SAFETICA ENDPOINT CLIENT MANUAL

www.safetica.com

safetica®

SAFETICA ENDPOINT CLIENT MANUAL

for Safetica version 5.5.0

You can download an outdated versions of Safetica documentation in Spanish a Japanese from the following links:
http://downloads.safetica.com/documentation/Safetica_503_SP.zip
http://downloads.safetica.com/documentation/Safetica_522_JP.zip

Author: Safetica Technologies s.r.o.

Safetica was developed by Safetica Technologies s.r.o.

For more information visit www.safetica.com.

Published: 2014

CONTENT

WELCOME!

SAFETICA ENDPOINT CLIENT

1 WELCOME!

Dear user,

Thank you for your confidence in choosing Safetica. We are certain that you will be fully satisfied. In this document you will find a detailed description of all components of the product and manual help for using the individual features. This documentation will guide you in detail from installation and initial deployment on the company network to common usage, evaluation of output and solving the most frequent problems.

If you do not succeed in solving a problem even after consulting this information, please contact technical support at http://www.safetica.com/support.

Safetica offers a completely new approach to internal security. It is the first security solution combining real prevention with actual protection against internal threats. By monitoring users it reveals their risk behavior, and by blocking unsolicited actions and protection against data leakage (DLP), it protects the company from the consequences of undesirable activities by employees. No other software application can protect a company against all major internal threats in such an all-encompassing manner.

If you want to install the software as quickly as possible, please read this *Safetica installation manual*. To quickly master basic practices and usage, use the *Safetica quick wizard*. Answers to frequently asked questions about using the software can be found in *Frequently asked technical questions of Safetica users*.

Thank you,

Safetica Technologies team, vendor of Safetica

2 SAFETICA ENDPOINT CLIENT

Safetica Endpoint Client is a part of Safetica. The module runs on client stations and allows the use of security tools and functions of Endpoint Security Tools on these stations.

You can use Endpoint Security Tools to quickly encrypt all storage devices - hard drives, USB drives, flash drives, floppy disks, ZIP drives, memory cards and many others. The data shredder can be used to safely and irretrievably delete sensitive information. You can also create an encrypted virtual drive which will behave as a classic full-fledged hard drive and work with it in the same way. Endpoint Security Tools also contain an advanced security manager for the organization of passwords and other information. All of this with a selection of the world's best ciphers. Using these and other functions of Endpoint Security Tools can ensure that your company data is safe and prevent a leak of sensitive information. This allows you to significantly contribute to the security of your company.

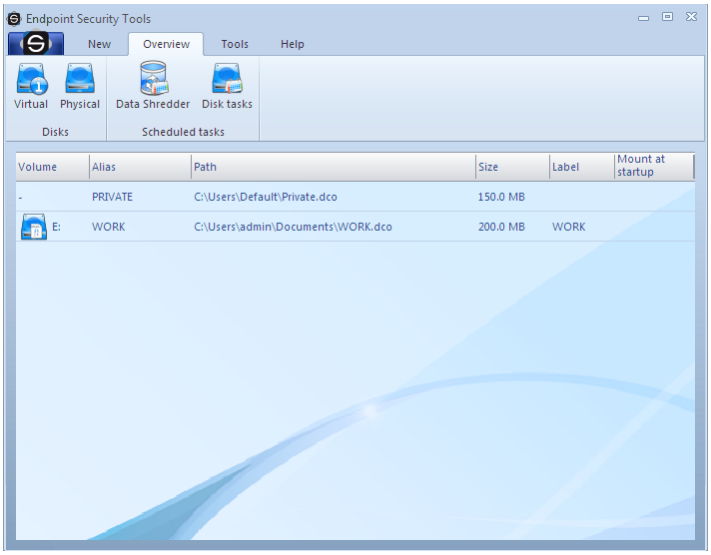
Safetica Endpoint Client is composed of two main parts:

- **Safetica Client Service** - launches on operating system startup as a service which communicates with the database and Safetica Management Service. The client service ensures that

the security and monitoring modules of Safetica have access to the client stations.

- Endpoint Security Tools - the user interface with security tools and contextual menu. Can work in the following modes, based on the administrator's settings in Safetica Management Console:

1. The Endpoint Security Tools user interface with all security tools and a contextual menu available by right click on in the tray.
2. Context menu mode (Quick menu) with no user interface and basic security functions.



2.1 Introduction

Dear user,

Thank you for your confidence in Safetica. In this *manual for Safetica Endpoint Client* you can find a detailed guide for the client part of the software Safetica - the component *Safetica Endpoint Client*. Should you encounter a problem when using the software, consult this document at first *Frequently asked technical questions of Safetica users* and if you cannot solve it, kindly contact the technical support at http://www.safetica.com/support.

If you have any questions after reading the *manual for Safetica Endpoint Client* we recommend that you consult *the complete documentation for Safetica* in which you can find detailed information ranging from the first deployment in the company network through the examples showing the use of the product up to the evaluation of outputs and solutions of the most frequent problems.

To master basic practices and ways quickly, use the *Safetica quick wizard*. The most frequently asked questions related to the use of the software are answered in a document called *Frequently asked technical questions of Safetica users*.

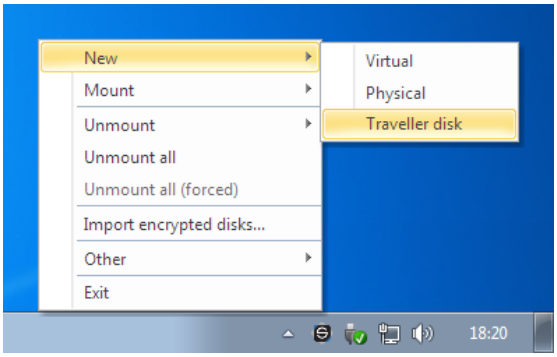
Thank you,

Safetica Technologies team, producer of Safetica

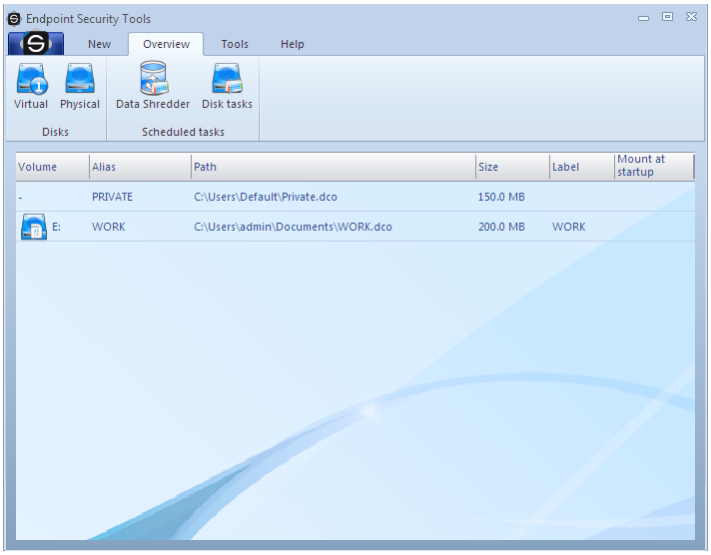
2.2 Endpoint Security Tools Description

Endpoint Security Tools user interface is composed of following parts:

1. **Quick menu** - Basic user menu marked by an icon . It provides first of all quick choices - disks disconnection, safety profiles set up, looking up existing archives or closing a program.



2. **Bookmarks** - Selecting a bookmark you select your goal. If you want to secure a disk or archive, view a overview of current options, use a tool or view the help, simply select the appropriate bookmark and an icon with target action in appropriate tab.
3. **Tabs** - Tabs will display a detailed selection of options corresponding with individual bookmarks.
4. **Desktop** - Displays all processing information about your safe disks, encrypted documents, planned tasks or others. User's complete activity with disks and archives is routed to the desktop.
5. **Contextual menu** - Allows creating encrypted archives or safely data removing by means of the contextual menu of the browser.



2.2.1 Overview

Tab Overview provides you menu with different overviews based on the description. There is a tab Overview on the image above.

1. Virtual disks

   This option shows a view of virtual disks only.

2. Physical disks

   This option shows a view of physical disks only.

3. Wipe Tasks

   Views wipe tasks.

4. Disk tasks

   Views disk tasks

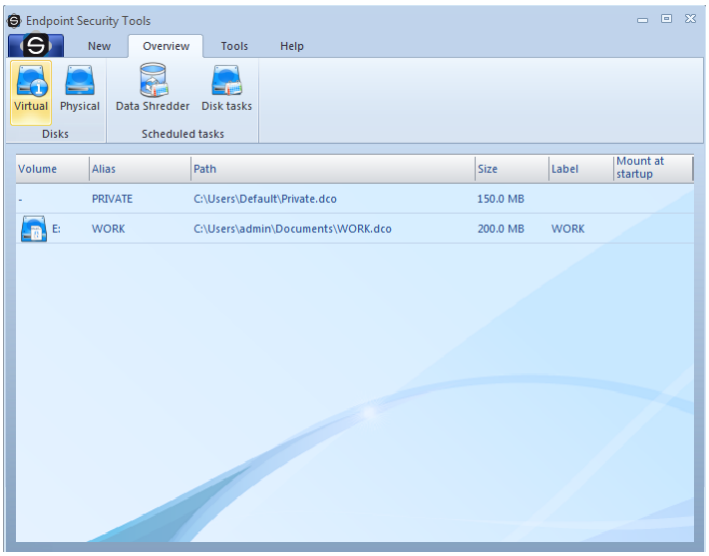
Navigation buttons make for simplifying the orientation in the program, switching between individual

views of disk types and setting up Safetica® properties. For more information on other navigation features click on individual options of a help.

2.2.1.1 Virtual disks

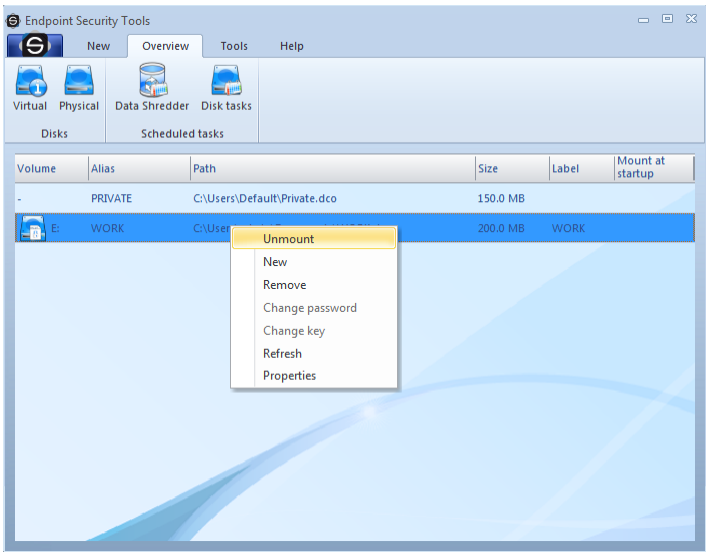
Virtual disk is a file encrypted by the Endpoint Security Tools software that behaves as a classical hard disk after connection. It means that you can create, modify, and copy files or otherwise work with your data on this disk. Furthermore, you can do low level operations with this disk such as formatting, defragmentation etc. There is one exception, however - the entire content will be encrypted with a security on an army level.

Virtual disks make a favorite way of data encryption. You do not have to use the whole disk for encryption as you have to in the case of physical disks. You just need enough free space on the disk. A guide through adding a virtual disk creates a file, the content of which is interpreted by the operating system as a physical disk.



The view of Virtual disks shows an overview of the virtual disks available. After adding a file of a virtual disk click on a Quick Menu - search virtual disks. Afterwards, select a path to the directory, where the file with a virtual disk is located and confirm your selection.

It is possible to manipulate with disks via a subnavigation the same way as with the physical disks. A subnavigation consists of the following items:

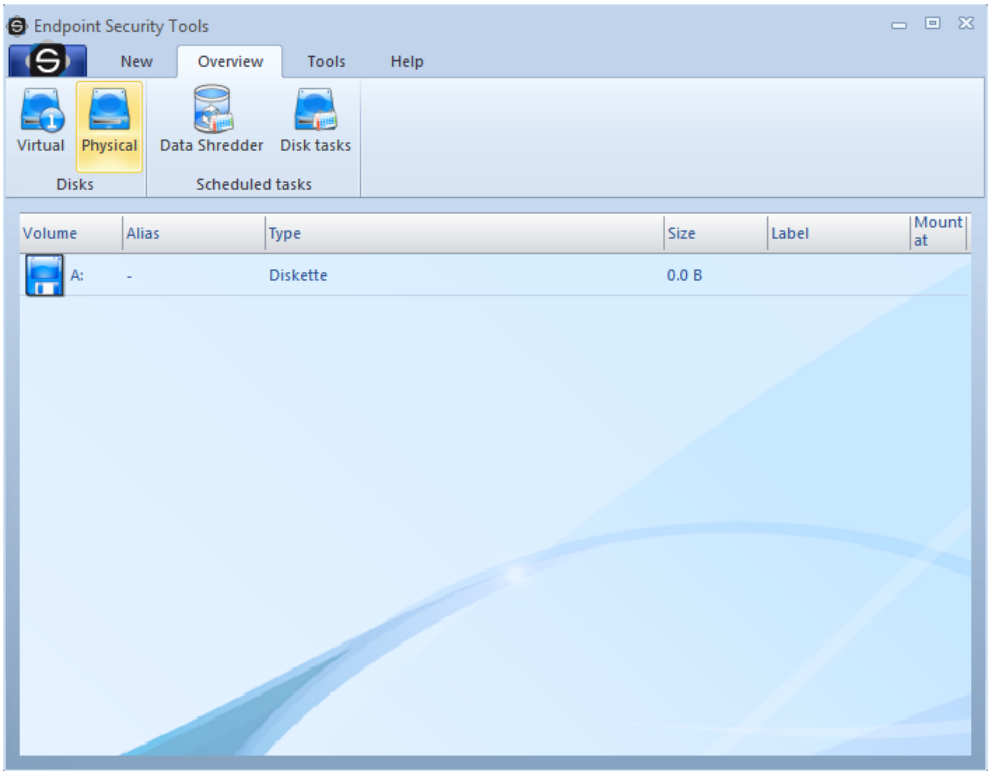


1. **Mount / Unmount** - The selected disk gets connected by clicking on this button provided that it is not connected yet. Otherwise, the disk gets disconnected.
2. **New** - Launches a guide that encrypts the disk selected.
3. **Remove** - Removes the encrypted format from the disk selected.
4. **Refresh** - Renews the information about selected disks.
5. **Properties** - Displays advanced information about a particular disk. Enables to change some disk properties.

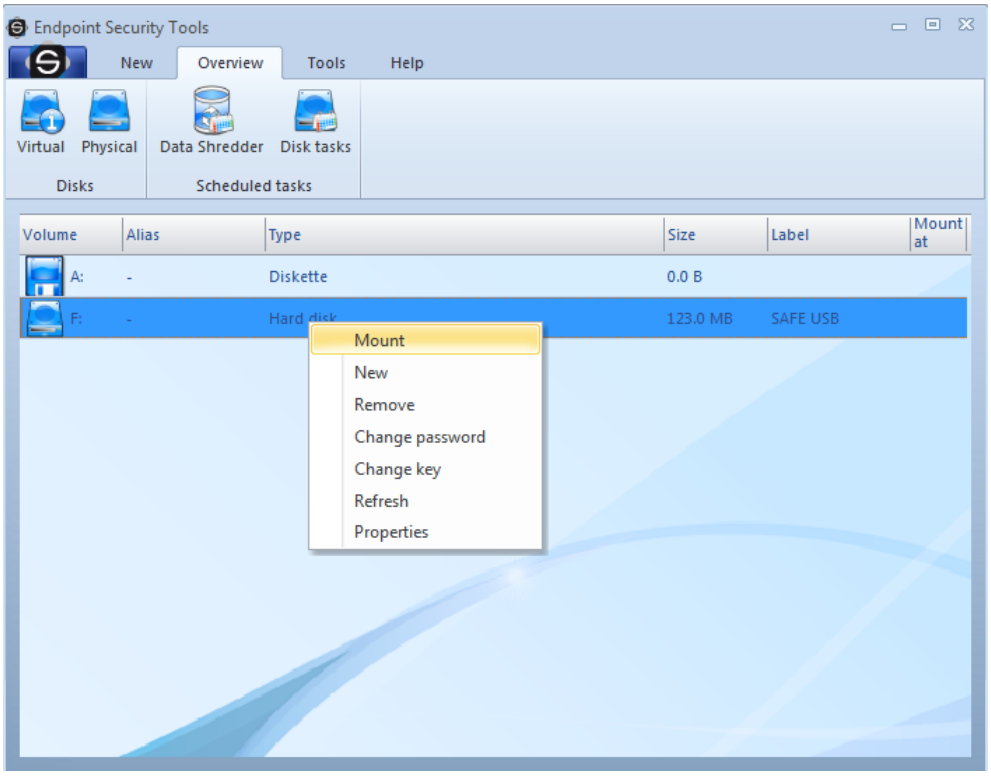
2.2.1.2 Physical disks

Physical disk is a medium capable of a random access. Namely, hard disks, disk partitions, exchangeable disks, flash disks, floppy disks 3,5", Zip drives etc. If you have a memory card reader, you can also encrypt any memory card. For example, Secure Digital, Compact Flash, xD-extreme Digital etc. But this is definitely not the end of the list of physical media. New and new types of storage devices emerge on the market every day. The encryption system Endpoint Security Tools is able to secure these devices as well.

The view of physical disks on the desktop shows an overview of the existing hard as well as exchangeable disks, Flash memories and floppy disks of all types. Every disk is represented by one line with detailed information.



Before manipulating with disks a selection of a particular disk on the desktop is required. You can manipulate with disks via subnavigation that consists of the following items:

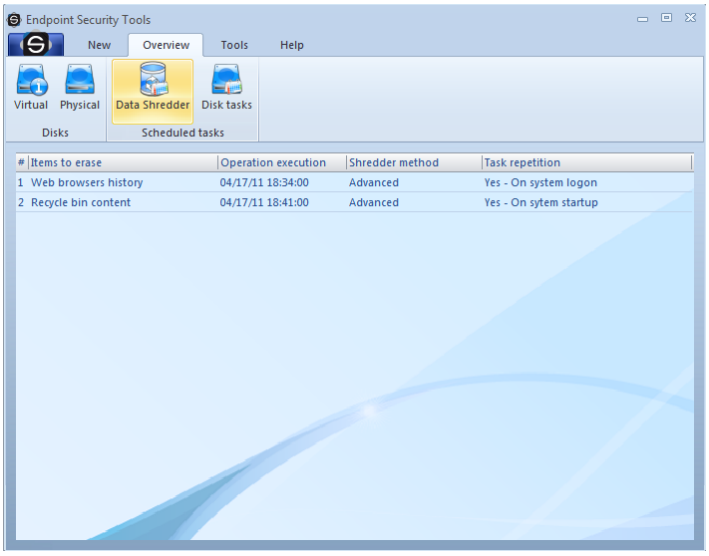


1. **Mount / Unmount** - If you click on this button, the selected disk gets connected provided that it was not connected before. Otherwise, the disk gets disconnected.
2. **New** - Launches a guide to the encryption the selected disk.
3. **Remove** - Removes the encryption format from the selected disk.
4. **Refresh** - Renews information about the selected disks.
5. **Properties** - Displays advanced and useful information about the disk selected.

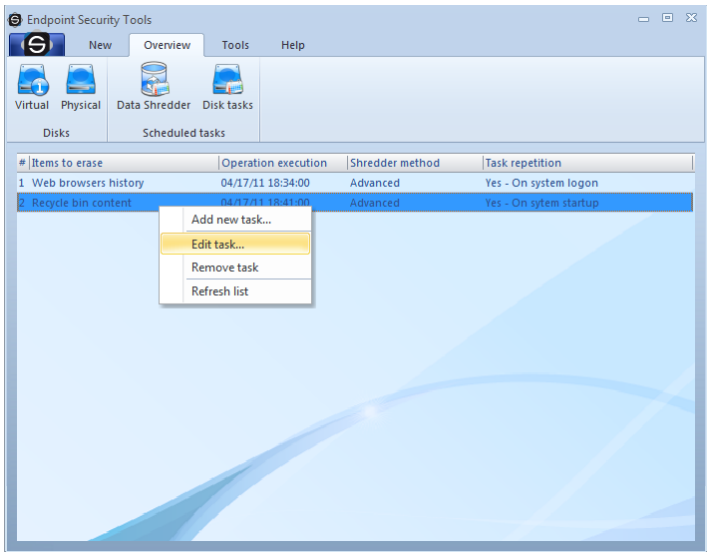
Note. Although the usage of the expression physical disk is not entirely accurate, it is used further in the text for simplicity.

2.2.1.3 Data Shredder

Shredding tasks is another feature of the Endpoint Security Tools. The activity of the shredder can be planned. It is possible to periodically safe-remove unnecessary data, for example temporary files created by surfing on the web. Just click on the tab Overview and Scheduled tasks.

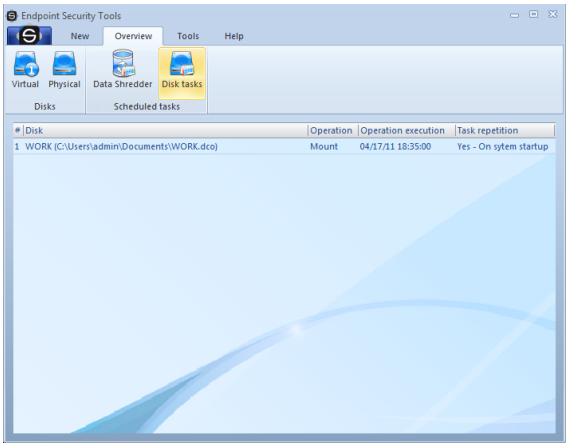


You can simply add or remove scheduled tasks.

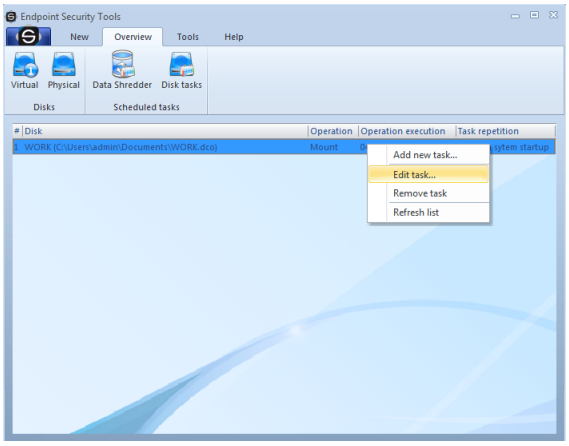


2.2.1.4 Disk tasks

With Endpoint Security Tools you can also create disk tasks. Disk tasks allows you to plan connection or disconnection of disks (to specific time, after logon). To view disk tasks, click the *Overview* tab and *Disk task* card.

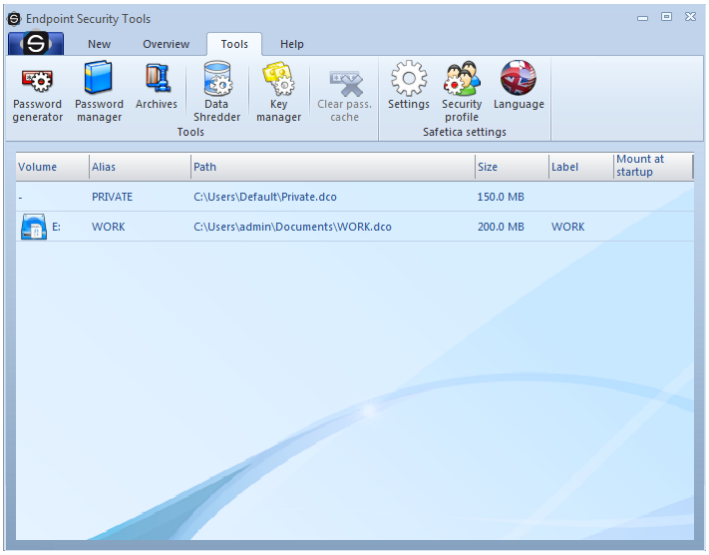


You can simply add, remove or edit disk by right-clicking on task in list.



2.2.2 Tools

The Tools tab mainly includes the access to Program Setting and to functions like Password manager, Archives, Key Manager or PC Lock.

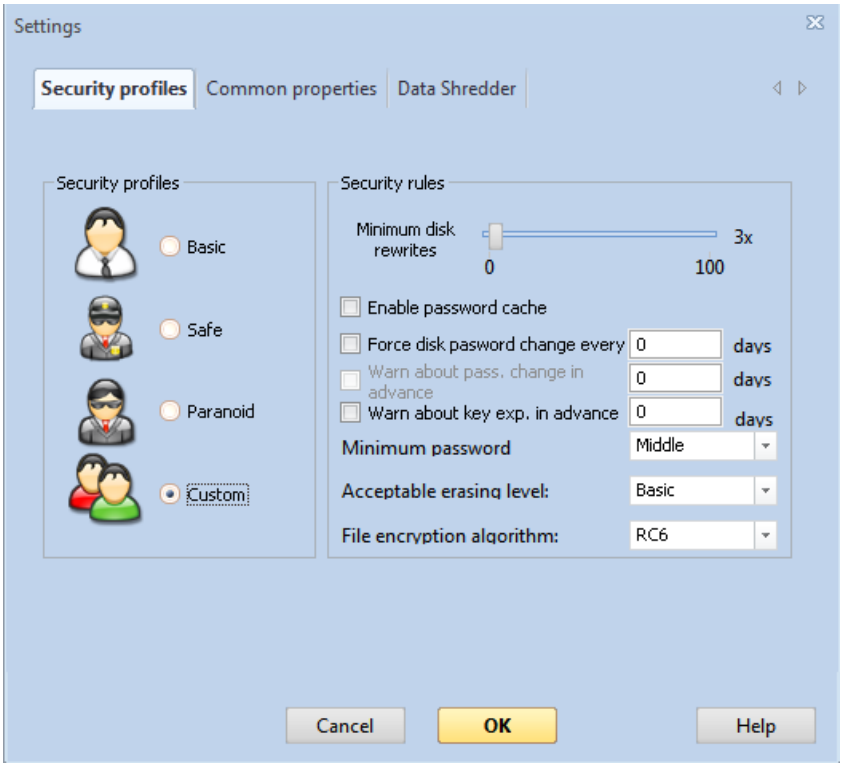


2.2.2.1 Settings

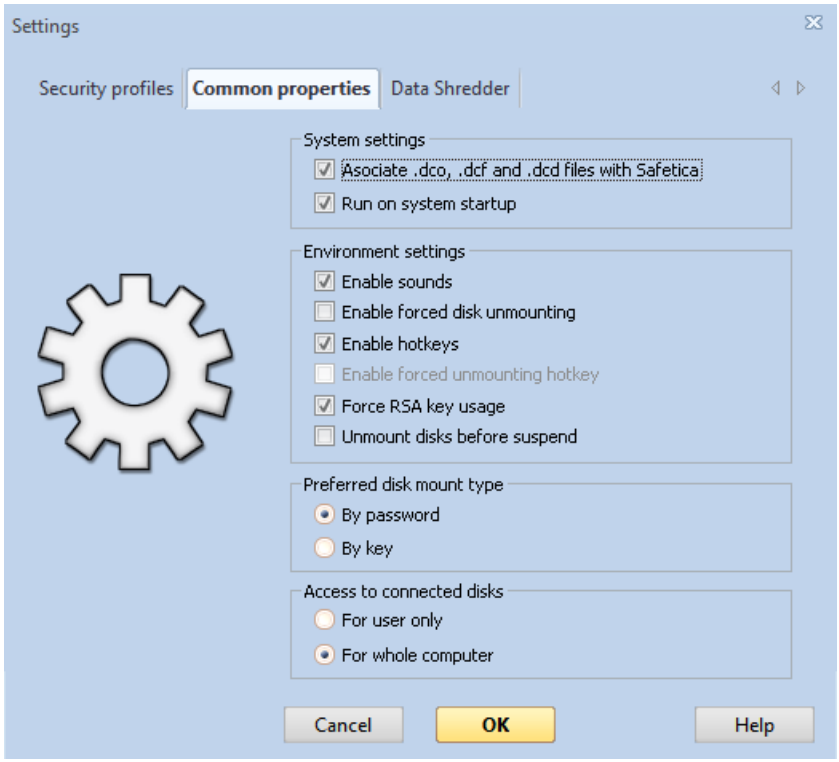
In the program setting you can switch on, off or change some useful options the Endpoint Security Tools offers. Thus it enables you to tune the program behavior according to your needs. You will be able to manage general and specific features as well as particular security functions.

Security profiles

Setting of security profiles is an option specifically for advanced users. In this setting you can change profiles from standard to User one by means of which you have set advanced security features on your own.



General features



From the system setting you can set general features related to your operation system.

- **Associate .dco, .dcf and .dcd files with Safetica**

  By clicking on a .dco type file in the Windows Explorer which is standard file of virtual encrypted disk of the system.

- **Run on system startup**

  Enables or restricts automatic launch of the Endpoint Security Tools jointly with operation sys-

tem start.

The Program setting enables you to better use the Endpoint Security Tools optional features according to your needs.

- **Enable sounds**

Sets use of sound effects at various program activities.

- **Enable forced disk unmounting**

Only advanced users are recommended to tick this option. This option enables hard disconnection of disks which means disconnection of disks even when the system works with them. This option is strongly not recommended because it may cause data damage on encrypted disks.

- **Enable hotkeys**

Comfortable option for all users. By pressing the Win-Ctrl-U key combination you ensure disconnection of all disks in standard manner.

- **Enable forced unmounting hotkey**

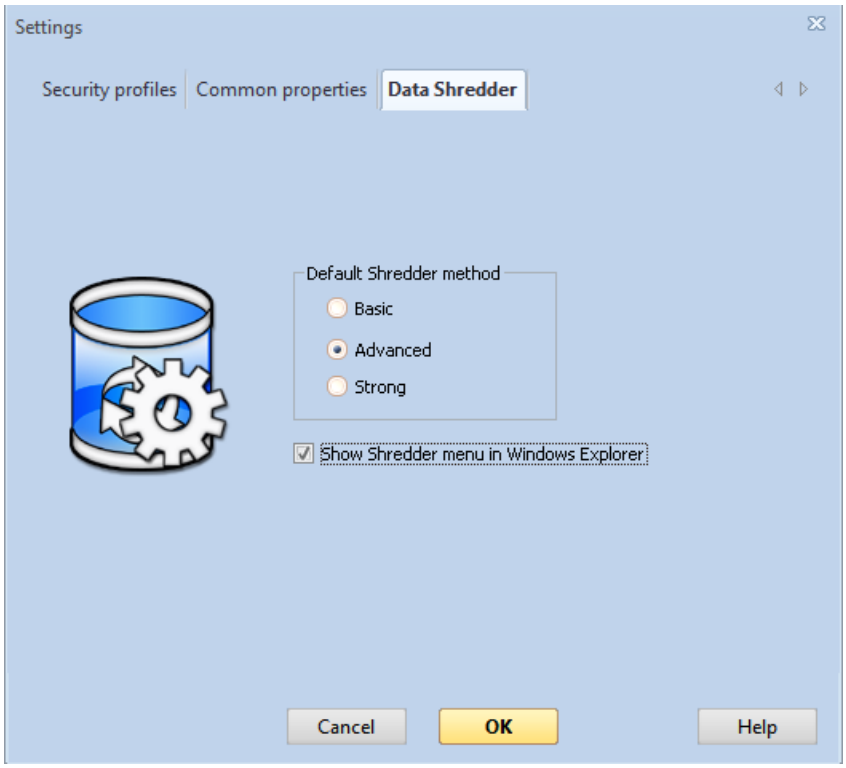
By the Win-Ctrl-Q hot key you ensure disconnection of all encrypted disks in hard mode.

- **Force RSA key usage**

By this option you will set the Endpoint Security Tools behavior so that the system will require use of security key at each disk creation from the user. This setting is suitable as prevention and possible rescue in case of password loss however it requires great caution. More in the chapter Security keys.

Data shredder

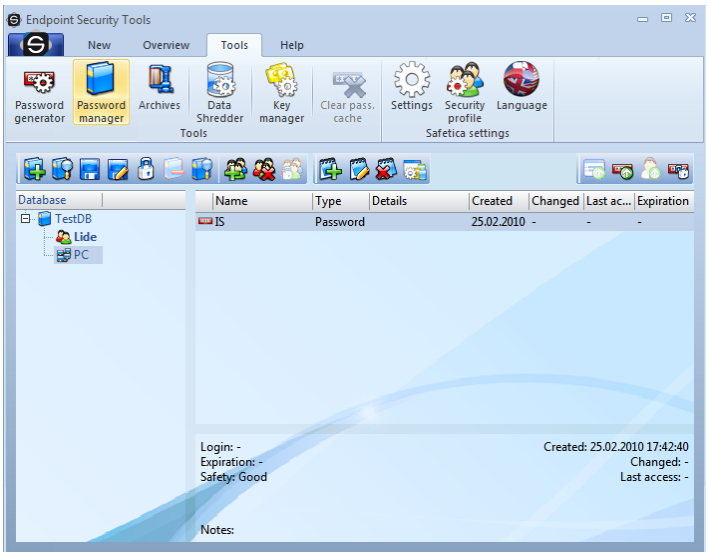
Setting of data shredder automatically sets the level according to the selected security profile. If you have your own security profile then you define the security of shredding algorithms on your own.



2.2.2.2 Password manager

The Password manager within the Endpoint Security Tools product provides secure control and overview of the most sensitive information we have. User names, passwords, access codes, PINs, payment card numbers, security keys, certificates and whatever other short text data and files can be organized and secured on the highest level by the Endpoint Security Tools through main strong password on army level.

All these information are saved in encrypted local structured databases. Various types of information can be divided in groups and subgroups, in types as for example password, contact, file or security key. Every other level can be secured by further password or security key according to information importance.



There is the Tree of your databases and groups on the left, on the right in the main part the records and details of selected database, group or record are shown. This view is dynamically changed upon concrete selected item. There is a toll bar in the upper part, divided in groups according to functions for databases, groups and records. Rightmost on this bar there are functions for copying of record in the box or showing of passwords in detail.

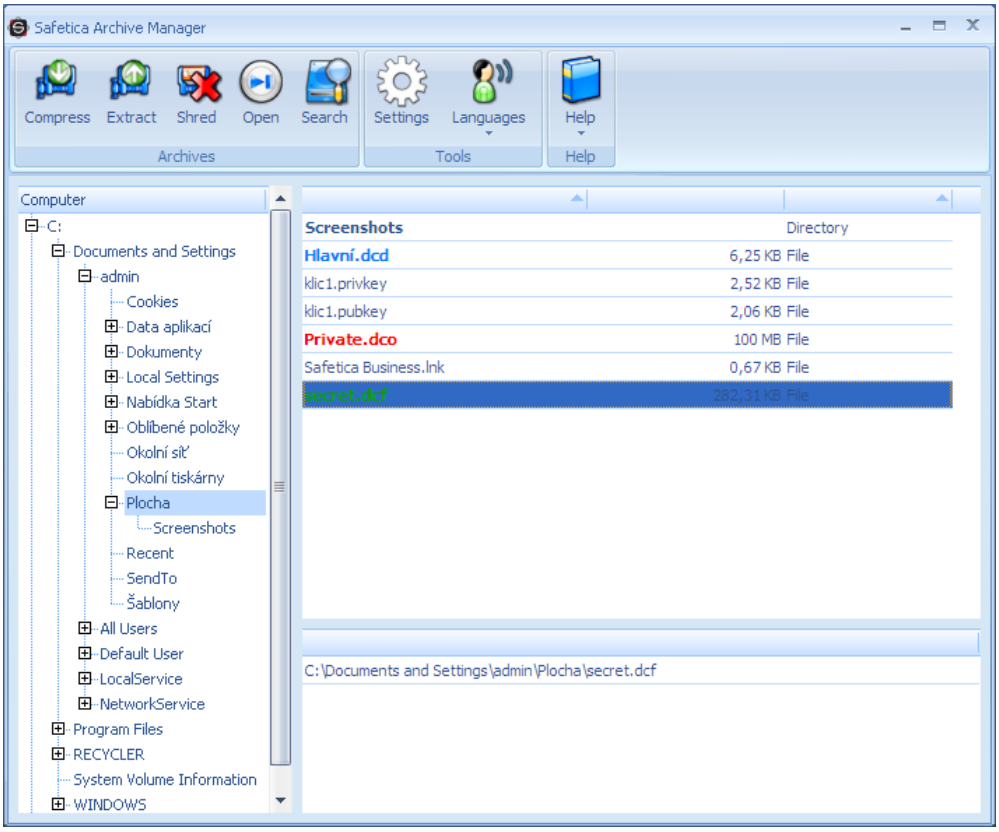
More detailed information on how to use the Password manager you will find in this chapter.

2.2.2.3 Archives

You certainly use the ZIP, RAR or eventually other archives. There are many expensive products supporting only archives and that do not offer any other options. In addition to the privacy security itself the Endpoint Security Tools also provides user with support of compression archives. The Endpoint Security Tools manages with all common archive files of ZIP, RAR, ARJ type and many others. Therefore you do not need to buy a separate and expensive compression software for nothing.

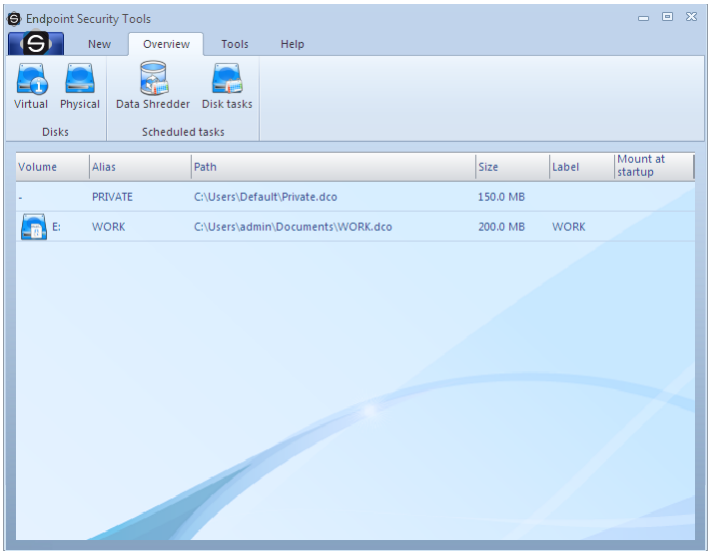
Endpoint Security Tools also supports the practical self-extracting archives. The data are simply packed into an executable file, transferred to another PC and unpacked by mere click and entering a password in. By use of self-extracting archives there is absolutely no need to use the Endpoint Security Tools software in target computers.

Beside the safe DCF format you can easily archive data in favorite type like: ZIP, GZIP, TAR, BZIP2. With Safetica Archive Manager you easily unpack common formats like: RAR, ZIP, CAB, ISO, ARJ, LZH, CHM, Z, CPIO, RPM, DEB and DCF.

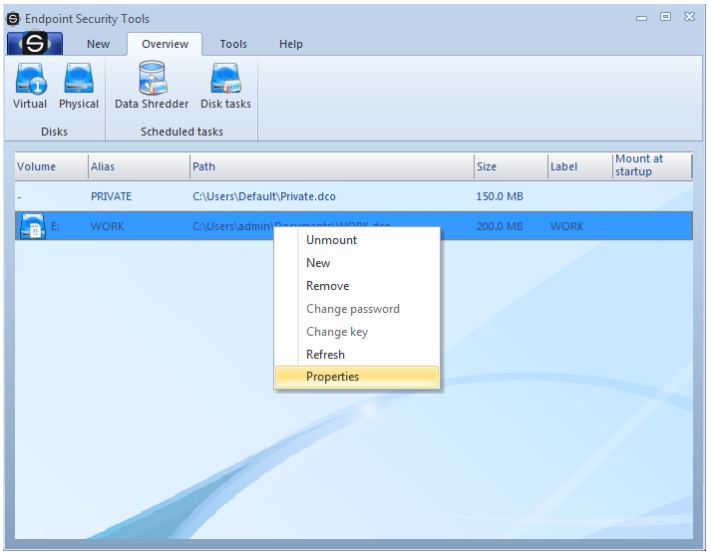


2.2.3 Desktop

The desktop includes the list of all encryptable disks. It also includes a detailed description of disk properties such as drives, labels, sizes, disk types, cipher types, and connection modes.



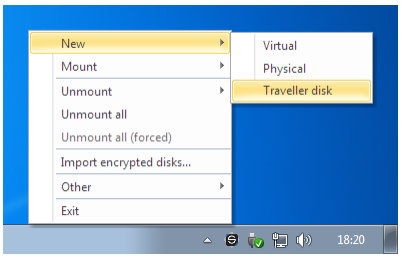
All important information about a particular view of an encrypted disk is collected on the desktop. Each line corresponds to one item.



Right-clicking on the desired disk brings up a menu for working with this disk. This menu is variable according to the view.

2.2.4 Quick Menu

The quick menu can be opened by right-click on the following icon in the tray. It allows you to perform the following operations over encoded drives (virtual, physical):



- *Open Endpoint Security Tools* – displays the main graphical user interface
- *New disk* – here you can create a new Virtual, Physical or Travel disk
- *Connect* – menu for connecting to Safetica disks
  - *Virtual* – virtual encrypted disks
  - *Physical* – physical encrypted disks (Safetica versions 5.4.0 and later)
  - *BitLocker* – physical disks encrypted with BitLocker.
  - Unknown – disks not formatted or physically encrypted disks created with Safetica versions 5.3.2 and earlier are listed here. Disks created up to this Safetica version can be connected via the Unknown menu. On Safetica versions 5.4.0 and later, physical Safetica disks are listed in the section Physical.
- *Unmount* – drive disconnection menu.
- *Unmount all (force)* – everything is disconnected, even if the drives are currently working. Data loss may occur.
- *Import encrypted disks...* – opens the dialog for a virtual drive import.
- *Other* – allows other operations over drives:
  - *Remove* – selects the drive to be removed from a list.
  - *Properties* – displays the properties of the connected drive.

- *Change password* – select the drive for password change.
- *Change key* – select the drive where the security key should be changed.

? *Update* – updates disk lists in the quick menu.

- *Exit* – closes the Safetica Endpoint Client graphical interface (the client service keeps running).

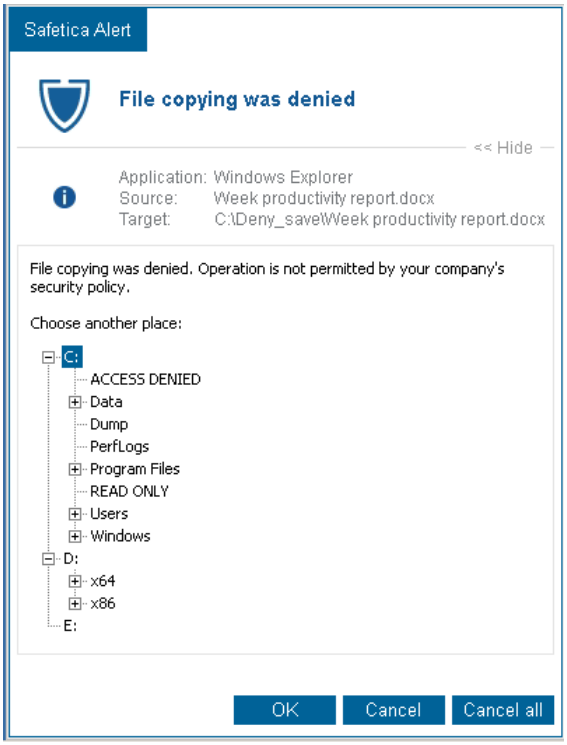
2.2.5 User Dialogues

Using the announcement dialogs, Safetica Endpoint Client displays for the end users messages about forbidden or allowed activities or displays queries and notifies of important events.

The dialogs display in the lower right corner of your desktop. There are several types of announcement dialogs. Individual types of dialogs require different interaction with the user (confirmation, rejection, selection from options or paths).

Description of announcement dialog

The announcement dialog has its name included in the header. In the center is the name of the announcement with the announcement itself. Below the announcement are buttons for confirmation, cancellation and other buttons depending on the announcement dialog type. In the lower left section you can switch between the announcements if there are more unread ones.

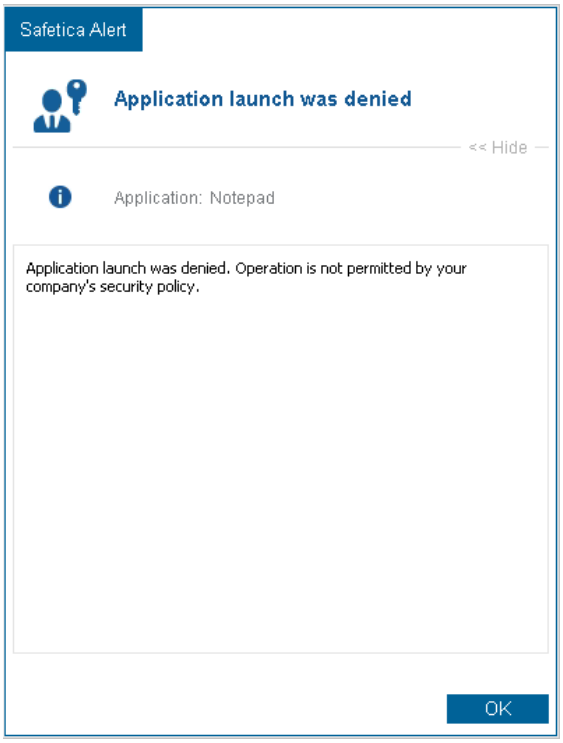


Types of announcement dialogs

Notification dialogs

Information dialogs only inform you about the situation that occurs. Such as blocking of a forbidden application or a USB disk.

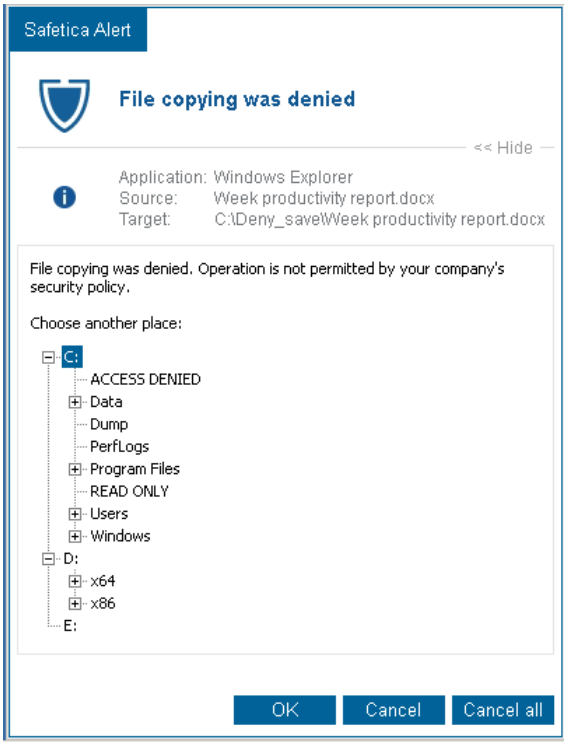
Following is an example of dialog:



Query dialogs requiring larger intervention of the user

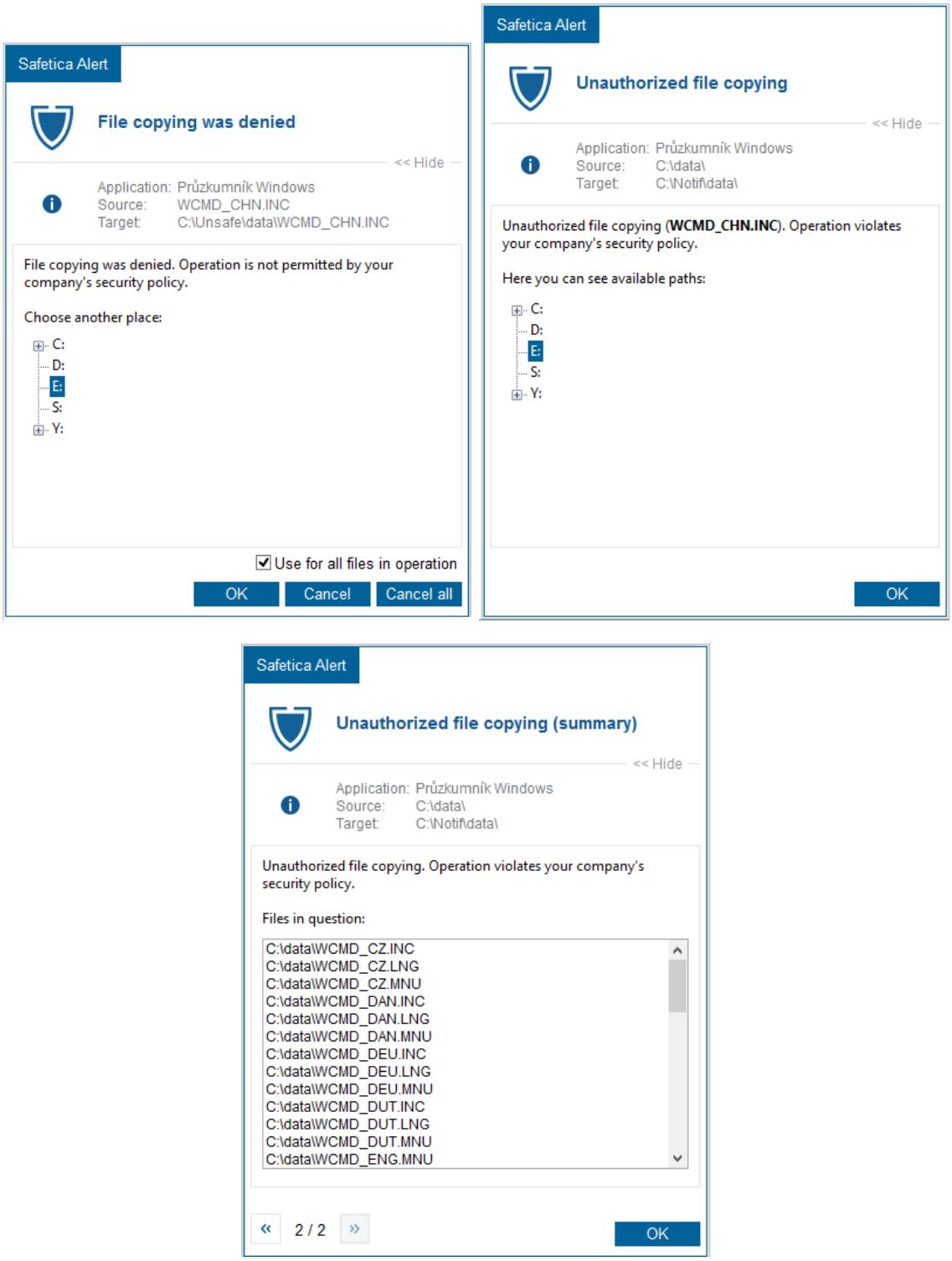
This type of a dialog is displayed only by the DLP module. In addition to the read confirmation as in the previous type these dialogs require a more extensive action. For example, when copying a secured file to an unsecured location you are notified of this fact and you can select a secured target location etc. The options you will have at disposal depend on a type of the particular action.

Following is an example of dialog:



Note: When handling multiple files subject to a security policy, the user will see only one dialog with a summary of all corresponding files.

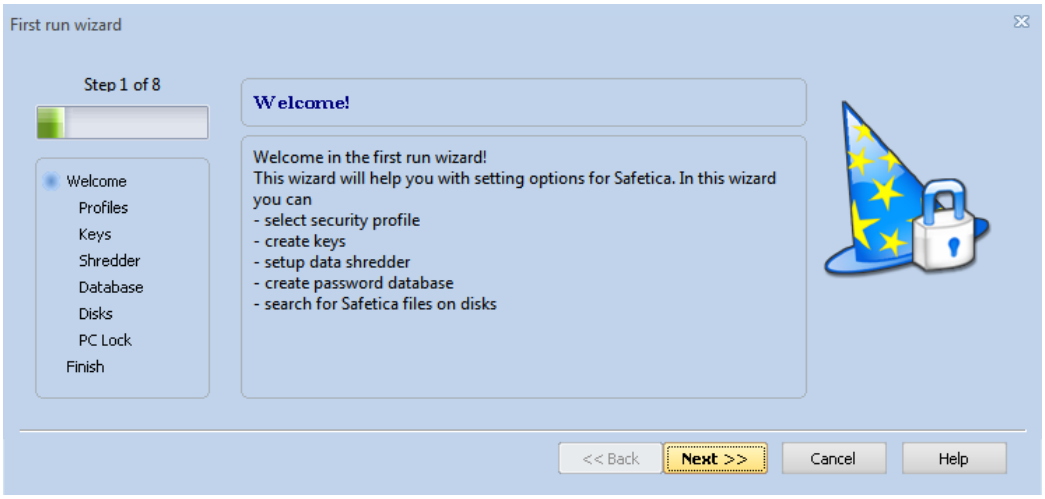
If the user needs to use the dialog (due to a security policy) to specify or change the operation, the user can apply the change to all files within the operation by toggling the checkbox Use for all files within the operation.

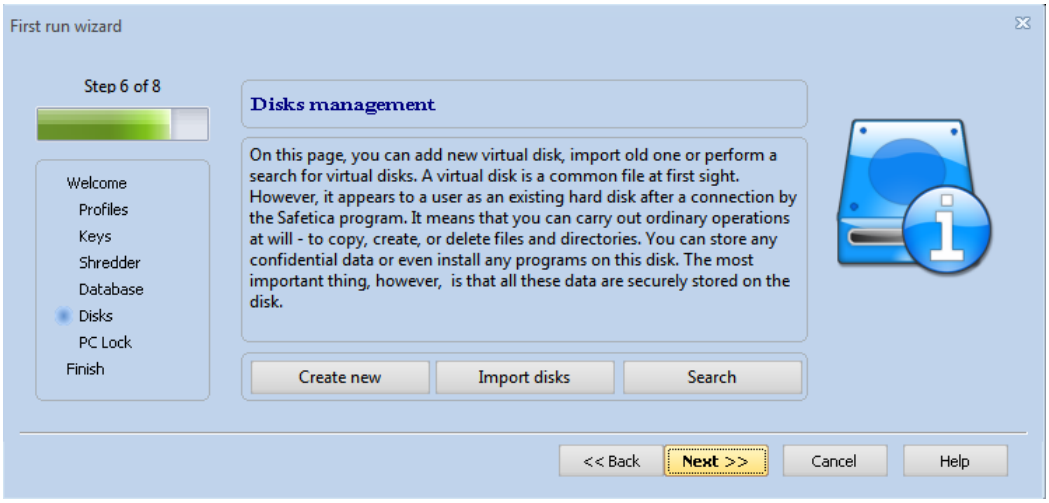


2.3 Using Endpoint Security Tools

2.3.1 First launch

For acceleration and improvement of work with the Endpoint Security Tools the program will guide you by first run wizard. It will reliably guide you through the Endpoint Security Tools so that even a less experienced user can use it. From selection of security profile through formation of access data database to creation of virtual disk or import of old settings.





Having finished the wizard the Endpoint Security Tools welcomes you by its main window. After first run we recommend to study the Help first in order you are able to control the Endpoint Security Tools even more easily. Therefore select in the Help tab the item Help topics.

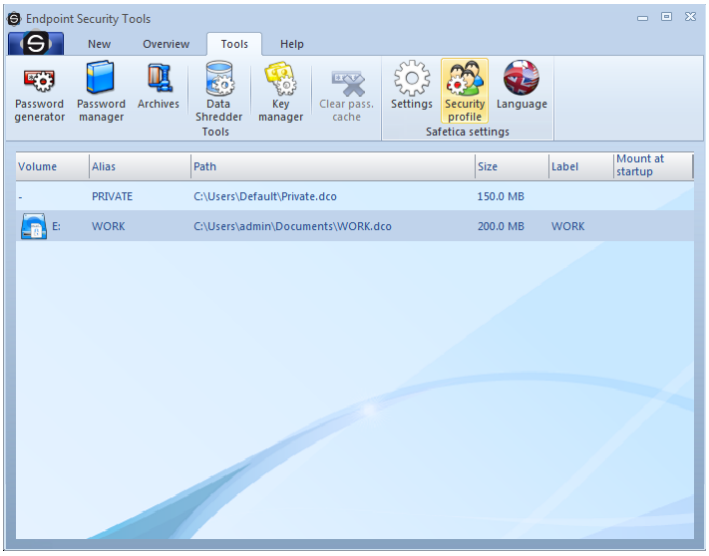
You will also find the contact button here which will direct you to our pages with contacts to technical support. You can also display Tips of the day which are shown after the start. If you want to pass again through the program setting, create new disks, databases or keys in one step, use again the First start wizard.

If you wish to secure your disks, continue by clicking the chapters about disk creation: How to create a physical disk, New virtual disk creation.

2.3.2 Security profiles

Security always begins with the choice of a good and a high quality password. Another choices - such choosing of cipher algorithms and levels of shredding-are recommended much more for advanced users. Common user does not have to bother with these particular settings and can let Endpoint Security Tools to set it for them. Endpoint Security Tools will offer you a choice from prepared security profiles - from the basic up to the most safe one.

For advanced users there is a Custom profile, where you can set every part of security feature yourself, after choosing this profile, the settings will be available in Settings section. In the tab Tools select Security profiles.



The wizard helps you to select the right profile for you.

Security profiles:

- **Basic** – Allow medium level of passwords, automatic choice of quick and safe cipher and data shredder with 3 cycles.
- **Safe** – forced use of high level passwords, the AES cipher will be used (winner of the new encryption standard), data shredder with 7 cycles, permitted password remembering.
- **Paranoid** – password remembering is not allowed, data shredding in 35 cycles (according to Gutmann standard of department of defense of USA), used the most safe block cipher Serpent and forced frequent password changing.

For common use it is just enough the Basic profile, but we recommend the Safe profile.

2.3.3 Security keys

An important feature of the Endpoint Security Tools is the possibility of restoring the user data from the virtual disks, as well as the physical ones. The security key is in case of forgetting the password the only possibility, how to make an access to your data.

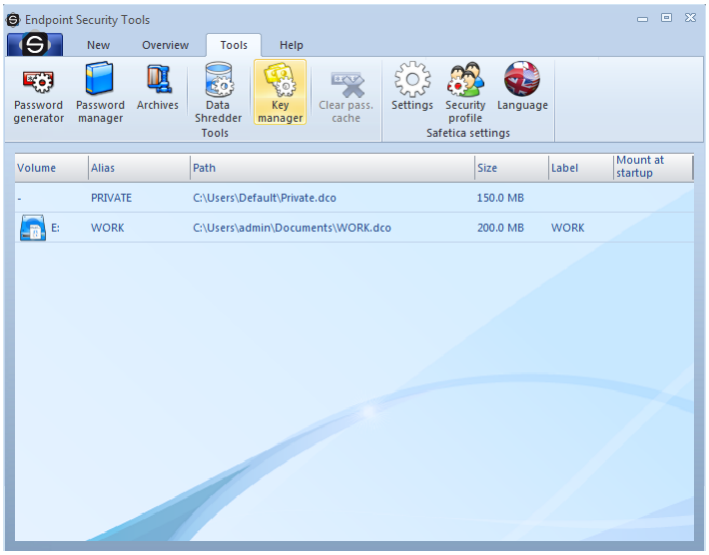
Every security key consists of two subkeys - the *private security key* and the *public security key*. The private key serves for unlocking of the encrypted disk in case of losing the password; on the contrary, the public key creates in the Creating disks wizard a lock for the private key, which will open this lock. The private key is saved as a file on the secured and reliable place (like a CD disk and saved in the safe), while the private key is possible to move among computers and use it for mutual creating of the security locks to your data. For the distribution of the public keys the import and export commands serve, which will be inscribed below. You can find more about this also in

the chapter about the exporting and importing.

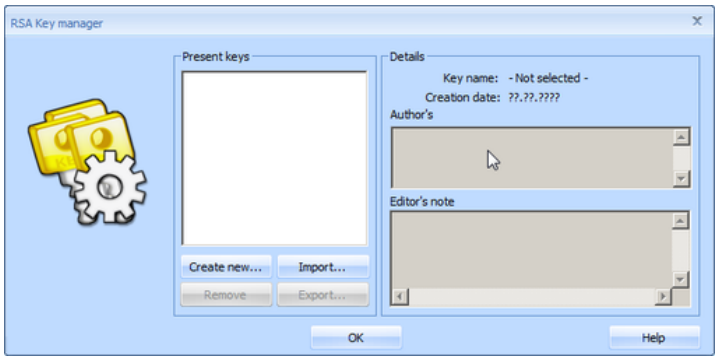
Every security key pair is mutual. If you create more security keys (pairs - the private key and the public one), only the corresponding pairs will cooperate. With the concrete public key you interlock only one concrete private key. You can use the private key to lock only these disks, which are locked by the same private key.

2.3.3.1 Creating of the Security key

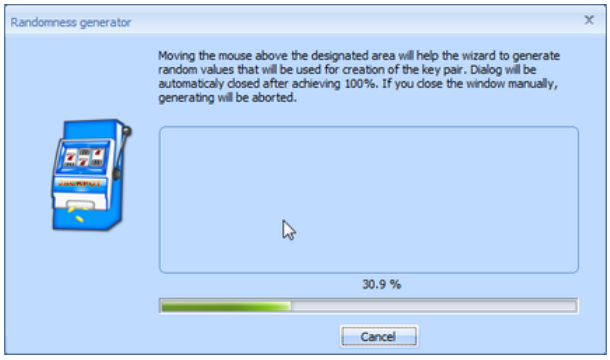
When you first run the main Endpoint Security Tools, there will be a question about the possibility of creating your security key. In the Key Manager dialogue you can create the security key manually - in the menu click on the *Tools -> Key Manager.*



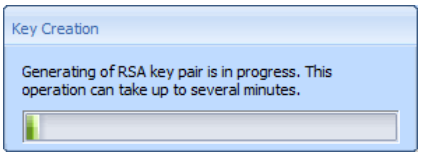
If you haven't created a security key yet, click on the Create new button.



The creating of the security key wizard will guide you through the process step by step. In the first step the wizard asks you to do an unusual thing. In the middle of the dialogue an empty rectangle will show up. You will move the mouse cursor randomly as to how the image shows you. The wizard gains amounts of random data, so that he can ensure a generating of a high-quality key to your disks.



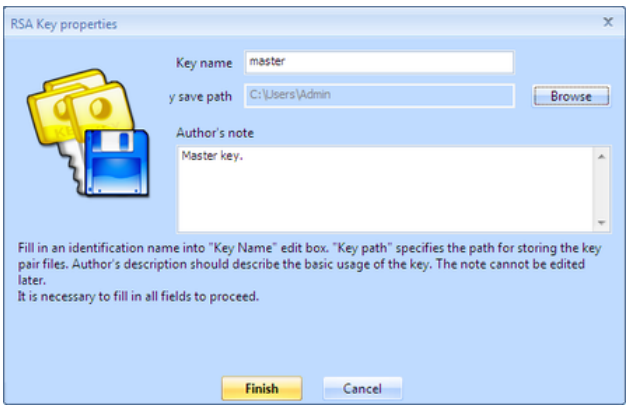
Once the sufficient amount of random data is gathered, the wizard immediately starts the generating of the security key. This operation may take several minutes depending on the speed of your computer.



The key is now created. The wizard asks you for entering the name of the key as well as its description, which you can use, when you want to recognize it. Now click on the Browse button and choose a secured place, where you save the file with its private key.

WARNING!

It is necessary to save the private security key to maximum secured and reliable place within the range of possible attacker. Using the private security key it is possible to unlock the data on your disks, which are created using the security key. Devote to choosing of the place maximum precaution.

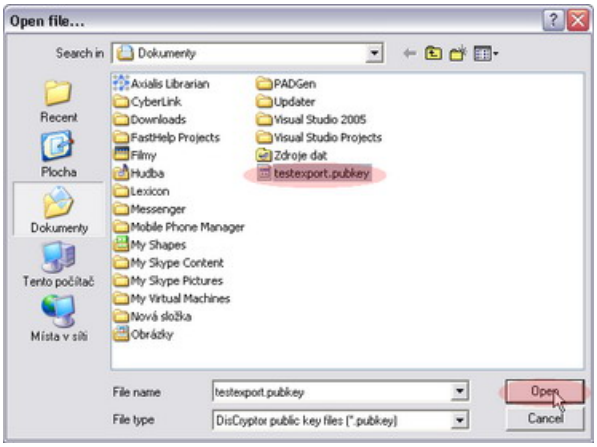


As soon as the choosing of the place is complete, click on the Save button and finish the wizard by the Finish button. If everything went well, the dialogue about the successful saving of the private key will show up. Now click on the OK button. Now your security key has been placed to the Endpoint Security Tools, you can abandon the Key Manager.

2.3.3.2 Key administration

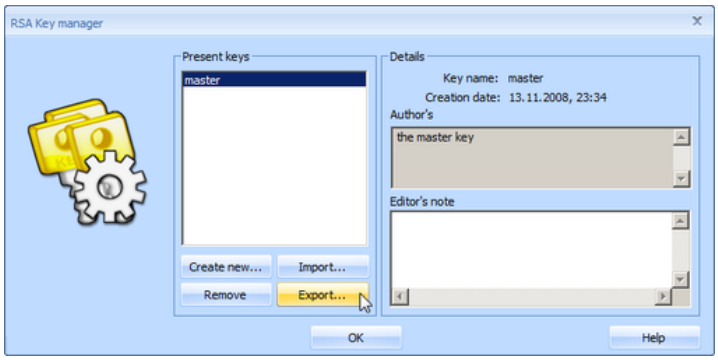
The main administration of the security keys you can perform in the Key Manager - in the menu click on the *Tools -> Key Manager*. If you are the server administrator, you can force the user to use the key.

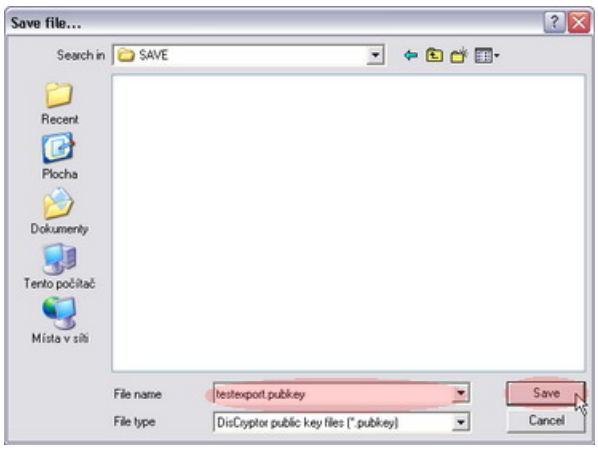
After the addition of the created public security key click in the Key Manager on the Import button. Choose appropriate security key and confirm this by clicking on the Open button.



Exporting of the created key

For the distribution of the public key it is necessary to export this key to the file at first. Choose the key in the table and click on the ***Export*** button. In the dialogue choose a file, which will be used for saving the key and click on the ***Save*** button. Keys exported this way you can distribute e.g. on another computers in your whole network.

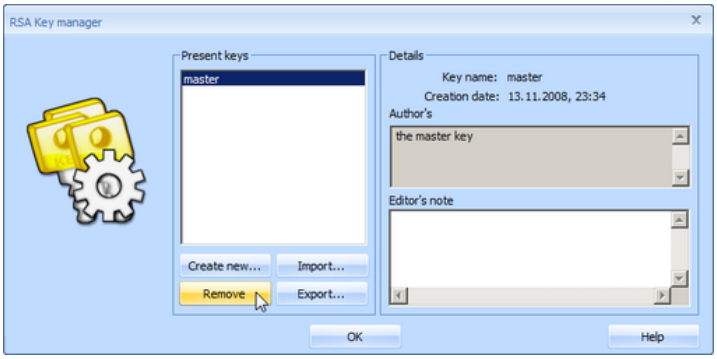




Deleting of the security key

The existing keys you can also erase. Choosing the key and clicking on the Remove button you erase the public security key from the list. The Key manager allows you only erasing of your public security keys. The private keys keep untouched. You can therefore restore data from the disks by the private key.

But by erasing of the present keys list you will no longer be able to create alike disks for the restoration by the same private key! Thus we don't recommend removing the keys!



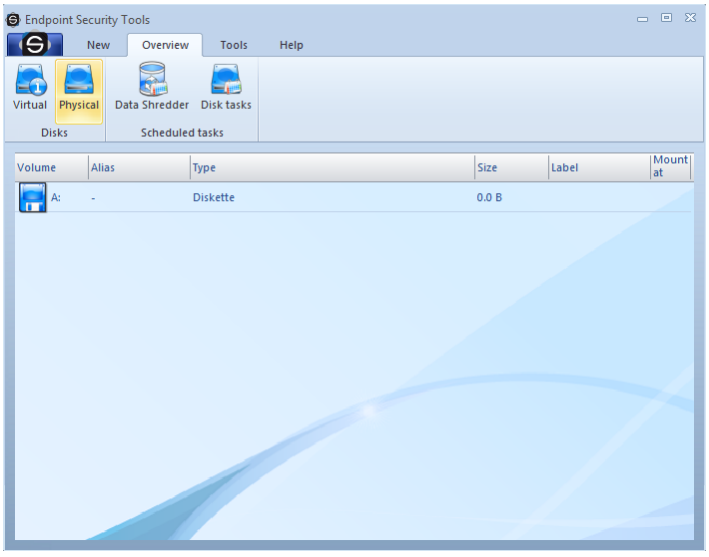
2.3.4 How to create a disk?

2.3.4.1 Encryption of an existing physical disk

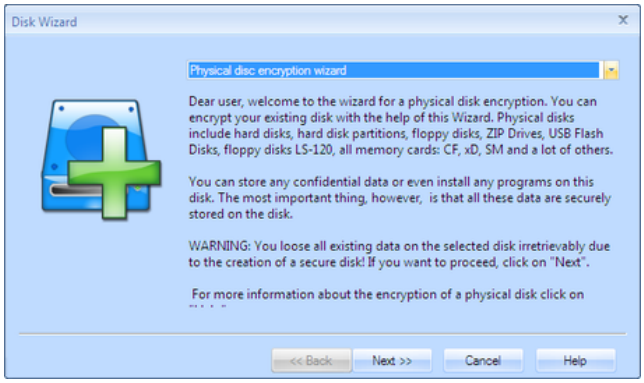
Physical disk is an existing disk of the following type: hard disk, USB disk, flash disk, floppy disk 3.5", ZIP Drive, memory cards, and a lot of other types of exchangeable disks. Physical disk is also a hard disk partition. Endpoint Security Tools is able to encrypt all of these devices very easily.

WARNING: You lose all original data by encryption. Do a backup of all data prior to the encryption! After the encryption process is finished, you can copy your data back to the encrypted disk.

In order to encrypt a physical disk, click on the navigation button Physical disks, select the disk you want to encrypt on the desktop and click on the subnavigation button New. Then a guide opens that guides you step by step through the encryption.

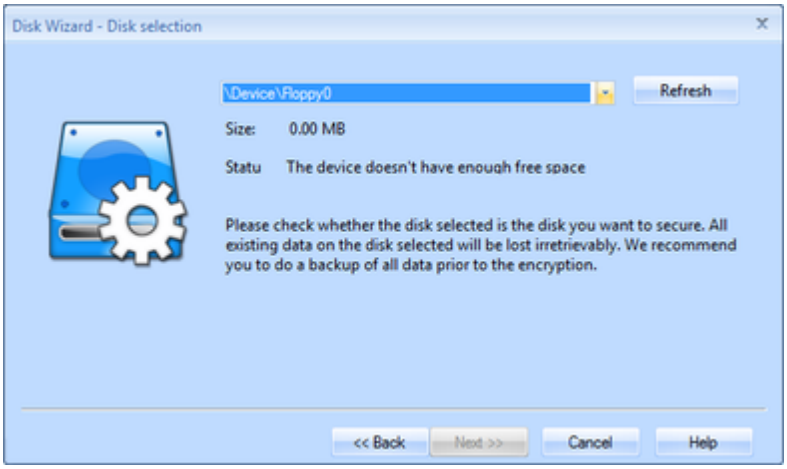


After you read the information on the first page of the guide, click on *Next*.

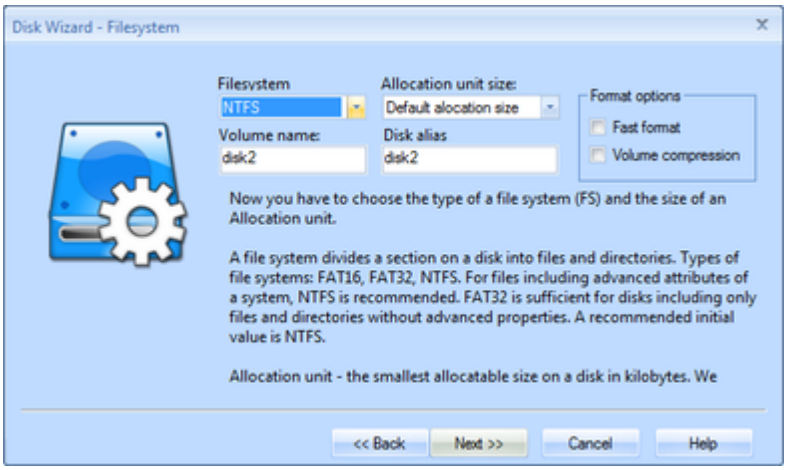


In contrast to a virtual disk, the size of which you can choose at will, a physical disk always has a fixed value.

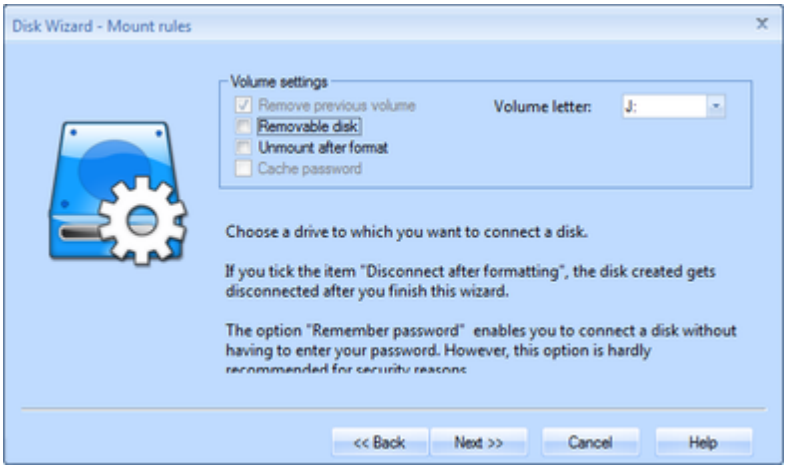
Check whether the disk you selected is the disk you want to encrypt. Then click on ***Next***.



Now you have to choose a file system, an allocation unit and a disk label. If you want to encrypt a physical disk or its partitions, the NTFS file system is highly recommended. We also advise you to set the size of an allocation unit to the *initial size of allocation*. For exchangeable disks, in particular for those of smaller size, FAT32 is enough. After you perform these actions, click on *Next*.



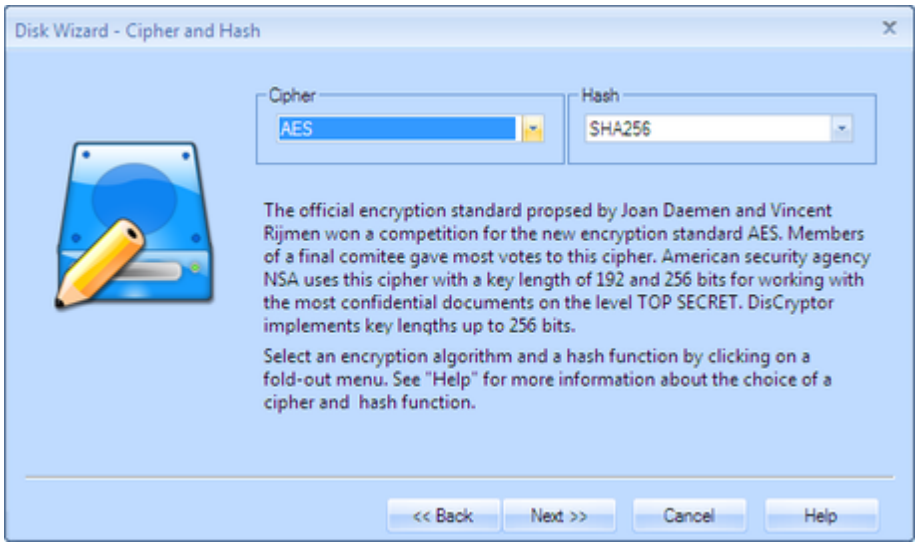
In the next window you can choose a drive you want to connect a disk to or you can just keep previous settings. After you finish your selection, click on **Next**.



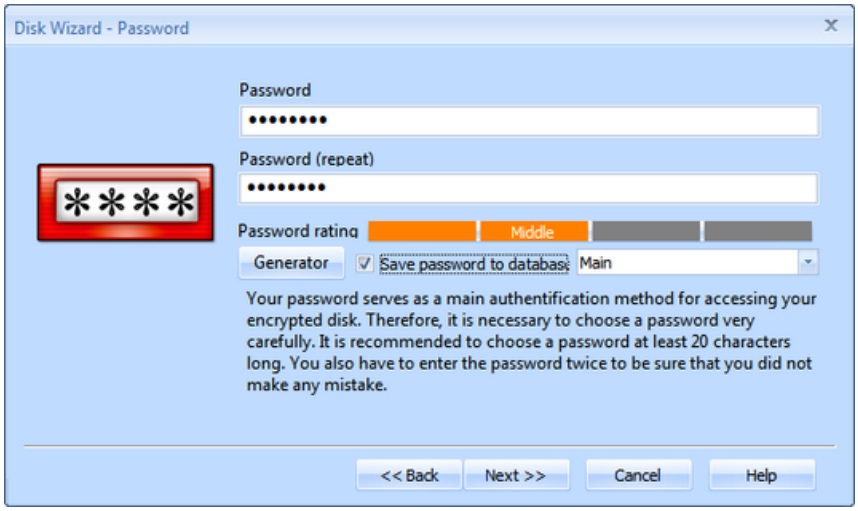
The next step is the choice of ciphers. You cannot make a mistake whichever cipher you choose. We did our best to choose optimal ciphers and sizes of their keys with emphasis on their security and speed.

In case you save very risky stuff or programs, we recommend you to use the following ciphers: Serpent, Twofish, Rijndael(AES) or Blowfish. On the contrary, for less inhospitable conditions, and for frequent and bulky file transfers the RC5, RC6, or Twofish are recommended. These ciphers excel not only in security but also in the speed.

Generally, we have to point out, however, that the choice of a cipher itself is a secondary matter. Above all, we recommend you to choose your access password very carefully. You can learn more about the security of ciphers in the chapter Frequently asked questions. To confirm your selection click on Next.



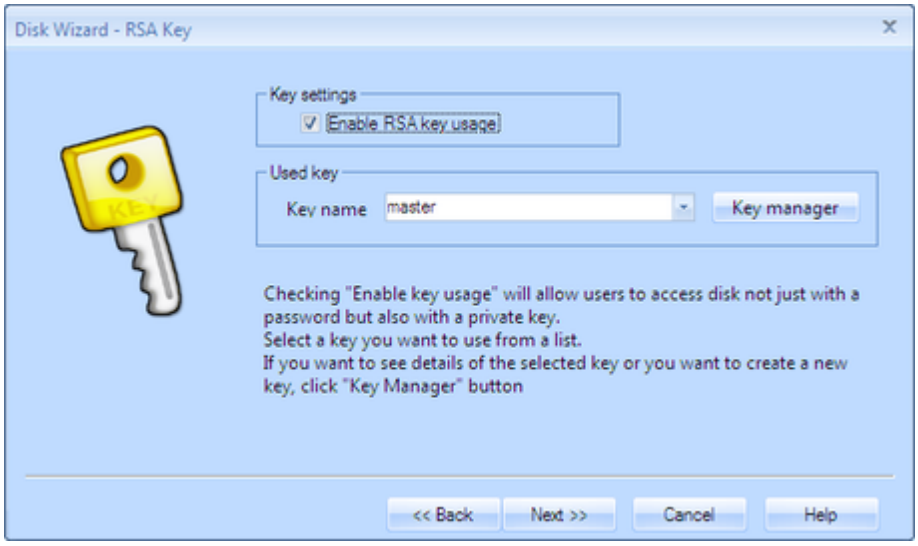
A key decision in the whole guide is the choice of a suitable password. There is a special chapter on this topic. To generate a safe password can you use the Password generator, which is integrated in the dialog. Your password can be immediately stored in any database or group in the Password manager. Before you choose a password, we recommend you to study materials given here. Generally, it is recommended to choose a password with al least twenty characters. After you enter your password and re-enter it for verification, click on Next.



The wizard has automatically generated the disk key, which will be used for the encryption of the disk.

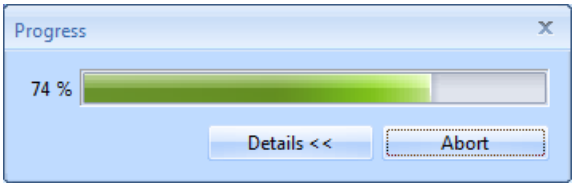
According to the program settings you can or must choose the using of the rescue security key for the creating disk. This security key is used for the access to the creating encrypted disk in the case of forgetting its access password. It is therefore a rescue fail-safe, but it is necessary to treat with it very carefully. If the security key comes at unwanted, the attacker can easily abuse the disk, on whose the security key is used. In the case in the Endpoint Security Tools exists no security key, the wizard will be automatically engaged. You can create or import a key in this wizard. You can allow using of the security key by ticking the Allow using of the security key and choosing the key from the highlighted menu. When the choosing is finished, click on the *Next* button.

You can learn more about the security key problems in the Security keys chapter.



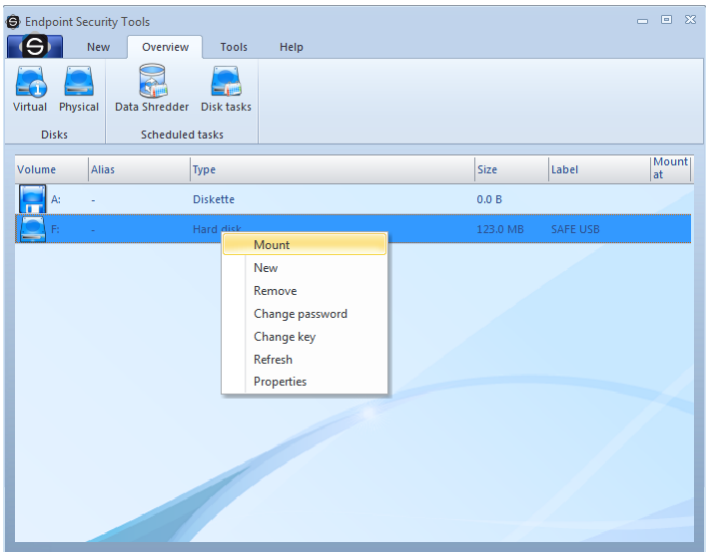
Check the entered data for the last time and click on the *Finish* button.

It is also necessary to format a disk before you use it. The guide is just doing it for you.

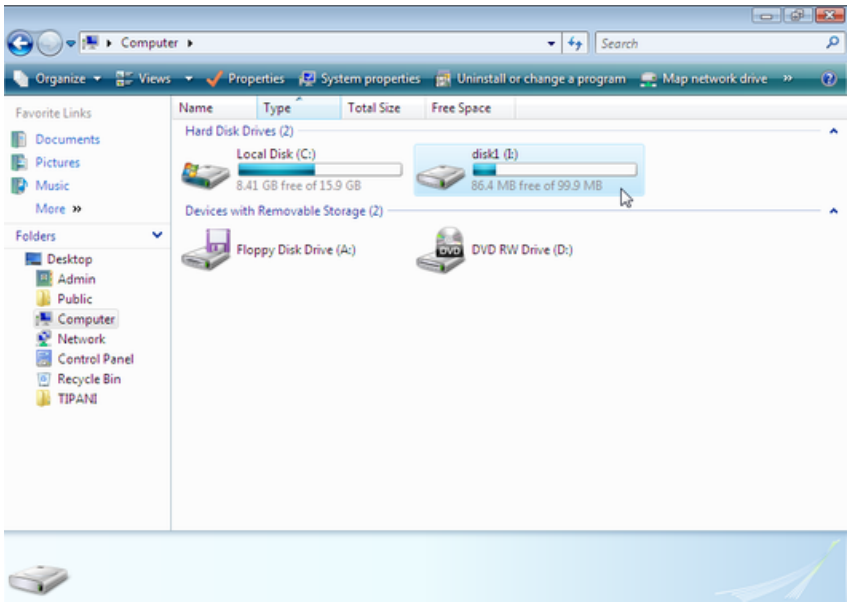


Congratulations! Your physical disk has just been encrypted and connected automatically. The

highlighted line displays the newly encrypted disk. You can open this disk by a double-click in Windows Explorer. If you want to connect this disk later, simply click on the view of Physical disks in the navigation, right-click on the line with this disk and select Connect.



This disk will show up in the system as a drive you selected in the guide, in our case drive I: From now on you can use this disk as any other disk. If you click on "My computer" in your Windows system, your encrypted disk will be displayed together with other disks.

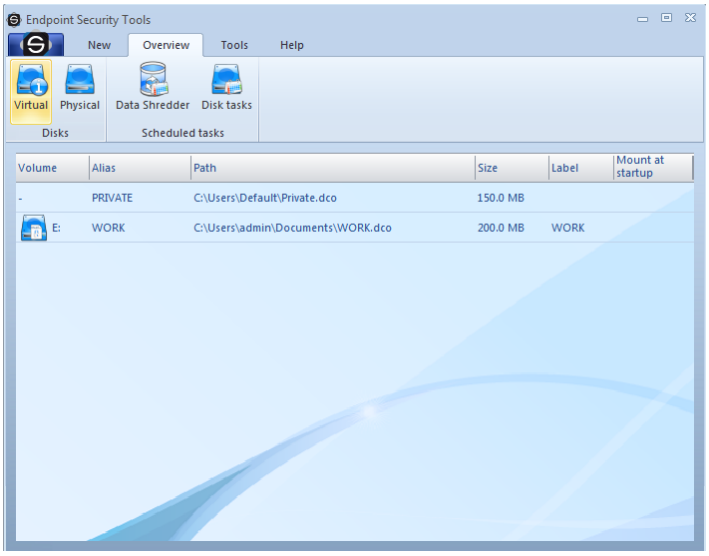


2.3.4.2 Creating a new virtual disk

Virtual disk is a file encrypted by the Endpoint Security Tools, which behaves same as an existing physical hard disk after connection. It means that you can create, modify, and copy files or otherwise work with your data on this disk. You can do low level operations with this disk such as formatting, defragmentation etc. There is one exception, however - the entire content will be encrypted with a security on an army level.

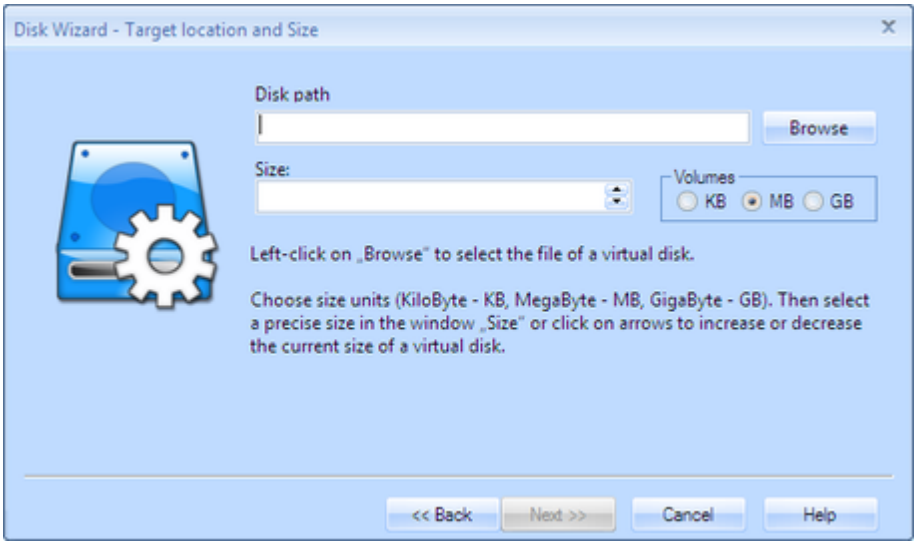
If you want to make your data accessible even on computers where the Endpoint Security Tools is not installed, choose the guide to a Travel disk. This utility of Endpoint Security Tools prepares a directory with a file of a virtual disk. Later on you can burn it on a CD/DVD or save it on another memory medium. If you insert this medium into a computer, you are automatically requested to enter your access password. After you do so, Endpoint Security Tools enables you to access your virtual disk.

In order to create a new virtual disk, click on the navigation button Virtual disks and the subnavigation button New. A guide to adding a virtual disk opens. This guide is an ideal aid, with the help of which you can quickly and easily create your secure virtual disk. The guide prepares, creates and formats the disk on its own. It also helps you with key choices you have to make throughout this procedure.



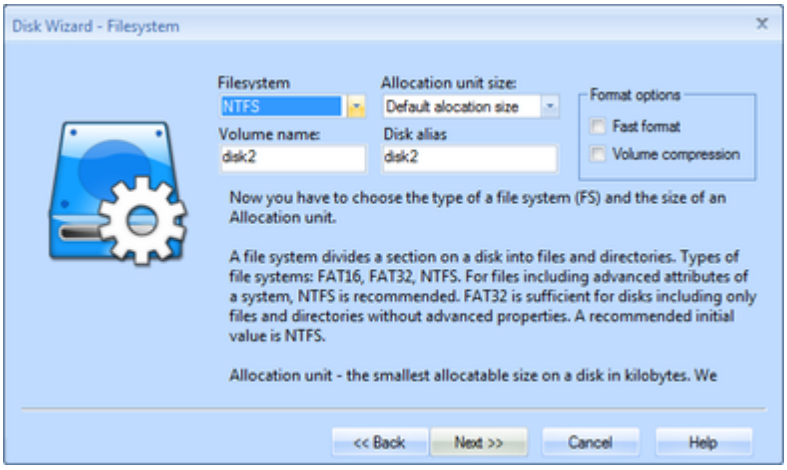
In the first step the guide welcomes you and gives you a brief information about a physical disk itself and about its creation. Click on ***Next***.

By clicking on *Browse* pick up the file that will represent your new virtual disk and choose its size. This file will then take a corresponding amount of space on the host computer. Next you can enter a disk label. After that click on *Next*.

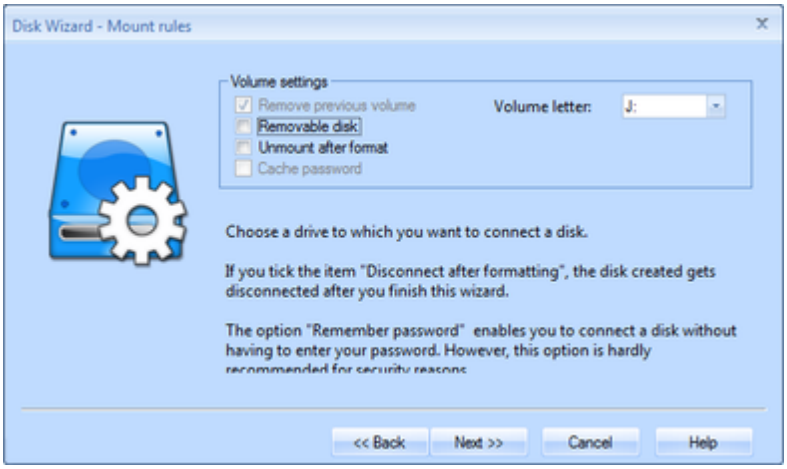


The size and location have been chosen already. Now you have to select a file system and an allocation unit. Manual selection of an allocation unit size is recommended only for experienced users. Generally, however, we recommend you to set the size of an allocation unit on the initial value of an allocation.

The choice of a file system is a dilemma. While the FAT32 file system is rather simple, the NTFS file system offers a lot of other options, in particular file and directory permissions as well as a possibility of compression. With regard to the character of new Windows operating systems we recommend to use NTFS. If you are ready with this selection, click on *Next* again.



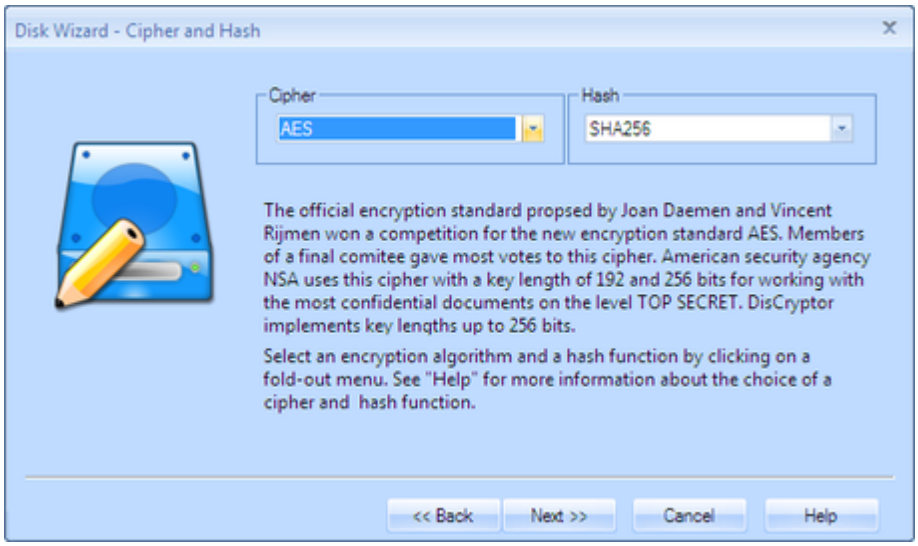
Choose a drive to which you will connect your virtual disk. After you are ready with this selection, click on *Next*.



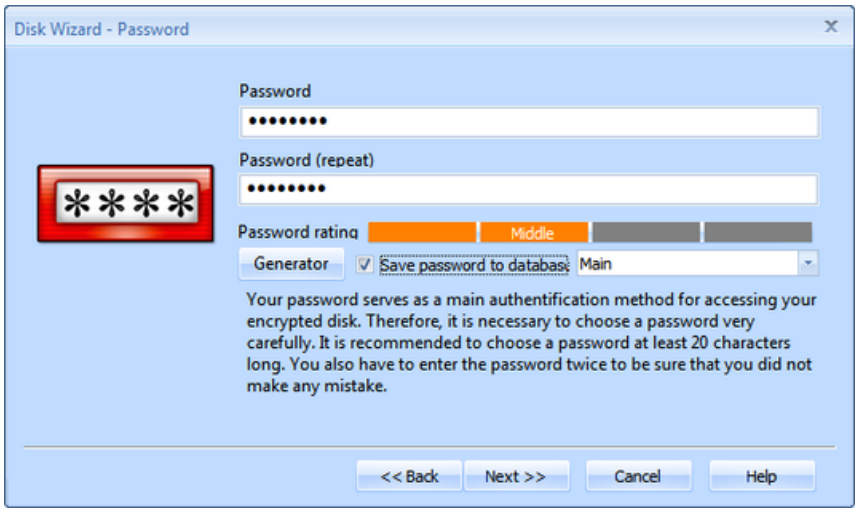
The next step is the choice of ciphers. You cannot make a mistake whichever cipher you choose. We did our best to choose optimal ciphers and sizes of their keys with emphasis on their security and speed.

In case you save very risky stuff or programs, we recommend you to use the following ciphers: Serpent, Twofish, Rijndael(AES) or Blowfish. On the contrary, for less inhospitable conditions, and for frequent and bulky file transfers the RC5, RC6, or Twofish are recommended. These ciphers excel not only in security but also in the speed.

Generally, we have to point out, however, that the choice of a cipher itself is a secondary matter. Above all, we recommend you to choose your access password very carefully. You can learn more about the security of ciphers in the chapter Frequently asked questions. To confirm your selection click on *Next*.



A key decision in the whole guide is the choice of a suitable password. There is a special chapter on this topic. To generate a safe password can you use the Password generator, which is integrated in the dialog. Your password can be immediately stored in any database or group in the Password manager. Before you choose a password, we recommend you to study materials given here. Generally, it is recommended to choose a password with al least twenty characters. After you enter your password and re-enter it for verification, click on Next.

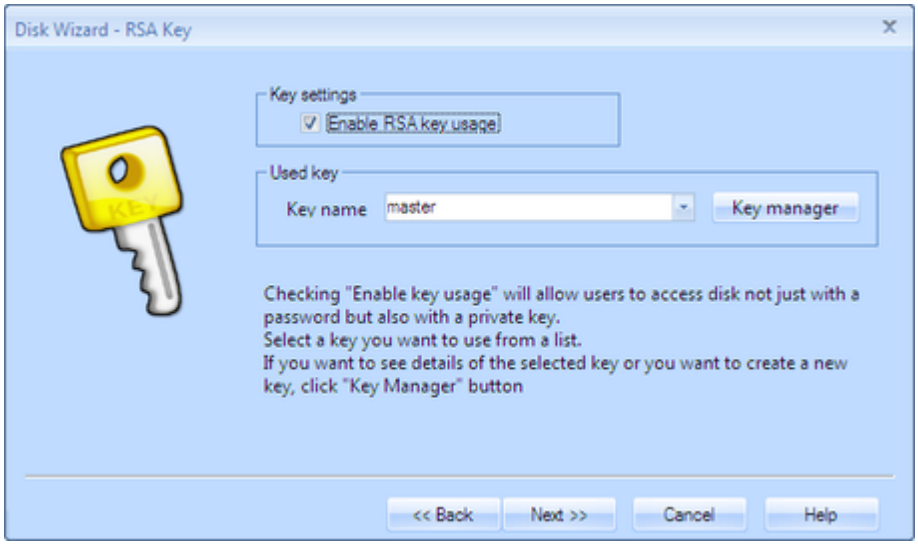


The wizard has automatically generated the disk key, which will be used for the encryption of the disk.

According to the program settings you can or must choose the using of the rescue security key for

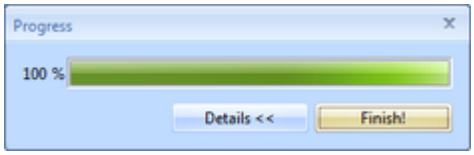
the creating disk. This security key is used for the access to the creating encrypted disk in the case of forgetting its access password. It is therefore a rescue fail-safe, but it is necessary to treat with it very carefully. If the security key comes at unwanted, the attacker can easily abuse the disk, on whose the security key is used. In the case in the Endpoint Security Tools exists no security key, the wizard will be automatically engaged. You can create or import a key in this wizard. You can allow using of the security key by ticking the Allow using of the security key and choosing the key from the highlighted menu. When the choosing is finished, click on the Next button.

You can learn more about the security key problems in the Security keys chapter.

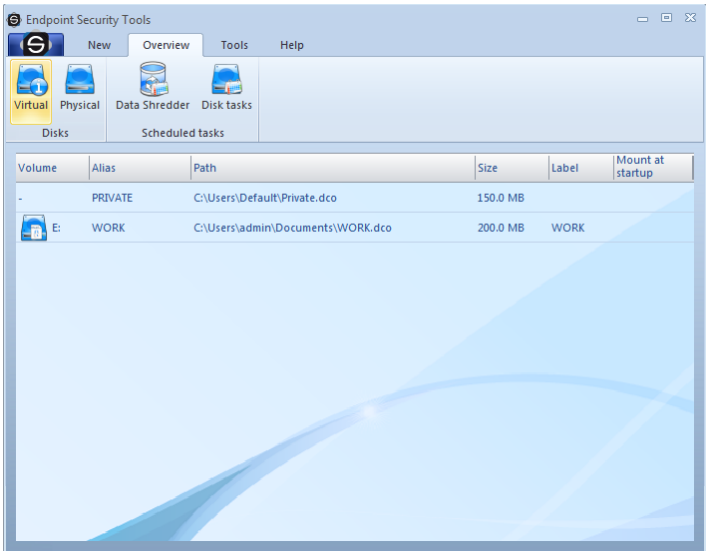


Check the entered data for the last time and click on the *Finish* button.

It is also necessary to format a disk before you use it. The guide is just doing it for you.

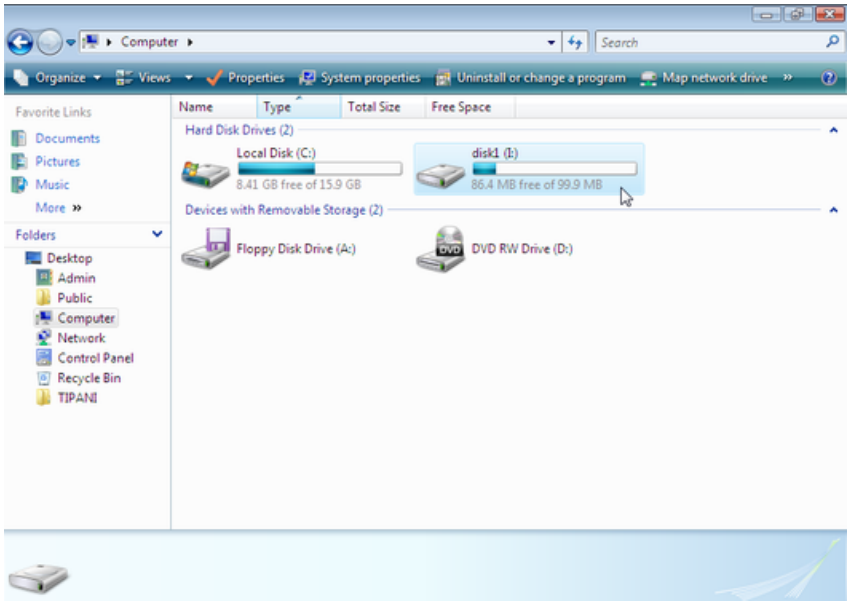


Congratulations! Your new virtual disk has just been successfully created. This disk will show up in the system as a drive you selected in the guide, in our case drive E:



From now on you can use this disk as any other disk. If you click on "My computer" in your Win-

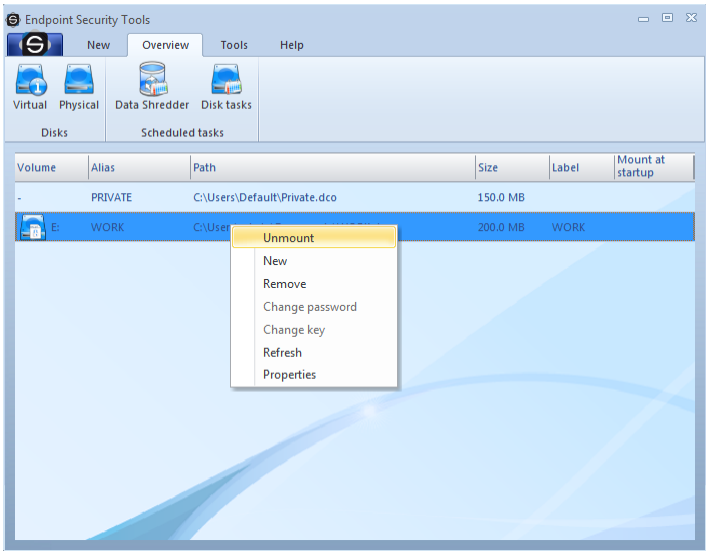
dows system, your encrypted disk will be displayed together with other disks.



2.3.4.3 Overwriting an existing disk

If you want to replace an existing encrypted disk by a new encrypted disk, you have to do the procedure the same way like when you create a new disk. However, a guide to removing a current disk will be launched in this case at first. You can overwrite any type of a disk (either physical or virtual).

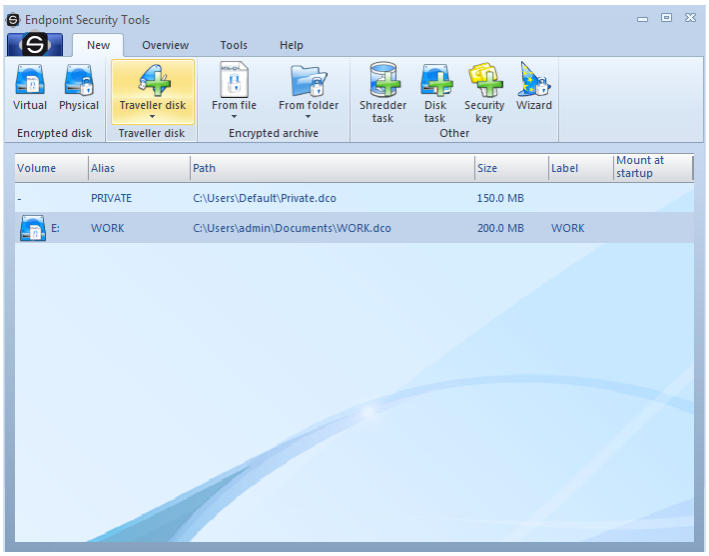
Click on the corresponding encrypted disk on the desktop that you intend to overwrite a choose *New* in the subnavigation.



Immediately after clicking you are welcome by a new guide - it is either a guide to a disk encryption or a guide to adding a virtual disk. After you go through this guide a new disk is created.

2.3.4.4 Traveller disk

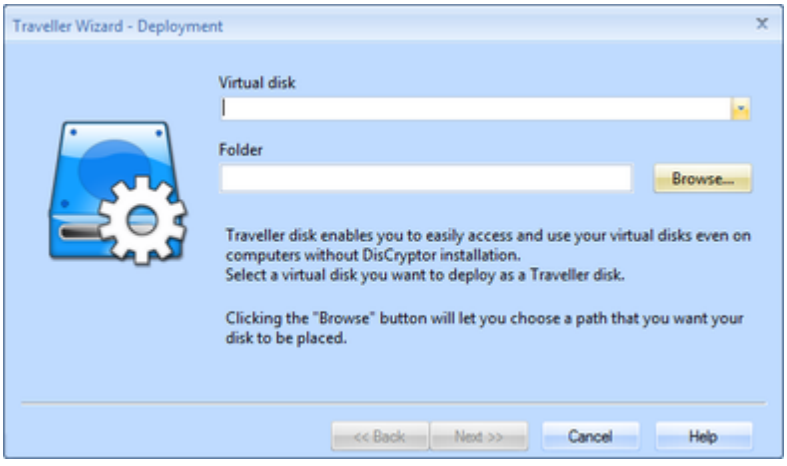
One of the main benefits of Endpoint Security Tools is the feature Traveller Disk.



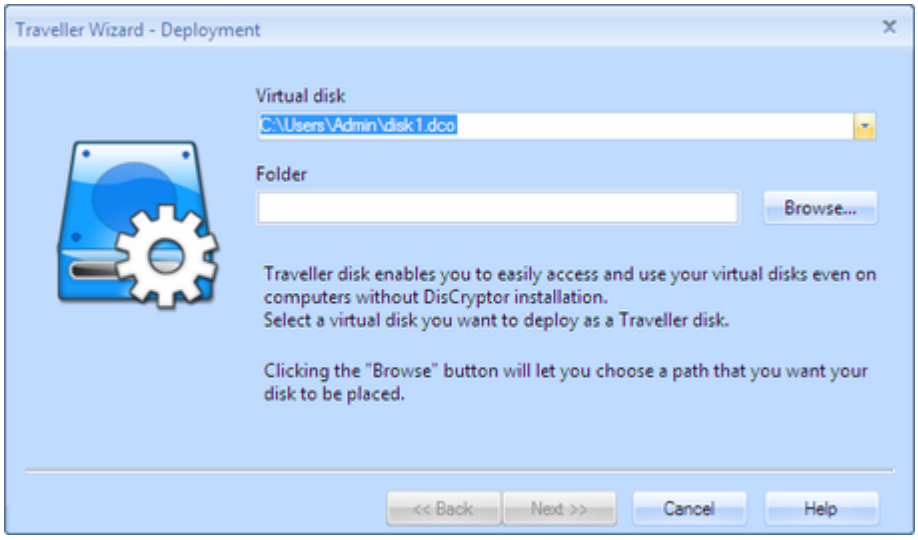
Traveller disk allows you to simply access virtual disk even on computers, which do not have the Endpoint Security Tools installed. Travel disk has equal security level like another types of disks encrypted with Endpoint Security Tools. It means - if you lost your traveller disk, the data will be absolutely unreadable for thieves.

To create a new travel disk select the tab New and then select the option Travel disk. If you want to use an existing virtual disk to export to a travel disk choose desired disk from desktop and select the option *From virtual disk...*. Otherwise just choose *New disk...*. The wizard is very similar to Creating a new virtual disk - you can follow the link.

Next description is for option *From virtual disk...*.



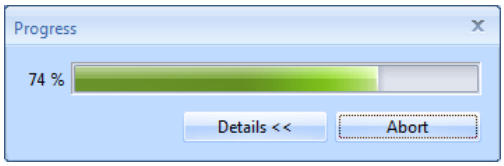
Endpoint Security Tools welcomes you with Traveller disk wizard. If you correctly selected the disk from desktop it will automatically find its path. You can still change this by clicking on the arrow on the right of the first line - there will be list of existing disks.



In the next step choose the path where your future traveller disk will take a place. If you are going to place it on CD or DVD just place it to some temporary folder and then burn it with your favorite burning software on the disk. In case of using flash disk, just choose a place on that disk.

Now click *Finish*.

And that is all. There will show up progress dialog and the rest is on Endpoint Security Tools. At the end just click *Ok*.

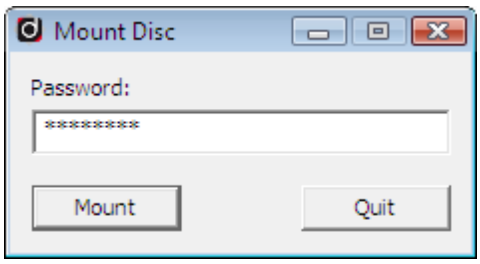


Congratulations. Your new secured traveller disk has been created.

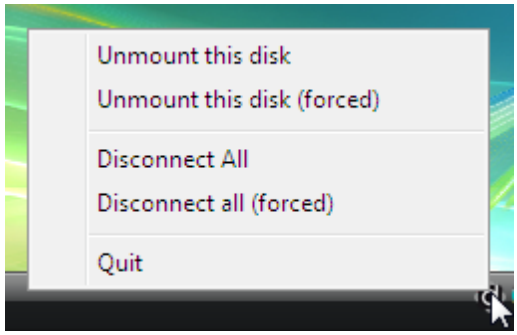
How to access the traveller disk?

Due to the automatic start of inserted disk with this option turned on in Windows (autorun), you can choose *Connect encrypted disk* and Endpoint Security Tools automatically asks you to enter password and connects the disk.

Enter now your password, which you have entered in the Travel disk wizard and confirm by clicking *Ok*.



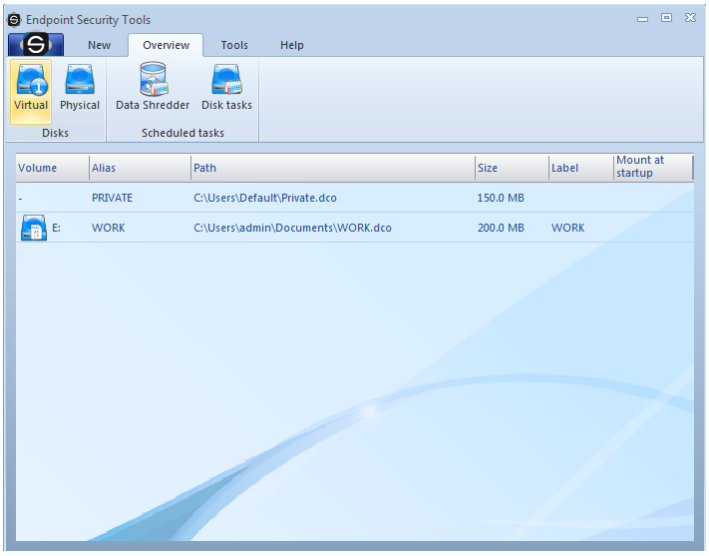
If you wish to disconnect the disk, just right-click on the tray icon , choose your travel disk to *Unmount this disk*.



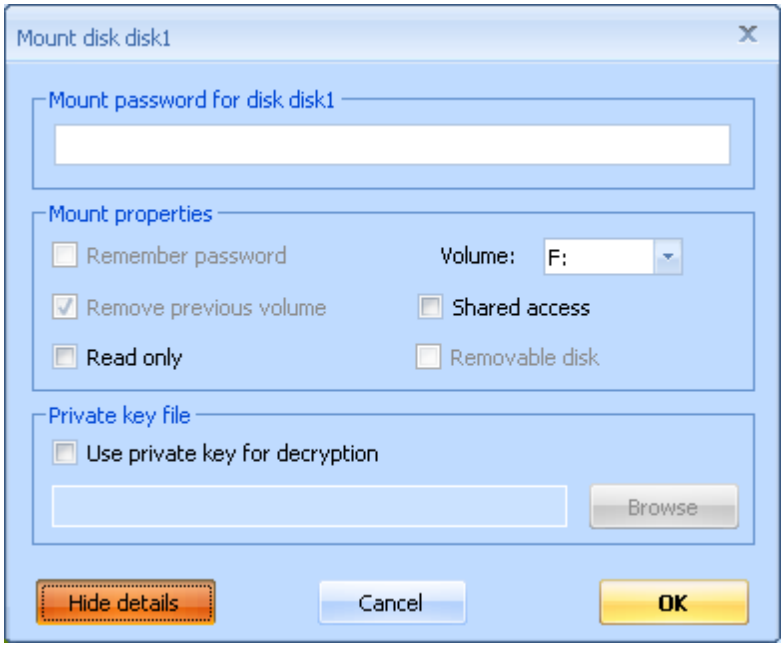
2.3.5 Disks administration

2.3.5.1 How to connect a disk?

The easiest way how to connect a disk is to choose an overview of all disks by clicking on the navigation button *Overview*. Then choose a disk you want to connect - right-click on the desired disk on the desktop and select "Mount".



To access your disk enter your password and confirm by Enter. You can also do some additional settings in the window of a disk connection.



Connecting options:

1. **Remember password** - If you want to use that option, you have to allow it first in Settings. From security reasons we do not recommend using this option! Password is remembered through all the computer activity until shutdown. If you wish to delete the remembered password just choose the tab Tools -> Delete remembered passwords.
2. **Remove previous volume** - (only for physical disks) Endpoint Security Tools removes the original drive while the disk is connected.
3. **Read only** - By turning on this option it will be not possible to write on the disk.
4. **Shared access** - shares access to disk
5. **Removable disk** - (only for physical disks) Choose in the case that the device you are connecting is containing removable disks like card reader, ZIP Drive, etc.
6. **Use private key for decryption** - if you enable this option you will be able to connect a disk by your private key.

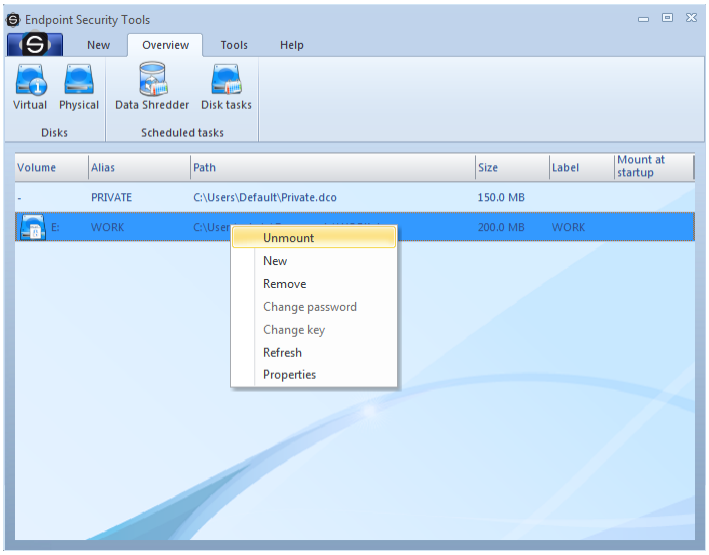
If you want to connect a virtual disk that is not known in the list of virtual disks, click on the view of virtual disks in the navigation, and then on "Search" in the subnavigation. Choose a path where your file with a virtual disk is located and confirm by clicking on "Open". After the disk is found proceed in connection as described in the second paragraph of this section.

2.3.5.2 How to disconnect a disk?

There are two ways how to disconnect an encrypted disk.

1. **Forced** (hard) - disconnects all disks even if they are being used. Therefore, we recommend you to use this way of disconnection only in case of security emergency - when your data are in danger (by default using WIN-Ctrl-Q keyboard combination). However, this function has to be enabled in settings.
2. **Unforced** - a standard way of disconnection. A disconnection cannot be carried out in this way if a disk is being used. If you want to disconnect a disk and the disconnection does not work, terminate all applications that utilize a disk and try to disconnect it again. You can perform the disconnection of all disks by a keyboard combination WIN-Ctrl-U.

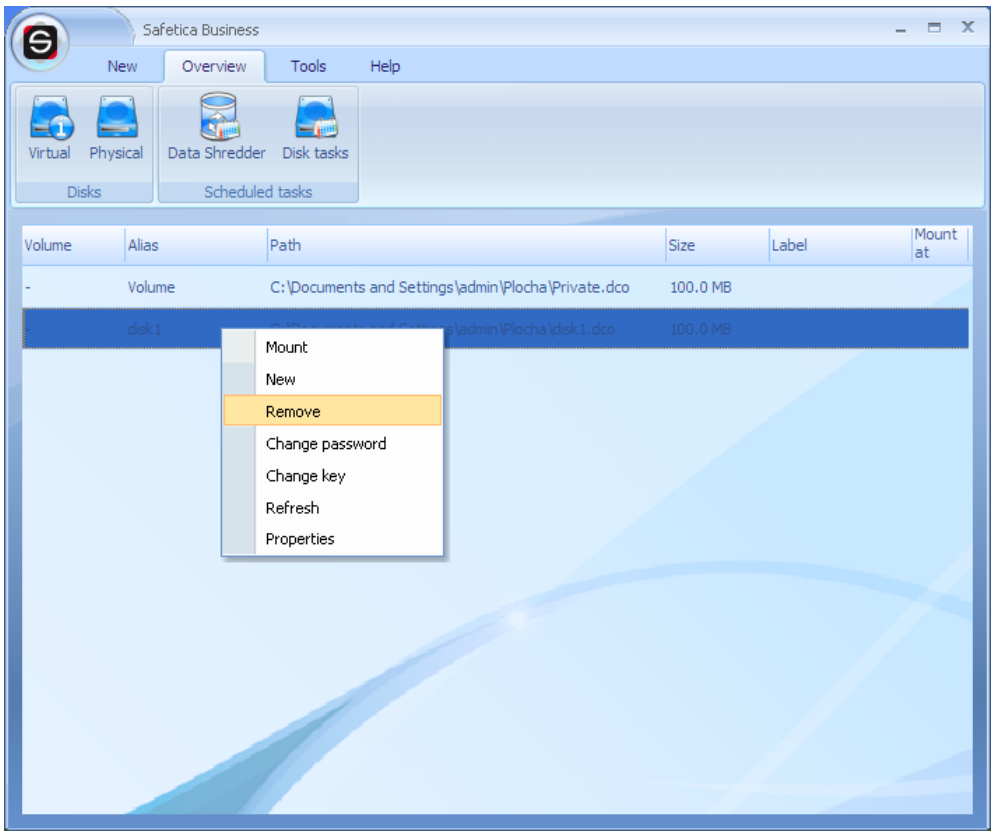
You can carry out a disconnection of particular disks by their selection on the desktop and by right-clicking on the particular disk and by selecting "*Unmount*".



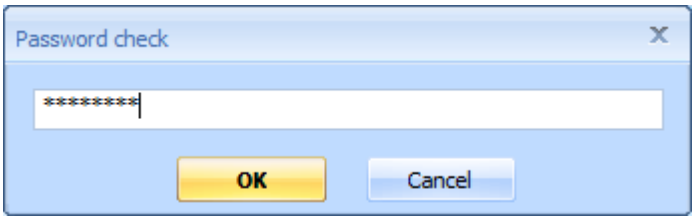
If you are right now working in Windows and you do not want to open the main window of Endpoint Security Tools, just click on the icon in tray and choose Disconnect and the disk you want to be disconnected.

2.3.5.3 How to remove a disk?

If you want to remove a disk, select the disk to be removed on the desktop and right-clicking on the particular disk and by selecting "*Remove*". If you really want to remove the disk, click on *Yes*.



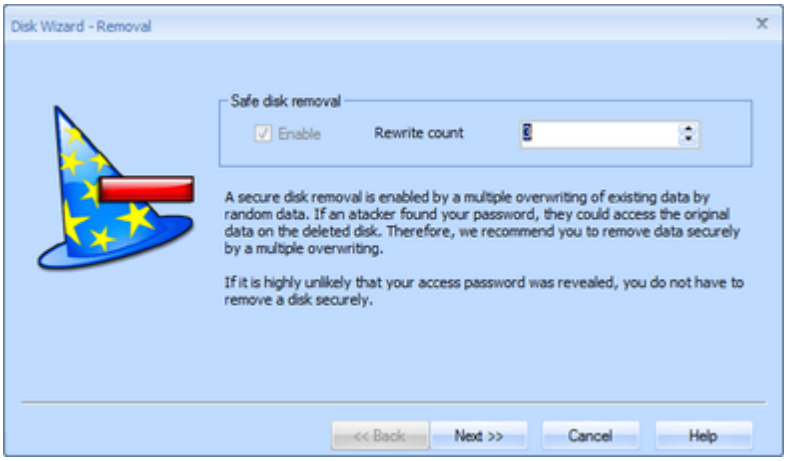
Before the removal itself, you have to enter your access password.



After you enter the password, you have to choose the type of removal.

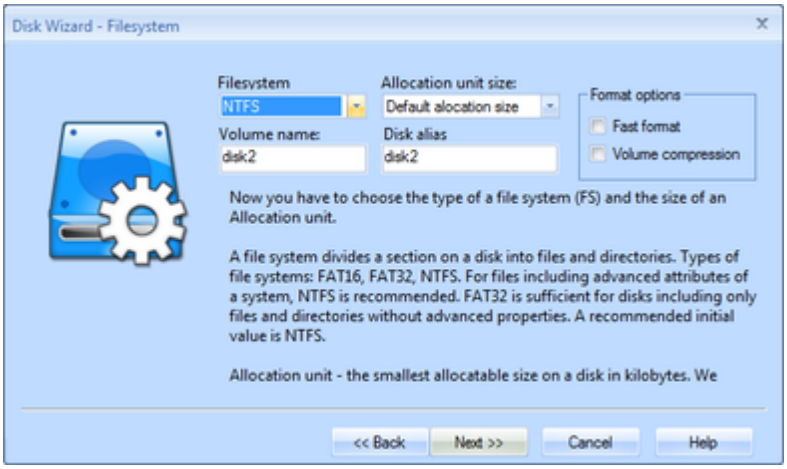
There are two types of disk removals.

1. **Deleting** - Deleting is the most common way of a disk removal. In case of a virtual disk it is just a deletion of a file with a virtual disk that is carried out. In case of a physical disk the disk is only formatted.
2. **Secure removal** - a markedly more secure way of removal. In case you need to remove your data from the disk on suspicion of a password leak, select *Enable*. A disk is overwritten several times by random data. Users themselves set the number of overwritings in Program settings. Five overwritings are sufficient for the most common needs. A very secure way of removal is the choice of *at least 15 overwritings*. The probability of reading original data is negligible, indeed, with such a high number. Thirty overwritings are recommended for military purposes. The process of a secure removal may take a long time depending on the number of overwritings.



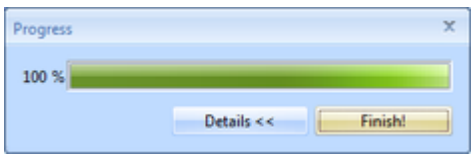
Choose the way of removal and proceed by clicking on *Next*. Confirm the removal.

In case you remove a virtual disk, the removal of the disk is carried out already in this step. At the end just terminate the guide by clicking on *Close*. If you remove a physical disk, you also have to format the disk so that it can be prepared for its next usage. Select a drive under which you want to use the disk subsequently and click on *Next*.



Select a file system you want to use on the disk and you can optionally enter a stream label. Then click on *Next*.

The process of disk formatting:



This procedure can take a long time depending on the number of overwritings and depending on the speed of the disk used. After the disk formatting the disk is prepared for a common usage under the drive chosen before.

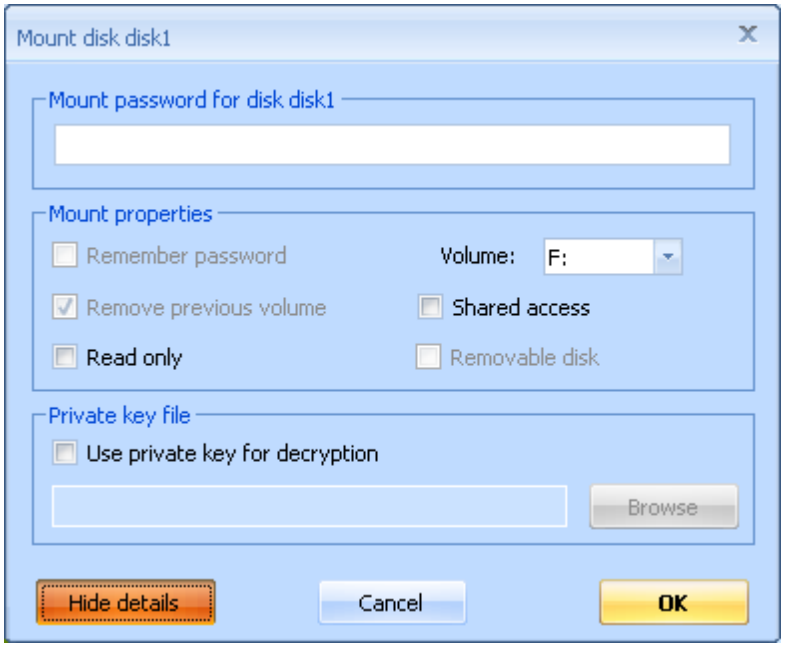
2.3.5.4 Forgotten password?

The private security key is used for unlocking the disk. For a successful unlocking the disk is needed. If the disk hasn't been created by the security key, the disk isn't in no manner possible to unlock in the case of forgetting the password. The picture shows you the system of the unlocking.

Choose the path to the private security key file, which has been used for creating the unlocking

disk.

You can connect the disk similarly like in the Connect disk dialogue. But you do not enter the password, but the path to the private security key. In the connection dialogue, which appears soon, click on the *Show details*, then enable Use private key for decryption, click on the *Browse* button, choose the private key file and confirm the choice by clicking on the Open button. You can start up the opening by clicking on the *OK* button.

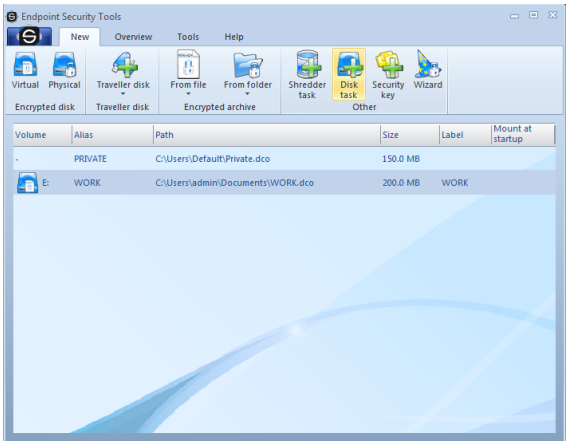


The disk is now connected and if you have forgotten the password and wish to change it, click on the desktop by the right mouse button on the appropriate disk and in the menu choose *Change password*. In the dialogue enter the path of the private security key file, two times enter your new password and confirm by clicking on the *Change* button.

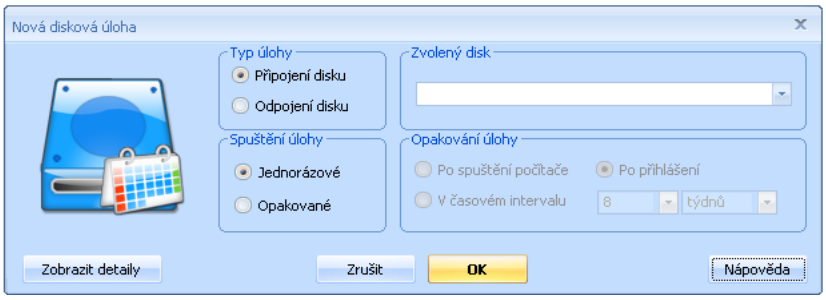
2.3.5.5 How to create disk task?

Disk task allows you to connect or disconnect the selected virtual or physical disk in a given time.

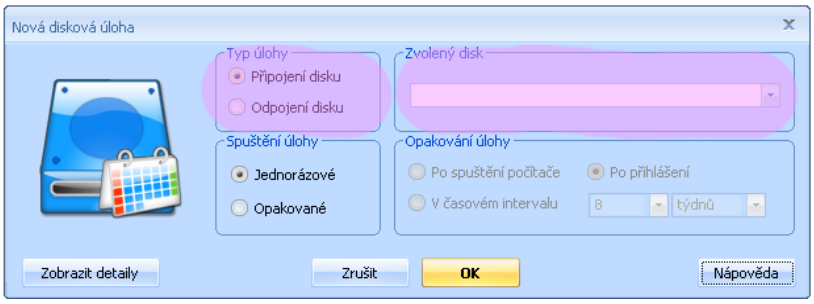
You can create a new disk task by clicking the *Disk task* icon in the *New* tab.



The following transparent dialogue will appear.

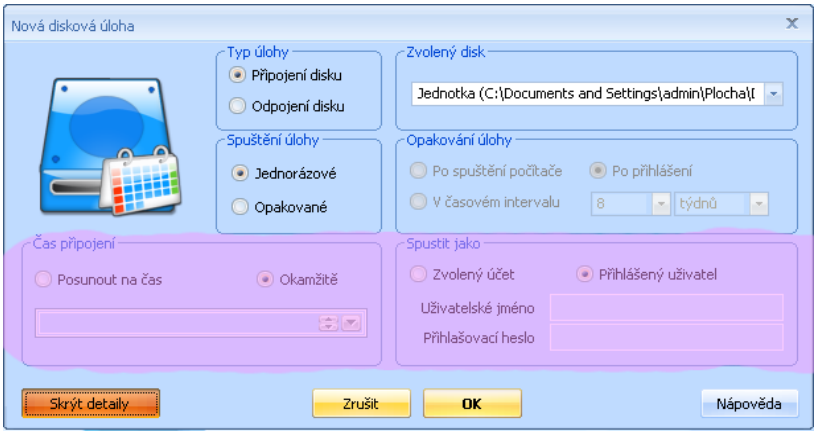


In the first step, choose the drive from. Next choose if you intend to connect or disconnect the drive. Additionally, you can choose whether to join the disc once or repeatedly. If you choose repeatedly, you can specify when (when you start your computer, after logging), and in what interval.

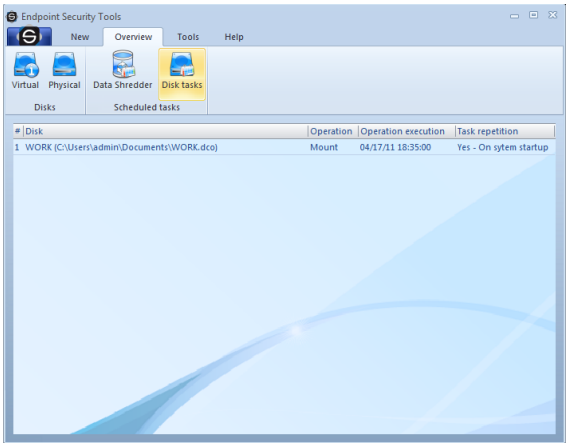


Disk task can be also set in detail. When you click *Show Details* button in the lower left corner, the dialog with detailed disk tasks setting will appear. You can set the exact date and time of connection, or under what user account will have access to.

You can hide detailed setting by clicking *Hide Details* button. If you have done the disk task setting, click ***OK*** to add it to the Windows Task Manager.



You can view created disk tasks by clicking the *Overview* tab and *Disk tasks* icon.

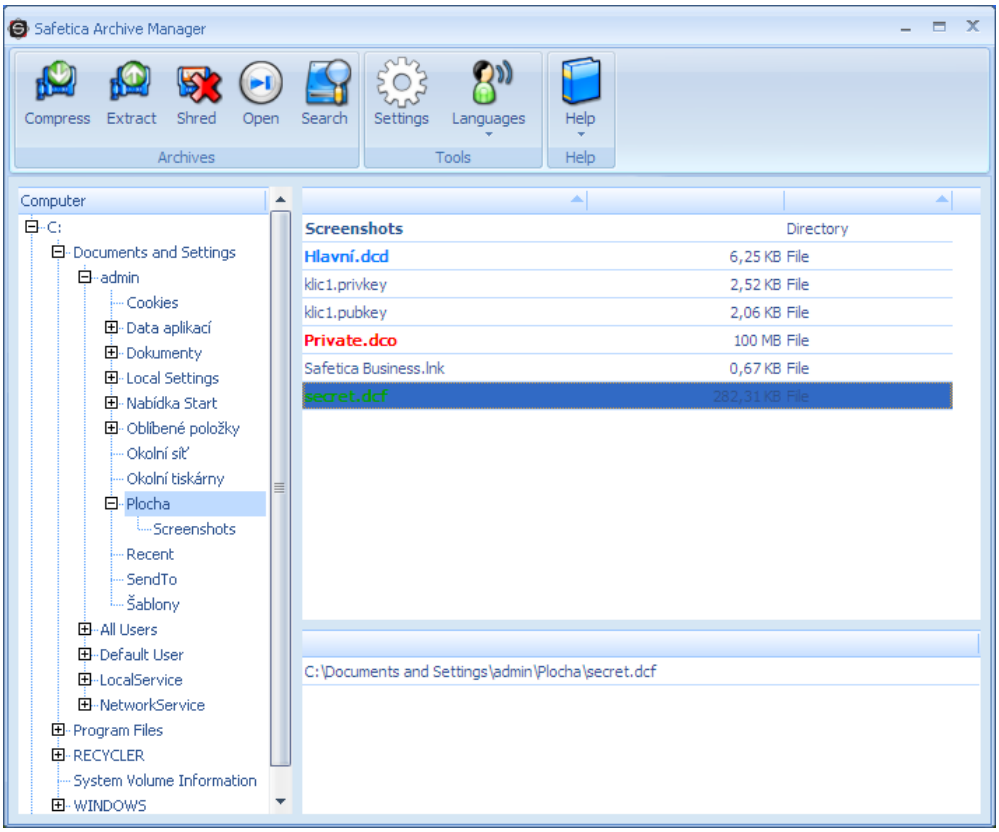


2.3.6 Archives

2.3.6.1 Overview

The Safetica Archive Manager is part of the Endpoint Security Tools. It includes file and folder encryptions in DCF archives (note: formerly encryption on file level, context offer - Encrypt..., Encrypt and Send...), which were separate in the previous editions.

In addition to file and folder encryption in own DCF format this component serves for complete work with archives and data compression. Beside standard formats compression methods the program enables to simultaneously encrypt and compress files or folders in the self-extracting EXE archive.



The Safetica Archive Manager is launched separately from the tab *Tools -> Archives*. Main window contains likewise the Windows Explorer two parts - directory structure tree on the left and currently opened folder or disk on the right (it also shows the content of archives). In the bottom window only archives from the given folder are displayed for better overview. All relevant items are highlighted at the same time.

There is a function with following options in the upper part of the window.

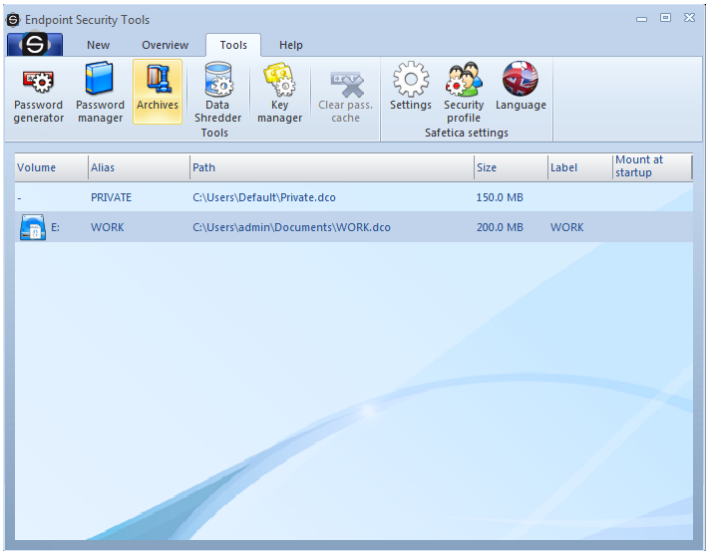
- *Compress* – selected files or folders will be packed in the required format.

- *Extract* – extracts selected archives to required path.
- *Shred* – by means of Data Shredder it deletes selected items from the disk.
- *Open* – opens or launches selected items.
- *Search* – opens searching dialogue.
- *Settings* – opens Setting dialogue.

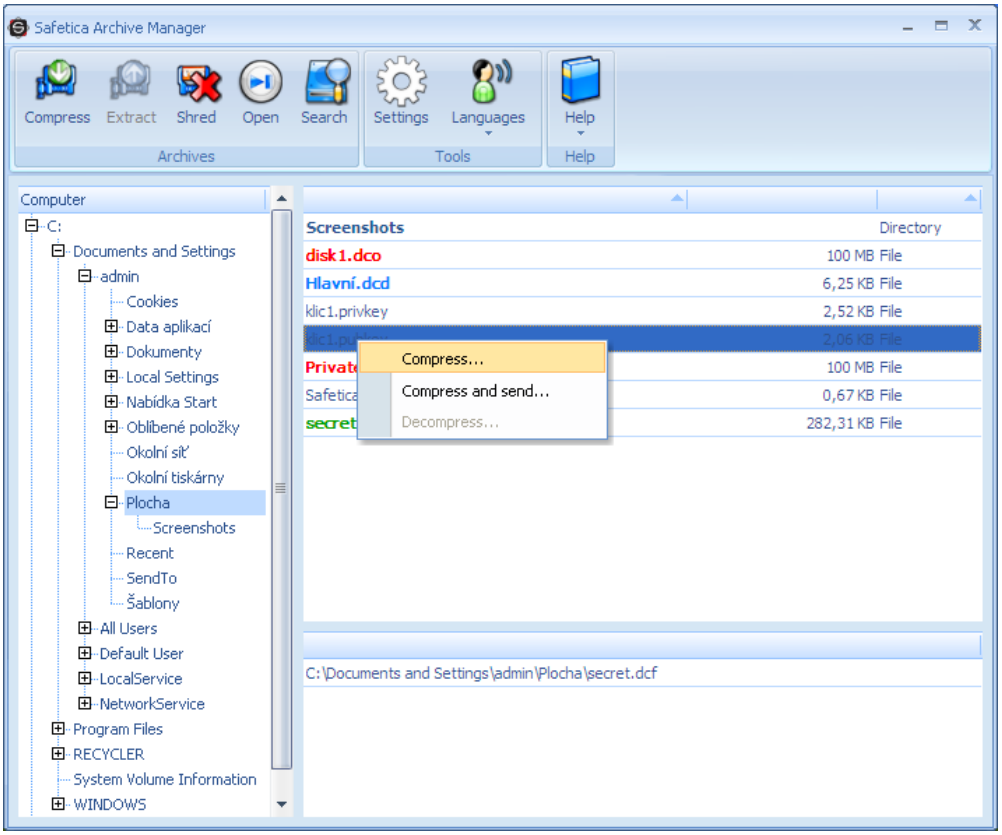
Note: Safetica archives DCE and DCF, which were created in Safetica 5.2.3 and later versions, can not be expanded in the lower versions of Safetica. The archives that were created in Safetica 5.2.2 can be expanded in newer versions of Safetica without limitations.

2.3.6.2 Compression files and folders

For security or compression of a file and folder open the Safetica Archive Manager in the Tools tab as illustrated in the picture. The compression also includes the encryption of selected items if the DCF format is used.



Further select the required file or folder and then select from the function bar the option Compress or click with the right button and from context menu select Compress. If you wish to send the encrypted files safely by e-mail click on the chapter bellow.

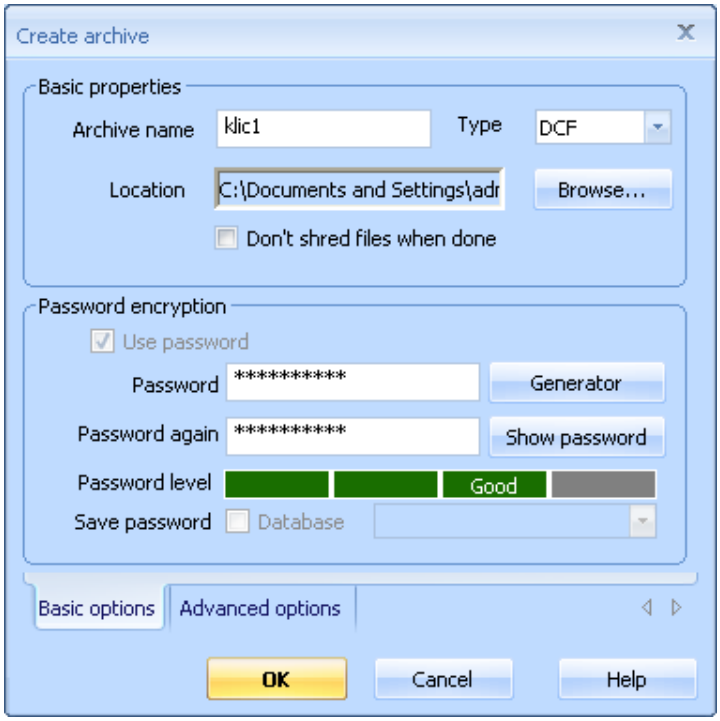


If you prefer the Windows Explorer just click with the right button on the file or folder and select the particular option.

The dialogue with request for entering the access password appears immediately. Select the format you want to use for compression, name of output archive and location. If you wish the original files to be removed tick the option Shred files after archiving.

Warning: Shredding is a time-consuming operation and subject to selected data size it may take even several hours (shredding of 4 GB data may take more than ten hours). It is not recommended to encrypt big folders or system folders (like Documents and Settings, Users etc.). Your key decision comes – selection of correct password. For secure password generating you can use the Password generator integrated directly within the dialogue. The given password can be immediately added to any database or group in the Password manager. This important questions are described in separate chapter. The password to the given archive you can save directly to your con-

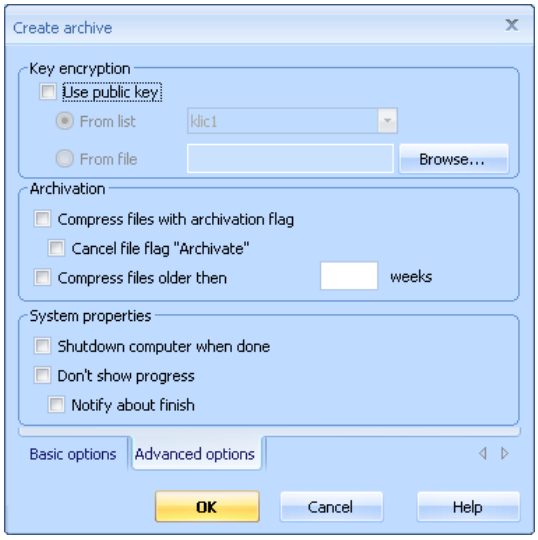
nected database. Before selecting the password we recommend to study materials about correct password selection. Enter your password once more for control and click the OK button.



Now the dialogue with indicator of compression course will be displayed and new archive will immediately appear in the same directory and as a new item of archive list. Just confirm by clicking OK. Any encrypted file by the Endpoint Security Tools is easily recognized according to .DCF extension and Safetica logo icon.

If you transfer the encrypted files to other computer, it will be necessary to decrypt them again! How to decrypt files and folders quickly is described in the following chapter.

Option to use the password is obligatory only with DCF archives (this one is only one secure with password use because it is encrypted!), with others this possibility is optional if available.

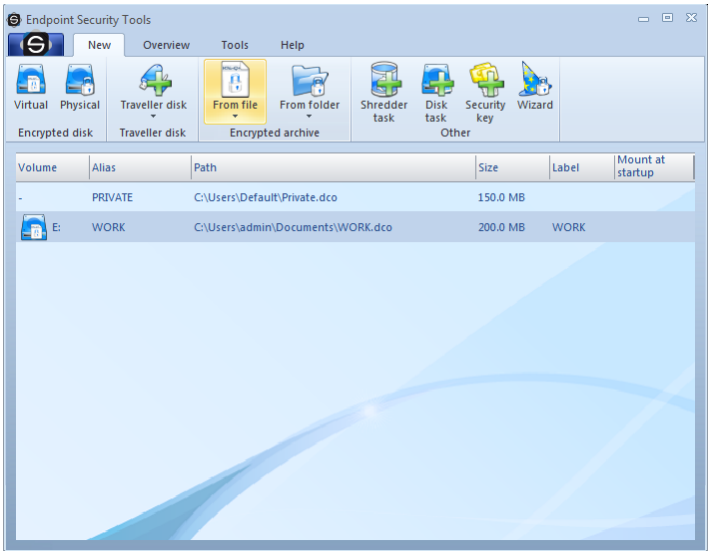


Advanced setting

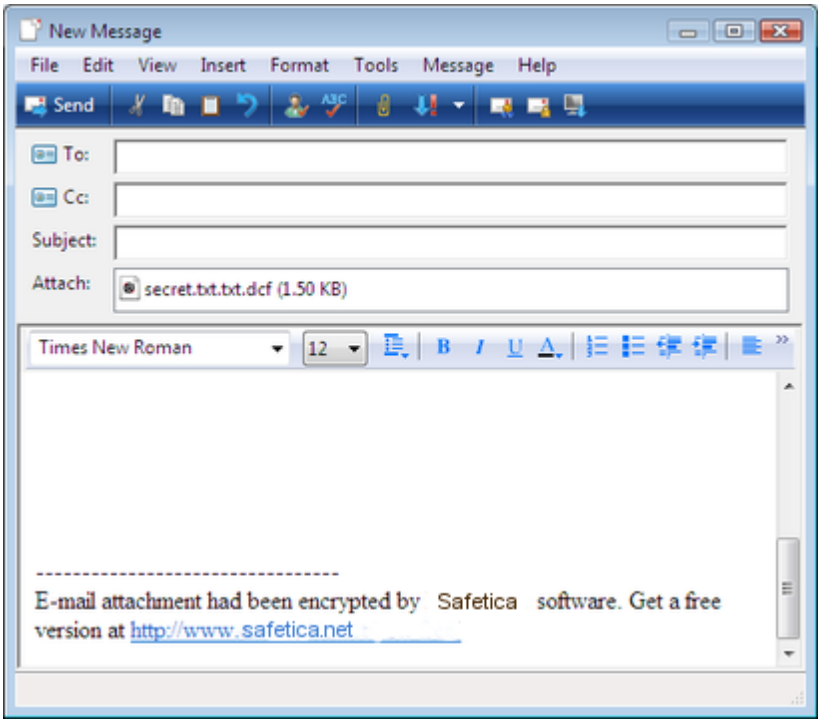
In this tab details of archive formation can be set. The use of public key for file encryption is the most important in case you would have forgotten the password.

2.3.6.3 Compression and sending in an email

Click the tab New and then either From file or From folder icons as shown in the picture. Then click the option Encrypt the file/folder and send by e-mail..., and select the required file which you want to securely send. The same dialogue as described in the previous chapter will be opened.



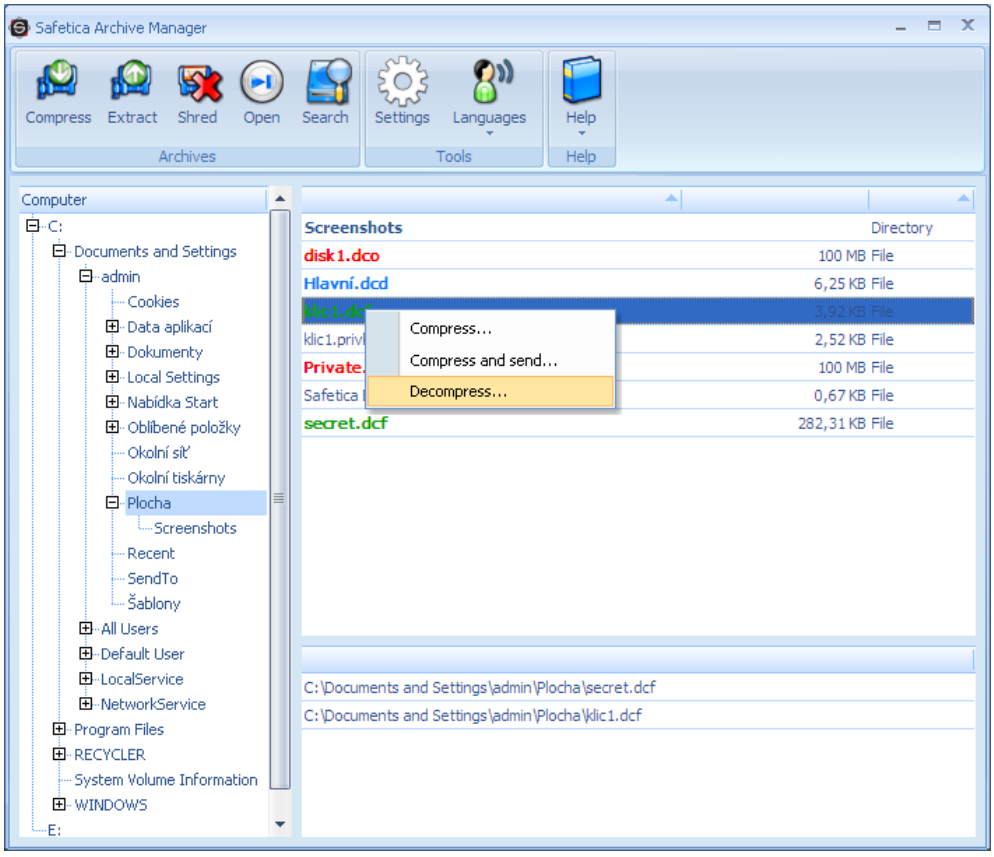
If you prefer the system Explorer just click with the right button on file or folder and select the option Compress and send. The same possibility you can also find in the context menu of the Safetica Archive Manager.



In the last step your favorite email client will be launched and the encrypted file will be automatically connected as attachment. It is enough to fill in the e-mail address of the recipient and send the e-mail. The recipient will receive automatically enclosed instructions how to encrypt the attached file easily. If you use the self-extracting EXE archive the recipient does not need to install any software. The recipient has to obtain from you the password and then he is able to decrypt the file easily. **However we do not recommend to send passwords by e-mail!**

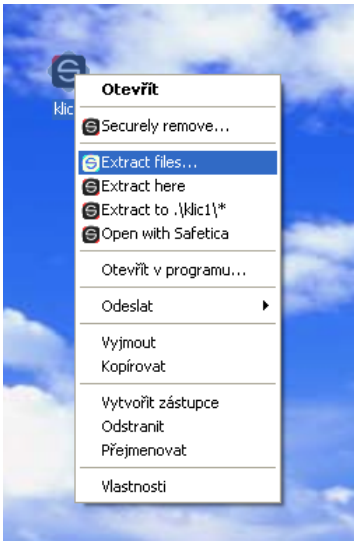
2.3.6.4 Decompression archives

The decompression of archives is very easy. In the Safetica Archive Manager select by right button the required archive and select the Extract option.

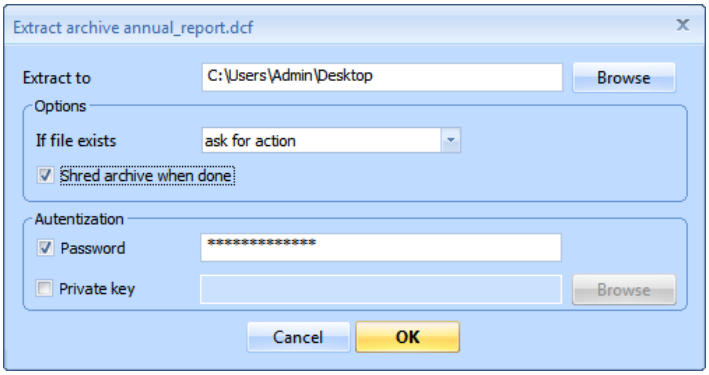


Compressed files and directories are very well recognizable thanks to Safetica icon by which all encrypted files are presented within the system.

In the Windows Explorer double click the compressed file icon or click just once with the right button and select the Extract option as illustrated in the picture bellow.

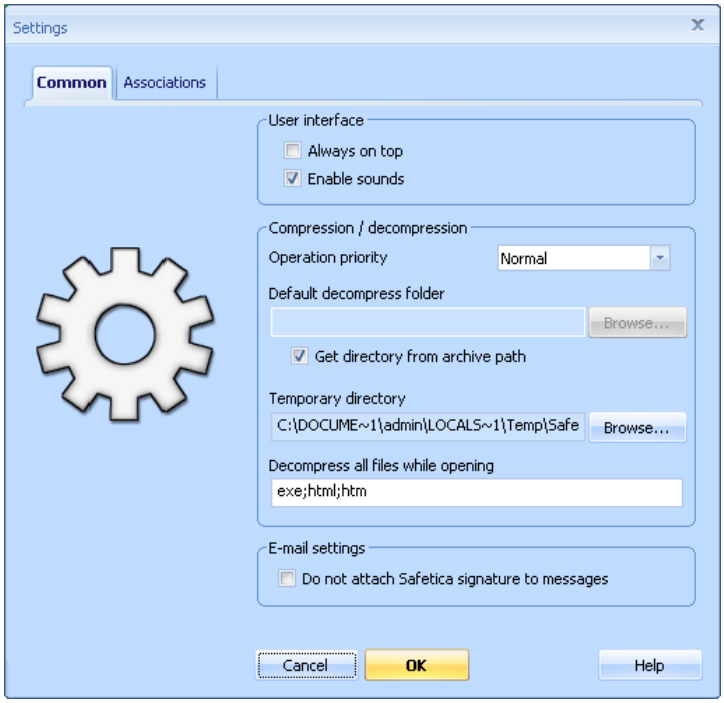


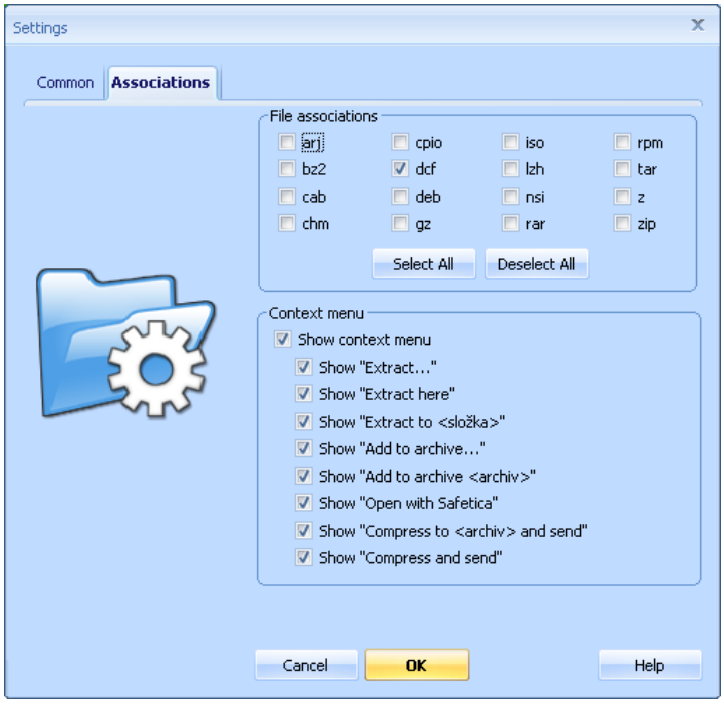
Enter the original password in for decompression or decryption if the DCF archive or some other with use of a password was used. If it is the DCF archive and the public key were used for encryption, for decryption you can use the private key.



2.3.6.5 Setting

Setting of the Safetica Archive Manager includes some useful options. Thus it enables you to tune the program behavior according to your needs.

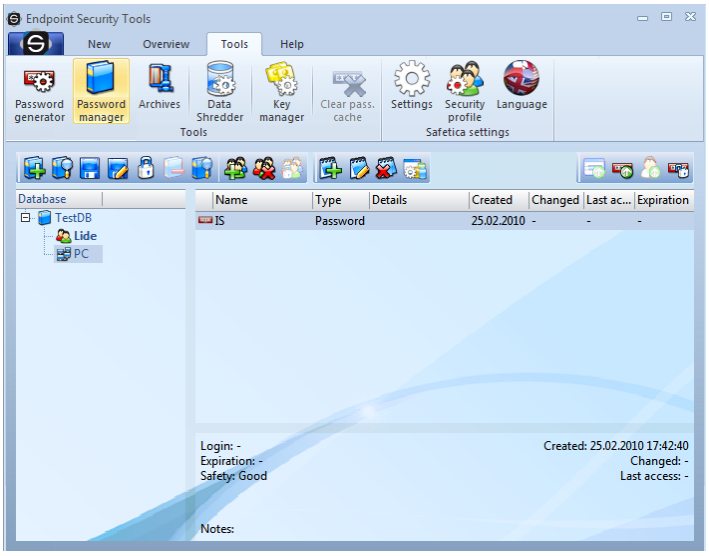




2.3.7 Password manager

2.3.7.1 Database

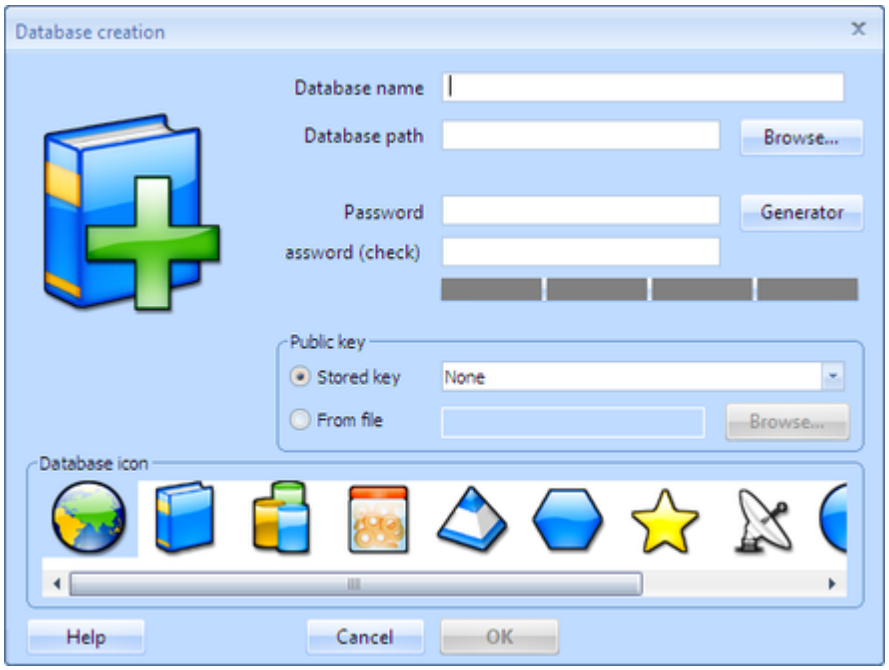
Database is a default structure to store records. They are stored and encrypted locally on your computer and their count is limitless. Working with database is similar to working with a word document. All changes must be saved and the data are in that process encrypted. Database can contain groups, subgroups and mostly the records. Password for database is mandatory unlike for the groups. Level of this password is set according to the chosen security profile and it is recommended to use the strongest password as possible. You can also use the security key.



To manage databases there are first six icons from the left on the toolbar. All of these actions can be reached also in the context menu. You can unlock or lock database with double-click in itself.

1. **New database** - opens a dialog to create a new database
2. **Import database** - imports an existing database into the list
3. **Save database** - saves all changes
4. **Save database as...** - saves database at the selected path as a new file

5. **Unlock/Lock database** - unlocks or locks the database - icon and tooltip changes dynamically
6. **Remove database** - removes the database from the list and asks if you want to remove the database also from the disk



When creating a database, it is important to fill in name, path and password. Icon and security key is optional.

2.3.7.2 Groups

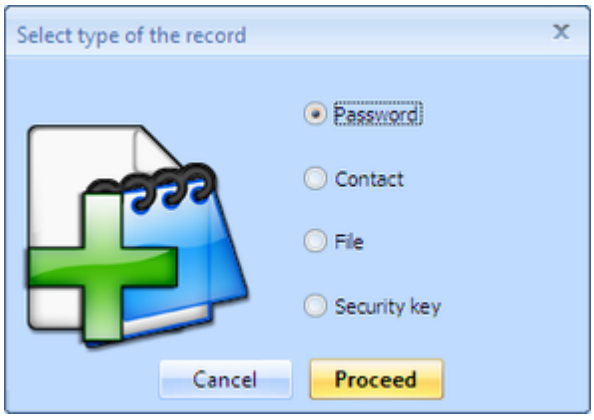
With groups you can separate records into logical structures. The structure of groups depends only on your needs and groups can have subgroups. You can set for every group a different icon, password and security key (which is by groups optional).

1. **Create group** - opens dialog for creating of a new group
2. **Remove group** - removes selected group with all its subgroups and records
3. **Unlock/Lock group** - unlocks or locks the group - icon and tooltip changes dynamically

Mandatory field is only name of the group, everything else is optional.

2.3.7.3 Creating records

Elementary item in the database is a record. Record can be placed in the root of the database or into groups or subgroups. To create a record just click on desired database or group, which you want to place it in and select the icon "Create record" from the toolbar, or use right-click and select the option from context menu. After that will appear the dialog, where you can select type of the record. Mandatory field in all records is only the name.

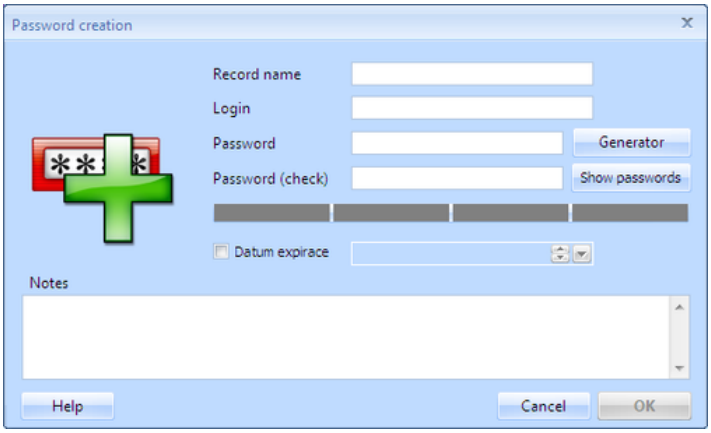


Record are divided into four types

- **Password** – this record stores user names and passwords.
- **Contact** – it allows to store all information typical for a contact record.
- **File** – stores the file directly into the database (e.g. an e-certificate).
- **Security key** – secures in database a private and a public key.

Password

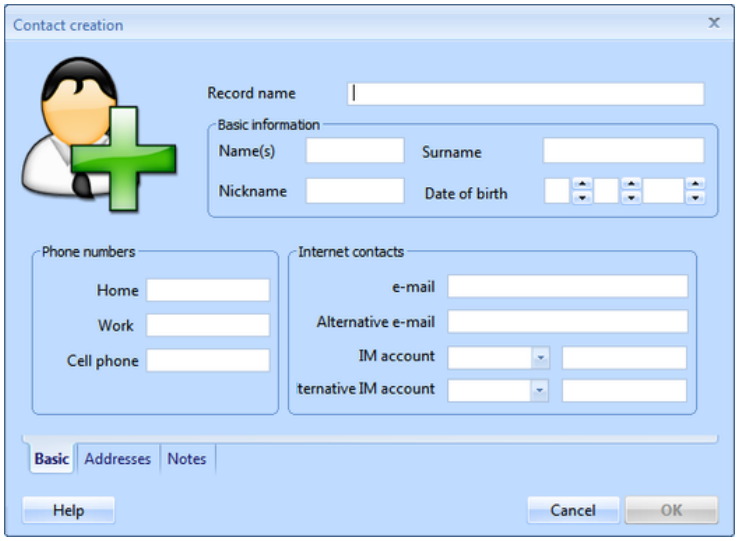
Password record represents for example authentication information such as login and password. You can write a note or set a date expiration as well. If you are right now creating a password, you can use directly the Password generator.



You can copy into clipboard the login or the password from an existing password record. Using the toolbar icon or through the context menu.

Contact

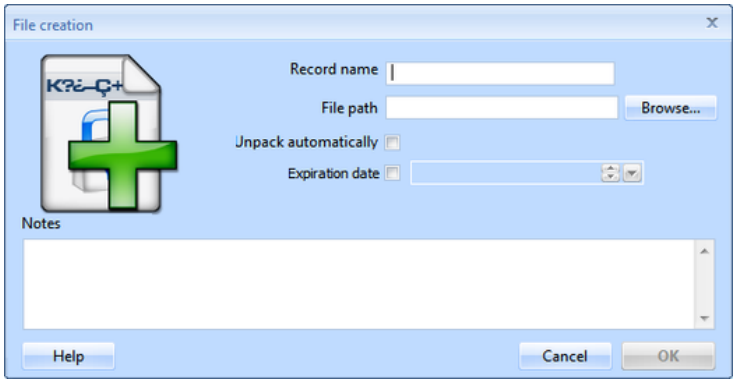
The contact record can store all contact information for a person or a company. From name, address, to IM contact or internet address. You can use with this record the Safetica as an electronic diary as well.



In the lower section of the dialog, there are tabs which switch into different views for different kinds of information.

File

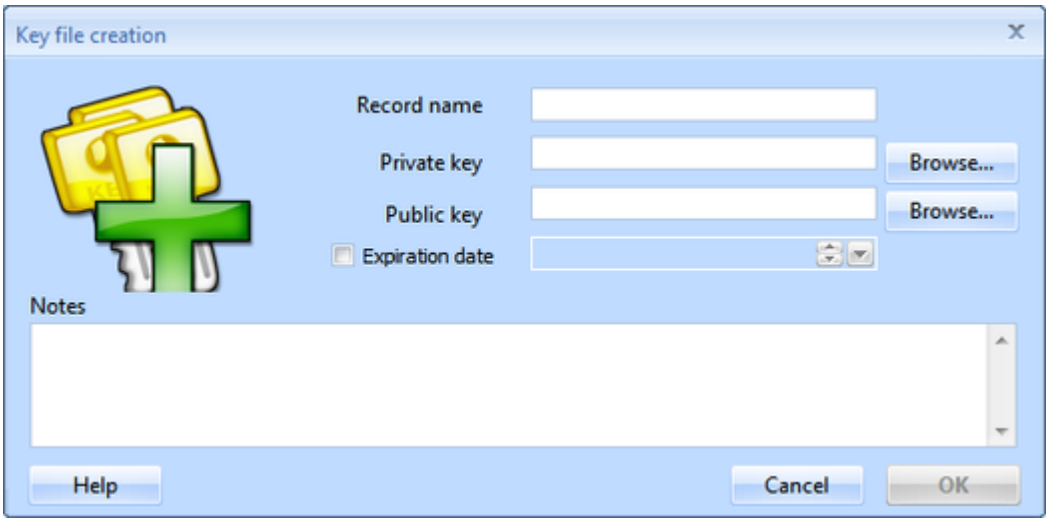
In the database can be stored files as well - it is useful for files like electronic certificates, etc. Of course you can store any kind of file. It is recommended to store smaller files.



The option Default extraction causes after every unlock of the database export of the file to the path from which it was selected, otherwise it can be exported through context menu. You can write a note or set date of expiration as well.

Security keys

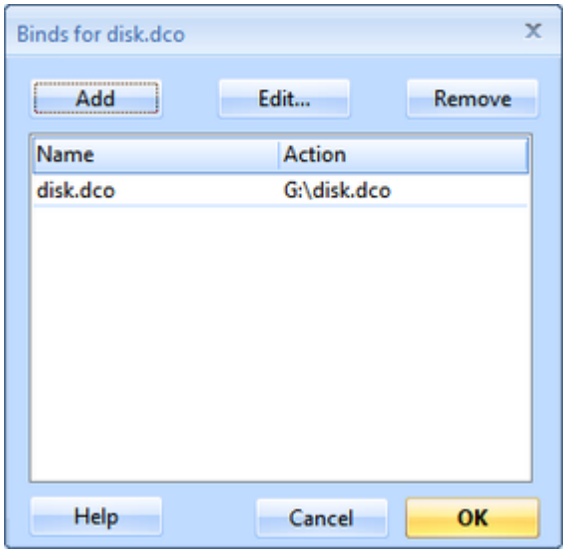
The last type of record is Security keys from Safetica.



Like in every other record the date of expiration and a text note can be set. Keys can be exported from the database through the context menu.

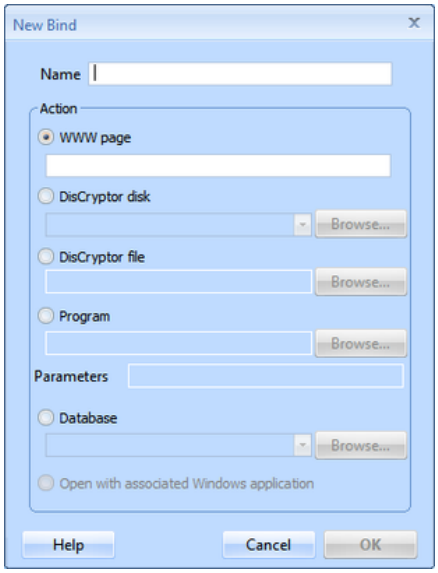
2.3.7.4 Bindings

For every record a different kind of action can be set, which appears then in the context menu. To create user defined actions select "Set actions" from the context menu. There can be limitless number of actions and they can be edited.



Actions which can be set:

- **WWW page** - opens a web page
- **Safetica disk** - from the record password or security key connects a disk
- **Safetica file** - from the record password or security key decrypts a file
- **Application** - runs an application - parameters can be set as well
- **Database** - from the record password or security key connects a database
- **Open with an associated application** - runs an application according to the settings of the system

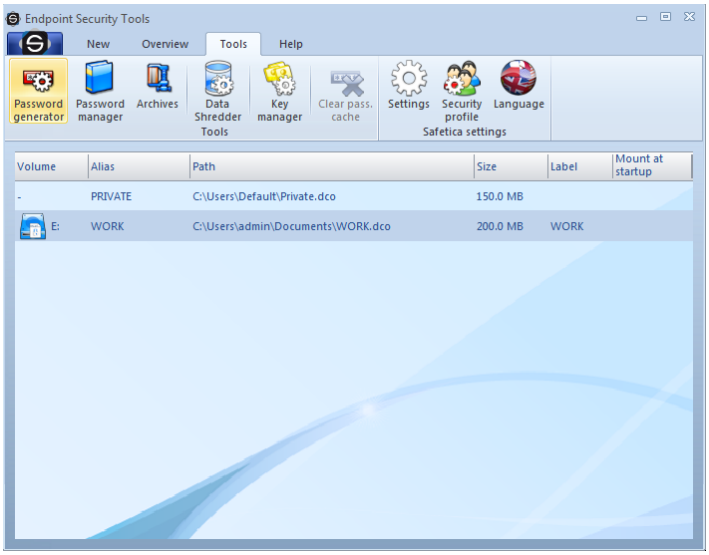


2.3.8 Password generator

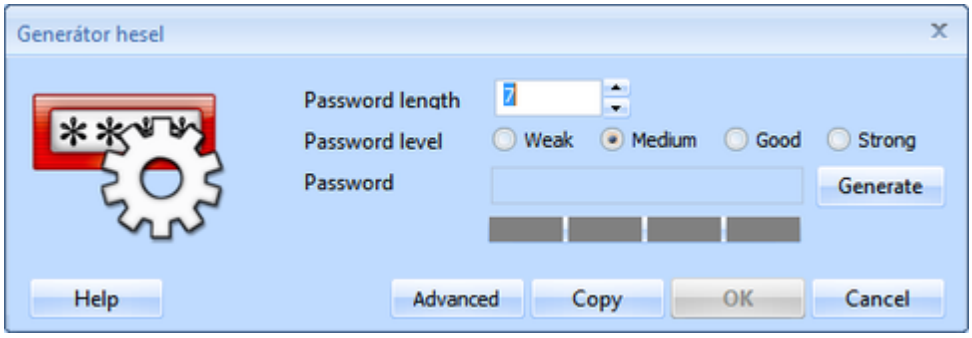
We have often to choose different passwords and not every time passwords like „alice“ are safe enough. Logical tendency is to use known words, names, birth dates or similar phrases. Unfortunately these options are the first ones the attackers try with techniques like dictionary attack or brute force attack. Requirement for a safe password are combinations of small and capital letters, numbers, special characters, minimal length, etc. When this combination is strong enough, it is impossible to break such password not even in hundred years.

It is complicated to create such password. With the help of the Password generator integrated in Endpoint Security Tools this task is matter of seconds. Simply choose the level of password you want or length, combination of characters and the rest does Endpoint Security Tools for you.

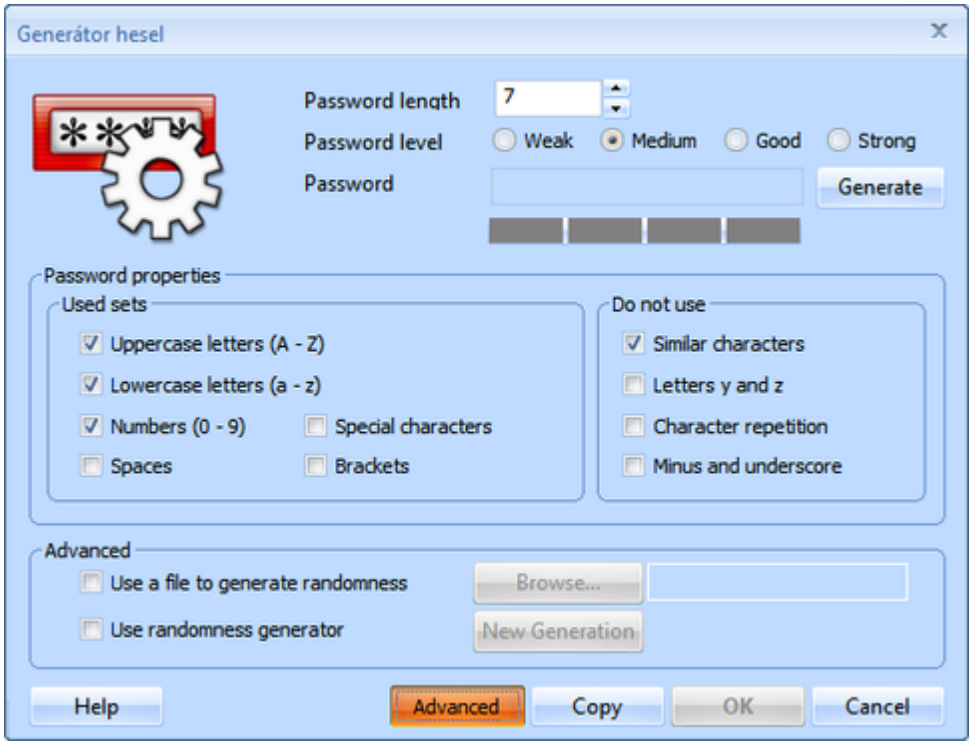
Password generator is integrated into all required sections of Endpoint Security Tools - you can directly from the dialogs for choosing a password open this generator and generate a password. And not only that, you can store immediately the password into database as well.



This tool is accessible from the tab Tools and from all passwords dialog as well.



In the basic view of the generator, you can choose simply what level of password and its length you need and after selecting the button Generate, the desired password will appear. Password can be immediately copied into clipboard and used in a web service registration for example.



The advanced view allows to set detailed options and to select what characters the password will contain or not.

To generate random passwords we use standardized randomness generators. To generate totally random sample you can use a picture file for example or use a widget, where you, by moving the cursor in a window, generate random sample, as well.

2.3.9 Choosing a password

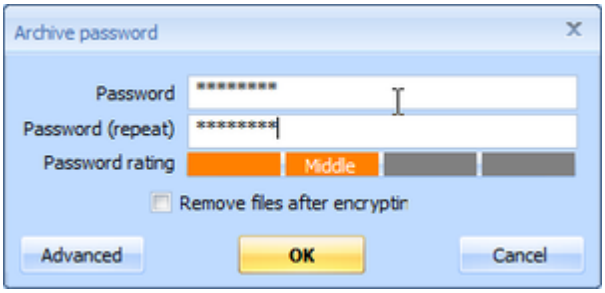
It is not the choice of an encryption algorithm that plays a key role in data security but a correct choice of an access password. Main keys are derived from the password by means of complicated algorithms. These keys are indirectly used for the encryption process itself.

If an attacker was able to solve one DES cipher within one second, they would solve one AES cipher in 149 trillion years provided that the key size is 128 bits. If the access password was "aaa" under the same conditions one could hardly speak about a real security of the data saved. An attacker would have a trivial access to your data by using an attack of dictionary type. A recommended length of a password is at least 20 characters. The password should contain small as well as big letters, numbers, and special characters (~!@#$%^&*():"<>?{}|\][;'/.,`).

A password should not contain:

- Name or surname of the user, their relatives or parts of their names
- Dates of birth of a user and their relatives or other memorable days.
- Names and relationships related to the user
- Well-known names or words, or words that exist in the Czech or English language.

You do not have to be afraid from choosing safe password - the dialog of Endpoint Security Tools will immediately analyze your password and graphically shows you level of password. If the bar is green you can be sure you entered a safe password.



How to remember a long password?

Do not get scared because of the length of the password. You can use mnemonics, for example a rhyme, to remember your password. A password can be then composed of letters at the beginnings of words in the rhyme.

Example:

Abbtsbpobichtwm.Ithftbhdntma!

"A big broken tooth should be pulled out because it could hurt the whole mouth.

I told him five times but he did not take my advice!"

How to store password?

The absolute recommendation of storing password is by remembering it. At no cost do not give anybody your password and do not write it down nowhere and do not store it in any other way! Endpoint Security Tools never stores password (unless you choose it from advanced options, but this is not recommended) neither the encryption key and if this key is stored in computer memory, it prohibits to the Operation System to store it on the hard drive (see paging). From this view the weakest part of Endpoint Security Tools is the Human Factor - so we strongly do not recommend to underestimate the choice of good password! If you will learn, how to enter safe passwords, you do not have to be afraid of loosing your data.

I forgot the password, what now?

If you are using security keys, you do not have to be worried. The procedure how to recover data is here.

2.3.10 Recommendations for increasing security

Security is not a permanent state but a long-time process...

1. **Important!** Switch off hibernation in Windows. If you switch your computer to a hibernation mode, the whole content of internal memory will be stored on a disk. After leaving the hibernation mode this content will be reloaded and the system will be at the same place as before hibernation. In case the hibernation mode was used it could happen (highly likely) that the a part of memory with the encryption key would be saved on the disk in the non-encrypted form. This risk is extremely huge and the program cannot fight back.

   You can disable Hibernate in this way

   Click on:

   Start -> Control Panel -> Power Options -> Hibernate

   Then untick: Enable hibernate mode If your computer supports other modes of hibernation it is not recommended to use them and we advise you to disable them. Otherwise, you take a risk of a key leakage in case of theft.

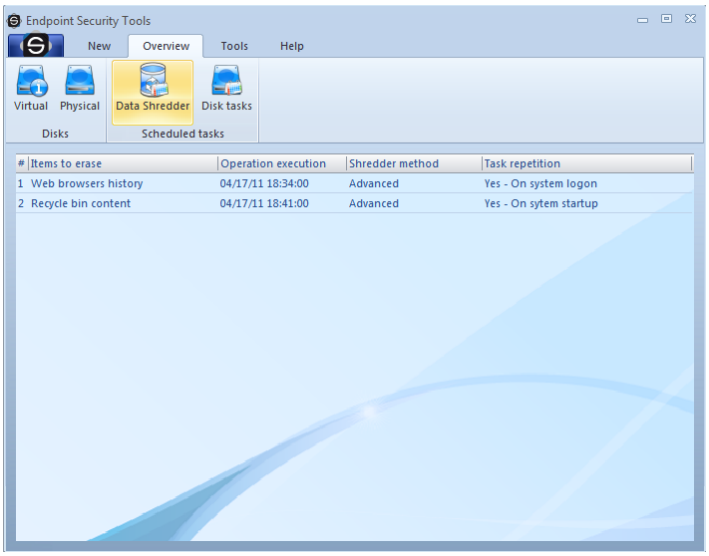
2. **Important!** Never tell your password to anybody else, do not keep your password in any form. Password is the most important thing you need to be able to access your data. We

recommend you to study the following topic about choosing a suitable password.

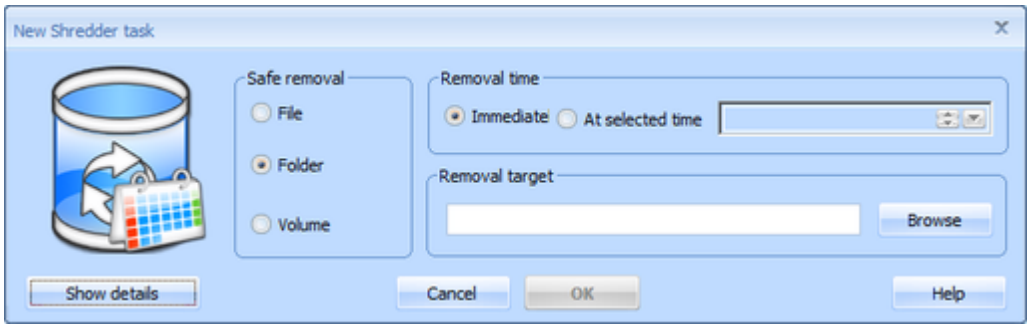
2.3.11 Data shredder

Did you know, that by deleting the files, you cannot ensure their safe removal? Even data from formatted disks can be easily recovered. Shredded data can never be renewed (not even in an IT lab).

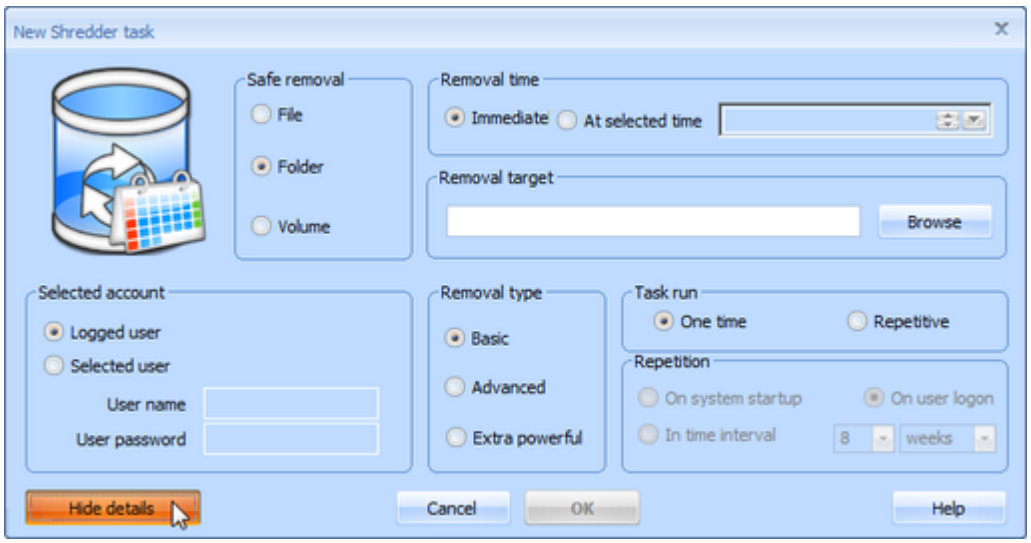
You can start the shredding by choosing from the tab *New -> Data shredder*.



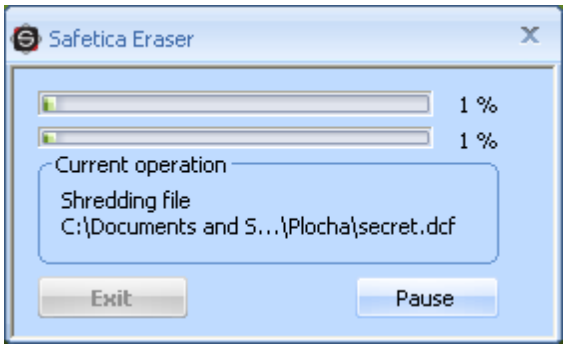
There will appear a simple dialog.



In the first step choose which data you want to shred - files or whole folders or even empty place on the drive.



At the end choose method and time of shredding and confirm it by clicking Ok. If time of the task is selected "Now" it will immediately start after selecting Ok. Otherwise at the time you selected (and it can be periodically if you wish).



For those, who prefer removing data straight from Windows Explorer or from favorite file manager, they can do it from context menu, which is reachable by right-clicking on the file/folder.

2.4 Advanced security

Security is at this time the most actual topic in IT. Today, there are practically no problems with the speed of executing the data, data saving, or in the slow access to such data or lack of storage holds. The most information problems of today and tomorrow are in securing such data

Endpoint Security Tools ensures a full protection of all your data against theft, and also against dangerous or curious colleagues. Our cutting-edge security Endpoint Security Tools will in case of a theft, give the attacker just worthless and unreadable data. With the help of advanced security methods, you will be able to protect your software and valuable data, which are necessary for your work.

The encryption mode of the Endpoint Security Tools is build on the PKCS #5 v2.0 encryption standard with the support of the safest hashing functions.

The ciphers were carefully chosen and there is not missing the AES cipher, certified by the American organization - National Institute of Standards and Technology (NIST) for use in the most strict conditions for TOP SECRET materials and used by the government of the USA. Endpoint Security Tools contains really only the most modern encryption standards.

2.4.1 The choice of cipher

You cannot make a mistake whichever cipher you choose in Endpoint Security Tools. We did our best to choose optimal ciphers and sizes of their keys with emphasis on their security and speed for a demanding business use.

In case you save very risky materials or programs we recommend you to use ciphers Serpent, Twofish, Rijndael or Blowfish. On the contrary, for the needs of frequent and huge data transfers RC5, RC6 or Twofish are recommended.

Generally, however, we point out that the choice of cipher is a secondary matter from the security point of view. We recommend you to focus on a careful choice of an access password.

2.4.2 Selection of hash functions

Hash function is a secret function that is needed especially when deriving a password. For all common operations the SHA-256 function is sufficient. It is not necessary to address this topic.

For an interested person we give an explanation and description of these functions:

The choice of a hash function is uniquely motivated by its simplexity and the absence of collisions. These attributes have been recently broken through in case of a lot of world wide recognized and frequently used functions (RIPEMD, MD5, SHA-0). These functions are naturally not implemented in Endpoint Security Tools. We have employed only the best quality algorithms consisting of Tiger algorithms and the SHA-2 family. We recommend you to use the initial SHA-256 function. Hash functions SHA-384 or SHA-512 are made-to-measure for truly intransigent advocates of security and military bodies.

- **TIGER** – A new method of generating prints have been invented by researches Ross Anderson and Eli Biham in 1995. This method is ready to fully exploit the potential of the forthcoming 64-bite architecture of a new computer generation. It generates a 20- or 24-byte print fully meeting the needs of an advanced disk encryption.
- **SHA-2** - The latest hash class SHA (Secure Hash Algorithm). The specification of this class includes definitions of new variants (sometimes collectively denoted as SHA-2) that include SHA-256, SHA-384 a SHA-512. It generates 32,48 or 64-byte prints.

2.4.3 Ciphers used

- **Blowfish** – One of the most secure ciphers proposed by a specialist in cryptology Bruce Schneider. Although it has been designed already in 1993, it is still one of the best and most often used ciphers. Blowfish is used as a standard cipher in the OpenBSD operating system, that is still considered by specialists as one of the most secure operating systems in the world. We offer this cipher with a key length of *448 bits*.
- **CAST5** - Created in 1996 and used by the Canadian government and its spy services Communications Security Establishment for a long time. Authors are Carlisle Adams a Stafford Tavares. It enables encryption by a *key 40-128 bits* long. Endpoint Security Tools supports a key length of 128 bits.
- **CAST6** -derived from CAST5, created by the same authors in 1998 and often used until now. This cipher has also been proposed as a AES standard. Its main advantage over CAST5 is a longer key - *256 bits* for a double size of an encrypted block compared to the predecessor.
- **MARS** – Another cipher from the AES top-five, designed in cooperation with the IBM corporation. Its author, Don Coppersmith, worked as a coauthor on the creation of the DES encryption standard in 1975. MARS has a quality design, works with a key *448 bits* long and is intended for inhospitable environments.
- **RC5** – RC is an abbreviation for Rivest Cipher according to the name of its author Ronald Rivest. This cipher was designed in 1994, it is fast and has a variable key lengths. We have implemented RC5 with a key length of *512 bits*. It is recommended to use this cipher on disks where big amount of data are often processed.
- **RC6** – a successor of RC5, that was also a runner-up in the AES final group. Overtakes a quality design, which is manifested not only in the security but also in the speed of an algorithm. Complements the RC5 cipher with an increased security and a key length of *512 bits*. Because of its speed we recommend you to use this cipher in case a big amount of data is often saved.
- **Rijndael (AES)**: an official advanced encryption standard proposed by Joan Daemen a Vincent Rijmen, it is a winner of the contest for a new AES encryption standard. Members of a final committee gave most votes to this cipher. The National Security Agency (NSA) classified this cipher with key lengths of 192 and 256 bits for the application on materials with the level of secrecy *TOP SECRET*. The key length for the Rijndael-AES cipher in Endpoint Security Tools is *256 bits*.
- **Serpent** – considered by cryptologists as one of the most *secure block ciphers*. Its excellent security parameters classify it among the leading ciphers in a secure storage of confid-

ential materials. In case of using the new 64-bit computer architecture it's implementation in Endpoint Security Tools is not only very secure but also very efficient. The key length is *256 bits*.

- **Twofish** - Another high quality encryption method. As a Blowfish-successor it fully meets the requirements on a high security and speed of encryption. It is also an AES runner-up and has very good security results. The implemented Twofish cipher is *256 bits*.

2.4.4 Deniability

One of other benefits that the Endpoint Security Tools provides is the deniability of data. Data are protected by strong ciphers that are impossible to decipher within real time. Encrypted data protected by Endpoint Security Tools look on the original disk as common random data and they appear for other potential attackers as if there were no data. Therefore, you can deny the existence of the data whenever you want.

All materials protected in this way for any needs are not detectable.

2.5 List of definitions

- **Allocation unit** - The smallest part of a disk space that we can use for saving a file. An example: Let's choose the size of an allocation unit to be 32kB. If a small file of 1kB size is written on a disk the whole 32kb cluster is occupied. On the one hand, increasing the size of an allocation unit leads to a speed up of access for disk operations, but on the other hand it is wasting of disk space in case of small files. It is recommended in the Endpoint Security Tools to keep the initial value.
- **Bit** - A basic unit of information. It takes the value 0 or 1.
- **Byte** - A unit of information quantity, a sequence of 8 bits.
- **Cluster** - see Allocation unit.
- **DES** - A standard encryption algorithm from the middle 1970's. It is very obsolete nowadays and today's modern computers can break this cipher within a couple of hours.
- **File system** - see File system.
- **Hash function** - It is a formula for the calculation of a check sum (print) for a message or a bigger amount of data. It can serve for controlling data integrity, fast comparing of a pair of messages, indexing, searching etc. It is an important constituent of cryptographic systems for digital signatures.
- **Simplexity** - It is a property of a hash function which indicates that it is computationally impossible to obtain an original pattern from a hash value already computed.
- **Disk label** - A text string representing the name of a particular disk partition.
- **Collision of a hash function** - An undesirable phenomenon upon which a couple of input texts are found within real time such that a hash function creates the same print for them.
- **Compilation** – The process of making up a program from source files, written by programmers, into an executable form (e.g. the well-known “.exe“ extension).
- **Operating system** (OS) – Basic software of a computer. Program equipment enabling elementary work with computer hardware and a communication with additional devices. Among the best-known operating systems are e.g. systems of Microsoft® Windows® family.
- **Dictionary attack** – Trial and error method for determining a password by trying possibilities derived from a list of words in a dictionary.

- **File system** - A designation for the way of organizing information (files) stored on memory devices (hard disks, tapes, CDs, DVDs). A file system divides a section on a disk into files and directories. Examples: FAT16, FAT32, NTFS.
- **Paging** - It is a process during which a less-used part of internal memory is temporarily stored by an operating system on a disk so that space can be made for new and more-used data. The reason for that is a more optimal usage of memory space, the disadvantage is a slower operation of an operating system at a frequent disk activity.
- **Encryption key** - It is a block of data used as a key for encryption. Its length is usually given in bits. This block of data has to be kept in confidence. Otherwise it looses its sense.
- **Internal memory** - Memory for the work of a computer processor. It is fast, much faster than external memory - hard disks etc.

2.6 Frequently asked questions (FAQ)

A list of **frequently asked questions** and the corresponding answers follows. Choose from the list on the left.

2.6.1 I forgot the password! What now?

If you created a disk with the security key, continue to the Forgotten Password chapter. For security reasons it isn't possible to restore the data from the disks, which do not contain the security key.

2.6.2 How secure are the ciphers used?

Let's give one example. Computer experts have recently succeeded in deciphering one cipher of the old DES encryption standard within a couple of hours and they needed a large computational farm to be able to do that. If there was a high performance computer capable of deciphering one DES cipher within one second, it would decipher one AES-Rijndael cipher (one of the ciphers used in Endpoint Security Tools) with a key length of 128 bits in 149 trillion years. This cipher is, however, provided in Endpoint Security Tools with a key length of 256 bit. Thus, it would take 149 billion x 149 billions years to decipher the cipher. Other ciphers implemented in Safetica have a similar performance.

A complicated standardized process has earned the cipher mentioned above the first place in the contest for a new encryption standard. This cipher was approved by the American National Security Agency (NSA) for usage with materials up to the level of secrecy TOP SECRET.

2.6.3 I have important data on the physical disk I want to encrypt. Can I access these data after encryption in the same way as until now?

Yes, but not directly. You have to follow this procedure:

Do a backup of all data on the disk using your backup program.

1. Encrypt the disk. It is necessary to use initial drive for compatibility reasons.
2. Copy your data back to your disk after disk encryption and connection.

2.6.4 If the Safetica software is uninstalled, are its disks removed as well?

For security reasons no. In case you want to remove encrypted disks, right-click on the corresponding line with a disk on the desktop and select remove. A guide helps you with the removal.

2.6.5 Is it possible to have a different password for every encrypted disk?

Yes, of course. Options providing better security and convenience for users were implemented preferably throughout the development including the option of different passwords for different encrypted disks.

2.6.6 Is it possible to change a password for a disk without having to create the disk from the very beginning?

Yes. You can change password simply by right-clicking on the particular disk on the desktop and selecting the item *Change password*.

2.6.7 Do the encrypted disks get disconnected after a user logs out?

No, they do not. You can carry out a simple disconnection of all disks by using a keyboard combination WINKEY-CTRL-U. For more information see here.

2.6.8 Which disks can I encrypt?

You can encrypt either virtual disks or physical disks. Click on these items to display a help how to encrypt disks.

2.6.9 Can I install programs into encrypted disks?

Yes, of course. A full functionality of any programs on the encrypted disks is one of the most important features available in Safetica.

2.6.10 If I want to remove the encryption, shall I choose a disk cleanup or a simple disk removal?

It depends on the circumstances, especially the extent of danger and hazards in the particular environment. We recommend to choose the disk cleanup.

2.6.11 I use RAID type of disk fields. Can I encrypt these fields as well?

Yes, of course.

RAID disk fields often used on servers with a high accessibility are an ideal environment for the usage of the Endpoint Security Tools. Data are protected by the RAID system against damage and by Endpoint Security Toolsagainst disclosure. If you install your RAID system, it is necessary to reboot your computer prior to the encryption.

2.6.12 Can I encrypt a system disk?

No. The system disk (typically called the C: drive) includes critical files and programs. Therefore, Endpoint Security Tools does not enable its direct encryption yet. It is possible, however, to overcome this limitation by creating the so called virtual disks on a system disk. Nevertheless, we are still working on this option.

2.6.13 Why is the startup of Safetica so slow?

The first startup is accompanied by installing program drivers into the memory of your computer and therefore, it takes more time than other startups. Please wait and do not start the program more times in the belief that the program does not start up. Thanks for your understanding.

2.6.14 Can I change the cipher type without having to create a disk again?

No, it is unfortunately not possible for security reasons. You have to overwrite the disk to change the cipher type.

2.6.15 Which file system shall I use?

The choice of a file system matters if you intend to use advanced file properties that are available in Windows 2000 and later. In such a case we recommend you to use the NTFS file system, that can be used from 3 MB up to the theoretical values of 256 TB (256*1024 GB). FAT32 is sufficient for common disk file systems. FAT32 can be used for disks of sizes ranging between 260 MB a 32 GB). The old FAT file system (0.5MB-4GB) can be used for small disks and floppy disks 3,5". However, the usage of this file system is limited by the length of filenames.

3 List of definitions

Term	Synonym	Abbreviation	Description
Safetica	product		Product name.
Auditor	Auditor		One of the main Safetica modules.
DLP	DLP		One of the main Safetica modules.
Supervisor	Supervisor		One of the main Safetica modules.
Safetica Management Service	server service	SMS	A service representing one branch.
Safetica Management Console	console	SMC	A management console for Safetica.
Safetica Endpoint Client	client station	SEC	A client on the employees' end stations. It is responsible for enforcement of the security policy and alternatively it enables the employees to use the security instruments.
Safetica Client Service	client service	SCS	A service on the client station that handles connection with the server service and database.
Endpoint Security Tools		EST	Security instruments on the client station. Available only with a valid DLP license.
Module			General identification of Auditor, DLP or Supervisor module.
Function			General description of the parts of the individual modules such as Disks, Anti-keylogger , Applications....
Main menu			The upper bar in the Safetica Management Console interface containing the controls.
User tree			Identification of the main user tree in the left part of Safetica Management Console containing users, computers, groups and branches (SMS servers).

View			General identification of the part of the graphic interface in Safetica Management Console that serves for displaying the settings and visualization of the selected functions.
Branch			General identification of one SMS together with the users, computers and groups that are connected to it and the corresponding database.
Visualization mode			Name of the console mode used for viewing data and graphs obtained from monitoring.
Setting mode			Name of the console mode used for setting modules and functions.
Log			List of records with detailed information
Web categories			Identification of the database of webs for categorization
Application categories			Identification of the database of applications for categorization
Extension categories			Identification of the database of suffixes for categorization
Alerts			Automatic notifications sent when a certain event occurs.
Tag			The mark of the product Safetica that is saved together with the file or folder and places it in a certain group of secured data unambiguously.
DLP			Data Loss Prevention/Protection

INDEX

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- K -

- M -

- O -

- P -

- R -

- S -

- T -

- V -

- W -

www.safetica.com