

Manual

PROTECTORION

Universal Encryption Suite



<http://en.protectorion.com>

info@protectorion.com

This Manual is made available with the software Protectorion within the framework of an end user license agreement of the producer of the software Braincell consult & research GmbH. It is only allowed to be used in accordance with the license agreement. All rights reserved, in particular the right of copy, dispersion, modification as well as translation. Excluded are those cases, which are explicitly permitted by the license agreement. This manual is also copyrighted when it is not made available in connection with a license agreement. The content of the manual can be modified at any time without prior notice by the producer. For inaccurate information or incomplete content in this manual and thereof possible resulting damage (e.g. damage to or loss of data), no liability and/or warranty whatsoever is assumed. Protectorion is a registered trademark in the European Union. The holder of trademarks rights is the Braincell consult & research GmbH. Should other trademarks be used in this manual, this happens exclusively in order to indicate the ownership of the corresponding products and services by the relevant trademark holder. Windows®, Windows XP®, Windows Vista®, Windows 7®, MS Office® and MS Word® are brands and/or registered trademarks of the Microsoft Corporation in the USA and/or other countries. Adobe® and Acrobat Reader® are brands and/or registered trademarks of Adobe Systems Incorporated in the USA and/or other countries.

Table of contents

1.	Protectorion for PC, cloud, network, external device	2
2.	Installation on computer	3
3.	Installation on external device	3
4.	First steps.....	3
4.1	Username, master password and password hint	3
4.2	Safe creation	3
4.3	Safe manager	4
4.4	Copy data to file safe	5
4.5	Export as unencrypted from the file safe	5
4.6	File location of data in the file safe	5
5.	Working with the file safe	6
5.1	Manage data	6
5.2.	Delete data	6
5.3	Protect data	6
5.4	Customize user interface	7
5.5	Navigate the file safe	7
5.6	Standby mode	7
5.7	Activate/deactivate password inquiry on PC	7
5.8	Copy between two file safes	7
6.	Working with the password safe.....	7
6.1	Open password safe	8
6.2	Create passwords and groups	8
6.3	Sign in via Fast-Login	8
6.4	Password backup	9
6.5	Encrypted passwords in the cloud/on a network	9
6.6	Position of the password safe	9
7.	Create a cloud or network safe (multiuser)	9
8.	Protectorion in multiuser operation	11
9.	Change password/username	12
10.	Rename safe or safe location	12
11.	Create backup of safe configuration	12
12.	Configure options	12
13.	Quit Protectorion	12
14.	Update Protectorion	12
15.	Uninstall Protectorion.....	12
16.	Buy Business Edition	13

Welcome to Protectorion Encryption Suite!

From the time of the first computer networks to the birth of the Internet was a mere 30 years. From huge amounts of data in data banks to social networks and Smartphones, everything today is connected. However, these new possibilities also harbor many dangers. In the third millennium cybercrime and cyberespionage are no longer mere buzzwords but serious realities.

Hackers engage in raids, the booty is confidential data, passwords and credit card information. For experienced hackers, common security measures are no obstacle. With the help of viruses, trojans, rootkits and keyloggers they manage again and again to access computer systems, cloud storage and networks to misuse sensitive data. Coworkers and flatmates, led by curiosity, pose a threat to confidential data as well. Confidential data lands unencrypted in the cloud and sensitive information saved on company networks becomes accessible for everyone. Avoid having your sensitive data fall prey to criminal intrigue and contemporary curiosity.

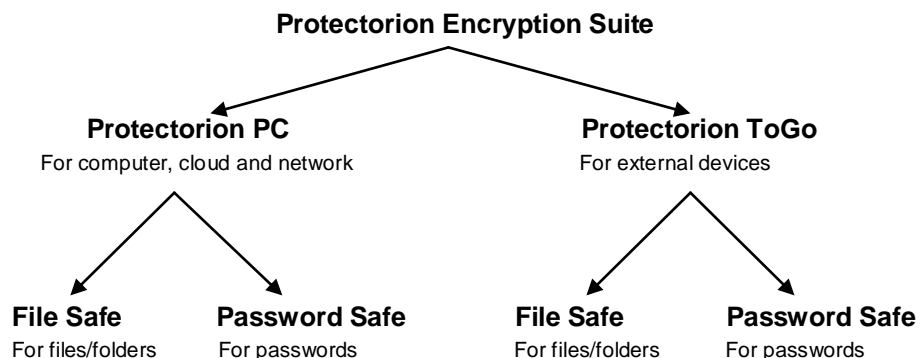
Not only is your computer at home or in the office at risk, but also laptops, which can be stolen, and USB-sticks, which can be lost. Protectorion works on USB-sticks and external devices to keep your data safe, no matter where it is stored!

Protectorion protects your files, folders and passwords! Use Protectorion on a PC, in the cloud, on a network and on external devices to keep data safe as an individual user or to manage encrypted data and password with others in the cloud or on a network drive.

1. Protectorion for PC, cloud, network, external device

Protectorion comprises **Protectorion PC** and **Protectorion Togo**. **Protectorion PC** is for use on a computer, in the cloud and on a network. **Protectorion Togo** works on USB-sticks and external drives.

Protect confidential files and folders by putting them in the **File Safe**. The **Password Safe** serves to protect usernames and passwords.



2. Installation on computer

After downloading Protectorion, install it on your computer by following the installation program's instructions.

Once the installation is complete, **Protectorion** is ready for use on your computer. Click on the Protectorion icon on your Windows® desktop to start **Protectorion**.

3. Installation on external device

Often confidential information is stored on USB-sticks and external drives. For these devices, use **Protectorion ToGo** to protect your data.

First, install **Protectorion** on your computer. Start **Protectorion** and click in the **Safe Manager** on the tab **Protectorion ToGo** or **Protect external devices** to install **Protectorion ToGo** on external devices (e.g. USB-sticks). When you activate the ToGo installer, a quick explanation on how to install and use Protectorion ToGo on external devices will appear.

4. First steps

4.1 Username, master password and password hint

Immediately **create** your **username**, **master password** and **password hint** after the initial startup of Protectorion. The master password protects all your data in Protectorion. This password grants access to the data in the file safe and the password safe. Choose a password that is easy for you to remember, but difficult for others to guess.

When choosing a password, consider the fact that a longer password, which includes a combination of letters (upper- and lowercase), numbers and special characters, offers a higher level of security. See Protectorion's security index to determine the strength of your password.

Master Password	Security
6 or 7 characters, with at least 2 numeric or special characters	very weak
8 or 9 characters, with at least 2 numeric or special characters	weak
10 or 11 characters, with at least 2 numeric or special characters	average
12 or 13 characters, with at least 2 numeric or special characters	strong
14 or 15 characters, with at least 2 numeric or special characters	very strong
16+ characters, with at least 2 numeric or special characters	excellent

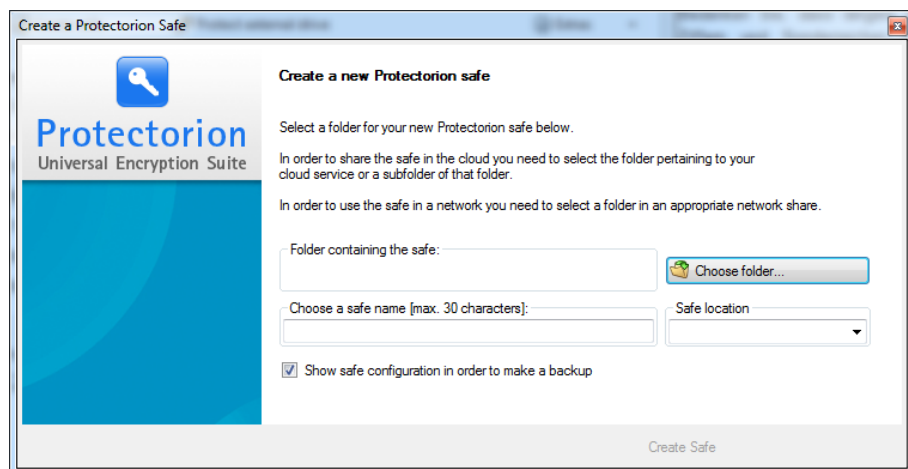
Be sure to remember your master password and keep it confidential. You will be prompted to enter this password when you open Protectorion and to access the data in the safe. You can change the master password at any time in the future.

Should you forget the master password, the **password hint** serves as an aide to recall your password.

The **username** is necessary when multiple users access a safe in the cloud or on a network, and when an individual accesses encrypted data on a cloud or network safe from various computers (**multiuser operation**).

4.2 Safe creation

After selecting a username, master password and password hint, the **safe creation** assistant opens automatically. Follow the instructions and select the **place**, where the safe should be created:



a. On a computer for personal use:

Select a folder on your PC, where you would like the Safe to be created.

b. In the cloud (e.g. Dropbox, MS Skydrive, Google Drive)

Select a folder, in which the content is synchronized with cloud storage (e.g. the Dropbox, Skydrive or Google Drive folder). Files that you later copy in the cloud safe are first automatically encrypted and then synchronized with cloud storage. This way your files in the cloud are protected from unauthorized access.

If necessary, you can grant other individuals access to encrypted files and passwords in the cloud safe and access these yourself from different PCs (**multiuser operation**).

c. On a network

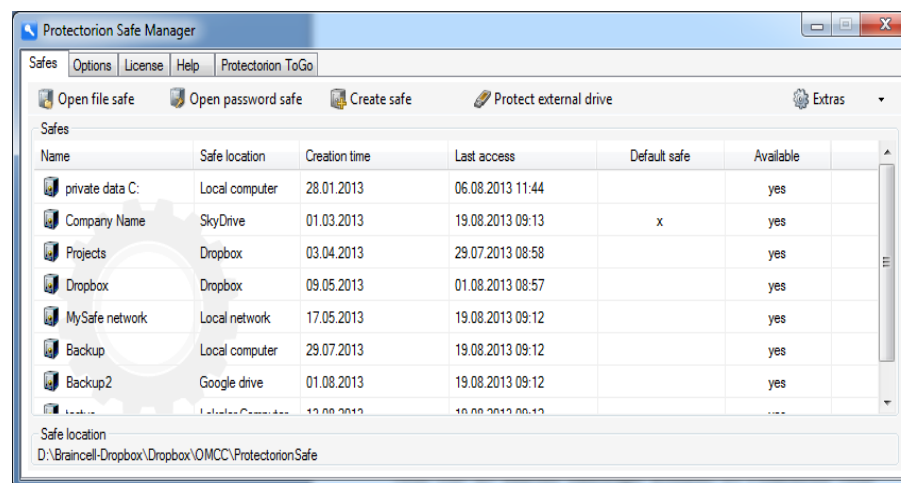
Select a folder on a network drive. Files that you later copy to the network safe are automatically encrypted before they are saved on the network. This way your files on the network are protected from unauthorized access.

If necessary, you can grant other individuals access to encrypted files and passwords in the network safe and access these yourself from different PCs (**multiuser operation**).

Give the safe a meaningful **name** (e.g. Dropbox safe Company name). It is advisable to make a backup of the safe configuration. This has all the critical information related to your safe, namely your master password and the 40-character safe key, with which you can restore the safe, if necessary.

4.3 Safe manager

After you have created the safe, it will be registered in the **Protectorion Safe Manager**. A list of all safes, which you have created, is listed in the safe manager.



Protectorion's **Safe Manager** offers an overview of created safes and provides easy safe management. Use the safe manager to access, create, delete and rename safes, and to send safe invitations.

4.4 Copy data to file safe

Just like a traditional safe, objects are only protected when they are physically inside of the safe. In order to protect data in the file safe it is therefore necessary to first copy the data to the safe. Data is copied with Protectorion in the same manner as you are used to in Windows®.

First, open your file safe. Drag files and folders with the mouse from Windows® to the file safe (**Drag & Drop**) or use copy and paste (CTRL + C and CTRL + V). Additionally, this can be done by highlighting the file in Windows®, right-clicking with the mouse and selecting "**Import to <Safe name> and protect**" in the list.

Protectorion now copies the selected data to the file safe. After the data is successfully copied, you will see it in the safe. It is automatically encrypted and immediately protected with your unique **master password** and **safe key**. Without this master password and safe key access to the information in the file safe is impossible.

After the data is copied to the file safe, it still exists in Windows® as before. The original data in Windows® (source data) is located outside of the file safe and is **not protected**. Therefore Protectorion asks if you want to delete the source data in Windows®.

If you **Delete the source data**, it will be permanently deleted in Windows®. It is not possible to recover the data in Windows®, even with special software. Your data now only exists in the file safe and is protected there.

4.5 Export as unencrypted from the file safe

In the file safe, use the function "**Export as unencrypted**" (Main menu "file" or by clicking with the right mouse button on the desired file or folder) to decrypt data and copy it from the file safe to Windows®. Select the file location in Windows® to which the selected data should be exported.

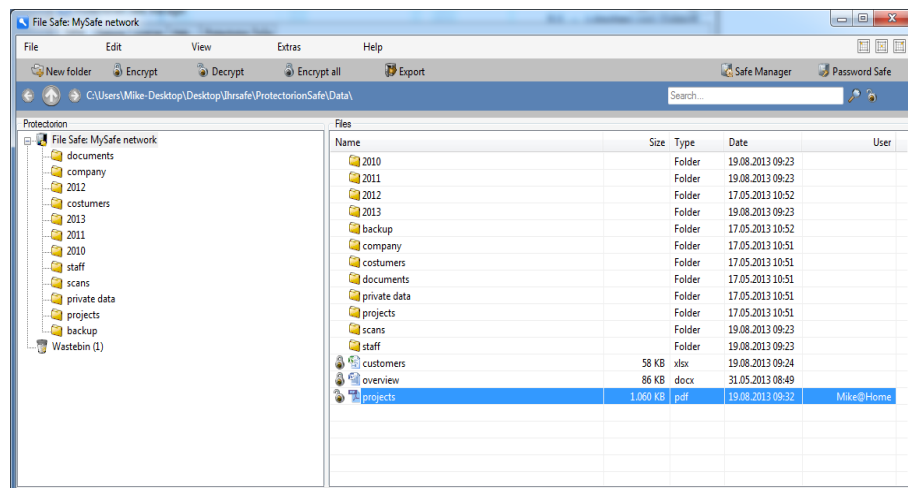
4.6 File location of data in the file safe

You see the file location of your data in the file safe in the *Folder view* directly under the Toolbar. The folder view is dynamic. That means that the folder shown is always up to date. In the Main menu option *View*, you can select between **long and short folder view**.

When you navigate with Windows® Explorer in this folder, you can see that the content and names of the files and folders are encrypted. This data can neither be opened, nor modified, outside of Protectorion! Additionally, the real names of the files and folders in the file safe are only readable in Protectorion.

5. Working with the file safe

5.1 Manage data



You can work with your data in the file safe as you would in Windows®. **Copy, Paste, Delete, Edit, Save, Rename** – everything works exactly like in Windows®.

In order to work with data in file safe, you must first **select** them: single files and folders can be selected with the left mouse button. Select multiple files and folders by pressing SHIFT + Up or SHIFT + Down. Select distributed files and folders by pressing the left mouse button while holding down the CTRL button. Press CTRL + A to select all files and folders.

Open files and folders by clicking on them with the left mouse button. **Open with...** lets you choose which program opens the file. You can edit files in the file safe directly, and also save modified files.

You can create new folders by selecting **Create folder...** (Right-click/Create folder...). Files and folders can be **Copied, Cut, Pasted and Deleted** by

either dragging with the mouse (**Drag & Drop**) or using the respective function by right clicking with the mouse (e.g. Right-click/Cut). To delete data drag it with the mouse to the Recycle Bin.

All functions can also be executed from the Main menu under *File* or *Edit*. In the Main menu options next to the respective functions are their corresponding hotkeys (e.g. CTRL + X).

5.2. Delete data

When you delete data in the file safe it is moved to the Recycle Bin. You can select single files in the Recycle Bin and delete them permanently from the Recycle Bin by using the function **Delete** (Right-click/Delete).

The complete contents of the Recycle Bin can be deleted by selecting the Recycle Bin and then **Empty Recycle Bin** (Right-click/ Empty Recycle Bin).

Both the deletion of files and folders in the Recycle Bin and the emptying of the Recycle Bin **deletes the data permanently**. The data cannot be recovered, even with the use of special software.

To restore data, which is in the Recycle Bin, **Cut** (Right-click/Cut) it in the Recycle Bin and then paste it to the desired folder in Protectorion. Just as with the Delete function, you can also recover it with **Drag & Drop**. Drag the data with the mouse to the Recycle Bin to delete or drag it from the Recycle Bin to the desired location to restore.

5.3 Protect data

Through the integrated, powerful encryption Protectorion offers effective protection for your data and passwords on PCs, in the cloud, on networks and on external devices. Protectorion uses the secure and renowned Advanced Encryption Standard (AES) with a key length of 256 bit. This standard is also used employed by government agencies and large corporations such as banks and insurance firms.

You protect file and folders in the file safe by clicking on **Encrypt** (Right-click/Encrypt). To remove this protection on files and folders, click on **Decrypt** (Right-click/Decrypt). Selecting multiple files will encrypt or decrypt, respectively, the selected files.

All functions can also be executed from Main menu File as well as from the Toolbar. In the Main menu options next to the respective functions are their corresponding hotkeys.

5.4 Customize user interface

By the modifying the user interface, you can personalize the appearance of the file safe to best suit your needs.

Protectorion can hide and unhide the **buttons** in the file safe (Main menu *Display*, submenu *Less buttons* or *More buttons*). Additionally, you can choose between a **long** or a **short Folder display** (Main menu *Display*, submenu *Protectorion path* or *Windows path*). If you would like grids shown in the file view, use the function **show grids** (Main menu *Display*, submenu *Show grids*). To immediately show changes to files in the file view, select **Refresh** (Main menu *Display*, submenu *View refresh*).

In the Main menu option *Display*, you will find next to the respective functions are their corresponding hotkeys.

5.5 Navigate the file safe

Use the **arrow keys** in the *Folder display* to move between the folders backward, forward and upward. You can also navigate by clicking on individual folders with the mouse.

5.6 Standby mode

After closing a safe or the file manager, it can be re-opened at anytime by clicking on the **Protectorion icon in the System tray** (Standby mode).

Several functions are available while Protectorion is in Standby mode. These can be selected by right-clicking with the mouse on the Protectorion icon in the *System tray*. From there you can **Open safes** and the **Safe manager**.

5.7 Activate/deactivate password inquiry on PC

Your master password is required to open Protectorion. If you use Protectorion throughout the day and do not want to re-enter your password each time you access the program, select „**Remember password while Protectorion is active**” in the password prompt screen.

5.8 Copy between two file safes

You can copy information in Protectorion from one file safe to another on the same computer. To do this, open both file safes and copy the data from the first safe to the second safe by **Drag & Drop** or **Copy and Paste**.

6. Working with the password safe

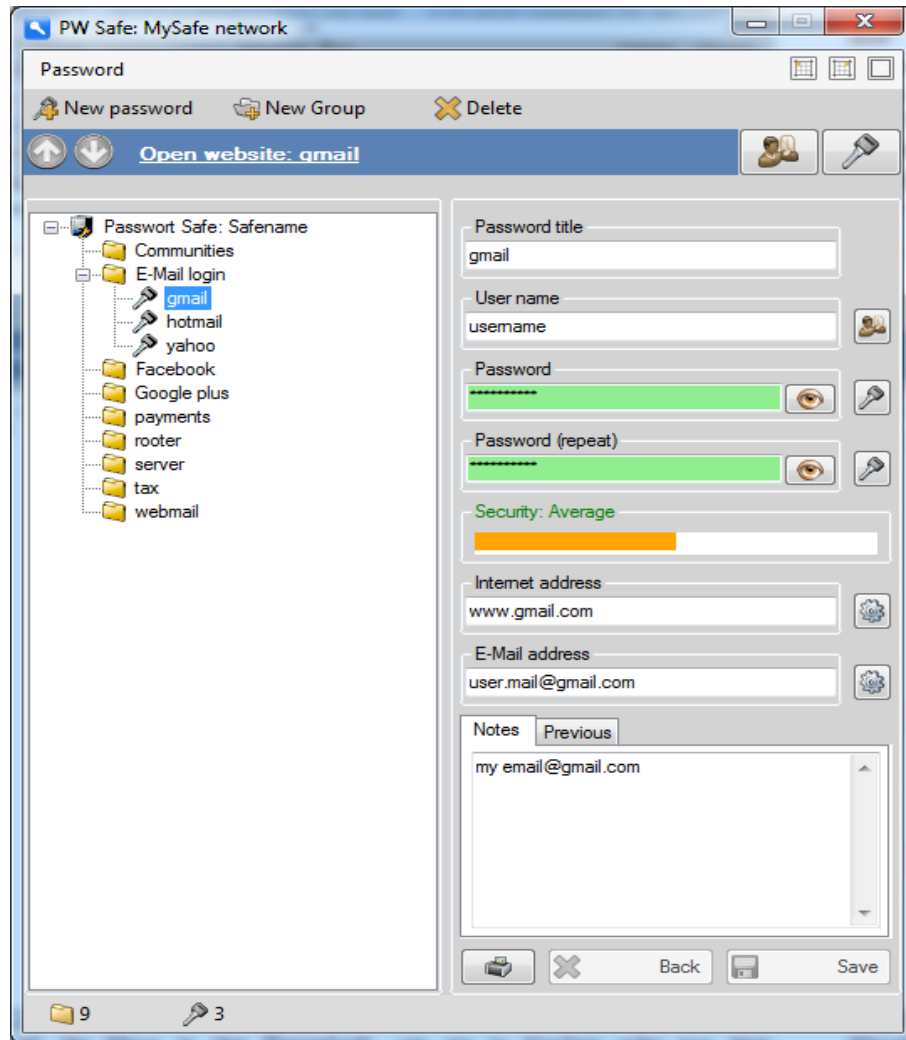
The **Password safe** manages your user names and passwords for email accounts, online banking, Twitter, Facebook, etc. All usernames and passwords are automatically encrypted and saved in the password safe with AES 256 bit. The data—like the data in file safe—is protected by your **master password**.

Instead of keying in usernames and passwords on the keyboard, you can simply copy them from the password safe to the appropriate login field of a website.

Encrypted usernames and passwords in the password safe can be managed by multusers in the cloud or on a network, as well as be accessed from different computers.

6.1 Open password safe

Click on **Password Safe** in the safe manager or in the file safe:



6.2 Create passwords and groups

In the password safe, you can create **password entries**. These password entries contain your usernames and passwords. The password entries can be organized into password groups.

You can create a password entry with **New password...** (Right-click/New password...). By selecting the password you can modify it (Right-click/Lock, Rename, Delete). You can also save usernames, passwords, and the corresponding login address (e.g. a website). Additionally, you have the option to make notes and record email addresses for these password entries.

New group... (Right-click/ New password group...) allows you to create folders in the password safe, in which you can better organize your password entries. Select the password group to edit it (Right-click/Rename, Delete).

All functions can also be executed from Main menu Password as well as from the Toolbar.

Password entries can be moved by dragging them with the mouse (**Drag & Drop**) from one password group to another.

6.3 Sign in via Fast-Login

With the help of the password safe you can quickly and easily sign in everywhere. It is not necessary to enter in usernames and passwords via the keyboard, instead simply copy and paste them in the designated fields (**Fast Login**).

Open the login address (e.g. website) where you want to sign in by clicking on the link in the password safe (above in the *Quick access bar*). You can **copy** your **username and password** directly from the *Quick access bar* to the Windows® clipboard and then **paste** them to the necessary fields.

6.4 Password backup

The password safe offers the possibility to secure and recover all encrypted or unencrypted password entries.

By selecting **Password** in the password safe you can create an encrypted backup of your password or export it in a decrypted state (Main menu, *Password*, submenu items *Create a backup...*, *Recover a backup...*, *Export as unencrypted...*).

6.5 Encrypted passwords in the cloud/on a network

When you have created a Protectorion safe in the cloud or on a network, you can access the password safe from other PCs. You can also grant other people access to your encrypted usernames and passwords in the cloud (**multiuser operation**).

6.6 Position of the password safe

The Position functions of the password safe (in the upper right of the *User interface*) allow you to adjust the position of the safe to suit your needs. The **Password safe** can be docked on the upper left, upper right or middle of the screen as well as be minimized or maximized.

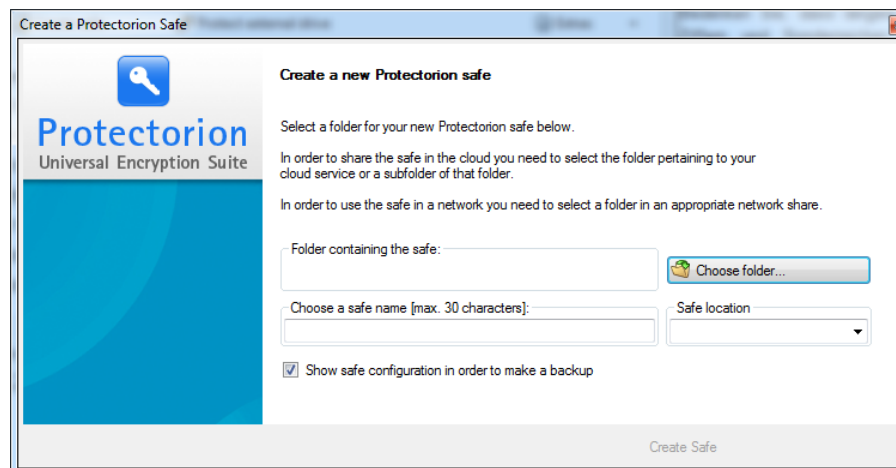
7. Create a cloud or network safe (multiuser)

With Protectorion you can create safes in the cloud (e.g. Dropbox, MS Skydrive, Google Drive) or on a network. This allows you to share encrypted information and passwords in the safe with others, as well as access this information from more than one computer.

When you copy data to the Protectorion safe in the cloud or on a network, it is **automatically encrypted before it is uploaded to the cloud/network**. Your data will **never enter** the cloud/network **unencrypted!**

7.1 Set up a safe in the cloud/on a network

To set up a safe in the cloud/on a network, click on “**Create new safe**” in the Protectorion **safe manager**.



Select the **cloud folder** (e.g. Dropbox folder) or the **network drive**, or whichever folder whose contents is synchronized with the cloud storage or is saved on the network drive:

Give the safe a **meaningful name** (e.g. Company name Dropbox, Company name Network) and close the safe creation window. It is advisable to create a backup of the **safe configuration**.

The cloud or network safe is **automatically registered** in the safe manager. Any information that you copy to this safe is **first automatically encrypted and then saved to the cloud storage or network**.

7.2 Safe invites

If necessary, you can **grant other persons access** the encrypted data and passwords stored in the cloud/on the network. Just the same, **you can access** this encrypted data **from more than one computer**.

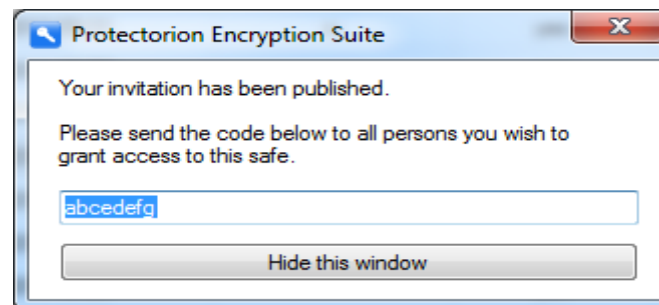
Create a safe invite by first selecting the safe that you want to share in Protectorion's **safe manager**. Next right-click with the mouse on the selected safe and choose "**Invite to safe**". A window will pop up to ask you to **assign a connection code**. Choose an appropriate connection code, keeping in mind that a longer code, which includes a combination of numbers, upper- and lowercase letters, and special characters, is more secure.



You can **assign a new connection code** for the safe **at anytime**.

Please keep in mind that the recipient of the safe invite **must be connected to the cloud storage**, in which the safe is located, or **have access to the network**, on which the network safe has been established.

Convey the connection code to the person(s), with which you want to share the cloud/network safe.



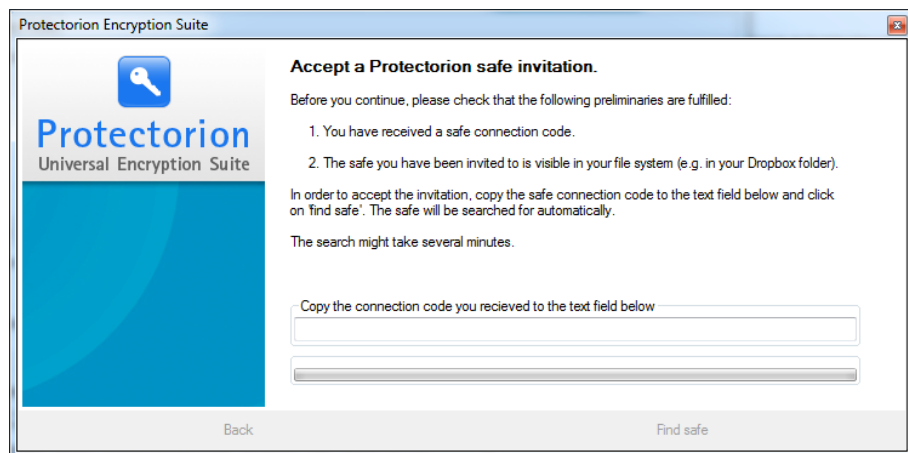
7.3 Accept an invite to a cloud/network safe

After the **recipient has received the connection code**, this person can connect to your cloud or network safe.

In the case that you want to access your safe in the cloud or on a network from another computer, you would be the recipient of the invite.

Once the recipient has the connection code, this person can click on "**Accept invite**" in the **Protectorion Safe manager** under **Safe actions**. Next follow the assistant's instructions.

Please keep in mind that the recipient of the safe invite **must be connected to the cloud storage or network drive**, in which the safe is located, in order to access the safe.



Enter the connection code into the appropriate field and click on “**Search for safe**”.

Protectorion **searches for the new safe** in the cloud or on the network and automatically registers it in the safe manager.

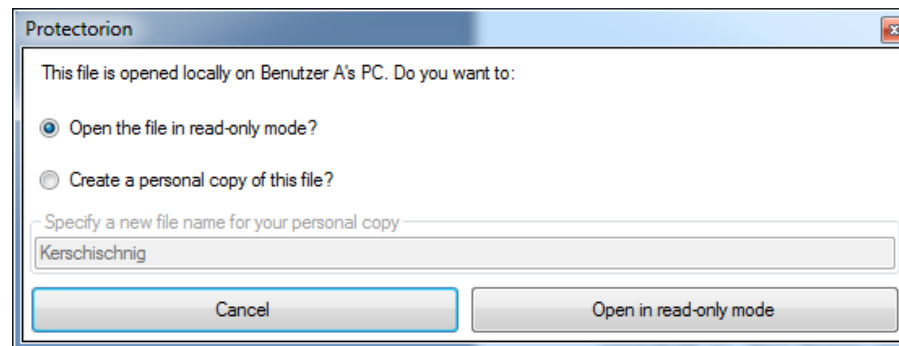
The recipient **immediately has access to the encrypted data and passwords** in this safe. Both parties can now manage the information in the safe. In the case that you are setting up access for yourself for multiple computers, you are now able to access the safe from this computer.

8. Protectorion in multiuser operation

Protectorion supports **shared access to the encrypted data and passwords from more than one PC**. This makes it possible for teams and companies to safely manage and work on their confidential information in the cloud or on a network.

When a file is opened by a user of the safe, it is displayed in the “user” column to show which user currently has the file open. This allows other

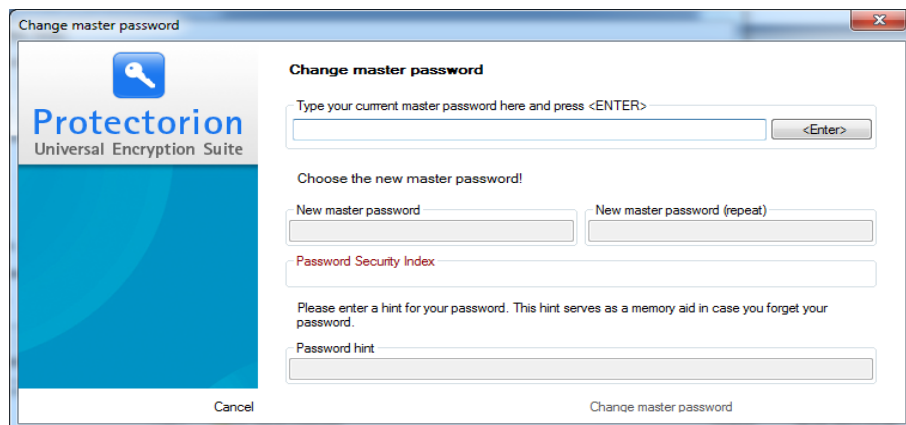
users to **see who has the file open and access it** either by opening a read-only copy, or creating a personal copy of the file:



In addition, Protectorion allows the **shared management of encrypted login information (usernames and passwords) by multiple users**. This way all users have access to current login information at any time.

9. Change password/username

You can change your master password and username at any time with **Change username...** or **Change master password...** in the Protectorion safe manager (Main menu *Safe actions*, submenu *Change username...* or *Change master password...*).



10. Rename safe or safe location

You can change the safe name and the safe location at any time with **Rename safe name/Safe location...** in the Protectorion safe manager (Main menu *Extras*, submenu *Rename safe name/Safe location...*).

11. Create backup of safe configuration

You can create a **backup of the safe configuration** with **Show and save safe configuration...** in the Protectorion safe manager (Main menu *Safe actions*, submenu *Show and save safe configuration...*).

12. Configure options

In the Protectorion safe manager under the Options tab, you can personalize Protectorion to fit your needs. For example, you can **Start Protectorion**

automatically with Windows® and configure Protectorion to **remember your master password** while the program is active (also while in Standby mode).

13. Quit Protectorion

Quit Protectorion if you want to completely close the program and do not want to activate Protectorion's Standby mode.

You can **quit Protectorion** at any time by right-clicking the Protectorion icon in the System tray.

When you quit Protectorion all unencrypted data in the safe is automatically encrypted. This **assures that all data in the safe is protected** when you quit Protectorion.

Protectorion cannot quit when files, which are located in the file safe, are open in other programs. Only after all these files have been closed can Protectorion be quit.

14. Update Protectorion

Protectorion regularly searches for new **updates** and informs you when these are available. In the case that Protectorion notifies you of an available update, simply quit and then restart Protectorion, and the update will install. If you want to continue working, the update will install the next time you start Protectorion.

15. Uninstall Protectorion

Uninstalling Protectorion does not delete the files and folders incorporated in Protectorion, nor does it delete your license information!

Use **Uninstall** (under Windows® in *Start/Program/Protectorion* or under Windows® in *Start/Control Panel/Programs*), if you want to remove Protectorion from your computer.

16. Buy Business Edition

Protectorion Free allows you to manage files, folders and passwords for personal use on a maximum of two computers and one external device. You can use up to two safes at the same time on a computer, in the cloud or on a network, and additionally set up Protectorion ToGo on an external storage device.

If you would like to use Protectorion for business purposes, **please acquire a suitable Business Edition from our webshop (<http://en.protectorion.com/shop>).**

You can purchase the appropriate **license key** on our web shop. You can get there by Main menu *Help*, Submenu *Buy now...* or in the safe manager by clicking on "*License*" in the *Status Bar*. You obtain the license key immediately after purchase.

Enter the license key along with your name in the field provided in the Safe Manager under the Main menu (tab) *License*. Restart Protectorion Free after entering in the license key. The license for the Business Edition will be active.

No additional software is necessary. After the transfer of Protectorion Free to a Business Edition you can continue working with your data in Protectorion as before.

Protectorion Encryption Suite – Play IT Safe!