10. JANUAR 2022

VIRTUAL SAFE PROFESSIONAL 3.5
USER GUIDE

ENCRYPTION OF FILES AND DIRECTORIES

MARCEL SCHEITZA
SOFTWARE DEVELOPMENT, MARCEL SCHEITZA

CONTENT

1 OVERVIEW

1.1 PRODUCT DESCRIPTION

"Virtual Safe Professional" encrypts data and thus protects it from the prying eyes of unauthorized persons. After you have created a virtual vault, important documents, password files or personal data can be stored in the assigned vault directory. The files are only accessible by providing the correct password. The AES-128 and AES-256 encryption algorithms provide reliable protection.

1.2 FEATURES

The following is an overview of the most important features of the software:

- Creation of any number of virtual safes of any size
- Specifying one or more root paths
- Sharing backup manager settings among configured root directories
- Change the password for virtual safes
- Rename virtual safes
- Encryption of virtual safes via AES-128/AES-256
- Use of keys up to 32 characters in length
- Automatic backups when definable actions occur
- Manual creation of backups via the Backup Manager
- Columns of the safe for archiving in several parts
- Assembling the safe from several parts
- Built-in shredder for shredding files and/or directories
- Start Virtual Safe Professional automatically with Windows
- Publish one or more virtual safes with Virtual Safe Professional Portable
- Creating Virtual Safe Professional Portable from within the application

2 QUICK START

2.1 STARTING VIRTUAL SAFE PROFESSIONAL

After installing Virtual Safe Professional on your Windows operating system, a shortcut will be created on your desktop:
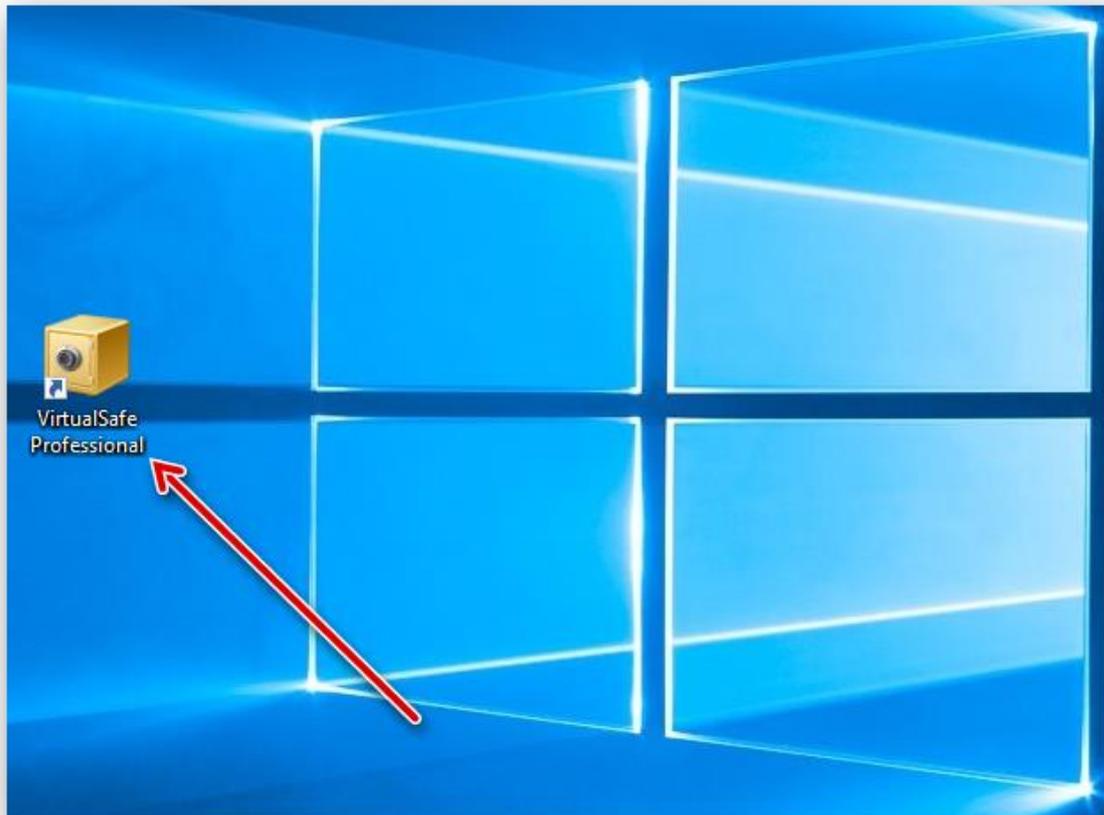

By double-clicking on the shortcut icon, the application can be started.

2.2 START AUTOMATICALLY WITH WINDOWS

To start Virtual Safe Professional automatically with Windows, select the "Advanced" tab in the application and then "Settings".
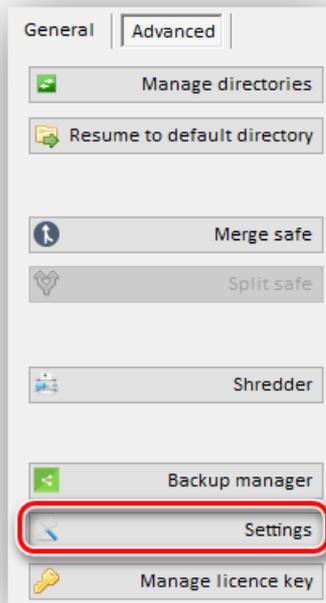
In the settings mask you now have the option to activate the checkbox "Run program at windows startup".

Hint:
This checkbox can only be edited if you have the necessary rights to update windows registry data.

2.3 DEFINE ROOT DIRECTORY

2.3.1 DEFAULT DIRECTORY

If you create virtual safes and have not made any additional configuration, they are created in the **default directory.** The **default directory** is in the application data of your user profile at:

Documents\VirtualSafes

By default, backups are stored in the following directory:

Documents\VirtualSafe Backups

Tip:

- Press the Windows key + R
- Enter %userprofile%\Documents\VirtualSafes

To go directly to the default virtual safes directory

2.3.2 CHANGING ROOT DIRECTORY

To change the directory where you want to manage virtual safes, do the following:

- In the menu, select "Advanced" and then "Manage directories"
- Right-click in the list view or click on the "plus icon"
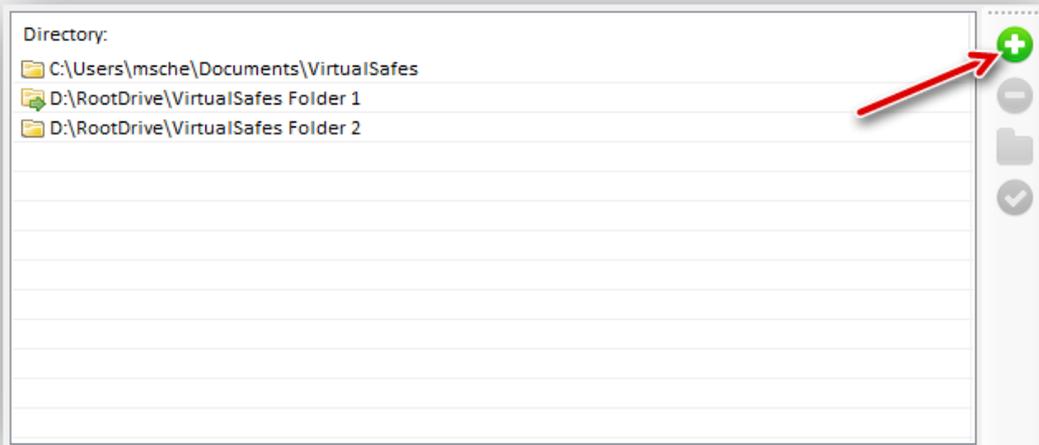
Enter the path to your destination directory and confirm the selection.

Hint:
In this view, you can now define several root directories and jump back and forth dynamically via a double-click or right-click, "Select Directory". (e.g. to a Google Drive or OneDrive directory or another hard drive)

Then select the directory by double-clicking or right-clicking, "Select directory".

Virtual Safe Professional now stores and manages all virtual safes under this directory.

2.3.4 REMOVING THE ROOT DIRECTORY

Each manually added root directory can also be removed from the list of stored root directories. Note that this does not affect the active root directory.

Hint:
The default directory cannot be removed from the list.

2.4 SETTING BACKUP SETTINGS

For security, backups are created from your virtual safes.

When and where backups are created, you can define either for each safe **individually** or **globally** for the entire root directory.

2.4.1 SELECT THE SCOPE

By clicking on the tab "General configuration" (default) or "Individual configuration" you can select the scope, in which the configuration applies.
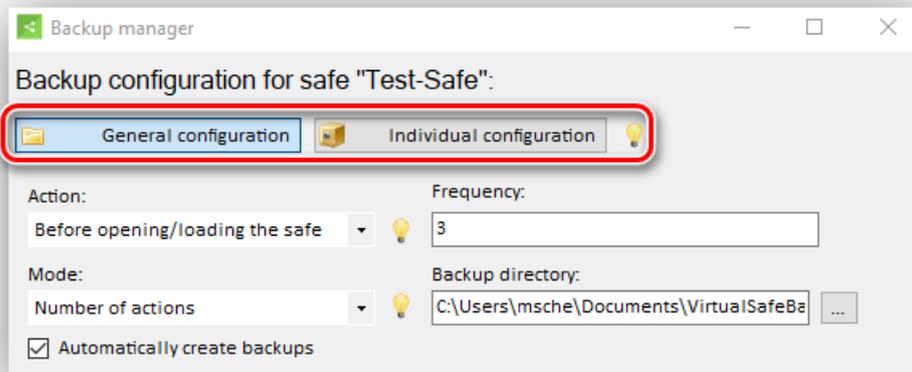
Everything you then configure applies either to the safe directory (General) or only to the selected safe (Individual).

2.4.2 CHANGING BACKUP SETTINGS

You can adjust the (default) settings individually for each safe via the Backup Manager**.**

To open the Backup Manager, right-click on one of your safes and select "Backup Manager".
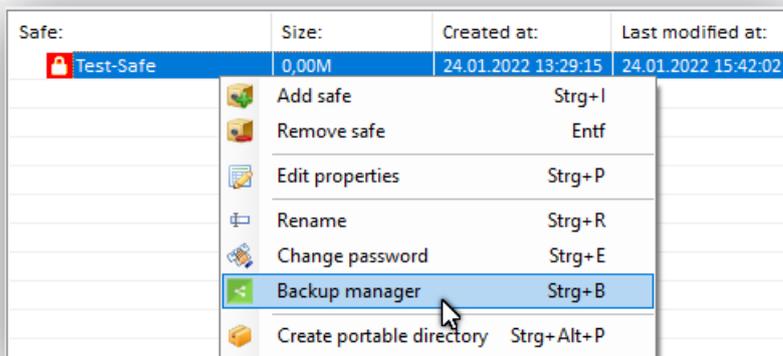
In the Backup Manager, you can set the following properties:

| ATTITUDE	DEFAULT	DESCRIPTION
ACTION	Before opening the safe	When should a backup be created?
FREQUENCY	Every 9th time	How often should a backup be created?
BACKUP DIRECTORY	Documents\VirtualSafe Backups	Where should the backup be created?
AUTOMATICALLY CREATE BACKUPS	Yes	Do you want to create automatic backups?

Changes to these settings always affect the current scope, either "General" or "Individual.

Use-Cases:

Disable backups:

Deactivate the checkbox "Automatic backups", then the backup creation will be deactivated for the current scope.

Change backup directory:

If you change the backup directory, the backups for the current scope are created in the selected directory.

Change frequency:

If you change the frequency, the backups for the current scope are generated in the selected frequency.

Change action:

If you change the action, the backups for the current scope are generated, when the specific event occurs.

2.5 MANAGING VIRTUAL SAFES

2.5.1 CREATING A NEW SAFE

To create a new safe in your working directory, either right-click in the Safe Overview and select "Add safe" or select the "Add safe" button from the menu under "General":
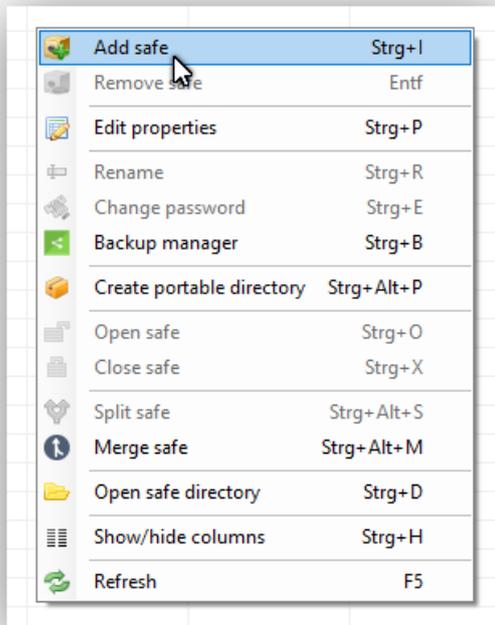
Then enter a name and password for your safe **twice.**

Finally, click on "Create safe". You should assign a secure password, which consists of at least 10 characters with included uppercase, lowercase letters, numbers and special characters.

2.5.2 Open safe

To open a safe in the Safe Overview,

1. select the safe with the left mouse button,
2. then enter your password and
3. click on "Open safe".
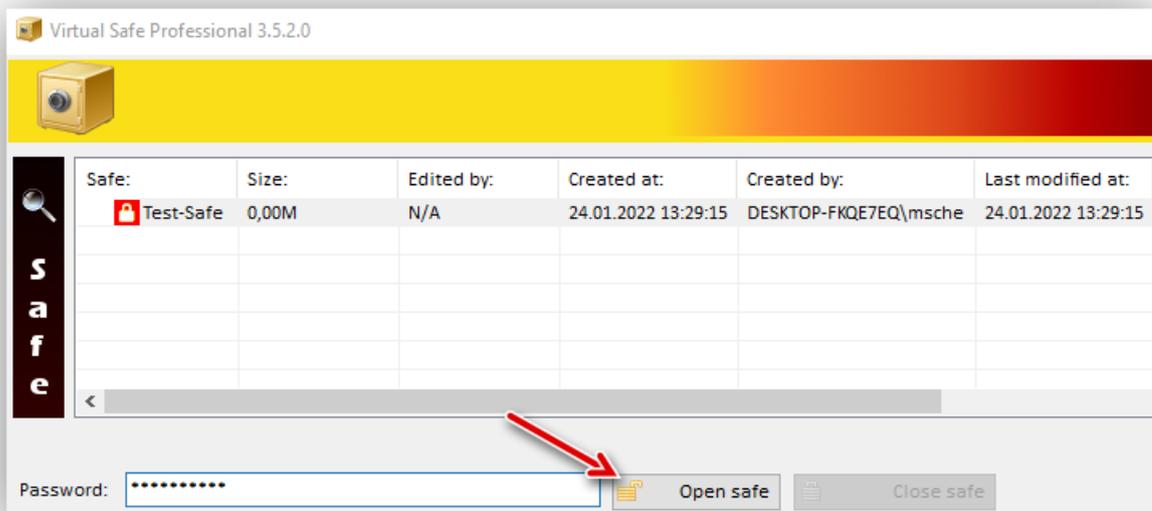
Then a Windows directory opens in which you can store your files and or directories.

Create files below this directory or drag and drop them into the directory.
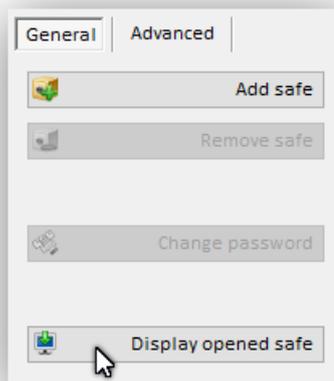
Tip:
If you have closed the Windows directory once, you can display it again via the application: Select the menu item "Show safe" under "General".

Hint:
Closing the Windows directory does not close the safe. The safe must be explicitly closed via the "Close safe" button.

2.5.3 CLOSE THE SAFE

To close an open safe again and thus securely encrypt your files and directories, either right-click on your safe and select "Close safe" or click on the "Close safe" button.
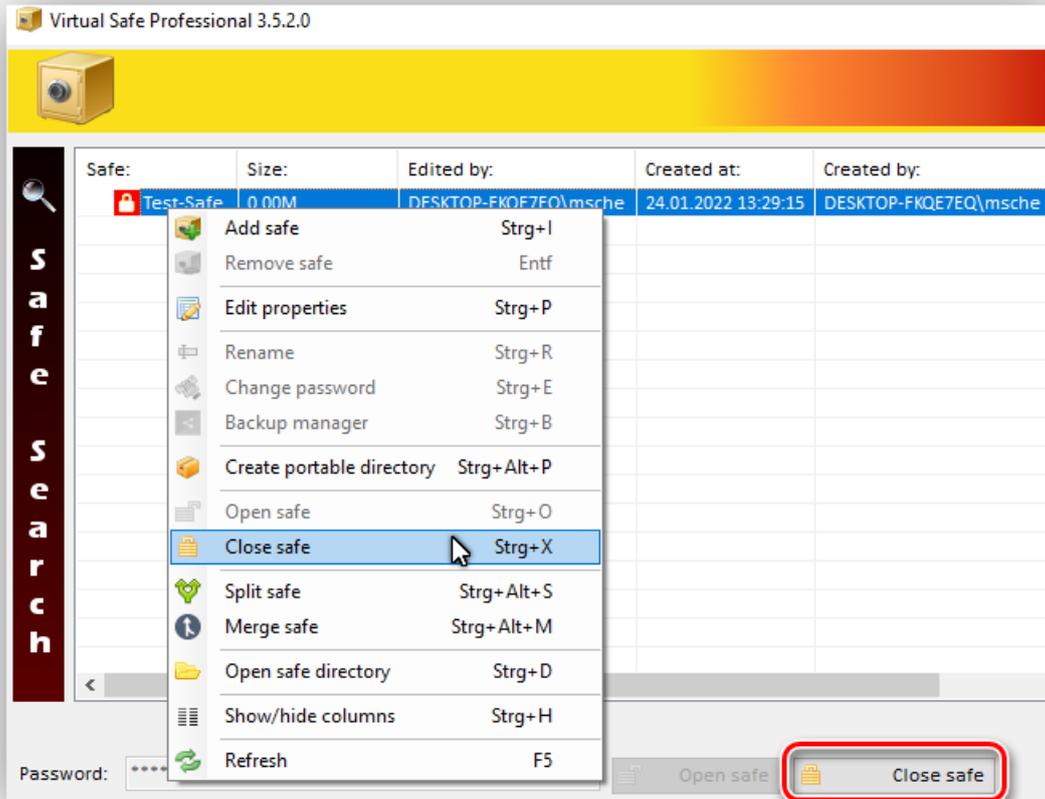
2.6 APPLICATION

2.6. 1 TRAY ICON

As soon as Virtual Safe Professional is started, a tray icon is created in the Windows taskbar at the same time. This icon can be used to pull out the application by double-clicking if Virtual Safe Professional has been closed by closing the window. In addition, the currently opened safe can be displayed directly or closed.
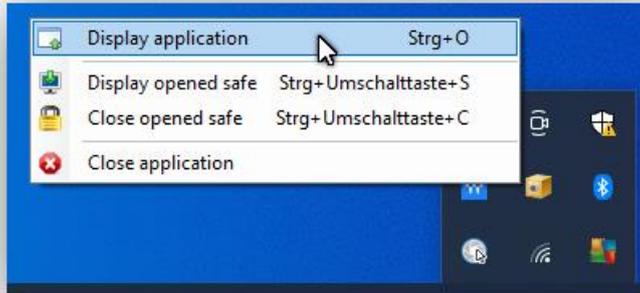
If the application is closed, you can retrieve it by double-clicking or right-clicking on the tray icon and the menu item "Show application".

You can also launch the application at any time from the desktop icon.

2.6.2 CLOSING BEHAVIOR

The behavior when closing the main window of Virtual Safe Professional is configurable:

Under "Advanced", "Settings" you could select either "Keep in tray" or "Close".

Standards:

For the different versions of Virtual Safe Professional, individual default values for the closing behavior have been defined:

Variant	Default
Professional	Keep in tray
Business	Keep in tray
Portable	Close

3 ADDITIONAL FUNCTIONS

In addition to the standard functions, Virtual Safe Professional contains various additional functions for secure archiving and data cleansing.

3.1 SHREDDING FILES AND DIRECTORIES

If you have closed your virtual safe, the temporary files will be shredded automatically.
However, you also have the option of shredding other files or directories.
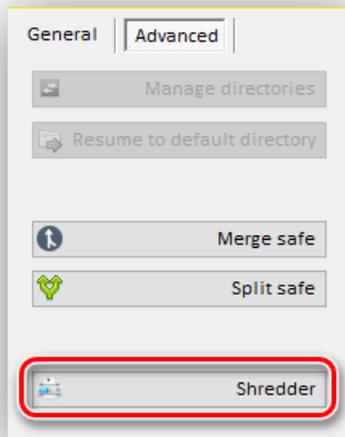
To do this, select the "Shredder" function under "Advanced" in the menu.

In the following dialog you can drag and drop your files and/or directories to be shredded.

By clicking on "Shredder file(s)" the files are destroyed.

Hint:
The directory structures remain in place and must (if desired) be removed manually afterwards.
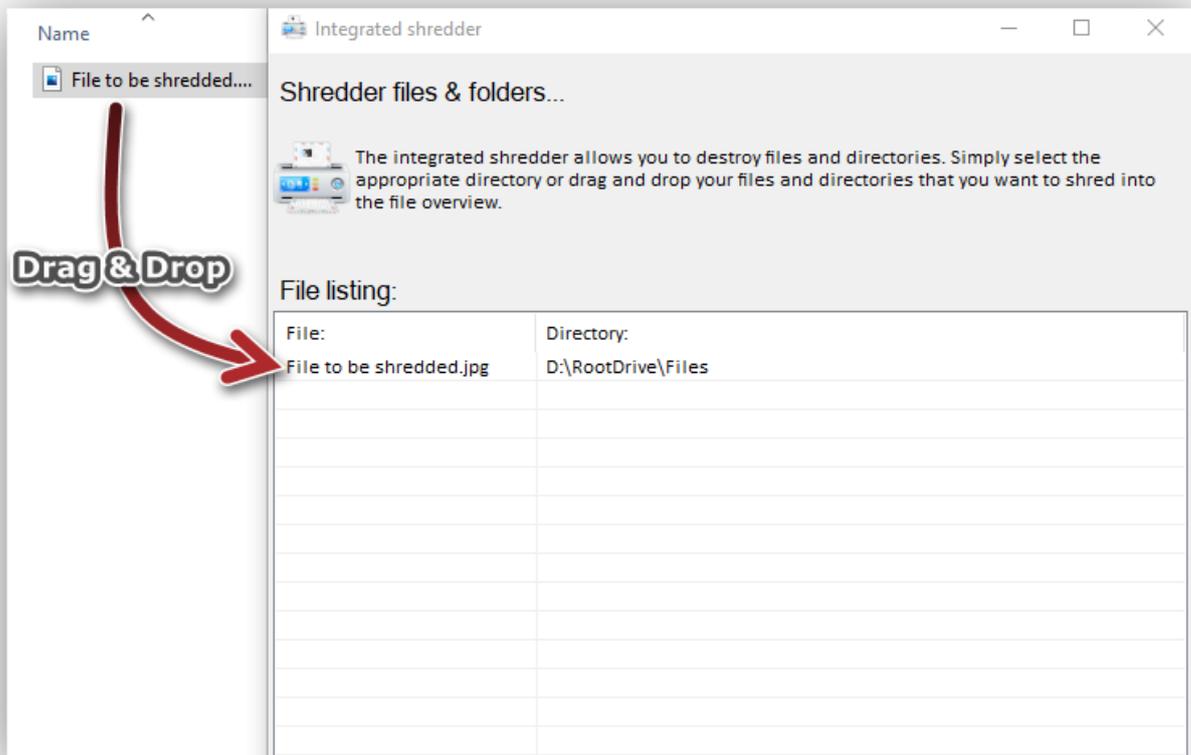
3.2 SPLITTING THE SAFE

For secure archiving, Virtual Safe Professional offers the possibility to split your safes into several parts.

To do this, proceed as follows:

Under "Advanced", select the menu item "Split Safe".
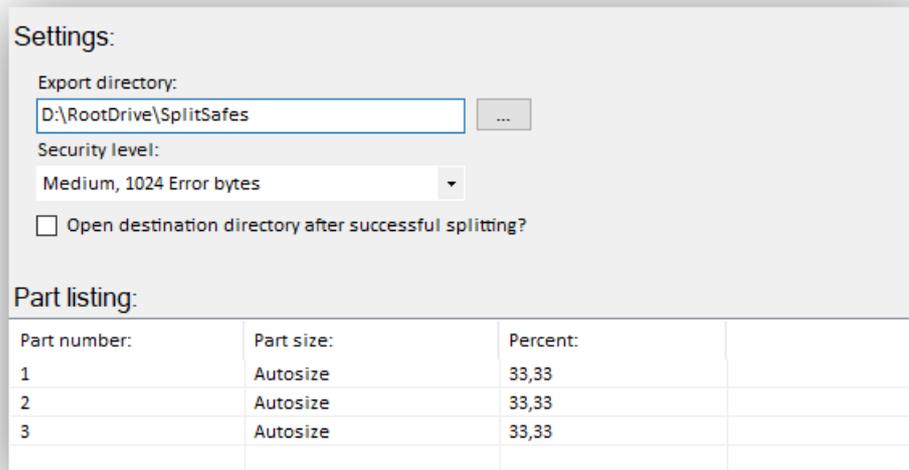
1. Select your destination directory.
2. Specify Security Level.
3. Specify the number of parts by right-clicking→Add Part.
4. Click Perform Splitting.

The safe you selected is then broken down into several parts in the target directory. In addition, a *.Masterpart file is created, which is required for the correct assembly of the safe.

3.3 ASSEMBLING THE SAFE

To reassemble your split safe, select the menu item "Merge safe" under "Advanced". Enter the path to *.Masterpart file, as well as the new name of the safe.

Important note:
All parts of the safe must be in the same directory as the *.Masterpart file.

Then click on "Assemble safe" to create your safe from the individual parts.

3.4 CREATING A PORTABLE DIRECTORY

At the push of a button, the user can create portable directories from his virtual **safes,** which can be securely passed on via USB stick or cloud services, for example. In addition to the data of the safes themselves, a portable version of the „Virtual Safe Professional Portable" application is copied to the publishing directory.   Only those who are in possession of the keys can access the data contained in the safes.

Step 1: Set Safe Selection

First, in the main window, select one or more virtual safes with the left mouse button that you want to publish. Then right-click in the list view and select the menu item "Create portable directory".

Step 2: Create a portable directory

Then another window opens, which displays the selected safes together with other settings:
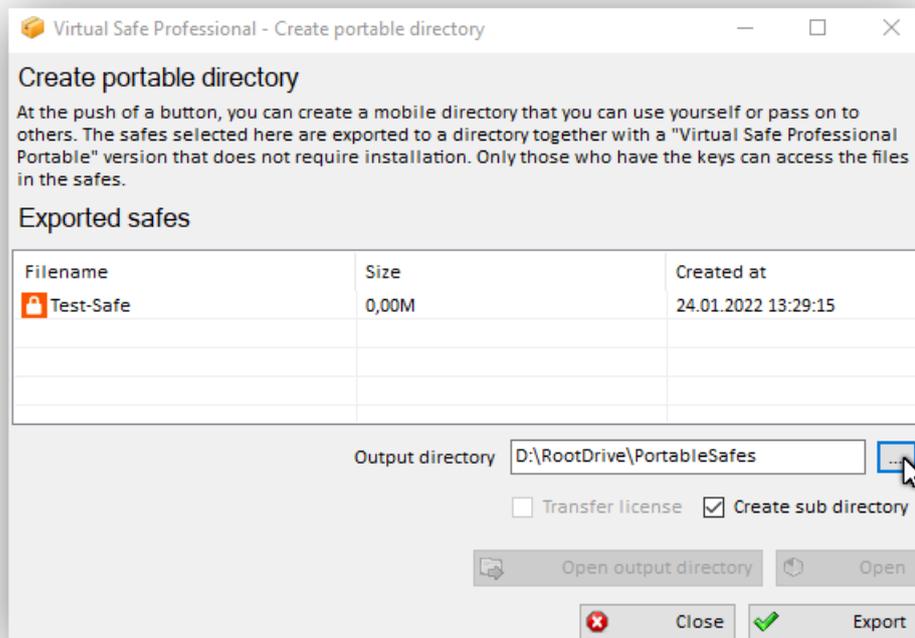
Select the "Output Directory" and click "Export".

You can then use the "Open" or "Open Output Directory" buttons to jump directly to the output directory or start "Virtual Safe Professional Portable" in the output directory.

3.4.1 ACCEPT LICENSE

Do you want the target group of published safes to be able to add or edit files to safes? Then you can activate the checkbox "Apply license". Keep in mind, however, that the other party is in possession of your license key, which may be used on a maximum of three end devices. Therefore, only   share the license key with trusted people.

3.4.2 CREATING AN EMPTY PORTABLE DIRECTORY

It is possible to create an empty portable directory for further work, e.g. on an USB stick.

To extract Virtual Safe Professional Portable from the application, proceed as follows:

Step 1: Right-click in the virtual safes list view

- Make sure no safe is selected.
- In the list view, right-click to call up the context menu.
- Select "Create Portable Directory"

Step 2: Create a portable directory

Then another window opens, which only provides settings.

The license is distributed by default because it is assumed that the virtual safes are created and managed via Virtual Safe Professional Portable.

Note on the trial period:

If you are still in the trial period, unfortunately no license can be passed on. The creation or management of virtual safes is therefore not possible.

4 VIRTUAL SAFE BUSINESS PROFESSIONAL

4.1 FEATURES

Virtual Safe Business Professional extends the Professional version with important functions that you need in the business environment to securely encrypt your or your customers' data and to find it quickly.

- Working with multiple users on a root directory:
  - Entry and display of the current processor- Definition of an access type before Safe Access- Read access for all
  verified users, if Safe is currently in progress
- Sharing the property model and master key settings among configured root directories
- Classify safes using user-specific properties
- Assign value lists to properties for easy entry and search
- Safe-Search: Search for properties across all safes in a root directory
- The master password: Critical operations, such as deleting safes, can only be performed by selected users or administrators.
- Master-Key function: Use the master password to decrypt all safes in an emergency.

4.2 QUICK START

Step 1:
If you have opened Virtual Safe Business Professional for the first time, you should first set your root directory. To do this, proceed as described in Chapter 2.3 Define root directory

Step 2:
Once you have set your root directory, create your first virtual safe. To do this, follow the steps in Chapter 2.5.1 Creating a new safe

Step 3:
Now set your property model as described in the following chapter.

4.2.1 CREATING A PROPERTY MODEL

A property model can be created using the same view as property values for safes: Select a safe in the current root directory and open the context menu:
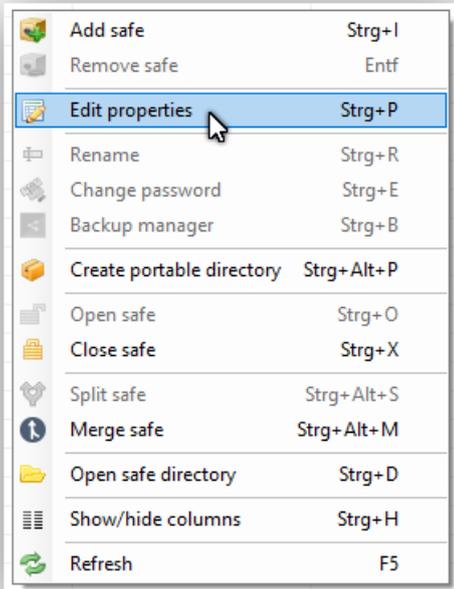

Select manage properties. If you have selected a safe, you can now create properties directly and assign values to this safe.

If you have not selected a virtual safe, you can only maintain the data model.

Select manage properties. In the next view, right-click in the empty table.
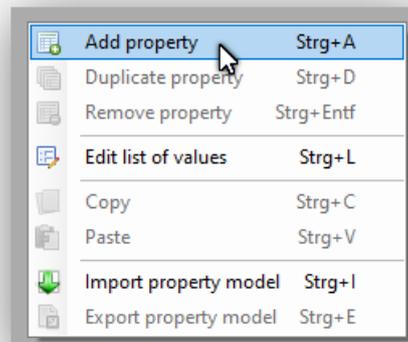
You can now enter values one after the other in the selected dataset:
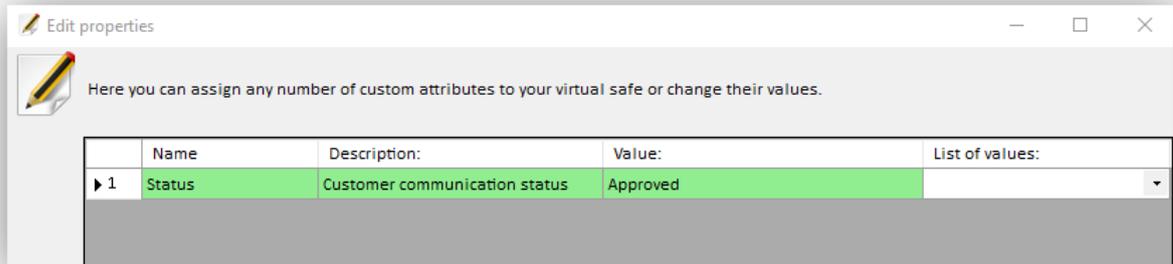
Or add more properties:
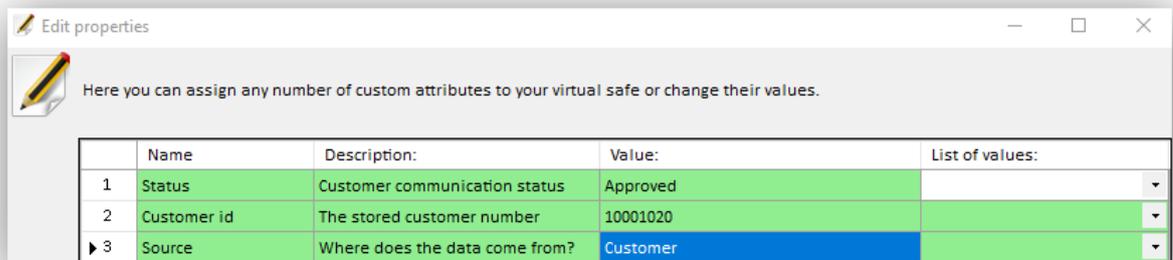
Once you have created all your properties, you can close the property management view by clicking on "Apply".

The following window will then appear:
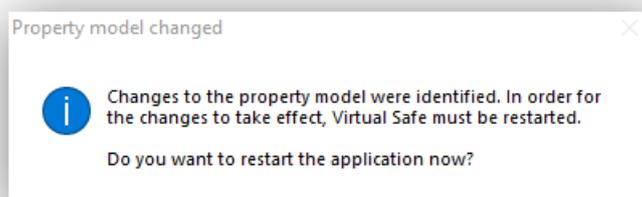
The application has detected properties, which were added via property management. In this case, Virtual Safe Professional must be restarted for the changes to take effect.

Note:
By default, each root directory has its own property model. However, configurations of the property model can be shared by other directories. For more information, see the chapter "Sharing Settings".

4.2.2 ADDING OR EDITING VALUE LISTS

Value lists help the user with both data entry and data search: The user can choose from a previously configured list of possible input values. At the same time, Virtual Safe Business Professional always offers the possibility to enter a value that does not appear in the value list.

To add a value list to a property, right-click the property in the Property Manager:
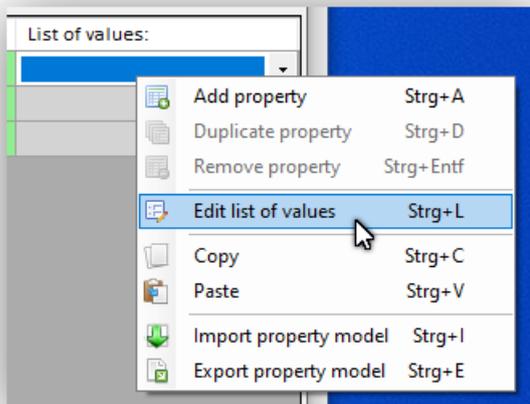
Now select "Edit list of values".
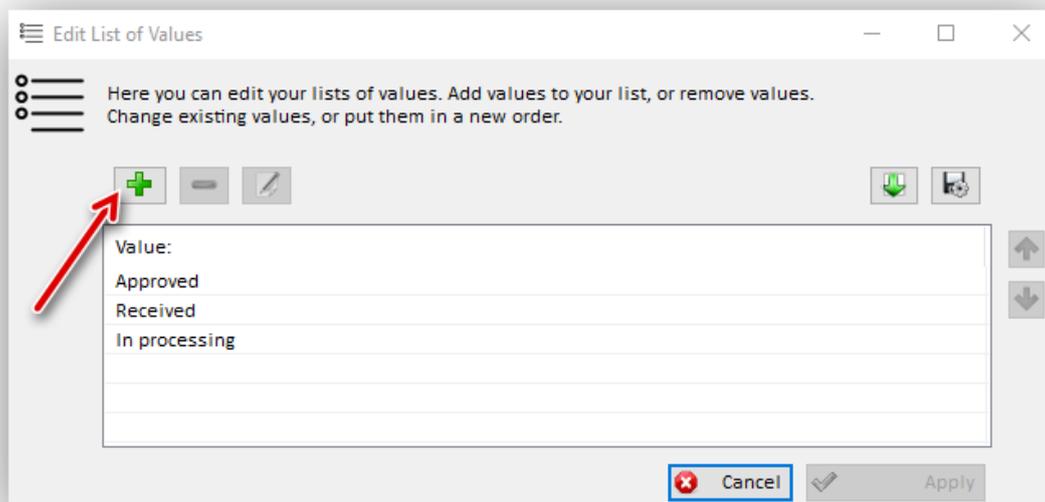
Using the icons or the context menu, you can:

- Add values
- Remove values
- Edit values
- Sort values

- Export value list completely
- Import value list completely

Once you've finished editing, click "Apply".

4.2.3 EDITING PROPERTY VALUES

To edit a property value for a virtual safe, right-click the safe and select Manage Properties.

You now see a separate record for all properties created in the property model.

Here you can either select a value under the "Value" column if a value list has been set or enter a value.

To apply the changes, click "Apply".

4.2.4 SAFE SEARCH

With the help of the "Safe Search" you can search for one or more search criteria in the current root directory over all safes.

You can use the following standard search fields as search criteria:

PROPERTY	DESCRIPTION	DATA TYPE
NAME	Name of the safe	Text
SIZE	Size of the safe in megabytes	Number
CREATED ON	Creation Date	Date
CREATED BY	Creator	Text
MODIFIED ON	Alteration date	Date
MODIFIED BY	Last modifier user	Text
ENCRYPTION	Encryption type: AES-128 or AES-256	Selection
OPENED BY	Currently opening user	Text

Properties created in the property model can also be used as a search criterion:

In this case, a customer number of type Text, a status with a stored value list, and a source specification of type Text have been defined.

Default textual search behavior:
By default, for text fields, the search function only considers values that begin with the text you are looking for.

Wildcard:
You can use the wildcard symbol (*) in the search text at any time to ignore e.g. the beginning or a value in the middle of a text during the evaluation.

4.2.5 SHOW/HIDE COLUMNS

In the Virtual Safe Business Professional version, you have the option of defining the detailed view of the Safe Overview or its columns:

- Show/hide default properties
- Show/hide your own properties

To do this, right-click in the Safe overview and select "Show/Hide column(s)".

By default, all columns are displayed.

You can now **hide** individual properties by clicking in the corresponding checkbox.

4.2.6 THE MASTER PASSWORD

If you assign a master password, you can secure access to Virtual Safe Business Professional.

The following options can be activated under "Advanced", "Settings":

- Deleting virtual safes should only be possible with a master password.
- Changes to the property model should only be possible with a master password.
- Master key function should be activated.

4.2.6.1 THE MASTER-KEY FUNCTION

From the moment this setting is activated, created safes can be opened with the master password. Safes created before enabling this setting cannot be opened with the master password.

5 SHARING SETTINGS

5.1 OVERVIEW

Certain settings can be used across roots in both product variants. These include:

- Backup Manager settings

Only included in the Business Professional product variant are:

- Property model
- Master password settings

To share these settings, you must add a reference to a configuration directory at your root directory.

5.2 WHAT IS A COMMON CONFIGURATION DIRECTORY?

A shared configuration directory manages shared settings. Any existing directory can be used as a common configuration directory. These can also be existing Virtual Safe Professional root directories.

Once configured, the root directory uses the shared configuration directory as a source for loading and storing the settings.

5.3 VIRTUAL SAFE PROFESSIONAL IN YOUR IT INFRASTRUCTURE (APPLICATION EXAMPLE)

Let's assume that you have several departments in your company that want to securely store your documents on network drives. Some departments have the same requirements for the master data managed for the safes. As part of the collaboration, for example, a customer document is received, which is provided with an order number and then further processed by the next department.
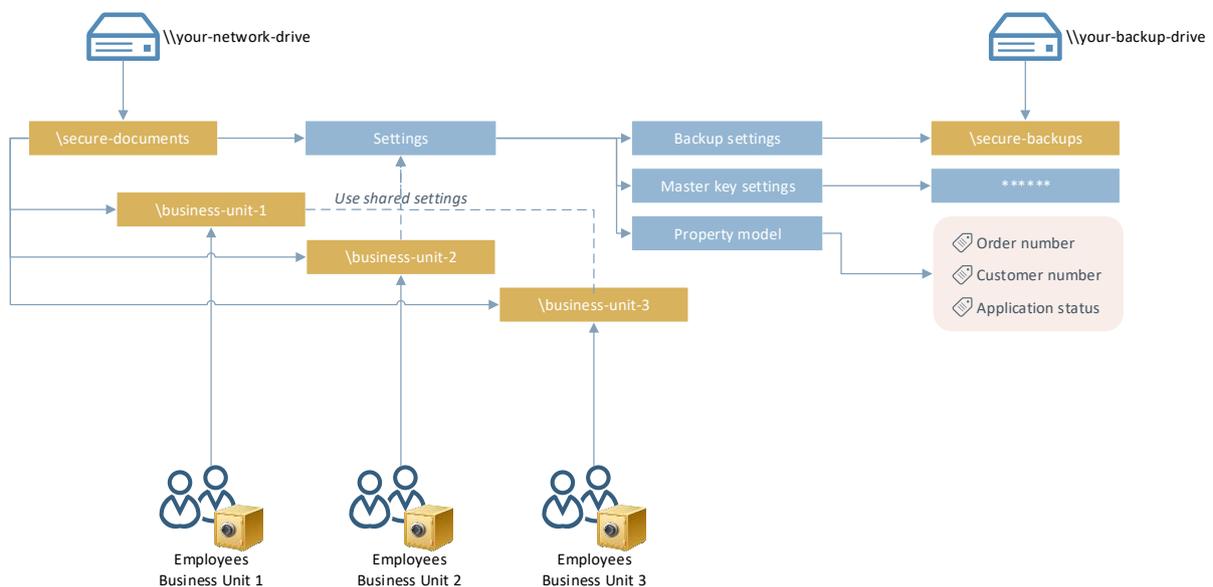

In this case, for example, you create a separate root directory for each department ("\business-unit-1", "business-unit-2", "business-unit-3"). In addition, you use a central, common configuration directory to define configurations across departments ("\secure-documents").

To learn how to set a directory as the parent configuration directory, see the next chapter.

## 5.4 DEFINING SHARING SETTINGS

To store a common configuration directory, proceed as follows:

Select "Advanced" from the menu and then "Manage directories".
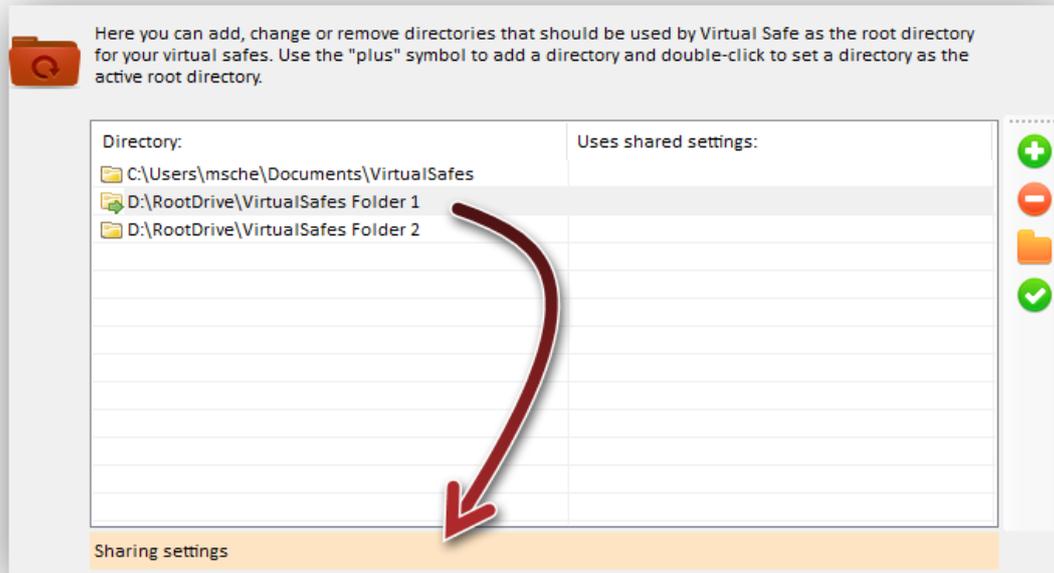
By clicking on your root directory and then on "Sharing settings" another mask opens. Here you can define a common configuration directory.

As soon as a common configuration directory has been selected, the individual settings can be registered for shared use via the checkbox.
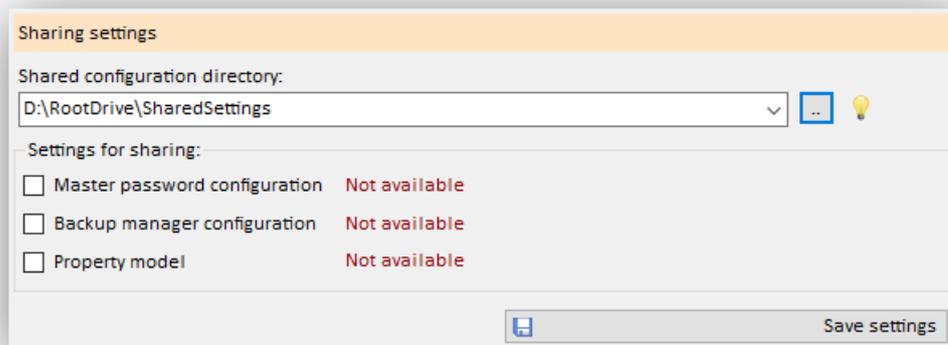
Once you have made your selection, you can apply your adjustments via the "Save settings" button.