Password Agent

User's Manual

Revision 2019.6.27

Contents

Introduction

Description

Password Agent is a powerful yet compact and easy to use password manager program that allows you to store all your passwords and data snippets in a single, easy to navigate and secure database. It is not limited to storing only passwords – you can store any information you want, like key codes and serial number of purchased software programs, bank account numbers, credit card numbers, membership numbers etc. Storing all your useful information in one secure place makes it very easy to find it when required and you can also backup all this data at once just by copying single small data file.

Main idea of the program is to protect all your sensitive information with one master password – you need to remember only one password. That makes it possible to use strong random passwords like *SJocLSj4DXW0fGH* for all your web site accounts, as you don't need to remember each and every password any more. You just need to remember one master password which allows you to open your password database and then you can use special functionality of *Password Agent* which allows you to log into your web sites semi-automatically, by pressing a global hot key on login pages.

***Password Agent* stores all your sensitive data locally, in your computer, not in the internet "cloud".** While service providers push cloud storage as solution for all data storage issues (of course, they can charge monthly fee that way, plus they can also track your online behavior and re-sell that information for more gains!) and it is true that internet storage allows very convenient data access from different devices, you need to keep in mind that **cloud storage is not good location for your sensitive data like passwords.** *"There is no cloud. It's just someone else's computer"* – and that is not a joke! With *Password Agent* you are master of your secrets, not someone else.

In addition to storing data securely, *Password Agent* will also help you to **automate your web site logins without needing any separate web browser plug-ins**. See "Automatically filling login forms" on page 26.

Password Agent was designed with security in mind from ground up. While most password managers you can download from the internet focus mainly on encrypting your data on disk, ***Password Agent* uses secure plain text handling also for all in-memory operations**. Data is always kept in memory fully encrypted. In addition, in normal viewing and browsing mode **there is no moment in time where all fields of an item are decrypted into plain text at the same time**. Item fields are decrypted one by one only when needed to be drawn on screen, after drawing plain text is immediately "burned". Whenever possible plain text is not passed to *Windows API*. All that minimizes possibility of plain text leaks to memory and scratch disk. If you consider all this additional behind the scenes overhead, performance of *Password Agent* user interface is excellent. Also, **native 64-bit version makes use of additional security offered by 64-bit Windows.**

***Password Agent* uses only strong, standardized and U.S. government accepted cryptographic primitives** like PBKDF2 with SHA2-256 for key derivation, AES (or optionally Twofish) for encryption.

Your textual data is stored in UTF-8 character encoding, which means **most world languages and international characters are supported**.

Password Agent is a valuable tool for system administrators who need to maintain bigger databases of users. One can easily store thousands of items in one data file and **tabbed interface allows opening of multiple data files at time**. That makes it easy to **move data from one file to another securely** – copy and paste between files is fully secure (no sensitive plain text is copied to clipboard). **Multiple users can also access same file simultaneously over network**, although only the first user gets read/write access (others get only read access).

Password Agent does not lock you away from your data. You can **export all your data from *Password Agent* to common XML or CSV format any time** you need to migrate to some other password manager.

Password Agent is a self contained program, **no special installation nor external framework dependencies are needed**. That also means you can just start it directly off removable drive, like USB flash drive, making is very portable. You can also share it easily on file server without need of local installation on client computers.

What's new in version 2016

This new version is completely re-written and contains many changes, of which only major ones are listed here. Version 2 was released in 2002, so it has offered you solid service for 14 years! Not many software packages offer such long service.

Starting with this release I'll use new approach to releasing updates. There will be no more major updates like jump from version 2 to 3 – both small and big updates will be released as more frequent updates. That also makes moving from one version to the next less painless as there are less changes between versions. Your license includes 365 days of free updates, so you'll get any updates, small and big for one year.

Major new features in version 2016 (for additional detailed list of smaller changes see **Help | Changes log**):

- **Improved security**. Data is kept in memory fully encrypted, like as on disk (in version 2 data was scrambled in memory but not encrypted). During normal viewing/browsing mode there is no moment in time where multiple fields of item are decrypted into plain at the same time. That minimizes possibility of plain text leak via memory dump or swap file. Item fields are decrypted one at a time only when needed to be drawn on screen. The same also in item details panel. Instead of putting all fields into edit mode at the same time, you can now only edit one field at time. That may first seem uncomfortable but is much more secure as if you capture program memory at time of editing item fields, you can possibly only capture contents of one decrypted field being edited, not all fields of the item.
  For key derivation PBKDF2 with SHA2-256 is used, the old version did not use key stretching. Now you can also switch to alternative Twofish encryption cipher if desired. File contents is now authenticated before decrypting to detect file tampering and corruption. In addition, a serious bug in implementation of encryption was found in code base of version 2. That bug reduces security of files saved with version 2.
  For all the reasons listed above it is highly recommended to migrate to version 3 of *Password Agent*. This is critical security update for anyone using any older version.
- **Full Unicode application**. Now all text fields are support Unicode character encoding, so text can be in any language.
- **Autofill matching item**. New *Autofill matching item* function can detect link from current web browser window, automatically find corresponding item and autofill from it. There is no need to first select the item to autofill from in *Password Agent*. You can work in web browser and when you need to login, just press global *Autofill matching item* shortcut key and voila, *Password Agent* that runs on the background retrieves current link from web browser, finds matching item in your data file and sends autofill text to browser. No web browser plug-ins are used. See topic “Autofill matching item (new in version 2016)” on page 26.
- **Two different fully user customizable item list views**. Each view can display 1-3 lines of text about each item. If you liked compact 1-line item list view of version 2 more than the new default 2-line view in version 3 then you can press *Alternative view* button on toolbar to change view. To customize current view further choose **View | Customize**.
- You can now **open multiple files simultaneously**. If more than one file is open you see tab for each file to switch between files. You can also switch to different file from keyboard by pressing [Ctrl]+[1..9]. If more than one file is open then autofill function fills from currently selected file. You can copy and paste items and groups between files in fully secure manner, no plain text is stored in clipboard during such operations.
- New **password generator with policies**. Uses cryptographically secure random number generator. You can create named policies which are saved inside data file.
- Now you can **attach external files to items**. That is meant for adding only small files like license or key files and not for encrypting external large files like photos, because all attachments are always kept in memory and are embedded in data file.

- **Template items**. Items in *Templates* folder can be used as templates for new items. When you create new item based on template then all properties of template item are inherited. New item is a copy of template item, except title. See topic “Template items” on page 20.
- Now you can choose from **hundreds of item icons**, plus you can also change icon background color for each item separately. To change item icon first display item properties (double-click item) and then press button that displays item icon.
- **Item list allows selecting multiple items at time**, so you can select multiple items to copy, move, delete, print etc.
- To offer better portability, **program settings are stored in .INI file** instead of registry. Settings are stored in user's roaming profile in *%APPDATA%\Moon Software\Password Agent* folder.
- **Native 64-bit version** is also included.
- **Support for high DPI monitors (200+ DPI)**.

Lite vs. Unlimited edition

Password Agent comes in two editions – free *Lite* edition and paid *Unlimited* edition. The *Lite* version can be considered free demo version, it is free to use in both private and commercial environments but there are few limitations:

1. *Lite* edition can store up to 20 entries per file. The *Unlimited* version can store virtually an unlimited number of entries per file.
2. *Lite* edition can unlock only 1 file at a time. *Unlimited* edition allows simultaneous opening of multiple files, each file is opened on a different tab, so you can switch between multiple unlocked files and copy/move data between these.

Physically both *Lite* and *Unlimited* editions are the same program and installed from same installer. Once you purchase a license to use the *Unlimited* edition you'll receive your personal license key code. You'll then need to enter this key code into installed free *Lite* edition to turn it into *Unlimited* edition. See “Entering a license key” on page 42.

Privacy

***Password Agent* has no built-in functions that can contact us without your knowledge or send any of your information to us without your knowledge**. *Check for Update* functionality that can be used to check if there is a new version of the program available may send name of the program, major, minor and build numbers and your license key code (not your master password) to our server. **In no circumstances will *Password Agent* send us your data file or any of your secret data stored in data files.**

If you use *Copy System Information* function to send us your system information along with tech support request or bug report, this information includes your non-default *Password Agent* settings. Sending us these settings help to reproduce your working environment in case issue only occurs with certain program settings. You can remove any parts of the information you do not wish to send us when submitting your system information.

Warning: Be careful when using *Password Agent* in public computers (at work, internet cafes etc). Using special logging and spy software it is possible to log all computer activity, including your master password and other data you enter or view on screen. If such program is installed then someone can steal your master password and other data you enter through *Password Agent*. This is true for all Windows applications, not only for *Password Agent*. For example it is possible to log all passwords you enter manually into your web browser or all text you enter using keyboard; all active programs, mouse clicks etc. See “How secure?” on page 7 for more information.

How secure?

People often ask, how secure is *Password Agent*. Is it 100% secure? Even when the data file is encrypted using one of the best strong encryption algorithms and key is derived with another current top algorithm, your actual security usually depends on other factors. And unfortunately these others factors are often overlooked, making people think that total security depends on the “key length” that is used to encrypt you data.

Assume there is someone who is planning to get access to secrets you are keeping in *Password Agent*. You need to know that there are several ways someone may try use to get access to your secrets, so lets analyze them and make some conclusions.

Stealing your data file

If someone will get access to your data file, don't worry too much. He will not get access to the secrets if he doesn't know your master password. It is very unlikely someone is able to decrypt the file without valid master password using today's computers. But as today's best encryption methods are considered "strong", something may happen tomorrow that will make them obsolete instantly. This is unlikely, but still possible. But nevertheless, whenever possible don't share your data files. **Risk – very low**.

Dumping memory

Another potential way to steal your info is to use specially crafted malicious program to dump running *Password Agent*'s memory to a disk file, then later try to find any plain text or key info from this file. To prevent this, *Password Agent* keeps data in memory in encrypted form and its entire design is to prevent plain text leaks to memory, as there is no point in time where all fields of an item are decrypted to plain text at the same time. In addition all plain text is "burned" after use to prevent leaks (see "Security" on page 9). **Risk – low**.

Swap file and hibernation file

Windows manages a swap file – it is memory extension on hard disk, called virtual memory or page file. Since programs and data files may be very large nowadays, everything can't be kept in limited computer memory at the same time, so Windows now and then writes data and running programs not used at the moment from RAM to hard disk. That means on one moment *Password Agent* and any other program may end up written to swap file along with all memory in use and there is no way to prevent this. Also all computer memory is written to a disk file when computer is put into hibernation or hybrid sleep mode. That is almost identical to our previous "Dumping memory" case, but done regularity by Windows itself! If you are on a public computer then someone can potentially try to search the swap or hibernation file for plain text or key info, but *Password Agent* does not keep plain text in memory (see "Security" on page 9). **Risk – low**.

Social engineering

That is old truth and known to everybody – the simpler the password the easier is to guess it. Don't use simple master password. Don't use your name, your dog's name, your wife's name, your childrens name, your favorite actor name, any of your favorite things, known dates etc as your master password. If someone is trying to get access to your secrets, that is what he will try first. Use something much more abstract, like several random words combined with some numbers or even better, totally random string. **Risk – high**.

Spy programs and key loggers

There are countless spy programs available that allow someone to secretly watch and record your every key press, including your master password you type, text you copy to clipboard, screen captures, mouse movement and clicks etc. Basically everything you see on the screen can be also recorded, so **on public computers is impossible to warrant secure work environment**. Using the program in public or other people's computers is not recommended. Use your own mobile device instead. However, many internet viruses install key loggers as well. So it is also possible that, literally, your own computer is spying on you. **Risk – very high**.

Conclusions

As you can see, final security depends mostly on other factors than encryption algorithm and key length used. Your file may be encrypted using the best encryption available, but if someone can easily just steal or guess your master password, then even the best encryption will not help you.

If you work with very sensitive data then only use *Password Agent* on your personal computer that is kept free of viruses and is regularly updated with security patches.

To make long story short – security of your data depends mostly on you.

Security in more detail

Note: This topic is for advanced users.

This topic discusses how exactly *Password Agent* works behind the scenes, what kind of encryption is used in *Password Agent* and also some possible weak points of the program that may potentially leak your information when used inappropriately. You can then decide if this kind of security is enough for you or not.

Encryption

Data files (*.pwa files) are encrypted with strong U.S government approved AES (default) or Twofish algorithm using 256-bit key that is derived from master password using PBKDF2 with SHA2-256. Iterations used for KDF can be changed and default iteration count is random number that produces delay of around 0,7 seconds (assuming it takes longer on a mobile device). The master password itself is not stored in disk file, only hash of key derived from master password.

Microsoft Crypto API is used for generating random numbers.

Data in memory

While most password managers you can download from the internet focus mainly on encrypting your data on disk, *Password Agent* uses secure plain text handling also for all in-memory operations. Memory data is always kept fully encrypted. In addition, in typical viewing and searching mode **there is no moment in time where all fields of an item are decrypted into plain text at the same time**. Item fields are decrypted one by one only when needed to be drawn on screen, after drawing on screen plain text is immediately burned (note that you can edit only one field of an item at a time, not all fields). Whenever possible plain text is painted directly to screen instead of using built-in Windows controls which may leak plain text. All that minimizes possibility of plain text leak to memory and scratch disk. If you consider all this additional behind the scenes overhead, performance of *Password Agent* user interface is excellent. Also, **native 64-bit version makes use of additional security** of *Windows X64* platform, like improved ASRL and DEP, which help to make attacks against running application more complicated.

All textual data fields of all items and folders are encrypted, including item and group titles.

Possible plain text leaks

Plain text leak means that some of your decrypted secret data may potentially end up in Windows swap file or memory (RAM) and when a specialist is specially looking for it, he may find it. It does not mean that *Password Agent* will leave temporary files or text files on your disk, readable by anyone.

The most common plain text leak, initiated by the user, is when copying text to clipboard. That means using *Copy Password*, *Copy Note* and all other similar functions that copy decrypted item data to clipboard. *Password Agent* will clear clipboard automatically after specified time, but nevertheless copied text may remain in memory and may be swapped to disk due to Windows design. There is nothing we can do about it.
Exception in clipboard functions are plain *Copy*, *Cut* and *Paste* commands that operate on entire item or folder. Use of these commands does not result any plain text in clipboard (only item or folder ID is stored), so use of these commands is fully secure, even when pasting from different file.

When you use data export to common XML or CSV format, resulting file is in plain text and readable by anyone with a text editor. So be sure to delete these export files after use. And keep in mind that the program you use to process these plain text files may also behave unexpectedly. For example if you double-click an XML file it may be opened by system default web browser but the web browser may copy the data file to his cache on disk, meaning that the plain text data may remain somewhere on your disk even after you delete the original XML file. This has nothing to do with *Password Agent*, but you should be aware of situations where your data may leak.

Finally, while *Password Agent* tries hard not to leave any plain text in the memory, unfortunately we can't take responsibility about all the other software where you send your secrets using autofill, over clipboard or by any other means.

No backdoors

There are no backdoors in the program – if you forget your master password, we can't help you to open your file. Master password is not stored anywhere, only "fingerprint" of it, so there is no way to retrieve master password from file as it can't be reconstructed from that fingerprint. That is the point of the program – allow access to data only with one master password. So take care of your master password.

Tutorial

Choosing a strong master password

Choosing a strong password, one that you also can remember, is not trivial and that is why people don't use strong passwords.

As big web services are continuously compromised and user data, including user passwords, are leaked, we can have look at top passwords that users like to use. For some, it may be eye opener to read Gizmodo's article The 25 Most Popular Passwords of 2015: We're All Such Idiots. Here are top 10 most common passwords from that article:

```
123456
password
12345678
qwerty
12345
123456789
football
1234
1234567
baseball
```

The reality is that there are lists of millions of user passwords around and it is easy to use these password lists in addition to available dictionary word lists when breaking in into web services and programs like *Password Agent*. So **you should take care not to choose a common password or a dictionary word as your master password**.

To choose a strong password, Bruce Schneier's advice is useful:

"Take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". *That nine-character password won't be in anyone's dictionary."*

If you would like to learn more and get some good ideas then please read these web articles:

Choosing Secure Passwords – schneier.com

How Secure Is Your Password? A Friendly Advice from a Company That Breaks Passwords – elcomsoft.com

Your Password is Too Damn Short – codinghorror.com

Warning: Never trust a 3rd party with your important passwords.

Note: *Password Agent* contains built-in list of 10 000 most common passwords and will warn you if you are using a very common master password. If you get no warning then that does not mean that your password is strong, though.

Creating new data file & setting master password

Password Agent stores all your logins and other secret items in a single portable data (database) file. The data file acts as a container for all the items you store. If needed you can also create multiple data files, like in case of multiple family members using the program on one computer. Then each user can have his/her personal file protected with master password only he/she knows.

If you are new to *Password Agent,* you'll need to create at least one data file and assign master password to it. Here are the steps to create new data file:

1. Choose **File | New** command from menu. Now *Create new file* window is displayed, asking for file name.
2. **Type name for your password data file**, it is good idea to use your name (like "John") if there are more users for your computers besides you. You can select also different folder if you wish, but by default your file is saved in your *Documents* folder. It is good practice to keep your data in your *Documents* folder for easy backup, don't try to save it to your program files folder. Also don't use something like "Johns passwords" as file name as it generates higher interest against this file when someone accidentally gets access to your files. *Password Agent* will append file extension *.pwa* to your file. **After typing your file name, press *Save* button**.
3. Now *Master Password* window is displayed. Every password database file must have master password specified. It is used to restrict access to the file, so only people who know the master password can open the file and see its contents. You are required to supply your master password every time you want to unlock your file.

   It is important to understand that **master password is assigned to each file separately.** Master password is not a password that allows you to get access to the *Password Agent* program, but *Password Agent* uses it to encrypt and decrypt data file contents. For example, if your friend brings his own *Password Agent* database file to your computer, then only his/her master password can be used to open his file.

   Choose a master password for your file and enter it in the *New Password* field (don't worry about the disabled *Current Password* field, it is not used this time). You need to choose a strong password, since if anyone guesses your master password, they will have access to all your other passwords stored in the *Password Agent* database file too. See topic "Choosing a strong master password" above on how to choose a strong master password. Enter the same master password once again, into the next field. This is for making sure you did not make a typo then entering it the first time.
   The window has also *Encryption settings* tab but here we accept default encryption settings which are adequate and can be changed later, if desired.
4. If you are finished assigning your master password, press **OK** to finally create your new data file.

At this point *Password Agent* has finished creating your file and you can start entering your data. See the following topics about program layout and how to add your first items.

Warning: You should be very careful not to forget your master password, because if you forget it, no one, even us, can open the file.

Saving file

Saving your file is done automatically each time you change any information, so there is no separate *Save* command that can be triggered by the user. This reduces the risk that your computer crashes and you'll lose important changes in your data.

Tip: After saving file *Password Agent* can automatically copy your data file to a secondary location(s), like different folder or different computer in a network. See program settings, *Backup* section, to define a secondary location(s).

Previous file versions

When a file is updated, previous version of the file will be available with the extension *.old1*. By default the program keeps 5 previous versions of the file – *.old1* being the newest and *.old5* being oldest. You can configure how many copies of old backup files are kept in program settings, *Backup* section.

Each previous version has one change less, so only the latest file has all latest modifications. So .old*1* file has 1 last modification missing and *.old5* file has 5 last modifications missing. However, if your main file becomes damaged you can restore from *.old1* file in case you don't have another backup. But keep in mind it does not contain last modification made you your original file.

Maintaining old versions of course does not mean that you should not make backup of your password database. **Always make a backup of your data files off your computer since otherwise if your storage device fails or computer gets stolen you'll lose all data.**

Locking a file

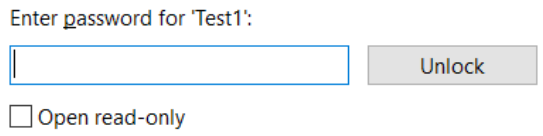
The **File | Lock** command or **Lock** toolbar button allows you to lock your open file without closing the program. When file is "locked" then it is actually completely unloaded from memory, so no need to worry that someone can somehow just bypass the unlock screen to see your sensitive data.

The program has also several settings that allow you to specify whether the program will lock or close itself automatically after specified period of user inactivity etc. See program settings, *Security* section.

Warning: If a file is automatically locked by user inactivity timeout then any pending editing is discarded. Current design is that any text field will be saved as soon as you press *Enter* key or move focus away from the field, but it is possible to leave a text field in edit mode and leave computer, so inactivity timeout will force the file to close. Pending text field edit is not saved to file on such case. As you can only edit one field at a time then it is possible only to loose edit of one single field. So it is a good practice to properly finalize any text field edits, so changes are always saved to file.

Unlock screen

If you load a file or lock open file then unlock screen is displayed.



Here you enter master password to unlock file. On image above *"Test1"* is name of the file you are unlocking. If you want to see full path of the file move your mouse pointer over the label *Enter password for 'Test1'* and full path of the file name will be displayed as hint.

The *Open read-only* checkbox allows you to open the file in read-only mode to avoid accidental modifications. After you have opened a file in read-only mode, you can toggle read-only mode of unlocked file with menu command **File | Read-only**. If you rarely use the *Open read-only* checkbox on unlock screen you can hide it by changing program setting *Show "Open read-only" checkbox*.

Tip: If you after typing master password press `Ctrl+Enter` instead of just `Enter`, then after unlocking file *Password Agent* will be automatically minimized. Useful if you use mostly new *autofill matching item* functionality that does not require you to select item in item list to autofill from.

Opening a file

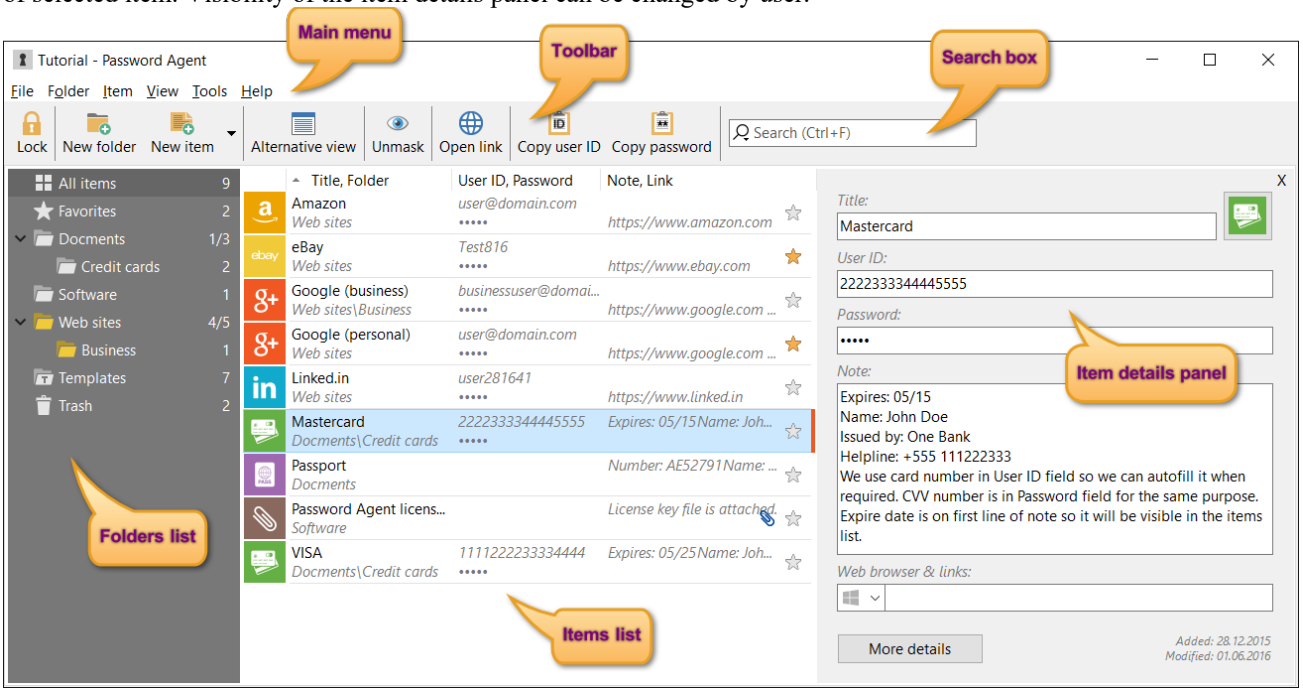
If you work with only one file, then you usually don't need to load the file manually – *Password Agent* will automatically load last used file at start-up. You can override this under program settings, in *Start-up* section, by specifying your custom start-up file(s) and options.

If no data file is loaded at start-up or you just want to load additional file choose menu command **File | Open** or pick a recently used file from list in **File | Open recent** sub-menu. Also, you can drag and drop files from *Windows Explorer* to *Password Agent* window to load the files.

Tip: If you use menu command **File | Open** frequently you can customize the toolbar to show *Open file* button for quick access.

Program window explained

Password Agent has a simple layout similar to *Windows Explorer*. In addition to main menu and toolbar the main window has 2 or 3 vertical panels, depending on current configuration. First vertical panel is folders list at left, then comes item list that lists items from selected folder and then there is optional item details panel which can display details of selected item. Visibility of the item details panel can be changed by user.



Menus

Main menu contains commands that allow taking actions. Main menu commands are grouped into *File*, *Folder*, *Item, View* and other menus, where *File* menu contains commands for selected file, *Folder* menu contains commands for selected folder, *Item* menu contains commands for selected item(s), *View* menu contains command to alter current view and so on.

In addition to main menu, **many objects on screen have local right-click menu**, called context menu. You can invoke that by right-clicking the object with the mouse. Objects that have local context menu containing common commands are toolbar, folders list, item list, column headers in item list, data fields in item detail panel, file tabs etc.

Toolbar

The toolbar displays buttons for the most common menu commands. You can customize the toolbar by right-clicking it with the mouse (not on *Unmask* button, which has different right-click functionality) and choosing *Customize* command from context menu. You can hide the toolbar buttons you don't use to de-clutter the toolbar.

Folder list

On the left side you see a hierarchical tree that displays folders, lets call it the folders list. Initially the folders list only displays few built-in folders like *All items*, *Favorites*, *Templates* and *Trash*. When you click a folder with the mouse, items from that folder are displayed in next panel (item list).

To better group your items you can create your own folders, including sub-folders.

Right-click a folder in the folders list to display context menu of the folder.

Item list

Item list displays all items from folder selected in folders list, or when search is active, it displays search results.

If you want to see details of an item then double-click the item (or press *Enter* when focus is in item list) to toggle visibility of item details panel.

Right-click item in the list with the mouse to display context menu of the item.

Item list column headers

The item list displays column headers where header of each column acts like a push button you can click to toggle sorting by that column between ascending or descending order.

To re-arrange column order you can drag a column with the mouse to a new location.

Right-click a column header to display context menu of that column. That context menu also has command *Customize* which allows you to fully **customize the item list display to your liking**.

Search box

On the toolbar after the toolbar buttons you see the search box. By typing into the box search (filter) is activated and only items matching entered text are displayed in the item list. Search is not case sensitive. Search box has *Search options* button that displays menu that allows you to select which data fields are searched, useful if you want to search other fields than *Title* field.

To de-activate search press *Cancel search* button at the right end of the search box, press *Escape* key when focus is in the search box, or click any folder in the folders list to display contents of that folder instead of search results.

Tabs for multiple open files

You can open multiple files simultaneously. On that case tabs are displayed for each file, so you can switch between open files easily by clicking the tabs with the mouse. Tabs are not displayed if you only have one file open.

Right-click a tab with the mouse to display context menu.

Folders

You can create folders to keep related entries together. You don't need to create any folders at all to use *Password Agent*, but folders may help you to organize your data better. Folders in *Password Agent* are similar to folders in your file system.

Password Agent displays also some built-in folders, like *All items*, *Favorites*, *Templates* and *Trash*. ***All items*** is a virtual folder that displays all items stored in file, except templates and trashed items. ***Favorites*** is a virtual folder that lists items

you have marked as favorite. If you drag items to *Favorites* folder these are not physically moved but just marked as favorites. So *Favorites* folder displays all your favorite items from all folders, that's why it's called a virtual folder.

Templates folder contains user-customizable templates for new items. See “Template items” on page 20.

If you delete items they are not immediately deleted but moved to ***Trash*** folder, so you can restore any items you have deleted by mistake. To empty *Trash* folder right-click it and choose command *Empty* from context-menu. That will permanently delete your items and folders that were in *Trash* folder.

Tip: You can perform common folder-related commands by right-clicking a folder.

Adding a folder

1. Select parent folder inside which new folder will be created – a new folder will be created as a sub-folder of selected folder. To create new top level folder select virtual *All items* folder as parent.
2. Press *New folder* toolbar button, choose **Folder | Folder** command from main menu or right-click parent folder and choose *New folder* from context menu. Folder properties window is displayed.
3. Type in the title for your new folder and press the **Enter** key.

Moving a folder

There are two ways to move folder – by dragging with the mouse or using **Folder | Cut** and **Folder | Paste** menu commands.

By dragging one folder over another using the mouse and then releasing mouse button will make the dragged folder sub-folder of the target. To move folder to top level drag it to *All items* virtual folder.

To cancel already started mouse drag operation, drag the folder outside the folder list or press the **Esc** key.

Note: You cannot move built-in folders like *All items*, *Favorites*, *Templates* and *Trash.* Also you cannot create new folders inside these folders, except *All items*.

You can also copy or move entire folder including its sub-folders and items to a different file. This cannot be done by dragging the source group with the mouse but you need to open both files and use **Folder | Copy** (or **Folder | Cut**) and **Folder | Paste** commands. This performs secure transfer of folder from one file to another.

Viewing and changing folder properties (title, icon color etc)

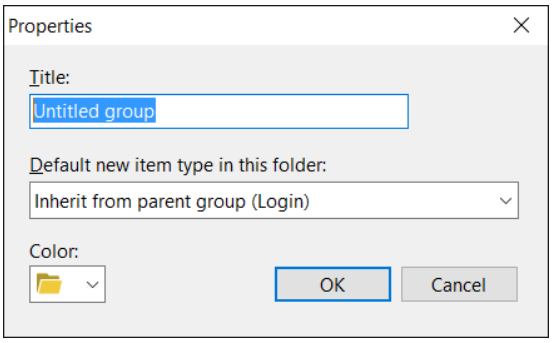
You can change properties like title and icon color of folders you have created.

To display properties of a folder right-click it with the mouse and choose **Properties** command from context menu,

or

1. Select the group whose properties you want to see or change.
2. Choose main menu command **Folder | Properties,** or alternatively, press the **F2** key.

Folder properties window will be displayed.



Title – Title or name of the folder, that is displayed in the folders list.

Default new item type in that folder – Here you can override what type of item is created when this folder is selected and you click *New item* toolbar button or **Item | New** menu command. Note that in addition to login and note items you can specify a custom template item here. That means you can specify that all new items in this folder are of certain type, based on certain template. Even if you specify template you can also create other types of items in that folder as well, when required. Template items listed here are from your *Templates* folder. For more info see "Template items" on page 20.

Color – Color of folder icon. If you want to make some folders stand out you can change folder icon color here.

Deleting a folder

1. Right click the folder you want to delete and choose *Delete* command from context menu,

   or

1. Select the folder you want to delete.
2. Choose the **Folder | Delete** command from main menu. Alternatively you can press the **Delete** key while keyboard focus is in folders list.

Note: You cannot delete built-in groups like *All items*, *Favorites*, *Templates* and *Trash*.

Items

Password Agent stores your web site logins and data snippets in data file as "items". So an item may be a web site login or just a text note. Each item can store user data in properties like User *ID*, *Password*, *Note*, *Link* etc, although any field besides *Title* can be left empty.

There are two kinds of items – logins and notes.

A **login item** is a collection of information related to a service that requires providing user ID and password. Most common such services are web sites that require you to log in using personal user ID and password.

In addition to login items you can create **note items**. These are simple items that can be used to store free form textual information, like your software serial numbers, credit card numbers, secret notes etc. Note entries differ from login items that they don't have *User ID* and *Password* fields. You simply use the *Note* field to store your information.

People are sometimes confused how they can store their credit card or other specific data when there is no special credit card item type. The note item allows you to store any kind of textual data, just don't think you are not allowed to type your data here because the field is named *Note*. Also, there is now a template for credit cards.

All items also accept binary data as attachments.

Adding items

There are several ways to create new item in currently selected folder.

Most common way is to click **New item** toolbar button, or use **Item | New** menu command, or press **Ctrl+N** keyboard shortcut (or just **Insert** key if focus is in item list). This creates new item of kind specified as default item kind of selected group. The factory default item kind is login but this can be changed via folder properties window.

If you want to to create specific kind of item, like note or item based on a template then use special commands in **Item** menu, or from pop-up menu that is displayed when you click drop-down arrow next to **New item** toolbar button.

Now new item is added and its properties are displayed in item detail panel. If you added login item then the *Password* field may be already filled with random pre-generated password. To enable or disable pre-generated passwords for new login items you can modify program setting *When adding new item / Assign random password*. The password was generated using password generator template named *Default settings for new passwords*, which can be modified.

Moving items

You can move selected items from one folder to another by dragging them with the mouse just like you can drag files in *Windows Explorer*. Alternatively you can also use **Item | Cut** and **Item | Paste** menu commands. Latter must be used if you want to move or copy items to another open file.

Editing items

Editing item means making visible item details panel on right side of the screen and changing item values there. To toggle visibility of item details panel do one of the following:

1. Double-click an item with the mouse.
2. Choose **View | Item details** command from main menu or **Item details** command from context menu of item list.
3. When keyboard focus is in item list press the **Enter** key.

See next topic about detailed description of item details panel

Deleting items

1. Select one or more items you wish to delete.
2. Press the **Delete** key, or choose **Item | Delete** menu command. Alternatively you can also right-click selected item and choose **Delete** command from context menu. Another alternative is to drag selected items to the *Trash* folder.

Favorite items

It is possible to mark some items as favorites. The benefit is that then these items appear in virtual *Favorites* folder for quick access without using search box. What's more – you can also make your *Favorites* folder default selected folder when the program starts, listing only your favorite items instead of all items.

To change folder that is selected by default on program start, change program setting *Folder selected by default*.

To toggle if selected item is favorite use menu command **Item | Favorite** or double click on the item's "star" image in item list. The "star" image can also be shown/hidden by customizing view of item list (**View | Customize current view**), so it may not be always visible. On that case you can use the menu command.

Changing item kind

You can create two kinds of items – login items and note items. Sometimes you may want to change item kind later. For example you have note item and then there is need to add user name and password to that item. Instead of creating a new login item you can convert kind of an existing item – you can convert note item to login item and login item to note item.

To change kind of an existing item right-click it with the mouse and choose context menu command **Item | Convert to**.

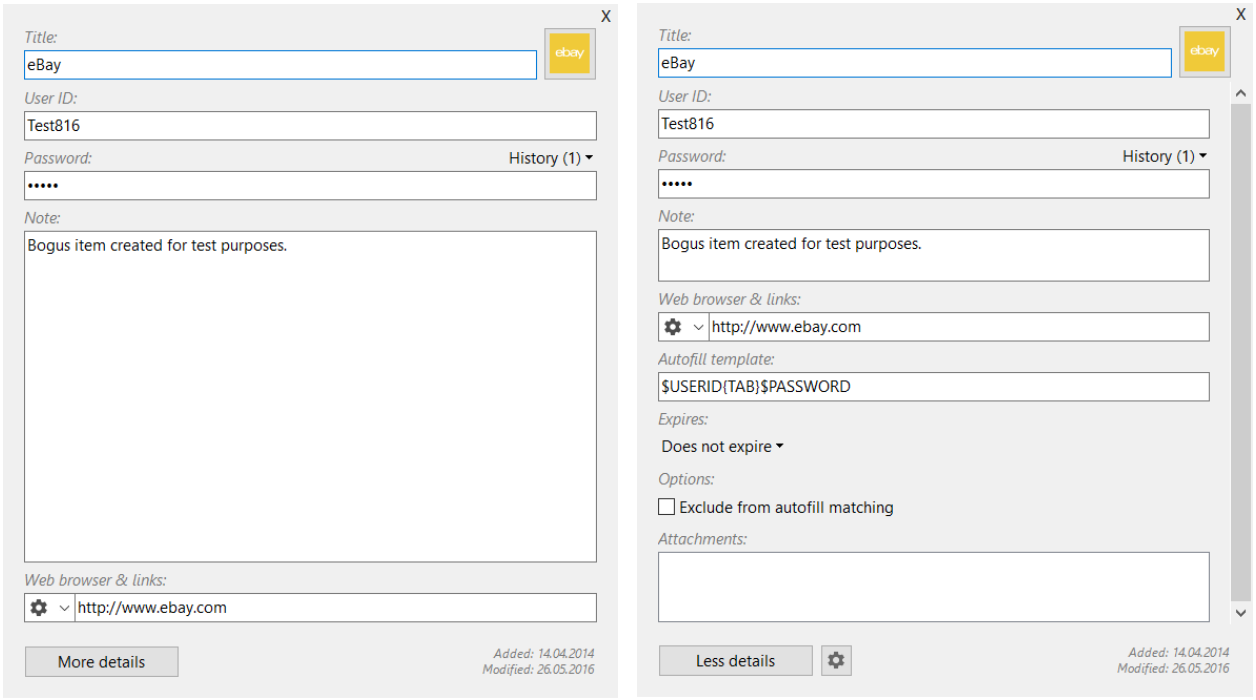
If you convert login item to note item then values from *User ID* and *Password* fields are merged to *Notes* field, so you will not lose contents of these fields.

Item details panel

Item details panel is displayed when you create a new item or edit an existing one. You can toggle visibility of item details panel by double-clicking an item in the item list or by menu command **View | Item details**. Alternatively you can also press **Enter** key when keyboard focus is in item list.

Text fields you see in the item details panel are not traditional edit boxes. To put such field into edit mode you need to first click it with the mouse. This may seem inconvenient at first but is designed to offer more secure editing, as only one item field is being edited at a time. Typical password manager (and also older versions of *Password Agent*) puts all fields into edit mode at the same time and this fact combined with the use of Windows edit boxes result that plain text data from all these fields may leak into memory and later to disk by swapping. Or, a malicious program may capture memory

of a password manager program at the moment it starts editing item, resulting all decrypted fields of an item being captured at once. Editing each field separately minimizes size of leak.



Above you see image of item details panel displaying details of a login item. On second image the panel is in *more details* mode, displaying additional fields like *Autofill template*, *Expires*, *Options* and *Attachments*.

Title – the name you give to your entry. For example, if you want to add an item for your eBay login, you can name it "eBay" or "eBay.com" (without quotes). Be descriptive when naming your items, because after few years you may have a collection of hundreds of items and descriptive names will help you to find the right item quickly.

Icon and color – You can choose a different image to represent this item. By default, *Password Agent* chooses a key icon for login items and a note icon for note items. That way you can distinguish note entries from logins in the item list. Note that you can change colors of all login and note items globally by program setting *Colors / Default item color*. Here you can override default color for specific items, if needed.

User ID – this is user name or user ID field, typically used in pair with the *Password* field. Nowadays many services use your e-mail address as user ID which means several of your items may share the same user ID. If you move mouse over *User ID* field you see *Assign e-mail address* button, which allows you to assign your e-mail address quickly once you have added it to the list of your e-mail addresses. This field is displayed for login items only, not for note items.
When user ID history list is not empty you may see user ID history label above the *User ID* field. Pressing the label will display list of previous user IDs (in use before current user ID was assigned). To remove a user ID from the history list right click the ID you want to remove and choose *Delete* from context menu.

Password – If you have not been given a ready made password by a third party, you can enter your own password, or *Password Agent* can generate a random password for you if you press the *Generate password* button displayed when you move mouse over *Password* field. This field is displayed for login items only, not for note items.
When password history list is not empty you may see password history label above the *Password* field. Pressing the label will display list of old passwords (password in use before current password was set). To remove a password from the history list right click the password you want to remove and choose *Delete* from context menu.

Web browser – Web browser drop down box allows you to use specific web browser for this item. This is taken into account when you invoke **Item | Open Link** command. If specific browser is specified for this item and that browser is installed in your system then *Password Agent* tries to use that browser when opening link.
Note: If you want to change default browser for all items then you can do so in program settings, *Web browser* section. In addition you can define a custom browser there, which may be any executable program.

Note – Any comments you may want to add about this entry. If you are creating a new note entry, this is where you put your important information you want to store.

Links – Web site URL or full path of executable program. If web site URL is provided, *Password Agent* can open that web page with the **Item | Open link** menu command. A web site URL must start with "http://" or "https://", otherwise *Open link* command will fail. Also, you can write full path to a program executable file here, so you can run that external program using **Item | Open link** menu command. If executable path contains spaces then you need to enclose executable path between double quotes.
Assigning web page URL is very useful when combined with the *autofill matching item* functionality, which helps you to log into your web sites semi-automatically. See "Automatically filling login " on page 26 for more information.

Autofill template – Template that is used by *Autofill* function. Don't change this if you don't know what you are doing. See "Automatically filling login " on page 26 for more information.

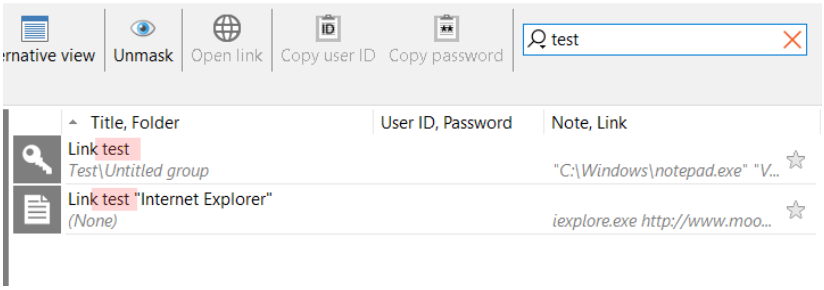
Expires – Allows to assign an expire date to the item. Basically this may be useful for password accounts that expire after certain date but also for system administrators who store their user accounts in a *Password Agent* database. Press drop-down arrow to display menu with related commands. If expire date is specified and **View | Highlight expired items** option is activated, *Password Agent* will color code expired and soon to expire items in item list with colors specified in program settings, section *Password expiration*.

Attachments – Lists attached files. You can add small external files as attachments. These attachments are stored within database and you can save them back to file system when needed. *Password Agent* does not allow you to attach big files as all attachments are kept in memory.
Right-click attachments list to display context menu with related commands.

Added & modified dates – On bottom the item details panel you see label with date the item was first added to the database and also date of last modification. To save space only date is displayed but if you want to see exact time move the mouse pointer over the label and both date and time will be displayed as hint.

Searching for items

Password Agent makes it easy for you to find your item quickly – just type text you want to find into the search box on the toolbar. *Password Agent* filters all items in real time as you type to match your query.



On illustration above phrase *"test"* was typed into the search box, resulting only items having the phrase "test" in title being displayed in the item list. Search is not case sensitive, so you'll get the same results when searching for *"TEST"*.

You can define which fields are searched by clicking the **Search options** button at left side of the search box. By default only *Title* field is searched but you can include any other fields you want to search. This setting is saved between sessions, so next time *Password Agent* uses the same search options you have selected in the context menu.

To change keyboard focus from the search box to the item list you can press **Enter** key when focus is in the search box.

To cancel search you can either press **Escape** key when focus is in the search box or click **Cancel search** button on right side of the search box. Alternatively, click any folder in the folders list to display contents of that folder instead of search results.

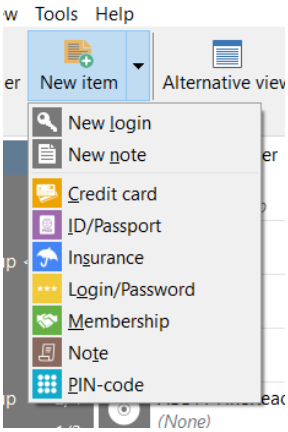
Tip: When you unlock a file, input focus is automatically moved to the search box, so you can start typing there immediately. If focus is in other control you can use keyboard shortcut **Ctrl+F** to change focus to the search box.

Using clever search phrases

To minimize typing try to use clever search phrases. For example if your entry is titled *ShareIt*, you don't need to start typing "*share*" as it will also return other titles that contain the word "*share*", like "*shareware*" etc. On this case type something that is unique to the item you are trying to find, like phrase "*reit*". Or when you have item titled *PayPal*, you don't need to type full "*paypal*" but try "*ypal*" instead to save a few keystrokes.

Template items

Items in built-in *Templates* folder can be used as templates for new items. When you create new item based on template item then all properties of template item are inherited by new item. Or in other words, new item is a copy of template item.



If you click drop-down arrow next to *New item* toolbar button you see pop-up menu. Topmost menu commands *New login* and *New note* just create new standard items. But all other commands below are listing of template items from your *Templates* folder. If you create new items in *Templates* folder then this menu will also list your new template items allowing you to create new items based on template items.

For example you see *Login/Password* template listed. It is basically same as standard *Login* item, but has different icon assigned. So all login items you create based on this *Login/Password* template will have this yellow icon. That way you can use custom icon for all new login items easily.

Tip: It is possible to specify default new item kind for a folder. By default if you press *New item* toolbar button a new login item is created. You can change that behavior so *New item* toolbar button will create other type of item by default, including item based on template. See "Viewing and changing folder properties (title, icon color etc)" on page 15.

Printing

To start printing choose menu command **File | Print**.

Options in *Print* window:

Print as graphics – By default *Password Agent* sends printout to printing sub-system as bitmap graphics, so text search can't be used by attacker to find plain text from intermediate files produced by spooler. All this may be overkill for average home user but is something to be aware of.

If secure printing fails or produces jagged printout you can unselect that option to print traditional way.

Changing sort order of items

You can order (sort) items in the item list by different criteria: by title, by user ID, by date or even by password length etc. By default, items are sorted by Title in ascending order.

The item list displays column headers where header of each column acts like a push button you can click to toggle sorting by that column. If you click a column header that is already used for sorting then sorting will toggle between ascending or descending order.

Another way to change sort order is through menu command **View | Sort By**.

Tip: Sub-menu **View | Sort By** allows you to sort by additional fields that are not currently visible in current view.

Copying data to clipboard

Password Agent makes it easy to copy your data like passwords and user IDs to clipboard in plain text format. That makes this data available to other program via clipboard, but you need to remember that once you copy your secret data to clipboard in plain text form, you don't have much control over it and that plain text may eventually end up stored somewhere on your disk for days or months. This is due to Windows clipboard design. Also, it is trivial to make a program that will immediately record all text that is copied to clipboard from any application. So keep this in mind when using the program on computers that are not fully under your control. See topic “Possible plain text leaks” on page 9 for more security information.

Password Agent will automatically clear clipboard 20 seconds after you copy plain text. After text is copied to clipboard you'll see green progress bar on taskbar button, that progress visualizes countdown to the moment when clipboard is automatically cleared. So after copying your text you need to paste it to target application before clipboard is automatically cleared. To adjust this timeout you can change program setting *Clear clipboard timeout*.

Password Agent will clear your copied plain text from clipboard also on exit.

Password generator

Password generator allows you to easily generate difficult to guess random passwords. You can use it to generate passwords for login items stored in your data file or just as a stand-alone tool to generate passwords used outside of *Password Agent*.

To invoke stand-alone password generator, use menu command **Tools | Password Generator**. Password generator tool is accessible even if you don't have any files open in *Password Agent*.

If you need to generate new password for an item stored in your data file then there is *Generate password* button visible if you move your mouse pointer over *Password* field in item details panel. Clicking that button will display context menu with a some read-made passwords for you to pick, or you can choose to show password generator interface if you need to tweak password generation options or use non-default password generator template. Assigning (new) password to your item that way is the most secure because the new password is not transferred though insecure clipboard.

Program settings

There are many settings you can change to further customize the program to your needs.

To display *Settings* window choose menu command **Tools | Settings**.

To **restore default values for all settings** on a page press *Restore defaults* button. To **restore default value for a single setting** or settings group, right-click the setting or group and choose *Restore default value* from context menu.

If something happens to the settings file so that when running *Password Agent* its main window is not displayed then you can try to load default settings on program start-up. as instructed in topic “How to start with default settings” on page 36.

Main tab

Security

Show file name on title bar – By default file name is displayed on title bar and thus on program button on Windows taskbar. By not displaying file name you may enhance security as someone looking at your screen does not know with what file you are working on. If you have multiple files loaded then file name is displayed on file tab anyway.

Save recent and session file names – Specifies if file names you are working with are stored in recent files list or not. You can specify not to store file names which can enhance security as if someone runs your *Password Agent* he does not know where your data file is located as recent files list is empty. On that case also last used file is not automatically loaded on start-up. Note that Windows may store your last used files in the registry anyway, so someone can likely find your used file names from there.

Save *Unmask* button state between sessions – By default the state of *Unmask* button is not saved and when your start the program unmask feature is not active, so all your sensitive data is properly masked for protection. Here you can specify to save state of unmask feature if you really want next session to start in unmask mode if you previously used that mode.

Show list of pre-generated passwords – By default list of pre-generated passwords is displayed when you press *Generate password* button of *Password* field in item details panel. You can then quickly pick desired password from the list, without the need to open password generator window.

Block screen capture (return black screen) – Blocking screen capture by default helps to prevent malicious programs from secretly recording your *Password Agent* window contents. Disable it only if you get black *Password Agent* window when accessing your computer remotely using *TeamViewer*, *LogMeIn* or other remote connection software.

Clear clipboard timeout (seconds) – Timeout after which text copied to clipboard by *Password Agent* is cleared from clipboard for additional security. *Password Agent* is smart enough to clear only text it has copied to the clipboard, it does not clear text you have copied from other programs.

User inactivity timeout (minutes) – Select timeout in minutes after which the action specified by the setting *Inactivity action* is invoked.

User inactivity action – Select action to take when inactivity timeout defined by the setting *Inactivity timeout (minutes)* occurs.

Computer sleep or hibernate action – Select action to take when computer goes to sleep (stand-by) or hibernation mode.

Workstation locked action – Select action to take when the workstation is locked by Windows or by user.

Monitor sleep or screen saver action – Select action to take when monitor goes to sleep (stand-by) mode or screen saver is activated.

Lock on minimize – Select if you want all unlocked files to be locked when program is minimized. You can combine this setting with other settings like *Minimize after autofill.*

Sensitive data mask – Specify symbols to be used instead of sensitive data for masked fields. You can cheat someone by writing say "12345" here, then looking at your screen it looks like you use the same password *12345* for all items.

General functionality

Pressing *Esc* key will – Specify action when pressing *Esc* key on keyboard.

Show item details panel by default – Select if item details panel is visible by default when the program is started.

Show icon in notification area (system tray) – Specify if notification icon will be displayed in system tray/notification area. Then Password Agent button is not displayed on taskbar when Password Agent window is minimized, only notification icon is displayed.

Folder selected by default – Specify whether *All items* or *Favorites* folder will be selected by default when the program is started.

Expand all folders by default – Specify if the folders list is fully expanded when the program is started. The *Folders* menu has commands to expand and collapse the folders manually.

Play audio feedback when searching – While you are typing a search phrase that results zero matching items then audio feedback "*eek*" is played. While you are typing a search phrase that results one matching item, likely the item you were looking for, then "*pop*" sound is played. These sounds help you to stop typing when it is known that match is either found or not found.

Run automatically on Windows start-up – By selecting this option the program will be launched automatically when Windows starts. While you can easily start the program from a shortcut manually, when needed, running it on Windows start-up has advantage that then you can use global hot keys of *Password Agent* ("*Autofill e-mail address*" or "*Show Password Agent*"). Global hot keys only work while *Password Agent* is running. **Note:** This option may not work if *Password Agent* is installed as Windows app (UWP).

Item list

Double-clicking item will – Specify what happens when you double-click an item in item list.

Pressing Return key in item list will – Specify what happens when you press *Return (Enter)* key when focus is in item list.

Default sort field – Specify default sort field (column). You can sort by another field by clicking another column header.

Default sort direction – Specify default sort direction.

Web browser

Default web browser – Select web browser you want to use for opening web links that are launched from within *Password Agent* using *Open link* command. Default value is "*system default*", which means system default web browser is used. Listed are several popular web browsers, but you need to have specific browser installed to use it. If you select "*custom*" browser you need to specify full command line by next setting *Custom browser command line*. Note that you can also specify web browser for each item separately.

Custom browser command line (use $LINK variable) – Command line of custom web browser or external program used to open links with *Open link* command when web browser of selected item is set to "*custom*" or when global setting *Default web browser* is set to "*custom*".
If path of the executable contains spaces you need to include the path between double quotes. You can specify command line parameters. Use optional variable `$LINK` in place where you want to pass value of *Link* field to the custom program. If `$LINK` variable is not used then value of *Link* field is passed as last parameter. For example the following command line will launch *Internet Explorer* in *InPrivate* mode (on 64-bit Windows):

"C:\Program Files (x86)\Internet Explorer\iexplore.exe" -private $LINK
Then all items that have web browser set to to "custom" are opened using *Internet Explorer* in *InPrivate* mode.

Unlock screen

Show "Open read-only" checkbox – Allows hiding "*Open read-only*" checkbox on unlock screen in case you don't use it.

Backup

Number of old files to keep when saving – Specify number of old file versions to keep when saving file. *Password Agent* maintains file history in case you need to revert back to previous version on some reason. See "Saving file" on page 11.

After saving, copy file to these directories – Here you can specify optional secondary locations where to copy your data file after each change. It can be local or remote directory. Separate multiple directories with semicolon ";" (without quotes). It is a good idea to keep up to date copy of your data file in remote computer or network attached storage (NAS) device.

When adding a new item

Assign random password – Specify if a random password is automatically assigned to *Password* field of new login item.

Assign title and link from URL in clipboard – Selecting this setting allows you to assign *Title* and *Link* fields of a new item automatically, in case there is an URL in clipboard when you create a new login item. *Link* field gets entire URL from clipboard as value and *Title* gets server part of the URL as value.
Activating this setting allows the following work flow when adding new login items. Imagine you are browsing eBay web site and want to create new login item in *Password Agent* for that web site. Then you first copy URL of eBay web site ("*http://www.ebay.com*") to clipboard and switch to *Password Agent*. There you invoke command to create new login item. Notice new item has URL "*http://www.ebay.com*" from clipboard already assigned as value to *Link* field and *Title* field is set to "*ebay.com*", saving you some steps. If a random password is also assigned to the new login item, you can always replace it with a different one in case your service provider already assigned you a password.

Autofill

Settings in this section are related to *autofill* feature which allows you to automatically fill login prompts on web sites. For more information see topic "Automatically filling login forms" on page 26.

Default autofill template – Default template used for *autofill* functionality.

Minimize after autofill – Specifies whether the program window will automatically minimize after filling a login prompt.

Notify if browser AutoComplete is enabled – Most web browsers have built-in password managers that store user ID and password and want to type it for you. If you use *autofill* function then that is no good if both web browser and *Password Agent* are trying to type in your password at the same time, rendering the password invalid. When this setting is selected then *Password Agent* tries to detect if your target browser has its auto-complete for passwords enabled and notifies you. Otherwise your automatically filled logins may just fail with no apparent reason.

Files to load

Files to load on start-up – Specify which files to load when the program starts. If you select value "*custom*" then specify custom file(s) by following option *Custom start-up files*.

Custom start-up files – Specify one or more files to load on start-up. By default the program automatically loads files that were loaded during previous session, but here you can override that with custom files which will be loaded regardless of files that you were working in last session. Separate multiple files with semicolon ";" (without quotes). If you specify any files here you need to set previous setting "*Files to load on start-up*" to value "*custom*" as well.

Fonts

Password font – This is a special font used to draw passwords on screen and when printing. The font should be able to make reading passwords easier, should make it possible to make a difference between O, 0 and o, 1 and l. The default font *DejaVu Sans Mono* is built-in but here you can specify another installed font, if needed.

Password expiration

Expire time template – By modifying this template you can configure what date ranges will be included in context menu that is displayed by clicking button next to *Expires* field in item details panel. The context menu allows you to quickly set password expire date using pre-defined periods, like after 30 days, 3 months, 1 year etc. The default template is `15D 30D 3M 6M 1Y` and this will produce the following entries in the context menu: *15 days, 30 days, 3 months, 6 months, 1 year*. If you are not satisfied with the pre-defined periods then you can change the template here to include different time values. Rules are that you need to write number, followed by D (days), W (weeks), M (months) or Y (years). Multiple entries need to be separated by a space. For example to change the context menu to include only *10 days* and *2 weeks* entries, use `10D 2W` as template here.

Highlight expired items – Specify whether to mark expired and to be expired items with color stripe in item list. You can specify color by **Expired item color** and **Item expiry warning color** settings.

Item expiry warning time (days in advance) – *Password Agent* can highlight entries that will expire after day count specified here. Highlighting occurs only if you have **View | Highlight expired items** setting active.

Hints & notifications

In this section you can enable or disable some of the notification messages that *Password Agent* displays.

Hot keys tab

Here you can assign global hot keys to invoke *Password Agent* functions when it is not active application on your screen. ***Password Agent* must be running on background for these hot keys to work.**

Most hot keys are related to autofill function and are discussed in topic “Automatically filling login forms“ on page 26.

Activate Password Agent – This hot key will bring up *Password Agent* window to your screen if it is minimized or not the topmost application.

Autofill e-mail address – Types your e-mail address automatically on a web page or in another application. E-mail address is taken from your e-mail addresses list, defined on *E-mail addresses* tab of settings.

Note: Do not try to simplify these by using only Ctrl+A for example, such hot keys will conflict with system and application hot keys. Always use Ctrl+Shift and your desired key.

E-mail addresses tab

Usually web sites use your e-mail address as user ID. You can list your common e-mail addresses here so you can easily assign them to new login items without need to type. First address from this list is considered default and is also used by *“Autofill e-mail address”* function (see topic “Hot keys tab” above).

File association tab

Associating *Password Agent* data files (*.pwa) with Windows shell allows convenient opening of these files by double-clicking. Here you can set up or remove file association with the shell.

Note: Administrator rights are required to change file association. See topic “How to run as administrator” on page 35.

Automatically filling login forms

One exciting *Password Agent* feature is the ability to fill in login forms of web sites or software programs semi-automatically with user ID and password stored in the data file. That is somewhat similar to web browsers' internal auto complete feature, but big difference is that *Password Agent* is browser independent, meaning it stores your data outside a specific web browser in secure way and it can work with different web browsers and basically your login can be sent to any Windows application, be it a web browser, FTP client program or an accounting program, among others. Also it does not use any web browser plug-ins, meaning hassle free use with multiple web browsers.

Important: To send text to another application *Password Agent* uses "*send keys*" method. That means it simulates keystrokes, as you were typing the text on keyboard. That is also the downside, meaning that potential key logging programs will likely be able to capture your logins sent using autofill the same way they can capture your logins entered on keyboard. In other words, using autofill function is not much more secure than typing your login by keyboard. So the autofill function must be thought as a means to speed up login process, not to make you logins more secure by protecting you from potential key logging programs.

Autofill matching item (new in version 2016)

Note: This feature works with most common web browsers *Chrome*, *Internet Explorer*, *Edge*, *Firefox* and *Opera*.

Autofill matching item feature of *Password Agent* makes logging into web sites very easy. When you need to fill login form on a web page you need to press global hot key combination and then *Password Agent* will detect URL from your web browser, will find an item matching to the URL from your data file and will type user ID and password of the item for you. Filling web forms is not fully automated as you will need to press global hot key to initiate autofill, thus we call the process semi-automatic. To make this all work you need to assign web site URLs to *Link* fields of your login items, so *Password Agent* can match an item to the URL from browser.

Note: If you have multiple files loaded then autofill will search for matching item only from currently selected file. So be sure to switch to proper file before using autofill.

Note: You can change all global autofill hot keys under program settings. In the examples below default hot keys are used.

Step-by-step example

Lets imagine you have an account on eBay auction site and you have an item stored in *Password Agent* titled "*eBay*", your eBay user ID and password are assigned to appropriate fields of the item. To use *autofill matching item* functionality with eBay you need to assign eBay URL to *Link* field of your eBay item.

Just assign eBay URL to *Link* field of your eBay item, so it contains:

`https://www.ebay.com`

In addition to making possible to open eBay web site by **Item | Open link** command, this has added benefit that *Password Agent* can now find your eBay item by the eBay URL.

Now it is time to test how the *autofill matching item* feature works. Keep *Password Agent* running and your data file must be open (not locked). *Password Agent* window can also be on background and minimized.

1. In your web browser open eBay web site (navigate to http://www.ebay.com). Once there **navigate to sign in page, so sign in form is displayed**. If you are already signed in, you need to sign out first for this test.
2. **Set focus to *User name* box by clicking it with the mouse**. That way you select the edit box where *Password Agent* sends your user ID.

3. **Press global hot key Ctrl+Shift+Q** (hold down both *Ctrl* and *Shift,* then press *Q* so you press total 3 keys simultaneously). Note how your eBay user ID and password are automatically filled. When you pressed the global hot key combination then *Password Agent* detected URL of your current web page from active browser, looked up its database for an item whose *Link* field matches to the URL of your current web page and then sent contents of *User ID* and *Password* fields of the matching item to your web page. It all happened very quickly on the background, without you needing to leave your web browser.

If you use different international eBay sites then you need to add all these different site URLs to your eBay item. If you sign into eBay UK and DE then add these international domains as well, separated by space, so contents of the *Link* field of your eBay item looks like this:

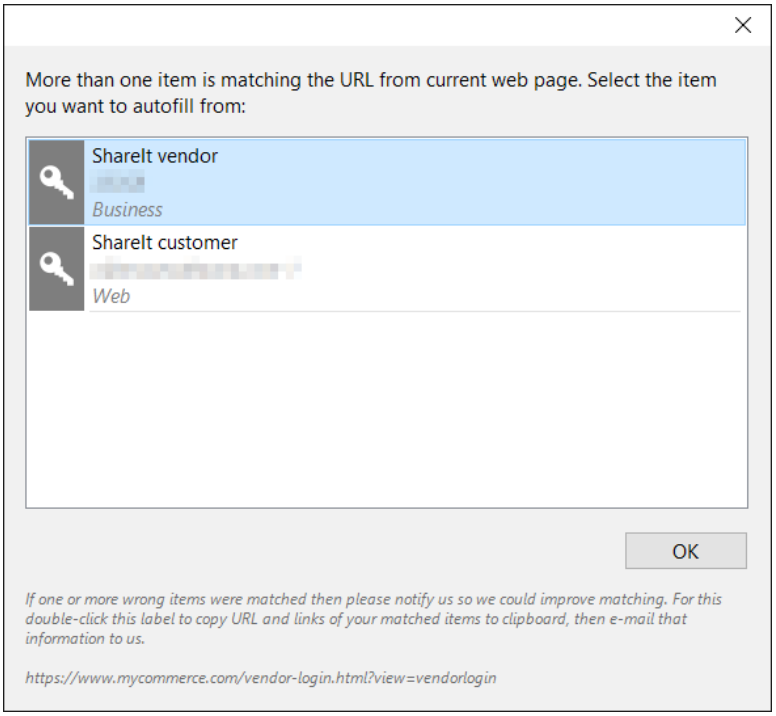
```
https://www.ebay.com https://www.ebay.de https://www.ebay.co.uk
```

Note: If *Link* field contains multiple URLs the first URL is considered default and that is used when you invoke *Open Link command*. Others are only used for matching the item to different web domains.

Note: *Autofill matching item* fills from an item matching to the URL of a web page, not from an item you have currently selected in the item list. Your current item selection is not changed.

When multiple items match the same URL

It may happen that in your data file you have multiple login items that share the same URL, like multiple user accounts that consume the same service or separate private and business accounts of the same service.



Above we see what happens when we want to login at https://mycommerce.com by pressing global hot key to autofill matching item, but *Password Agent* found 2 items that match the link https://mycommerce.com. When it finds more than one matching item it does not know from which one you want to autofill, so it presents window with all the matches and you'll need to manually select the item you want to autofill from. In this example the file had 2 login items for the same web site, one login for private and another for business use. To select the item to autofill from double-click it with the mouse or select it and press *OK*. To cancel autofill press *Escape* key or just close the window.

It is possible to exclude an item from autofill matching. In the example above, if you rarely use the "*ShareIt customer*" login and mainly use "*ShareIt vendor*", then you can mark the "*ShareIt customer*" with *Exclude from autofill matching* flag. On that case the item is ignored by autofill matching function, meaning you'll not see this prompt for this web site. Then "*ShareIt vendor*" item is automatically used to login as it is the only match. You can set the *Exclude from*

autofill matching flag for each item separately on item details panel (in *more details* mode). See topic “Item details panel” on page 17.

Autofill matching item to another application (not a web browser)

You can also autofill matching item to another application, like a FTP client or bookkeeping program, or any other program that requires you to provide user credentials. For this to work you need to add program's executable file name to the *Link* field of an item. For example if you have login item with credentials to log into a FTP server and you use *FileZilla* FTP client program to log into the FTP server, you can write `filezilla.exe` to the *Link* field of the item (use full path to executable, between double quotes, if you also want to run it with *Open link* command). Then when *FileZilla* prompts you for user ID and password to log into the FTP server, you can just press global hot key Ctrl+Shift+Q and *Password Agent* will autofill user ID and password from the item that has `filezilla.exe` assigned to *Link* field. On that case you don't need to use the (insecure) internal bookmark manager of *FileZilla* to store your logins.

Autofill selected item

With *autofill selected item Password Agent* does not try to match *Link* to current application like on case of *autofill matching item*, but just **sends text of an item that is currently selected in the item list**. So no *Link* field is involved and no value needs to be assigned to item's *Link* field to use this kind of autofill. This mode is not automated, so you'll first need to manually select the item to autofill from, meaning you need to switch between *Password Agent* window and your web browser.

Tip: Whenever possible use alternative *autofill matching item* function described above as it offers more automation and does not require you to switch between your web browser and *Password Agent*.

Autofill selected item using hot key

Work-flow to autofill selected item:

1. In *Password Agent* **select the item that matches the web site you want to log into**. You can use search box to find the item quickly.
2. If the item has web site link assigned to *Link* field, you can use *Open Link* command to open the corresponding web page. If not, **open your web browser and navigate to the login page** manually.
3. **Set focus to *User name* box by clicking it with the mouse**. That way you select the edit box where *Password Agent* sends your user ID.
4. **Press global hot key Ctrl+Shift+A** (hold down both *Ctrl* and *Shift, then* press *A* so you press total 3 keys simultaneously). Note how your user ID and password are automatically filled from item selected in *Password Agent*.

Autofill selected item using *Autofill* toolbar button

In older versions of *Password Agent* there was dedicated *Autofill* toolbar button in addition to hot key. As use of the toolbar button for autofill is not very dependable the button is not any more visible on the toolbar by default. You can customize the toolbar to make the button visible again but it is not recommended to use the *Autofill* toolbar button because with the toolbar button window where you want to send text is not well defined, it is last window that was active before you switched to *Password Agent* to press *Autofill* toolbar button. Using hot key is much quicker and requires less steps, especially the new *Autofill matching item* function, described in previous chapter. So use of toolbar button is not promoted and not described in detail here. Please take some practice and learn to use hot keys instead, for your own good.

Listing of all autofill-related global hot keys

On some cases you may need to autofill only *User ID* or *Password* field separately, not both simultaneously. For example a web site may already have populated *User name* field on login page. Then on the web page set focus to the password field and autofill only password. Or user ID and password may be asked on separate pages, so you need to send both one by one.

Autofill matching item (user ID + password)	Ctrl+Shift+Q
Autofill matching item password	Ctrl+Shift+W
Autofill matching item user ID	Ctrl+Shift+E
Autofill selected item (user ID + password)	Ctrl+Shift+A
Autofill selected item password	Ctrl+Shift+S
Autofill selected item user ID	Ctrl+Shift+D
Autofill e-mail address	Ctrl+Shift+F
Bring *Password Agent* window to front	Ctrl+Shift+P

Tip: You can change any of the hot key combinations under program settings. However, do not try to simplify these by using only Ctrl+A for example, such hot keys will conflict with system and application hot keys. Always use Ctrl+Shift and your desired key.

Autofill template and non-standard login forms

Most login forms have two text fields – user name and password. Typical scenario is that you fill both boxes, and then press submit button to log in. *Password Agent* does not parse login forms, it assumes that the web form has same basic layout – user name field and following password field. When filling target login forms *Password Agent* by default sends *User ID*, then simulates *Tab* key press to jump to the next, password field, and then sends *Password*. If you display details panel of an item, then press *More details* button to display all fields of an item, you'll also reveal *Autofill template* field. The default template for login items is the following:

```
$USERID{TAB}$PASSWORD
```

`$USERID` variable will be replaced with your actual data from *User ID* field, `$PASSWORD` variable will be replaced by your actual password and `{TAB}` variable is a special instruction to simulate *Tab* key press.

In addition you can use the `$NOTE` variable to send text from *Note* field. If your form requires you to press *Tab* key several times to jump to correct text field then you need to include the same amount of `{TAB}` variables in your autofill template or use special instruction `{TAB n}` where *n* is number of tab key presses to simulate.

For example, the following slight modification to item's autofill template automatically presses *Enter* key after filling in your form, so the form will be automatically submitted after filling, saving you from need to click *Submit* button on the form. Also, it presses *Tab* key 2 times between *User ID* and *Password*:

```
$USERID{TAB 2}$PASSWORD{ENTER}
```

To insert **pause between sending some fields**, you can use special `{WAIT}` variable. Each `{WAIT}` variable will generate 0.5 second pause. You can also specify length of pause by specifying milliseconds. The following variable will pause for 1 second: `{WAIT 1000}`. Generally, you don't need to use the `{WAIT}` variable, it is provided for special conditions.

You can also **include plain text in template to send some text that is not coming from a field of item:**

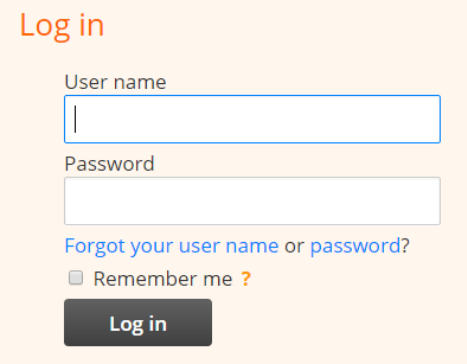
```
$USERID{TAB}Free form text 1{TAB}Free form text 2{TAB}$PASSWORD{ENTER}
```

That may be useful for some advanced login prompts that may require you to provide more info than just user ID and password.

Note: You can change autofill template of each item separately. In addition, under program settings you can modify global autofill template. **Global autofill template is used for all items which do not have custom autofill template**. For example if you want login forms to be automatically submitted by simulating *Enter* key press after sending user ID and password, you can change global autofill template to be `$USERID{TAB}$PASSWORD{ENTER}`

Toggling checkbox on web form using autofill

Sometimes login pages have additional *"Remember me"* type of checkbox next to *"User name"* and *"Password"* fields.



If you want to automatically select *Remember me* checkbox when autofilling *User name* and *Password* fields, you can use the following autofill template for your login item:

`$USERID{TAB}$PASSWORD`**`{TAB}{SPACE}`**

Note there is additional `{TAB}{SPACE}` added to the end of default template. After filling *User name* and *Password* fields, this template simulates *Tab* key press to move focus to *Remember me* checkbox, then simulates *Space* key press to toggle checkbox state. The template above assumes you need to press *Tab* key once to jump from *Password* field to *Remember me* checkbox, but in the reality forms can be different, so you need to first test real keyboard navigation sequence of your web form and adjust your template accordingly. To test keyboard navigation sequence from *Password* field to *Remember me* checkbox first put focus to *Password* field, then press *Tab* key until focus is moved to *Remember me* checkbox. If you needed to press *Tab* key more than once, say 3 times, you can adjust your template to:

`$USERID{TAB}$PASSWORD{TAB 3}{SPACE}`

To test your modified template put keyboard focus back to *User name* field, initiate autofill by pressing global hot key and see if all fields, including *Remember me* checkbox are properly filled.

Disable browser's auto-complete

Most web browsers now have built-in password manager that is enabled by default. To use autofill function you must first disable your web browser's built-in *AutoComplete* of passwords, otherwise both your web browser and *Password Agent* will try to enter password simultaneously, resulting corrupt password to be entered on web form. *Password Agent* will try to detect if target browser's *AutoComplete* is enabled and if so, will notify you (unless you have disabled this notification in program settings).

Note: Typically **built-in password managers of web browsers store your passwords insecure manner** and numerous programs exists that allow someone to retrieve your passwords from built-in password managers, so it is more secure to use *Password Agent* to store your logins. Another plus with *Password Agent* is that you'll get browser independent password storage.

Chrome

To disable AutoComplete in Chrome, open browser Settings and click *Advanced* at bottom of the *Settings* page. Then, click on the *Manage passwords* section, and switch password management service off. Restart Chrome to apply your changes.

Internet Explorer

To disable AutoComplete in Internet Explorer open *Internet Options*, switch to the *Content tab* and then click *Settings* in the *AutoComplete section*. In the *AutoComplete Settings* window, un-check *User names and passwords on forms*, and then click OK.

Microsoft Edge

To disable AutoComplete in Microsoft Edge, open browser *Settings* and click *View advanced settings* at bottom of the *Settings* pane. Then toggle *Offer to save passwords* off.

Firefox

To disable AutoComplete in Firefox, open browser *Options*, change to *Privacy & Security* section at left, and then un-check *Remember logins and passwords for websites*.

Opera

To disable AutoComplete in Opera, open browser *Settings*, change to *Privacy & security* section at left, then locate the *Passwords* section and un-check *Offer to save passwords I enter on the web*. Restart Opera to apply your changes.

Other features

Portable version

Password Agent is a self contained program – no special installation and external run-time libraries are needed. That also means you can just run it off removable drives, like USB flash drives, making is very portable.

Take with me

It is possible to take *Password Agent* and your password database file(s) with you on a removable drive like USB flash drive. That way your passwords and secrets are always with you and you can run the program off the removable disk – you don't have to install it on target computer. Only main executable file and your data file are required to run the program, but can include also program settings and license key files.

Warning: Typing your master password to open your data file on public computers is not safe. Such computers may have key loggers and other unwanted programs installed that can record your keyboard and screen. Instead, it is recommended that you use mobile version if you need to take your passwords with you, although entering a password safely via keyboard remains issue with Windows platform. See topic "How secure?" on page 7.

Take with me function makes it easy to copy and update *Password Agent* files on a removable drive. You need to have your data file open, then select menu command **File | Take with me**. If the *Take with me* command is grayed out, you

don't have a file open (for security reasons you need to have a data file open, otherwise a by-passer could quickly copy your files to a removable disk).

In *Take with me* window you select which files you want to take with you and also destination drive letter where to copy them.

Select items to copy – Select which files you want to copy. The *License key* option allows you to include your license key code, so your program will be always started as *Unlimited* edition, even on computers where there is no *Password Agent* installed. Data files listed here are from your recent files list. If a data file you would like to include is not listed then you first need to open it once in *Password Agent*, causing file name to be added to recent files list and then it will also be listed here next time you invoke *Take with me*.
When copying your data files, previous versions that were in destination drive will be available as *.old* files. So if you accidentally overwrite important data on removable disk, you can still access the *.old* files.

Target disk, disk label or folder – Specify your removable drive, where selected files will be copied. One nice feature here is that you can also specify disk label*, not drive letter. That is useful for drives whose drive letter may change depending how many other removable disks you have connected at the moment. Specifying your USB flash disk label here will insure that files will be copied to it regardless its current drive letter.

** Disk label search will start from letter C, it can't be used with A and B drives. If there are multiple disks with the same label, first of them will be returned.*

Running Password Agent from removable drive

Password Agent has some special features when the program is started from a removable drive:

1. If there is a data file in the application folder, *Password Agent* will open it by default.
2. If there is file with program settings in application folder then this settings file will be used instead of settings file of current computer user (under user profile).
3. If license key file is present in application folder then it will be used, so you can run *Unlimited* edition even if it is not installed on target computer.

To run the program from removable drive execute program file `PwAgent.exe`. If you are running on 64-bit Windows, you can also execute `PwAgent64.exe` instead, if present, but `PwAgent.exe` will load `PwAgent64.exe` anyway if it detects that it has been started on 64-bit Windows.

Command line switches

Password Agent has the following command line syntax (instructions between brackets are optional):

```
pwagent.exe ["file 1"] ["file 2"] ["file n"] [/MINIMIZE] [/LOCK] [/DAKF]
```

File names must include full path, put them between double quotes if path contains space. If file name is specified on command line then that file will be loaded in addition to last used files from a previous session.

/MINIMIZE switch can be used to force the program to start up minimized. That is useful if you want to run it on start-up.

/LOCK switch allows to lock any open files in currently running instance. If you have *Password Agent* already running and you execute `pwagent.exe /LOCK` then already running instance is locked and no new instance is launched.

/DAKF switch allows to disable anti keylogging features in secure edit boxes, like the one used to enter master password. Use only when you get frequent and unjustified "Invalid password" error messages when entering master password.

Export and import XML/CSV

Warning: If you need to migrate your *Password Agent* data file from one computer to another don't use import and export! Import and export are designed to move data between different programs from different manufacturers and these actions may cause loss data. Instead, see "How to migrate data to different computer" on page 35.

Export

Warning: When you use data export to common XML or CSV format, resulting file, including all your passwords, is in plain text and readable by anyone with a text editor. So such files must be immediately deleted after use. See topic "Possible plain text leaks" on page 9 for more details.

The menu command **File | Export** will show *Export* window.

Available output formats:

XML –XML is the best export format if you want to transfer your data to another program or database. With XML you can export folder hierarchy and folder and item IDs which are not exported in case of CSV format. Date values are exported in `xsd:dateTime` format without time zone (`2002-05-30T09:00:00`).

CSV – Comma-separated values (CSV) is a basic data interchange format. Resulting CSV file conforms to RFC4180. Resulting file has no optional header line. No double quotes are used around fields unless field contains CRLF, comma or double quote ("). If field contains double quote (") then that double quote is escaped by another double quote. Date values are exported in format specified by user locale.

Import

Coming soon.

Multiple users on one computer

Multiple users can use *Password Agent* in one computer without problems. Since *Password Agent* can operate with different data files, every user can create a personal data file, if desired.

If each user has separate Windows account then there are no special steps to take. On that case each user can also customize *Password Agent* to his/her liking as program settings are stored per user.

If each user does not have separate Windows account then for example every user can place shortcut to his or her file on the Desktop (open desired file, then use the **File | Create shortcut on Desktop** command). Next time the user wants to access his/her file, he/she can just double-click the shortcut and given file is loaded in *Password Agent*. On this case program settings are shared between all users as the program actually runs under one Windows user account.

FAQ

Where is my data stored?

When you first create a data file and assign master password to it, you choose a file system folder where it will be saved. Default location offered by the program is your *Documents* folder, but you can select any other writable folder. Over

time you may forget where your file was stored because *Password Agent* automatically loads last used file on start-up, so there is no need to manually select a file to load.

To see data file location of a file that is loaded to *Password Agent*, choose menu command **File | Open file location**. For security purposes that command is only enabled when the file is unlocked.

If you have no files open in *Password Agent*, you can open **File | Open recent** sub-menu and see, if there are some last used files listed there.

If the list of recent files is empty you can search your file system for all *Password Agent* data files by the file extension *.pwa*

Where is my license key stored?

When license key is entered by menu command *Help* | *Enter license key* then file `PwAgent.key` is created in user profile folder or application data folder, depending if it is being installed for current user or all users of the computer.

If the license key was entered for current user, then `PwAgent.key` file is stored under your roaming user profile `%APPDATA%\Moon Software\Password Agent`. It is the same folder where settings file is stored. That path resolves to `C:\Users\<YourUserName>\AppData\Roaming\Moon Software\Password Agent`. You can use menu command *Tools* | *Locate settings file* to open the location.

If the license key was entered for all users, then `PwAgent.key` file is stored under `%PROGRAMDATA%\Moon Software\Password Agent`. That path usually resolves to `C:\ProgramData\Moon Software\Password Agent`. Until version 2017.12.12 license key for all users was stored in the registry and these older versions do not find shared license key from `%PROGRAMDATA%`.

When Password Agent looks for license key file, it checks 3 folders for presence of `PwAgent.key` file. First it checks folder of program executable file (special case for deploying on removable media or by file server), then current user profile under `%APPDATA%` and last shared profile under `%PROGRAMDATA%`. First found key file is loaded, which makes it **possible to override a key file installed for all users in `%PROGRAMDATA%` with a key file for specific user** by putting different key file to user's `%APPDATA%` folder.

Note: If Password Agent is started as administrator (page 35) then location of already installed license key can be changed by *Help* | *Enter license key*.

See also topics "Portable version" (page 31) and "Error: Reference source not found" (page Error: Reference source not found).

I have lost my license key

If you have no access to your license key as described in topic above then you may be able to retrieve your license key at out web site:

http://www.moonsoftware.com/lookup

Where are program settings stored?

Menu command **Tools | Locate settings file** locates your settings file.

Program settings are stored in `PwAgent.ini` file under your roaming user profile:

`%APPDATA%\Moon Software\Password Agent`

That path resolves to `C:\Users\<YourUserName>\AppData\Roaming\Moon Software\Password Agent`.

If `PwAgent.ini` is missing from that folder then default settings are used.

If there is `PwAgent.ini` in the application folder then that settings file is used instead the one from user's profile. That makes *Password Agent more* portable. See topic “Portable version” on page 31.

How to migrate data to different computer

Migrating data is quite easy as all your items and folders are stored in a single data file. It is also possible that you have created more than one data file. By default data files are created in your *Documents* folder but real location can be different and specified by you when you created you files.

If the files you want to migrate are open in *Password Agent* then use menu command **File | Take with me**. In *Take with me* window mark files you want to copy by checking checkbox of desired files and select target removable drive you want use for transfer of the files. Don't copy program files.

If your data files are not loaded in *Password Agent* then see topic “Where is my data stored?” on page 33, that helps you to find your data files. Copy your data file(s) to your removable drive.

On second computer:

1. Install *Password Agent Lite.* You can download the latest version from our homepage.
2. Copy your data file(s) from removable drive to your *Documents* folder.
3. In *Password Agent* use menu command **File | Open** and select your data file(s) you just copied to *Documents* folder. Now unlock screen of the file(s) will be displayed in *Password Agent*.
   If you need to copy your license key manually from source computer then you can see your installed license key by **Help | Enter license key**. You can also copy your license key file, see topic “Where is my license key stored?” on page 34.

Why there is delay when unlocking a file?

When generating key from user's master password high number of rounds is now used by key derivation function (KDF) to create intentional delay. That means by default key is calculated about 200000 rounds, which makes it more time consuming for an attacker to try different passwords in brute force attack. Iteration count that causes the delay can be changed by menu command **File | Master password & encryption settings**. It is recommended to keep iteration count such that it will cause at least 0.5 second delay, actually best is as high as is tolerable when opening files. You can also set iteration count to a low value to eliminate the delay but that is not recommended as it weakens security.

Note: Mobile devices have less computing power, so calculating a key on a mobile device will usually take few times longer than on a desktop PC. If you also use mobile device you'll need to keep that in mind when specifying iteration count.

I have forgotten master password, what now?

If you have forgotten your master password then first don't panic too much – it is possible that you'll recall it later. However, if you have really forgotten it and are unable to recall, then please understand that there is no way to open your data file without valid master password.

The program does not have any “back doors” and we can't magically “reset” your file if you have lost your master password, so be careful. Your master password is not stored in data file, only a “fingerprint” of it, so it is not possible to “retrieve” it from your file.

How to run as administrator

On few occasions (setting up file associations with the shell, entering license key for all users) you may have need to run *Password Agent* with administrator rights. By default Windows Vista/7/8/10 execute programs under limited user account even if you are logged in as administrator. This new feature is called User Account Control (UAC) and it is a good feature to minimize damage malicious program can make.

Warning: It is important that you only run *Password Agent* as administrator for certain tasks only, not always. Running it always as administrator is a security risk and should not be done.

To start *Password Agent* as administrator:

Windows 10

1. Be sure *Password Agent* is not currently running (even in system tray)
2. Open Windows Start Menu (Ctrl+Esc from keyboard)
3. Locate *Password Agent* icon or if it is not visible then start typing "password" and it will be revealed as search result.
4. Right-click on *Password Agent* icon, context menu is displayed. In this menu you see *Run as administrator* command among others, or if it is not directly visible then there may be *More* sub-menu that contains also *Run as administrator* command. Click *Run as administrator*. If *Run as administrator* is not visible click *Open file location*, then right-click already selected file to see pop-up menu and choose *Run as administrator* from that menu.
5. Windows asks for confirmation by displaying *"Do you want to allow the following program to make changes to this computer?"* and shows program name *"Password Agent"*. Click *YES*.
6. Now *Password Agent* is running with administrator rights.

Windows 8

1. Be sure *Password Agent* is not currently running (even in system tray)
2. Go to home screen (press Ctrl+Esc to go to home screen from desktop)
3. Locate *Password Agent* icon on home screen or if it is not visible then start typing "password" and it will be revealed as search result.
4. Right-click on *Password Agent* icon and note that on bottom of home screen new button bar is displayed. On this bar you see *Run as administrator* command among others. Click *Run as administrator*. If *Run as administrator* is not visible click *Open file location*, then right-click already selected file to see pop-up menu and choose *Run as administrator* from that menu.
5. Windows asks for confirmation by displaying *"Do you want to allow the following program to make changes to this computer?"* and shows program name *"Password Agent"*. Click *YES*.
6. Now *Password Agent* is running with administrator rights.

Windows Vista and 7

1. Be sure *Password Agent* is not currently running (even in system tray)
2. Right-click on icon you use to launch *Password Agent* and choose *Run as Administrator* command from pop-up menu.
3. Windows asks for confirmation by displaying *"Do you want to allow the following program to make changes to this computer?"* and shows program name *"Password Agent"*. Click *YES*.
4. Now *Password Agent* is running with administrator rights.

For more background information about User Account Control (UAC) see official Microsoft document.

How to start with default settings

If program settings file gets corrupt or main window is off the screen (main window is not displayed but you see program as running on taskbar) **you can start *Password Agent* with default settings when you hold down *Shift* key while starting the program** (from a shortcut or executable). If *Shift* key is held down during *Password Agent* start-up then it will prompt you to load default settings.

Or, you can also delete program settings file (be sure to close running instance of *Password Agent* first). See topic "Where are program settings stored?" on page 34.

Note: If you are able to run the program so you see its main window then you can load default setting for specific items in program *Settings* window. For that right-click a setting and choose *Load default value* from context menu. Or, you can load default values for all settings on selected tab by pressing *Restore defaults* button on bottom of the window.

How to revert to older version of data file

Important: Here we restore an older version of data file, which is likely missing latest modifications. To restore the latest version you should always restore your original data file from backup. If you specified alternative file locations in *Backup* section of program settings then *Password Agent* always copied data file to alternative location after saving.

Previous versions of data file have extension *.old* plus number, like *.old1*, *.old2* etc. These version files will be kept in the same directory as your data file. Newest old file version has extension *.old1*, others are older in increasing order. For example *.old5* file does not contain last 5 changes. The number of available old file versions depends on *Number of old files to keep when saving* program setting.

You can open an .old file to see its contents and to test if it is readable and un-lockable with your master password. For this invoke menu command **File | Open** and in the *Open* dialog select file type as *Old data files (*.old)* instead of default *Data files (*.pwa)*. Then only old version files are listed and you can select one to open. Old version files will be only opened in read-only mode.

You can manually rename file extension *.old* to *.pwa*, then you can start using it as your data file.

It is also possible to revert to old file by Password Agent interface:

1. Open old file you want to revert to using **File | Open** window as instructed above, then unlock it with your master password.
2. Select menu command **File | Revert to .old file** (this command is only visible if you have unlocked your old file). After confirming your data file will be reverted to selected old version. Your original .pwa file will be renamed to .delete file, which will be automatically deleted after 30 days.

Solving common problems

Autofill does not send anything

The autofill feature is popular and powerful, but it may not work with all applications. Autofill is basically sending simulated keyboard input to another program, but depending on design of the target application, that may not always work. Some programs can't process keyboard input so quickly, others are not designed for this kind of input etc. While the autofill feature works with majority of applications, there may be some that do not accept input that way.

If autofill to certain application completely fails – nothing is sent. First, for autofill to work you need to put input focus in destination application to text field where you want autofill to type text for you. That means you need to click the field with the mouse or press *Tab* on keyboard until caret starts blinking in the field, usually *User name* field. Only after that you can press global autofill hot key to initiate autofill.

Recent *Windows* versions contain feature named *User Interface Privilege Isolation* (UIPI). Among other things this means that you can't send user input into another application that runs with higher privileges that your application. Or in other words, if you run *Password Agent* as limited user (or you are administrator under UAC), then you can't autofill to another application that has been started as administrator (and currently runs with administrator privileges). On that case *Windows* does not allow this kind of communication and silently "eats" autofill, so it will never reach destination application.

Also it is possible that **autofill does not work with certain application**, but works with others – then usually the problem is not in *Password Agent*. The target program probably uses non-standard input boxes that do not accept simulated input very well. If only part of the data (user ID or password only) is transferred to the target application, then you can try adding `{WAIT}` variable to your autofill template, something like `$USERID{TAB}{WAIT 500}$PASSWORD{WAIT 500}`. That will just give the target application a bit more time to process pending input. If that does not work, then you are out of luck and this application can't be used as autofill target. It is also possible that you need to press *Tab* key multiple times to move input focus from one field to another. See "Autofill template and non-standard login forms" on page 29.

Tip: To figure out whether *Password Agent* misbehaves or is it your target application, try using *Notepad* as the target application. Run *Notepad* with a new text file, then select an item in *Password Agent*, switch back to *Notepad* and press *autofill selected item* hot key Ctrl+Shift+A to send *User ID* and *Password* fields of selected item to *Notepad*. If everything is sent to *Notepad* properly, autofill generally works but you'll need to figure out why the target application does not accept input sent from *Password Agent*.

Autofill works but login (sometimes) fails

If you use autofill function then you must disable your web browser's internal *AutoComplete* setting for passwords, otherwise both your web browser and *Password Agent* will try to autofill your password at the same time, rendering the password invalid.

See topic "Disable browser's auto-complete" on page 30.

Command "Open link" does not open web pages

First, all your web site URLs assigned to *Link* field must start with "*http://*" or "*https://*", so link must be in form "***http://www.moonsoftware.com***" and not "*www.moonsoftware.com*".

If you have links in proper format then the problem likely is that you have no default web browser properly set. Try to set your favorite web browser as default browser again:

Chrome – Start *Chrome*, open *Settings* via menu button. Press *Make Google Chrome the default browser* button at bottom of settings page, in *Default browser* section.

Internet Explorer – Start *Internet Explorer, s*elect menu command *Tools* | *Internet Options*. Change to *Programs* tab. See the state of *Internet Explorer should check to see whether it is the default browser* checkbox. If it is not selected, then select it and press *OK* button. If it is already selected, then un-select and press OK. Now do everything starting from step 1 again.

Firefox – Start *Firefox*, select menu command *Tools* | *Options*. Note the *Default Browser* section in *General* tab. Be sure *Firefox should check to see if it is the default browser when starting* checkbox is checked. You can also test the association by pressing *Check Now* button. Press *OK* to close *Options* window. Close all *Firefox* instances and start it again.

Now try to *Open link* command in *Password Agent* again.

If the previous steps did not give desired result, you can also select a system default web browser globally from *Control Panel*. This action requires administrator privileges for current user.

1. Open *Add or Remove Programs* applet from *Windows Control Panel*.
2. Switch to *Set Program Access and Defaults* section by clicking that button on left side of the window.

3. In the *Choose configuration section* select *Custom* option and press arrows on right side of the window to expand that section downside.
4. In *Choose a default web browser* section select the browser you want to use and also be sure *Enable access to this program* checkbox is selected.
5. Press *OK* to close *Add or Remove Programs* window.

Web links open in the same browser window

By default *Internet Explorer* may open links in an existing browser window, not in a new blank window. If you prefer that *Open link* command should launch your web sites in new browser windows, follow these steps:

1. Start *Internet Explorer*, then choose **Tools | Internet Options**
2. Change to **Advanced** tab
3. In the list, under **Browsing** node unselect **Reuse windows for launching shortcuts** checkbox
4. Press **OK**

Jerky scrolling of item list

Password Agent keeps your secret data in memory in encrypted form and needs to decrypt everything you see on screen each time screen is updated. For example if smooth scrolling feature wants to update item list 50 times per second to create smooth scrolling effect, all text you see displayed in item list needs to be decrypted also 50 times per second. If you have high resolution monitor, processor may not be able to decrypt everything so quickly, resulting list being updated not so smoothly.

If scrolling the item list is too jerky you can disable Windows' *smooth-scrolling* feature. Smooth scrolling is enabled by default but unfortunately does not work so smoothly in many applications, including *Password Agent*.

To change Windows' *smooth-scrolling*:

1. Open *System* applet in *Windows Control Panel*
2. Switch to **Advanced** tab
3. In *Performance* group, press **Settings** button
4. On *Visual Effects* tab, unselect **Smooth-scroll list boxes**
5. Press **OK**

Deployment

Installer command line parameters

Installer in form of EXE file is made using Advanced Installer 12 and is MSI installer with EXE bootstrapper.

EXE setup file

Advanced Installer comes with a Setup program which can be used as a Bootstrapper. This is useful if you want to create an EXE installation package or if your package has some prerequisites.

If you build your EXE setup with the installation files outside (MSI, CAB etc.), the Bootstrapper will use an INI file to store its settings. It can also receive command-line options.

Standard command-line switches

The EXE Bootstrapper supports all msiexec command-line options (basically all the command-line parameters you can use for an MSI package). A command-line received by the EXE Bootstrapper will be passed to msiexec when launching the main MSI. This command-line overrides the one specified in the "Install Options" from the Configuration Settings Tab.

"//" marker

The // marker is automatically replaced by the EXE Bootstrapper with <path_to_msi>. Msiexec command-line parameters need to be appended to this command.

Example of an uninstall command passed to the EXE Bootstrapper:

```
C:\Setup.exe /x // /l*v install.log
```

The command above will be automatically converted by the Bootstrapper to:

```
msiexec.exe /x C:\Setup.msi /l*v install.log
```

Caution! The // sequence of characters is not supported when used in a property value set by the Bootstrapper command-line. If you want to use this sequence (for example a URL which starts with "http://"), you can add the | character in front of //. This way, you will have something like http:|//.

To learn more about how pass commands to your MSI and MSP packages see the Msiexec page.

Proprietary command-line switches

These commands affect only the language selection dialog and the dialogs in the prerequisite wizard. To also affect the MSI package please use the standard MSIEXEC command-line parameters. Note that the MSI parameters must come after the Bootstrapper parameters.

```
/extract <path>
```

Extracts the MSI contained by the EXE to the specified location. The full path to an existent folder is required. If the path contains spaces you must enclose it in quotes:

Example

```
Mypackage.exe /extract "C:\My work"
```

This command will extract the Mypackage.msi file in the "My work" folder.

```
/? and /help
```

Both these commands will display a help dialog containing the command-line options for the EXE setup.

```
/exenoui
```

Launches the EXE setup without UI.

```
/exebasicui
```

Launches the EXE setup with basic UI. The UI level set using the above command-line options will overwrite the default UI level specified when the package was built.

```
/listlangs
```

Lists the languages supported by the EXE setup.

`/exelang <langId>`

Launches the EXE setup using the specified language. This command-line option will have effect only if the EXE setup was built with the language selection dialog. You can use both a UI level and /exelang command-line options at the same time.

`/username`

Sets the username used by the proxy server in case the Installer needs Internet access. This command is deprecated, and you should use /proxyusername instead.

`/password`

Sets the password used by the proxy server in case the Installer needs Internet access. This command was deprecated and you should use /proxypassword instead.

`/proxyusername`

Sets the username used by the proxy server in case the Installer needs Internet access.

`/proxypassword`

Sets the password used by the proxy server in case the Installer needs Internet access.

`/exelog <path_to_log_file>`

Creates a log file at the specified path with the specified name. If a path and name are not specified, then the log file will be created next to the EXE installer having the same name as the installer and the extension .log.

`/exenoupdates`

Using this switch will force the Bootstrapper to cancel/discard the update checks if any is declared in the Updater Page.

Command-line switches order

When passing proprietary command-line parameters to an EXE setup, you cannot mix them with the standard MSI ones. The correct order is to first specify the proprietary EXE switches and then the standard MSI switches.

For example, a correct command-line would be:

```
Setup.exe /exelang 1033 /exenoui /qn /norestart
```

as opposed to an incorrect command-line:

```
Setup.exe /norestart /exelang 1033 /exenoui /qn
```

Return code

The EXE Bootstrapper will return -1 if the user presses the "Cancel" button, while installing the prerequisites. Otherwise, it will show the code returned by MSIExec.exe after running the main MSI.

Important! The Setup EXE provides the MSI it launches with the SETUPEXEDIR property which contains the folder path from where it was executed.

Network installation

Due to simple self-contained design that does not require external dependencies it is very easy to make *Password Agent* available over network from file server.

1. Create new shared directory on your file server, you can name it “Password Agent”. Lets call it shared application directory for now on. Set network users access permissions of this directory to read-only.
2. Copy *Password Agent* program files installed by the installer (from `C:\Program Files\Moon Software\Password Agent`) to your shared application directory. At minimum executable files `PwAgent.exe` and `PwAgent64.exe` are required, although copying all files including documentation is recommended.

3. Copy license key file `PwAgent.key` to your shared application directory, then each user who starts the program remotely will automatically run *Unlimited* edition, not *Lite* edition and there is no need to enter license key on each workstation. See topic “Where is my license key stored?” on page 34 for more info about license key file.
4. Optional: If you want all network users to use the same specific program settings then you can copy settings file `PwAgent.ini` to your shared application directory. If you do that then users will not be able to permanently change program settings – on next session the settings from this file are used again because if user exits the program, the program is unable to write settings file back to this settings file – your shared application directory is read-only. You can delete some data like recent file history from the settings file, otherwise it will be shared to all network users. If settings file is not present in shared application directory then *Password Agent* creates private settings file for each network user under user's roaming profile. See topic “Where are program settings stored?” on page 34 for more info about program settings.

Now network users can start *Password Agent* from your shared application directory by running `PwAgent.exe`. If the executable detects that user has 64-bit Windows then it will automatically launch `PwAgent64.exe` instead.

Note: When a new version of *Password Agent* is released don't forget to update program files on your shared directory, otherwise network users will have older version.

Note: When sharing *Password Agent* on server, **you’ll need license for each user** who runs the program off the server. Cost effective multi-user and site licenses are available.

How to buy

How to buy

Password Agent is distributed as free limited *Lite* version. See topic “Lite vs. Unlimited edition” on page 7 for more information.

To buy *Unlimited* edition of *Password Agent* please visit our online store at:

http://www.moonsoftware.com/store

You’ll usually get your personal license key within minutes after placing order!

On purchase you'll receive personal license key that entitles you free program updates for the following 365 days (1 year). After 365 days you'll not get more free updates but your existing version will keep working. Then you can upgrade your license for another year if you wish to get updates.

Entering a license key

After purchasing *Password Agent* you will receive a personal license key. You need to enter this key code into *Password Agent Lite* to turn the *Lite* edition to the *Unlimited* edition.

To continue you need to have the free *Password Agent Lite* version installed.

To enter your key code, follow these steps:

1. Run *Password Agent Lite*. **Important!** If you want to make *Password Agent Unlimited* available to all Windows user accounts on your computer then you need to run it as administrator (see topic “How to run as administrator” on page

35). If your computer only has one user account or you only want to make it available only to your current account then there is no need to run as administrator.

2. Choose menu command **Help | Enter license key**. A window to input your license key will be displayed.
3. Copy your multiline license key block, which consists of name and numbers, from e-mail and paste it to the window. If you type manually then use the same capitalization, punctuation and spacing as in the e-mail – if you make one mistake the key will not be accepted.
4. If you are running *Password Agent* as administrator you can make choice whether to enter the license key for current user only or for all user accounts of the computer. If the radio buttons are disabled the license key will be installed for current user account only.
5. Press the **OK** button. You will see a message that tells if the procedure was successful. If the license key was entered correctly your "licensed to" name along with other information will be displayed in the **Help | About** window.

Note: It is usually not possible that a license key you received from us when purchasing the program is not accepted. If the program is telling you that your license key is invalid, first check if you are entering it into the right version of *Password Agent*. That means serial numbers of version 1 or 2 of *Password Agent* do not work with newer version of the program. You need to buy upgrade if you want to use newer version. But if you are sure your program version is right, then just be sure you enter your license key block exactly as it appears in the e-mail. It is **case sensitive** and must be entered exactly as it appears.

Tip: Print out the entire e-mail that contains your license key and order number for future reference. You will need this information again when you reinstall Windows, or want to install *Password Agent* on a different computer.

See also topic "Where is my license key stored?" on page 34.

Uninstalling

The following steps remove the program from your system, but your data files will remain on their present location. You can delete your data files manually, if required.

1. Open the *Add/Remove Programs* applet in *Windows Control Panel*
2. Find the *Password Agent* entry in the list and select it.
3. If you are reading this documentation on screen then note step 4 and then close this document file. Otherwise the uninstaller cannot delete it from your system because it is in use.
4. Press the *Remove* button to start removing the application.