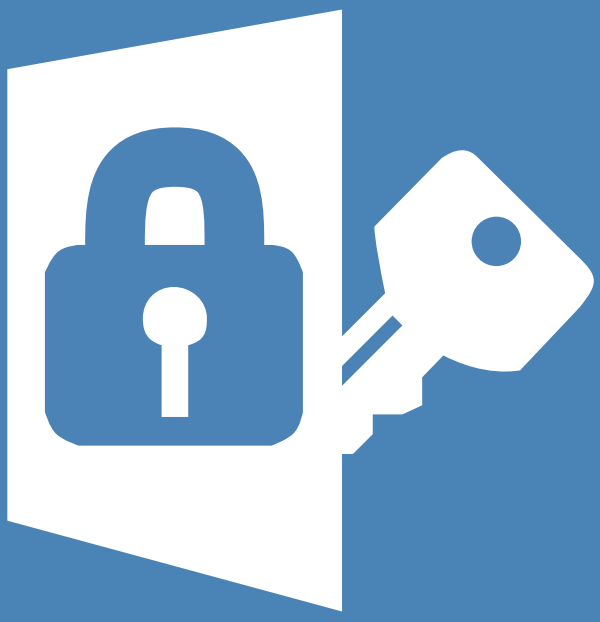
Password DEPOT

User Manual

Password Depot 11

Last Updated: 29.01.18



AceBIT
Every Bit an Ace!

Table of Contents

Welcome to Password Depot!

Congratulations for deciding to rely on **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 business companies, banks, agencies, and private users.

What is so special about Password Depot?

Password Depot is a **powerful**, **technically mature**, and, first of all, **secure** application for managing your passwords and access data. Different from conventional freeware and shareware utilities, Password Depot provides sophisticated security mechanisms and a well-conceived, wide range of functions and can also be employed in professional environments where strict security standards apply.

Security

Password Depot provides very high security standards in several ways:

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

- **Anti-keylogging protection:** All passwords have an internal protection against various types of key logging.

- **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.

- **Program protection:** Several new options optimize the protection of **Password Depot** itself: When the program enters the locked state, all sensitive data is cleared from memory. The program is able to auto-minimize/auto-lock when the computer switches to standby or hibernate mode, when the current session changes, etc.

- **Secury shredding**: The software **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 deletion of temporary files is also very important because they can contain data that could be extracted by someone. Deleting files in Windows Explorer is not secure, because only the filename will be deleted. To destroy a file beyond recovery, you must overwrite the file before deleting it.

- **Lock funktion**: You can restrict other users' access to **Password Depot** using the program's lock function. In this way, you can leave the software running on your computer without running the risk that someone else looks through your passwords.

High Functionality

Password Depot protects your most important and confidential passwords and access data from external access while offering maximum user-friendliness and a complete range of functions!

- The integrated **Password Generator** creates virtually uncrackable passwords which can be inserted into the corresponding field using drag & drop. **Password Depot** generates true-random data which cannot be predicted. Many conventional random generators create random data that are based on system time and can thus be predicted or reproduced.

- The **auto-complete** function allows to automatically complete fields on a web page 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 which appears at the top of the screen and which can be moved as you like.

- **USB flash drive support** allows installing **Password Depot** on a USB storage device. That way you have access to your passwords from any PC.
- You can also place your encrypted databases on the **Internet** and enjoy access to all of them, no matter where you are!
- The **Server Module** allows simultaneous access to databases available on a network by several clients. The system or network administrator assigns certain rights to the clients. For example, he can determine whether files may only be opened in read-only mode or may be modified.
- Free **apps for smartphones** allow to use the software on mobile devices, as well. Supported are the operating systems of iOS and Andoid.

Clarity

The user interface of **Password Depot** is very clear and easy to use:

- The databases are organized in the form of a **tree structure**, with the "stem" dividing up into different lists, similar as in Windows Explorer.
- An important feature of the user interface is the option to display the program as a **top bar**. The top bar window is a small bar positioned on top of all other applications, thus providing constant access to the passwords stored by the software and making Web surfing a lot easier.
- You can quickly localize passwords using the **search function**.

User-friendliness

Password Depot helps you to manage your passwords in an easy and structured way:

- For every password stored in the program, you may enter any **additional information** you wish, e.g. a description or the internet address accessed by the password in question.
- By means of a single mouse click, you **get directly to the URL** that is linked to a stored password entry.

- Data from your password entries may be copied **directly into the clipboard**, e.g. the password itself or its corresponding URL, but also any further fields you have defined yourself.
- You can make the program **automatically fill in** your passwords data into web forms.
- The passwords' organization in **groups** allows an efficient management of your data.
- For a clear overview of your databases you can add a **description** to every file. These descriptions will then be shown at every opening of the databases.

What's new?

Our software is being developed and updated constantly. In order to see what makes this software better than the previous versions please visit our website.

Getting Started

Quick start

Do you want to start immediately without having read the entire user manual? The following instructions will help you::

1. Install **Password Depot.**
   In order to be able to add passwords directly from the browser and the information to be filled in automatically on the website, you need to install the browser add-ons.
   If the add-ons are not installed, passwords can be added only manually and the the completion process needs to be started manually.(The add-ons can also be installed subsequently.)

2. Start **Password Depot**.

3. Create a new database, by clicking on **File** > **Database Manager** > **Local System** > **New Database**.

4. Open a database by authenticating yourself with the method configured in step 3.

5. Add passwords by clicking on **Add**. If the add-ons are installed, you can simply log in in the browser and **Password Depot** will ask if you wish to save this information in the opened database.

6. Create folders to group your entries. In order to create a folder right click on the left panel and select **NEW**.

7. If necessary, make adjustments to the entry, by clicking on **Modify**.

   > **Tip**: To make sure 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. The 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 click on the login button.

See also Auto-completion.

Installation

To install **Password Depot** on your computer, please perform the following actions:

1. Go to the **Password Depot** website and select the **Download** menu.
2. Click the indicated download link.
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. After successful installation, always go to the **Update Manager**. This way, you make sure that you are using the latest version of **Password Depot**.
6. Go to **Help** > **Unlock** to request a free activation key and enter your valid unlock code you received by e-mail to unlock the program.

Activation

To work with **Password Depot**, you need to activate the software. To work with the freeware version or the trial version, you can simply use the program without activating it.

The software activation is done within the program itself. To do so, please click on the **FILE** tab -> **Additional** -> **Unlock**. There opens a dialog window offering two options:

- If you have already purchased an unlock code, select **Step 2 - Unlock to full version**.
- Alternatively, by selecting **Step 1 – Get unlock code**, you get to the website where you can order an unlock code.

NOTE: Please note the difference between activation key and unlock code! The Unlock code is sent to you after you have ordered your software whereas an activation key is requested within the software itself by clicking on the corresponding button.

NOTE: In order to activate the software, you need to be **connected to the internet**.

The activation wizard takes you through following three steps in order to unlock **Password Depot.**

1. Enter Personal Information

At first, the wizard asks you to enter your personal details. All fields marked with an asterisk are obligatory and must be filled in.

> **IMPORTANT**: Your activation key will be sent to the email address you indicated in your personal data. Therefore, please enter an email address that is valid and that you can access during the registration process. Do not use the email address of a third person.

2. Request Activation Key

Click the **Request Activation Key** button. A free activation key will be sent to the email address you had previously specified within a few minutes.

Having received the activation key, enter it into the corresponding field.

> **NOTE:** You can request a new activation key if you need to activate your software again. This is for free and can be done as often as necessary.

3. Enter Unlock Code

Enter the unlock code which you received when ordering the software.

> **NOTE**: You can check if your activation of the program has been successful if you go to the **main menu** -> **Additional** and look at the field on the right side. Here it should be written that the programm is licensed for you.

Update Manager

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

In order to open the Update Manager, click onto **Help** > **Update Manager**.

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

Use this command 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 10.1.1 to 10.1.2), not however fee-based upgrades from one version to a higher one.

Introduction

How to Use this Manual

The user help offers explications concerning all functions of **Password Depot**.

If you need help concerning 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.

When you need assistance regarding 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 you miss a help topic in the manual, please contact our technical support.

In order to facilitate the manual's usage, different text contents are differenciated from one another by means of their design:

- *This type design stands for buttons and symbols.*
- **This type design stands for dialog fields, menus and menu items.**
- `This type design stands for Keys of the keyboard.`
- This type design stands for tips.
- This type design stands for examples.
- This type design stands for hints.
- This type design stands for warnings.

Password Depot Features

Password Depot is a powerful and very user-friendly password manager which helps to organize all of your passwords – but also, for instance, information from your credit cards or software licenses.

The software provides security for your passwords – in three respects: It safely stores your passwords, guarantees you a secure data use and helps you to have secure passwords.

However, **Password Depot** does not only guarantee security: It also stand for convenient use, high customizability, marked flexibility in interaction with other devices and, last but not last, extreme functional versatility.

Safe Password Storage

- **Best possible enryption** . In Password Depot, your information is encrypted not merely once but in fact twice, thanks to the algorithm AES or Rijndael 256. In the US, this algorithm is approved for state documents of utmost secrecy!

- **Double protection**. You can secure your databases doubly. To start with, you select a master password that has to be entered in order to be able to open the file. Additionally, you can choose to protect your data by means of a key file that must be uploaded to open the file.

- **Protection against brute-force attacks**. After every time the master password is entered incorrectly, the program is locked for three seconds. This renders attacks that rely on the sheer testing of possible passwords – so called “brute-force attacks” – virtually impossible.

- **Lock function**. This function locks your program and thereby denies unauthorized access to your passwords. The locking conditions are determined by you yourself, for instance every time the program has not been used for a certain time.

- **Backup copies**. Password Depot generates backup copies of your databases. The backups may be stored optionally on FTP servers on the Internet (also via SFTP) or on external hard drives. You can individually define the time interval between the backup copies’ creation.

Secure Data Use

- **Protection from keylogging**. All password fields within the program are internally protected against different types of the interception of keystrokes (Key Logging). This disables that your sensible data entries can be spied out.

- **Traceless Memory**. Dealing with your passwords, Password Depot does not leave any traces in your PC's working memory. Therefore, even a hacker sitting directly at your computer and searching through its memory dumps cannot find any passwords.

- **Clipboard protection**: Password Depot automatically detects any active clipboard viewers and masks its changes to the keyboard; after performing auto-complete, all sensitive data is automatically cleared from the clipboard.

- **Virtual keyboard**. The ultimate protection against keylogging. With this tool you can enter your master password or other confidential information without even touching the keyboard. Password Depot does not simulate keystrokes, but uses an internal cache, so that they can neither be intercepted software- nor hardware-based.

- **Fake mouse cursors**. Typing on the program’s virtual keyboard, you can also set the program to show multiple fake mouse cursors instead of your usual single cursor. This additionally renders impossible to discern your keyboard activities.

Verified Passwords

- **Uncrackalble passwords**. The integrated Password Generator creates virtually uncrackable passwords for you. Thus in future, you will not have to use passwords such as “sweetheart” anymore, a password that may be cracked within minutes, but e.g. "g\/:1bmVuz/z7ewß5T$x_sb}@<i". Even the latest PCs take millennia to crack this password!

- **Verified password quality**. Let Password Depot check your passwords' quality and security! Intelligent algorithms will peruse your passwords and warn you against ‘weak’ passwords which you can subsequently replace with the help of the Passwords Generator.

- **Password policies**. You can define basic security requirements that must be met by all passwords which are added or modified. For instance, you can specify the passwords’ minimum length and the characters contained therein.

- **Security warnings**. Password Depot contains a list of warnings which always keep an eye on your passwords' security. For instance, the program warns you in case you use the unsafe FTP protocol and in this case advices you to use SFTP instead.

- **Protection against dictionary attacks**. An important warning featured in Password Depot is the notification in case you are using unsafe passwords. These are passwords which are frequently used, therefore appear in hacker dictionaries and are easily crackable.

- **Warning against password expiry**. You can set Password Depot to warn you before your passwords expire, for instance before the expiry date of your credit card. This ensures that your password data always remains up-to-date and valid.

Convenient Access

Password Depot is very easy to use and spares you a lot of work.

- **User-friendly interface**. Password Depot's user interface is similar to that of Windows Explorer. This allows you to effectively navigate through your databases and to quickly find any password you happen to be searching for.

- **Auto-completion**. If you wish, Password Depot automatically fills in your password data into websites opened within the common browsers. This function runs via an internal setting on the one hand, and via so called browser add-ons on the other hand.

- **Automatic recognition**. You can set the program to automatically recognize which password information corresponds to the website you have called up and to then pre-select this password entry for you – as well as, if desired, to finally automatically fill this information into the website.

- **Top bar**. The program's form can be reduced to a narrow bar whose position may be individually determined: whether freely movable or stuck to the screen edge (Application Desktop Toolbar). In this way, the software is always at your hand without disturbing you.

- **Direct opening of websites**. URLs belonging to password entries saved in Password Depot may be opened directly from within the program. This spares you the hassle of having to manually copy website addresses and then paste them into your browser.

- **Usage via mouse click**. Using your password information may be done super easily via simple clicks with your mouse cursor. By means of a single mouse click, you can copy data to the clipboard and can even drag it directly into the target field on the website.

- **Hotkeys**. Pasword Depot features keyboard shortcuts for often-used commands in Windows (“Hotkeys”). By means of these hotkeys, you can easily turn Password Depot’s format into a top bar or call it into the foreground when minimized to the system tray.

- **Unicode support**. Password Depot supports Unicode, the international standard defining a digital code for every character. This allows you to use international characters such as “ä” or “ç” within your password information.

- **Recycle bin**. Password Depot features a recycle bin that stores deleted password data and enables their restoration. In this way, data you may have accidentally deleted, for instance, is yet not lost irrevocably.

Individual Settings

You can configure Password Depot individually and in this way adapt it precisely to your needs.

- **Configurable program options**. Thanks to many program options, Password Depot may be individually configured to the slightest detail – not only in view of its external layout, but also regarding its internal functions such as the use of browsers or networks.

- **Custom browsers**. You can determine yourself the browsers you would like to use the program with. In this way, you are not bound to the common browsers such as Firefox or Internet Explorer but can also use e.g. Opera.

- **Individual user modes**. As new user, you can work with only few functions in the Beginner Mode, while as expert you can use all functionalities in the Expert Mode or can define your own Custom Mode.

- **Personal favorites**. The list of favorites contains the passwords you use most frequently. As you will likely want to have this often-used data always ready at hand, the list of favorites may be accessed directly via the top bar.

- **Custom fields**. You can extend the existing data input fields by any number of self-defined fields. This is possible both for a single password entry (“Custom Field”) as well as for the entire passwords file (“Global Field”).

- **Password icons**. You can save icons for your password entries enabling you to easily find and place them. These icons are even available if you open your passwords file on a different PC as they are saved directly within the passwords file.

- **Individual safety warnings**. You yourself can determine the warnings you would like Password Depot to show and which not. Additionally, you may individually set whether the program should warn you in case your passwords expire and, if yes, how many days prior to the expiry.

- **Password statistics**. Clear statistics show at a glance how often you have used which password. In this way, you might also realize which entries you do not use at all and can therefore delete in order to keep your passwords file up-to-date.

Flexible Interplay

Password Depot is able to work together with many other applications - flexibly and without problems.

- **Server module**.Password Depot features a separate server model enabling several users to access the same passwords simultaneously. The access to the databases may run either via a local network or via the Internet.

- **USB stick**. You can copy both your databases and the program Password Depot itself onto a USB stick. In this way, you can carry the files and the software along wherever you go, always having them ready to use.

- **Cloud devices**. Password Depot supports web services, among them GoogleDrive, Microsoft OneDrive and Dropbox. In this way, Password Depot enables you to quickly and easily enter the Cloud!

- **Password files on the Web**. You can optionally deposit your encrypted databases on the Internet. By this means, you can always access your passwords, no matter where you are! To access, you can use the protocols HTTP, HTTPS, FTP or SFTP as required

- **TAN support**. Password Depot supports the input and management of TAN numbers. In this way, it facilitates the life of all of those users that refer to online banking, securely storing their sensible banking data.

- **URL placeholders**. Entering URLs into Password Depot, you can replace any number of characters by placeholders, namely an asterisk (*). Using this symbol, you can thus match several URLs to a single password entry instead of having to enter one entry for each URL.

Versatile Functions

Password Depot can do a lot more than 'only' securing and managing your passwords…

- **Cards, identities, licenses**. Password Depot protects and manages not only your passwords but also your information from credit cards, EC cards, software licenses and identities. Each information type offers a separate model, with e.g. the credit card window featuring a PIN field.

- **File attachments**. To your password entries, you may add file attachments containing e.g. additional information. These attachments can be opened directly from within Password Depot and may additionally be saved on data storage media.

- **Transfer passwords**. You can both import password entries from other password managers into Password Depot as well as export entries from Password Depot. To do so the software offers you special wizards that facilitate importing and exporting password information.

- **Synchronize databases**. Password Depot supports you in synchronizing two different databases. This is relevant e.g. if you are using a single passwords file on two different PCs. This being said, the file synchronization works in both directions.

- **Clean-up databases**. This function discovers password entries that you have not used for a long time or have even already expired. Afterwards, the found entries can be directly deleted. This guarantees that your databases always remain up-to-date.

- **Search for password entries**. By means of this function, you can search any character string within your passwords file – no matter if within the passwords themselves or within e.g. their descriptions and URLs. To refine your results you are able to limit the search to specific areas.

- **Encrypt external files**. Password Depot permits you to encrypt external files and to then directly save them as individual entries within the software. In this way, Password Depot enables you to make confident documents inaccessible to third parties.

- **Self-extracting files**. When encrypting external data by means of Password Depot, you can additionally generate encrypted self-extracting files. This method enables other people who do not have Password Depot to also decrypt the core files.

- **Delete external files**. With Password Depot you can delete external files, regardless of their format. In doing so, the software does not leave any traces on your hard disk which means that the files cannot be restored by any application however refined.

Professional Version Benefits

These are the advantages of the Professional Version of **Password Depot**:

- **No restrictions on the number of databases:** In the Professional Version you can create and use an unlimited number of databases, whereas the Freeware Version allows you to manage one file only.

- **No restrictions on the number of passwords:** In the Professional Version you can manage an unlimited number of passwords, whereas the Freeware Version allows you to manage 20 passwords only.

- Free use of **Enterprise Server** for up to 3 users: The Professional Version of **Password Depot** allows to use the Server Module with up to three users for free. A server license is only required for greater numbers of users.

- Registered users can get help from our **technical support** when they have questions or problems.

- **Notification of upgrades** and other products via e-mail.

- The **integrated Update Manager** automatically keeps your software up-to-date via the Internet.

Click here to go to the online ordering page.

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 Do 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 irrevocably delete confidential data.
- Brute-Force Attacks: Find out more about brute-force attacks and how you can protect yourself against them.

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 according upgrade for your version. The purchase of upgrades is less expensive than the purchasing of new versions.
2. Having completed your order, you will receive an **unlock code** for the current version.
3. Now **install** the current version. If you old version is not (anymore) installed on your PC, you do not need to re-install it. If it is already installed, however, you do not need to uninstall it. Yet we would recommend a deinstallation as this enables a better overview.
4. **Open** the newly downloaded current version.
5. Go to **Help** -> **Unlock** and select **Step 2 - Unlock to full version**.

6. Follow the wizard's instructions. First you will need to request a free **activation key**. In the next step you can enter the **unlock code** you received when you ordered a license.

7. Finally, you can open your database from the old version in the new version: Go to the main menu and click **Open** and then **Browse** and select the path to your file. By default, your file is to be found at "My documents" (XP) viz. "Documents" (Vista, Windows 7, 8 and 10). Confirm your choice with **OK** and authenticate for the file by using your master password and/or key file.

NOTE: For very old versions (versions 1 and 2) you will first need to install the trial version of a later version (version 3 or 4). Within this later version, please open and save your file. Subsequently, you can take over your file into the current version.

User Interface

General Description

Password Depot's user interface is designed for an intuitive use.

The buttons located in the toolbar include the most important and most used functions and are divided into tabs:

- **File**: Here you will find basic functions regarding databases and the program.
- **Home**: Offers functions for managing your passwords (e.g. add, modify. delete and print passwords) and the software (e.g. minimize it to a top bar or change into a different user mode). You can also access the program **Options** and the database **Properties**.
- **View**: Here you can modify the design of the program. On the one hand you select the **sort order** and the **view** for your passwords. On the other hand you can select the areas of the main view. The main view consists of maximally five windows: **Passwords**, **Files on server**, **Groups**, **F**avorites and **Details**. The **Passwords** window is always displayed; the four others can be shown or hidden. All of these four windows are explained below.
- **Tools**: Contains additional functions, such as Synchronizing and USB installation.
- **Password**: Offers functions for copying password elements to the clipboard, as well as other functions e.g. opening an URL or auto-completion.

> **NOTE**: In **Password Depot** there are many key shortcuts available helping you to quickly access frequently used functions.

Customize Appearance

Password Depot has a very flexible interface that can be modified in the **View** tab according to your requirements:

Areas

Here you set up the general appearance by choosing which areas of the main window should be displayed.

You can choose from five areas: **Passwords**, **Navigation Area**, **Files from Server**, **Details** and a **Toolbar**.

Passwords

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

This windows provides access to your passwords, showing all the passwords from the selected **folder**.

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 in the in the **View** tab.
- In order to edit password entries, switch to the **Home** tab. Here 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. Over this menu you can:

- **modify**, **delete** or **print** the selected password(s),
- **cut**, **copy**, **insert** and **duplicate** the entry or add it to your favorites list,
- copy the password's information to the **clipboard**,

- create a **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 **Passwords** window, you can also move passwords from one group to another. Just select the passwords you want to move and then drag & drop them into the desired group.

Navigation area

This area provides a tree 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.

If you are using **Enterprise Server** you can quickly access the files from the server here as well. To display the files in this area, click on **Navigation Area** and activate the option **Files on Server**. The files on the server are only displayed if you are connected to the server.

Details

This window is situated on the right side of the screen. Its purpose is to display the information about a selected password in a more compact space, so that it is easier to read.

Toolbar

Displays a toolbar on the top of the passwords area. Through this toolbar you have quick access to the most important password functions.

View

Here you can choose how your entries are displayed, e.g. as a **List**, **Symbols** or **Icons**.

Arrange

Sort

Here you can choose how the password entries are sorted, e.g. by their **Description** or **Importance**.

Direction

Here you can decide if the sort order should be **Ascending** or **Descending**.

Grouping

Here you can choose if the entries should be grouped. They can be grouped by their **Type** or **Category**.

Top Bar

The **top bar mode** is a very useful and unique feature of **Password Depot.** You can switch to this mode using the **Top bar** button of the toolbar.

The **Top bar** function minimizes **Password Depot** to a small bar that has the property to stay on top of all other applications, thus enabling constant access to the stored passwords.

The **Top bar** can be moved anywhere on the screen by simply pressing the left mouse button and dragging the mouse.

The **Top bar** allows you to select a specific password.

1. Select a group from the **Groups** field. After a group is selected, the passwords from the selected group are automatically displayed in the **Passwords** field. If the selected group is empty, no passwords will appear in the **Password** field.

2. Select a password from the **Password** field.

On the right side of the top bar, you will find various icons to access various program functions. In order to customize these icons, right-click on the top-bar and then click on **Customize**. The following icons can be displayed in the top bar:

- **Program options**: Opens the program options. Here, you can also adjust the settings of the top bar, via the **Top Bar** tab
- **Open Database Manager**: Allows you to open another database you have stored.
- **Save database**: Saves the current changes in your database.
- **New password**: Opens the dialog for creating a new password entry.
- **Modify password**: Allows you to modify the currently selected password in the according dialog.
- **Search**: Enables you to search for passwords according to their description, user name or URL.
- **Favorites**: Here you can directly choose a passwords from a list of often-used passwords.
- **Global Fields**: Shows a list of the global custom fields you entered. Click one of them to copy its content to the clipboard.
- **User name**: Copies the user name of the password to clipboard. You can also drag&drop the user name to a field on a web page.
- **Password**: Copies the password to the clipboard. You can also drag & drop the password to a field on a web page.
- **TAN:** Copies the TAN to the clipboard. Alternatively, you can use SHIFT+Click to emulate drag & drop.
- **Partial password**: Opens the Partial Password Builder.
- **Custom Fields:** Click on a custom Field from the list to copy its content to the clipboard. Alternatively, you can use SHIFT+Click to emulate drag & drop.
- **Inserts data**: Click onto this option and then into the first entry field in the target window. You will then be asked if you would like to fill in the user name or the password. Your choice will then be filled in automatically into the selected field.

- **Suggest password for URL**: By clicking this function, you enter the **Suggest password mode**. Click on the address line of the browser to display possible passwords.
- **Open URL in browser:** Opens the URL address of the password in your standard browser. With the little arrow button you can choose to open it within a different browser that is also installed.
- **Password Generator**: Helps you to generate a random password.
- **Insert URL**: You can either drag & drop the URL of the according password into a field (for example into your browser address bar) or click the button to copy the URL to clipboard.
- **Auto-completion:** Automatically completes fields on a Web page, normally with user name and password. If you click this function, you will enter the **Auto complete mode.** If you want to exit the **auto-complete mode**, click on *Cancel* in the **auto-complete mode** window situated at the top right of the screen.
- **Restore:** Restores **Password Depot** to the normal main window
- **Minimize:** Minimizes **Password Depot**
- **Lock:** Has the same function as in the main window of **Password Depot**.
- **Exit**: Quits the program.

Virtual Keyboard

The **virtual** (on-screen) **keyboard** allows you to insert keystrokes directly into password fields without using the keyboard. The virtual keyboard does not emulate the keyboard events, so no hardware or software key loggers 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**: If activated, multipple fake cursors will be emulated to protect you from other persons that might watch your screen.
- **Disable press effect**: If activated, the keys you click on won't be highlighted.

Password Files

Add Database

1. Open the file manager by clicking on **Database** > **Database Manager**.
2. Select the desired storage location in the left panel.
3. Click on **New Database**.
4. Enter the required information.
5. Click on **OK** when you are ready.

Open Database

1. Open the file manager by clicking on **Database** > **Database Manager**.
2. Select the desired storage location in the left panel.
3. Select a database and click on **Open**.

If the file is not listed, click on **Browse** and navigate to its storage location.

Save Database

In order to save the open 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 does the same as **Save**, with the difference that you can specify another name for the file, so you don't overwrite the old file.

NOTE: In the Options dialog box, you can set **Password Depot** to save your database each time you change it.

Save Databases on Internet Servers

Password Depot allows you to store databases or backup copies on Internet servers. In order to centrally manage these servers, there is the option **Manage Internet Servers**.

To manage your Internet servers, click on the **Tools** tab and then on **Internet servers**. In the window that opens, you have following options:

- **Add**: Allows you to enter a new Internet server. (More explication, see below.)
- **Edit**: Enables to change an existing Internet server. (More explication, see below.)
- **Delete**: Clears the server that you selected in the list.

Add/Edit Internet Server

If you click on **Add** or **Edit**, there opens the dialog box **Internet Server Profile**. Here, you can enter or edit the following information:

- **Protocol**: As protocol, you can choose between FTP, HTTP, SFTP, HTTPS, FTPS and FTPES.

  ADVICE: Generally, you should use the **SFTP** protocol as it allows **read and write** access and is additionally more **secure** than FTP. If you only need **read-only** access to a file on the Internet, however, the **HTTP** protocol is sufficient.

  NOTE: If you select **HTTP** or **HTTPS**, you **cannot upload new files** onto the server. Thus in this case, in the Database Manager, the function for uploading new files is disabled. New files can only be uploaded to FTP or SFTP servers.

- **Host**: Enter a host computer, e.g. "ftp.myserver.com" or "www.myserver.com". Enter a path, not a filename, into this field!
- **Port**: The default entry in this field is *Auto*; Password Depot will automatically search for the correct port.

- **Path**: Enter a complete path in this field. Do not enter a filename here! For accessing the root directory, enter only a slash (/).
- **User name**: Enter the user name. This entry is required for FTP servers.
- **Password**: Enter the password. This entry is required for FTP servers.
- **Passive**: Allows to switch between active and passive FTP mode.

> **NOTE**: The function **Passive** is only available if the protocol is set to **FTP**.
>
> **EXPLANATION**: The terms "passive" and "active" refer to the server's behaviour during data transfer with the client. In the **passive mode**, the server is **passive**, the data transfer being initiated by the client. In the **active mode**, by contrast, the server is **active** and asks the client for the port via which the data should be transferred. If the firewall on the client notices the incoming connection, however, it might stop this connection and thereby also stop the data transfer. Therefore if the firewall on the client does not allow for incoming connections, you should use passive FTP.

- **Mask password**: If you check this option, the characters of the password you entered are shown as dots. If the option is unchecked, you can see your password's actual characters.

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 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 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 list is stored under the URL *http://www.myserver.com/privatestuff/secret.psw*.

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

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

File Manager

Database Manager

Using the **Database Manager**, you can add new databases and open existing files.

Passwords files can be created and saved at following locations (each of which has its own tab within the Database Manager):

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

> **NOTE**: If you try to create a new database and the current database contains unsaved changes, you will be prompted to save your changes first.

Database Manager - New Database

The New Database window has the following fields in it:

- **Password list file name:** Enter a valid file name (e.g. "My Passwords") without any extension. The file will be saved with the entered name and the extension psw7.
- **Password list description**: This description will be displayed in the **Open file** dialog box. This field is optional.
- **Hint for master password**: Enter a hint for your master password. This hint will be displayed in the **Open file** dialog box if you have problems remembering the password. This field is optional.
- **Authentication by**: Select an authentication method for your database:
    - **Master password:** The common and safe (depending on the passwords complexity) method to encrypt your database.

    - **Master password and key file:** The most secure way to protect your database. You will need both a password and a key file to access it.

    - **Key file:** The database will be protected by a key file. Key files contain a complex key that are very secure and can't be cracked by brute force attacks. However, please note that anyone who has access to your key file and the database can open it. The key file can be compared to a common key for a safe and should be stored accordingly (e.g. on a USB drive).

- **Master password:** Required if selected as a **authentication method**. If you forget you master password, there will be no way to access your database. However you can enter a that will help you remembering it (see above).

    - You can either enter your master password into this field or use the **Generate master password** function (orange icon) to generate a random one. Lower and upper case letter are differentiated.

- **Re-enter master password:** Re-enter the previously entered password for safety reasons. Both entries must be identical.

WARNING: If you forget your **master password** and didn't enter a hint or the hint doesn't help you, there will be NO POSSIBILITY to recover your password inside the file. Please use a password you will remember.

- **Quality of master password:** Z Shows how safe the entered password is. The bigger the bar, the safer the password. Don't use passwords where a red bar is displayed. In addition to that, the **estimated crack time** will show you approx. how much time a professional hacker would need to crack your password.

NOTE: Please make sure to use a safe **master password**. It should be at least 8 characters long and contain numbers and letters as well as special characters.

- **Key file:** Required if selected as a **authentication method**. Enter an existing one by using the **Open key file** button on the right, or **Generate a key file** by clicking on the button next to it.

After you filled in all required fields you can click on **OK** to save the new file.

Database Manager - Local System

In **Password Depot**, you can open and save databases on your local system. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **Local System**. There are following options available:

- **New Database**: Enables you to create a new passwords file on your local system. A detailed description of this process is provided here.
- **Refresh**: Refreshes the list of databases on your local system, e.g. after you have made changes to the files.
- **Delete**: Deletes a selected passwords file from the list.
- **Browse**: Allows to search the local system for a specific passwords file and to the load this file.
- **Open**: Opens a passwords file selected in the list. In case the desired file is not shown in the list, simply search your local system for this file, using the function **Browse**. Then select the file and click on **Open**.

Database Manager - USB Storage Device

In **Password Depot**, you can open and save databases on a mobile disk, e.g. a USB stick. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **USB Storage Device**. There are following options available:

- **Drive**: Allows to select a USB storage device.
- **New Database**: Enables you to create a new passwords file on your local system. A detailed description of this process is provided here.
- **Refresh**: Refreshes the list of databases on your local system, e.g. after you have made changes to the files.
- **Browse**: Allows to search the local system for a specific passwords file and to the load this file.
- **Open**: Opens a passwords file selected in the list. In case the desired file is not shown in the list, simply search your local system for this file, using the function **Search**. Then select the file and click on **Open**.

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

Database Manager - Internet Server

In **Password Depot**, you can open and save databases on an Internet server. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **Internet Server**. There are following options available:

- **Server**: You can choose an existing server from which you can open a file and by means of which you can generate a new file.
- **New Database**: Enables you to create a new passwords file on your Internet server.

NOTE: The function **New Database** is only active and usable if the Internet server protocol is set to **FTP** or **SFTP**. New files can not be uploaded to **HTTP** or **HTTPS** servers. To find out and/or change the protocol currently used, go to the **Internet Servers** function.

- **Refresh**: Refreshes the list of databases in this storage location, e.g. after you have made changes to the files.
- **Manage Servers**: Allows you to add new internet servers on which you can subsequently generate databases.
- **Read-only**: If this option is checked, the program will open the file that you selected in the list in read-only mode.
- **Open**: Opens a passwords file selected from the list. In case you would like to open a desired file that is saved on a different server, simply click on **Manage Servers**. You can now create a new server. Then click on **Refresh**, select the desired file and click on **Open**.

Database Manager - Enterprise Server

In **Password Depot**, you can open and save databases on the Enterprise Server module. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **Enterprise Server**. There are following options available:

- **Login**: Directs you to the login site from Enterprise Server. Here, you enter all of the information indicated below this list. After the inscription, all databases that you can access will be listed.
- **Logout**: Logs you out of Enterprise Server.
- **Refresh**: Refreshes the list of available databases, e.g. after you have made changes to the files.
- **Change password**: Allows to change the password for Enterprise Server.
- **Read only**: If this option is checked, the program will open the file that is selected from the list in read-only mode.
- **Open**: Opens a passwords file selected in the list.

> **NOTE**: Passwords files for 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.

Enterprise Server: Login

Having clicked on **Login**, you will need to indicate your server information:

- **Server Address**: Type in the address from which Enterprise Server is executed. Generally, this is the local address, e.g. 90.0.0.1.
- **Port:** Enter the port from which Password Depot can be reached. By default, this is port 25803.
- **User name**: Enter the user name assigned by the administrator.
- **Password:** Enter the password assigned by the administrator.

Finally, click on **Login**.

> **NOTE**: Via the tab **Enterprise Server**, you can only open files for which you possess the required access rights. These rights are assigned to you by your network or system administrator.

TIP: If you have **Password Depot** (i.e. an unlocked version) or run **Password Depot** in the **30 Day Trial Mode**, you can manage up to **3 users for free** using the **Enterprise Server** module! In order to do so, please download the server module from our website and install it on one of the network's computers.

Database Manager - Dropbox

In **Password Depot**, you can open and save databases on Dropbox. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **Dropbox**. There are following options available:

- **Login**: Directes you to the Dropbox login site.
- **Logout**: Allows you to log out from Dropbox.
- **New Database**: Enables you to create a new passwords file on Dropbox.
- **Refresh**: Refreshes the list of databases on your local system, e.g. after you have made changes to the files.
- **Open**: Opens a passwords file selected in the list.

Database Manager - Google Drive

In **Password Depot**, you can open and save databases on Google Drive. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **Google Drive**. There are following options available:

- **Login**: Directes you to the Google Drive login site.
- **Logout**: Allows you to log out from Google Drive.
- **New Database**: Enables you to create a new passwords file on Google Drive.
- **Refresh**: Refreshes the list of databases on your local system, e.g. after you have made changes to the files.
- **Open**: Opens a passwords file selected in the list.

Database Manager - Microsoft OneDrive

In **Password Depot**, you can open and save databases on Microsoft OneDrive. In order to do so, please open the **Database Manager** (tab **FILE**) and click on the tab **Microsoft OneDrive**. There are following options available:

- **Login**: Directes you to the Microsoft OneDrive login site.
- **Logout**: Allows you to log out from Microsoft OneDrive.
- **New Database**: Enables you to create a new passwords file on Microsoft OneDrive.
- **Refresh**: Refreshes the list of databases on your local system, e.g. after you have made changes to the files.
- **Open**: Opens a passwords file selected in the list.

Database Manager - Recent Files

On the tab **Recent Files** tab in the **Database Manager**, you can see all files you have last accessed. This concerns both local files as well as files that were opened on e.g. an Internet Server or via **Enterprise Server**.

Simply select the desired file and click on OK in order to get to the window for entering the file's master password and/or key file.

> **NOTE**: The tab **Last Used** is only available if the program keeps a list of the last-used files. You can (un-)check this via **Options** > **General** > **Store list of last used files**.

Database Manager - Backups

This tab contains a list of all backups from the backups working directory. The working directory paths can be changed in **Options** (F10) > **Save**.

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

After you opened a backup, you should save it again in its original format by clicking on **File** > **Save as**.

Password File Properties

Database Properties

The **Properties** function displays the properties of the database and can be used to change some settings.

There are the following four tabs:

- General
- Advanced
- Notes
- Backup

Properties - General

On the **General** tab of the file properties you can view some basic information about your database and change them if applicable.

At the top you are shown the **Name** of your database. This cannot be changed in this dialog.

Below is shown following 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 **Save as** command in the main menu or make those changes in the Windows Explorer.
- **Size**: Shows the size of your passwords file in kilobytes and bytes.
- **Drive type**: Indicates the type of drive, e.g. "Permanent drive."
- **Free space**: Displays the storage space that is still available.

In the middle of the window, there is further information about your database. Most of this data is only for your information and can thus not be modified in this context:

- **Created**: Informs about the file's creation date.
- **Last modified**: Informs about the date of the file's last modification.
- **Contains**: Indicates the number of groups and passwords contained in your databases, as well as the number of passwords that have already expired.
- **Custom icons**: Shows the number of custom icons your passwords file is using.
- **Attachments**: Shows the number of attachments contained in your passwords file.
- **Delete icons/attachments**: Via these buttons, you can clear the icons and/or attachments contained in your passwords file. This will decrease your file's size.

> **NOTE**: If your database takes a lot of time to be loaded, you may need to consider to review your **attachments** and **custom icons** as they increase the size of your database. You can either use the **Clean-Up** function on the **Tools** tab to find entries and attachments which are no longer used or you can delete your custom icons and attachments via the **file properties** if your file is getting to big.

At the window's bottom, you can modify e.g. the database's authentication method:

- **Authentication**: Shows the currently used authentication method for this database.
- **Change**: Leads you to the window for changing the authentication settings.
- **Ignored Websites**: Opens a window listing the websites that are ignored by the browser add-ons and thus not automatically filled in.

Properties - Advanced

On the **Advanced** tab of the file properties you can define different settings regarding the password policy and password history.

Passwords Policy

- **Passwords hidden by default**: If this option is checked, passwords are hidden and will be shown as asterisks (***), e.g. in the **Modify Password** dialog. If you uncheck this option, passwords will be shown as clear text, meaning that you can see their actual characters. This is not recommended for security reasons, however, as showing your passwords' characters makes it easier to copy them.

- **Check passwords quality against dictionary attacks**: If you activate this option, the software will check every password for character strings which may be part of a dictionary. Having found such strings, the program will issue a warning. If you do not want or need such warnings, simply uncheck the present check box.

- **Force new/edited passwords to comply with the following rules**: 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 satisfy the defined policy you will be prompted to modify the password.

    - **Minimum length**: You can determine a minimum length, which means that all passwords must contain at least the number of characters which you indicate here.

    - **Password must include**: You can specify that all passwords must include certain characters. In this respect, you can set that passwords must contain either *all* or a *some* of the four symbol types shown below.

NOTE: In the field **(Password must include) At least x of the selected symbol types**, the number of character types you can set is limited by the number of types checked below. If you have checked two types, for instance, you can only set a "1" or a "2" into the field, not a "3" or a "4."

History

- **Keep passwords changes history**: If this option is checked, a new entry will be added to the password history whenever you change a password. You will find these stored changes on the **History** tab in the **Modify Password** dialog. The password history will for example help you if you created a new password and did not save it in the according account by mistake.

- **Max. number of changes in history**: Here you can limit the number of changes in the history that is saved.
- **Clear passwords history**: It can make sense to clear the passwords history for all passwords if many changes have been recorded in the course of time. Deleting them will help you to decrease the file size and to keep track of all password changes.

Properties - Notes

On the **Notes** tab of the file properties you can change the notes which you want to store for your database and for the master password.

- **Comment:** You may edit the comment on the database in this field.
- Hint: You may enter a new hint for the master password in this field.

Both notes will be shown in the dialog for entering your master password when you open a file.

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

Properties - Backup

In the dialog window **Backup** in the file properties, you can set the storage location and the creation of backup copies.

Backup Location

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

- **Internet Server**: In case you would like to save the backup copies on a Internet server, use the **Manage Servers** button in order to select an existing server or to create a new one.
- **Local System**: If you prefer to save the passwords file locally on your PC, select the according path via **Browse**.

Backup Settings

- **Create automatic backup every:** To create backups automatically and regularly, check this option and enter the number of days.
- **Create Backup**: Allows you to create a backup now.

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

Password File Authentication

Enter Master Password

When you open a database, 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 use this, the corresponding key file. The name of the passwords file that you are about to open is shown at the top right of the dialog title.

Show Details

Below the section for entering master password and key file, there is the option **Show details** viz. **Hide details**. Using these functions, you can show viz. hide the description of the passwords file your are opening.

If you have the details shown, you will see the button **Load last-used file at program start**. Depending on whether you check or unckeck this option, the passwords file that you have last used in **Password Depot** will be loaded upon opening the program.

Forgot your Master Password?

In case you have forgotten your master password and had indicated a hint to this password when generating it, you can click on **Forgot your password?** 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 retype the **master password**.

> **NOTE:** After each wrong entry, the **OK** button is disabled for three seconds to prevent brute force attacks.

Change Master Password

In order to change your master password, open the program **Properties** and select the tab **General**.

Change Authentication

In order to change the authentication for an open database, click on **Properties** (CTRL + i) > **General** > **Change**. This will start an assistant where you can change the authentication.

First you have to enter your current credentials and click on **Next** in order to authenticate.

After that you can select another authentication method or just define a new master password for the file.

Authentication by: Here you can choose one of several methods of protection for your database:

- **Master password** - The classic and (depending on the complexity of the master password) safe method of encrypting a database using a master password.
- **Master password and key file** - The database is protected by means of a master password and a key file.
- **Key file** - The database is protected by means of a key file. Key files contain complex encryption keys which are very safe and cannot even be cracked 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 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.

Key File Generator

You can use the Key File Generator at two moments:

- when you are creating a new passwords file,
- when you are modifying the authentication of an existing file.

In order to be able 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 only key file).

Having made this selection, you can click on the smal wheel symbol at the right of the field **Key file**.

There opens the Key File Generator. In order to now generate the key file (256 bit key), simply move your mouse cursor across the generator's field. In this way, you randomly select characters that will then make up your key. After you have generated the key, click on **Save** in order to save the key as a proper file.

WARNING: Keep the generated key in a safe place and do not forget to make backup copies. We highly advise **against** using only an external keys for authentication since this means that anyone who has access to the PSW file and the key file can read your passwords without having to enter a master password.

Backup Copies of Password File

Backups

In **Password Depot**, you can create backups of your databases.

Backup copies increase the security standard. For instance, you can recreate the content of a file that was accidentally deleted by using a backup file.

Basically, backup copies are identical with regular databases. The only difference is their file extension name ".bck".

> **NOTICE**: We highly recommend the use of backup copies!

Backup location

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

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

This backup location you can access via **Options** > **Save** > **Working directories** > **Backups**.

In order to change this backup location, you have two options. Either you enter a different local directory, or you choose an Internet server.

- In order to choose a different local directory:
  - either: **Home** > **Properties** > **Backup**
  - or: **Options** > **Save** > **Working directories** > **Backups**.
- In order to save the backup copies on an Internet server, click on the tab **Home** > **Properties** > **Backup**.

How to create Backups

Backup copies can be created in two different was: manually by the user or automatically by **Password Depot**.

Creating backups manually

You can manually create backup copies of your current passwords file. To do so, open the tab **File** and click on **Backup**.

Creating backups automatically

You can tell the program to create backups regularly and automatically. For this, there are three options:

- **Automatic**: You can set the program to create automatic backups and can additionally specify how often they should be created. This can be cone via **Properties** > **Backup**.
- **Upon opening the passwords file**: You can specify that a backup copy should be created upon every opening of the passwords file, via **Options** > Save > **When database is opened**.
- **Upon saving the passwords file**: Also, you can set the program so it will create a backup copy every time the passwords file is saved, via **Options** > Save > **When file is saved**.

How to open Backups

The backup files generated by **Password Depot** have the file extension .bck or .bckx and are stored by default in the following folder:

- Documents\Password Depot\Backup

In case your database is damaged or was 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 **File** > **Database Manager**.
3. Click on **Backups**.
4. Select a backup of your file from the desired date and click on **Open**.

5. Authenticate using your master password and/or key file.
6. Click on **File** > **Save as** in order to save the file in its original format (.psw8 or pswx).

Password Entries

Adding & Modifying Password Entries

Basic Password Entry Operations

Add Password Entry

In order to add new entries, clck on **Home** > **Add**. The new password will be saved in the currently opened folder (shown in the navigation area).

Click on the upper half of the **Add** button in order to add a password or on the lower half of it (arrow down) in order to add one of the following entry types:

- Password
- Credit Card
- EC-Card
- Software License
- Identity
- Information
- Encrypted File

Modify Entry

In order to modify existing password entries, please open the **Modify Entry** dialog window.

This window can be accessed in two ways:

- Either you select the password and then click on **Home** > **Modify**,
- or you right click the password and choose the option **Modify**.

NOTE: The function **Modify Entry** can only be accessed if you have previously selected a password entry from the list.

You can modify all types of password entries that are possible in **Password Depot**:

- Password
- Credit Card
- EC-Card
- Software License
- Identity
- Information
- Encrypted File

Add/Modify Entry - Password

To add or modify a password entry, click on the **Add** or the **Modify** button and then select **Password**.

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

- **Description**: Enter a description for the new password. The description is the name that will be displayed in the Passwords window.
- C**hange Icon** (button left of Description): Changes the icon for this entry. There opens a drop-down menu offering following options:
    - **Select Icon**: Enables to choose an icon from a list of default icons or to elect one that is stored on your PC.
    - **Load from URL**: Click on this button if you want to use the standard icon (favicon.ico) of the URL you entered.
    - **Reset Icon**: Resets the standard password icon of **Password Depot**.
- **User Name**: Enter the password's user name.

- **Password**: Enter the password.
- **Show/Hide password** (three dots next to the password box): Changes whether the password is shown or hidden (and represented by dots).
- **Confirmation**: Retype the password.
- **Generate random password** (wheel symbol at the right of the confirmation box): Opens the wizard for generating random passwords After you have generated your password, the **Enter Password** and **Confirmation** fields will be automatically completed with the newly generated password.
- **Quality**: Shows how secure or insecure your password is. In addition, you will be shown how long it approximately takes to crack your password.
- **Importance**: Select an importance level for your password.
- **The password is secure**: Check this box if you believe the password is secure and don't want to be warned about it.
- **Category**: Categories help you to structure your passwords.
- **Expires on**: You can use this option if you want to be remembered about changing your password. You can either enter a date when the password will expire or click on the button next to the date field, to select how long the password will be valid.
- **Comments**: Add any further comments to the new password.

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

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

- **URLs**
- **Additional**
- **Custom Fields**
- **TANs**
- **Attachments**
- **History**

Add/Modify Entry - Credit card

To add or modify a credit card entry, click on the **Add** or the **Modify** button and then select **Credit Card**.

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

- **Description**: name for the credit card which helps you to identify this entry
- **Card Type**: select the type of card you are entering
- **Card Holder**: card owner's name
- **Card Number**: card number
- **PIN**: card's PIN number
- **Valid thru**: card's expiry date
- **Security Code**: card's security code
- **Service Phone**: Enter the telephone number of the credit card company
- **Additional Code**: if needed, supplementary code
- **Service URL**: bank's URL
- **Additional Info**: if needed, supplementary information
- **Comments**: if needed, supplementary information

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

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

- **Additional**
- **History**

Add/Modify Entry - EC Card

To add or modify an EC card entry, click on the **Add** or the **Modify** button and then select **EC Card**.

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

- **Description**: Enter a name for the EC card here which helps you to identify this entry
- **Account Holder**: Name the owner of the card
- **Account No.**: Enter the number of your bank account
- **Bank Code:** Enter the code which identifies your bank
- **Bank Name**: Enter the name of your bank
- **BIC**: Enter the BIC code of the bank for international transfers
- **IBAN**: Enter the BIC code of the bank for international transfers
- **Banking URL**: Enter the address for online banking and enter your user name and password for the login.
- **Login Name**:
- **Password**:
- **Valid thru**: card's expiry date
- **Card Number:**
- **Service Phone**: bank's telephone number
- **Legitimacy ID**: if need, additional code for online banking
- **PIN**: card's PIN number
- **Comments**: if needed, additional information

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

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

- **Additional**
- **History**
- **TANs**

Add/Modify entry - Software license

To add or modify a software license entry, click on the **Add** or the **Modify** button and then select **Software License**.

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

- **Description**: a name for the software license here which helps you to identify this entry
- **Product**: product's name
- **Version**: product's version number
- **Registered Name**: name of the person the software is licensed to
- **Order No.**: product's order number
- **License Key**: product's license key
- **Additional key**: if needed, an additional key (e.g. the license key of a previous version)
- **Download URL/File**: URL or file where the product can be downloaded
- **Download is password protected**: indicates whether the download requires a password
- **Purchase Date**: With the help of the calendar function, select the date when you bought the product
- **Espires on**: license's expiry date
- **Email Address**: email address used for the license's purchase

- **Comments**: if needed, additional data

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

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

- **Additional**
- **Attachments**
- **History**

Add/Modify Entry - Identity

To add or modify an identity entry, click on the **Add** or the **Modify** button and then select **Identity**.

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

- **Description**: Enter a name for the identity here which helps you to identify this entry
- **Account/ID**: Enter a nick name or another identification here
- **E-Mail-Address:** Enter the e-mail address here
- **First/Last Name**: Enter the name of the person here
- **Date of birth**: Enter the birth date of this identity/contact here
- **Company**: Enter the company here
- **Address 1/Adress 2**: Enter some postal address information here, for example a street and house number
- **City**: Enter the name of the city here
- **State**: Enter a state or district here
- **ZIP**: Enter the postal code of the city here

- **Country**: Enter the country here
- **Phone/Mobile/Fax**: Enter the telephone and fax number here
- **Website**: Enter the URL of a website into this field
- **Comments**: Enter some additional data here

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

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

- **Additional**
- **History**
- **Attachments**

Add/Modify Entry - Information

To add or modify an information entry, click on the **Add** or the **Modify** button and then select **Information**.

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

- **Description**: Enter a name for the information here which helps you to identify this entry.
- **Content**: Enter some text you want to save here. You can format your text using the buttons below.

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

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

- **History**
- **Attachments**

Add/Modify Entry - Encryped File

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

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

- Click on **Home** > **Add** > **Encrypted File**
- Encrypt a file via **Tools** > **Encrpyt.**
- Right-click on a file in the Windows Explorer and click on **Password Depot 10** > **Encrypt** (it will automatically be taken over into **Password Depot**).

In the dialog window, following functions are available:

- **Description**: Add a description for the encrypted file.
- **Password**: Enter a password for the encrypted file.
- **Files**: Shows a list of encrypted files belonging to the selected password entry.
- **Decrypt**: Select a file in the list and click on **Decrypt** in order to decrypt it by means of the entered password.
- **Add**: Enables you to add an encrypted file to the list.
- **Delete**: Removes all files you do not need anymore from the list.
- **Delete Invalid Paths**: The software automatically detects if the file is no longer available at the original path. These files will be greyed out. If this applies to more than one file, you can use the button **Delete Invalid Paths** to remove all of these files from the list.

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

Advanced Password Entry Operations

Add/Modify entry - Tab URLs

When you add or modify a password entry, you can modify both its default URL and link it to other URLs. To so do, please open the tab **URL** in the windows for adding/modifying an entry.

Default URL

Enter the URL of a website or the path of a file you would like to use with this entry.

> **NOTE**: This field doesn't support wildcards (*). In order to add masks with wildcards in them, use the list below this field.

Associate account with following URLs

Below, you can associate the selected entry with other URLs that use the same login data. In this way, you do not need to make separate entries for each of these URLs anymore.

> **EXAMPLE**: For instance, the same password and user name might be used on the websites http://forum.example-url.com/log/ and http://example-url.com/login.htm.

In the URL dialog window, you have following options:

- **Add**: Adds a URL that uses the same login data as the selected entry's URL and that you would therefore like to link to the entry's default URL.
- **Replace**: Replaces the URL that is selected in the window by a different URL.
- **Delete**: Deletes an URL selected in the window.
- **Clear**: Deletes all URLs show in the window.

> **NOTE:** Since most websites use as well URLs with www. (e.g. *www.example.com*) as URLs without it (e.g. *example.com*, masks like ***example.com*** work best.

Add URLs

When you add URLs, you can either enter precise URLs or use masks for them. In such a URL mask, several characters can be replaced by a specific single character. In Password Depot, this replacing single character is represented by an asterisk (*) that can be placed at the beginnening and/or end of a 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**: **example-url.com** includes all possible sites of this domain.

> **NOTICE**: The button **Add** only becomes active and usable (recognisable by the button's change in color from grey to black) if you enter characters into the field above.

Add/Modify entry - Tab Additional

Command line parameters

Specify here the parameters string to be used when opening a local executable file or document.

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

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

Example: The correct way of indicating a command for putty is as follows:
> Create a new password entry.
> Enter your log-in data 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**.
> Into the field **Open local file with command line parameters**, you need to enter the following: <USER>@12.345.678.123 -pw <PASS> (Replace "12.345.678.123" with your IP address.)
> 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

If you would like to use the auto-completion function, check the according field and select an auto-complete sequence from the list. (This is not needed for the browser add-ons.)

If none of the existing sequences matches, click the **Add** or **Edit** button to open the Auto-complete sequences dialog box. Here you can define your own auto complete sequence.

Auto-complete method

Select here one of the following methods to use it in auto-complete mode (ligthning symbol):

- **Clipboard I** - In this case user name, password and other fields copied into clipboard and then pasted into target windows using emulation `Shift` + `Insert` key combination.
- **Clipboard II** - In this case user name, password and other fields copied into clipboard and then pasted into target windows using emulation `Ctrl` + `V` key combination.
- **Keyboard** - In this case user name, password and other fields are inserted into target windows using emulation of keyboard typing.

- **Multi-Channel Obfuscation** - This method is very helpful against keyloggers, because the password is not transferred in one piece, but by several auto-complete methods chosen randomly. For example, the first character might be inserted from the clipboard, the second one via a keyboard simulation and so on. This way, a keylogger would only be able to log parts of the password.

Normally, you will not need to change this information, but if you problems with auto-completion of a website which uses a non standard implementation the problems can be solved by changing the auto-complete method.

Preferred browser

If there are several browsers installed on your computer (e.g. Firefox, Opera), you can connect your password entry with the browsers you wish. This can be helpful if specific websites are only shown correctly with a special browser and if you have not configurated this browser as default browser.

Open URL in private browsing mode

If there are several browsers installed on your computer (e.g. Firefox, Opera), you can connect your password entry with the browsers you wish. This can be helpful if specific websites are only shown correctly with a special browser and if you have not configurated this browser as default browser.

Use second password

You can use a second password with a password entry. This is only useful when using the enterprise server, as you can additionally secure important passwords. Other users can only use this entry if they enter the second password correctly.

Use entry with browser add-ons

Here you can determine whether the chosen log-in data should be filled in automatically via the browser add-ons or not.

Change Second Password

Here you can change or set the second password. If a second password already exists, you must first enter the old password before you can change it.

Update web form data

You can manually update the web form data associated with a password here. This can be useful if the autofill via the addons does not work correctly.

Add/Modify entry - Tab Custom Fields

You can add custom fields to your password entry, by going to the **Custom Fields** tab while adding or editing a password entry.

- Click **Add** to create a new field. In order to do this you have to enter a name for the field and the value which the field should have. If you check the option **Visible in top bar**, this custom field will appear in the top bar and you will be able to insert it from there directly.
- Click **Edit** to change the value or the name of a field.
- Click **Delete** to erase the selected field from the list.
- Use **Move Up** and **Move Down** to change the order of your custom fields.
- If you uncheck the option **Mask Values** you will be able to see the values you entered for each field.

Click **OK** when you are ready.

Add/Modify entry - Tab TANs

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

- **Add:** Click the **Add** button to open the Add TAN dialog box, where you can enter new TANs.
- **Edit:** Click the **Edit** button to open the Edit TAN dialog box for editing existing TANs.

- **Delete:** Deletes all selected TANs after prompting for confirmation.
- **Clear:** Deletes all TANs after prompting for confirmation.
- If you uncheck the option **Mask Values** you will be able to see the values you entered for each TAN.
- **Mark as used:** Sets the status of all selected TANs to "used".
- **Mark as unused:** Sets the status of all selected TANs to "unused".
- **Import:** Allows you to import TANs from a file. The file formats available are CSV, XML, and TAN lists (plain text). The TAN lists format expects a text file containing exactly one TAN per line. Since banks usually 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:** Allows you to export TANs to a file. The formats available are CSV, XML, and TXT.

Add/Edit entry - Tab Attachments

To add an attachment to your password entry, go to the **Attachments** tab when adding or editing a password.

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

Click **OK** when you are ready.

Add/Modify entry - Tab History

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

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

- At **Changes history** you can decide whether you want to keep a history for the according password or not. By default, the global settings you set in the options will be applied.
- 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 history list.
- **Restore** will take the password back to the selected state.

Click **OK** when you are ready.

Importing & Exporting Password Entries

Import/Export Password Entries

The **Import** and **Export** functions (**Tools** tab) allow you to import passwords from a file or to export the current database to a file. These functions are especially useful for the interaction between **Password Depot** and other password managers.

By clicking on the following respective notion, you will find detailed information about **exporting** and **importing** passwords with **Password Depot**.

> **NOTE:** Your database is a very confidential document. Make sure that no other persons gain access to the list. Store the list in a secure location.

Exporting entries

The content of the open database can be exported through **Tools** > **Export**.

Supported Formats

Password files can be exported into the following formats:

- **XML** (Extensible Markup Language)
- **CSV**
- **TXT** (text files)
- **HTML** (Hyper Text Markup Language)
- **PSWX** (***obsolete*** file format used by Password Depot for mobile devices).

In order to export a file into one of the first 4 formats, click on **Tools** > **Export** > **Export Wizard**.

> **WARNING**: The first four file formats (XML, CSV, TXT, HTML) don't support encryption. Anyone who has access to those files, can read their content.

In order to export a file into the PSWX format, click on **Tools** > **Export** > **Export to PSWX**.

> **NOTE**: PSWX files will be encrypted with a master password defined by the user.

How to export

Before you can export the content of the file, you need to authenticate first.

Afterwards you can define the following:

- **Export format**: Select the format in which you want to export the content.
- **Target file**: Click on **Browse** in order define the storage location and the file's name.
- **Original folder**: Select the folder you wish to export from the drop-down menu.

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 tab **Home**.

Supported Import Formats

The software supports following file formats for importing passwords:

- **XML**
- **CSV**
- **Password Depot Format**

Import process

In order to launch the import wizard, you first have to enter your master password. Then, you are asked for following information:

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

Click the **Next** button to continue.

> **NOTE**: In relation to Enterprise Server, the **Import** function may not be executed while you are connected to the server. If you would like to import passwords, please contact the administrator. He/She then has to open the passwords file into which the passwords are to be imported via **Password Depot Client** as a local copy (tab **Local System**). Only on the client, 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.

Import Wizard - CSV File Import

This page is used to adjust parameters for importing passwords from a CSV file.

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

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

If the first line of the CSV dile contains the field description, please check this control box in order to end the import's first line. Subsequently, the depiction in the wizard will be updated.

To continue, click the **Next** button.

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.

If you import passwords into **Password Depot**, however, the import wizard (tab **Tools**) 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 KeeePass

If you want to import KeePass data into **Password Depot,** please first export this data into 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** and choose the exported CSV file.

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 according **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 operation and number of actually processed items.

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 (group **Additional** at the very right), 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; not used and/ or expired entries only unnecessarily overload the program.

There are six options available:

- **Show entires expired before**: Shows all passwords which have expired before the day you have selected.
- **Show entries not used after**: Shows all passwords which have not been used since the day you have selected.
- **Show never-used entries**: Shows all passwords which you have never used since you created them.
- **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.
- **With custom icon**: Shows all passwords which have been customized by the user.
- **With History**: Shows all passwords for which Keep changes history has been previously set.

After you have set the desired filter options, you see all passwords which meet the criteria you have chosen. Additionally, there is corresponding information (e.g., Expiry Date and Frequency of Use) displayed in the list.

For the clean-up of the displayed passwords, four options are available:

- **Delete:** Deletes all passwords which you have selected in the list.
- **Delete Attachments:** Deletes attachments of the selected passwords.

- **Delete History:** Deletes Changes history of the selected passwords.
- **Reset Icon:** Resets the standard icons of the selected passwords.

> **NOTE**: Deleted passwords will be moved to the Recycle bin.

Delete Password Entries

The **Delete** function on the **Home** tab clears both password entries and groups.

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

> **NOTE**: Note that 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 are moved deleted password entries.

You can find the bin in the main view in the group window, the latter being by default placed at the left hand side.

By clicking onto the bin symbol, there opens a new tab with the same name. Under this tab, you will see a list of all deleted entries and have following options:

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

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 passwords file upon quitting the program, you will 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 (on the bar **Passwords**, always visible in the main window) allows you to search for password entries within the currently opened passwords file.

In order to search for an entry, enter a search term into the search field. Password Depot will look for the information while you enter it and display live search results.

Simultaneously to your click into the search field, there opens a new tab called **Search**. This tab allows you to specify detailed search criteria, in view of e.g. description, user name, URL and comments.

NOTE: If you do not have **any information** regarding a certain search criterion, simply leave this field empty. The empty field will not be taken into account by the search algorithm.

NOTE: If you only have **partial information** about one of the search criteria, you can enter this information as well. The search algorithm takes into account any possible matches.

Furthermore, you have following options:

- **Open containing folder**: When you right-click on a search result, you can open the parent folder of it by clicking on this option.
- **New Search**: If you click this button, the last search will be cleared and you are able to start a new one.

- **Exit Seach**: Allows you to exit the present search process.

If you would like to directly work with a found password, e.g. modify it or copy it to the clipboard, simply right click on this password. There will open a list of available actions.

Sort Password Entries

Entries can be sorted by clicking on **View** > **Sort**. See Customize appearance for further information.

Print Password Entries

Password Depot offers the possibility to print out passwords. This function can be found on the **Home** tab.

Before being able to print, you need to enter your master password. This ensures that no unauthorized person is trying to get a print copy of your passwords. Having entered your master password, there opens the print window with three tabs.

Print Preview

The tab at the left shows a **Print Preview** of the list of passwords that is to be printed. Via the blue buttons you can switch between the single pages. By means of the button **Print**, you start the printing process.

Through the **Export to PDF** button you can create a PDF file with your passwords.

Content

On the **Content** tab 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**). Choose a group from the drop down list to select this group and check the option **Include sub-groups** if you want to print any groups included in that group as well. You can uncheck specific passwords if you want to exclude them from being printed.

To get a better overview of the passwords inside the group you can sort them. Use the **Check All** and **Uncheck All** buttons to select all passwords or to remove their selection.

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).

Layout

The print layout of a database can be changed on the **Layout** tab.

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 at the four sides in millimeters.

At the bottom of the dialog, you can change the **font type** and **font size** of the title, of the groups and of the entry lines. Simply click the according box and make your changes in the dialog that opens.

To see the result of the changes you made, you can return to the **Print Preview** tab.

In order to print your passwords, simply click on the **Print** button available on each tab.

> **NOTE:** Your password printout is a very confidential document. Make sure that no other persons gain access to the list and store it in a secure location.

Synchronize Password Entries

The **Synchronize** function at the **Tools** tab can be used to compare two databases and update them, for example if you have a second copy of your file on a USB device or on a server.

First select the file with which you would like to compare the currently opened file and click **Open**. Next you have to enter the master password for the second file.

NOTE: Only files which came from the same source file can be synchronized. Use the **Save as** function in the main menu to save a copy of your database which you can later synchronize with your current file. To combine two totally different files, use the **Import** function on the **Tools** tab.

NOTE: To be able to synchronize it is necessary that both files are from version 6. You can, for example, not synchronize a file from version 4 with one from version 6.

Now you are shown an overview of all differences.

On the left side you see the file with which you are synchronizing your current file. On the right side you have the currently opened one.

To ensure that you can compare the two files you are shown the **size of each file** and the **date of the last changes**.

The entries are divided into three categories: **Not existing entries**, **Different entries** and **Identical entries**.

Next to each password which has been changed you are shown the date of the last modification, so that you can decide which version you would like to use in both files. To be able to see details of the changes, select the according password and right-click it or select View differences on the left bottom.

You can transfer entries from each file to the other or substitute one password with the other. Alternatively, you can erase entries or skip this passwords to change neither one. All these options can be found in the middle between the entries. Select the desired option from the drop-down list.

Then click **Synchronize** to realize all the chosen changes.

Compare Password Entries

To be able to view all differences that two passwords have in the synchronization, have a look at the Differences Report. Here you get a list of differences which helps you to identify all changes.

As 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 go back to the synchronization dialog click **OK**.

Folder Properties

This dialog box allows you to view and edit the properties of a selected folder of password entries.

You can call this window up by right clicking on a folder and then selecting **Properties** in the window that opens.

In the window's upper third, you have following options:

- **Name**: Allows you to modify the folder's name, simply by typing into the field.
- **Change Icon**: Click this button to change the icon that represents the folder in the navigation area. There opens the window Select Image. Here you can either choose from a large number of integrated symbols (tab **Standard**) or select your own icon (tab **Custom**).
- **Reset Icon**: Sets the icon back to its initial state.

In the middle of the window are fields providing additional information about the selected folder:

- **Type**.
- **Location**: Indicates the path to this folder.

  NOTE: The field **Location** is empty if the selected folder is the root directory (i.e. it contains all other folders), as it does not have a path in this case. However, if the selected folder represents a subfolder (i.e. it is within one or several other folders), then the field shows the corresponding path, along the pattern "Root\Subfolder1\Subfolder2\etc.".

- **Contains**: Informs about the folders and passwords contained in the folder, as well as about the number of passwords that have expired.

At the window's lower end are two further fields:

- **Category**: If you like, you can assign a category to the folder. Either you type in a description yourself, or you choose one of the names from the drop-down list.

- **Comments**: Provides space for any text you might like to add, e.g. a description of the folder.

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 **Tools** tab and choose **Categories**.

Use the following command buttons to edit the categories list:

- **Add**: adds a new category to the list.
- **Rename**: Renames a selected category.
- **Delete**: Deletes a selected category.
- **Clear all**: Deletes all categories from the list.
- **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 thsi cas, you can simply save the categories in a file and then load it within a different passwords file, via **Load from file**.
- **Load from file**: Loads categories from a file.

After you have edited the categories, click **OK**.

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

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
Application Restore/Minimize	CTRL + SHIFT + P
Topbar Mode/Minimze	CTRL + SHIFT + T
Open list ...	Ctrl + Alt + O
Save list	Ctrl + S
Save list as ...	Ctrl + Alt + S
Print list ...	Ctrl + P
Backup now	Ctrl + B
Lock	Ctrl + L
Update Manager	Ctrl + Alt + U
Exit	Ctrl + X
Add ...	Ctrl + Ins
Modify ...	Ctrl + M
Delete	Ctrl + Del
Properties ...	Ctrl + I
Copy password to clipboard	F2
Copy user name to clipboard	F3

Copy URL to clipboard	F4
Open URL in Primary Browser ...	F5
Auto completion	F6
Select all	Ctrl + A
Auto-complete sequences	Ctrl + Q
Search ...	Ctrl + F
Top bar	Ctrl + T
Options	F10
Program help	Ctrl + H

Open URL

The **Open URL** function can be found in the Password menu. This function opens a new Web browser session and goes to the URL address of the selected password.

You can always change a password's URL from the Modify password dialog box.

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

Copy Information to Clipboard

The **Copy to clipboard** functions moves information (e.g. password and user name) to the clipboard.

These functions can be found in the Password menu and also in the top bar.

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

- **Password**: Copies the selected password to the clipboard.
- **User name**: Copies the user name of the selected password 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.
- **URL**: Copies the selected password's URL address 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 and select the tab **Clipboard**.

Auto-completion of Web Forms

Browser Add-ons

You can set **Password Depot** to fill in web forms automatically - with your user name, password and any further log-in data. there are two methods to do this:

1. the Auto-complete function (flash symbol in the top bar).
2. the browser add-ons.

In the following you will find more information about the **browser add-ons**. For details on the **Auto-complete** function, please see here.

Explanation of the Browser Add-ons

Add-ons can fill in web forms automatically. Additionally, they can import new log-ins directly into **Password Depot**, so you don't have to create the entry manually.

Browser add-ons are launched together with the browser and come into action after you opened a website containing a log-in. Currently, the software includes add-ons for **Internet Explorer**, **Chrome** and **Firefox**.

If you **do not want to use** the browser add-ons, you can uncheck the browser add-on option in the installer, so they won't be installed. In order to disable already installed browser add-ons, use the browser's settings.

> **NOTE:** The browser add-ons won't work while a dialog (e.g. Modify entry) is opened in Password Depot, if **Password Depot** is closed or locked.

Automatic Completion of Log-ins

If you open a URL that is already saved in one of your password entries and the browser add-ons are enabled, the information (user name, password and other log-in data, if available) will be inserted automatically into corresponding fields.

If the URL you have opened is saved in **several password entries**, the add-on will ask you to select one entry.

You *never* want to log-in automatically to web forms:

1. From the **Home** tab select the button **Options**.
2. In the window that opens select **Browsers**.
3. Uncheck the checkbox **Auto-fill web forms using add-ons**.

You do not want to log-in automatically to *particular* sites:

- Either add the URL(-s) to the list of **Ignored Websites**.
- Or disable the auto-completion for a specific password.
    1. Select the password.
    2. Go to the **Home** tab.
    3. Select the button **Modify**.

4. On the **Additional** tab, check the checkbox **Do not autocomplete this password via the browser add-ons**.

If your log-in information has changed, you can update your **Password Depot** entry after you typed in the new information into the log-in fields.

Automatic Import of new passwords

If you log in to a site not yet contained in **Password Depot**, the program will ask you to save it after you have entered your log-in data.

If you would like to disable this function, please follow these steps:

1. Go to **Home** > **Options**.
2. Select **Browsers**.
3. Uncheck the option **Add new passwords from web browsers**.

> **NOTE**: If the program suggests adding a new entry although there already is an according entry in your database, it is most likely that the URL does not match with the saved one. In this case, add a corresponding URL mask to the respective password entry.

Ignored websites

This dialog shows all websites that are currently ignored by the browser add-ons.

You can open this dialog by going to **Home** > **Properties** > **General**.

- **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.
- **Delete All**: Clears the entire list of ignored websites.
- **Save to File/Load from File**: Saves the ignored website to a file or loads a website from a file.

Auto-completion

You can set Password Depot to automatically fill in web forms for you - with your user name, password and any other eventual log-in data. To do so, there are two options:

1. the **Auto-complete** function (flash symbol in the top bar)
2. the browser add-ons.

Differences in the Auto-complete Methods

Auto-Completion	Browser-Add-ons
Accessed in the program itself (flash symbol in the top bar)	**Separate** modules; accessed via browser
Launched **manually** by user	Launched **automatically**

Process: User clicks on flash symbol (top bar); software fills in the log-in data that is saved for the password entry selected from the list	Process: User opens URL; add-on compares opened URL with URLs saved in the passwords database; if it finds a corresponding URL, it fills in the log-in data linked to this URL
Condition: There is a **auto-complete sequence** saved for the password entry in question	Condition: The opened website is **not ignored** by the add-ons

In the following will be explained the auto-complete function. For details on the browser add-ons, please see here.

Auto-complete Function

To automatically fill in a Web form, please perform following steps:

1. Switch the program into the top bar mode.
2. Select a password from the list.
3. Click the **Auto Complete** button (flash symbol).
4. There opens a window at the top right informing you about the next steps und indicating that the program is now in the **auto complete mode**.
5. Click the first field of the log-in you want to fill out. Now **Password Depot** automatically completes the fields of the window.
6. If you would like to cancel the auto-complete action, click on **Cancel auto-complete mode** in the window that had opened upon your clock on the flash symbol.

> **NOTE:** The **order** in which the data relating to a password is automatically entered can be set in the Auto complete sequences dialog box.

NOTE: The auto-complete function is only active and usable if a password has been selected from the database.

Auto-complete Sequences

An **auto-complete sequence** is the order in which the fields of a Web page will be filled in with your user name, password and other commands (like TAB and ENTER). You can find out the right auto-complete sequence for a password by visiting its URL address and looking for the completion order of user name and password.

The **Auto-complete sequences** function can be accessed in two ways:

- via **Tools** > **Auto-complete sequences**
- in the dialog boxes Add Entry and Modify Entry, in both cases on the **Additional** tab.

The **Auto-complete sequences** window includes the default auto-complete sequence of **Password Depot**. You can add, new sequences and remove or review your old sequences.

- **Add**: Creates a new sequence.
- **Edit**: Modifies the selected sequence.
- **Delete**: Deletes the selected sequence if you do not need it anymore.
- **Clear all**: Removes all custom sequences from your list, leaving only the default sequence.

EXAMPLE: You would like **Password Depot** to fill in automatically a web form that consists of **two web pages**. For instance, on the first web page you enter your client number, on the second page you enter your user name and password.

In this case you would do the following:

1. Create a **custom field** for the client number which you call e.g. "Client Number."
2. Create a corresponding **auto-complete sequence**. To do so, imagine the steps the program has to take:

- First, the software enters the client number (<Client Number>),
- then it 'jumps' to the enter button (<TAB>),
- it presses this button (<ENTER>);
- on the second web page, the program enters the user name (<USER>),
- it 'jump' to the next entry field (<TAB>),
- enters the password (<PASS>),
- finally presses the enter button (<ENTER>).
- This results in the following auto-complete sequence: <Kundennummer><TAB><ENTER><USER><TAB><PASS><ENTER>

Add & Edit Auto-complete Sequences

In the dialog box **Auto-complete Sequences** you can determine the order in which certain commands are carried out.

In order to modify auto-complete sequences, click on the tab **Tools** in the tool bar and then on **Auto-complete sequences**. There opens a window enabling you to **Add** new auto-complete sequences and to **Edit** or **Delete** existing sequences.

If you click on **Add**, you see a list of all actions that are momentarily carried out when you use the auto-complete sequence. In order to generate your own auto-complete, select from the buttons below:

- **CLEAR: Clears the target edit box.**
- **USER**: Adds a username.
- **PASS**: Adds a password.
- **Custom**: You can also use your defined custom fields for auto completion. For more information refer to Add new password.

- **TAB: Jumps to the next input element.**
- **ENTER: Emulates the key "Enter" click.**
- **SPACE**: Emulates the key "Space" click.
- **Additional: Enables to add Arrow buttons, e.g., and Delays** to your sequence which helps fill out dynamic web forms. Simply select DELAY and set the delay's duration.

Once you have added an action, you will see a short description of it.

- **Move Up/Down**: Changes the items' order.
- **Delete**: Removes an action you selected from the list.
- **Clear All**: Deletes the sequence you created, allowing you to start over again.

Having created a correct sequence, click the **OK** button and add your newly created sequence to your list.

Clipboard Monitor Alert

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

Password Depot can 'mask' the changes it makes to the clipboard from other clipboard viewers but it cannot 100% guarantee that your PC is clean from any clipboard monitors. Click the **Protect** button to proceed with 'masking' the changes to the Clipboard. Note, **Password Depot** can detect only certain types of keyboard viewers and cannot replace a full-featured anti-spyware program.

If you are sure that the detected program is safe and eligible to read the data **Password Depot** copies to the Clipboard, click the **Ignore** button, otherwise click **Cancel** and try to find out more about the detected program or process.

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 is thus eligible to read the data which **Password Depot** has put 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 that the program applies the option you have now selected to all future actions.

Passwords

Analyze Passwords

Using the **Passwords Analyzer**, you can analyze your passwords' quality.

To go to this function, select the option **Analyze** from the **Tools** tab.

The dialog window **Passwords Analyzer** consists of four columns:

- **Description**: Shows the passwords contained in the opened passwords file.
- **Strength**: Shows your passwords' strength using the bit unit. The higher the number of bits, the stronger the password.
- **Quality**: This column contains a colored bar indicating the passwords' quality. The longer the bar, the higher the password's quality. The quality of a passwords depends on its length and on whether it contains different characters types. You will achieve the best quality if your password consists of the following characters: lowercase letters, uppercase letters, numbers and special characters.
- **Crack Time**: Indicates how long it would approximately take to crack your passwords, if a professional hacker tried to do so via brute force or dictionary attacks. It is only an approximate value, which is nevertheless calculated with sophisticated algorithms and thus more reliable than many other estimations you will find on the Internet.

If you click on one of the column titles, the passwords will be sorted according to this column's content.

In order to improve the quality of a password, select the corresponding password and click **Edit**, at the bottom left of the window. (This button is inactive as long as no entry is selected.) The Modify Entry dialog box opens where you can modify the password.

Generating Passwords

Password Generator

The **Password Generator** is a tool for creating random passwords.

This tool can be opened in different ways:

- in the dialog fields for adding and modifying password entries, by clicking on the wheel symbol at the right of the field **Confirmation**.
- via the top bar, by clicking on the wheel symbol.

In order to generate a random password, proceed as follows:

1. **Characters used to generate password**: Choose which characters will be used for the password's creation (e.g. lowercase and/or uppercase letters).
2. **Exclude similar-looking characters**: Sets whether the program may use characters that look similar in order to create the password.
3. **Maximum number of password characters**: Limit the maximum number of characters of the final password. Up to 256 characters may be used.
4. To generate the password, now move your mouse cursor across the field below showing random data (in green). Your cursor's movements will select characters randomly and thereby generate a password.
5. **Password**: In this field will be shown the just generated password.
6. **Clear** (rubber symbol at the right of **Password**): Erases the generated password and enables you to create a new one.
7. **Copy to Clipboard** (file symbol at the right of **Password**): If you are content with the generated password, you can copy it directly to the clipboard.
8. **Show/Hide Password** (three dots at the right of **Password**): Displays the password either as 'normal' characters ("show") or as dots ("hide").
9. **OK/Copy to Clipboard**: Click here if you are content with the generated password. The password will then be copied to the clipboard or, if the window for adding/modifyin passwords is opened in the background, directly inserted into the fields **Password** and **Confirmation**.

If you need some more advanced options to be able to generate a very specific password, please refer to the Advanced tab.

Advanced Password Generator

By means of the Advanced Password Generator, you can generate a random password and define exactly what it should consist of. 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 orange wheel symbol. There opens a dialog window 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 passwords template. You can save it under a name you choose by clicking the **Save** button at the right. The next time you create a password, this template will also show in the drop-down list for templates. To delete a template you no longer need, select this template in the list and click the **Delete** button on the right (cross symbol).
- **Default settings for new passwords**: Applies the software's default template for generating passwords.
- **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 takes over the existing entry's settings for this new password.

Password settings

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

- **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 contain only these six characters.

- **Use the following character groups with relative frequencies**: Check all the characters groups which the password should contain, for example Lower case, Numbers and Special characters. Using the slider next to each group you can set a percentage which indicates how frequently the selected character group will be used for the password. At **Custom** you can enter some characters like umlauts 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 group selected above**: Select this option to ensure that at least one character from every group is used for the password. For example: If you select upper case letters, numbers and special characters as groups and check this option, the created password will at least contain one upper case letter, one number and one special character, even if it is only five characters long.

- **Exclude similar-looking characters**: If you check this option, the password will not contain similar-looking characters like for example zero and the letter "O".

- **Excclude consecutive identical characters**: Select this option to avoid that the same character is used twice in a row in the password, for example ZZ.

- **Password length**: Define the number of characters of which the password will consist. You can select a number between five and 256.

- At **Tries to reach maximum password quality** you can define how many passwords the password generator will try to get the best possible result with the settings given. A number between 300 and 500 is normally enough to get a satisfyingly secure password.

Generator:

In this section, the password will be created and the quality rated.

- Click the **Generate** button to create a password with the current settings.

- The **Password quality** is shown graphically on the one hand, but on the other hand there is also an approximate value showing you how long a hacker would need to crack your password. Thus, you will be able to better compare the passwords regarding their security.
- With the buttons next to the password you can copy it to **clipboard** and see what it looks like on plain text.

After having found a password, click **OK**. The password will then automatically be added to the **Password** and **Confirmation** fields.

Partial Password Builder

Password Depot offers a **Partial Password Builder**. To open it, select a password entry from your list and then go to the **Password** tab.

The partial password method is an authentication method for passwords with the purpose to increase the protection against password theft. The method in question asks the user to only insert certain characters of his passwords instead of entering them completely. As there is always only a part of the password shown, this renders it more difficult to find out the password by common 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**: To every character of the chosen symbol the Builder assigns a number; the first character has the number 1.
- **Password**: Here stands your password. If the function **Hide Password** (below) is checked, the password's characters are represented by dots. Else, 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 bottom line, the partial password created by the Builder will be shown, according to the characters you had previously selected in the line above.
- **Hide Password**: If this function is checked, the password's characters are represented by dots. Else, 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 safe and at the same time also easy to remember.

You can launch this generator when creating a new passwords file and then, in the corresponding window, clicking on the button **Create Master Password** (wheel symbol at the right of the field **Master Password**).

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

- **Please enter below...**: Here, you enter a phrase that should contain at least eight words. You can invent the phrase yourself but should be sure to be able to remember it! Having entered your phrase into this field, the button **Generate Password** becomes active. Click on this button in order to make the generator create a password.
- **Generated password**: Shows the password that the password generator has created from the phrase you had entered above.
- **Password quality**: Shows the generated password's quality.
- **Convert phrase using**: You can chose from a number of options concerning lower and upper case letters and the conversion table being used. You also have the possibility to keep the original case letters of your sentence. After all, the most important thing is not only a secure password, but also one you can remember!
- **Template used**: Here, you can see how the initial letters of your original phrase were changed. To understand the meaning of each template element, please refer to the **Template Legend**.
- **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.

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 bother that someone could take a look at your database.

Lock Password Depot

If you lock the program, this moves the application into the tray bar and in this way secures ('locks') it. The **Lock** function can be found at two places:

- in the toolbar on the **Home** tab,
- in the top bar.

Unlock Password Depot

To restore 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**.
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 an "Invalid master password/key file" **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 the **OK** button.

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

USB Installation

The **USB Installation Wizard** (tab **Tools**) 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.

1. **Removable drive**: Select the drive of your storage device.
2. **Copy/update databases**: Having selected a drive, you will see in this window all files stored on the selected device. Check those files that you would like to copy or update.
3. **Update Password Depot configuration file [...]**: If you check this option, your settings for the program will be transferred to the device as well.
4. **Update Autorun.inf [...]**: 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) can't 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 and iOS.

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

To synchronize the file on your mobile phone with the one on the PC again later, transfer your pswd file back to your PC, by using the **Synchronisation** function on the **Tools** tab to detect any differences.

Operating System Android

1. Download the **Password Depot** app for Android via the Android Market and install it.
2. Connect your mobile phone to your computer and transfer the .pswd file to the phone.
3. Start **Password Depot** Androuid Edition and load the file.

Please consult the manual for more information.

Operating System iOS

1. Download the iPhone app via the AppStore and install it.
2. Start iTunes
3. Connect the iPhone, go to the Apps tab and scroll until you reach the File Sharing section. Select the **Password Depot** App and add the database on the right side.
4. Now you can use your database in the iPhone App.

Please consult the manual for more information.

Command Line Parameters

Password Depot supports the following command line parameters:

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

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

-encrypt: File encryption

-decrypt: File decryption

-erase: File erasion

<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 - full paths to all the selected files

Encrypt & Decrypt External Files

Using **Password Depot**, you can easily encrypt or decrypt external files regardless of their fomat. The files will be decrypted with the safe algorithm AES 256-Bit.

You can find the corresponding functions **Encrypt** and **Decrypt** on the tab **Tools**.

Encrypt external files

With the function **Encrypt external files** you can encrypt any files using a password so that no non-authorized person can access your data.

To encrypt your files proceed as follows:

1. From the **Tools** tab select the option **Encrypt**.
2. In the dialog box that opens select the file(s) you wish to encrypt and click **Open**.

3. Enter the password which you will use to decrypt the file later into the **Enter password** field.

4. Repeat the password in the **Confirm password** field.

5. To remove the original file, check the option **Delete original file(s) after encryption**. This option is useful if you wish to encrypt a file that has been accessible for several people and to delete the version which could be accessed by all. The original file is then deleted without any traces from the hard disk thanks to secure algorithms.

6. Select the option **Create a self-extracting archive** if a user which has not installed **Password Depot** on his PC should be able to open it.

7. In case you have chosen more than one file, you can select the option **Create a single output file** to encrypt all files in one file.

8. If you want to save the password for the encrypted file in **Password Depot** check the option **Store password in Password Depot**. To do so you will need to have your database open. In the next dialog, confirm that you want to add the password to your file and it will automatically saved as an encrypted file entry.

9. Click **OK** to encrypt the file(s).

Decrypt external files

With the function **Decrypt external files** you can decrypt any encrypted files if you have a valid password.

To decrypt files proceed as follows:

1. From the **Tools** tab select the option **Decrypt external files**.

2. In the dialog box that opens select the encrypted file (*.pwde) which you wish to decrypt.

3. Click **Open**.

4. Enter the corresponding password of the file into the **Password Depot - Encrypt** dialog box.

5. To remove the encrypted file afterwards, check the option **Delete encrypted files after decryption** if you no longer need it.

6. Click **OK** to decrypt the file.

Erase External Files

Using **Password Depot**, you can erase external files from your hard disk, regardless of their format. This erased file cannot be restored even by specialized programs as it will be overwritten several times.

To erase files, follow these steps:

1. From the **Tools** tab select the option **Erase**.

2. In the dialog box that opens select the file you wish to erase.

3. Click **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 **Yes**.

Global Custom Fields

The **Global Custom Fields** function on the **Tools** tab provides often-used information, such as email addresses or nick names, and thus saves the trouble of having to enter them anew for every password.

- **Add**: Opens the window **Edit Custom Field** for creating a new global field (see below).

- **Edit**: Allows to change an existing field.

- **Delete**: Eemoves a selected global field from the list.

- **Mask values**: If checked, hides the content of the fields in the list. If unchecked, allows to see the fields' contents.

Click **OK** once you have completed all the desired changes.

Edit Custom Field

If you click on the **Add** button in the **Global fields** window, a new window opens in which you can edit the global fields.

- **Name**: Enter a meaningful title for the field. You can either write a name yourself or select a name from the drop down menu, e.g. "Address" or "Birth Date."
- **Value**: Enter the value you would like to have for the field you are editing.

> **EXAMPLE**:
> Name: Email address
> Value: info@example.com

- **Visible in top bar**: Check this option if you would like this custom field to be displayed in the top bar.

Customize Password Depot

Customize Browsers

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

To add a browser, proceed as follows:

1. Open the tab **File** > **Options** > **Browser** > **Custom Browsers**.
2. In the window that opens, click **Add**.
3. Select a **Description** for this browser.
4. Below, you can select the **Path to the .exe file** by clicking **Browse** on the right side.
5. Confirm your new browser with **OK** then.

You can always change an existing browser via **Edit** or use **Delete** to remove it from the list.

Customize Icons

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

To open this dialog, call up the properties of the password (via Modify Entry) or group 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 you *own* icons (**Custom** tab).

> **NOTE**: If you have opened a file from **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 **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:

- **Add**: 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.
- **Delete**: Deletes a selected icon from the list.
- **Clear**: Deletes all icons from the list.

In the drop-down list **View Size**, you can decide about the size of the custom icons: whether they should be displayed in **large** or **small** size.

Customize Appearance

Password Depot has a very flexible interface that can be modified in the **View** tab according to your requirements:

Areas

Here you set up the general appearance by choosing which areas of the main window should be displayed.

You can choose from five areas: **Passwords**, **Navigation Area**, **Files from Server**, **Details** and a **Toolbar**.

Passwords

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

This windows provides access to your passwords, showing all the passwords from the selected **folder**.

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 in the in the **View** tab.
- In order to edit password entries, switch to the **Home** tab. Here 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. Over this menu you can:

- **modify**, **delete** or **print** the selected password(s),
- **cut**, **copy**, **insert** and **duplicate** the entry or add it to your favorites list,
- copy the password's information to the **clipboard**,
- create a **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 **Passwords** window, you can also move passwords from one group to another. Just select the passwords you want to move and then drag & drop them into the desired group.

Navigation area

This area provides a tree 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.

If you are using **Enterprise Server** you can quickly access the files from the server here as well. To display the files in this area, click on **Navigation Area** and activate the option **Files on Server**. The files on the server are only displayed if you are connected to the server.

Details

This window is situated on the right side of the screen. Its purpose is to display the information about a selected password in a more compact space, so that it is easier to read.

Toolbar

Displays a toolbar on the top of the passwords area. Through this toolbar you have quick access to the most important password functions.

View

Here you can choose how your entries are displayed, e.g. as a **List**, **Symbols** or **Icons**.

Arrange

Sort

Here you can choose how the password entries are sorted, e.g. by their **Description** or **Importance**.

Direction

Here you can decide if the sort order should be **Ascending** or **Descending**.

Grouping

Here you can choose if the entries should be grouped. They can be grouped by their **Type** or **Category**.

Program Options

Program Options

In the **Options** dialog you can configure important program features individually. To open the **Options** dialog select it from the quick access toolbar or click F10.

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

- General
- Actions
- Top bar
- Passwords
- Save
- Clipboard
- Layout
- Network
- Browsers
- Warnings

At the bottom left of each tab, you will find the possibility to **Restore the 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 accesses via the respective file's Properties.

> **NOTE**: The Freeware version can be used only in the Beginner Mode. This means that only a limited number of settings can be changed in the freeware. The full scope of settings is available only in the Expert Mode of the Trial- and the Professional version.

Options - General

In the program's Options, the tab **General** allows to modify the program's start and its hot keys.

User interface

- **Language:** Here you can select the language of the user interface.
- **Theme:** Here you can select one of the predefined themes (skins), which will change the design of the user interface.

Program Start

- **Start mode:** From the drop down list, how **Password Depot** will be started: In a normal window, minimized to tray, in 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 systray.
- **Launch application on Windows startup:** Activate this option if you wish to start the program when you start Windows.
- **Open last used database at program start**: Activate this option to the same database as last time when starting the program.
- **Store lists of recent files**: Check this option and the program will save a list of files which you have used recently. You can see your recently used files in the main menu and on the **Most Recently Used** tab when opening a file.

System-wide Hot Keys

- **Restore/Minimze**: The key combination which will automatically bring **Password Depot** to the screen if it is minimized or in the system tray and which will minimize the program if it is currently in focus. By default, the hot key is `CTRL`+`SHIFT`+`P`.
- **Top Bar/Minimize**: The key combination which will switch **Password Depot** to the top bar mode or minimize the program from the top bar. By default, the hot key is `CTRL`+`SHIFT`+`T`.

You can change both hot keys by clicking into the according field. Then click the key kombination which you would like to use instead.

Options -Actions

In the program's Options, the tab **Actions** allows for the following settings:

Auto-complete

> **NOTE**: These options refer to the normal auto-completion only (via F6 or the flash symbol). It does NOT refer to auto-completion by means of the browser add-ons.

- **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 according button **Open URL** from the top bar or manually.
- **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.

Double-click Actions

- **Action # 1**: Select the option which you want to be taken if you double-click on a password in your file.
- **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**: Here you can define after which period of non-using the program the auto-minimize function should be activated. Select this option and specify the desired time period in minutes and seconds. To additionally lock the program when it is not used, activate the option Close passwords file 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 when you click the Close button.

Close passwords file and lock program

- **When the computer is idle for**: Here you can define after which period of not using the computer the auto-minimize function should be activated. Select this option and specify the desired time period in minutes and seconds.
- **When the current user (session) changes**: The program is automatically minimized and locked when the active desktop user or terminal session changes.
- **When the computer enters Standby/Hibernate mode**: The program is automatically minimized and locked when the computer goes into standby or hibernate mode.
- **When the program is auto-minimized**: If you select this option, the program is locked automatically when it is auto-minimized.
- **Always when program is minimized**: If you select this option the program is locked automatically when it is minimized.

Options - Top Bar

In the program's Options, the tab **Top bar** allows to make settings regarding the position and appearance of the **Password Depot**'s top bar 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.
- **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.

- **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 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 dropdown list allows you to define on which monitor the top bar is to be displayed.

Appearance

- **Use theme colors**: If this option is activated, the top bar appears in light-grey, and the bar's symbols are colored in blue and yellow.

- **Custom color gradient**: 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 offered by the software are not enough for you, you can click on **Select** in the drop-down list and will then have a broader color choice.

- **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.**

- **Width of drop-down lists:**

- **Customize Buttons: Click this button to select the buttons you want to have in the topbar and to put them in the order you want to have. Learn more.**

- **Large/Small icons:**
- **Show server file selector: Dieses Kontrollfeld hat nur Auswirkungen, wenn Sie mit Enterprise Server verbunden ist. Ist es aktiviert, so erscheint in der Top-Leiste ein Dropdown-Feld, aus welchem Sie eine Datei auswählen können, welche Ihnen Ihr Administrator auf dem Server zugewiesen hat.**
- **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.**
- **length of drop-down lists:**

Options - Customize Top Bar

In order to call up the dialog for modifying the top bar, there are two possibilities:

- Open the program's options, click on the **Top Bar** tab and then onto the button **Customize buttons...** .
- 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; on the right are all buttons that currently appear in the top bar.

You are now able to make 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 in the right list.
- **Remove**: To remove an item from the topbar, select this item in the right list and click on **<-Remove**. The selected button will now be cleared from the right list and instead appear in 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 in 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.

Options - Passwords

In the program's Options, the tab **Passwords** allows to modify the settings of your saved passwords.

Editing

- **Default auto-complete method:**
- **Default auto-complete sequence:**
- **Default expiration period for passwords**: You can define a period here 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 **Modify** and change the according option on the **General** tab.
- **Show warning for expired passwords**: If you check this option you will receive a warning by the program when any passwords have expired. If you check it you can set the number of days which you will be shown a warning before the password expires.
- **Hide expired passwords**: Use this option if you don't want to be shown expired passwords.
- **Warn about identical passwords for different URLs**: If this option is checked, the software will issue a warning when you add a password entry that matches an already existing entry (same user name, password and URL).

Password Analyzer

Password Depot automatically analyzes new passwords, e.g. when you add a password entry. Additionally, the sofware shows how long it would approximately take to crack this password. This analysis is based on a standard value of three billion calculations per second, which corresponds to the power of a high-performance computer.

You can either leave the setting to **Default** or you can choose **Custom** in order to set your own values. In doing so, you can determien how many work stations are used by the imagined attacker and how many calculations per second can be executed by his/her work stations. In accordance with your specifications, the estimated value for cracking the password changes.

> **NOTE:** As a rough guideline you can say that one could crack about one million passwords per second using a regular PC. This means that the calculations supposed by **Password Depot** really would be performed by a high-performance computer. It is not to be assumed that a 'normal' user would invest the criminal energy and the time in order to crack passwords by means of brute force attacks or dictionary attacks.

Options - Save

In the program's Options, the tab **Save** allows to determine e.g. how often the passwords file and backup copies are saved.

Save passwords

- **For every change**: If you activate this option, any change to your database will be saved automatically. This improves the safety of your data.
- **On selection from the menu:** Your database will be saved when you exit the program. If you are not concerned about data safety, activate this option.

Backup passwords

- **When database is opened**: If you select this option, you will have to select the **Backup** function from main menu to create backups.

- **When file is saved:** If you select this option, a backup copy of your database will be created each time you select **Save list** or **Save list as** from the **File** menu. Below, you can also specify how many backup copies you would like to have all in all.

Remote files

Here, you can define if the local copy of your database should be deleted after you have finished working with files from an Internet server.

Working directories

Here you can modify the directories of your database and of the backup copies. To do so, click on one of the buttons at the right of the corresponding field (**...**) and select a new directory.

Options - Clipboard

In the program's Options, the tab **Clipboard** allows to configure the program's actions in relation to the clipboard.

Clipboard

- **Copy password to clipboard**: You can define for passwords to be copied to the clipboard either **On mouse click** or **On selection from the menu** by activating the corresponding option.
- **Delete password from clipboard after**: You can define the number of minutes after which the password is going to be deleted from clipboard. This function helps you to prevent passwords from staying in the clipboard by mistake. You can also enter a value below 1.

Monitoring

- **Activate clipboard monitor alert:** Activate this option if **Password Depot** should check before using the clipboard whether other applications are reading the clipboard and might intercept secret passwords.

- **List of trusted clipboard viewers**: Here you can enter trusted applications to avoid that these applications cause a warning message when they access the clipboard. You can also add applications to this list via the dialog box Clipboard monitor alert after an alarm has been set off.

Options - Layout

In the program's Options, the tab **Layout** allows to select the fields that will be displayed in the main window. Simply check all of the elements you would like to be displayed.

Options - Network

In the program's Options, the tab **Network** allows to set the options regarding your prxy server and the server module of **Password Depot**.

Enterprise Server

- **Automatically reconnect on network errors**: If you check this option, the software will automatically try to reestablish a connection after errors regarding the network connection.
- **Reconnect interval**: Here you can set the temporal distance (in seconds) between the automatic attempts at reconnection.
- **Reconnect attempts**: Allows you to set how often the program should try to reestablish a connection.

SSL/TLS Settings

If your administrator installed a certificate for the Enterprise Server, you can here define the settings for the SSL/TSL connection to the server.

Options - Browsers

In the program's Options, the tab **Browsers** allows to make set different options regarding the standard browsers and the browser add-ons.

Internet Browsers

- **Default browser (F5)**: 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 in 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 flash 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 (given that 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.

> **NOTE**: All options regarding the browser add-ons only refer to the three browsers **Internet Explorer, Chrome** and **Firefox**, as only these three browsers offer add-ons at the moment.

Add-ons online

Here you will find the links for installing the add-ons.

Options - Warnings

On the **Warnings** tab of the program options you can define which warnings you want to see and which you want to ignore. Thus, you can decide for yourself which warnings are helpful to you.

Uncheck all the warnings which you no longer want to see.

Click **Check all** to activate all the available warnings.

Click **Uncheck all** to disable all the warnings shown.

User Modes

Mode

In **Password Depot** you can choose from three different modes. The mode you choose determines the functionalities that will be available.

In order to change the mode, select the **Home** tab and click on the **Mode** button.

You can now select one of three modes:

- Expert Mode (available only in the trial and professional version)
- Beginner Mode
- Custom Mode

Additionally, here you can change the settings for the **Custom Mode** by clicking Edit Custom Mode.

Expert Mode

In **Password Depot** you can choose from three different modes. The mode you choose determines the functions that will be available.

In order 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 can not be used in the Beginner Mode. Due to its full scope of functions, the Expert Mode is especially apt for users who know the program very well and intend to use all of its functions.

In order to use only the program's basic functions, choose the Beginner Mode. In order to determine yourself which functions you would like to use, choose the Custom Mode.

> **NOTE**: The freeware version can be used only in the **Beginner Mode**. In order to switch to the **Expert Mode** with additional functions and settings, Password Depot must be unlocked.

Beginner Mode

In **Password Depot** you can choose from three different modes. The mode you choose determines the functions that will be available.

In order to change the mode, click on **View > Mode**.

In the **Beginner Mode**, only the **most important** and **most simple** functions of the program are available. Any advanced functions (like Synchronisation, Clean-Up, TANs etc.) are disabled and only available in the Expert Mode and Custom Mode. Due to its restricted functions, the Beginner Mode is especially apt 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.

In order to use all functions offered by the program, switch to the Expert Mode. In order to determine yourself which functions you would like to use, choose the Custom Mode.

> **NOTE**: The freeware version can be used only in the **Beginner Mode**. In order to switch to the **Expert Mode** with additional functions and settings, Password Depot must be unlocked.

Options

The following **Options** (F10) are available in the **Beginner Mode**:

User interface

- **Language:** Here you can select the language of the user interface.
- **Theme:** Here you can select one of the predefined themes (skins), which will change the design of the user interface.

Browsers

- **Default browser (F5)**: 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 in 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 flash 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 (given that 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.

> **NOTE**: All options regarding the browser add-ons only refer to the three browsers **Internet Explorer, Chrome** and **Firefox**, as only these three browsers offer add-ons at the moment.

Display

Here you can select the fields that will be displayed in the main window. Simply check all of the elements you would like to be displayed.

Monitoring

- **Activate clipboard monitor alert:** Activate this option if **Password Depot** should check before using the clipboard whether other applications are reading the clipboard and might intercept secret passwords.
- **List of trusted clipboard viewers**: Here you can enter trusted applications to avoid that these applications cause a warning message when they access the clipboard. You can also add applications to this list via the dialog box Clipboard monitor alert after an alarm has been set off.

Custom Mode

In **Password Depot** you can choose from three different modes. The mode you choose determines the functions that will be available.

In order to change the mode, click on **View > Mode**.

In the **Custom Mode**, you can choose yourself 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 the program does not need in order to work properly. Functions that can be deactivated comprise e.g. synchronization and decryption. Due to its personally defined scope of functions, the Custom Mode is especially apt for users who know the program very well and exactly know which functions they need.

In order to use all functions offered by the program, switch to the Expert Mode. In order to use only the program's basic functions, choose the Beginner Mode.

Edit Custom Mode

In **Password Depot** you can choose from three different modes. The mode you choose determines the functions that will be available.

If you want to determine yourself which functions of **Password Depot** you would like to use and which you do not need, you can 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**. On the left side, you see a number of **categories** into which the functions which you can enable or disable are split. If you select a category on the left, you will be shown the according functions on the right side. Remove the check mark if you do not want to use a function in your customized mode.

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 synchronization or encryption of external files.

Click **OK** to save your changes.

Support

Technical Support

AceBIT GmbH provides customers with high quality support and assistance. If you encounter a problem, or have a question or need any other help with our products and solutions, here are a some ways to get an answer or find a solution:

- Consult the product's User Manual.
- Visit the Password Depot website for updated information.
- Information on Enterprise Server you will find on the corresponding product website.
- Visit our Support-Center. Here you can:
- 1.) read articles in the **Knowledgebase** (FAQ),
- 2.) consult our **forum** and either read about problems experienced by other users or create your own thread,
- 3.) send us a **message**. On weekdays, emails are normally answered within 48 hours.

To provide the answers you need quickly and efficiently, the support staff needs some information about your computer and your software:

- Program name and version number (to be found in the **Help->Info** dialog box of the main menu),
- Operating system and version number,
- Used browser(-s).

Contacting AceBIT GmbH

Click here if you have ordered one of our software products and wish to **view your order data**. Do you have any queries regarding the ordering process, payment or delivery? Please contact our Customer Service to find out more.

You would like to order **Password Depot**? Please click here, and you will be redirected to the order page for Password Depot Version.

If you have **technical queries or problems** in relation to one of our software products, please visit our Help Desk.

For journalists and editors, we offer a special Press Service.

Address: AceBIT GmbH
Holzhofallee 15
D-64295 Darmstadt

- Germany -

Phone*: +49 61 51 136 50-0

Fax: +49 61 51 136 50-20

Email: info@acebit.de

* Note: You can contact us by phone from 9 a.m. until 5 p.m (CET). We do not offer support by phone. We **only** deal with support inquiries via our Help Desk or our forum.

Inquiries will be answered within 48 hours on working days.

FAQs

On the product website you can find an overview of frequently asked questions on **Password Depot** with suggested solutions.

Please click here to open the FAQ section ("Knowledgebase").

If your question is not answered there, but you need a fast answer, please also visit the forum.

License Agreement

This License Agreement and Limited Warranty constitute a legally binding agreement (hereafter referred to as the "License Agreement") between you (as an individual person or organization) and AceBIT GmbH (hereafter referred to as "AceBIT") as regards the use of the software product Password Depot (hereafter referred to as the "Software"), including other software, media and accompanying documentation made available in electronic or printed form.

BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEEMENT.

The terms under which you as the end user (hereafter referred to as the "licensee") are permitted to use AceBIT software are explained below. By installing the software, you agree to be bound by these terms. It is therefore important that you carefully read the text below. If you do not agree with these terms, you may not install the Software. In this case, promptly return the Software to the place from which you obtained it for a full refund.

Terms of the License Agreement

1. Subject matter of agreement

(1) Subject matter of this agreement shall be the permanent handing over of the software product Password Depot in the object code including the complete documentation (hereafter collectively referred to as "Software") as well as granting rights of use in accordance with §2.

(2) AceBIT wishes to emphasize that, given to the current state of technology, it is not possible to create computer software that works properly in all applications and possible combinations with other software products. This License Agreement therefore covers only Software that is in principle considered to be useable in accordance with the program description and user manual. Any warranties or procurement obligations shall only be valid if they were explicitly designated as such.

2. Use of Software

(1) With registration the licensee is granted a non-exclusive right of use for the Software that is unlimited in time. The maximum number of persons to use the Software at the same time shall not exceed the number of licenses originally ordered by the licensee. Admissible use of the Software comprises installation, loading it to the main memory of the computer as well as proper use of the Software by the licensee. Under no circumstances the licensee may rent or provide any sub-licenses of the purchased Software to third parties, present the software publicly via wired or wireless communication means or make the Software available to third parties gratuitously or for a consideration, as for example Application Service Providing or "Software as Service". Sub-point 4 shall remain unaffected.

(2) The licensee is entitled to create a security copy if necessary to secure future use of the Software. The licensee shall explicitly label this security copy as such with "Security Copy" and a corresponding copyright notice of the manufacturer.

(3) The licensee is entitled to decompile and copy the Software where this becomes necessary to secure the interoperation with other programs. This shall only apply if AceBIT on request did not provide the licensee with all necessary information within an appropriate period of time.

(4) The licensee is entitled to permanently hand over the purchased copy of the Software as well as the complete documentation to a third party. By doing so, the licensee agrees to completely give up the right of use for the Software, to delete all installed copies from his computer(s) as well as copies on any other data storage device or to return all copies to AceBIT, provided that the licensee is not legally obliged to store the copies for a certain period of time. At AceBIT`s explicit request the licensee is obliged to confirm in written form that the mentioned measures have been carried out or if necessary to state reasons for a longer period of storage. Furthermore the licensee and the third party shall explicitly agree on the observance of rights of use in accordance with §2.

(5) If the licensee uses the Software to such an extent that the rights of use obtained with purchase are exceeded qualitatively (with regard to proper use) or quantitatively (with regard to the number of purchased licenses), he shall immediately purchase the necessary rights of use. If the licensee fails to do so, AceBIT is entitled to assert her rights in accordance with this agreement.

3. Registration

(1) In order to use the Software, the licensee must register with AceBIT. Registration is completed automatically by means of an e-mail message generated by the Software and sent to AceBIT, containing the entered personal details (name, company, postal address, e-mail address, telephone number) of the licensee. After receipt of this e-mail message, AceBIT will send a confirmation e-mail to the licensee.

(2) The personal details mentioned above are stored electronically by AceBIT for internal purposes and are not made available to third parties. By installing the Software, the licensee agrees to the dispatch of contact details and the subsequent storage of this data by AceBIT. AceBIT reserves the right not to grant users rights, if incorrect personal details were submitted upon registration.

4. Ownership of Rights

(1) By purchasing the Software the licensee only becomes owner of the physical data storage device on which the Software or relevant files are stored. Purchasing the product does not imply any further property rights on the Software for the licensee.

(2) AceBIT preserves all rights, including publishing rights, copyrights, adaptation rights as well as exploitation rights for the Software.

5. Warranty

(1) AceBIT guarantees for the agreed quality of the Software and that the licensee is entitled to use the Software without violating rights of third parties. Warranty of quality shall not be applied if a defect results from improper use of the Software or using the Software on systems that do not fulfill the stated system requirements.

(2) If the licensee is an employer, he is obliged to check the Software for obvious defects immediately upon receipt and if provided to communicate the defect immediately to AceBIT, otherwise those defects shall not be covered by warranty. The same applies to any defects that are claimed later. §377 HGB shall be applied.

(3) If the licensee is an employer, AceBIT is entitled to provide supplementary performance in case of any material deficiency, i.e. at AceBIT`s choice remedy of defects ("repair") or substitute delivery. If necessary the licensee shall be provided with an updated version of the Software in the content of substitute delivery, provided that does not imply unreasonable restrictions. In case of deficiencies in title, AceBIT shall give the licensee a legally indisputable opportunity to use the Software or shall make appropriate amendments that rights of third parties will no longer be violated.

(4) AceBIT is entitled to provide warranty in the premises of the licensee. AceBIT carries out its duty of "repair" by providing automatically installing updates for free download from the company`s website or by offering technical support via telephone or email in case of any other problem occurring during the installation procedure.

(5) The licensee`s right of withdrawal or right to reduce the purchase price after the remedy of defect or substitute delivery has failed two times remains unaffected. Right of withdrawal is not applicable in case of insignificant defects. If the licensee claims compensation for damages or futile expenditures, AceBIT is liable according to §6.

(6) If the licensee is a consumer, statutory warranty regulations shall be applied.

(7) With the exception of claim for damages any warranty claim because of material deficiency becomes statute-barred within two years or within one year, if no consumer is involved in the transaction. Statutory limitation shall begin in case of a sale on a data storage device with delivery of the software, in case of a download after installation and provision of unlock data or rather with the provision of access data for the download area. Claims for compensation or compensation for futile expenditures are applicable according to §6.

6. Liability

(1) AceBIT shall be liable

- in case of intent and gross-negligence

- in case of injury of life, body or health

- according to the German Product Liability Act

- within the scope of warranty

(2) In case of slightly negligent violation of contractual duties that are of considerable importance for the fulfillment of the contract (cardinal obligation), liability of AceBIT is limited in amount to the damage that is foreseeable and expectable for this kind of business.

(3) Any further liability of AceBIT shall be excluded.

(4) Preceding limitation of liability shall also apply to personal liability of AceBIT employees, representatives and bodies of the company.

7. Miscellaneous

(1) The licensee shall transfer any claims against AceBIT to third parties only after written consent of the same. §2 sub-point 4 remains unaffected.

(2) The customer may only offset against claims that are undisputed or which have been determined as legally valid.

(3) All changes and amendments to this agreement shall be valid only if made in writing.

This shall also apply to amendments or the suspension of this clause. Electronic documents in shape of text matter do not fulfill the requirements of the written form.

(4) General terms and conditions of the customer shall not be applicable.

(5) The contractual Software may be subject to (re-)export restrictions, e.g. from the United States of America or the European Union. The customer is obliged to act according to these regulations in case of resale or any other exportation.

(6) For this contract the law of the Federal Republic of Germany applies to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods of 11 April 1980.

(7) Sole place of performance is the company seat Darmstadt. Provided that each contractual party is trader, legal person or without general place of jurisdiction, sole place of legal venue for all disputes among the parties arising out of and in relation to this agreement is the company seat Darmstadt.

(8) If any provision of this sales contract is or becomes ineffective or impracticable or if there is a loophole in this contract, this does not affect the effectiveness or enforceability of all other provisions. The contracting parties shall endeavor to find, in lieu of the ineffective provision, an effective one that comes as close as possible to having the economic significance of the ineffective one.

If you have any questions concerning this License Agreement, please write to: AceBIT GmbH, Holzhofallee 15, D-64295 Darmstadt, info@acebit.de

Index