the list of available databases saved on the Enterprise Server.
- **Change server password:** Allows you to change the password for Enterprise Server.
- **View server certificate:** If a certificate was installed earlier, you can view its details here.
- **Search:** If there are multiple databases, search for the desired database in the corresponding Enterprise Server.

NOTE: Databases for the Enterprise Server can only be created via the server's control panel. In case you would like to share a file on your local PC with other users, you would need to send this file to the system administrator first.

NOTE: Once you have opened a database from the Enterprise Server, you can quickly and easily switch between the databases you have access to in the tab bar without having to reopen the home screen.

Enterprise Server: Login

Having clicked on [Sign in](#), you will need to indicate your server information:

- **Server address:** Type in the address from which **Enterprise Server** is executed. Generally, this is a local address, e.g. 90.0.0.1.
- **Port:** Enter the port through which Password Depot can be reached. A specific default port is defined for every main version. For **Password Depot 19**, the default port is **25019**.
- **Authentication:** Select the correct authentication mode (**Standard Authentication** with username/password, **Integrated Windows Authentication**, **Windows Domain Credentials**, **Azure AD/Entra ID**, **OpenID Connect** or **WebAuthn/Passkeys**).
- **Domain / Username:** The domain of the server and/or your username.
- **Password:** Enter your password here.

Finally, click on **OK**.

NOTE: In the **Enterprise Server** tab, you can only open files which you are allowed to access. Those rights are assigned to you by your server administrator. If you have logged on to the Enterprise Server successfully and see a message that no database has been assigned to your user's account yet, please contact your server administrator because otherwise working with the Enterprise Server will not be possible at all.

How to authenticate on the Enterprise Server?

In general, the server administrator decides how users should authenticate on the Enterprise Server. Thus, when connecting to the Enterprise Server, it is only required for users to select the correct authentication mode to establish a secure client to server connection. The **Password Depot Enterprise Server Login window** offers different authentication modes to choose from:

- **Standard Authentication (username & password)**
- **Integrated Windows Authentication (SSO)**
- **Windows Domain Credentials**
- **Azure AD/Entra ID**

- [OpenID Connect](#)
- [WebAuthn/Passkeys](#)

Standard Authentication

You can use the [Standard Authentication](#) to connect to the Enterprise Server if your Password Depot Server administrator has created local users and assigned usernames and passwords to single users. To login, enter the username and password which was assigned to you by your server administrator and also make sure to use the correct server address and port.

Integrated Windows Authentication

If you would like to use the Integrated Windows Authentication, also called [Single Sign-On](#), to login on the Enterprise Server, you have to be a member of an Active Directory. Besides, your server administrator must perform the Active Directory synchronization in the Server Manager (prior to the user login) to add Active Directory users to the Password Depot server. If this is the case, please select the Integrated Windows Authentication in the [Password Depot Enterprise Server Login window](#) and make sure to use the correct server address and port. Your Windows NT access data will then be used to login. If settings are correct, your logon name as well as the corresponding domain are already displayed in the login window. Finally, just click **OK** to proceed and establish a client to server connection. The access data sent will be validated in the background and you will be logged in as soon as the data has been proven valid.

Windows Domain Credentials Authentication

With [Windows Domain Credentials](#) authentication, you log on to the Enterprise Server using your Windows domain credentials. To use this method, your user account must be a member of an Active Directory domain. In addition, your server administrator must have added you as a user in the Server Manager as part of Active Directory synchronization.

If these prerequisites are met, select [Windows Domain Credentials](#) in the [Password Depot Enterprise Server Login](#) window and make sure that the server address and port are correct. Then enter your domain user name (e.g. `DOMAIN\username` or `username@domain.tld`) and the corresponding password.

Click [LOGIN](#) to start the sign-in process. Your domain credentials are verified in the background. If the account and password are correct and your account has the required permissions, you are logged on to the Enterprise Server and can open the server databases that have been shared with you.

Azure AD/Entra ID Authentication

If you would like to use the [Azure AD/Entra ID](#) Authentication, you have to be a member of an Azure Active Directory. Besides, your server administrator must perform the Azure AD synchronization in the Server Manager (prior to the user login) to add Azure AD users to the Password Depot server. If this is the case, please select the Azure AD Authentication in the [Password Depot Enterprise Server Login window](#) and make sure to use the correct server address and port.

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

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

Open ID Connect Authentication

This authentication method allows users to log in using credentials from an OpenID Connect (OIDC) identity provider. Once integrated, users can be imported from the external provider into the Password Depot Server and authenticate directly through the Password Depot Client using their federated credentials.

To authenticate via OIDC, ensure that the Password Depot Server administrator has configured [at least one valid OpenID Connect provider](#) in the server settings. If required, obtain the server address and port number from your administrator.

In the Password Depot Client, enter the server address and port number, select [OpenID Connect](#) as the authentication method, and choose the predefined OIDC identity provider from the drop-down menu. If the identity provider does not appear, click the [Discover Identity Providers](#) button (green icon) to initiate a discovery request to the server.

Next, click [Login](#). You will be redirected to the identity provider's login page. Enter your external account credentials (e.g., Microsoft Entra ID, Auth0) and, upon successful authentication, you will be redirected back to the client and granted access to the server – based on your assigned roles and permissions.

WebAuthn/Passkeys Authentication

The [WebAuthn/Passkeys](#) authentication method enables passwordless login to the Enterprise Server. Instead of a password, you use a WebAuthn/FIDO2-based authenticator, such as a FIDO2 security key, Windows Hello or another compatible passkey.

To use this method, your server administrator must have enabled WebAuthn in the Server Manager and registered at least one passkey for your user account. If necessary, ask your administrator for the correct server address and port number.

In the [Password Depot Enterprise Server Login](#) window, select [WebAuthn/Passkeys](#) as the authentication method and verify the server settings. Then click [LOGIN](#) to start the authentication process. The corresponding WebAuthn dialog of your operating system will open. Follow the instructions shown there – for example, touch your FIDO2 security key, enter a PIN if required, or confirm the login using fingerprint or facial recognition via Windows Hello.

After successful cryptographic verification, you are automatically logged on to the Enterprise Server and, based on your assigned roles and permissions, gain access to the server databases that have been shared with you.

Home - Internet Server

In **Password Depot**, you can open and save databases on an Internet server. To do so, please open the [Home](#) screen, click on **Add location storage** and then on **Internet Server (FTP / WebDav / HTTP)**. A new dialog window will open where you are able to edit the settings of the Internet Server:

Name: Enter a custom name for the storage connection.

Service: Choose a service type. The following services are available to you:

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

Protocol: Select the file transfer protocol.

Advanced...: Click here to access additional configuration options (only available for SFTP, FTPS, and FTPES).

Address: Enter the domain or IP address of your remote server (e.g. ftp.example.com).

Port: Specify the port used to connect to the server. If set to "Auto", the application will use the default port for the selected protocol.

Path: Enter the directory path on the remote server where your files should be stored or retrieved.

User name: Enter the user name used to log in to the server.

Passive: The terms "active" and "passive" refer to the server's behavior during data transmission with a client. In passive mode, the server is passive: the client initiates the data connection. In active mode, the server takes initiative and requests the client to specify which port to use for data transfer. However, if a firewall is active on the client that blocks incoming connections, it may interrupt this connection – thus also halting data transmission. Conclusion: If the client's firewall does not allow incoming connections, passive FTP should be used.

NOTE: The "passive" option is only available and applicable when **FTP** is selected as the protocol.

Password: Enter your password. You can click the eye icon to show or hide the entered text.

NOTE: You can only upload new files to the cloud server if the internet protocol selected is **FTP** or **SFTP** – this is not possible with the HTTP or HTTPS protocols. To view and/or change this setting, navigate to the **properties of the entry** by right-clicking on it in the Home list.

HINT: It is generally recommended to use the SFTP protocol, as it allows both read and write access and is more secure than the FTP protocol. However, if you only need read access to a file located on the Internet, the HTTP protocol is sufficient.

If Internet Server entries have already been added to Password Depot, the following actions are available:

- **Open:** Opens a selected database. To do this, select the desired file in the view and click **Open**.
- **New database:** Create a new database. A detailed description of this process can be found [here](#).
- **Delete database:** Delete a selected database from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.

- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the database list view.
- **Filter:** Choose which file formats should be displayed in the storage location's list view.
- **Search:** Search for specific databases in the selected storage location.

Additionally, storage locations can be edited, renamed, or deleted by selecting a location storage and right clicking on it:

- **Properties:** Edit the properties of a storage location.
- **Rename:** Rename a storage location.
- **Delete:** Delete a storage location from the list.

Examples for entering an Internet server

EXAMPLE 1: You would like to store your passwords and access them via FTP in the directory **privatestuff** on your web server with the domain <http://www.myserver.com>. The complete path using a browser would thus be <http://www.myserver.com/privatestuff/>

First you create an FTP account for this directory in your provider's control panel and assign this FTP account the directory `/privatestuff` as the home directory. Any user who logs in to your server using this FTP account will only see this directory.

- **Protocol:** FTP
- **Host:** myserver.com
- **Path:** /

EXAMPLE 2: You wish to store your passwords in the directory **privatestuff** on your web server with the domain <http://www.myserver.com>. The complete path using a browser would thus be <http://www.myserver.com/privatestuff/>

You do not want to create a new FTP account, but use your main account, which gives you access to all directories on the server. This means you have to specify the directory **privatestuff** as the path.

- **Protocol:** FTP
- **Host:** myserver.com
- **Path:** /privatestuff

EXAMPLE 3: You would like to access a database, but only know its URL, not the FTP access data. The file is stored under the URL <http://www.myserver.com/privatestuff/secret.psw>.

- **Protocol:** HTTP
- **Host:** www.myserver.com
- **Path:** /privatestuff

NOTE: You will enter the file names when creating or opening databases. In the **Manage Internet Servers** dialog box, you only specify server information.

Home - Dropbox

In **Password Depot**, you can open and save databases on Dropbox. To do so, please open the [Home](#) screen, click on **Add location storage** and then on the option **Dropbox**. The following options are now available:

- **Open:** Opens a selected database. To do this, select the desired file in the view and click **Open**.
- **New database:** Create a new database in Dropbox. A detailed description of this process can be found [here](#).
- **Delete database:** Delete a selected database from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.
- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the database list view.
- **Filter:** Choose which file formats should be displayed in the storage location's list view.
- **Search:** Search for specific databases in the selected storage location.

Additionally, storage locations can be edited, renamed, or deleted by selecting a location storage and right-clicking on it:

- **Properties:** Edit the properties of a storage location.
- **Rename:** Rename a storage location.
- **Delete:** Delete a storage location.

If you save your databases on Dropbox, Password Depot uses the following default path:

```
\Apps\Password Depot\
```

WARNING: It is strongly recommended **not** to create this path manually. Instead, log in to Dropbox with Password Depot and allow the program to create the path, in case it does not yet exist. Once Password Depot has created the directory/folder, you can upload your existing password databases through Windows Explorer or your browser.

NOTE: Whenever you deposit your databases on a cloud service, your confidential data **always** "touch" the data medium of the cloud service in AES 256-bit encrypted format – never unencrypted. Your databases are always and only decrypted locally.

Home - Google Drive

In **Password Depot**, you can open and save databases on Google Drive. To do so, please open the [Home](#) screen, click on **Add location storage** and then on the option **Google Drive**. The following options are now available:

- **Open:** Opens a selected database. To do this, select the desired file in the view and click **Open**.
- **New database:** Create a new database in Google Drive. A detailed description of this process can be found [here](#).
- **Delete database:** Delete a selected database from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.
- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the database list view.
- **Filter:** Choose which file formats should be displayed in the storage location's list view.
- **Search:** Search for specific databases in the selected storage location.

Additionally, storage locations can be edited, renamed, or deleted by selecting a location storage and right-clicking on it:

- **Properties:** Edit the properties of a storage location.
- **Rename:** Rename a storage location.
- **Delete:** Delete a storage location.

WARNING: Since Google changed its policy, resulting in certain permissions no longer being available, the use of Google Drive is generally **not** recommended. More information can be found [here](#).

If you save your databases on Google Drive, Password Depot uses the following default path:

```
\Password Depot\
```

WARNING: It is strongly recommended **not** to create this path manually. Instead, log in to Google Drive with Password Depot and allow the program to create the path, in case it does not yet exist. Once Password Depot has created the directory/folder, you can upload your existing password databases through Windows Explorer or your browser.

NOTE: Whenever you deposit your databases on a cloud service, your confidential data **always** "touch" the data medium of the cloud service in AES 256-bit encrypted format – never unencrypted. Your databases are always and only decrypted locally.

Database Manager - OneDrive

In **Password Depot**, you can open and save databases in OneDrive. To do so, please open the [Home](#) screen (menu **Home** → **Add location storage**) and click on the option **Microsoft OneDrive** or **Microsoft OneDrive for Business**, respectively. The following options are now available:

- **Open:** Opens a selected database. To do this, select the desired file in the view and click **Open**.
- **New database:** Create a new database in OneDrive. A detailed description of this process can be found [here](#).
- **Delete database:** Delete a selected database from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.
- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the database list view.
- **Filter:** Choose which file formats should be displayed in the storage location's list view.
- **Search:** Search for specific databases in the selected storage location.

Additionally, storage locations can be edited, renamed, or deleted by selecting a location storage and right-clicking on it:

- **Properties:** Edit the properties of a storage location.
- **Rename:** Rename a storage location.
- **Delete:** Delete a storage location.

If you save your databases on OneDrive, Password Depot uses the following default path:

```
\Files\Documents>Password Depot
```

WARNING: It is strongly recommended **not** to create this path manually. Instead, log in to OneDrive with Password Depot and allow the program to create the path, in case it does not yet exist. Once Password Depot has created the directory/folder, you can upload your existing password databases through Windows Explorer or your browser.

NOTE: Whenever you deposit your databases on a cloud service, your confidential data **always** "touch" the data medium of the cloud service in AES 256-bit encrypted format – never unencrypted. Your databases are always and only decrypted locally.

Home - HiDrive Cloud

In **Password Depot**, you can open and save databases on HiDrive. To do so, please open the [Home](#) screen, click on **Add location storage** and then on the option **HiDrive Cloud**.

The following options are available:

- **Open:** Opens a selected database. To do this, select the desired file in the view and click **Open**.
- **New database:** Create a new database in HiDrive. A detailed description of this process can be found [here](#).
- **Delete database:** Delete a selected database from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.
- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the database list view.
- **Filter:** Choose which file formats should be displayed in the storage location's list view.
- **Search:** Search for specific databases in the selected storage location.

Additionally, storage locations can be edited, renamed, or deleted by selecting a location storage and right-clicking on it:

- **Properties:** Edit the properties of a storage location.
- **Rename:** Rename a storage location.
- **Delete:** Delete a storage location.

If you save your databases on HiDrive, Password Depot uses the following default path:

```
\Password Depot\
```

WARNING: It is strongly recommended **not** to create this path manually. Instead, log in to HiDrive with Password Depot and allow the program to create the path, in case it does not yet exist. Once Password Depot has created the directory/folder, you can upload your existing password databases through Windows Explorer or your browser.

NOTE: Whenever you deposit your databases on a cloud service, your confidential data always "touch" the data medium of the cloud service in AES 256-bit encrypted format – never unencrypted. Your databases are **always** and only decrypted locally.

Home - Box Cloud

In **Password Depot**, you can open and save databases on Box. To do so, please open the [Home](#) screen, click on **Add location storage** and then on the option **Box Cloud**. The following options are now available:

- **Open:** Opens a selected database. To do this, select the desired file in the view and click **Open**.
- **New database:** Create a new database in Box Cloud. A detailed description of this process can be found [here](#).
- **Delete database:** Delete a selected database from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.
- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the database list view.
- **Filter:** Choose which file formats should be displayed in the storage location's list view.
- **Search:** Search for specific databases in the selected storage location.

Additionally, storage locations can be edited, renamed, or deleted by selecting a location storage and right-clicking on it:

- **Properties:** Edit the properties of a storage location.
- **Rename:** Rename a storage location.
- **Delete:** Delete a storage location.

If you save your databases on Box, Password Depot uses the following default path:

```
\Password Depot\
```

WARNING: It is strongly recommended **not** to create this path manually. Instead, log in to Box with Password Depot and allow the program to create the path, in case it does not yet exist. Once Password Depot has created the directory/folder, you can upload your existing password databases through Windows Explorer or your browser.

NOTE: Whenever you deposit your databases on a cloud service, your confidential data **always** "touch" the data medium of the cloud service in AES 256-bit encrypted format – never unencrypted. Your databases are always and only decrypted locally.

Home - Local backups

In **Password Depot**, you can open and save backup files. If a file got corrupted or was deleted by mistake, you can open a backup file of the database. To do so, please open the [Home](#) screen (**Home** → **Backups**) and click on the tab **Local backup**. The following options are available:

- **Open:** Opens a selected backup file. To do this, select the desired file in the view and click **Open**.
- **New database:** In the tab **Local backup**, the option **New database** is greyed out (since it is not applicable to backup files).
- **Delete database:** Delete a selected backup file from the list.
- **Back:** If you have changed directories in the file browser, you can use this button to jump back to the previous directory.
- **Forward:** If you have previously navigated back one directory in the file browser, you can use this button to jump forward again.
- **Level up:** Goes to the parent directory in the file browser.
- **Refresh:** Refresh the list view of the backup files stored under **Local backup**.
- **Filter:** Choose which file formats should be displayed in the backup files' list view.
- **Search:** Search for specific backup files.

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

Database Properties

Database Properties

Each Password Depot database has properties. Unlike program options, these properties are linked to a database and can be defined for each database individually. To view and modify/change your database properties, click in the tab **Database on Properties** (**Ctrl** + **I**) or click on the **Properties** icon in the tool bar.

There are six tabs in the **Properties** dialog:

- **General**: Displays a number of information fields (location, size, last modified, number of folders and passwords); allows for change of authentication; offers deletion or refreshing of icons used in databases. Furthermore, you can use compression to reduce the database size.
- **Content**: In this tab you can edit your database content. This includes, for example, the recycle bin settings, the history of your passwords as well as custom icons, attachments and ignored URLs.
- **Advanced**: Allows for definition of password policies in a database. Plus, you can active the option that authorized users have to set a second password.
- **Notes**: Allows for modifying/editing of comments and master password hints – both are shown when opening databases.
- **Backup**: Allows for creating and saving backup files on the internet or other remote servers and setting intervals for these backups, independent from regular backup files which are defined through the program options.
- **Entries**: You can choose different types of entries and deactivate those you are actually not working with or 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.

See also: [General](#), [Content](#), [Advanced](#), [Notes](#), [Backup](#), [Entries](#), [Security](#)

Properties - General

In the **General** tab of the database properties, you can see some basic information about your database and make some changes, if necessary.

At the top, you can see the **name** of your database. It cannot be changed here. Below you can see further information:

- **Location:** Indicates the storage location of your database. The location cannot be changed in this dialog. To change the name of your database or the file path, you can either use the **Database → Save as** command in the main menu or make those changes in the Windows Explorer.
- **Size:** Shows the size of your password file.
- **Last modified:** Shows the date of the file's last modification.
- **Contains:** You can see your database's total number of folders and entries.
- **Authentication:** Shows the currently used authentication method for this database and also allows for its **Change**.
- **Use compression to reduce the Database size:** Makes the database smaller by compressing it.

NOTE: Always keep your databases up-to-date and avoid unnecessary information. If your database takes a lot of time to load, you may need to consider reviewing your **attachments** and **custom icons**, as they increase the size of your database. You can either use the **Clean-up** function in the **Tools** tab to find entries and attachments which are no longer being used, or you can delete custom icons and attachments in the tabs **General** and **Content** of the database properties.

See also: [Content](#), [Advanced](#), [Notes](#), [Backup](#), [Entries](#), [Security](#)

Properties - Content

In the **Content** tab in the properties of a database you can adjust various settings concerning the database content.

Database objects

- **Custom icons:** Specifies the number of user-defined symbols related to your entries within the database.
- **Delete icons:** Delete the user-defined symbols of your entries. Please note that in this case ALL user-defined symbols will be irrevocably deleted.
- **Attachments:** Indicates how many attachments the opened database contains as well as their combined size.
- **Delete attachments:** Delete the attachments that are currently stored in the opened database. Please note that in this case ALL attachments will be irrevocably deleted. Deleting attachments can possibly reduce the file size and thus speed up the loading of the database again.
- **Ignored URLs:** Specifies the number of ignored web pages, that is, which web pages are not considered by the add-on.
- **Edit URLs:** The **Ignored Websites** dialog box opens and you can see the list of URLs that are currently ignored by the browser add-ons. You can edit the list here by deleting URLs from the list or adding new ones.
- **Update icons and window titles:** This option allows you to update the custom icons and window titles of your entries within the database.

History

- **Keep history of password changes:** When this option is checked, an entry is always made in the history of a password when you change it. You can then find it on the **Versions** tab of the **Properties** dialog (**Ctrl + M**) of an entry, which allows you to change or edit passwords.
- **Max. number of changes in history:** Set the maximum number of changes in the history.
- **Delete history:** Deletes the history for all passwords in the database.

Recycle bin

- **Delete entries immediately:** Select this option if you want to delete entries directly without moving them to the recycle bin first. Note that the deletion is irrevocable in this case.
- **Move entries to the recycle bin:** Select this option if you want to move entries to the recycle bin first before deleting them permanently. This way, they can be restored if necessary.
- **Max. number of objects in the recycle bin:** If you have activated the **Move entries to recycle bin** option, then you can define the maximum number of objects that the recycle bin of your database may contain. The default setting is 1000 objects. The maximum value is 10,000. Once the defined number is reached, you will not be able to move anything to the recycle bin, but will have to either restore or permanently delete entries first.
- **Empty recycle bin:** Use this button in the database properties to empty the recycle bin completely. Before the deletion process, you will be asked again whether the objects contained in the recycle bin should really be irrevocably deleted.

HINT: You can also access the recycle bin settings by right-clicking on the recycle bin within your database and choosing **Settings**. In addition, this also takes you to the **Empty recycle bin** and **Restore all** options.

You can learn more about the recycle bin [here](#).

See also: [General](#), [Advanced](#), [Notes](#), [Backup](#), [Entries](#), [Security](#)

Properties - Advanced

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

Passwords 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. This includes lowercase, uppercase, special characters and numbers. You can select that passwords should contain all or only a selected amount of these character types.
 - **Exclude characters:** Define which characters should be excluded from passwords, e.g., 0 and O or special characters.

Second password

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

See also: [General](#), [Content](#), [Notes](#), [Backup](#), [Entries](#), [Security](#)

Properties - Notes

On the **Notes** tab of the database properties, you can change the **comment** and the **hint** which you want to store for your database and for the master password. This information is shown whenever you open a database and are prompted to provide the master password.

- **Hint:** You may enter a new hint for the master password in this field. This field is optional, and must never contain the actual master password!
- **Comment:** You may enter a description of your database. This can be particularly helpful if you work with many different databases. This field is optional, and must also never contain the actual master password!

When opening a database, both the comments and the hints are also displayed in the login window when prompted to enter your database's master password.

NOTE: In these two fields, do not enter any information which could help a third party to guess or even find out your master password. If you enter a hint, it should merely serve as a helpful reminder for you alone and nobody else.

See also: [General](#), [Content](#), [Advanced](#), [Backup](#), [Entries](#), [Security](#)

Properties - Backup

The remote backup file is an **additional** option for creating backup files. This should not be confused with the standard backup file, which is set via **Edit → Options** (**F10**) → **Save**.

In the dialog window **Backup** in the database properties, you can set the storage location and the creation/settings of remote backup files.

Remote backup locations

Choose whether you want to save your backup locally and/or on an Internet Server.

- **Server:** In case you would like to save the backup files on an Internet server, check the box and select an existing server or create a new one.
- **Local System:** If you prefer to save the passwords file locally on your PC, check the box and select the corresponding path via **Browse** (file symbol) or type in the field.

Remote backup settings

- **Create automatic backup every:** To create backups automatically and regularly, check this option and enter the number/interval of days. The maximum value selectable is 100 days.
- **Create Backup:** Allows you to create an instant backup at the defined storage location.

NOTE: The **Create Backup** button is only active and usable if you have selected a backup location above!

See also: [General](#), [Content](#), [Advanced](#), [Notes](#), [Entries](#), [Security](#)

Properties - Entries

You can see all **types of entries** which are available in Password Depot **by default** in the **entries** tab of the database properties. You can see these types of entries also when creating a new entry and going to **Edit → New** or you can also see them in the **drop-down menu** when creating a new password.

You can uncheck now all types of entries you do **not use** or you **don't want to work with** – all unchecked types of entries then will not be available anymore when creating a new type of entry, that is why you will not see them in the drop-down menu anymore. This way, you can **adjust the list of available types of entries individually**. This will help you to organize your personal database further.

See also: [General](#), [Content](#), [Advanced](#), [Notes](#), [Backup](#), [Security](#)

Properties - Security

In the **Security** tab, you can find security-related options for the entire database.

- **Use a second password:** You have the option to define a second password for accessing this database. This option is particularly useful if you need or want to ensure a four-eyes principle. Accordingly, this additional security measure only makes sense if you are using your database on the Password Depot Enterprise Server with multiple users. This option is not recommended for private databases.
- **Change second password:** If you are already using a second password, you can change it here. Before doing so, you will be prompted to enter the previous second password.

HINT: If you want to remove the second password, simply uncheck the box for "**Use a second password**".

See also: [General](#), [Content](#), [Advanced](#), [Notes](#), [Backup](#), [Entries](#)

Database Authentication

Enter Master Password

To open a database, you will first need to authenticate yourself. A small dialog box, showing the name of the database you are going to open, will appear. In this window, you will have to enter your master password and, if you previously chose this option, the corresponding key file. If you encrypt your database with a master password and a key file, we speak of a Two-Factor Authentication (2FA). In this case, this applies for databases stored on your local system or in one of the offered cloud services.

Forgot your (Master) Password?

In case you have forgotten your master password and had indicated a hint for this password when generating it, you can click on [Forgot password?](#) (top left corner) which will then display the hint.

Entering a wrong Master Password

If you enter a wrong master password or indicate a wrong key file, you will see an error message. Subsequently, you can re-type the [master password](#).

NOTE: After each incorrect input, the "LOGIN" button will be disabled for an exponentially increasing duration to make brute-force attacks more difficult.

Change Master Password

In order to change your master password, open the program [Properties](#) and select the tab [General](#).

Change Authentication

To change the **authentication** for an open database, click on **Database → Properties** (**Ctrl** + **I**) or **Properties** on the toolbar, and then **General → Change**, right to the text box **Authentication**. This will start an assistant for changing the authentication.

First, you have to enter your current credentials and then click on **Next** to authenticate yourself.

Afterwards, you can select another authentication method or just define a new master password for the database.

Authentication by: You can choose from one of several methods to protect your database:

- **Primary password:** The classic and (depending on the complexity of the master password) safe method of encrypting a database, using a master password. Enter your master password (and confirm this entry!), whether in clear text or concealed format (right-hand side eye icon), or open the [master password generator](#) (right-hand side star symbol) to generate a particularly safe master password.
- **Primary password and key file:** The database is protected by a master password and a key file.
- **Key file:** The database is protected by a key file. Key files contain complex encryption keys which are very safe and cannot be cracked, not even by a brute-force attack. However, please remember that anyone who has access to your key file and your database can read all your passwords! You should therefore treat your key file like a real "vault key" and always store it in a safe place (e.g., on a USB stick). Use the button [Generate key file](#) (small star symbol left of the input field) to create such a key file.

NOTE: If you use a hint for your authentication, make sure to update it as well. Otherwise, you might get confused when you need it later on.

HINT: Below, in the dialog field, you will see an estimate for your entered master password's security and quality.

Key File Generator

You can use the Key File Generator at two moments:

- when creating a [new database](#).
- when [modifying/editing the authentication of an existing database](#).

To open the corresponding dialog box, you need to select an authentication method involving a key file (i.e., either master password plus key file or key file only). Having made this selection, you can now click on the **star symbol** on the right-hand (when creating new databases) or left-hand (when modifying/editing existing databases) side of the field **Key file**.

To generate the key file (256-bit key) within the Key File Generator, simply move your mouse cursor across the generator's field. This way, you randomly select characters that will then form your key. Once you have generated the key, click on **Save** in order to save the key as a proper key file.

WARNING: Keep the generated key in a safe place and do not forget to create backup files. We highly advise **against** using **only** key files for authentication, since this means that anyone with access to the database and the key file at the same time can read your password entries without having to enter a master password.

Backup Copies of Database

Backups

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

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.

Basically, backup files are identical with regular databases. The only difference lies in their file extension name ".**bckd**".

NOTE: We highly recommend the use of backup files!

Backup location

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

C:\Users\<<USERNAME>\Documents>Password Depot\Backup

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

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.

Open Backup Files

The backup files generated by [Password Depot](#) have the file extension `.bckd` and are stored, by default, in the following folder:

```
Documents\Password Depot\Backup
```

In case your database is damaged or got deleted by mistake, you can open a backup file to restore your data.

How to open a backup file:

1. Open [Password Depot](#).
2. Click on [Home](#) → [Local backup](#).
3. Select a backup of your file from the desired date and click on [Open](#).
4. Authenticate yourself using your master password and/or key file.
5. Click on [Database](#) → [Save as](#) (**Shift** + **Ctrl** + **S**) to save the file in its original format (`.pswd` or `.pswe`).

Entries

Adding & Modifying Entries

Basic Entry Operations

Add Entry



To add new entries, click on **Edit → New** or use the **Add** button on the toolbar (**Ctrl** + **Ins**). The new entry will be saved in the currently open folder.

By clicking on the **password** 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, except for document, allow for the use of the [virtual keyboard](#). It can be found in the bottom left of each window. You also have the option to [change an entry type](#) retrospectively.

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

Modify Entry

To modify/edit existing password entries, please open the [Properties](#) dialog window.

This window can be accessed in five ways:

- Either you select the password and then click on [Properties](#) on the toolbar.
- Or you select the password and press (**Ctrl** + **M**).
- Or you right-click on the password entry and select [Properties](#).
- Or you use the menu [Edit](#) → [Properties](#).
- Or you select the password entry and double-click.

NOTE: The function [Properties](#) can only be accessed if you have previously selected a password entry from the list.

Entry Type: Password

To create a password entry, click on **Add** (**Ctrl** + **Ins**) in the toolbar. The new password will be saved in the folder currently opened (displayed in the left **Navigation area**).

Alternatively, use the tab **Edit → New → Password**.

In the **General** tab, you can alter the following categories (all entries except the description are optional):

- **Description:** Enter a description for the new password. The description also serves as the name displayed in the password area.
- **Change Icon** (Icon to the right of Description): To change the icon for the password, click **Change Icon** to the right of the description.
If you click directly on the icon with the left mouse button, the [Select Icon](#) window will open. If you click on the icon with the right mouse button, you have the choice between three options: **Select Icon...** (takes you to the [Select Icon](#) window), **Load from URL** (use the default icon (favicon.ico) of an entered URL), and **Reset Icon** (uses the default icon for passwords or resets the icon to this).
- **User:** Enter the username associated with this password.
- **Password:** Enter the password.
- **Show/Hide Password** (Eye icon): Changes whether the password is displayed in plain text or hidden (and displayed as asterisks).
- **Password Generator** (star symbol next to the input field): Calls up the [Password Generator](#). After a password has been generated, it will be automatically entered in the **Password** field.
- **Quality:** Indicates how secure your password is. You also receive an assessment of the quality of your password and information about whether it is contained in whole or in part in a dictionary.
- **Category:** [Categories](#) help you structure your passwords.
- **Importance:** Define the importance of your password using the **Importance** drop-down menu. Based on the selected option (High/Medium/Low), you can later identify which passwords are particularly important.

- **Expires:** If you want to specify a validity date for your password, activate the **Expires** option with a checkmark and type in a validity date or select it using the **Calendar function** (to the right of the input field); or select a time period via the **Extend** button, e.g., three months or five days. If your password does not yet have a validity date, you can still set a date to be reminded to change it at a specific date (which also activates the checkmark on the left). Please note the [Hints for secure passwords](#) to change passwords regularly.
- **Tags:** Assign tags for better filtering of entries.
- **Comments:** Optionally enter additional information here.

For this entry type, you also have the following tabs available:

- [URLs](#)
- [Additional](#)
- [Custom fields](#)
- [TANs](#)
- [Attachments](#)
- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you have the option to use the [virtual keyboard](#). It is located at the bottom left of the dialog box.

HINT: For additional flexibility in password management, you can also create a 'Linked Entry' that inherits the username and password from this entry. For more details, refer to the [Linked Entry](#) section.

Add/Modify Entry - Remote Desktop Connection

You can enter and 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](#). The new entry will be saved in the currently opened folder (shown in the [navigation area](#) on the left-hand side).

In the dialog [General](#), you can enter the following data (all entries apart from the description are optional):

- **Description:** Enter a description for the new Remote Desktop Connection. The description is the name that will be displayed in the password area.
- **Change icon** (Icon to the right of Description): To change the icon for a Remote Desktop Connection, click on [Change icon](#) to the right of the description. If you left-click on the icon, the [Select icon](#) window opens. If you right-click on the icon, you can choose among three options: [Select Icon...](#) (guides you to the [Select icon](#) window), [Load from URL](#) (using the standard icon of the URL you entered), and [Reset Icon](#) (resets the standard icon of RDP connections).
- **Computer:** Enter the address of the computer, e.g. 192.168.178.201. By clicking the globe symbol to the right, you can open the address immediately in the browser.
- **User:** Enter the password's user name.
- **Password:** Enter the password.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Password generator** (star symbol to the right of the Password box): Opens the [Password Generator](#) for generating random passwords. Once you have generated your password, the [Password](#) field will be automatically completed with the newly generated password.
- **Quality:** Shows how secure or insecure your password is, and whether it contains any character strings similar or identical to dictionary entries. In addition, you will be shown how long it approximately takes to crack your password.

- **Command line:** Optionally, you can enter additional command-line parameters that are known to mstsc. **Note:** Username, password, and address (computer) are automatically passed and should not be listed here.
- **Category:** [Categories](#) help you to structure your passwords.
- **Importance:** Define the importance of your password using the **Importance** drop-down menu. Based on the selected option (High/Medium/Low), you can later identify which passwords are particularly important..
- **Expires:** If you want to specify a validity date for your password, activate the **Expires** option with a checkmark and type in a validity date or select it using the **Calendar function** (to the right of the input field); or select a time period via the **Extend** button, e.g., three months or five days. If your password does not yet have a validity date, you can still set a date to be reminded to change it at a specific date (which also activates the checkmark on the left). Please note the [Hints for secure passwords](#) to change passwords regularly.
- **Tags:** Define tags for easy filtering of your entries.
- **Comments:** Add any further comments to the new entry.

NOTE: Remote Desktop Protocol (RDP) connections **do not support passwords** that contain **double quotation marks (")**. This limitation arises from the way Windows handles command-line input and passes credentials to the Credential Manager. To avoid connection issues or processing errors, ensure that RDP passwords **do not include** double quotation marks.

Apart from the present entry tab, the following tabs are available:

- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Add/Modify Entry - TeamViewer

With the entry type **TeamViewer**, you can enter your TeamViewer data in Password Depot for connecting via TeamViewer very easily. To create the type of entry **TeamViewer**, click in the menu on **Edit → New → TeamViewer** or, alternatively, choose this type of entry from the drop-down menu when creating a new entry. In the **General** tab, you can see the following options (everything is optional except of the description):

- **Description:** Enter a description for the new entry TeamViewer. The description is the name that will be displayed in the password area.
- **Change icon:** To change the icon of TeamViewer, click **Change icon** to the right of the description. If you left-click the icon, the [Select icon](#) window opens. If you right-click the icon, you can choose between three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard TeamViewer icon).
- **Partner ID:** Enter the partner ID with which you would like to connect to.
- **Password:** Enter the corresponding TeamViewer password of your partner in order to start a connection.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Password generator** (star symbol to the right of the Password box): Opens the [Password Generator](#) for generating random passwords. Once you have generated your password, the **Password** field will be automatically completed with the newly generated password.
- **Quality:** Indicates how secure your password is. You also receive an assessment of the quality of your password and information about whether it is contained in whole or in part in a dictionary.
- **Mode:** Select whether you want to connect via **remote control** or want to carry out a **file transfer**.
- **Category:** [Categories](#) help you to structure your passwords.
- **Importance:** Define the importance of your password using the **Importance** drop-down menu. Based on the selected option (High/Medium/Low), you can later identify which passwords are particularly important.

- **Expires:** If you want to specify a validity date for your password, activate the **Expires** option with a checkmark and type in a validity date or select it using the **Calendar function** (to the right of the input field); or select a time period via the **Extend** button, e.g., three months or five days. If your password does not yet have a validity date, you can still set a date to be reminded to change it at a specific date (which also activates the checkmark on the left). Please note the [Hints for secure passwords](#) to change passwords regularly.
- **Tags:** Define tags for easy filtering of your entries.
- **Comments:** Add any further comments to the new entry.

Apart from the present entry tab, the following tabs are available:

- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This feature is situated in the lower left-hand corner of the dialog box.

Entry Type: PuTTY Connection

You can enter and manage your PuTTY Connections in Password Depot to establish a connection to the server with one click. To add new **PuTTY Connection** entries, it is necessary to install PuTTY in a first step. You can do so [here](#). As soon as you have successfully installed PuTTY, click on **Edit → New → PuTTY Connection**. The new entry will be saved in the currently opened folder (shown in the **navigation area** on the left-hand side).

In the dialog **General**, you can enter the following data (all entries apart from the description are optional):

- **Description:** Enter a description for the new PuTTY Connection. The description is the name that will be displayed in the password area.
- **Change icon** (button to the right of Description): To change the icon for a PuTTY Connection, click on **Change icon** to the right of the description. If you left-click on the icon, the [Select icon](#) window opens. If you right-click on the icon, you can choose among three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard icon of PuTTY connections).
- **Protocol:** Choose between four options and select the connection protocol (**ssh**, **telnet**, **rlogin**, or **raw**).
- **Host:** Please enter the host's address.
- **Port:** Enter the server's port number through which you want to communicate.
- **User:** Enter the password's user name.
- **Password:** Enter the password.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Key file:** Please enter your key file's path, either by typing or left-clicking on the right folder icon.
- **Key password:** Enter your key's password.
- **Show/Hide key password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).

- **Command line:** Enter the full PuTTY command line, including the session name or connection details.
- **Category:** [Categories](#) help you to structure your passwords.
- **Importance:** Define the importance of your password using the **Importance** drop-down menu. Based on the selected option (High/Medium/Low), you can later identify which passwords are particularly important.
- **Expires:** If you want to specify a validity date for your password, activate the **Expires** option with a checkmark and type in a validity date or select it using the **Calendar function** (to the right of the input field); or select a time period via the **Extend** button, e.g., three months or five days. If your password does not yet have a validity date, you can still set a date to be reminded to change it at a specific date (which also activates the checkmark on the left). Please note the [Hints for secure passwords](#) to change passwords regularly..
- **Tags:** You can enter additional tags/keywords for your PuTTY entry here. This option will help you to further filter and structure your database's entries.
- **Comments:** Add any further comments regarding the new entry.

Apart from the present entry tab, the following tabs are available:

- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This feature is situated in the lower left-hand corner of the dialog box.

Entry Type: 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** (button to the right of Description): To change the icon for a credit card, click on **Change icon** to the right of the description. If you left-click on the icon, the [Select icon](#) window opens. If you right-click on the icon, you can choose among three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard icon of credit cards).
- **Card:** Select a credit card type. You can choose between **MasterCard**, **Discover**, **Visa**, **American Express**, **JCB**, **Diners Club**, and **Other**.
- **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.
- **Additional Information:** Enter any additional information if required.
- **PIN:** If applicable, enter the PIN of your credit card. By clicking the eye symbol, you can hide or display it in plain text.
- **Category:** [Categories](#) help you to structure your passwords.
- **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.

NOTE: In this dialog box, you may use the [virtual keyboard](#). This feature is situated in the lower left-hand corner of the dialog box.

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. The new entry will be saved in the currently opened folder (shown in the **navigation area** on the left-hand side).

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** (button to the right of Description): To change the icon for a banking entry, click on **Change icon** to the right of the description. If you left-click on the icon, the [Select icon](#) window opens. If you right-click on the icon, you can choose among three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard icon of banking entries).
- **User:** Enter the user name.
- **Password:** Enter the password.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Password generator** (star symbol to the right of the Password box): Opens the [Password Generator](#) for generating random passwords. Once you have generated your password, the **Password** field will be automatically completed with the newly generated password.
- **Card Holder:** Enter the name of the 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 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 card.
- **Category:** [Categories](#) help you to structure your passwords.
- **Comments:** You can add further notes.

Additionally, the following tabs are available:

- [URLs](#)
- [Additional](#)
- [IANs](#)
- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This feature is situated in the lower left-hand corner of the dialog box.

Entry Type: 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. The new entry will be saved in the currently opened folder (shown in the **navigation area** on the left-hand side).

In the dialog **General**, you can enter the following data (all entries apart from the description are optional).

- **Description:** Enter a description for the new software license entry. The description is the name that will be displayed in the password area.
- **Change icon:** To change the icon of a software license entry, click **Change icon** to the right of the description. If you left-click the icon, the **Select icon** window opens. If you right-click the icon, you can choose between three options: **Select Icon...** (guides you to the **Select icon** window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard software license icon).
- **Product:** Enter the product's name.
- **Version:** Enter the product's version number.
- **Registered Name:** Enter the name of the person the software is licensed to.
- **Email Address:** Enter the email address used for the license's purchase.
- **License Key:** Enter the product's license key.
- **Additional Key:** Enter an additional key (e.g. the license key of a previous version).
- **Download URL:** Enter the URL where the product can be downloaded. You can choose between the following input options (from left to right): typing, browsing through your folders, and opening in your standard browser.
- **User Name:** Enter the user name linked to software license key.
- **Password:** Enter the corresponding password for the user name above.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Purchase Date:** With the help of the calendar function, select the date on which you bought the product.
- **Expires:** Indicate software license key's expiry date, or **Extend** the date, if applicable.

- **Order Number:** Enter product's order number.
- **Category:** [Categories](#) help you to structure your passwords.
- **Comments:** Enter, if needed, supplementary information.

Apart from the present entry tab, the following tabs are available:

- [Additional](#)
- [Attachments](#)
- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

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. The new entry will be saved in the currently opened folder (shown in the **navigation area** on the left-hand side).

In the dialog **General**, you can enter the following data (all entries apart from the description are optional).

- **Description:** Enter a description for the new entry. The description is the name that will be displayed in the password area.
- **Change icon:** To change the icon of an identity entry, click **Change icon** to the right of the description. If you left-click the icon, the **Select icon** window opens. If you right-click the icon, you can choose between three options: **Select Icon...** (guides you to the **Select icon** window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard identity entry icon).
- **Account Name/ID:** Enter an account name or another form of ID.
- **First Name:** Enter the first name.
- **Last Name:** Enter the last name of the person.
- **Email Address:** Enter the email address.
- **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.
- **Street:** Enter the street of the postal address.
- **House number:** Enter the house number of the postal address.
- **Address 2:** Enter any further address information.
- **City:** Enter the name of the city.
- **State (Province):** Enter a state, province, or district here.
- **ZIP:** Enter the postal code of the city.
- **Country:** Enter the country.

- **Phone:** Enter the telephone number.
- **Mobile:** Enter the mobile phone number.
- **Fax:** Enter the fax number.
- **Category:** [Categories](#) help you to structure your passwords.
- **Comments:** You can add further notes here.

Additionally, the following tabs are available:

- [Attachments](#)
- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Entry Type: Information

To add new **information** entries, click on **Edit → New → Information** or use the arrow on the **Password** button on the toolbar. The new entry will be saved in the currently opened folder (shown in the **navigation area** on the left-hand side).

In the dialog **General**, you can enter the following data (all entries apart from the description are optional):

- **Description:** Enter a description for the new information entry. The description is the name that will be displayed in the password area.
- **Change icon:** To change the icon of an information entry, click **Change icon** to the right of the description. If you left-click the icon, the [Select icon](#) window opens. If you right-click the icon, you can choose between three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard information icon).
- **Category:** [Categories](#) help you to structure your passwords.
- **Content:** Enter the information that you would like to save in Password Depot.

Apart from the present entry tab, the following tabs are available:

- [Attachments](#)
- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Entry Type: Encrypted File

Password Depot offers the possibility to encrypt external files with the secure algorithm AES 256 Bit. The password which you need to decrypt the file afterwards can be stored within your database.

There are four ways how you can create an entry for an encrypted file:

- Click on **Edit → New → Encrypted file**.
- Encrypt a file via **Tools → Encrypt external files**.
- Select **Add** on the toolbar, click on the right-hand down-arrow button and choose **Encrypted file**.
- Right-click on a file in the Windows Explorer, click on **Show more options**, and then click on **Password Depot → Encrypt** (this will automatically take you to **Password Depot**).

In the dialog window **General** (shown after the first and third options), the following functions are available (apart from the description all optional):

- **Description:** Enter a description for the new encrypted file entry. The description is the name that will be displayed in the password area.
- **Change icon:** To change the icon of an encrypted file entry, click **Change icon** to the right of the description. If you left-click the icon, the [Select icon](#) window opens. If you right-click the icon, you can choose between three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard encrypted file icon).
- **Password:** Enter a password for the encrypted file.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Category:** [Categories](#) help you to structure your passwords.
- **Importance:** Define the importance of your password using the **Importance** drop-down menu. Based on the selected option (High/Medium/Low), you can later identify which passwords are particularly important.
- **Comments:** Enter, if needed, supplementary information.

On the second tab **Files**, you have the following options:

- **Files:** Shows a list of encrypted files belonging to the selected entry. They can be sorted 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 on **OK** to save changes, or on **Cancel** to close the window without saving changes.

NOTE: Encrypted files are always saved and deposited on your own data storage medium, whereas Password Depot's database **only** contains the password and link to the encrypted file. If you delete the file from your computer, e.g. via Windows Explorer, you will no longer be able to access it. In contrast to this, the entry type **Document** saves your file directly within Password Depot's database, i.e. documents are **part** of your Password Depot database.

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Add/Modify Entry - Document

You have the possibility to enter your documents in [Password Depot](#). The documents will thereby be added to your encrypted database. To create a new entry for a **Document**, click on **Edit → New → Document** or use the arrow on the **Add** button on the toolbar.

When you add a new document, you must select the file first.

The following fields are filled in automatically after file selection and cannot be edited:

- **Document:** The name of the file.
- **Change icon:** To change the icon of a document, click **Change icon** to the right of the description. If you left-click the icon, the [Select icon](#) window opens. If you right-click the icon, you can choose between three options: **Select Icon...** (guides you to the [Select icon](#) window), **Load from URL** (using the standard icon of the URL you entered), and **Reset Icon** (resets the standard document icon).
- **Type:** The type (file name extension) of the file.
- **Size:** The size of the file.
- **Modified:** [Date/Time] of the last change.

The following options are also available:

- **Original path:** The original path of the file. With **Erase**, you can, if desired, delete the original file irrevocably from your hard drive.
- **Default folder:** The default folder for actions with this file (e.g. Export). You may either type or click on the right-hand folder icon to set a path.
- **Category:** [Categories](#) help you to structure your passwords.
- **Comment:** Enter further information, if applicable.

The following functions are available at the bottom of the tab:

- **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 data carrier.

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

NOTE: The **Document** entry type stores a file directly within Password Depot, i.e. documents are **part** of your Password Depot database. The entry type **Encrypted file**, on the other hand, is always stored on your data carrier and stored in the database of Password Depot are **only** the password and the link to the encrypted file. If you delete the file from your computer (for example, using Windows Explorer), you can no longer access it.

Entry Type: Certificate

To add new [certificates](#), click on [Edit → New → Certificate](#) or use the arrow on the [Add](#) button on the toolbar. The new entry will be saved in the currently opened folder (shown in the [navigation area](#) on the left-hand side).

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:** To change the icon of a certificate, click [Change icon](#) to the right of the description. If you left-click the icon, the [Select icon](#) window opens. If you right-click the icon, you can choose between three options: [Select Icon...](#) (guides you to the [Select icon](#) window), [Load from URL](#) (using the standard icon of the URL you entered), and [Reset Icon](#) (resets the standard certificate icon).
- **Public key:** You can select a certificate by clicking the folder icon, view it by clicking the magnifying glass icon, or save it by clicking the floppy disk icon.
- **Private key:** You can select a certificate by clicking the folder symbol, view it by clicking 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.
- **Show/Hide password** (eye icon to the right): Changes whether the password is shown or hidden (and represented by dots).
- **Category:** [Categories](#) help you to structure your passwords.
- **Importance:** Define the importance of your password using the [Importance](#) drop-down menu. Based on the selected option (High/Medium/Low), you can later identify which passwords are particularly important.
- **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:** You can add tags to allow for better filtering of your entries.
- **Comments:** You can add further notes.

Additionally, the following tabs are available:

- [Versions](#)
- [Conditional access](#)
- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Entry Type: Custom

[Password Depot](#) allows you to use custom templates for entries. To add a custom entry, click on [Edit → New → Custom](#) or use the arrow on the [Add](#) 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 entry type](#) (**Shift** + **Ctrl** + **N**). 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](#)
- [Conditional access](#)

- [Security](#)

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Entry Type: Linked Entry

The type [Linked Entry](#) allows users to create entries that inherit the username and password from another already existing entry.

In order to create a linked entry, right-click on the entry you would like to link to. Choose the option [New linked entry](#).

[Password Depot](#) is able to [create multiple linked entries](#) with different URLs to a single master entry. This feature supports and simplifies the use of one account across multiple websites.

Functionality

A linked entry utilizes the username and password of another entry of the "Password" and "Remote Desktop Connection" type. This simplifies password management, especially when multiple services or applications use the same login credentials.

Editable Fields

In linked entries, all fields can be edited except for the username and password fields. These are always inherited from the "parent entry." Any changes made to the parent entry will automatically apply to all linked entries.

NOTE: Linked entries can only be generated from the [Password](#) and [Remote Desktop Connection](#) entry types.

Advanced Entry Operations

Add/Modify Entry - Tab URLs

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/File

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

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 at the bottom left.

Add/Modify Entry - Tab Additional

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

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\OFFICE16\WINWORD.EXE) in **General/URL/Local Document** and indicate the path of the document that is to be opened (e.g. C:\mydocument.docx).

If the program you would like to open with command line parameters is password-protected and opened via a DOS command line parameter (e.g. PuTTY), you can use the 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 **Enter the parameters string used to open a local file**, you need to enter the following: <USERNAME→@<IP_ADDRESS→ -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 do 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

Define whether the password policy compliance of an entry should or should not 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](#).

TOTP Generation Settings

The **TOTP Generation Settings** button provides additional advanced options for configuring the 2FA key. These advanced options allow you to adjust TOTP codes precisely to the requirements of the respective service and thus also support scenarios where the usual default parameters do not apply.

After clicking **TOTP Generation Settings**, a dialog opens with the following options:

- **2FA Key/Secret:** Enter the secret key (secret) provided by the respective application or website for two-factor authentication into this text field. Password Depot uses this secret as the basis for generating the TOTP codes.

In the **Advanced** section, you can adjust the parameters for TOTP generation:

- **Digits:** Defines how many digits the generated TOTP code should contain. You can choose a value between 4 and 16 digits.
- **Period (seconds):** Determines the validity period of a TOTP code in seconds. The period can be adjusted in steps of 10 from 10 to 300 seconds. When this time interval expires, a new TOTP code is generated automatically.
- **Algorithm:** Selects the hash algorithm used to calculate the TOTP code. The following options are available: SHA1, SHA256 and SHA512. Use the algorithm required by the respective service.
- **Default values:** Resets all advanced settings (digits, period, algorithm) to the recommended default values. This option is useful if you want to undo individual adjustments or return to a known baseline configuration.

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 at the bottom left.

Add/Modify Entry - Tab Custom Fields

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

You can add custom fields to your password entry by going to the **Custom Fields** tab while [adding](#) (**Edit → New**) or [editing](#) (**Edit → Properties**) a password entry.

Here, you are shown a list of all existing custom fields. The columns of the list are labelled:

- Name
- Type
- Value

In the lower part of the tab **Custom Fields**, you will find six buttons for working with customized fields:

- Click **Add field** to create a new field. To do this, you have to enter a name for the field and the value which the field should have.
- Click **Edit field** to change the value or the name of a field.
- Click **Delete field** to erase the selected custom field from the list.
- Use **Move up** and **Move down** to change the order of your custom fields, e.g. to find certain passwords more quickly on the top bar.
- If you uncheck the option **Mask values**, you will be able to see the unmasked values you entered for each field.

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

See also: [Global Custom Fields](#)

Add/Modify Entry - Tab TANs

In this window/tab, you can enter **TANs** associated with your password. For example, if you store your bank details in **Password Depot**, you can enter the TANs which you received by your bank for certain transactions.

Columns are labelled: **No.**, **Value**, **Used On**, **Amount**, **Confirmation Code**, and **Comment**.

The buttons in the lower part of the tab offer the following options:

- **Add TAN:** Click this button to open the **Add TAN** dialog box, where you can enter new TANs.
- **Edit TAN:** Click this button to open the **Edit TAN** dialog box for editing existing TANs.
- **Delete TAN:** Deletes all **selected** TANs after prompting for confirmation.
- **Import TANs:** Allows you to import TANs from a file. The file formats available are CSV, XML and TAN lists (in plain text). The TAN lists format expects a text file containing exactly one TAN per line. Since banks may issue printed TAN lists, you may require an OCR (optical character recognition) software to convert your TAN list from hardcopy to the file format required by **Password Depot**.
- **Export TANs:** Allows you to export TANs to a file. The formats available are CSV, XML, and TXT.
- If you uncheck the option **Mask values**, you will be able to see the unmasked values you entered for each TAN.

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Add/Modify Entry - Tab Attachments

To add an attachment to your password entry, go to the **Attachments** tab while [adding](#) (**Edit → New**) or [editing](#) (**Edit → Properties**) a password entry.

Columns are labelled **Name** and **Path on Disk**.

The buttons in the lower part of the tab offer the following options:

- Click **Add attachment** to select the desired file where it is currently located and saved. It will now be added to your list of attachments. On the right-hand side, you see the file's path.
- Via **Delete attachment**, you can remove a file from your password entry.
- Using the button **Delete from Disk** will delete the file from its original place, but it will still be saved and available in **Password Depot**.
- **Extract to Disk** will save an item wherever you like.
- The **Open with Internal Viewer** button will open the current file.

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

WARNING: Using attachments is **not** recommended. In connection with the server, attachments have already been deactivated. Instead, please use the new entry type **Document**.

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Add/Modify Entry - Tab Versions

On the **Versions** tab, you can see how a password has developed and changed in case there was data loss or you have accidentally overwritten an entry.

Here, you see a list of all changes that have been made for a password.

Columns are labelled **Creation date**, **Changes** and **Author**.

The buttons in the lower part of the tab offer the following options:

- Clicking **View Differences** will show you all differences between two versions of a password in detail.
- Via the **Delete** button, you can erase an item from the versions list.
- **Restore** will take the password back to the selected state.
- Via **Versions**, you can decide whether you want to keep a history for the respective password or not. By default, the global settings you set in the options will be applied.

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

NOTE: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Add/Modify Entry - Tab Conditional Access

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.

Show the warning message on access

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**. Clicking **Cancel** closes the dialog box. The properties of the entry cannot then be accessed.
- **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. The entry can only be opened by clicking **OK**. Clicking **Cancel** closes the dialog box. The properties of the entry cannot then be accessed.

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: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Add/Modify Entry - 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 be 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: In this dialog box, you may use the [virtual keyboard](#). This function is situated in the lower left-hand corner of the dialog box.

Importing & Exporting Entries

Importing and Exporting Passwords

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 (on the **Tools** menu) are especially useful for the interaction between **Password Depot** and [other password managers](#).

By clicking on the respective functions, you will find detailed information about [exporting](#) and [importing](#) passwords with **Password Depot**.

NOTE: Your database is a highly confidential document. Make sure that no other person gains access to the list. Store the list in a secure location.

WARNING: When you export your database, it will be saved to your hard drive in an unencrypted format. Please take this into consideration.

Exporting Entries

Databases and database entries can be exported into another file format through [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)
- [PSWE](#) (Password Depot database file)

To export a file into one of these formats, click on [Tools → Export](#).

WARNING: The file formats XML, CSV, TXT, HTML do not support encryption. Anyone with access to those files can read their content.

NOTE regarding the .csv file: Every .csv file contains one password per line. Up to 13 fields are assigned to each password in turn, separated by a comma: Description, Importance, Password, Last modified, Expiry Date, User Name, URL, Comments, Category, Tags, Author, Sequence, and UUID.

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 and afterwards, choose one of the offered options depending on the data you would like to export:

- **All entries in the database**
- **Entries in the active view**
- **Selected folder**

HINT: If you choose the option **Selected folder**, you can further select individual folders within your database for export and also decide whether you want sub-folders to be included or not. Besides, additional features are at your disposal here (e.g. **Check All**, **Uncheck All** and **Invert Selection**) which are accessible through right-clicking with the mouse on the list of entries being displayed. The option **Entries in the active view** includes all entries of the last view of your database before starting the export wizard.

Click **Next** again to continue. The wizard will show you the export result. Select **Finish** to complete the export. When using the .csv format, an intermediate step will be required where you can specify export parameters for the CSV file.

HINT: You can check the option **Show the exported file in Windows Explorer**. If you select this option you will be forwarded to the Windows Explorer and corresponding directory as soon as you finish the process and close the export wizard. This may be helpful, for example, if you do not remember the directory you chose for storing the exported file when launching the wizard.

NOTE: In this dialog box, you may use the [virtual keyboard](#) for entering the master password. This function is situated in the lower left-hand corner of the dialog box.

Import Wizard

With **Password Depot**, you can both import passwords from external files and **export** them into an external file. These functions are to be found on the **Tools** menu.

Supported Import Formats

The software supports following file formats for importing passwords (**Tools** → **Import**):

- **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)

HINT: To simplify the import of databases from other providers, numerous preconfigured import formats are available — for example, for LastPass or 1Password.

Import process

To launch the import wizard, you have to enter your **master password** first. Then, you are asked to provide 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 should be imported.

Click the **Next** button to continue, and then **Finish** to complete the process.

NOTE regarding the Enterprise Server: The **Import** function cannot be executed while you are connected to the server. If you would like to import passwords, please contact the administrator. They then have to open the database into which the passwords are to be imported via **Password Depot Client** as a local copy (via **Home** → **Local system**).

Only then the **Import** function is available. Now import the desired passwords, save the file and finally add it back to the server or save the file directly on the server directory.

NOTE: In this dialog box, you may use the [virtual keyboard](#) for entering the master password. This function is situated in the lower left-hand corner of the dialog box.

Import Wizard - CSV File Import

On this page of the wizard, you configure the parameters for importing a CSV file and map the columns of the CSV file to fields in Password Depot.

If the source file was created with the same version of Password Depot, you can usually keep the mappings suggested by the wizard. If the CSV file was created with a different version or by a third-party application, you should carefully review the column mappings and adjust them if necessary.

First line contains field names: Enable this option if the first row of your CSV file contains column headers (e.g. **Description**, **User name**, **Password**, etc.). The first row will then not be imported as a data record but used only to display the column names.

Delimiter: The character used in the CSV file to separate individual fields. Typically this is **;**, **,**, or another defined character.

Text qualifier: The symbol used to enclose text values (e.g. full sentences). In most cases this is a double quote (**"**).

Column mapping

In the central area you see a table with three columns:

- **#**
Sequential numbering of the columns from the CSV file.
- **CSV Column**
Displays the column header or detected field name from the CSV file, e.g. **Description**, **Importance**, **Password**, **Modified**, **Valid until**, **User name**, **URL**, **Notes**, **Category**, **Tags**, **Author**, **Sequence** or **UUID**.
- **PD Attribute/Field**
In this column you define to which Password Depot field the respective CSV column should be mapped. Click in a cell to open the drop-down menu and select the desired target field.
The following options are available: the standard fields (e.g. **Description**, **User name**, **Password**, **URL**, etc.) as well as:
 - **Custom Field** – maps the CSV column to a custom field.

- **Entry Path** – uses the column to specify the entry path within the database structure.

Clear assignments: Resets all previously defined column mappings so that you can reconfigure the mapping of CSV columns to Password Depot fields from scratch.

After you have reviewed and adjusted all mappings, click **Next** to continue the import.

Import Wizard - Import from other password managers

Importing passwords from one password manager to another (e.g. KeePass, 1Password, etc.) may prove to be a very tedious task in case you have to do this manually and must transfer each password individually. That is why **Password Depot** includes import templates from other password managers to make this step easier for you.

If you import passwords into **Password Depot**, however, the **import wizard** (via **Tools → Import**) will help you. First, you have to export your passwords contained in the other passwords manager into a .csv or .xml file, then you can import this file via the import wizard into **Password Depot**.

EXAMPLE: Import from KeePass

If you want to import KeePass data into **Password Depot**, please first export this data into the CSV format.

The KeePass CSV file contains only the main fields "Account", "Login", "Name", "Password", "Web Site", and "Comments".

In **Password Depot**, click **Tools → Import**. You can choose the **Import format**, the **Source file** (i.e., the exported CSV file) as well as the **Target folder**.

On the next page enter a comma "," as delimiter. Now you will see all available fields from the KeePass file in the left column.

Please assign them as follows:

1. Click the field **Account** in the left panel.
2. In the right panel, choose the corresponding **Password Depot** field, which is **Description**.
3. Now click the icon >> to make the assignment.

Proceed with the remaining fields as follows:

- Login Name → User Name
- Password → Password
- Web Site → URL

- Comments → Comments

After that, check the option **First line contains field names** and click the **Next** button.

Import Wizard - Import Completed

This page displays the results of the import process and the number of processed items.

To complete the import process and to insert the imported passwords into the database, click the **Finish** button.

Cleaning-up & Deleting Password Entries

Clean up Password Entries

Using the **Clean-up** function on the **Tools** tab, you can see at one glance all of the passwords which you have not used for a long time or which have expired. Additionally, you can directly delete those entries which you no longer need.

NOTE: Make sure that your database is up-to-date; as unused and/or expired entries overload the program unnecessarily.

To find passwords, six 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 number of KB you entered. This option allows you to quickly find big attachments which might cause delays in loading your database.
- **Entries not used after:** Shows all passwords which have not been used since the day you have selected.
- **Unused entries:** Shows all passwords which you have never used since you created them.
- **With change 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 you have set the desired filter options, you will see all passwords which meet the criteria you have chosen. Additionally, there is corresponding information (e.g. **Expires on** and **Frequency of use**) displayed in the list.

For the clean-up of the displayed passwords, several 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.

NOTE: Deleted passwords will be moved to the [Recycle bin](#).

Click **Close** to complete the process.

Delete Passwords

The **Delete** function on the **Edit** tab (**Ctrl** + **Del**) or the button of the same name on the toolbar clear both password entries and (sub)groups.

Whenever you choose to delete one or several passwords, you will be asked if you are sure that you want to proceed. This way, you cannot delete passwords by mistake.

NOTE: If you delete a group, all its passwords and **subgroups** will **also** be **deleted**.

NOTE: Deleted entries are moved to the [Recycle bin](#) and can be restored from there.

Recycle Bin

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

You can find the bin in the main view of the navigation area, the latter being placed on the left-hand side by default.

By left-clicking onto the **recycle bin** symbol, a new tab with the same name opens. In this tab, you will see a list of all deleted entries and have the following options (either by right-clicking on the entire recycle bin or selected entries):

- **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 again be in the recycle bin and you can now restore it. In case you have activated the option for **automatically saving** the database upon quitting the program, you may need to refer to backup copies of your file. These are, by default, saved here: C:\Users\<>USERNAME>\Documents\Password Depot\Backup.

Program-internal Password Entry Functions

Search Password Entry

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 are not shown in the search results.

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 both social and security .
OR	social OR security	Finds items that contain either social or security .

Quotation marks	"social security"	Finds items that contain the exact phrase social security .
→	date:→11.05.2025	Finds items with a modification date after 11.05.2025.
	size:→500	Finds items with attachments whose size exceeds 500 bytes.
<	date:<11.05.2025	Finds items with a modification date before 11.05.2025.
	size:<500	Finds items with attachments whose size is less than 500 bytes.
..	date:11.05.2025..11.10.2025	Finds items with a date beginning on 11.05.2025 and ending on 11.10.2025.

NOTE: The operators are not localizable. Even if the program has a user interface language other than English, **AND/OR/NOT** needs to 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.

See also: [Seach and Replace](#), [Advanced Search](#)

Advanced Search

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

- Description
- User name
- Password
- URL
- Other fields
- Comments
- Tags
- Modified after/before
- Expired after/before
- Category
- Importance
- With attachments larger than (KB)
- 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.

See also: [Search Password Entry](#), [Search and Replace](#)

Search and Replace

The **Search and Replace** function (**Ctrl** + **R**) on the **Search** menu allows you to search the entire database for the occurrence of one string of characters and replace it with another.

- **Search for:** Enter the character string you are searching for and which you then replace.
- **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.

Search options and display of search result can be refined even further, e.g. for lowercase/uppercase spelling, inclusion of subfolders, etc.

WARNING: This operation cannot be undone.

See also: [Search Entries](#), [Advanced Search](#)

Sort Password Entries

Entries can be sorted by clicking on **View → Sort by**. See [Customize appearance](#) for further information.

Print Password Entries

Password Depot offers you the possibility to print passwords. This function can be found on the **Database** menu (**Database → Print**, or **Ctrl + P**).

Before you can print, you need to enter your master password. This ensures that no unauthorized third party is trying to get a print copy of your passwords. Having entered your master password, the print window opens.

After having entered your master password you will see the **print preview** of the list of passwords or database that is to be printed subsequently. Via the arrow buttons, you can switch between the single pages. By clicking the button **Print**, you start the printing process.

With the buttons **-** and **+**, you can change the scale of the page to be printed, e.g. down to 50% of the original. With the **Export to PDF** button, you can create a PDF file with your passwords.

Content

On the **Content** tab (in the middle), you can determine what exactly you want to print. At the top of this dialog, you can define if you want to print **All passwords** in your file or a specific group only (**Selected passwords**). For the latter, choose a group or database from the drop-down list to select this group or database and check the option **Include sub-folders** if you want to print any folders included in that group or database as well. You can uncheck specific passwords if you want to exclude them from being printed.

To print the passwords according to a specific **sorting order** (e.g., by importance), select this criterion and specify whether you want to print them in ascending or descending order.

Below you can select which fields of your entries you want to print. If you uncheck any of the available fields, they will not be printed for any of the selected passwords or entries. By default, the program also prints the number of attachments (although not the attachments themselves).

NOTE: The field **Description** is necessary and cannot be deselected.

Layout

The print layout of a database can be changed on the [Layout](#) tab to the right.

At the top, you can enter a [Title](#) for the print-out.

In addition, you can choose either [Portrait](#) or [Landscape orientation](#) for the printed page.

If you would like to define [Margins](#) – e.g. in order to hole-punch the sheet – please indicate the margins for the four sides in millimeters.

At the bottom of the dialog, you can change the [Font type, style](#), and [Font size](#) of the title, of the folders and of the entries. Simply click the corresponding box and enter your changes in the dialog: [Click here to change the font](#) that opens.

To see the result of the changes you made, you can return to the [Print Preview](#) tab.

To print your passwords, simply click on the [Print](#) button available on each tab.

NOTE: Your password printout is a highly confidential document. Make sure that **no other person gains access** to the list and store it in a secure location.

Synchronize Password Entries

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

First, you have to open both databases in **Password Depot**. Afterwards, select **Tools → Synchronize** to start the synchronization assistant. You will see an overview of all available databases with information on the storage location ("Storage"), the date of last modification ("Modified") and the database size ("Size"). Choose the databases you would like to synchronize and click **Select**.

You will now see an overview of all differences. On the right-hand side, you will see the file with which you are synchronizing your current file. On the left-hand side, you will see your current database.

The entries are divided into three categories:

- **Not existing items**
- **Different items**
- **Identical items**

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 into the other. Furthermore, you can delete entries. In the bottom left, if applicable, you can see **Recommended actions**.

Lastly, click **Synchronize** to finish.

Compare Entries

To view all differences that two passwords have in the synchronization, view the [Report on Differences](#). Here, you get a list of differences, which helps you to identify all changes.

By default, passwords and other sensitive data like the user name are masked. If you would like to see them in plain text, uncheck the option [Mask passwords and other sensitive data](#) on the left bottom side.

To return to the synchronization dialog, click [OK](#).

Organize 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 folder**, and name the folder.

Repeat this process to create sub-folders.

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

Categorize Password Entries

In **Password Depot**, you can assign self-chosen categories to passwords, e.g. when [adding a new entry](#) or [modifying an existing entry](#).

To edit the categories, go to the **Edit** menu and choose **Categories**.

Use the following command buttons to edit the categories list:

- **Add**: Adds a new category to the list.
- **Replace**: Renames a selected category.
- **Delete**: Deletes a selected category.
- **Clear**: Deletes all categories from the list.
- **Load from file**: Loads categories from a file.
- **Save to file**: Saves the selected category within a file. This function is ideal if you are using **different** databases and, within these, would like to have the **same** categories, without having to manually edit each file's categories. In this case, you can simply save the categories in a file and then load it within a different database, via **Load from file**.

Once you have edited the categories, click **OK** to apply the changes.

NOTE: The buttons **Add** and **Replace** only become active and thus usable after you have entered characters into the entry field above.

Grant Access to Entries

NOTE: This option is only available up to Password Depot 18. With Password Depot 19, this function was subsumed under [Create Shared Secret](#).

When working with Enterprise Server databases users can share **single entries** with other Enterprise Server users. This allows temporary access to data that is normally not accessible to the corresponding users without the need of changing the rights management in the Enterprise Server by the server administrator.

NOTE: This option is only available in the client if the server administrator has enabled it in the Server Manager.

By performing a right click on the desired object, a drop-down menu with several actions available for this entry will open, including the option **Grant access** (**Shift** + **Ctrl** + **G**).

A new dialog window will open. You can now choose another user you want to authorize for the entry.

Permission for

If desired or required, you can limit the shared access by entering a date to start in the **Valid from** box and also entering a date of end in the **Valid to** box. If you do not want to limit the shared access, you can uncheck the box **Valid to**. The shared access will then be possible without any time limit.

Access level

You can choose from different access levels and decide which one(s) you would like to assign to the user who will be authorized to the entry or folder by you: **Use/Read/Modify/Delete**. You can either choose one or several options here. If the other user should only be allowed to use the entry, he will be able to use it and, for example, for the login on a website. If you also want to grant **read** and **modify** access, for example, he will also be able to see the entry in clear text and modify it etc.

Select **Next**, if you have checked all options as required.

You can finish the process here if you want to grant access to an entry only and do not want [sealed access](#). To do so, select **Finish**.

The user who has been authorized to an entry or folder can now login on the Enterprise Server with his access data. The user will then see the database included in his list of the **Home section**. Depending on the access level the user can either use the corresponding element or modify and delete it.

Shared Entries

If you go to **Tools → Shared entries** users which are allowed to grant access to entries to other users on the Enterprise Server can see which entries and folders they are currently sharing with others. This dialog window contains the following information:

- **Description**
- **Path**
- **Shared with**
- **Valid from**
- **Valid to**
- **Rights**

Here, users being able to share entries on the Enterprise Server with other server users can remove the granted access to entries and folders at any time if they do not want to share the data anymore. To do so, select the corresponding element from the list of shared entries and folders and select **Revoke permissions** next. The granted access will be revoked and the user who had been authorized to use the element can neither access the database nor the corresponding entry/folder anymore. Next time they will log in on the Enterprise Server, the corresponding database will not be displayed anymore.

Seal Entries

If a user authorizes another user on the Enterprise Server to access entries, he can also **seal** those elements. In this case, the user who has been authorized by another user has to ask for an approval in order to use the corresponding element. Please note that without the correct approval, access to sealed entries is **not possible**.

After the access has been granted to a single entry by a user, the issuer selects **Next** and he will be forwarded to the sealed access subsequently.

If you would like to provide sealed access, please check the corresponding box in the dialog window. Afterwards, it is required to select one or several users who can send the approval to the corresponding user asking for access permission. Finally, select **Finish**, if you have made all necessary adjustments.

NOTE: Only users with admin rights can send approvals for accessing sealed entries.

The user who has been authorized to access a sealed entry can login on the Enterprise Server afterwards. The user will then see the database containing the entry or folder he has (temporarily) been granted access to. Please note that the user will only see those objects within the database he has actually been granted access to; other entries/folders and data in general will not be displayed.

By double clicking on the corresponding entry, the user can ask for approval. It is required to enter a reason for the access. Finally, click on **Request approval**.

An authorized person with admin rights now has to grant the approval. This is done in the Server Manager. For more information on this topic, please refer to the [Enterprise Server documentation](#).

If the approval has been granted, the user can double click on the corresponding element again. Password Depot will then ask the user if they are sure they want to break the seal and access the entry. Select **Break seal** to break the seal and access the entry. Depending on the user's access level, they will be able to open, edit, and use the corresponding element, etc.

NOTE: Seal status can be changed by an authorized person in the Server Manager at any time, if required. Thus, an already broken seal can be revoked and sealed access can be set again. In this case, a new approval will be necessary for the user if they want to access the element again. The process will start all over again as described above.

See also: [Grant Access to Entries](#)

Change type

You can change the entry type by highlighting an entry in the main view and going to **Entry → Change type**. For example, you can convert a "Password" entry into a "Credit card" entry. Automatically converting entries into another type of entry simplifies work since you do not have to carry out the required steps manually in **Password Depot**. Please find more information below on how to proceed when changing the type of entry.

The dialog window **Change entry type** displays the following information or moreover you can specify the following here:

- **Current type:** You can see here the entry's current type of entry.
- **Convert to:** Select the desired target type of entry from the drop-down menu, that is the type you would like to convert to. Custom entries have been added to the list of entry types.
- **Associate field names:** Specify how to proceed with the field names of the current type during conversion. For example, if you would like to convert a "Banking" entry into the entry "Software license", you can assign the field names of the current "Banking" type to the field names of the target "Software license" type. This way, a "Card holder" might be the "Username" after converting.

WARNING: If you **do not assign any** field names, the converter will only take information into consideration which is available for both entry types, for example the username/user or password field which are available for nearly every type of entry. To avoid data loss, we strongly recommend assigning the field names before starting with conversion since each **Password Depot** entry type basically uses a different template.

As soon as you have finished assigning the field names, click **Convert** to start the process. You will be forwarded to Password Depot's main view where you can see that conversion has been completed and the information saved to another type of entry.

HINT: You may also select multiple entries of the same entry type and convert them into another type at the same time provided these entries should be converted into the same target type.

Using Password Entries on the Internet

Key Shortcuts

To quickly access the most important functions of [Password Depot](#), use the following key shortcuts:

Function	Shortcuts
Favorites	Alt + C
Save Database	Ctrl + S
Save Database as ...	Shift + Ctrl + S
Print Database	Ctrl + P
Close Database	Ctrl + W
Create Backup file	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	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: Password Depot's keyboard shortcuts listed above are fixed and cannot be changed by users. In addition to that, there are several other global shortcuts which do work both outside Password Depot and within the program itself. You can define those shortcuts individually in the program options. To do so, please go to [Options → Hotkeys](#).

Open URL

The **Open URL** function can be found in the [Password menu](#) (**Ctrl** + **Ins**) → **URLs** or the menu **Entry** → **Open URL** (**F5**). This function opens a new Web browser session and goes to the URL address of the selected password.

You can always change the URL in the **URLs** tab from the password's **Properties** ([Modify password](#), **Ctrl** + **M**) dialog box.

NOTE: This function for opening the URL is only available if a password is selected from the database!

Open URL with

The **Open URL with** function can only be selected if a URL has been assigned to the entry (**Properties → URLs** Tab). If a URL has been linked to the entry, you can access the **Open URL with** option by right-clicking the corresponding entry.

You have the following options:

- **Internal Browser:** Opens the internal secure browser, which simplifies handling of your passwords. The internal browser offers all the functions of a standard browser. In addition, Password Depot features are available to make password management easier for you (**Open URL**, **Insert username**, **Insert password**, **Insert OTP code**, **Fill out the form**, **Search entry**).
- **System Default:** Opens the assigned URL in your default browser. The browser shown depends on which one you have set as default.
- **Mozilla Firefox:** Opens the assigned URL in Mozilla Firefox.
- **Google Chrome:** Opens the assigned URL in Google Chrome.
- **Internet Explorer:** Opens the assigned URL in Internet Explorer.
- **Microsoft Edge:** Opens the assigned URL in Microsoft Edge.

Copy Information to Clipboard

By right-clicking on an entry or via the tab **Entry**, you can access the **Copy to clipboard** functions.

These functions can be found in the [Password menu](#) and also in the [top bar](#).

NOTE: The options are only active if a password is selected from the list.

- **User name:** Copies the user name of the selected password to the clipboard.
- **Password:** Copies the selected password to the clipboard.
- **URL:** Copies the selected password's URL address to the clipboard.
- **TAN:** Copies the selected entry's TAN to the clipboard.
- **Custom fields:** Copies the selected entry's custom fields to the clipboard.

In order to define after how many minutes the information copied to the clipboard will be deleted, open the [Options](#) dialog box (under the **Edit** menu) and select the tab **Clipboard**.

Auto-completion of Web Forms

Browser Add-Ons

Password Depot can fill in web forms with user names, passwords and other login data for you. There are two methods how 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 activated when you open a website with a login. The communication with the Browser Add-Ons has been switched to **Native Messaging**. Currently, we offer add-ons for the following browsers:

- **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.

HINT: If you are encountering any difficulties with the browser add-ons, please have a look at our [Add-On](#) section in our [service center](#).

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.

HINT: 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 → 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.

HINT: 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 change it directly on a website within your browser, Password Depot will ask if you would like to update the already existing entry. Click **Update** to save the changes in Password Depot.

Some websites cause problems with automatic filling for various reasons due to the add-on. In such cases, you have the option to manually [correct or update the forms](#).

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.
- **Add a bookmark:** Add a bookmark for the visited website.
- **Settings:** Choose whether passkeys and passwords should be saved by the add-on. Also, you have the option of adding **Ignored URLs**, which will be ignored by the add-on.
- **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:** Opens the Password Depot website.
- **Rate Us:** We would be very happy if you could rate our add-on and its features!

Ignored URLs

This dialog shows you all websites that are currently ignored by the browser add-ons and therefore should not be filled in automatically.

You can open this dialog by going to **Database → Properties → Content → Edit URLs**. The dialog box **Ignored Websites** will open.

The following options are available:

- **Add:** Add a site to this list of ignored web sites, enter the URL into the text field above **Add** and then click the button. Alternatively, you can click **Ignore** after you have filled in a new log in and the program asks you if you would like to save this new password entry.

NOTE: The button **Add** will be activated (recognizable by the button's change in color from grey to black) only after you entered at least one character into the text field for ignored websites.

- **Replace:** Replaces the selected URL from the list with the URL from the text field below it.
- **Delete:** Erases the selected URL from the list of ignored websites so that it will be used again with the browser add-on.
- **Clear:** Clears the entire list of ignored websites.
- **Load from file/Save to file:** Saves the ignored website to a file or loads a website from a file.

NOTE: If you included a website here, you can still fill in its data via the [auto-complete](#) function.

Auto Completion

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 input 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** 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 on a website are filled with your user name, password and special characters such as **TAB** or **ENTER** .

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

- By going to **Edit → Auto-complete sequences** (**Ctrl** + **Q**)
- In the **Password** or **Properties** windows in 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.
- **Clear 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**: Inserts user name into the target edit box.
- **TAB**: Jumps to the next input element.
- **PASS**: Inserts password into the target edit box.
- **ENTER**: Emulates click on the key **Enter** .
- **SPACE**: Emulates click on the key **Space** .
- **CLEAR**: Clears the target edit box.
- **TOTP**: Inserts the current TOTP code into the target field
- **Additional**: Allows the addition of arrow keys, the keys **Home** , **End** , **Del** , **Backspace** , or a **delay**.

- **Custom:** You can also use your defined custom fields for auto-completion. For more information, see [here](#).

For the added elements, the following options are available:

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

After creating the desired sequence, click **OK**.

Clipboard Monitor Alert

This dialog box is shown when **Password Depot** is about to move sensitive data to the clipboard and detects that an unknown application monitors changes to the clipboard, using clipboard viewer technology.

NOTE: This alert does not automatically mean there is a real threat or infection. It is mainly a notification that you should keep track of.

Password Depot can 'mask' the changes it makes to the clipboard from other clipboard viewers, however, it cannot guarantee 100% that your PC is protected from any clipboard monitors. Note that **Password Depot** can only detect certain types of keyboard viewers and cannot replace a full-featured anti-spyware program.

When this dialog box shows, you have four options:

- Click the **Protect** button if you would like that the program proceeds to mask its changes in the clipboard.
- Click the **Ignore** button if you are sure that the detected program does not pose any risk and thus is eligible to read the data which **Password Depot** has added to the clipboard.
- In case of doubt, click **Cancel** to find out more about the detected program or process.
- Check the box **Save Selection** if you want the program to apply the option you have currently selected to all future actions.

Passwords

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.

Our application integrates with the Pwned service to check the security of user passwords. We ensure privacy and security by never sending the actual password or its complete hash to any external server, including Pwned's.

Process Flow

1. [User Input](#): The user enters a password into the application.
2. [SHA-256 Hashing](#): The password is hashed using SHA-256 locally on the user's machine.
3. [Partial Hashing](#): Only a portion (e.g. first 5 characters) of this hash is sent to the Pwned service.

4. **Pwned Query:** Pwned returns a list of hashes that have the same initial characters as our partial hash.
5. **Local Comparison:** We compare the full local hash with the list of similar hashes received.
6. **Result:** If there's a match, the user is alerted that their password has been compromised in the past and is advised to create a new one.

Key Points

- **Privacy:** At no point is the user's actual password or complete hash transmitted externally.
- **Efficiency:** The partial hash is sufficient for Pwned to return a list of possibly compromised hashes, keeping data transmission minimal.
- **Local Processing:** All comparisons are made locally, providing an extra layer of security.

Considerations

- **Performance:** The operation is lightweight and should not introduce noticeable latency.
- **False Positives:** Extremely unlikely, given the length and complexity of SHA-256 hashes.
- **Network Security:** Although only partial hashes are sent, ensure your network connection to Pwned is secure (usually via HTTPS).

By implementing this approach, we maintain a robust level of security while also respecting user privacy.

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

- **!:** This column displays the importance of an entry as determined by you in the properties of the entry. Therefore, it does not reflect an assessment of quality.
- **Description:** Displays the name of the individual entries.
- **Length:** Displays the length of the password.

- **Entropy:** The term "entropy" in relation to passwords is a measure of the uncertainty or predictability of a password. The higher the entropy, the more difficult it is to guess the password because there are more possible combinations. Entropy is usually expressed in bits and is a logarithmic measure. Each additional bit of entropy doubles the number of possibilities to guess. For example, an entropy of 10 bits means that there are 1,024 (2^{10}) possible combinations.
- **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.
- **Breaches:** Indicates how many possible breaches of your password there have been in the past.
- **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 entry**.

Generating Passwords

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**, the **Advanced** generator and the **Passphrase**.

Standard

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

- **Character types:** Choose what character types should be included for the generation of the password (Lowercase, Numbers, Uppercase, Special).
- **Length:** Allows you to define the maximum length of a generated password. The 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 as you wish.
- **Password policy:** 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 (to be found on the **Advanced** tab) 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 password settings:** 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 the 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:** Choose the length of your password.
- **Use only following characters:** If this option is enabled, the password only consists of the characters that have been chosen.
- **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:** Allows you to choose at least one of the character types.
- **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 as you wish.

- **Exclude consecutive identical characters:** Select this option to avoid consecutive identical character for better memorability.
- **Exclude strings from dictionaries:** Select this option to avoid strings of characters that can be found in dictionaries to increase security.

Generator

Here, the password is being generated and its quality is being assessed.

- **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:** Your generated password will appear here. Below it, you'll see a security meter—the longer and bluer the bar, the stronger your password.
- **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**.

Passphrase

On the **Passphrase** tab of the password generator, you can create secure, easy-to-remember passphrases based on dictionary words. The main advantage of passphrases over traditional passwords is their higher entropy while still being easier to memorize.

Options

Under **Options**, you define the parameters for generating the passphrase:

- **Words:** Specifies the number of words the passphrase should consist of. You can enter values between **3** and **32**.
- **Separator:** Defines the character used to separate the individual words (e.g. -, _ or .). Any single character can be used.
- **Language:** Specifies from which dictionary the words should be taken:

- **German** – uses German words only.
- **English** – uses English words only.
- **Mixed** – uses a combination of German and English words.
- **Capitalize:** When this option is enabled, the words in the passphrase are capitalized according to the predefined rules (e.g. with an uppercase first letter).

Passphrase field

- **Passphrase:** This text field displays the currently generated passphrase. You can also edit the passphrase manually here if required.

The following buttons are available:

- **Generate:** Creates a new passphrase based on the currently selected options (**Words**, **Separator**, **Language**, **Capitalize**) and displays it in the **Passphrase** field (button to the right of the passphrase field).
- **Clear:** Clears the currently displayed passphrase from the text field so that you can start again with empty input (button to the right of the passphrase field).
- **Copy:** Copies the passphrase currently shown in the **Passphrase** field to the clipboard (button to the right of the passphrase field).
- **Copy to Clipboard:** Copies the passphrase currently shown in the **Passphrase** field to the Windows clipboard so that you can paste it directly elsewhere (e.g. into a password entry). This button is located at the bottom of the dialog.
- **Cancel:** Closes the passphrase generator without applying further changes. This button is also located at the bottom of the dialog.

Advanced Password Generator

With the [Advanced Password Generator](#), you can generate a random password and define exactly which characters it should contain. In addition, you can save these settings as a template and use them for any other password which you later create with this password generator.

You can use the Advanced Password Generator when you add or modify a password entry. In the dialog window for adding or modifying an entry, click on the small [star symbol](#) (usually on the right-hand side), labelled [Generate](#). A dialog window will open, in which you then switch to the tab [Advanced](#).

Template

First of all, select a [Template](#) from the list:

- [Custom password settings](#): Allows you to create your own password template. You can save it under a name of your choice by clicking the [Save](#) button to the right. The next time you create a password, this template will also be shown in the drop-down list for templates. To delete a template you no longer need, select this template on the list and click the [Delete](#) button on the right-hand side.
- [Default settings for new passwords](#): Automatically adopts [global default settings](#).
- [Deduce settings from the current password](#): If you are currently modifying (and not adding) an existing password, the program will automatically choose this option which adopts the existing entry's settings for the new password.

Password settings

Here, you can define the characters the password should consist of:

- [Password length](#): Define the number of characters the password should consist of. You can select a number between five and 256.
- [Use only following characters](#): Enter some characters here, from which your password should be created. For instance, if you enter "abcdef" into this field, the generated password will only consist of these six characters.

- **Use following character types with relative frequencies:** Check all the character types which the password should contain, for example lowercase, numbers and special characters. Using the slider next to each type, you can set a percentage which indicates how frequently the selected character type will be used for the password. Via **Custom**, you can enter some characters which you would also like to be part of your password.

NOTE: Because UTF-8 is too extensive (64,000 characters), only the first 256 ASCII characters are supported.

- **Use at least one character of each type selected above:** Select this option to ensure that at least one character from every type is used for the password. For example: If you select uppercase letters, numbers and special characters as types and check this option, the created password will contain at least one uppercase letter, one number and one special character, even if it is only five characters long.
- **Exclude characters:** You can activate this option and define specific characters to be excluded by the password generator when creating new passwords. Please enter all characters you would like to exclude. By default, you can see some pre-selected characters which look similar and may therefore be mistaken (for example the 0=zero and O=the character O). You can add or remove as many characters as you like.
- **Exclude consecutive identical characters:** Select this option to avoid that the same character is used twice in a row in the password, for example ZZ.
- **Exclude strings from dictionaries:** Select this option to avoid using character strings that are included in dictionaries. Such sequences of characters or words can be remembered easily, but also belong to the most crackable passwords.

Generator

Here, the password is being generated and its quality is being assessed.

- **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:** Your generated password will appear here. Below it, you'll see a security meter—the longer and bluer the bar, the stronger your password.

- **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

Password Depot offers you a **Partial Password Builder**. To open it, select a password entry from your list and right-click on it, selecting **Partial Password** (**Shift** + **Ctrl** + **P**). Alternatively, click on **Entry → Partial Password**. Or, if activated, click on **Partial Password** on the top bar.

The partial password method is an authentication method for passwords, with the purpose of increasing protection against password theft. The method in question asks the user to insert certain characters of his passwords only, instead of entering all of them. As only a part of the password is always shown, this renders it more difficult to find out/intercept the password through common hacker techniques such as keylogging.

If you select a password entry and then open the Partial Password Builder, you will see four lines in the window:

- **Position:** The Builder assigns a number to each character of your password; the first character has the number 1.
- **Password:** Your password is shown here. If the function **Hide Password** is checked, the password's characters are displayed as dots. Otherwise, you will see the password's characters themselves.
- **Select:** In this line, you can select certain characters of your password, by clicking onto the desired boxes and thereby placing a check mark within them.
- **Partial Password:** In this line, the partial password created by the Builder will be shown, according to the characters you had previously selected in **Select**.

Here, the following options are available:

- **Hide Password:** If this function is checked, the password's characters are represented by dots. Otherwise, you will see the password's characters themselves.
- **Always on Top:** If checked, the window of the Partial Password Builder will be always at the front and visible.
- **Copy to Clipboard:** Copies the generated partial password to the clipboard.
- **Close:** Exits the Partial Password Builder and returns to the main window.

Master Password Generator

The **Master Password Generator** assists you in finding a password which is particularly safe and at the same time also easy to remember.

You can launch this generator when creating a new database and then, in the corresponding window, clicking on the button **Create Master Password** (star symbol to the right of the field **Master password**).

To create your master password, the generator takes a phrase of your choice as the starting point. The generator will then use the phrase's initial letters and change some of them in a random manner, using the Leetspeak Conversion Table (see second tab).

- **Please enter below an easy-to-remember phrase of at least 8 words:** Enter a phrase that contains at least eight words. You can think of the phrase yourself, but be sure to remember it! Having entered your phrase into this field, the button **Generate Password** becomes active. Click on this button to create a password.
- **Generated password:** Shows the password that the password generator has created from the phrase you had entered above.
- **Password quality:** Shows the generated password's quality.
- **Convert phrase using:** You can choose 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. After all, the most important thing is not only a secure password, but also one you can remember!
- **Template used:** 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.
- **Leetspeak Conversion Table:** On this second tab of the currently opened window, you can see the Leetspeak Conversion Table and also change the default table in use.

Click **OK** afterwards to use the generated password as the master password of your database.

NOTE: It is essential that you are able to remember the password based on the original sentence!

Password Depot Operations

Lock Password Depot

The **Lock** function is one of **Password Depot's** most important local security features: It allows you to safely leave **Password Depot** running on your computer without having to worry that someone else could take a look at your database.

Lock Password Depot

The **Lock** function can be found in three places:

- In the **Database** menu, under **Lock** (**Shift** + **Ctrl** + **L**) to lock the current database, and under **Lock all** (**Ctrl** + **L**) to lock all opened databases. If you lock the program via **Lock all**, this moves the application into the tray bar and in this way secures ('locks') it.
- In the blue toolbar, on the far-right side (lock icon).
- In the top bar (if used), on the far-right side (lock icon).

Unlock Password Depot

To restore and unlock the application, you must enter the authentication method of the currently opened file – i.e. its **master password** and/or **key file**:

1. Click on the tray bar icon of **Password Depot**. Alternatively, simply select **Password Depot** from your normal program applications.
2. A window opens, asking for the file's **authentication**.
3. Enter the **master password** and/or select the path to the **key file**.

NOTE: If you have entered a **wrong master password** and/or selected a wrong key file, you will receive a "The master password and/or key file are incorrect" **error message**. The application will be locked briefly. Afterwards, you can re-enter the master password and/or re-select the key file.

4. Click on the **OK** button.

NOTE: As long as the application is locked, you **cannot perform any actions**: neither edit the currently opened list, nor add a new list, nor open a different list. This may seem obstructing, but only this guarantees the highest security standard possible on your computer.

USB Installation

Optionally, you can run **Password Depot** via USB stick. This can be helpful if you want or need to keep your confidential documents, passwords, and other confidential information – which you manage via Password Depot – always at hand. If you would like to use Password Depot on such a removable storage device, then you will need to install it via the **USB Installation** function – **not** via the standard installation wizard!

The **USB Installation Wizard** (menu **Tools → USB Installation**) helps you to install Password Depot on removable storage devices, e.g. USB flash drives. Additionally, it lets you update both the program and your files stored on these devices.

To perform these tasks, proceed as follows::

1. **Removable drive:** Select the drive of your storage device.
2. **Copy/Update databases:** Having selected a drive, in this window, you will see all files stored on the selected device. Check those files that you would like to copy or update.
3. **Update Password Depot configuration file on the target medium:** If you check this option, your settings for the program will be transferred to the device as well.
4. **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.
5. **Next:** Click on this button to run the installation or to upgrade automatically.

NOTE: Certain functions that require a local installation (e.g. browser add-ons) cannot be used with the USB installation.

NOTE: When upgrading **Password Depot**, please **first** update the program on your local system!

Mobile Versions

You can also use **Password Depot** on mobile devices. Currently, we offer editions for the following mobile operating systems:

- Android
- iOS

These editions are currently **free** of charge.

You can easily export your PC's database to use it on your smartphone.

To synchronize the file on your mobile phone with the one on your PC, transfer the file by using the **Synchronize** function on the **Tools** tab to find any differences.

Operating System Android

1. Download the **Password Depot** app for Android via [Google Play](#) and install it.
2. Connect your mobile phone to your computer and transfer the .pswe file to the phone.
3. Start **Password Depot** Android Edition and load the file.

Please consult the [manual](#) for more information.

Operating System iOS

1. Download the **Password Depot** iPhone app via the [App Store](#) and install it.
2. Start iTunes.
3. Connect the iPhone, navigate in iTunes to **Devices → Your iPhone**. There, go to the **Apps** tab and scroll until you reach the File Sharing section.
4. Select the **Password Depot** App and add the database on the right side.
5. Now you can use your database in the iPhone App.

Please consult the [manual](#) for more information.

Command Line Parameters

You can start **Password Depot** using command line parameters. **Password Depot** supports the following command line parameters:

PasswordDepot.exe

PasswordDepot.exe [FileName.psw] – Launches **Password Depot** and loads the database "FileName.psw"

pdFileTools.exe

pdFileTools.exe <-encrypt|-decrypt|-erase> <FileName>

-encrypt: File encryption

-decrypt: File decryption

-erase: File deletion

<FileName> – File which contains the names of the working directory and the files to be processed

The format of this file has to be as follows:

First line – full path to the current directory

Next lines – relative paths to all selected files

Encrypt & Decrypt 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 indicating the strength of the chosen password.
- 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 of any format from your hard drive. These erased files cannot be restored, not even by specialized programs, since they are overwritten multiple times during their deletion.

This function can also be found in the **Tools** menu. Proceed as follows:

- 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**.

Erase External Files

With **Password Depot**, you can erase external files of any format from your hard disk, regardless of their format. These erased files cannot be restored, not even by specialized programs, as they will be overwritten several times.

To erase files, follow these steps:

1. From the **Tools** menu, select the option **Erase external files**.
2. In the dialog box that opens, select the file(s) you wish to erase.
3. Click on **Open**.
4. A warning message will appear to tell you that the selected files will be erased. If you wish to erase the files completely, click on **Erase**.

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:** Creates a new field. Name it and enter a value. The window **Edit custom field** opens.
- **Edit:** Edit the name or value of an existing field.
- **Delete:** Removes a custom field from your list.
- **Move 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:** Enter the name of an appropriate HTML input element.

Search Duplicates

This compact feature/function ([Tools → Search for duplicates](#)) searches up to three main fields of your database for duplicates:

- User name
- Password
- Default URL

While the user name can often be the same (e.g. due to representing your email address) and duplicate entries can also occur for the URL, **the password must never be identical**.

However, you also have the option of combining analyses by, for example, searching user name and password. You can use the operators AND/OR.

Then, click on [Find Duplicates](#) to start the process.

Note that the results that correspond to the previously selected fields and the operator will be grouped together.

You can use the following functions by right-clicking in the results list:

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

Click the [Export](#) button to export the list of possible duplicates found in your database into an external [CSV file](#) and save it to your local system.

Offline Mode

Enterprise Server databases can also be used in offline mode. This allows you to access your data when you're on the road or if the server is temporarily unavailable. You can continue working even if you are disconnected from the server, whether unexpectedly or intentionally. Once the server connection is re-established, all data should automatically synchronize with your server database. The access to offline databases can be limited in time.

Required settings on Password Depot Enterprise Server

The server administrator must enable the option **Save local copies for server databases** in the Server Manager. The following settings are required:

- Go to **Manage → Server Policies** and set the option **Save database locally** to either **Enabled** or **Not defined**.
- In the database area, select the desired database and enable the option **Save local copies** for individual users or groups at the database level. To do this, go to **Databases → Permissions → Select a user/group → Properties**, then check the option **Save local copy**.

Note: Any rights set in the server policies apply to the entire server and all users or groups. Therefore, if you want to exclusively grant the right to save local copies to individual users or groups, it is recommended to set the option in the server policies to **Not defined** and decide which users or groups can save local copies at the database level.

Required settings in Password Depot Client

In the Windows client, the following settings are required to properly use offline mode:

- Go to **Edit → Options → Save** and check the option **Database from Enterprise Server: Save local copy**. This ensures local copies of the server databases are automatically saved to the local system, so users don't have to save them manually. If this option is enabled, a copy of the server database is stored in the local directory **C:\Users\%USERNAME%\Documents\Password Depot\Network** automatically after

each session. If the option is deactivated, offline mode can still be used, but you must manually save the server database(s) before working offline.

How to use the offline mode

Once these settings are configured, you can use offline mode, when you are unable to connect to the internet. To use the offline mode, open the client and go to [Home → PD Enterprise Server](#). In the login, click the button to enable [Offline](#) mode.

Once you switch to offline mode, select the database you want to work with and enter the password you normally use to log in to the Enterprise Server.

After that, you can work with the database in offline mode and make changes as needed. All changes will be saved to the local copy of your server database automatically.

The next time you connect to the server, log in as usual at [Home → PD Enterprise Server](#).

Open the database while connected to the server. If any changes were made to the database in offline mode, they will automatically synchronize with the server database, when the option [Autosync all offline server files upon connecting](#) is enabled in [Remote databases/Databases from Enterprise Server](#) under [Edit → Options → Save](#).

If that option is [disabled](#), Password Depot will prompt you upon the next server connection to synchronize the changes made in offline mode with the server database.

To manually synchronize entries changed in offline mode, select them and click [Post](#) to trigger synchronization. All offline changes will be synchronized with Password Depot Enterprise Server in the background, ensuring your database is up to date.

Note: If multiple users have modified the same entry during offline mode, Password Depot will recognize this upon the next server connection and prompt you to synchronize the changes. You can review the changes and choose which data to synchronize to ensure only valid changes are applied.

Offline mode access conditions

The offline mode is currently available under the following conditions:

Offline Access with Standard Authentication (Password Depot user credentials)

Scenario	Clients	Notes
1: Password Depot Server (PD_Service_18) is running, and Internet connection is available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	Databases can be accessed via Offline Mode.
	Web client	Offline Mode is not available in the web client.
2: Password Depot Server (PD_Service_18) is running, and Internet connection is not available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	Databases can be accessed via Offline Mode.
	Web client	Offline Mode is not available in the web client.
3: Password Depot Server (PD_Service_18) is not running, and Internet connection is available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	Databases can be accessed via Offline Mode.

4: Password Depot Server (PD_Service_18) is not running, and Internet connection is not available.	Web client	Offline Mode is not available in the web client.
	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	Databases can be accessed via Offline Mode.
	Web client	Offline Mode is not available in the web client.

Conclusion: Offline Mode in Password Depot, using **Standard Authentication** (Password Depot user credentials), allows users on Windows, Android, and iOS clients to access databases even if the Password Depot Server is offline or there is no Internet connection. This enables continued access and usability of data during server downtime or Internet outages. However, it is important to note that **Offline Mode is not supported in the web client**, which requires an active server connection and Internet access to operate with Standard Authentication.

Offline Access with Integrated Windows Authentication

Scenario	Clients	Notes
1: Password Depot Server (PD_Service_18) is running, and Internet connection is available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	SSO authentication is not available on Android or iOS devices. Please use Standard authentication and enter the

		Windows user credentials instead.
	Web client	Offline Mode is not available in the web client.
2: Password Depot Server (PD_Service_18) is running, and Internet connection is not available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	SSO authentication is not available on Android or iOS devices. Please use Standard authentication and enter the Windows user credentials instead.
	Web client	Offline Mode is not available in the web client.
3: Password Depot Server (PD_Service_18) is not running, and Internet connection is available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	SSO authentication is not available on Android or iOS devices. Please use Standard authentication and enter the Windows user credentials instead.
	Web client	Offline Mode is not available in the web client.
4: Password Depot Server (PD_Service_18) is not running, and Internet connection is not available.	Windows	Databases can be accessed via Offline Mode.
	Android/iOS	SSO authentication is not available on Android or iOS

devices.
Please use Standard authentication and enter the Windows user credentials instead.

Web client

Offline Mode is not available in the web client.

Conclusion: With **Integrated Windows Authentication (IWA)**, Password Depot provides offline access to databases for Windows clients across all scenarios, regardless of whether the Password Depot Server or an Internet connection is available. However, **IWA** is not supported on Android or iOS devices. On these mobile platforms, users must use **Standard Authentication** by entering their Windows credentials manually to access databases in Offline Mode. It is also important to note that **Offline Mode is not supported in the web client**, which requires both an active server connection and Internet access to function with IWA.

Offline Access with OpenID Connect

Scenario	Clients	Notes
1: Password Depot Server (PD_Service_18) is running, and Internet connection is available.	Windows	Databases can be accessed via Offline Mode.
	Android/ iOS	Offline Access with OIDC authentication is currently not available on Android devices. Offline Access with OIDC authentication is available on iOS devices.
	Web client	Offline Mode is not available in the web client.
2: Password Depot Server (PD_Service_18) is running, and Internet connection is not available.	Windows	An Internet connection is required to obtain a valid authentication token.

	Android/ iOS	An Internet connection is required to obtain a valid authentication token.
	Web client	Offline Mode is not available in the web client.
3: Password Depot Server (PD_Service_18) is not running, and Internet connection is available.	Windows	Databases can be accessed via Offline Mode.
	Android/ iOS	Offline Access with OIDC authentication is currently not available on Android devices. Offline Access with OIDC authentication is available on iOS devices.
	Web client	Offline Mode is not available in the web client.
4: Password Depot Server (PD_Service_18) is not running, and Internet connection is not available.	Windows	An Internet connection is required to obtain a valid authentication token.
	Android/ iOS	An Internet connection is required to obtain a valid authentication token.
	Web client	Offline Mode is not available in the web client.

Conclusion: Password Depot provides varying levels of offline access depending on device type, server status, and Internet availability, with key requirements around **OpenID Connect (OIDC) authentication** for mobile devices. When both the Password Depot Server is running and an Internet connection is available, offline access is supported on Windows and iOS devices using OIDC, although Android devices currently lack offline support with OIDC authentication.

However, an Internet connection is essential to obtain a valid authentication token on all platforms (Windows, Android, iOS) when the server is running without internet connectivity or when both the server and Internet are unavailable, disabling offline access. Additionally, the **web client does not support offline mode** and always requires

both server and Internet connectivity for access. This configuration underscores the importance of an active Internet connection to obtain authentication tokens, especially for OIDC-based authentication on Android and iOS devices.

Customize Password Depot

Customize Browsers

In **Password Depot**, you can define your custom browsers which the program has not recognized as such.

To add a browser, proceed as follows:

1. Open the menu **Edit → Options → Browsers → Custom browsers...**
2. In the window that opens, click on **Add** (plus symbol).
3. Select a **Description** for this browser in the new **Custom Browser** window.
4. Below, you can select the **Path to .exe file** by clicking **Browse** on the right-hand side.
5. If applicable, please define additional **Parameters**.
6. Then, confirm your new browser with **OK**.

You can always change an existing browser via **Edit** or use **Delete** to remove it from the list. You can remove all created browsers from the list by clicking **Clear all**.

Customize Icons

In the dialog box **Select Icon**, you may associate a certain password entry or an entire folder with a specific symbol.

To open this dialog, call up the properties of the entry (via **Properties/Modify Entry**) or **folder** (e.g. via right-click) in question. In the respective dialog windows, you then click on **Change Icon**.

To assign an icon, you may either select a **predefined** icon (**Standard** tab) or one of your **own** icons (**Custom** tab).

NOTE: If you have opened a database from the **Enterprise Server**, you can choose new icons for the passwords, but it is not possible to delete and sort the custom icons. To delete custom icons, open the file locally (via the **Home → Local System** tab), make your changes and then ask the administrator to upload the changed file via the Control Panel.

Standard

On this tab, you can choose from several predetermined icons. To do so, select the desired icon and then click on **OK**.

Custom

The **Custom** tab allows you to manage the collection of your icons via the following commands:

- **Import:** Opens a dialog box where you may select an external graphic file to load. You can either select a file from the local system, from a URL or from the cache. This is also possible with the right arrow button.
- **Export:** Opens a dialog box where you can export a file from your PC. You can choose between **Export all** and **Export selected** with the right arrow button.
- **Delete:** Deletes a selected icon from the list.
- **Clear:** Deletes all icons from the list.

In the drop-down list **View Size**, you can determine the size of the custom icons: whether they should be displayed in **Large** or **Small** size.

Customize Appearance

The user interface consists of a maximum of five simultaneous windows or areas: **Password area**, **Navigation area**, **Statusbar**, **Toolbar**, **Tab bar** and **Details**.

Password Area

This is the main window. It is therefore placed in the center of the screen and cannot be closed or hidden.

This window provides access to your passwords.

A password's description and additional **information** can be displayed such as last modified, user name, URL, and category. Go to **Edit → Options → Layout** and change the layout according to your personal needs.

If the details view is enabled, you can select the details that should be displayed by right clicking on the details bar.

- You can select a different view for the list of passwords in the **View** tab.
- To edit password entries, switch to the **Edit** tab or **right-click on an entry**. This way, you can add, modify, delete, and print entries.

By right-clicking on an entry, you open the **password menu**. The menu's functions can only be used, however, if the information needed for this function – e.g. a TAN – is existent.

With this menu, you can:

- **modify ("Properties")**, **delete** or **print** the selected password(s), similar to the functions in the **Database** and **Edit** tabs.
- **cut**, **copy**, **insert** and **duplicate** the entry or add it to your list of favorites.
- copy the password's information to the **clipboard**.
- create a **Windows Shell Link**. This is a shortcut to a password that you can save anywhere on your system (e.g. on your desktop) and that allows you to access the password quickly.

From within the **Password Area window**, you can also move passwords from one group to another. Just select the passwords you want to move in the navigation area to the left of

Password Depot (which means this feature needs to be activated) and then drag & drop them into the desired group.

Navigation Area

This area displays a hierarchic structure of the folders inside the opened database, similar to Windows Explorer. Additionally, it also displays the [Favorites](#), the [Recycle Bin](#) and the [Search Results](#) after a search for quick access.

Types

In the navigation area, you can display the list of all types of entries available in Password Depot no matter if you have already used those entries or not. In general, you will see all entry types here. Double click a specific type of entry to display all entries of the same type currently available in your database in the main view. This will temporarily hide all other types of entries within the database in the main view and might be helpful, for example, if you would like to work with "Password" or "Information" entries only for some time.

Categories

You can do the same with the categories of your database. In the navigation area, all available categories will be displayed, that is both the built-in ones as well as the categories you created yourself. If your entries have been assigned to specific categories, you can double-click on a specific category in the navigation area to call up all entries that belong to the corresponding category (all types of entries included). Those entries will then be displayed in the main view. This way, you can search for entries using the categories they have been assigned to and display them in the main view.

If you are using the [Enterprise Server](#), you can quickly access the files from the server. To display the files in this area, click on [View](#) and activate the option [Databases on Server](#). The files on the server are only displayed if you are connected and logged in to the server.

Statusbar

If you have set the [Statusbar](#) function under [View](#), you will find a blue bar at the bottom edge of Password Depot, including information for version, license status (or remaining days for the trial mode), number of objects, "local system" (or network), and overall statistics (number of folders and passwords/entries).

Toolbar

Above the navigation and password areas, you will always find the **Toolbar**, offering quick access to Password Depot's important core functions, e.g. **Password** (create new password, second symbol from the left). Further to the right, there is a box/field for a file **path** as well as the basic **search function** ("Search entry").

Tab bar

The tab bar is positioned above the toolbar and displays all currently opened databases. This layout facilitates efficient management and operation when working with multiple databases. To open additional databases, click the **Home** button.

Details

This window is situated on the right side of the screen.

Its purpose is to display the information of a selected password in a more compact manner, so that required entries can be identified more quickly.

Furthermore, different actions are available in the details area which can be useful for your entries:

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

With these actions you can easily access any data stored in Password Depot and further use it.

HINT: If you have added custom fields to an entry, you will also see them in the details area on the right. However, information will not be displayed in clear text but hidden. If you want to read it, click on the eye icon. The information will be shown in clear text for

a short time. Next to it you can use the corresponding icon for pasting the information of a custom field to the clipboard.

NOTE: If you select the icon for **Custom Fields** in the details area, both custom fields referring to this entry and global custom fields which you may have added under **Edit** → **Global custom fields** will be displayed here. Thus, you can select the required information.

You can also see a star in the details area on the right. A yellow star means that this entry is one of your favorites.

Sort by

Here, you can choose how password entries are sorted, e.g. by their **Description** or **Importance**. When choosing the option **Custom sort**, you can change the arrangement of entries in the password area via **Drag & Drop** accordingly. To do so, select an entry from the list, and drag & drop it to the correct position.

Direction

Decide whether the sort order should be in **Ascending** or **Descending** order.

Group by

Choose if and how the entries should be grouped. They can be grouped either by their **Type** or **Category**.

Program Options

Program Options

In the **Edit → Options** dialog (**F10**) or by clicking on the **gear symbol** in the top-right corner, you can configure important program features individually.

The **Options** dialog box has the following tabs:

- [General](#)
- [Actions](#)
- [Hotkeys](#)
- [Topbar](#)
- [Passwords](#)
- [Save](#)
- [Clipboard](#)
- [Layout](#)
- [Network](#)
- [Browsers](#)
- [Warnings](#)
- [Search](#)

At the bottom left of each tab, you will find the possibility to **Restore default settings**. Use this option in case the program does no longer work as expected due to a specific combination of options.

Certain security-related functions are not stored within the program's Options, but within the database itself. These functions can be accessed via the respective file's [Properties](#).

Options - General

In the program's [Options](#) ([Edit → Options](#) or **F10**), the tab **General** allows you to change the following settings:

User interface

- **Language:** You can select the language of the user interface, e.g. English, German, French, Spanish or Dutch.
- **Theme:** Pick your preferred theme: **Light**, **Dark** or **System**. The selected theme will be applied each time you close the options by clicking **OK**.

Program start

- **Start mode:** From the drop-down list, define how **Password Depot** should be booted: in a normal window, minimized to tray, in the top bar or in the last state it was used.
- **Start in locked mode:** The program is always launched in locked state so that you will have to enter the master password to unlock it from the system tray.
- **Launch application on Windows startup:** Activate this option if you wish to start the program when launching Windows.
 - **Delay start for:** It may be helpful to delay the start of Password Depot by a certain number of seconds. For example, if your Windows needs some time before connecting to required network drives. The maximum value that can be set is 300 seconds.
- **Open last used database at program start:** Activate this option to load the same database as last time when starting the program.
- **Store lists of used databases and key files:** Check this option and the program will save a list of databases and key files which you have used recently. You can see your recently used files in the main menu and on the **Recent** tab when opening a file.
- **Restore tabs from the previous session:** Check this option if you want to restore the database tabs from the previous session.

Update settings

- **Automatic updates:** Choose between three options for automatic updates – "Download updates and prompt to install", "Notify when updates are available," and "Do not check for updates automatically".
- **Interval:** Choose an update interval, measured in days. You can set a maximum value of 365 days.

Options - Actions

In the program's [Options](#) ([Edit](#) → [Options](#) or **F10**), the tab [Actions](#) allows you to change the following settings:

Auto-complete

NOTE: These options refer to the normal [auto-completion](#) only (via **F6** or the lightning symbol). It does NOT refer to auto-completion by means of the [browser addons](#).

- **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. If you disable this option, you can open the URL/file via the corresponding button [Open URL](#) from the top bar or manually.
- **Window position:** Choose from four window position options (bottom left, bottom right, top right, top left).
- **Auto-complete delay:** Determine a value for the delay with which the program enters data. Normally you do not need to modify the default values, but on slow computers, this value may be increased to make the auto-complete function more stable (though slower). You can select values from 10 to 1000 msec.

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:** In case it makes sense with your first action, you can select another option here which will be taken after the first one.

Minimize program

- **Automatically minimize when the program is inactive for:** Set the period of inactivity after which the program should automatically minimize. Select this option and specify the desired time period in minutes. Values up to 600 minutes can be

entered. To additionally lock the program when it is not used, activate the option **Close database and lock program: When the program is auto-minimized**.

- **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

- **When the computer is idle for:** Specify the period of computer inactivity after which the auto-minimize function should activate. Select this option and specify the desired time period in minutes. Values up to 600 minutes can be entered.
- **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 automatically locked when it is auto-minimized.
- **Always when the program is minimized:** If you select this option, the program is automatically locked when it is minimized.

Options - Hotkeys

Several system-wide hotkeys are available in [Password Depot](#) which do work both within the program itself as well as outside Password Depot. Those global shortcuts are predefined by default and can be found under [Options → Hotkeys](#). You can define them individually in the options.

In Password Depot, by default those system-wide hotkeys are defined as follows:

Function	Hotkey
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 insert TOTP	Ctrl + Alt + O
Find and auto complete	Ctrl + Alt + A
Insert selected username	Ctrl + Shift + Alt + U
Insert selected password	Ctrl + Shift + Alt + P
Insert selected TOTP	Ctrl + Shift + Alt + O
Auto complete selected	Ctrl + Shift + Alt + A

In addition to that, you can use the **WinKey** + **→**, for example, for docking Password Depot to the right on your screen, or **WinKey** + **←** for docking it to the left on your screen etc. This way, you can work with Password Depot in full mode and still change between different programs and windows on your screen very easily.

Options - Topbar

In the program's [Options](#) ([Edit](#) → [Options](#) or **F10**), the tab [Topbar](#) allows you to make settings regarding the position and appearance of [Password Depot](#)'s topbar mode.

Position

- **Floating:** Activate this option to be able to freely move the top bar on the screen. You can additionally activate the option [Always top left](#) to always display the top bar on the top left of the screen, from where you can move it to any position.
- **Top screen edge:** Activate this option to always display the top bar on the top screen edge. Use the options [Always on top](#) and [Auto hide](#) to further define the behavior of the top bar.
- **Bottom screen edge:** Activate this option to always display the top bar on the bottom screen edge. Use the options [Always on top](#) and [Auto hide](#) to further define the behavior of the top bar.
- **Always top left:** (Only available when [Floating](#) is selected.) Enable this option if you want to always display the top bar on the top left of the screen.
- **Always on top:** (Only available when [Top screen edge](#) or [Bottom screen edge](#) is selected.) Activate this option if you wish to display the top bar always on top of all other applications.
- **Auto hide:** (Only available when [Top screen edge](#) or [Bottom screen edge](#) is selected.) Activate this option to hide the top bar by default. To have the top bar displayed again, you will have to move the mouse to the upper or lower edge of the screen, respectively.
- **Monitor:** If you have several monitors connected to your computer, this drop-down list allows you to define on which monitor the top bar is to be displayed.

Appearance

- **Color scheme:** With this option, you can define the color scheme of your top bar. You can choose between [Themed](#) and [Custom](#).

- **Custom colors:** If you activate this option, you can determine the top bar's color yourself. In case you select the same start and end color, the top bar will appear **only** in this one color. In case you select different start and end colors, the top bar will be shaded in a **color gradient**: starting from the defined start color at the bar's upper edge to the end color at the bar's lower edge. If the colors provided do not suffice, you can click on **Define colors** in the respective field and have a broader choice of colors.
- **Show bar captions:** If this option is selected, you will see explanatory texts when you move your mouse cursor onto the symbols shown in the top bar.
- **Show search box:** Show or hide the search field.
- **Transparency of bar:** Define a transparency level for the top bar. If you set the cursor to the left, the top bar is clearly visible; if you set the cursor to the very right, the bar is virtually invisible.
- **Height of drop-down lists:** This setting refers to the height of the two drop-down fields for groups and passwords. If you set a **low** value (left), the drop-down lists will be relatively **short** and can therefore only show up to ten entries at once; if there are further entries, you need to scroll. If you, however, set a **high** value (right), the drop-down lists will be **long** and can therefore show more, perhaps even all, entries.

Control widths

- Here, you can define the width of the fields **Database**, **Folder**, **Entry**, and **Search**.
- **Customize Top Bar:** Click this button to select the buttons you want to have in the top bar and put them in the order you want to have. [Learn more](#).
- **Large/Small icons:** Define the size of icons in the top bar.

Options - Customize Top Bar

To call up the dialog for modifying the top bar, there are two possibilities:

- Open the program's [options](#) (**Edit → Options** or **F10**), click on the [Topbar](#) tab and then onto the button **Customize Top Bar**.
- In case the program is in top bar mode, you can also open the dialog in question by right-clicking on the top bar and then clicking on **Customize**.

In the window **Customize Top Bar**, you will see two lists: on the left are all buttons that could be shown in the top bar but are currently not shown ("Available toolbar buttons"); on the right are all buttons that currently appear in the top bar ("Current toolbar buttons").

You are now able to make the following adjustments:

- **Add:** If you would like to add a button to the top bar, select this button from the left list and click on **Add →**. The selected button will then be cleared from the left list and will appear on the right list.
- **Remove:** To remove an item from the top bar, select this item on the right list and click on **← Remove**. The selected button will now be cleared from the right list and instead appear on the left list.
- **Reset:** If you click on this button, the program's default settings for the top bar will be restored. In this case, the top bar will contain the 15 generally most-used functions, e.g. the automatic fill-in function.
- **Move Up/Down:** Using these buttons, you can change the order in which the symbols appear in the toolbar. To do so, please select an element on the right list and then click on **Move Up** or **Move Down**. With every click, the element will be placed one position higher or lower.
- **User name as text button/Password as text button:** By checking the boxes for user name and password, respectively, you can add those as custom options to the top bar. That means you can see your current entry in clear text/unmasked format on the top bar. For this purpose, you can also set the maximum length of text displayed (**Max. text length**).

Options - Passwords

In the program's [Options](#) ([Edit](#) → [Options](#) or **F10**), the tab [Passwords](#) allows you to modify the settings of your saved passwords.

Editing

- **Default auto-complete method:** Allows you to define which auto-complete method will be selected for new password entries by default.
- **Default auto-complete sequence:** Allows you to define which auto-complete sequence will be selected for new password entries by default.
- **Default expiration period for entries:** You can set a period, after which your passwords will expire by default (for example 3 months). This expiry date is used as a reminder to change your passwords regularly. If you want to change the expiry date for a specific password, select it, click [Properties](#) and change the according option on the [General](#) tab.
- **Show warning for expired entries:** If you check this option, you will receive a warning by the program if passwords have expired. If you check it, you can set the number of days on which you will be shown a warning before the password expires ([Days to warn before expiration](#)). You can enter values from 1 to 30 days.

Master Password Policy

You can create your own policies in this area to define the minimum quality of master passwords for new databases.

- **Minimum password length:** This policy sets the minimum number of characters a password must have. A higher value increases security by preventing weak, short passwords.
- **Password must include:** This policy defines the password composition requirements, such as uppercase letters, lowercase letters, numbers, and special characters. By combining different character types, password security is increased, making it harder to guess or crack.
- **Enforce password history:** This is a security option that prevents users from reusing the same password in a short period of time. When this option is enabled, Password Depot stores a specific number of previous passwords for each entry and ensures

they are not reused when selecting a new password. The value for this option can be set between 0 and 24, where 0 means no password history is enforced, and 24 is the maximum number of stored passwords.

- **Password expires in:** This is an option that indicates how long a user password is valid before it expires and the user is prompted to create a new password. The option can be set in days and can range from 0 to 730. If the value is set to 0, the password never expires.
- **Minimum password age:** This security setting determines the number of days that must pass before a password can be changed. This setting is designed to prevent passwords from being repeatedly changed immediately to bypass the password history. The value for this option can be set between 0 and 365 days. With a value of 0, no minimum age is set, and the password can be changed at any given time.

Options - Save

In the program's [Options](#) ([Edit](#) → [Options](#) or **F10**), the tab [Save](#) allows you to determine e.g. how often the database and backup files are saved.

Save and backup

- **Autosave database on every change:** If you activate this option, any change to your database will be saved automatically. This improves the safety of your data.
- **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](#) (**Ctrl** + **S**) or [Save as](#) from the [Database](#) menu (or [Save](#) on the tool bar). Below, you can also specify how many backup files you would like to have overall.
- **Create a backup copy on database opening:** If you select this option, you will have to select the [Backup](#) function from the [Database](#) menu to create backups.
- **Number of stored backup copies:** Select how many backup copies should be stored. Here, you can enter values from 2 to a maximum of 32.

Remote databases / Databases from Enterprise Server

Here, you can define whether the local copy of your database should be deleted after you have finished working with files from an Internet server ([Remote database: Automatically delete local copy when closing](#)) or saved and kept locally ([Database from Enterprise Server: Save local copy](#)).

NOTE: These settings may be disabled through direct server settings by your administrator.

Working directories

Modify the directories of your [databases](#) and of the [backups](#).

Options - Clipboard

In the program's [Options](#) ([Edit](#) → [Options](#) or **F10**), the tab **Clipboard** allows you to configure the program's actions in relation to the clipboard.

Clipboard

- **Delete password from clipboard after:** Define the number of minutes and seconds after which the password is going to be deleted from the clipboard. This function helps you to prevent passwords from staying in the clipboard by mistake. The smallest value you can enter here is 10 seconds. The maximum value is 59 minutes and 59 seconds.
- **Hide clipboard changes from external viewers:** This feature prevents external applications from detecting clipboard activity, providing an extra layer of protection for your sensitive data.

NOTE: Password Depot only recognizes particular clipboard viewers. Therefore, it does not replace a full-featured anti-spyware program. How to proceed if Password Depot detects a clipboard viewer, is explained [here](#).

Options - Layout

In the **Layout** tab of the program's **Options** (**Edit → Options** or **F10**), you can set the following:

Entries font

Change the **font of your entries**. In general, the **Default** font is pre-selected. Choose another one from the drop-down menu as the default font for all types of entries within your database.

Expired entries

In the **Expired entries** area you can define how to proceed with expired entries while using the program:

- **Hide expired entries from the lists:** Select this option if you do not want expired entries to still be displayed in the main password area.
- **Hide expired entries from the search results:** Select this option if you want expired entries to be excluded during search. In this case, they will not be displayed in the search results.

Options - Network

In the program's [Options](#) ([Edit](#) → [Options](#) or **F10**), the tab [Network](#) allows you to set the options regarding your proxy server and the server module of [Password Depot](#).

Enterprise Server

- **Default authentication mode:** Set a default authentication mode to login on the Enterprise Server. If you choose an authentication mode, it will always be pre-selected in the Enterprise Server login window by default. This way, you do not have to manually select the required authentication mode each time you would like to connect to the server. The following options are available: [Integrated Windows Authentication \(SSO\)](#), [Sign in with username and password](#), [Azure AD/Entra ID](#), [OpenID Connect](#), [Windows Domain Credentials](#), or [WebAuthn/Passkeys](#).
- **Default domain name:** The default domain name option allows you to predefine the domain name for PD Server authentication. This makes it easier for you to log in, as you only need to enter your username. The domain name will be added automatically in the DOMAIN\username format.
- **Default UPN suffix:** The default UPN suffix is an option that allows you to define the User Principal Name (UPN) suffix for PD Server authentication. Similar to the default domain name, this feature simplifies the login process, as you only need to enter your username. The UPN suffix will be added automatically in the [username@upn.suffix](#) format.
- **User logon name format:** Choose the appropriate logon format based on your organization's structure and security requirements.
 - **Simple:** With this format, you only need to enter your username to log in. No additional information such as domain or UPN suffix is required.
 - **<DOMAIN>\<sAMAccountName>:** In this format, the username is entered along with the domain. The input is in the form of "DOMAIN\Username". Here, "DOMAIN" represents the name of the domain where the user is registered, and "Username" represents the individual username.
 - **UPN (User Principal Name):** In this format, the username is entered along with the UPN suffix. The input is in the form of "[username@upn.suffix](#)". Here, "username" represents the individual username, and "upn.suffix" represents the

predefined UPN suffix. This option is helpful when users from different domains need to access the same server.

- **Internet Protocol version:** Choose from three options (Auto, IPv4, and IPv6) for the internet protocol.
- **Automatically switch to offline mode when disconnected from the server:** If you check this option, the software will automatically switch to offline mode when you are disconnected from the server.
- **Automatically reconnect on network errors:** If you check this option, the software will automatically try to re-establish a connection after errors pertaining the network connection.
- **Reconnect interval (sec):** Set the temporal distance (in seconds) between the automatic attempts at reconnecting. You can enter values from 5 to 300 seconds.
- **Reconnect attempts:** Allows you to set how often the program should try to re-establish a connection. Here, you can enter values from 1 to 10.

SSL/TLS Settings

If your administrator installed a certificate on the Enterprise Server, you can define the settings for the SSL/TLS connection to the server, i.e., whether the **server certificate should be verified**.

Options - Browsers

In the program's [Options](#) ([Edit → Options](#) or **F10**), the tab **Browsers** allows you to set different options regarding the standard browsers and the browser add-ons.

Internet browsers

- **Default browser:** Select a browser here which you want to use by default. It will now be opened via **F5** and is preset if you click [Open URL](#). You can either choose a browser from the list of browsers which **Password Depot** has found on your system or define a custom browser by clicking on the [Custom browsers...](#) button.

Browser add-ons

- **Auto-fill web forms using add-ons:** Check this option if you want the browser add-ons to fill out web forms automatically. If you prefer drag & drop or the auto-completion via the lightning symbol, uncheck this option.
- **Add new passwords from web browsers:** If you want **Password Depot** to suggest to add new passwords that are not yet stored while you are surfing the Internet, check this option.

Add-ons online

- Password Depot provides direct links to the three browser add-ons: [Firefox](#), [Chrome](#), and [Edge](#).

NOTE: All options regarding the browser add-ons solely refer to the [Firefox](#), [Chrome](#), and [Edge](#) browsers since add-ons are only available for these three browsers.

Options - Warnings

In the **Warnings** tab of the program's **Options** (**Edit → Options** or **F10**), you can define which warnings should be sent by the program and which you would like to ignore. Thus, you can decide for yourself which warnings are helpful to you.

Uncheck the boxes of all warnings you don't want to be shown any longer. You can choose between the following options:

- 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.
- Moving entries to Recycle Bin.

Alternatively, you can also select **Check All** to activate all available warnings or **Uncheck All** to disable all warnings from being displayed by the program.

Options - Search

In the program's [Options](#) ([Edit → Options](#) or **F10**), the tab [Search](#) allows you to determine the options for searching your Password Depot's databases.

Search options

Automatically start quick search when typing (with delay in ms): Select the correct time you want the program to delay before initiating quick search in milliseconds. Values from 100 up to 2000 ms can be entered.

Use depth-limited search in folder view (levels): Select how many levels should be searched of your Password Depot's databases. Here, values from 1 up to 255 can be entered.

User Modes

User Modes

With the introduction of **Password Depot 18**, the different modes have been omitted from the client.

The Version 18 windows client now exclusively runs in Expert Mode.

NOTE: In case you are using older versions than Password Depot 18, you can change the mode by clicking on **View → Mode**.

You can select one of three modes:

- [Expert Mode](#) (available only in the trial and full professional version)
- [Beginner Mode](#)
- [Custom Mode](#)

Additionally, you can change the settings for the **Custom Mode** by clicking [Edit Custom Mode](#).

Expert Mode

NOTE: This option has been disabled with the introduction of **Password Depot 18**. The expert mode is enabled by default in version 18 and cannot be changed.

If you are using an older version of Password Depot than version 18, please read the following instructions.

In **Password Depot**, you can choose between three different [modes](#). The mode you choose determines the functions that will be available to you.

To change the mode, click on **View → Mode**.

In the **Expert Mode**, all functions contained in **Password Depot** are available. Thus, this mode also provides functions that cannot be used in the Beginner Mode (such as **Synchronize databases** and **Clean-up** under **Tools**). Due to its full scope of functions, the Expert Mode is especially appropriate for users who know the program very well and intend to use all of its functions.

To select which functions you would like to use, choose [Custom Mode](#). To use only the program's basic functions, choose [Beginner Mode](#).

NOTE: The freeware version after the trial period can be used only in **Beginner Mode**. To switch to **Expert Mode** with additional functions and settings, Password Depot must be [unlocked](#).

Beginner Mode

NOTE: This option is not available with **Password Depot 18**. The expert mode is enabled by default in version 18 and cannot be changed.

If you are using an older version of Password Depot than version 18, please read the following instructions.

In **Password Depot**, you can choose between three different [modes](#). The mode you choose determines the functions that will be available to you.

To change the mode, click on [View → Mode](#).

In **Beginner Mode**, only the **most important** and **most basic** functions of the program are available. Any advanced functions (like [Synchronize databases](#), [Clean-Up](#), [Export](#) in the **Tools** tab) are disabled and only available in the [Expert Mode](#) and [Custom Mode](#) (if set accordingly). Due to its restricted functions, the Beginner Mode is especially appropriate for users who do not (yet) know the program very well and/or who would like to only work with the program's basic functions.

To use all functions offered by the program, switch to the [Expert Mode](#). To determine yourself which functions you would like to use, choose the [Custom Mode](#).

NOTE: The freeware version after the trial period can be used only in the **Beginner Mode**. To switch to the **Expert Mode** with additional functions and settings, Password Depot must be [unlocked](#).

Options

The following ([Edit → Options](#) or ) are available in **Beginner Mode**:

User interface

- **Language:** Select the language of the user interface.
- **Icons:** Select one of two options for changing the colors of the design.

Internet browsers

- **Default browser:** Select a browser here which you want to use by default. It will be opened via **F5** and is preset if you click **Open URL/File**. You can either choose a browser from the list of browsers which **Password Depot** has found on your system or define a custom browser by clicking on the [Custom browsers...](#) button.

Browsers add-ons

- **Auto-fill web forms using add-ons:** Check this option if you want the browser add-ons to fill out web forms fully automatically. If you prefer drag & drop or the auto-completion via the lightning symbol, uncheck this option.
- **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 corresponding password (assuming there is an entry with a password for the current URL). For this function to work, the browser add-ons must be activated.
- **Add new passwords from web browsers:** If you want Password Depot to suggest to add new passwords while you are surfing the Internet, check this option.
- **Warn about identical passwords for different URLs:** Let Password Depot warn you in case of identical passwords for different URLs.
- **Close the Select Password dialog box automatically in:** Set the dialog field for selecting passwords to close automatically, after an interval measured by seconds. The default value is 10 seconds.

NOTE: All options regarding the browser add-ons solely refer to the **Edge, Chrome** and **Firefox** browsers since only these three browsers are available.

Display

Select the fields that will be displayed in the main window. Simply check all of the elements you would like to be displayed. You can choose from the following:

- **Importance**
- **Description**
- **URL**
- **User name**

- Password
- Type
- Last modified
- Expiry date

Custom Mode

NOTE: This option is not available with **Password Depot 18**. The expert mode is enabled by default in version 18 and cannot be changed.

If you are using an older version of Password Depot than version 18, please read the following instructions.

In **Password Depot**, you can choose three different [modes](#). Depending on the mode you choose varying functions will be available to you.

To change the mode, click on **View → Mode**.

In **Custom Mode**, you can choose which functions contained in Password Depot you would like to use and which you want to deactivate. In doing so, you can of course only deactivate those functions that are not critical. Functions that can be deactivated comprise e.g. **Synchronize databases** and **Decrypt external files** (under **Tools**). Due to its personally defined scope of functions, the Custom Mode is especially appropriate for users who know the program very well and exactly know which functions they will need.

To use all functions offered by the program, switch to the [Expert Mode](#). To only use the program's most basic functions, choose the [Beginner Mode](#).

Edit Custom Mode

NOTE: This option is not available with **Password Depot 18**. The expert mode is enabled by default in version 18 and cannot be changed.

If you are using an older version of Password Depot than version 18, please read the following instructions.

In **Password Depot**, you can choose three different [modes](#). The mode you choose determines the functions that will be available to you.

If you want to determine which functions of Password Depot you would like to use and which you do not need, run the program in **Custom Mode**.

Click on **View → Mode** to select and edit the [Custom Mode](#).

A click on **Edit Custom Mode** opens the **Custom Mode Editor** with the tab **Available Commands**. On the left side, you see a number of **Categories** into which the functions which you can enable or disable are divided. If you select a category on the left, you will be shown the corresponding functions (**Commands**) on the right-hand side. Remove the check mark if you do not want to use a function in your customized mode.

The following categories are available to you:

- **Edit** (with the following commands: Auto-complete sequences, Duplicate, Categories, Internet servers, Global custom fields, Linked entry)
- **Entry** (with the following commands: Copy TAN to clipboard, Create Shell link, Print, Generate password, Partial password, Edit active TAN, Mark active TAN as used, and Regenerate password)
- **File** (with the following commands: Save as and Backup)
- **Folder** (with the following command: Properties)
- **Search** (with the following commands: Advanced Search as well as Search and Replace)
- **Tools** (with the following commands: Import, Export, Encrypt external files, Decrypt external files, Security check, USB Installation, Erase external files, Synchronize databases, Clean-up, and Search for duplicates)

However, you can only disable functions which are not needed by the program to work normally. This means you can only disable extended functionality like [Synchronize databases](#) or [Encrypt external files](#) (under [Tools](#)).

Click on [OK](#) to save your changes.

Support

Technical Support / Frequently Asked Questions (FAQs)

The following technical support options are available to you:

Personal and Business customers:

- **Knowledge Base:** Visit our [Knowledge Base](#) to find a comprehensive list of frequently asked questions about Password Depot and their corresponding solutions.
- **Support Ticket:** Create a [Support Ticket](#) with your inquiry.
- **Email:** Send an email to info@acebit.de.

Business customers:

- **Phone:** Call us at +49 6151 1365010
- **TeamViewer:** Schedule a [remote support session](#) to solve the problem directly on your computer.
- **Webinar:** Book a personal [Webinar session](#) for a live demonstration of Password Depot.

License Agreement

You can find the license agreement for Password Depot in the installation program and on our [website](#).

A

Actions [205](#), [205](#)

Activation [18](#), [18](#)

Add Auto [161](#), [161](#)

Add credit card entry [91](#), [91](#)

Add EC card entry [93](#), [93](#)

Add identity entry [97](#), [97](#)

Add information entry [99](#), [99](#)

Add New Password [83](#), [83](#)

Add software license entry [95](#), [95](#)

Advanced Password Generator [171](#), [171](#)

Android [180](#), [180](#)

Attachments [116](#), [116](#)

Auto Completion [160](#), [160](#)

B

Backup [77](#), [77](#), [79](#), [79](#), [71](#), [71](#)

Beginner mode [223](#), [223](#)

Browser Add [156](#)

Browser Add-Ons [156](#)

Browsers [218](#), [218](#)

C

Change Authentication Settings [75](#), [75](#)

Clean-Up [130](#), [130](#)

Clipboard [214](#), [214](#)

Clipboard Monitor Alert [163](#), [163](#)

Command line parameters [181](#), [181](#)

Comment [70](#), [70](#)

Compare passwords [143](#), [143](#)

Complete sequence [161](#), [161](#)

Copy to clipboard [155](#), [155](#)

Create Database [50](#), [44](#), [45](#)

Create Password List [50](#), [44](#), [45](#)

CSV File Import [125](#), [125](#)

Custom Browsers [195](#), [195](#)

Custom Mode [226](#), [226](#), [227](#), [227](#)

Customize top bar [210](#), [210](#)

D

Database Properties [65](#)

Default browser [218](#), [218](#)

Delete Passwords [132](#), [132](#)

E

Edit Categories [145](#), [145](#)

Edit TAN [115](#), [115](#)

Encrypt and decrypt external files [182](#), [182](#)

Encrypted file [100, 100](#)

Enter Master Password [74, 74](#)

Erase external files [184, 184](#)

Expert Mode [222, 222](#)

F

File Properties [65](#)

G

General [203, 203](#)

Generate Random Password [167, 167](#)

Global Custom Fields [185, 185](#)

H

Hint [70, 70](#)

History [69, 69](#)

How to use this Manual [21, 21](#)

I

Ignored websites [159, 159](#)

Import Completed [129, 129](#)

Import from other password managers [127, 127](#)

Import Wizard [123, 123, 125, 125, 129, 129](#)

Importing and Exporting passwords [120, 120](#)

Installation Wizard [179, 179](#)

Internet Server [50, 50](#)

iPhone [180, 180](#)

K

KeePass [127, 127](#)

Key File Generator [76, 76](#)

Key Shortcuts [151, 151](#)

L

Layout [215, 215](#)

License Agreement [230, 230](#)

Local System [44, 44](#)

Lock [177, 177](#)

M

Master password generator [175](#)

Master Password Generator [175](#)

Mobile versions [180, 180](#)

Mode [221, 221](#)

Modify Password [82, 82](#)

N

Network [216, 216](#)

O

Ons [156](#)

Open URL [153, 153](#)

Options [205](#), [205](#), [214](#), [214](#), [203](#), [203](#), [215](#), [215](#), [216](#), [216](#), [211](#), [211](#), [213](#), [213](#), [208](#), [208](#)

P

Password [116](#), [116](#)

Password Depot Server [45](#), [45](#)

Passwords [211](#), [211](#)

Passwords Policy [69](#), [69](#)

Print [140](#), [140](#)

Professional Version Benefits [22](#), [22](#)

Program options [202](#), [202](#)

S

Save [213](#), [213](#)

Save Database [37](#)

Save List [37](#)

Search Password [134](#), [134](#)

Select Image [196](#), [196](#)

Sort Entries [139](#)

Sort Password List [139](#)

Start Page [123](#), [123](#)

Strong Passwords [23](#), [23](#)

Synchronize [142](#), [142](#)

T

Technical Support [229](#), [229](#)

Top Bar [208](#), [208](#)

Top Bar Mode [32](#), [32](#)

U

Update Manager [20](#), [20](#)

Upgrade from previous version [19](#), [19](#)

User Interface [24](#), [24](#)

V

View [27](#), [27](#)

Virtual Keyboard [31](#), [31](#)

W

Warnings [219](#), [219](#)

Windows Mobile [180](#), [180](#)