

USER GUIDE

SafeHouse Explorer

Version 3.7

#### Acknowledgement and Copyrights

We the documentation team of SafeHouse Explorer privacy protection product are thankful to Microsoft

for the writing standards and guideline in Microsoft Manual of Style.

Copyright © All rights reserved

SafeHouse reserves the right to make changes to this document at any time and without notice.

One can use the user guide only for reference and not commercial use.

Table of Contents

[Introduction 1](#_Toc12882454)

[Data Storage 1](#_Toc12882456)

[Data Protection 1](#_Toc12882457)

[SafeHouse Explorer for data protection 1](#_Toc12882458)

[SafeHouse Explorer Data Security 2](#_Toc12882459)

[Protect Data Files inside Volumes 2](#_Toc12882460)

[Windows Explorer User Experience 2](#_Toc12882461)

[Important point about volume and explorer 3](#_Toc12882462)

[Getting Started 4](#_Toc12882463)

[Launching SafeHouse Explorer 4](#_Toc12882464)

[Setting up Tools & options 5](#_Toc12882465)

[Working with SafeHouse Explorer 6](#_Toc12882466)

[Basic working of SafeHouse Explorer 6](#_Toc12882467)

[Opening volume 6](#_Toc12882469)

[Working with explorer window 7](#_Toc12882470)

[Close All or specific Volume 7](#_Toc12882471)

[Managing Volumes 8](#_Toc12882473)

[Creating a New Volume 8](#_Toc12882474)

[Opening Volumes 13](#_Toc12882481)

[Close All or specific Volume 16](#_Toc12882482)

[Suspending Access to Volume 16](#_Toc12882483)

[Updating volume 19](#_Toc12882484)

[Changing password 21](#_Toc12882488)

[Enforcing Strong password for volume 21](#_Toc12882489)

[Setting password length and expiration date 21](#_Toc12882490)

[Sharing & Emailing files and volumes 22](#_Toc12882491)

[Setting Sound effects for volume activity 23](#_Toc12882492)

[Working with memory Sticks 24](#_Toc12882493)

[Support for Smartcards 25](#_Toc12882496)

[Troubleshooting 26](#_Toc12882499)

[FAQs 27](#_Toc12882500)

[Customer Care & Feedback 28](#_Toc12882501)

# Introduction

# SafeHouse protects the confidential data in a secure container which can be retrieved only after entering password. Its like keeping data in a house which is safe with a lock and opened only with a key.

## Data Storage

A data is stored in the form of ‘File’ in computer. There are 2 types of Data files:

1. A text file: Data stored in the form of text. e.g., a text document (.docx,.xls,.pdf etc)
2. Binary file: Data stored in machine language(binary) form. e.g., an image file(.jpeg)

These files are stored in the storage space(**devices**) like computer memory, hard disk, Compact Disc, memory sticks and so on. As the number of files increase, they need to be organised for easy access. Files are organised and placed in a collection or container called ‘**Folders’**. Folders thus contains files related to each other. Multiple folders are placed in turn placed inside bigger storage area called **Drives**

in windows (Examples C:, D: and so on).

## Data Protection

Files can contain confidential (secret) data which one doesn’t want to share with others or get incidentally accessed. Such sensitive data can be protected from un-intended users (un-authorised user access).

There are two types of data protection methods:

1. Password protection
2. Encryption

**Password** protection is like locking something in a safe-deposit. It means no one can get to the locked content without knowing the right combination(password). Unfortunately, there are a lot of ways **hackers** could obtain the password or hack in without it.+ For example, it could be obtained with the help of malware, or it might be guessed if the user chooses a **weak** password. The PDF documents, the passwords placed on them can be removed using the CMD window or specific [password recovery tools](https://www.cyclonis.com/how-to-open-protected-pdf-file-forgot-password/).

**Encryption** is the process of encoding data in such a way that only authorized parties can access it. The data is ‘**encrypted’(encoded)** using an encryption algorithm – a [cipher](https://en.wikipedia.org/wiki/Cipher) – generating [ciphertext](https://en.wikipedia.org/wiki/Ciphertext) that can be read only if ‘**decrypted’(decoded)**.

One should only use data privacy products which uses both password AND encrypting the contents of the file (strong encryption!). Password protection is not the same as encryption. You already are using passwords to log into Windows, but these passwords are not protecting your files from being snooped.

For protecting files hence opt for SafeHouse File Security. It uses both the methods to secure files.

For **Data Storage,** files need protection but it’s not feasible to protect or put a lock (password) on each file due to large numbers. Thus, lock is put on storage area. Such locked (safe) area or container is called **vault or safes**. These are like locked houses which can be opened only through a key (password and encryption).

## SafeHouse Explorer for data protection

SafeHouse Explorer hides (protects) private documents and files, keeping them safe from un-authorise access. It does so by both above mentioned data security methods i.e. password and encryption (double level security).

The encryption strength of the algorithms built into SafeHouse are some of the strongest available in the commercial world. The files include documents, photos, videos, spreadsheets, databases and so on. It can protect files residing on any drive, including memory sticks, external USB drives, network servers, CD/DVDs and even iPods.

# SafeHouse Explorer Data Security

## Protect Data Files inside Volumes

Explorer hides secures data files, by placing them in a safe house named ‘**Volume’**. Once the files are placed in these safe containers, no one else can access them without entering a code called password. It enforces of **strong** password plus maximum-strength 256-bit advanced **encryption** of data (double security). [Encryption standard can be chosen e.g. Twofish 128 and 256]

Volumes are large protected container or folders which can range in size from a few megabytes to hundreds of gigabytes. It creates Volumes on your local **hard drive** or **external media** to hold your confidential files.

SafeHouse volumes can hold as many files as the size of Volume which one has to specify while creating volumes. And if you do ever run out of room, you can either create any number of additional volumes or use one of our commercial SafeHouse software allows to expand an existing volume called as **Re-sizing**

**You must create at least one SafeHouse volume to use SafeHouse Explorer.**

This volume is called as **Primary** Volume. Other any no of Volumes (Secondary) can be created any time as required for better organisation

## Windows Explorer User Experience

Working with your Protected Files using SafeHouse Explorer is just the same as the popular Windows Explorer. One doesn't have to change the working habits.

SafeHouse keeps your files protected in **Volumes**. To access these volumes, one enters the secret password. After entering password SafeHouse Explorer window is opened. **Explorer** of SafeHouse It works nearly identically to Windows Explorer. After successful authentication Explorer's familiar **drag-and-drop** ‘**Windows Explorer-like’** interface.is opened. The only thing you need to do is remember to save your sensitive files to the SafeHouse drive letter instead of drive C: or other as you might normally do. Once you choose a volume to work with and enter your password, you can freely drag and drop files back and forth between Windows Explorer and SafeHouse's protected storage vaults

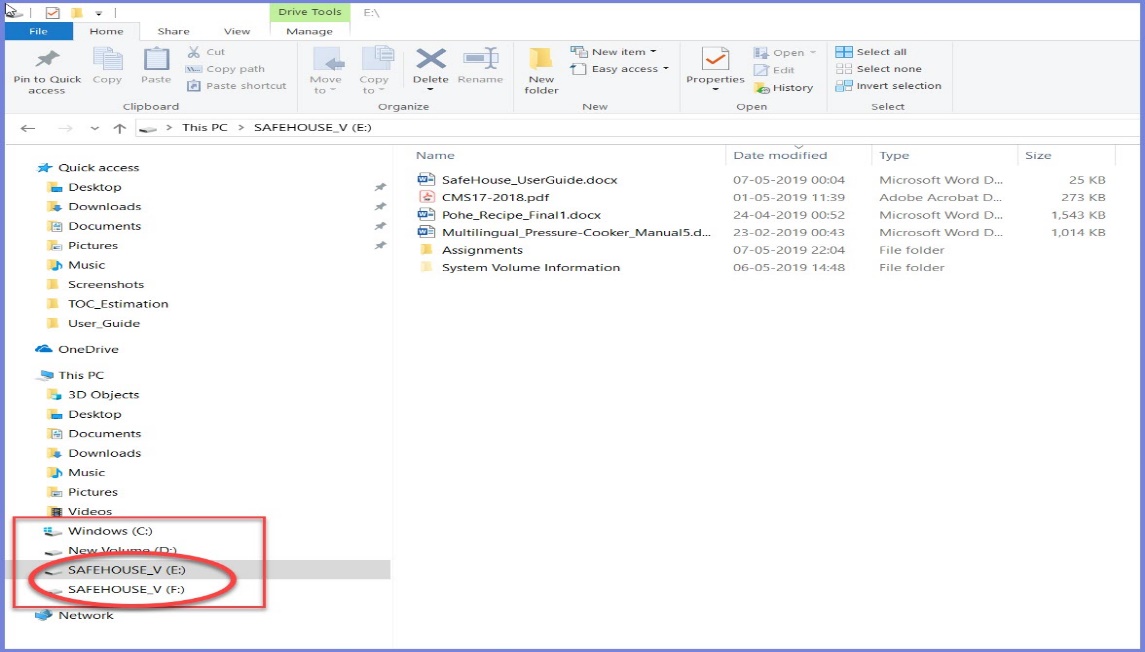


Figure 1: SafeHouse\_Explorer with Volume as windows Drive

As one opens windows explorer with short cut key ‘windows+E’, there is an ‘Explore files’ short cut in launching window (shown in figure 1) for opening SafeHouse Explorer. Files which are already

stored in volumes are displayed when explorer is opened or you can drag-and-drop files here for

safe storage. Once a Volume is opened by above methods, one can then open it from Explorer next time

by clicking on a Volume Drive created, similar to other windows drive example C:\.

## Important point about volume and explorer

|  |  |
| --- | --- |
| http://www.safehousesoftware.com/ExplorerHelp/IconVolume32.png | More on SafeHouse Volumes |

* Here's a few things you should know about SafeHouse volumes:
* Volumes are standard Windows files. You can view, move or delete them in Explorer just as you would with any other kind of file.
* The file extension for SafeHouse volumes is SDSK. You can easily identify them by their distinctive red folder icon (shown above).
* The maximum size for a volume is 2,000 Gigabytes, or the size of your hard drive; whichever is less.
* You can create as many volumes as you wish.
* Volumes can be located on internal and external hard drives, USB drives, memory sticks, CDs, DVDs and network servers.
* Every volume has a password. Passwords can be changed as often as desired.
* Volumes can be securely backed up to other drives, tape or DVDs using standard backup software.
* Windows will treat your volumes as new "virtual" hard drives which are only accessible once you enter your password.
* Volumes support all drag-and-drop file operations in Windows Explorer.
* When your files are saved inside a volume, they are protected using super-strong encryption.
* When you move a file out of a volume, it is no longer protected by SafeHouse.

A few simple rules:

* + - SafeHouse is 100% compatible with Explorer. Using Explorer is the easiest way to move your files over to SafeHouse.
    - If you "copy" a file from a normal folder on your C: drive to the SafeHouse drive, even though the copy inside SafeHouse is fully protected, you've still left your original copy in the old unprotected folder. The solution is to "move" instead of "copy". This way you're not leaving an unprotected copy of the file somewhere on your drive.
    - If you move or copy a file from your SafeHouse drive letter to some other drive or folder outside of SafeHouse, then that file is no longer protected by SafeHouse

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | | Getting StartedLaunching SafeHouse Explorer After installation, SafeHouse is visible as ‘System tray utility’ on Windows start menu. It runs as a system tray utility each time Windows starts.  Figure 2: System tray utility  SafeHouse icon (System tray utility) appears in the notification area located at the far right of the windows taskbar. Its the red padlock icon picture. If it doesn’t appear here then double click on the System tray utility shown above.  For Launching SafeHouse right click the red padlock icon. SafeHouse's main menu will be displayed as shown below:  Figure 3: Launching SafeHouse Setting up Tools & options There are several Tools available in SafeHouse which can be Launched by:   1. Right click the SafeHouse. red padlock icon in notification area of taskbar 2. Choose Tools & Options from the menu (Refer figure 1) 3. Click the Tools tab.   As shown in figure there are different wizards provided which will be explained in detail in further topics.    Figure 4: Tools and options menu Working with SafeHouse ExplorerBasic working of SafeHouse ExplorerFollowing steps are used to secure data in SafeHouse Explorer  1. Open Volume with password Authentication 2. Work with Files & Volumes (drag & drop) in Explorer 3. Close Volume  Opening volume Open Primary volume created during installation by right clicking Open Primary on launch menu.    Figure 5: Open Primary Volume  Authentication (entering password)    Figure 6: Enter password  One can hide and show password while typing by right clicking on the above window. But it’s alwaysrecommended to hide the password as shown in figure 15 while entering the same Working with explorer windowOpening Explorer Once password in entered the door of SafeHouse volume opens and takes us to  exploring files and folders in an Explorer window. The explorer is the place where all action of selecting files and folders to be copied takes place. There are different ways in which volume and in turn explorer can be opened (refer **Opening Volumes**) Moving Files & Volumes (drag & drop) Files dragged onto the surface from Windows Explorer are protected. Files dragged off back to Explorer are not protected.  Keep in mind that when you **copy** files into SafeHouse Explorer, the original remains in place until you remove it.  Volumes can also be dragged and drop  Figure 7: SafeHouse Explorer window Closing volume Close All or specific Volume from launch menu    Figure 8: Clos All or specific volume Managing VolumesCreating a New Volume One can create new volumes at any time. Make as many as you wish.  Some people like to create separate volumes for each area of work or subject. For example, you might create one for business and accounting, and then another to store your private photos.  The Create New Volume wizard shown in Tools tab (Refer figure ? of ‘Setting up Tools & options’ above) is used to create the container files (Volumes) which will house your private files and will protect them inside. Thus the Volume will turn to ‘Locked Safe HOUSE’ from a house.  This wizard will walk you through steps of picking a name, location, size and password.  If you're using smartcards with SafeHouse, the password you choose to protect this volume will automatically be written to your smartcard after your volume as been successfully created.  In figure below Click the Create New Volume button.  This wizard will advance through the following series of pages:  Additional Wizard Pages:   1. Name of Private Storage Area 2. Size of Your Private Storage Area 3. Auto-Resize preferences 4. Choose Encryption method 5. Specify password policy 6. Choose a Volume Password   Create New Volume Wizard on Tools Tab  Figure 9: Create New Volume Wizard on Tools Tab    Figure 10: Create New Volume Dialog box    Figure 11: Assign name to Volume  Figure 12: Set size of Volume    Figure 13: Auto re-size Volume   |  | | --- | |  | | |  | |
|  |

Figure 14: Choose Encryption Method

## 

Figure 15: Specify password Policy

## 

Figure 16: Assign password dialog box

## 

Figure 17: Assign Strong password

## Note: ‘Next’ button will be active only if strong password is chosen

Figure 18: Confirmation dialog

If all the details mention in confirmation dialog above are correct, proceed with clicking

‘Create Volume’

### Opening Volumes

SafeHouse provides 3 ways for you to open the [volumes](http://www.safehousesoftware.com/Manual/User_s_Guide/Where_SafeHouse_Keeps_your_Files.htm) containing your private files. The reason we provide so many ways is that everybody works differently, and it's important that we make getting at your files as easy as possible; no matter how you choose to work.

Open your volumes using:

1. The SafeHouse red padlock icon in notification area of taskbar
2. A desktop shortcut with red padlock icon
3. With windows explorer

All of these methods support using smartcards to fill in your password so you don't have to type them.

Method 1:

**Open Primary Volume**

Open your primary volume by either:

1. Double-clicking the red padlock icon. notification area of taskbar
2. Right clicking on the padlock icon and choosing the ‘Open Primary’ menu item. (Refer figure )

Both methods have the same result, which is to display the red password entry dialog shown below.



Figure 20: Enter password

Figure 19: Open Primary Volume

In the dialog box enter your password and press Enter or click. ‘Open’.

Note: This dialog is bypassed if you are using a smartcard and SafeHouse was able to automatically retrieve your password

TIP: If you would prefer to see the letters of your password as you type them, right click on the window caption and select the [Reveal Password](http://www.safehousesoftware.com/Manual/User_s_Guide/Reveal_Password_as_Typed.htm) option.

**Open Secondary volume with more options**

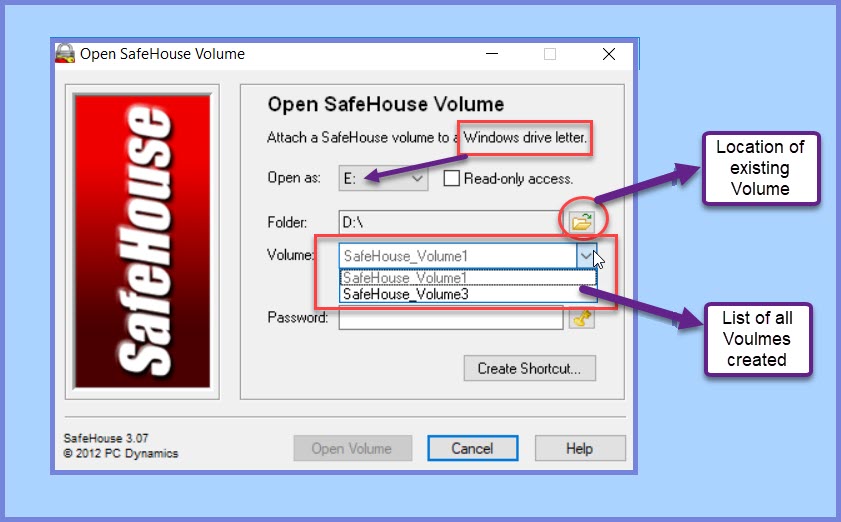
****To open other volumes, or if you need more flexibility in choosing how your volume is opened, select the ‘Open Volume’ (Refer figure 1) to display the long-form dialog box below. This dialog box gives you complete control over how your volume is opened.

Figure 21: Open Volume

Select a volume and drive letter, enter password and then click the ‘Open Volume’ button to accept.

(Note: The ‘Open Volume’ button is not activated till password is enter)

You may optionally check the Read-only access checkbox to simulate write-protected media. This guarantees that your files cannot be updated. With this option multiple Volumes can be opened at the same time Each one will appear as a separate drive letter

TIP: The key icon to the right of the password entry field takes you directly to the ‘[Change Password](http://www.safehousesoftware.com/Manual/User_s_Guide/Changing_Volume_Passwords.htm)’ dialog.

Method 2:

**Opening Volumes using a Desktop Shortcut**

Another way to open volumes that you use frequently is to create a desktop shortcut  Open http://www.safehousesoftware.com/Manual/PadlockIcon.pngSafeHouse Volume dialog pictured above.

SafeHouse will create a shortcut directly on your desktop which looks like the padlock icon shown here on the left.

Follow these steps to create a desktop shortcut:

Launch the Open SafeHouse Volume dialog.

Select a volume and corresponding Windows drive letter to be associated with it when opened.

Click the Create Shortcut button.

Double-clicking this shortcut launches the familiar red password dialog to receive your password. The password dialog will be bypassed if you are using a smartcard.

Method 3:

**http://www.safehousesoftware.com/Manual/IconVolume32.pngOpening Volumes using Explorer**

SafeHouse also allows you to open volumes using Windows Explorer.

SafeHouse volume files can be identified in Explorer by their distinctive red folder icon shown here on the left. Their default location is typically C:\SafeHouse, however you could choose to store them anywhere, including on other disk drives, memory sticks or even CD/DVDs.

To open volumes using Explorer, either:

Double-click the red folder icon corresponding to the volume file.

Right click on the red folder icon and choose the Open Volume menu item.

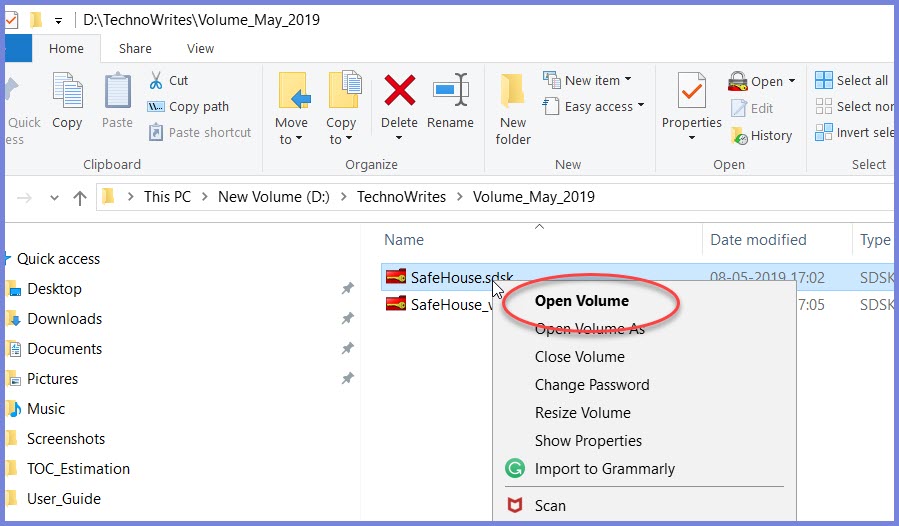
Both methods have the same result, which is to display the familiar red password entry dialog. This dialog is bypassed when using smartcards.

Figure 22: Open Volume through Windows Explorer

**Opening Volumes using a Smartcard**

When you are using smartcards with SafeHouse, the software will attempt to retrieve your volume passwords directly from your smartcard. If SafeHouse determines that you need to authenticate using your PIN, you'll see the dialog pictured below.



Figure 23: Opening SmartCard

Once your insert your smartcard, the cards name will be displayed in the lower left corner of the dialog.

If you click Cancel when this dialog is displayed, you'll be allowed to type your password manually.

### Close All or specific Volume

One can close all volumes from ‘**Close all**‘ option of launch safehouse dialog (Refer Launching SafeHouse). To close specific volume through launch SafeHouse dialog, click on **‘Close volume’** for the following dialog to open



Figure 24: Close Volume dialog

One can choose from many already opened Volumes.

### Suspending Access to Volume

SafeHouse includes a variety of features to help you guard access to open volumes. These features are important because they help with times when you don't want to close your open volumes, yet you also don't want to leave your files exposed. Or when you simply step away from your PC for a while, leaving it vulnerable to intruders.

The solution is to ‘suspend access’ to your volumes.

Suspending access to volumes is not the same as closing them. Technically, as far as Windows is concerned, the volumes are still open. However, under the hood, SafeHouse takes control and temporarily blocks all low-level disk activity to the open volumes. Access to the volumes will remain blocked until you enter your password.

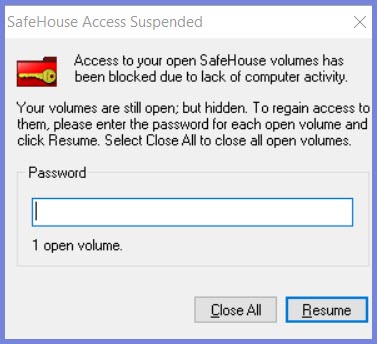
Once SafeHouse enters the suspended state, the dialog pictured below is displayed and your password will be needed to regain access to the open files.

Figure 25: Suspended access to volume

Enter the password for your open volume.

If you have more than one volume open when this dialog appears, you'll need to enter the passwords for each volume in order to exit this mode. The message under the password input field tells you how many passwords are still needed. Enter one password at a time and click Resume.

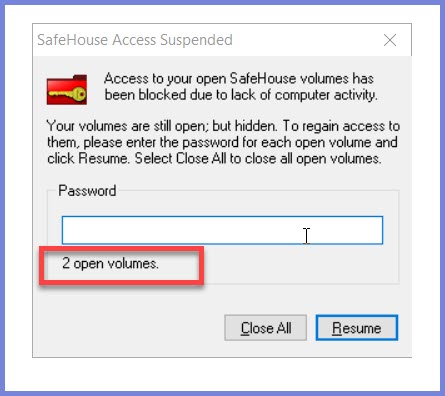


Figure 26: Multiple Volumes Suspended

Read password from Smartcard

When using smartcards with SafeHouse, clicking this button will cause SafeHouse to read your volume passwords from your smartcard and resume. Your smartcard PIN may be required; depending on your smartcard PIN cache configuration settings. In this case, there is no need to manually type your password in the field above.

If you have more than one volume open and are using multiple smartcards, you'll need to insert each card in turn and click this button to let SafeHouse find all the passwords it needs from your various smartcards.

Volumes can be suspended using any of the following methods:

• Manual suspension using a red padlock icon on notification area on far right of taskbar.

• Automatic suspension:

**Manually Suspend** Access to Open Volumes

You can manually suspend access to your open volumes by clicking the Suspend Access system tray menu option (Refer figure 1) The affect is identical to any of the automatic trigger options described on this page.

**Automatic Suspension** (Suspend action Triggers)

The suspend action to be taken when one of these events takes place:

is detected is determined by the Take this Action setting???

Th events or triggers causing suspension of volume are:

**Windows Hibernates**

SafeHouse will watch for when your PC enters a sleep or hibernation state. This is useful when your PC goes to sleep when you have sensitive files open and you don't want somebody later coming along and waking up your PC and having access to your files.

**Keyboard and Mouse are Inactive (period of inactivity)**

If you would like to trigger volume access restrictions after some period of inactivity. For this event to trigger, your keyboard, mouse and SafeHouse volumes must not see any activity for the specified period of time. This means that any background program that you have which routinely accesses files on an open SafeHouse volume will prevent this event from triggering.

When SafeHouse smartcard is removed

The final way to trigger restrictions on open volumes is by removing your smartcard when you've enabled smartcard removal detection as shown below.

In this case, the SafeHouse volume activity monitor is notified when smartcards are removed and it immediately suspend access to your open volumes.

**Suspend Access**

Choose this option to put your volumes into a suspended state when the activity monitor triggers.

Once volumes are placed into a suspended state, you will need to re-enter your password in order to begin using them again. This is not the same as closing them. Here, they remain open; just inaccessible. This is generally a safe state even when you have open documents or files on the volume.

Please note that some applications which automatically keep trying to access files on suspended volumes may at some point give up and report an error. This is something outside of the control of SafeHouse. Our job is to cut off access. If you are at the same time running applications which don't like this behavior, then you may need to choose which applications and features are most important to you.

Immediately Close All Open Volumes

Choose this option to close your open volumes when the activity monitor triggers.

Be careful in choosing this option. Closing a volume with open files could cause damage to your files.

These actions can be set from Activity Monitor wizard

**SafeHouse Activity Monitor**

The SafeHouse activity monitor runs silently in the background watching for certain events which might put your open volumes at risk. These include putting your PC to sleep or leaving your PC unattended when you have open volumes.

The SafeHouse Activity Monitor dialog is where you set preferences for the kinds of things SafeHouse will watch for, and the action which should be taken in the circumstance one of these events is detected.

How to Launch this Dialog:

1. Right click the [SafeHouse padlock system tray icon](mk:@MSITStore:C:\Program%20Files%20(x86)\SafeHouse\SAFEHOUSE.CHM::/User's_Guide/Tools_and_Options.htm).
2. Choose Tools & Options from the menu.
3. Click the Tools tab.
4. Click the Volume Activity Monitor button.
5. Suspend Access

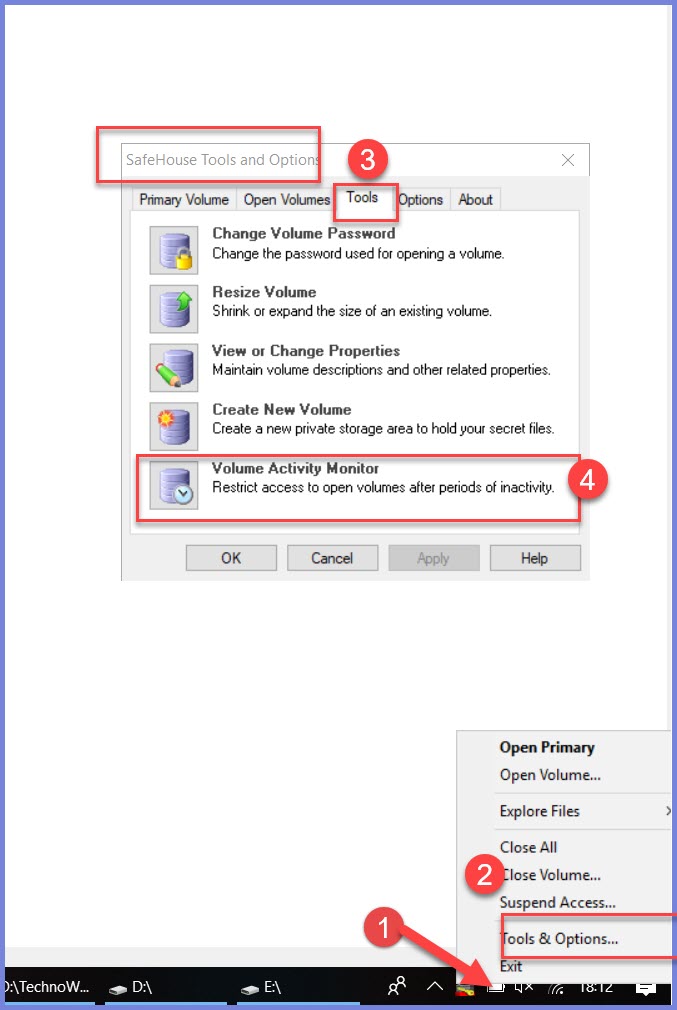


Figure 27: Activity Monitor

Choose this option to put your volumes into a suspended state when the activity monitor triggers.

Once volumes are placed into a suspended state, you will need to re-enter your password in order to begin using them again. This is not the same as closing them. Here, they remain open; just inaccessible. This is generally a safe state even when you have open documents or files on the volume.

Please note that some applications which automatically keep trying to access files on suspended volumes may at some point give up and report an error. This is something outside of the control of SafeHouse. Our job is to cut off access. If you are at the same time running applications which don't like this behavior, then you may need to choose which applications and features are most important to you.

### Updating volume

One can update volume or other properties form Tools Tab in ‘Tools & options’ of launch dialog

## 

Figure 28: Update Properties

On clicking ‘View or Change Properties’ following dialog will be opened.

Here you need to Authenticate yourself to make changes or updates (Modify button is not activate till then).

## 

Figure 29: Update or View Volume Properties

## 

Figure 30: Change Settings

# 

## Changing password

### Enforcing Strong password for volume

Figure 31: Choose Volume Password

Please choose the strong password for your volume. You can change your password as often as desired.

**Choosing Strong Passwords**

Be careful when you choose your passwords. Passwords are case sensitive, up to 255 characters.

Dos:

We recommend Password

* At least 10 or more characters.
* Add upper- and lower-case letters,
* Add numbers and punctuation symbols.
* Add at least 1 special character

Don'ts:

* Use your name, pet name or child's name.
* Use some number or date readily identifiable with your life or family members.
* Use passwords shorter than 8 to 10 characters. The more the better.
* Use common words found in the dictionary unless combined with other numbers and symbols.
* Write your password on a sticky note taped to your monitor. Yes, people do this all the time.

The Next button will be enabled only once you've entered an acceptable password.

**Strength Meter**

This password strength meter operates as a guide to help you choose strong passwords that are difficult to guess. The bar will turn green as you choose better passwords.

This meter is only a guide. We cannot guarantee with any certainty that specific passwords will never be guessed.

Choose your password and then type it again in the field below.

Retype

Retype your chosen password here to make sure it's what you think it is.

### Setting password length and expiration date

This option is available and can be set during creating a volume. (refer Creating new volume)

## Sharing & Emailing files and volumes

One can email or share files or volumes from the SafeHouse Explorer as shown in following figiure

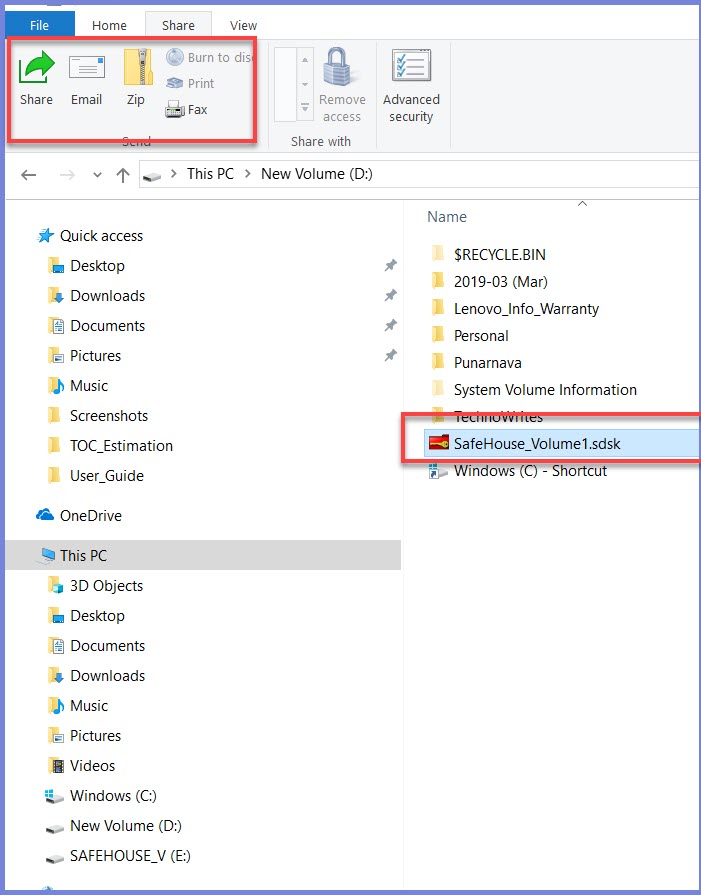


Figure 32: Sharing & Emailing Volume

Note: Files you drag out of SafeHouse and attach to emails are no longer protected by SafeHouse. If you need to email protected files, follow below steps

Sending Files

* Follow these steps:
* Senders should create a new volume just big enough to hold the files to be sent. Anything bigger than that will be wasted space and inefficient since you'll be sending the entire volume as an uncompressed attachment.
* This new volume is opened, filled with files, then closed. It's very important to close the volume before attaching it to emails.
* The sender must then find some way of telling the recipient what the password to the volume is. Obviously, it would be crazy to include it in the same email.
* This new volume file can then be attached to an email in the same manner as you would attach any other kind of file.
* About Compression
* SafeHouse volumes do not compress well. That is just the nature of encryption, because the data inside the volume is so random that common compression routines just don't have anything to grab on to (that's the point of encryption).
* We're often asked if ZIP files might help. Generally, they won't help much, but they won't do any harm either. Feel free to try. But if you see that you're not gaining much on size, it's probably better just to send the stand-alone volume file.

Receiving Files

* When you receive a SafeHouse volume as a file attachment, there are two primary requirements to view the files inside the volume:
* You must know the password.
* You must have SafeHouse installed.
* Hopefully the sender communicated the password to you by phone or some other way (but never in the same email).
* If you don't have SafeHouse installed, you can download a fully-functional trial copy from [SafeHouseSoftware.com](http://www.safehousesoftware.com/).
* To open the volume, either:
* Open it directly from the email (typically by double-clicking on the attachment icon) and enter the password.
* Copy the attachment to your desktop or some folder and open it from there by double-clicking on it. This allows you to easily make changes and send the updated material back to the sender.

## Setting Sound effects for volume activity

SafeHouse includes custom sounds which are played when volumes are opened and closed. You may change the sounds played by SafeHouse by placing specifically-named WAV files into the SafeHouse program files directory.

## Working with memory Sticks

Protecting Files Stored on Memory Sticks

|  |  |
| --- | --- |
| http://www.safehousesoftware.com/ExplorerHelp/USB8.png | SafeHouse Explorer is perfect for protecting files stored on memory sticks. In fact, this is one of the primary uses for the product.  You don't need to do anything special in order to use SafeHouse Explorer with Flash memory sticks. All that's needed is insert your memory stick into your PC and use the [Create SafeHouse Volume](http://www.safehousesoftware.com/ExplorerHelp/User_s_Guide/Creating_a_New_Volume.htm) wizard to instruct SafeHouse Explorer to create a new protected storage vault (volume) on the corresponding Windows drive letter.  SafeHouse really doesn't care where your volumes are located. Just point to them, enter your password, and drag and drop files back and forth. [Learn more...](http://www.safehousesoftware.com/ExplorerHelp/User_s_Guide/Tips_for_Memory_Sticks.htm)  SafeHouse really shines when it comes to working with USB memory devices. |

## SafeHouse can work with protected volumes on memory sticks just as easily as it can with volumes hosted on your local hard drive.

SafeHouse Trial Version on Memory Sticks

We recommend keeping a copy of the SafeHouse trial version on your memory stick just in case you ever need quick access to the files on your memory stick and you're not at your normal PC. The trial version is freely distributable and it's perfectly okay to put a copy on your USB device. This way, you have everything you need right with you if you need to get at your files using somebody else's PC.

SafeHouse Explorer

You should also know about our [SafeHouse Explorer](http://www.safehousesoftware.com/Manual/User_s_Guide/Product_Comparison.htm) software which is perfect for memory sticks. If you frequently access files on your memory stick from different computers, the primary benefit of using SafeHouse Explorer is that it doesn't need to be installed -- you can run the SafeHouseExplorer.exe program directly from your memory stick. SafeHouse Explorer is a freely-distributable companion product which can be downloaded from the [SafeHouseSoftware.com](http://www.safehousesoftware.com/) website.

**Creating Volumes on USB Memory Devices**

SafeHouse allows you to create new volumes directly on USB memory devices. You don't have to do anything special. The steps below will guide you through the process.

Alternatively, if your volume already exists on your hard drive, you can simply use Explorer to copy it to you USB drive (be sure the volume is closed before doing this).

Follow these steps:

1. Launch the [SafeHouse Create Volume wizard](http://www.safehousesoftware.com/Manual/User_s_Guide/Creating_a_New_Volume.htm) as you normally would to create any new volume.
2. When the wizard asks you to [choose a location or folder](http://www.safehousesoftware.com/Manual/User_s_Guide/SDWCREAT_Naming.htm) for the volume, click the tiny folder icon and browse to the drive letter for your USB device.
3. Pick any name you want for your volume file. The file can reside either in the root or any folder of the USB device.
4. Advance through the remaining pages of the wizard and create the volume directly on the device.

## Opening Volumes on USB Memory Devices

Follow these steps:

1. Insert your USB device into your PC.
2. View the files on the device using Explorer and locate the SafeHouse volume file.
3. Double-click on the volume file to open it up.
4. SafeHouse will prompt for your password and then open the volume identically to how it opens volumes located on your standard hard drive.
5. Your private files will then be fully accessible to you.

Please remember to close your volume before removing the USB device from your PC.

## Support for Smartcards

## Using Smartcards with SafeHouse

SafeHouse includes unprecedented support and integration for smartcards throughout the entire product. Store your SafeHouse passwords on a smartcard and never have to type them again.

## USB Memory Stick = Smartcard

Don't have a smartcard? SafeHouse can turn an ordinary USB flash drive or memory stick into a smartcard that has all the same features as commercial hardware solutions when it comes to storing your SafeHouse passwords. We call this our virtual smartcard.

Benefits of Smartcards

* Relatively inexpensive. You can even use an off-the-shelf USB memory stick!
* Small devices fit in wallets, purses and on key chains.
* Remember one PIN code no matter how many passwords are stored in the smartcard.
* SafeHouse can read your volume passwords directly from your smartcard.
* You can choose longer more-complex passwords for SafeHouse since you won't be needing to type them.
* Security is increased since both the smartcard and its PIN are needed to use them.

# Troubleshooting

This section describes possible solutions to problems you might encounter while using SafeHouse.

On Vista, my volumes seem to be read-only no matter what.

If you have a volume on a normal hard drive which seems to open in read-only mode no matter what you try, it is nearly always an ownership or permissions problem with regard to how Windows/Vista manages file access controls. This can happen sometimes when moving volume files from one PC to another; especially when you are upgrading to Vista and transferring all of your files.

First, make sure that the [read-only checkbox is not checked in Explorer](mk:@MSITStore:C:\Program%20Files%20(x86)\SafeHouse\SAFEHOUSE.CHM::/User's_Guide/Read-Only_Files.htm). If it is, this is the root of the problem and the solution is simple: uncheck this setting.

If the volume file is not marked read-only, then examine your file permissions. Windows is forcing the file into a read-only mode for your protection because it senses something is not quite right. You might try making a test volume in the same folder to see if that will work (because newly-created volumes will have the required permissions).

We have also noticed that Vista (but not XP or earlier versions of Windows) seems to place extra protections on files in the root of your system drive. If you place a volume in the root of your C: drive, you'll likely run in to this read-only problem. The solution is to move the volume into a folder.

If you can't seem to get the permissions right, try creating a new volume in the same folder with a size big enough to hold all of the files in the problematic volume. Open both the old and new volumes at the same time and use Explorer to drag all the files from the old volume to the new one. Once you're sure everything is working as needed, delete the old volume.

Please understand that file permissions are completely controlled by Windows, not SafeHouse.

How do I recover a damaged volume?

The best way to recover when you sense your SafeHouse volume has been damaged is to restore from your most-recent safety backup. If you don't have a recent backup, there still might be hope due to the fact that SafeHouse is frequently able to keep a shadow copy of certain critical information, and you can restore from that shadow in an emergency. See [How to Repair a Volume](mk:@MSITStore:C:\Program%20Files%20(x86)\SafeHouse\SAFEHOUSE.CHM::/User's_Guide/Repair_Volume.htm) for more information.

What to do when you notice some strange drive compatibility problem.

If you're experiencing some unexplained compatibility problem with SafeHouse, you might try telling SafeHouse to open your volumes as removable media instead of as fixed media. We've seen this cure a variety of ills over the years related to driver conflicts. This setting can be found on the [Options](mk:@MSITStore:C:\Program%20Files%20(x86)\SafeHouse\SAFEHOUSE.CHM::/User's_Guide/Setting_Options_and_Preferences.htm) tab.

SafeHouse worked fine for months, then suddenly there's a problem.

If you've been using SafeHouse for a long time and everything has been working just fine, and then suddenly you experience some strange problems, please don't simply assume the software has gone bad. Software doesn't change all by itself. Something on your PC changed. Listed below are some of the most-common causes.

You may have just recently installed some other new software that does not play well with SafeHouse.

You may have Windows automatic updates enabled and some new patch from Microsoft introduced a conflict.

You may have had some hard disk or registry corruption due to a virus of physical drive problem.

In many cases, the quick solution is to use the Restore Point feature built into Windows to restore your system to a known good state from a few days earlier.

# FAQs

Can SafeHouse volumes be backed up?

Absolutely. SafeHouse volumes are normal files and can be backed up using either Explorer or any standard backup software. See [Backing Up SafeHouse Volumes](mk:@MSITStore:C:\Program%20Files%20(x86)\SafeHouse\SAFEHOUSE.CHM::/User's_Guide/Backing_Up_SafeHouse_Volumes.htm).

Can multiple users use the same volume at the same time?

Yes, but there are some restrictions..

Does SafeHouse work on CDs and DVDs?

Absolutely.

Can SafeHouse be used to protect email attachments?

Yes. SafeHouse volumes can be emailed as attachments just like any other file..

Can SafeHouse Personal Edition read volumes created with the Professional Edition?

Yes. Although the Personal Edition does not support creating volumes with the wide variety of encryption schemes included in the Professional Edition, it can, however, read and write any volume created using either edition. And the same goes for the Professional Edition.

How do I delete a SafeHouse volume?

SafeHouse volumes are just normal files -- albeit much bigger than most other files. You can delete them using Explorer as you would any other file. Be careful about your Recycle Bin. You'll need to empty your Windows Recycle Bin to fully reclaim the space used by the volume. Alternatively, you can tell Explorer to bypass the Recycle Bin by holding down the keyboard shift key while clicking on the Delete menu item in Explorer (right click on volume file in Explorer, hold shift key and click Delete).

What happens if I lose my SafeHouse password?

SafeHouse passwords can only be reset if the resettable password feature was specifically enabled by your system administrator in advance. This feature is included in the Professional Edition only. See the [**Administrator's Guide**](mk:@MSITStore:C:\Program%20Files%20(x86)\SafeHouse\SAFEHOUSE.CHM::/Administrator's_Guide/Introduction.htm)for more information on resetting lost passwords.

Are the volumes compatible with SafeHouse Explorer?

Yes, SafeHouse Explorer uses the exact same volume file format as SafeHouse Personal and Professional editions.

What are the limitations of the trial version?

SafeHouse operates in trial mode whenever it is installed without entering an activation key. For the first 30 days, SafeHouse is 100% functional with the minor exception that it does not allow you to choose long passwords when creating volumes. After 30 days, the software changes to read-only mode, whereby you can still open volumes and read all files; however, you will not be able to write back or update them. As such, you will never be locked out from getting at your own files, even if you choose not to purchase the software. This also makes it easy to distribute encrypted data on CD/DVD since recipients can use the trial software to access the protected files.

Can the trial version be freely distributed?

Yes. You may freely distribute the SafeHouse trial version, including, but not limited to distributing it on CD/DVD, hard drives and USB devices. You do not need any special license to do this nor do you need to contact us or receive permission in advance. Please obtain the latest version of the SafeHouse software from [SafeHouseSoftware.com](http://www.SafeHouseSoftware.com). The download available from the SafeHouse website is a dual-mode installer which installs in trial mode when you do not enter an activation key.

How can I shrink a volume?

The SafeHouse Resize Volume wizard is the first place to look for shrinking a volume; however, it can only shrink within certain limits. It does not move any files around within the volume, so if you have large gaps between where files are located (something that can occur naturally in Windows) it may not be able to offer you the level of shrinkage you desire. Further, it cannot shrink lower than the original starting size. But there is a very simple solution for getting smaller. Create a new volume of the size you want, then open both old and new at the same time and drag the files over to the new one. When you're satisfied all is good, you can close the old volume and delete it.

Does SafeHouse have any Weaknesses?

Different manufacturers take different approaches to encryption and data privacy. Like any other kind of lock in the world, each approach has its pros and cons, conveniences and inconveniences. SafeHouse uses an approach known as virtual disk encryption. This is a very safe technology, however, there are some things you may want to be aware of just to be clear on what protection is provided, and what is not.

Things to know:

Windows keeps what is known as a "swap file" to help move data in and out of memory as it needs to make room for running multiple programs at the same time. This swap file is typically saved to drive C: and is frequently 1 to 2GB in size. SafeHouse does not protect the contents of this temporary Windows file. It is possible that if you were working on a sensitive document and Windows wrote some of the memory containing your confidential text to the swap file, fragments of your document could be found in the swap file for a very short period of time. Most security products do not encrypt the swap file since to do so would significantly slow down Window's performance. It would take a very skilled and determined intruder to extract any information from this file, and then, only very small bits here and there might be there.

SafeHouse cannot protect you from keyboard sniffers.

When a volume is open, all access to the volume is controlled by Windows, not SafeHouse. Therefore, a rogue program or virus could attempt to inspect or delete files within the SafeHouse drive letter - just as it might for your primary C: drive. Closed volumes are immune to such attacks. If you are surfing the Internet and are worried about some browser vulnerability allowing access to your disk files, you are advised to close your SafeHouse volumes before visiting unsafe websites.

It's important to know that the items mentioned above are common to the technology used by SafeHouse and not specific programming flaws within the software. SafeHouse is a very safe and secure product which has withstood the test of time.

# Customer Care & Feedback

You can contact support by e-mailing [support@SafeHouseSoftware.com](mailto:support@SafeHouseSoftware.com)

Please visit [SafeHouseSoftware.com](http://www.safehousesoftware.com/) for up-to-date contact information.