Introduction

SafeHouse for Windows from PC Dynamics is the key to PC data privacy.

Using SafeHouse, you can allocate a portion of your existing hard drive(s) to be reserved for encrypted data. This is accomplished using the create encrypted volume utility. SafeHouse encrypted volumes appear on your PC as another Windows drive letter. All encryption is performed automatically and transparently on the fly. You can do anything with a SafeHouse drive that you can do with a normal hard drive; only that with SafeHouse, the encrypted volume requires password authentication before the files become accessible.

SafeHouse Supports the Most Popular Encryption Algorithms

SafeHouse includes support for the most popular encryption algorithms of the day. This includes DES, triple DES, Blowfish, Twofish and the new Advanced Encryption Standard (AES) Rijndael cipher. By supporting such a wide variety of ciphers in various key strengths, SafeHouse is able to meet the encryption requirements for a diverse set of commercial and government environments.

Please note that the shareware version of SafeHouse limits key strengths to 40 bits to adhere to U.S. export guidelines.

Why is SafeHouse so Important?

If you work with sensitive data, you need SafeHouse. Hundreds of computers are stolen every day. Can you afford to have someone see your files? Do you have personal letters, client write-ups or financial information on your PC? How would you know if a coworker looked at your files? With SafeHouse, you can rest easy knowing that even when your computer is left unattended, nobody can access your files.

Getting Started is Easy!

You can be up and running with SafeHouse in just a few minutes. All SafeHouse utilities are designed as easy-to-use Windows wizards to guide you at every step. See Getting Started with SafeHouse.

Once this software is installed, save your sensitive data to your SafeHouse volume instead of your C: drive. The rest is automatic!

SafeHouse for Windows requires:

- Windows 95, 98, 98se, Me, NT, 2000 or XP
- 486, Pentium or equivalent CPU
- Approximately 5MB available hard disk space plus space for your data

The setup program will automatically detect your operating system and install the appropriate set of drivers and administration utilities.

Getting Started with SafeHouse

You can be up and running with SafeHouse in just a few minutes. Icons for each of the utilities referenced below were installed for you automatically during setup. Setup will also install icons into your Start menu and directly onto your primary desktop.

Icons installed for SafeHouse:

- SDW.HLP SafeHouse Help File
- SDWCREAT.EXE Create SafeHouse Volume
- SDWMAP32.EXE Map SafeHouse Volume
- SDWMAP32.EXE UnMap SafeHouse Volume
- SDWCHANG.EXE Change SafeHouse Password
- SDWEXPAN.EXE Resize SafeHouse Volume
- SDWACTIV.EXE Change SafeHouse ActivCards
- SDWSHOW.EXE Show Volume Properties
- SDWMON32.EXE SafeHouse Volume Monitor
- SDWTRAY.EXE System tray utility for quick access
- SAFEHOUSE.PDF SafeHouse Manual (Acrobat PDF format)
- DEPLOYHLP.EXE SafeHouse Deployment Tool
- README.TXT Readme File

Also Installed:

- Remove SafeHouse from your PC

SafeHouse for Windows requires:

- Windows 95, 98, 98se, ME, NT, 2000 or XP
- 486, Pentium or equivalent CPU
- Approximately 5MB available hard disk space

Use the SafeHouse system tray icon for quick access to all SafeHouse utilities:

The easiest way to access the various features and utilities included with the SafeHouse software is to use the convenient system tray icon found in the lower right corner of your screen. Right clicking on this icon displays the menu shown below. Select the properties option to display a dialog panel used to access the less-often used utilities for creating new volumes, changing passwords and resizing volumes.

If you do not see the SafeHouse "lock" icon in your system tray, you can run it manually by executing the SDWTRAY.EXE file located in the directory containing your SafeHouse program files.

To prepare for using SafeHouse, you must:

1. Run SDWCREAT.EXE to create an encrypted volume using the Create SafeHouse Volume menu shortcut.

The SDWCREAT.EXE create volume utility must be run once for each new encrypted volume you wish to create. You may have an unlimited number of SafeHouse volumes residing on your hard drive; however, you may only access these volumes when they are mapped (assigned) to a SafeHouse drive letter. Up to 10 drive letters may be mapped at a single time; more on NT/2000/XP. Volumes may be created in any size up to 2048 gigabytes if your operating system supports NTFS (NT/2000/XP) or up to 4GB host drives formatted using FAT32 (Windows 98, Me and sometimes 2000/XP). Some versions of Windows 95 and NT support only FAT16 hard drives and SafeHouse volume sizes are subsequently limited to 2GB on those platforms. Volumes may reside either on your local hard drive or on removable media such as diskettes or ZIP disks. Additionally, volumes may be created on local area network drives and accessed remotely. The wizard used for creating new volumes will help you choose volume sizes that are compatible with your current PC configuration.

SafeHouse integrates with the Explorer shell extensions to provide quick access to encryption features by right-clicking on SafeHouse volume files.

To work with files on your encrypted volumes:

- Run SDWMAP32.EXE to Map your SafeHouse encrypted volume to a Windows drive letter using the Map SafeHouse Volume menu shortcut.
- Create, read and write files to the volume as you would any other drive.
- When you are done, run SDWMAP32.EXE in the unmap mode using the UnMap SafeHouse Volume icon.

The SafeHouse setup program likely automatically created icons for mapping and unmapping volumes. Simply double-click the icon for the desired utility and fill in the blanks. You might want to consider placing the map volume icon into your Windows Startup group so that you'll be prompted to authenticate yourself automatically each time you turn on your PC. See Mapping and UnMapping Volumes.

To change your password:

- Run the SDWCHANG.EXE wizard utility using the Change SafeHouse Password menu shortcut.

You may change your SafeHouse volume password as often as desired. Note that it is possible to create SafeHouse volumes which specifically require periodic password changes. See Changing Volume Passwords.

To increase or shrink the size of a volume:

- Run the SDWEXPAN.EXE wizard utility using the Resize SafeHouse Volume menu shortcut.

You may increase or shrink the size of your volume(s) at any time. The maximum size of a volume is the lesser of available hard drive space and the expansion limit set by you when the volume was created. See Resizing Volumes.

To view or change a volume's properties:

- Run the SDWSHOW.EXE wizard utility using the Show Volume Properties menu shortcut.

You view or change a variety of properties related to your volumes, such as the minimum password length, as often as desired.

To monitor volumes and system activity:

- Run the SDWMON32.EXE wizard utility using the SafeHouse Volume Monitor menu shortcut.

You may have SafeHouse monitor your keyboard, mouse and hard drive activity, including power management sleep modes, in order to block access to mapped volumes when you are not actively using your PC.

To change the ActivCard service keys associated with a volume:

- Run the SDWACTIV.EXE wizard utility using the Change SafeHouse ActivCards menu shortcut.

You may change the ActivCard service keys associated with your volume(s) at any time. Each volume can hold up to five keys, thereby allowing five different people to authenticate themselves and gain access to the files. See Changing ActivCard Keys.

ActivCards are handheld security devices which can be used to provide an extra degree of protection by requiring users to have possession of the ActivCard in order to authenticate themselves to SafeHouse. ActivCards are sold separately.

SDW.HLP

This help file.

ReadMe.txt

The README.TXT file contains late-breaking news about SafeHouse.

SafeHouse.pdf

This is the printable manual in Adobe Acrobat PDF format.

Creating SafeHouse Encrypted Volumes

The SafeHouse encryption utilities require that the files and data to be protected reside in a separate space on your hard drive. This is accomplished by creating large files on your standard hard drive to act as file containers, otherwise known as virtual volumes. All files deposited into one of these containers are automatically encrypted and protected from unauthorized access.

The SafeHouse device driver is designed to make these large files look just like another hard drive attached to your system; hence the term virtual volume. Using this method, you can easily create, read, write and modify data files within any of these protected containers/volumes using the very same tools, utilities and applications you are already using on a daily basis. All you do is store your confidential information to the new Windows drive letter reserved for use by SafeHouse. The rest is automatic.

One of the greatest benefits of the virtual volume concept used by SafeHouse is that access can easily be granted or denied on a full volume basis. You need be authenticated only once to access any file contained within the volume. Authentication takes place at the time you map (associate) the volume to one of the new SafeHouse drive letters. Once mapped, a volume remains accessible until you either explicitly unmap or shut down your PC.

Before using an encrypted volume you must create it. This is accomplished from Windows using the SDWCREAT.EXE program. Simply double-click on the icon titled Create SafeHouse Volume and fill in the blanks.

Encrypted Volumes

SafeHouse encrypted volumes can reside in any directory of your local hard drive. In addition to local volumes, SafeHouse volumes may reside on removable media (diskettes, ZIP disks) and network servers. The default action taken by SafeHouse is to create volumes in your root directory using a .SDSK file extension.

Volume sizes can range from just a few kilobytes (KB) all the way up to 2048 gigabytes (GB) on NT/2000/XP, or 4GB on Win9x/Me, or the maximum available space on your hard drive. You'll be asked to choose an initial size for your volumes when they are first created. Afterwards, you can increase or shrink their sizes as often as desired using a supplied utility. 4GB+ volumes require that your operating system support the FAT32 hard drive format or that you manually reformat the volumes to NTFS after being created. Platforms supporting FAT32 include Windows 98, 98se, Me, 2000 and XP. Early editions of Windows 95 do not include FAT32 support, nor does NT4. Volumes larger than 4GB on 2000/XP, or 2GB on NT, require that host drives be formatted using NTFS (NT/2000/XP), and additionally, that if on NT4, that you manually reformat volumes to NTFS after being created. The wizard used to create new volumes keeps track of all these special cases and will only present you with choices which are compatible with your operating environment.

There is no limit to the number of different SafeHouse encrypted volumes allowed to be stored on a given hard drive. You are limited only to the number of volumes able to be mapped to drive letters at the same time.

Encrypted volumes can be created using a variety of protection mechanisms; the most obvious, of course, being encryption. All SafeHouse volumes are encrypted to a password. Each time you create a new volume, you'll be asked to choose a password and select from one of the available encryption methods.

You must choose an encryption algorithm to be used with each new volume. This algorithm cannot be changed for the life of the volume; however, you always have the opportunity of creating new volumes with different algorithms and copying files between them. If you are not familiar with the differences between the choices of algorithms, and you are not working under any federal guidelines requiring a specific choice, we recommend that you choose 128-bit Twofish. This algorithm is extremely fast, very secure, and is compatible with all SafeHouse features - including administrative password recovery. The DES algorithm which was popular a few years back has fallen out of favor in many circles due to its slow speed and vulnerability to attack by modern high-speed processors.

The next level of protection offered by SafeHouse is to configure your volumes to require ActivCard authentication. Each volume can hold up to five ActivCard service keys; thereby allowing five separate individuals to authenticate themselves to the system and gain access to the protected volume. Service keys are very large 64-bit secret serial numbers which are used to individually identify specific ActivCards. These numbers are so large, in fact, that it would take today's fastest supercomputers many years to guess at all the combinations. Keeping these keys secret makes it nearly impossible for anyone to duplicate your ActivCard. Further, since ActivCard keys cannot be viewed or tampered, you can temporarily allow a friend to use your card and be assured they they will be unable to make a duplicate while it's in their possession.

Tip

- Optimize your host hard drive (normally C:) after creating large SafeHouse volumes. This will make the volume file contiguous, thereby allowing faster access.

Note

- The SafeHouse software can be configured to operate without an ActivCard by choosing not to require ActivCard authentication when creating encrypted volumes.

Examples:

Creating encrypted volumes using the Windows create volume wizard is by far the easiest way to get started using SafeHouse. Although several command-line options are supported, none are required for normal use. Just run the SDWCREAT.EXE utility from your program manager or Windows Start menu and answer the questions. The icon for this utility is usually titled Create SafeHouse Volume.

```
SDWCREAT
SDWCREAT /create="c:\myvolume.sdsk" /description ="This is my volume" /size=500
SDWCREAT /create=c:\myvolume.sdsk /password="my_password" /activcard="1234 1234 1234 1234"
```

Mapping and UnMapping Volumes

Once a SafeHouse encrypted volume is created, it must be associated with a Windows drive letter before it can be accessed. This is accomplished using SDWMAP32.EXE which can be run by double-clicking the icon titled Map SafeHouse Volume. If you haven't yet created a SafeHouse volume, see Creating SafeHouse Encrypted Volumes.

When done using an encrypted volume it should be unmapped using these same utilities, but with a slightly different set of options. From your Windows desktop, you can simply double-click on UnMap SafeHouse Volume.

Mapping and UnMapping a Volume

When mapping and unmapping volumes, you can specify as little or as much on the command line as you desire. The map and unmap dialogs will prompt for any missing parameters. Using /GO and /SILENT on the command line will suppress the Windows dialog boxes altogether assuming you have provided enough parameters on the command line for the program to carry out the desired action.

If you don't specify any parameters on the command line, SDWMAP32.EXE will first ask you to choose to map or unmap. To help you bypass this first prompt and go directly to the desired dialog window, the SafeHouse setup program automatically installs two icons for SDWMAP32.EXE; one for mapping, the other for unmapping, specifying /MAP and /UNMAP, respectively, as the only parameters. This will allow you to go directly to the desired dialog window.

Tips

- Drag the Map icon into your Windows Start-Up group to map volumes automatically each time you run Windows.
- Use /EXPLORE on the SDWMAP32 command line to automatically open up an Explorer shell window for each mapped volume.

Examples:

```
SDWMAP32
SDWMAP32 /map /sound=off
SDWMAP32 /map="c:\volume.sdsk" /drive=d /password="my_password" /go
SDWMAP32 /unmap
SDWMAP32 /unmap=d /go /silent
SDWMAP32 /unmap=all
```

View/Change Volume Properties

Use the Show Volume Properties wizard to view or change the properties of your volumes. A limited amount of information will be displayed until you authenticate yourself by pressing the Open button and providing your password. The Open Using Backdoor button allows administrators to gain access to this wizard by using their administrative password for authentication. Administrators will not usually users' private passwords since these passwords should not be disclosed and should be changed often. This button will be enabled only for volumes that have been configured for administrative recovery.

Example:

```
SDWSHOW
```

Resizing Volumes

When you create a SafeHouse encrypted volume, you are required to choose an initial size. The size you specify is pre-allocated on your hard drive at that time. You are also asked to indicate the maximum size that you anticipate the volume will need to be expanded to during its life. The expansion limit determines how the internal structure of the volume will be arranged. The trade-off you should be aware of is that volumes with small expansion limits will allocate space for files more efficiently. This is similar to file efficiency issues you may already be aware of for normal hard drives.

Once a volume is created, you can increase or shrink its size as often as desired using the SDWEXPAN.EXE utility. This program is run from your Windows Start menu by double-clicking the icon titled Resize SafeHouse Volume.

Changing Volume Size

You can specify as little or as much on the command line as you desire. The expand volume wizard will prompt for any missing parameters. Using /GO and /SILENT on the command line will suppress the Windows wizard dialog pages altogether assuming you have provided enough parameters on the command line for the program carry out the desired action.

Example:

```
SDWEXPAN
```

Changing Volume Passwords

To change the password for an encrypted volume from Windows, run the utility by double-clicking the icon titled Change SafeHouse Password.

You can change passwords as often as desired.

Every encrypted volume must have a password. By default, you are not required to change a volume's password during its life. However, it is recommended that you change passwords every 30 days or so. This will make it harder for intruders to steal your password.

To help you remember when it's time to change passwords, the create encrypted volume wizard allows you to specify the maximum number of days between password changes. You can also specify a grace period whereby volume mappings will still be allowed even though you may not have chosen a new password yet. Once a password has expired, along with any corresponding grace period, you will not be allowed to map the volume for use until you first change its password.

Examples:

```
SDWCHANG

SDWCHANG /change="c:\myvolume.sdsk"

SDWCHANG /change=c:\myvolume.sdsk /password="my_old_pass" /newpassword="my_new_pass"
```

The Windows utility for mapping encrypted volumes includes a button on its main dialog for changing passwords. Choosing this button executes the SDWCHANG.EXE wizard.

Changing ActivCard Keys for a Volume

SafeHouse encrypted volumes may optionally be configured to require ActivCard authentication. Each volume can store up to five ActivCard service keys, thereby allowing five different people access to the volume's files, each using their own ActivCard. Volumes set up for ActivCard authentication will still require users to enter the encryption password.

The easiest to time add ActivCard authentication to an encrypted volume is when the volume is created using Create SafeHouse Volume from Windows. One of the wizard pages presented by this utility has fields for entering up to five ActivCard service keys.

Once a volume is created, you may modify its ActivCard authentication configuration at any time by running SDWACTIV.EXE from Windows. You can accomplish this by double-clicking the icon titled Change SafeHouse ActivCards.

To remove the ActivCard authentication requirement for an encrypted volume, run the Change SafeHouse ActivCards wizard and clear (set to blank) all five service key fields. From then on, mapping that volume will only require a password.

Example:

```
SDWACTIV
```

Command Syntax for the SafeHouse Utilities

Listed below are the Windows programs used for accessing encrypted volumes:

- SDWCREAT.EXE Utility to create encrypted volumes.
- SDWCHANG.EXE Utility to change encrypted volume passwords
- SDWMAP32.EXE Utility to map and unmap encrypted volumes to Windows drive letters.
- SDWEXPAN.EXE Utility to change the size of encrypted volumes.
- SDWACTIV.EXE Utility to change the ActivCard service keys for volumes.
- SDWMON32.EXE Utility to set volume shutdown and timeout parameters.
- SDWSHOW.EXE Utility to view or change a volume's properties.

Command Line Options

Listed below is the complete set of command-line parameters for working with encrypted volumes. Not all parameters are valid for all commands. Command parameters are not case sensitive.

All parameters which require a boolean state value such as ON or OFF will also accept 1, 0, Y, N, Yes, No, True or False.

Parameters requiring embedded spaces must be enclosed in double quotes. This includes long filenames, passwords and descriptions.

Upper case letters are used below to indicate the minimum number of characters required for the option to be recognized amongst all utilities.

- /Activcard
- /AUTOExpand
- /AUTOSHrink
- /AUTOSIzenotify
- /Changekeys
- /Changepassword
- /Create
- /Description
- /Drive
- /Encryption
- /EXPANdableto
- /Expandvolume
- /EXPIres
- /EXPLORE
- /FILESYSTEM
- /FINISH
- /FORCE
- /GO
- /GRace
- /Hidden
- /Map
- /MAxpassword
- /MInpassword
- /Newpassword
- /Password
- /Quickcreate
- /Quickexpand
- /READONLY
- /REMovable
- /SHELL
- /SHORTCUT
- /SILENT

- /Size
- /SOUND
- /STOP
- /Unmap
- /USEPASSWORDDLL

Missing Passwords

In most cases, all SafeHouse utilities which require passwords to be specified will prompt the user to enter any passwords not supplied on the command line. However, if /SILENT is specified and password(s) are missing, execution will terminate in error.

CONFIG.INI Parameters

Each of the SDWxxxx Windows utility programs included with SafeHouse will check for the existence of a file named CONFIG.INI in the same directory as the utility is run from. If this file is found, the utility will look for a [section] which has the same name as the utility and retrieve initial values for any specified paramters. For example, SDWCREAT.EXE will look for the section named [SDWCREAT]. Parameters specified on the command line override CONFIG.INI settings. Individual parameters have names identical to their command-line equivalents without the leading slash.

Example CONFIG.INI file:

```
[SDWMAP32]
        map=c:\mydisk.sdsk
[SDWCREAT]
        description=Confidential Files
        expandableto=128
        quickcreate=1
[SDWEXPAN]
[SDWACTIV]
```

Note:

- All CONFIG.INI parameters must follow the name=value standard INI file format. Example: GO=1.

Exporting Cryptographic Software

U.S. exporters can export and reexport all encryption items, except cryptanalytic products and their related technology, immediately to the 15 EU member states and Austra-lia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland and Switzerland without a license (i.e., under a license exception). Exports to worldwide offices of firms, organizations and governments headquartered in these nations and Canada are also permitted. U.S. exporters can ship their products under this new policy immedi-ately after submitting a commodity classification request to BXA, rather than waiting for the review and classification to be completed.

Many changes have recently taken place with regard to exporting cryptographic software outside of the United States. Please visit PC Dynamics' web site at http://www.pcdynamics.com/safehouse for up-to-date information and rules for exporting SafeHouse.

40-Bit Encryption

PC Dynamics offers a 40-bit version of SafeHouse which has been approved by the Bureau of Export Administration for general worldwide distribution with very few restrictions.

Troubleshooting

If you have problems using SafeHouse, please check here for answers before calling for technical support. Also, be sure to check our Internet web site for news announcements and product updates.

Problem: Explorer windows keep popping up.

We sometimes receive reports of Explorer windows popping up when mapping volumes even when the /explore feature was not selected; and in some cases, two windows when the /explore feature is selected. This is due to Windows detecting a new fixed drive coming online and trying to be extra helpful by showing you its contents in a window. Since Windows is popping up one Explorer window automatically, you may wish to remove the /explore option from the map shortcut to prevent SafeHouse from additionally showing an Explorer window. Alternatively, starting with SafeHouse v2.10, a /removable command line option is supported for mapping which forces SafeHouse volumes to appear as removable media instead of fixed drives. Windows does not automatically display Explorer windows for new removable media volumes. The only down side to this is that you lose the recycle bin inside the SafeHouse volume. Also, see the next topic.

Problem: A simple trick to always map volumes as removable media.

The simplest way to prevent Windows from popping up Explorer windows when you map volumes is to always map using the /removable option (starting with v2.10). This can be done by placing a file named *config.ini* in your SafeHouse program directory containing the two lines shown below. This file is available for download in the support section of the SafeHouse web site.

```
[SDWMAP32]
removable=1
```

Problem: SafeHouse fails to run after upgrading to Windows 2000 or XP.

If you installed SafeHouse on a PC running Windows 95/98/Me and then subsequently upgrade your system to Windows 2000 or XP, SafeHouse will fail to load its device driver. The reason for this is that a different driver is needed for 2000/XP. The solution is to run the SafeHouse setup program again. The required changes will be made automatically and SafeHouse will run fine after you restart your system. You do not need to uninstall and no changes will be made to your encrypted volumes during this procedure. Please note that you must use SafeHouse v2.10 or later on XP.

Problem: SafeHouse runs very slow after upgrading to Windows Me.

Microsoft introduced a new feature into Me called System File Protection which interferes with how SafeHouse interacts with encrypted volumes. Starting with SafeHouse version 2.00, SafeHouse switched to using .SDSK instead of .DSK as its standard volume file extension in order to circumvent this problem. Please make sure your volumes all use the new .SDSK extension. file

Problem: Cannot map a volume residing on a Novell file server.

SafeHouse supports mapping volumes on most network file servers. This feature is compatible with Novell servers when using the Novell Netware network provider de-signed by Microsoft and included with Windows. However, if you instead use the Netware network provider created by Novell, you will not be able to map SafeHouse volumes residing on your Netware file servers due to a known problem with this driver. This is not a bug in SafeHouse and is unfortunately out of our control.

Problem: How do I create a volume using NTFS on Windows NT or 2000?

SafeHouse volumes appear to Windows NT and Windows 2000 as normal SCSI hard drives. This allows you to use the standard Windows FORMAT.EXE program to refor-mat the volume to any desired format supported by your version of Windows. Please note that once you reformat a volume to a format that is not natively supported by SafeHouse, it can no longer be resized.

Problem: How do I use SafeHouse with CD ROMs?

SafeHouse volumes may be placed on CD ROMs and other read-only media and mapped directly to a Windows drive letter with needing to be copied to your hard drive. If the volume file is not already marked read-only, you must check the Read Only checkbox when using the mapping utility, or alternatively, specify the /READONLY option on the SDWMAP32.EXE command line.

Problem: I upgraded from the Shareware version to the full-strength retail version, yet my volume still uses the old weak encryption method.

SafeHouse does not automatically change the encryption method used on a volume when you upgrade to newer or stronger versions of the software. This is for your protection since any unexpected system failure would cause irreparable damage to your volumes. The solution is to create a new volume using the desired algorithm and size and then use a simple drag and drop operation to copy the files from the old volume to the new one. You will need to map both volumes at the same time to accomplish this. Once you are satisfied the transfer was successful, you may delete the old volume.

Problem: How can volumes be used by multiple users at the same time on a local area network?

Normally, SafeHouse places an exclusive file lock on a mapped volume to ensure its integrity. This is important because of the way Windows performs file system caching. SafeHouse may not, under any circumstances, allow two people to have write access to a volume at the same time. To have a volume be simultaneously accessible to more than one network user, all users must map the volume for read-only access. This is most-easily accomplished using the /READONLY command line option for the SDWMAP32.EXE utility. Once a volume is mapped in read-only mode by any network user, no other user will be allowed to map the volume for writing. A common practice used in this kind of environment is to have two copies of each public SafeHouse

volume; one is the master and updatable only by the administrator, and the other is a re-cent copy of the master and is used for public read-only access over the network.

Problem: Can SafeHouse volumes be copied to new hard drives?

SafeHouse volumes are not associated with a specific machine or hard drive. You may copy a volume at any time to a new drive, ZIP disk, network server or CD ROM.

Problem: How do I find out my password?

PC Dynamics cannot help you recover lost passwords. If we could, the product would not be secure. If you've lost your password, the only way to recover is to use the prod-uct's administrative password recovery feature - which must have been implemented in advance of creating the volume you are unable to access.

Problem: Can SafeHouse volumes be backed up?

SafeHouse encrypted volumes may be safely backed up to other drives or tape. To do this in a way that remains secure, you must unmap the volume and back up the large volume file. This is the only way your data will be stored in an encrypted format. If instead, you map your volume and instruct your backup utility to back up the Windows drive letter used by the volume, then the saved files will not be encrypted.

Problem: Can SafeHouse support other third-party authentication devices.

SafeHouse has been designed to allow quick integration of third-party authentication devices such as smart cards, fingerprint readers and access tokens. If you have a need to have SafeHouse utilize one of these devices, please contact PC Dynamics to discuss your requirements.

Problem: Your ActivCard is lost or stolen.

Your SafeHouse encrypted volumes are usually associated with an ActivCard. If this card is ever lost or stolen, you will not be able to access your data. You will need to purchase a new ActivCard and have somebody preprogram it with the same service key(s) used by your original card.

Removing SafeHouse

If you find it necessary to remove SafeHouse from your PC, the most important thing to consider is your data. What are you going to do with the files stored within encrypted volumes? Without the SafeHouse drivers, you will no longer be able to map your encrypted volumes to a drive letter.

Please follow the steps below to automatically remove SafeHouse from your PC.

Step 1.

Copy all important files and data contained within SafeHouse encrypted volumes to a normal unencrypted hard drive.

Step 2.

Run the REMOVE.EXE clean-up wizard. From Windows, this wizard is accessible via the control panel's Install/Remove Programs applet. Otherwise, locate the program in your SafeHouse directory and invoke it using your program manager (double click icon). Follow the wizard's on-screen instructions.

How to Contact PC Dynamics, Inc.

Please contact PC Dynamics, Inc. using the address and phone numbers listed below.

PC Dynamics, Incorporated
31332 Via Colinas, Suite 102
Westlake Village, CA 91362 USA

Phone: (818)889-1741 (Business office)
Phone: (818)889-1741 (Technical support)
Fax: (818)889-1014

Web site: http://www.pcdynamics.com

Email: support@pcdynamics.com or sales@pcdynamics.com

Installing the Device Driver

When using SafeHouse under Windows 95, 98, Me, NT, 2000 or XP, the setup program automatically installs and configures the device driver.

Windows 95/98/Me

The SafeHouse setup program will automatically detect Windows 95/98/Me and install the appropriate device driver used to access your encrypted volumes. This driver is named SAFDSK95.VXD and is usually located in your primary SafeHouse directory. No special steps are needed to load this driver since SDWMAP32.EXE loads the driver into memory whenever it is needed. Unlike NT, it is not necessary to reboot your PC after running setup to begin using the Windows 95/98/Me driver.

Windows NT 4.0, 2000 and XP

The SafeHouse setup program will automatically detect Windows NT 4.0, 2000 and XP, and install a driver named SAFDSKNT.SYS into your C:\WINNT\SYSTEM32\DRIVERS directory. Your system registry will also be updated to reference this new driver. You must reboot your PC after running setup to begin using this driver.

Monitoring System Activity

The SafeHouse Volume Monitor is an optional utility which may be used to quietly monitor your disk, keyboard and mouse activity to identify times when access to your currently-mapped volumes should be temporarily disabled. This feature functions very much like a password-protected screen saver; except that instead of blocking access to your screen, it blocks access to your sensitive files. Once access to your volumes is disabled, a password will be required to regain their use. In addition to monitoring user activity, this utility is also able to detect Advanced Power Management (APM) sleep modes and, then too, block access to mapped volumes until a password is provided. This feature is extremely important for laptop users who get into the habbit of putting their computers into a suspended state by closing the lid. The notion of being able to have your computer "always on" is certainly appealing. The SafeHouse volume monitor allows you to have your "always on" and stay secure at the same time. If you choose to enable either the activity monitor or the Advanced Power Management sleep mode monitor, this wizard will run silently in the background each time you start Windows.

The SDWMON32.EXE program is used to perform the monitoring.

Example:

```
SDWMON32
```

Create Volume Wizard

The SDWCTREAT.EXE create encrypted volume wizard will step you through the process of creating an SafeHouse encrypted volume. You will be asked few simple questions such as the filename and description for the volume, it's size and initial password.

SafeHouse volumes must reside on a local hard drive, removable media drive or network server.. By default, volumes are created on the root directory of your first hard drive. Alternatively, you may specify a hard drive subdirectory, network share, floppy, ZIP or MO drive. CDRW drives are also usually supported.

Supported sizes for SafeHouse volumes range from 2KB to 2048GB, depending upon your system configuration. You will only be shown choices for sizes and formats that are compatible with your operating environment. Space is allocated on your hard drive for the full volume size specified when volumes are created. Since the size of volumes can always be increased at a later time, you may want to be conservative in estimating the initial size of your volumes.

The maximum size for SafeHouse volumes on your PC is determined by the version of Windows you are using and the format of the host (typically C:) hard drive where the volumes will reside. On Windows 9x/Me, the maximum size for a single volume is 4GB. This is due to a limitation of the FAT32 disk format. Early versions of Windows 95 as well as NT4 do not support the FAT32 hard drive format and therefore have volume sizes limited to 2GB. Windows NT/2000/XP support the NTFS disk format which allows for much larger files. When hosting on NTFS, the maximum size of a volume is 2048GB. Further, since NT4 does not support the FAT32 format, volumes greater than 2GB created on an NT4 NTFS drive must be manually formatted to NTFS after being created. This step is not necessary on 2000/XP since FAT32 is supported. As confusing as all this sounds, don't worry, you will only be allowed to choose options which are compatible with your current PC configuration.

Once a volume is created, you must "map" it to a Windows drive letter before being allowed access to its contents. This is done using the Map SafeHouse Volume icon.

This wizard utility supports a variety of command line parameters should you find it desirable to automate the volume creation process.

See also:

SDWCREAT.EXE

Creating SafeHouse Encrypted Volumes

Volume Description and Location

Location

This is the hard drive (or floppy) directory where your volume will be created. By default, encrypted volumes are usually created in the root directory of your first hard drive. Volumes may be created on network servers, diskettes, ZIP media and CDRW media.

SafeHouse does support volumes located on standard CD ROMS and CDR media; however, you cannot create volumes directly on CD ROM media. What you should do in this case is create the volume on a local hard drive, map it and populate it with files, and then use the utility which came with your CDR drive to transfer the volume file to the CDR. Please note that mapping a volume which resides on a CDR or other read-only media requires that the Windows file attribute for the volume be set to read only, or that the /READONLY command line parameter be specified on the SDWMAP32.EXE command line; or alternatively, that you check the Read Only checkbox when mapping. If the /READONLY option is not specified, SafeHouse will evaluate the Read Only Windows file attribute for the volume to determine if the volume should be opened in read-only mode.

Filename

This is the Windows filename for your encrypted volume. Volume files always have .SDSK for their extension.

It is not important to choose a filename that's easy to remember since all SafeHouse utilities present the volume's description within their wizard pages instead of the filename.

Description

Type in a short description identifying this volume. The text you provide here is saved inside the volume file and later presented in dialogs and wizards used throughout this product. This field is required.

Volume Size and Attributes

Volume Size

Choose the initial volume size in Kilobytes (KB), Megabytes (MB) or Gigabytes (GB).

The maximum size for SafeHouse volumes on your PC is determined by the version of Windows you are using and the format of the host (typically C:) hard drive where the volumes will reside. On Windows 9x/Me, the maximum size for a single volume is 4GB. This is due to a limitation of the FAT32 disk format. Early versions of Windows 95 as well as NT4 do not support the FAT32 hard drive format and therefore have volume sizes limited to 2GB. Windows NT/2000/XP support the NTFS disk format which allows for much larger files. When hosting on NTFS, the maximum size of a volume is 2048GB. Further, since NT4 does not support the FAT32 format, volumes greater than 2GB created on an NT4 NTFS drive must be manually formatted to NTFS after being created. This step is not necessary on 2000/XP since FAT32 is supported. As confusing as all this sounds, don't worry, you will only be allowed to choose options which are compatible with your current PC configuration.

There is a mathematical correlation between the initial volume size and the maximum volume size. For example, you will notice that a 1MB volume cannot be expanded to 1GB. Such is due to limitations imposed by Windows. This wizard will only allow you to specify valid combinations of initial and maximum sizes. The Next button will only be active for valid combinations.

Resizable

Every volume must have an initial size. As the volume becomes full, you may increase the size using one of the other supplied wizards. Volumes may range in size from 2 Kilobytes (KB) to 4 Gigabytes (GB), or even as high as 2048GB on Windows 2000/XP when your host drive is formatted using NTFS. You should choose a size that is appropriate for the amount of data you wish to protect. Sizes between 10 and 50 Megabytes (MB) are very common. Something to consider when selecting a size is whether you plan to use a single large volume, or multiple smaller volumes. You will also notice that the maximum expansion limit for a volume is somewhat related to the initial size you choose. If you want the volume to be expandable, you should set the size range first and then set the initial Volume Size to fall within the indicated limits. If you're wondering why the minimum and maximum sizes shown for each size range seem to be rather odd values, it's because of how Windows performs certain calculations when it comes to figuring out the internal drive format.

One of the selections in the Resizable drop-down list is Not expandable. If you are abso-lutely sure you'll never need to expand the volume, selecting this option will allow your volume file to be slightly smaller since SafeHouse will not need to allocate certain internal drive structures which are otherwise required to plan ahead for expansion.

Please note that volumes which are manually formatted to use the NTFS disk format may not subsequently be resized. If you plan to use NTFS, you should create your volume at the exact size needed since that will be the size for the life of the volume.

File System

The File System drop-down list specifies the internal hard drive format to be used for your volume. The default choice is Automatic which indicates that SafeHouse should choose the most appropriate setting based upon your chosen volume size and limits. If you are not familiar with the differences between file system formats, we strongly recommend that you leave this set to Automatic and let SafeHouse figure out what's best. Specific File System choices include FAT12, FAT16, FAT32 and None, however, not all choices are available in all situations or on all operating platforms. You will be pre-sented only with choices which are compatible with your version of Windows and the size of volume currently selected. FAT32 is available only for volumes over 250MB. Early versions of Windows 95 and NT do not support FAT32 and should use FAT16 instead; which has a maximum size of 2GB. The maximum for FAT32 is 4GB under Windows 98/Me and 2048GB when using Windows 2000/XP on host drives formatted using NTFS. FAT12 is used primarily for small volumes residing on diskettes. If you specify None, then the volume will not be formatted and will require manual formatting using your standard Windows disk utilities prior to being used to store data. This is sometimes useful when you wish to use an alternative disk format such as NTFS which is not natively supported by this wizard. Volumes created using None cannot be subsequently resized since SafeHouse will not know which file system you are using.

Preinitialize Volume with Random Data

The Preinitialize Volume with Random Data checkbox is used to specify that SafeHouse should write a pattern of random data throughout the entire volume and check the volume for hard disk errors. This step is strongly recommended. The extra time needed to perform this process is about the same time as needed for Windows to perform a file copy of a normal file having the same size as your volume. Writing random data to volumes makes it extremely difficult for intruders to differentiate between the portions of the volume containing encrypted data and the portions that are still unused.

Hide Volume File

Check this box to make the encrypted volume file invisible to normal Windows Explorer listings. This is accomplished by setting the "hidden" attribute for the volume file. Please note that several popular file management utilities (including Windows Explorer) routinely ignore the hidden file attribute and display hidden files in their directory listings. Unfortunately, this is out of our control.

Space Available

Shows the maximum available volume size which may be created on the selected host drive.

Encryption Method

Please specify the encryption method to be used to encrypt (cipher) the data contained within your volume.Once a volume is created, its encryption method cannot be changed. If you ever decide that you need to change the encryption method for a volume, your only choice is to create a new volume (with the desired algorithm) large enough to hold your data and copy the files between them.

About Algorithms and Key Lengths

One issue that is sometimes confusing is that of key strengths and lengths. How many bits? How strong? What does it all mean? For a 128-bit key size, there are approximately 340,000,000,000,000,000,000,000,000,000,000,000,000 (340 followed by 36 zeros) possible keys.

- 3.4 x 1038 possible 128-bit keys;
- 6.2 x 1057 possible 192-bit keys; and
- 1.1 x 1077 possible 256-bit keys.

In comparison, DES keys are 56 bits long, which means there are approximately 7.2 x 1016 possible DES keys. Thus, there are on the order of 10 to the 21st power times more 128-bit keys than DES 56-bit keys. 40-bit keys are considered extremely weak and are able to be cracked within a few days using off-the-shelf computing technology.

Some algorithms, such as Rijndael, take longer to process as their key strengths increase. Others, such as Blowfish and Twofish, do not. Some algorithms are mandated to be used by regulatory agencies in certain environments, while others may be subject to export restrictions. Choosing an algorithm isn't always cut and dry; but fortunately, if you stick with at least 128 bits of key strength, you can't go wrong no matter which you choose. At 128 bits, they are all going to offer you a level of protection that meets even the most-demanding security requirements.

BLOWFISH

The Blowfish algorithm has been around for about a decade. It is highly respected, secure and very fast. SafeHouse offers this algorithm in several key strengths to meet various export and product feature requirements. The Blofwish encryption speed is the same for all key strengths. We generally recommend either 128- or 448-bit strengths. 448 bits offers the strongest protection, however, it is not compatible with SafeHouse's administrative password recovery feature which requires 128 bits or less. Please note that 128 bits is very strong. In fact, the number of possible keys is so large (with 36 trailing zeros) that this strength should be strong enough for almost any non-military application.

TWOFISH

The Twofish algorithm is fairly new. It was invented by the same scientist that created Blowfish and is supposedly faster and harder to break. This cipher was a finalist in the U.S. Government's contest to seek out a successor to DES for the new federal standard. Here again, it is offered in multiple key strengths to meet various commercial requirements. Only the 128-bit strength is compatible with SafeHouse's administrative password recovery feature.

RIJNDAEL (AES)

The Rijndael algorithm (pronounced Rine-Dahl) was selected by NIST in October, 2000, as the new Advanced Encryption Standard (AES) which is destined to replace the use of DES within the federal government. Rijndael is fast and secure. It is offered by SafeHouse in two key strengths: 128 and 256 bits. Unlike Blowfish, Rijndael takes longer to process at higher key strengths. The 256-bit version takes approximately 40% longer to encrypt than the 128-bit version. Only the 128-bit version is compatible with SafeHouse's administrative key recovery feature. As with Blowfish, 128-bits of key length using Rijndael encryption offers more security than anyone would likely ever need. And further, being the new AES, this algorithm comes highly recommended.

DES

DES stands for Data Encryption Standard. This algorithm has been around for over 20 years and has withstood the test of time; however, current thinking is that the algorithm has become vulnerable to attack due to its small key length as compared to newer ciphers. Also, this algorithm has been broken several times in recent years by chaining hundreds of PCs together over the Internet and leveraging their combined processing power. Use DES when you are required by some federal or institutional guideline to use it. Otherwise, you should consider one of the other algorithms such as Blowfish, Twofish or AES. Although the DES cipher is not known for being one of the fastest methods available, this specific implementation is written in highly-optimized assembly language to provide the highest achievable data throughput rate available on a PC.

Some demonstration or international versions of SafeHouse may not include this method due to U.S. export controls.

DES/40

This is a version of the DES algorithm which has been shortened to use only 40 bits of key data instead of the usual 56. The speed of DES and DES/40 are identical. This is extremely weak encryption. Its availability in the product is mostly for export and demonstration purposes.

FAST

The FAST algorithm is a proprietary method developed by PC Dynamics. This algorithm is extremely fast and efficient and well suited for protecting information that is generally private, yet not top secret. The FAST technique is so fast, in fact, that you will hardly notice any speed degradation. The encryption method used will guard your data against disk scanning utilities and most anyone you will generally come into contact with; however, it won't pose much of a hurdle for the sophisticated hacking

techniques used by professional cryptographers. Use FAST when you want the absolute minimum performance loss and only need to stop intruders armed with standard debuggers and disk editing utilities. The need for this algorithm has diminished significantly over time since PCs are now hundreds of times faster than they were a decade ago when this algorithm was originally developed. If you have a fast Pentium PC, you might be better off using a more-secure algorithm such as Blowfish.

TRIPLE-DES

The triple DES algorithm is essentially a hybrid that uses the DES cipher three times in a row; each time using a different portion of the key. Its original purpose was to increase the key strength of DES to 128 bits or more prior to some of the newer algorithms becoming widely available. The primary drawback of this algorithm is that it is three-times slower than DES -- and DES is ten times slower than some of the others. This algorithm should generally be used only when there is a requirement to do so.

Automatic Expansion and Compaction

If you choose to allow your volume to be resizable, a companion wizard page will follow which will ask if you'd like for the volume to be expanded or shrunk automatically each time you map based on specified thresholds. The Notify before changing size checkbox allows you to be prompted before SafeHouse makes any changes at map time.

The Maximum Percent Full field is used to determine when volumes need to be expanded. When your volume starts to become full, SafeHouse will try to increase its size such that the used portion of the volume represents no more than the specified percentage. Of course, the ability to increase the size of a volume is dependent upon the amount of space remaining on your hard drive and the maximum size limt chosen on the previous wizard page.

The Minimum Percent Full field determines when a volume should be automatically shrunk. The new volume size will be calculated to maintain approximately the selected minimum amount of free space inside the volume. For example, if the threshold is set to 10 percent, the volume size will be reduced if less than 10-percent of the volume is filled up. It will be reduced to approximately 10 times the amount of used space, so that the volume is about 10-percent full. The volume will never be reduced below the size set when the volume was created or last manually resized. The auto-shrink feature is useful only to automatically reduce the size of a volume which was previously automatically expanded. Please know that volumes may be reduced to sizes smaller than that at which they were initially created (within their established limits); however, this must be done manually using the Resize SafeHouse Volume wizard.

Access Control Method

Specifies the authentication method(s) required to gain access to this encrypted volume.

Password Only

You will be required to provide the correct password each time this volume is used. Passwords are from 1 to 255 characters and can be forced to expire on regular intervals. You will be asked to choose your initial password on a subsequent wizard page. Choosing Password Only is the usual choice for a software-only encryption solution.

Password AND ActivCard

You will be required to provide the correct password and complete an ActivCard authentication before being granted access to this volume. This two-step process provides for an extremely high degree of security since you must "know" the password and "have possession" of the ActivCard to gain entry.

An ActivCard is a handheld hardware security device (sold separately by ActivCard, Inc.) which if required, must participate in the process of mapping a volume. The security benefit is that the user must have personal possession of the device in order to gain access to the SafeHouse volume, thereby providing increased security over passwords alone which are subject to compromise. The ActivCard support integrated into SafeHouse conforms to the X.9 industry standard for such devices and can therefore work with other X.9 compatible devices from competing manufacturers such as CryptoCard and Enigma.

You will be allowed to specify the service keys for up to 5 ActivCards on a subsequent wizard page if you choose this option. Afterwards, you may edit (add, delete, modify) the service key values at any time using the Change SafeHouse ActivCards utility. By supporting up to 5 keys, SafeHouse volumes can be accessed by up to five individuals, each having separately-programmed ActivCards, but each also having knowledge of the single SafeHouse volume password.

Volume Password

Each SafeHouse encrypted volume requires a password. Usually, passwords are between 1 and 255 characters long. Spaces allowed. but not generally recommended since they are often confusing. If your company security policy requires a different password length specification, adjust the minimum and maximum password length fields to meet your requirements. All future passwords chosen for this volume will be required to fall within the min and max ranges set here.

Additionally, you may choose to force password changes for this volume after a specified number of days. Once a password expires, the volume will not be able to be mapped again until the password has been changed. An exception to this would be if you allow a grace period during which time the volume can still be mapped after displaying a message regarding the expired password.

For sensitive data, a good rule of thumb is to change your password once a month.

Note regarding ActivCard

- In case you may wonder why you must specify a password here even when the volume will require ActivCard authentication, the reason is because the password is used to encrypt the ActivCard service keys associated with this volume This is necessary since the PC does not provide a secure place to keep secret keys. Left unencrypted, hackers could easily change your keys using a simple disk editor. Key encryption using a password is not generally required in a client-server environment.

ActivCard Service Keys

SafeHouse encrypted volumes are uniquely designed to support the ActivCard challenge-response X.9 security authentication token. By specifying the 16-digit service keys for one or more ActivCards, each time anyone attempts to map this volume to a drive letter they will be required to authenticate themselves using one of the corresponding ActivCards. There is room to enter the keys for up to five cards.

ActivCard service keys are 16-digit values which are typically represented as four four-digit groups. You may input the key values with or without the space between each group.

We strongly recommend that you test the key values you input here by pressing the Test button to the right of each key field you fill in. This will simulate an actual challenge-response authentication for the corresponding ActivCard.

After a volume is created, you may edit (add, delete, modify) the ActivCard service keys associated with the volume at any time using the Change SafeHouse ActivCards Windows utility.

ActivCards are purchased separately from ActivCard, Inc. (visit http://www.activcard.com).

Final Step

This is the final screen. Press the Create Volume button to create the encrypted volume using the attributes displayed on this page. If anything needs changing, now is the time go back and fix it.

You will see a progress meter as your volume is being created. Afterwards, press Finish to exit.

The Finish button will not become active until after you create the volume. To exit without creating the volume, select Cancel.

Mapping and UnMapping

Encrypted volumes must be mapped to a Windows driver letter in order to be made accessible for use. Complete the dialog by filling in the required fields, then select the Map Volume button. This button will become active only when all required information is provided.

This mapping utility supports a variety of command-line parameters which may be helpful in automating common tasks. See SDWMAP32.EXE for details.

Tip

- Consider placing an icon or shortcut for this utility into your Windows Start-up group so that you will be prompted to input your SafeHouse password each time you start your PC.

Map to Drive

Select the SafeHouse Windows drive letter to be associated (mapped) with this volume. You will only be allowed to choose from drive letters that are already reserved for use by SafeHouse. Once mapped, all access to the volume will be through this drive letter. SafeHouse mappings are automatically canceled when you turn off your PC. To cancel a mapping manually, use the UnMap Volume icon.

Read Only

Check this box if you plan to map a volume for read-only access. This serves two purposes. First, for read-only media such as CD ROMs or write-protected ZIP disks, etc., this is required to prevent SafeHouse from attempting to write timestamp information back to the volume being mapped. Second, when attempting to share volumes on a local area network, checking this box will prevent SafeHouse from placing an exclusive file lock on the mapped volume. This is important because in the normal case where an exclusive lock is placed on mapped volumes, no other users will be allowed to map the volume at the same time, for reading or writing.

Location

This is the directory that contains the volume you wish to map. SafeHouse will list all volumes (files with SDSK extensions) contained in this directory in the drop-down list. The button to the right allows you to browse your hard drive. Most people place all their volumes in the same directory, or in the root of their primary drive, so this field rarely needs to be changed.

Please note that mapping a volume which resides on CDRs or other read-only media requires that the /READONLY command line parameter be specified on the SDWMAP32.EXE command line or that you check the Read Only checkbox when mapping. If the /READONLY option is not specified, SafeHouse will evaluate the Read Only Windows file attribute for the volume to determine if the volume should be opened in read-only mode.

Volume

Select the volume to map from the drop-down list. This list shows all SafeHouse volumes located in the directory listed above.

Password

Enter the current password for the selected volume. You may change this password by selecting the Change Password button.

Create Shortcut

Use this button to have SafeHouse create a shortcut on your desktop that has preset parameters matching those currently showing on this wizard page. The primary advantage of doing this is that by having all the parameters except the password specified in advance, SafeHouse will display a simplified dialog prompting only for the password.

NOTE: Preventing popup windows

If you are experiencing undesirable Explorer popup windows after mapping, try removing the /explore command line option from your mapping shortcut and/or using the /removable mapping option.

Some versions of Windows automatically attempt to display Explorer windows for new fixed drives similar to what SafeHouse does when the /explore option is specified. This is why removing the /explore option or using the /removable option to make the volume appear as removable media instead of as a fixed disk drive can help in this situation.

See also:

SDWMAP32.EXE

Mapping and UnMapping Volumes

Change Volume Password

Fill in the required fields and select the Change Password button. This button will not become active unless all fields are filled in properly.

You may change passwords as often as desired. Passwords are usually between 3 and 16 characters long. Spaces are not allowed. Some encrypted volumes may have had other password length limits established at the time they were created.

Location

This is the directory that contains the volume you wish to work with. SafeHouse will list all volumes (files with SDSK extensions) contained in this directory in the drop-down list. The button to the right allows you to browse your hard drive. Most people place all their volumes in the same directory, or in the root of their primary drive, so this field rarely needs to be changed.

Volume

Select the volume for which you intend to change its password from the drop-down list. This list shows all SafeHouse volumes located in the directory listed above.

Old Password

Enter the current password for this volume.

New Password

Enter the new password to be used from now on for this volume.

Confirm

Retype the new password to ensure it has been entered correctly.

See also:

SDWCHANG.EXE

Changing Volume Passwords

Resize Volume Wizard

This utility is used to increase or decrease the size of an existing encrypted volume.

On this first wizard page you must choose the target volume and be authenticated. Fill in the required fields, then select Next to display the page which allows you to choose a new size. The maximum size available to you will be the maximum expandable size selected when the volume was created; provided you have at least that amount of remaining space on your hard drive.

Location

This is the directory that contains the volume you wish work with. SafeHouse will list all volumes (files with SDSK extensions) contained in this directory in the drop-down list. The button to the right allows you to browse your hard drive. Most people place all their volumes in the same directory, or in the root of their primary drive, so this field rarely needs to be changed.

Volume

Select the volume needing to be resized from the drop-down list. This list shows all SafeHouse volumes located in the directory listed above.

Password

Enter the current password for the selected volume.

See also:

SDWEXPAN.EXE

Resizing SafeHouse Volumes

Resize Volume

Fill in the required fields and select the Next button. The Finish button will become active only after you have completed this step.

Maximum Size

Displays the maximum size which may be chosen for the encrypted volume. This is the size selected as the maximum size when the volume was created. This field is not editable.

Minimum Size

Displays the minimum size which may be chosen for the encrypted volume. This size is computed to conform to the math used internally by Windows for working with hard drives.

Current Size

Displays the existing size of the encrypted volume. This field is not editable.

New Size

Choose the new volume size in Kilobytes (KB) or Megabytes (MB). For example, if the new size should be 20 Megabytes, you may specify either 20 MB or 20000 KB.

Preinitialize with Random Data

The Preinitialize with Random Data checkbox is used to specify that SafeHouse should write a pattern of random data throughout the entire newly allocated area and check the volume for hard disk errors. This step is strongly recommended. The extra time needed to perform this process is about the same time as needed for Windows to perform a file copy of a normal file having the same size as your volume. Writing random data to volumes makes it extremely difficult for intruders to differentiate between the portions of the volume containing encrypted data and the portions that are still unused.

Note:

- If you are finding that you cannot get the Next button to go live, the likely problem is that you may be entering a size value that is slightly over the limit. This can happen when you are rounding to MB or GB. The solution is to input the maximum value exactly as shown in the dialog; possibly in KB. From the computers's perspective, it is not allowing you to input something like 4 GB when only 3.9999 GB is allowed; hence, the problem, and why inputting a value in KB can get you right up to the limit.

See also:

SDWEXPAN.EXE

Resizing SafeHouse Volumes

Final Step

Please confirm your choices and press the Expand (or Shrink) button to perform the expand/shrink operation.

See also:

SDWEXPAN.EXE
Resizing SafeHouse Volumes

Change ActivCard Keys for Volume

This utility is used to change (add, edit, delete) the ActivCard service keys associated with an encrypted volume.

SafeHouse encrypted volumes are uniquely designed to support the ActivCard challenge-response security authentication token. By specifying the 16-digit service keys for one or more ActivCards, each time anyone attempts to map this volume to a drive letter they will be required to authenticate themselves using one of the corresponding ActivCards. There is room to enter the keys for up to five cards.

On this first wizard page you must choose the target volume and be authenticated. Fill in the required fields, then select Next to display the page which allows you to edit the service keys.

Location

This is the directory that contains the volume you wish to work with. SafeHouse will list all volumes (files with SDSK extensions) contained in this directory in the drop-down list. The button to the right allows you to browse your hard drive. Most people place all their volumes in the same directory, or in the root of their primary drive, so this field rarely needs to be changed.

Volume

Select the volume needing to be changed from the drop-down list. This list shows all SafeHouse volumes located in the directory listed above.

Password

Enter the current password for the selected volume.

See also:

SDWACTIV.EXE

Changing ActivCard Keys

Specify ActivCard Keys

SafeHouse encrypted volumes are uniquely designed to support the ActivCard challenge-response security authentication token. By specifying the 16-digit service keys for one or more ActivCards, each time anyone attempts to map this volume to a drive letter they will be required to authenticate themselves using one of the corresponding ActivCards. There is room to enter the keys for up to five cards.

ActivCard service keys are 16-digit values which are typically represented as four four-digit groups. You may input the key values with or without the space between each group.

We strongly recommend that you test the key values you input here by pressing the Test button to the right of each key field you fill in. This will simulate an actual challenge-response authentication for the corresponding ActivCard.

ActivCards are optional handheld hardware security devices which may be purchased separately from ActivCard, Inc.

See also:

SDWACTIV.EXE

Changing ActivCard Keys

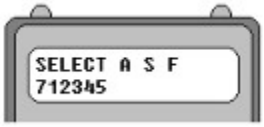
ActivCard Challenge

To complete the login, you must turn on your ActivCard, key in the challenge to generate the appropriate response, and finally, type the response (dynamic password) back into the dialog.

Turn on your ActivCard using the **ON/CE** key.

Enter your private PIN code and press **ENTER**.

Select the ActivCard Service Name for this authentication. The first name displayed is SafeHouse (drive encryption software bundled with ActivCard). To select any of the others, press the **Down Arrow** key several times until the desired service name appears on the display. Press **ENTER** to select the displayed service.

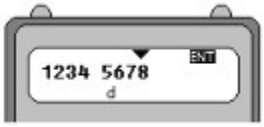


After selecting a service, the display will look as shown above. The **A S F** stands for authentication, secret and function; corresponding to keys on the ActivCard keypad. The number below is sometimes used for your login account user ID when such use is desirable for some specific service provider. Unless instructed otherwise, you can disregard this number. It is provided only for convenience and serves no essential purpose.
Press the **AUTH** key for authentication.

Type the challenge presented in the dialog and press **ENTER**.

Tips

- At this point you can have your ActivCard read the challenge right off the screen using its optical sensors. Hold the card up to the screen (touching) at a right angle, aligning the blue bumpers on the card with the blue dots on the screen. Hold for a single transmit cycle, then remove the card. This might take a little practice. The key is to hold the card up to the screen, or remove it, only during the still cycle when the blue dots are showing. Watch the timing. It's easy to get the hang of it. When the optical transmission is complete, the card will automatically display the response as shown below.
- The dialog provides two sizes for the optical patterns. Choose the size that fits the best. It is not necessary to have an exact size match. What's important is that you center the ActivCard up against the pattern. The software will remember your current size preference.
- If you don't get a good transmission, press **[ON/CE]** to clear, then **[AUTH]**, and try again.
- Optical challenge transmission may not work on LCD or some notebook computer screens.



The ActivCard then displays your one-time dynamic password as an eight-digit value. This is the number that must type into the dialog's Response field to complete your login. Enter the number exactly as shown. The letter 'd' under the password simply indicates that the password is comprised of decimal numbers 0 to 9.
Press the OK button on the dialog to finish.

See also:

SDWACTIV.EXE

Changing ActivCard Keys

View/Change Volume Properties

This utility shows the properties for a specific SafeHouse volume.

The volume's description and password properties may be changed if you know the current password and can authenticate yourself.

Location

This is the directory that contains the volume you wish to work with. SafeHouse will list all volumes (files with SDSK extensions) contained in this directory in the drop-down list. The button to the right allows you to browse your hard drive. Most people place all their volumes in the same directory, or in the root of their primary drive, so this field rarely needs to be changed.

Volume

Select the volume for which you wish to see its properties from the drop-down list. This list shows all SafeHouse volumes located in the directory listed above.

Open Button

Once you've selected the target volume, press Open to display an authentication dialog and enter the volume's password. If you enter the correct password the volume's extended properties will be listed in the scrolling window.

Change Settings Button

This button will become enabled only after you have authenticated yourself using the Open button. Click Change Settings to modify any of the volumes properties which are allowed to be changed after first being created. This generally includes its description and password authentication criteria.

Remote Administrative Volume Recovery

This utility allows SafeHouse administrators to remotely recover SafeHouse encrypted volume data when passwords are lost, forgotten or otherwise unavailable. This method of recovery is a secure alternative to the local recovery procedure.

The local volume recovery procedure which is built into the change password dialogs is the simplest and most convenient method for recovering a lost password. The problem, however, is that this method requires that the administrator have local access to the encrypted volume. Although convenient, this method cannot be used to help a stranded user over the telephone without divulging the administrator's passphrase.

The secure solution for remote recovery requires the SDWULOCK.EXE utility. This utility is needed only by the administrator. Everything the user needs is contained within their change password utility.

Initiating a Remote Recovery on the User's PC

Local and remote recovery is initiated on the user's machine by executing the Change Volume Password wizard and displaying its System Menu. The System menu is displayed by left-clicking on the small icon located at the far left of the caption bar. Located on the System Menu is an item named Backdoor. Once the Backdoor dialog is displayed, click the Remote Recovery button to display the special dialog which is the counterpart to this SDWULOCK.EXE utility.

Support personnel charged with helping users recover from lost passwords will need to talk their users through this process.

Using SDWULOCK on the Administrator's PC

The SDWULOCK.EXE program displays a single dialog window for the administrator. The first field contains a multi-line edit control which is where the administrator types in their secret passphrase. This is the same passphrase that was used when the SafeHouse files were branded using the SDWBRAND.EXE program. It is extremely important that the passphrase be entered exactly as it was entered during the branding process.

The second field provides a place to enter the challenge sequence generated by the encrypted volume's change password program. The administrator must instruct the remote user on how to obtain these numbers and either have the user read the numbers over the phone, or save them to a file via the clipboard and email them. The challenge sequence numbers do not need to be kept private. The remote user must not close their dialog window once their challenge sequence numbers are generated because these numbers will only work once. If the window is closed and then redisplayed, new sequence numbers will be generated.

Once the passphrase and challenge sequence numbers are entered, pressing the Response button will compute the recovery response values which must be conveyed back to the user and entered into their recovery dialog.

The challenge sequence numbers and response values which are exchanged between the remote user and administrator contain check digits to ensure their accuracy. If either the remote user or administrator enters an invalid number sequence an appropriate error message will be displayed.

Assuming this process completes correctly, the remote user will be asked to choose a new password and confirm it.

SafeHouse Volume Monitor

his utility is used to establish when mapped encrypted volumes should be automatically disabled. Its primary purpose is to help out in situations such as advanced power management sleep modes whereby PCs and laptops can be put into a suspended state without requires users to log off. This creates a security problem because the PC could be stolen while in the hybernated state and subsequently awakened by the thief. Without this type of safety monitor in place, SafeHouse volumes that were mapped just prior to entering sleep mode would remain mapped and be available to be browsed by the thief.

Once this volume monitor decides it's time to lock down your mapped volumes, the volumes will only become accessible again once you enter their passwords. It's important to note that a locked volume is different from an unmapped volume. Volumes that are locked remain mapped, yet inaccessible. This allows running Windows applications (word processors, etc.) to have open files during the lockdown period, and yet these files remain protected. Turning power off to a PC in the locked state forces an automatic unmapping of any mapped volumes.

You may choose to have volumes locked automatically either during any power management standby mode, or after some specified period of mouse, keyboard and drive inactivity.

The shortcut installed by setup is SafeHouse Volume Monitor.

This program usually attaches itself to the registry RUN= section to load into memory each time Windows is started. It will transparently watch drive, keyboard and mouse activity and disable access to your mapped volumes if the idle thresholds have been exceeded.

Turning the power to your PC off always unmaps volumes even when this utility is not used.

See also:

SDWMON32.EXE

Branding SafeHouse

The SDWBRAND.EXE branding utility is used by SafeHouse administrators to mark a set of SafeHouse program files with special messages and numeric codes prior to general deployment throughout your company. This wizard will prompt for several pieces of information and then modify several of the files contained in your SafeHouse working directory.

Although this utility is only needed by administrators, it does not present a security breach for end users to have it. The SafeHouse User's Manual describes methods for deploying branded filesets.

The branding wizard will ask you to supply the following information:

Contact Information

Since your company may have multiple administrators or administrative domains, it is important to provide complete administrative contact information for all encrypted volumes. This information is embedded into the volume's file header and can be displayed by users using a variety of utilities.

Create Volume Message

It is usually important for users to know that when they are creating SafeHouse encrypted volumes that the volumes are recoverable. For this reason, the branding utility allows you to provide a short text message which is displayed on the first page of the create volume wizard. This message is optional and can be any text of your choosing. A typical message might mention that the volume is recoverable and the name of the administrator. For example, *This volume will be recoverable by contacting John Smith*.

Administrator's Passphrase

The administrator must choose a secret passphrase. A passphrase is simply a long password which may contain letters, numbers, punctuation and spaces. The maximum length of a passphrase is 999 characters. The passphrase will be required each time a volume recovery procedure is initiated. End users must never learn this passphrase. Passphrases are most easily remembered when they are in the form of a sentence. For example: *The sun rises in the morning and sets at night.*

ActivCard Keys

For highly-sensitive environments, you may optionally require that all volume recoveries include an ActivCard challenge-response authentication. If this is desirable, you may enter in the service keys for up to five ActivCard security tokens authorized to authenticate the recovery procedure. When ActivCards are employed, volume password recovery can only be accomplished with knowledge of the administrator's passphrase and possession of a corresponding ActivCard.

More information about each of these topics is available by choosing Help on their respective wizard pages.

Contact Information

Please enter administrative contact information such as names, phone numbers or email addresses. Although filling in this field is optional, we strongly recommend that you at least provide enough information so that users with lost passwords will know who to contact.

A typical example is shown below:

> *For lost passwords, please contact:*
>
> *John Smith*
> *Computer Support*
> *(818)555-1212*

The text message you supply here will be embedded in all SafeHouse encrypted volumes created with your branded utilities. The message can be displayed by users by invoking the Backdoor option on their change password dialogs, or by displaying volume property information using the SDWSHOW.EXE utility.

Message for Create SafeHouse Volume Wizard

You may optionally enter a short message to be displayed on the first page of the Create SafeHouse Volume wizard. This message can contain any arbitrary information you wish to convey to your users before they create a SafeHouse volume.

A typical message is shown below:

> *Volumes created with this utility are the property*
> *of ABC Corporation. Passwords are recoverable.*

Administrator Passphrase

Please choose an administrator's password. We call it a passphrase only to emphasize that this field is not constrained to simple passwords. We suggest you enter your passphrase in the form of a normal sentence, complete with the usual capitalization and punctuation. The maximum length is 999 characters. The passphrase you enter here will be required each time you attempt to recover lost passwords for encrypted volumes.

It is extremely important that you keep this passphrase secret and that you remember exactly how you typed it.

Example passphrase:

The sun rises in the east and sets in the west.

The value you enter for your passphrase will be processed using a popular cryptographic formula known as MD5 to help form your administrator's public key. Longer passwords, or passphrases, are harder for hackers to guess.

Specify ActivCard Keys - Optional

You may optionally require that any administrative access to SafeHouse encrypted volumes first be authenticated using an ActivCard challenge-response security token. If you do not desire this added security, leave these fields blank. The primary benefit of using ActivCards is to protect against undesirable acts or espionage from disgruntled administrators or support personnel.

You may enter the service keys for up to five ActivCards on this page. We strongly recommend that you test each service key using its respective Test button.

When ActivCard authentication is required, all administrative access to encrypted volumes will require that the administrator know the administrator's passphrase and have physical possession of a corresponding ActivCard.

Final Step

This is the last page of the branding wizard. If you are satisfied with your responses on the previous pages, click on the branding button to perform the corresponding file updates.

When done, select Finish to exit the wizard.

/SOUND [=ON | OFF]

Enables or disables playing of sounds upon command completion. Separate sounds files (WAV) are played for each supporting utility; one for success, another for failure. Sound files are expected to reside in the same directory as their respective utility programs. Sound is ON by default. When /Sound is specified without additional parameters, such is the same as turning it on.

Your computer must have a Windows-compatible sound board installed to hear sounds. Several example sounds are installed automatically by setup.

- SDWCS.WAV Played by SDWCREAT.EXE after successfully creating a volume.
- SDWCF.WAV Played by SDWCREAT.EXE after failing to create a volume.
- SDWMS.WAV Played by SDWMAP32.EXE after successfully mapping a volume.
- SDWMF.WAV Played by SDWMAP32.EXE after failing to map a volume.
- SDWUS.WAV Played by SDWMAP32.EXE after successfully unmapping a volume.
- SDWUF.WAV Played by SDWMAP32.EXE after failing to unmap a volume.
- SDWHS.WAV Played by SDWCHANG.EXE after successfully changing a password.
- SDWHF.WAV Played by SDWCHANG.EXE after failing to change a password.
- SDWAS.WAV Played by SDWACTIV.EXE after successfully changing ActivCard keys.
- SDWAF.WAV Played by SDWACTIV.EXE after failing to change ActivCard keys.
- SDWES.WAV Played by SDWEXPAN.EXE after successfully expanding a volume.
- SDWEF.WAV Played by SDWEXPAN.EXE after failing to expand a volume.

Examples:

```
/Sound=ON
/Sound=OFF
/Sound=Yes
/Sound=1
/Sound=0
/sound=no
/Sound
```

Utilities Supporting this option:

- SDWACTIV.EXE
- SDWCHANG.EXE
- SDWCREAT.EXE
- SDWEXPAN.EXE
- SDWMAP32.EXE

/Finish

Causes the utility to bypass the display of any standard completion messages. This option is frequently combined with /GO and /SILENT to run invisibly and unattended in the background.

Utilities supporting this option:

- SDWCREAT.EXE
- SDWEXPAN.EXE

/CReate=d:\filename.ext

Allows the name of the file to be created to be specified in advance on the command line or from within a Windows shortcut. This parameter is optional.

The target filename must be a fully-qualified filepath beginning with a driver letter. By convention, encrypted volumes always use the .SDSK extension.

Examples:

```
/Create="c:\test.sdsk"
/Cr=c:\mydrive.sdsk /description="My new volume"
/Cr=c:\activsaf.sdsk /size=100MB
```

Utilities supporting this option:

- SDWCREAT.EXE

/DEscription="My Volume Description"

Allows you to specify the long internal name or description of an encrypted volume in advance on the command line. The quotations are required.

Examples:

```
/Description="This is a volume description"
/DE="MyDescription"
```

Utilities supporting this option:

- SDWCREAT.EXE

/SIze=NNN [MB]

This parameter allows you to specify the size of a volume to be created. By default, NNN is a decimal number of Kilobytes. Including MB after the number changes the value to Megabytes.

This parameter is optional.

The maximum supported volume size is 4 Gigabytes (4,000MB) on Win9x/Me, or 2048GB on NT/2000/XP, or the size of your hard disk, whichever is smaller.

Examples:

```
/Size=100            - 100 Kilobytes
/Size=100MB          - 100 Megabytes
/Si=1000MB           - 1 Gigabyte
```

Utilities Supporting this option:

- SDWCREAT.EXE

/Password = "mypassword"

Allows the password to be specified in advance on the command line. This parameter is optional. It is generally not desirable to place passwords into Windows icons and shortcuts since such would allow easy access for intruders.

Passwords may include letters, numbers and punctuation symbols. Spaces are allowed. Quotation marks are required.

All encrypted volume wizards and utilities are designed to prompt for missing passwords. The primary reason for making this parameter available as a command line switch was to allow for process automation in corporate environments.

Examples:

```
/Password="12345"
/P="birds.nest"
/pass="apple_boat"
```

Utilities supporting this option:

- SDWACTIVE.EXE
- SDWCHANG.EXE
- SDWCREAT.EXE
- SDWEXPAN.EXE
- SDWMAP32.EXE

SDWCREAT.EXE

The SDWCREAT.EXE Windows utility is used to create SafeHouse encrypted volumes. This program is implemented as a wizard to help step you through the various input parameters required to complete the process. The icon used to invoke this wizard is usually titled Create SafeHouse Volume. See Creating SafeHouse Encrypted Volumes for a full explanation of encrypted volumes.

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

Optional command line parameters:

The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /ActivCard
- /Autoexpand
- /Autoshrink
- /Autosizenotify
- /Create
- /Description
- /Encryption
- /Expandableto
- /Expires
- /Filesystem
- /Finish
- /Go
- /Grace
- /Hidden
- /Maxpassword
- /Minpassword
- /Password
- /Quickcreate
- /Silent
- /Size
- /Sound

See also:

Creating SafeHouse Encrypted Volumes

SDWMAP32.EXE

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

The setup program automatically creates two Windows icons for this utililty; one for mapping, the other for unmapping. These icons are named Map SafeHouse Volume and UnMap SafeHouse Volume.

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

Having Problems with Explorer Windows?

If you find that you are getting undesirable Explorer windows popping up after mapping SafeHouse volumes, first try removing the /explore option from your mapping shortcuts. This typically solves the problem when you get two windows and you only want one. Another approach is to use the /removable option which will make the volume appear as removable media. Windows does not automatically display Explorer windows for removable media.

Optional command line parameters:

The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /Drive
- /Explore
- /Map
- /Password
- /Silent
- /Sound
- /Unmap
- /Force
- /Removable

See also:

Mapping and UnMapping SafeHouse Volumes

SDWCHANG.EXE

This utility is used to change the authentication password for an existing SafeHouse encrypted volume.

The Windows icon setup by default for this utility is Change SafeHouse Password.

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

Optional command line parameters:

The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /Changepassword
- /Go
- /Newpassword
- /Password
- /Silent
- /Sound

See also:

Changing Volume Passwords

SDWEXPAN.EXE

This utility is used to resize an encrypted volume.

The setup program automatically creates a Windows icon for this utility named Resize SafeHouse Volume.

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

Optional command line parameters:

The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /Expandvolume
- /Finish
- /Go
- /Password
- /Quickexpand
- /Silent
- /Size
- /Sound

See also:

Resizing SafeHouse Volumes

SDWACTIV.EXE

This utility is used to add, delete or edit ActivCard service keys for an encrypted volume.

The setup program automatically creates a Windows icon for this utility named Change SafeHouse ActivCards.

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

Optional command line parameters:

The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /Activcard
- /Changekeys
- /Go
- /Password
- /Silent
- /Sound

See also:

Changing ActivCard Keys

SDWSHOW.EXE

Show properties for a volume and optionally allow changes. Allows volume description and password properties to be changed if you know the current password for the volume. The menu shortcut for this utility is named Show Volume Properties.

No command line parameters supported.

See also:

View/Change Volume Properties

SDWMON32.EXE

This windows utility is used to establish settings and parameters for disabling access to mapped encrypted volumes. For example, a volume could be disabled if it wasn't accessed for 20 minutes. This program is for Windows 95 and NT only. The setup program automatically creates a Windows icon for this utility named SafeHouse Volume Monitor.

To set volume shutdown parameters, run the Volume Monitor and indicate your preferences in the main dialog. These preferences will remain in place until you change them. If your settings require real-time monitoring each time Windows starts, this program will automatically include itself in the RUN= registry key so that it will be run transparently in the background each time Windows is started.

This utility supports a variety of command-line options which allow you to specify some or all input fields in advance. Information supplied on the command line will be stuffed into the wizard input fields before being presented to the user.

The /STOP option is used to force the monitor to remove itself from memory. This is sometimes useful for scripted administration and maintenance.

Optional command line parameters:

The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /Stop

See also:

Monitoring System Activity

/ENcryption= {code}

Specifies the encryption method for the volume being created in advance on the command line. By default, encryption is set to 2F128 (BF32 in shareware and international versions of product). This parameter is optional.

The codes for the supported algorithms are listed in parenthesis in the descriptions below. Additional encryption methods may be added to future software releases.

DES (DES and DES40)

DES stands for Data Encryption Standard, which is one of the strongest encryption algorithms available today. This algorithm has been around for over 20 years and has withstood the test of time. Although the DES cipher is not known for being one of the fastest methods available, this specific implementation is written in highly-optimized assembly language to provide the highest achievable data throughput rate available on a PC.

DES40 is a 40-bit version of DES. The standard DES key length is 56 bits. This DES40 algorithm has the key shortened to 40 bits to allow it to be exported outside the United States. DES40 runs at the same speed as normal 56-bit DES.

FAST (FAST)

The FAST algorithm is a proprietary method developed by PC Dynamics. This algorithm is extremely fast and efficient and well suited for protecting information that is generally private, yet not top secret. The FAST technique is so fast that you will hardly notice any speed degradation. The encryption method used will guard your data against disk scanning utilities and most anyone you will generally come into contact with; however, it won't pose much of a hurdle for the sophisticated hacking techniques used by professional cryptographers. Use FAST when you want the absolute minimum performance loss and only need to stop intruders armed with standard debuggers and disk editing utilities. This algorithm is included in SafeHouse mostly to remain compatible with legacy applications. We strongly recommend using TWOFISH or one of the other newer algorithms instead of FAST now that the processing power of PCs has greatly improved.

BLOWFISH (BF32 BF48 BF128 BF448)

Blowfish is significantly faster than DES and supports much larger key lengths. All key lengths (32, 48, 128 and 448) operate at the same speed. The primary reason multiple key lengths are offered in the product is for export control. The 448-bit version is not compatible with SafeHouse's key recovery feature. Blowfish is an excellent alorithm at 128 or 448 bits; however, you might find that Twofish is a bit faster.

Triple DES (TDES128 and TDES168)

Triple DES is essentially three rounds of standard 56-bit DES encryption. Each round uses a different permutation of your password. The 128-bit version is not as strong as the 168-bit version; however, the 128-bit code is fully compatible with SafeHouse's key recovery features, while the 168-bit code is not. Triple DES takes three times longer to encrypt than standard DES. This method is strong, but slow. Only the 128-bit version is compatible with SafeHouse's administrative key recovery feature.

TWOFISH (2F128 and TF256)

Twofish is very fast, secure and well-respected in the industry. This algorithm was a finalist in the NIST Advanced Encryption Standard competition.

RIJNDAEL (RJ128 and RJ256)

The Rijndael algorithm has been selected by NIST to become the new Advanced Encryption Standard (AES) and replace DES as the predominant algorithm used within the U.S. Government.

Examples:

```
/Encryption=DES
/en=des40
/encrypt=fast
/en=FAST
```

Utilities supporting this option:

- SDWCREAT.EXE

/EXPLORE

Specifies that the Windows shell Explorer program should be launched automatically after a volume is mapped.

Using this option, Explorer shows the window corresponding to the root of the mapped drive.

This command option is included by the default setup configuration. If you prefer not to have Explorer launch the drive window, remove this option from your SafeHouse volume mapping shortcuts.

It is important to note that some newer versions of Windows automatically attempt to detect when new fixed disk drives are mapped and subsequently display corresponding Explorer windows. This feature of Windows competes with this /explore option and you might see two windows instead of one. The solution is to not use the /explore option. Alternatively, you can use the /removable option to make your volumes appear to Windows as removable media. Since Windows does not automatically display Explorer windows for removable drives, the displaying of the drive windows will be dependent upon whether or not you use the /explore option.

Examples:

```
/explore
```

Utilities supporting this option:

- SDWMAP32.EXE

/FILESYSTEM = [AUTO | FAT12 | FAT16 | FAT32 | NONE]

Specifies the internal hard drive format to use for an encrypted volume. Default is AUTO.

Examples:

```
/Filesystem=AUTO
/Filesystem=FAT32
```

Utilities supporting this option:

- SDWCREAT.EXE

/Hidden

Specifies that the encrypted volume being created should be marked as hidden to the Windows file system. Using this option prevents the file from being seen in normal Windows directory listings.

Please note that some popular Windows file managers routinely display hidden files. Unfortunately, this is out of our control.

Examples:

```
/Hidden
/H
```

Utilities supporting this option:

- SDWCREAT.EXE

/SHELL

Specifies that the utility is being run from the Explorer shell right-click menu. This option informs the program that it should adjust its behavior and messages to account for being run from the context menu. Normal Windows shortcuts should not use this option.

Examples:

```
/shell
```

Utilities supporting this option:

- SDWACTIV.EXE
- SDWCREAT.EXE
- SDWEXPAN.EXE
- SDWMAP32.EXE
- SDWSHOW.EXE

/Quickcreate = [Yes | No]

Specifies that the encrypted volume about to be created does not need to have its entire contents zeroed out during the volume creation process. Normally it is a good idea to allow the create volume utility to zero out the data areas for newly created volumes; however, if you don't have time to wait, using this option will keep the create time down to just a few seconds.

Examples:

```
/Quickcreate=YES
/Q=Y
/q
/q=no
```

Utilities supporting this option:

- SDWCREAT.EXE

/Autoexpand = NN

Specifies the percentage full above which the encrypted volume will automatically be expanded the next time the volume is mapped. The default is 0, meaning that autoexpansion is not desired. For example, if you specify 75 as the parameter value, then each time the volume is mapped, the mapping utility will attempt to ensure that the volume remains 25% empty. Volume size increases only occur during the mapping process.

Examples:

```
/Autoexpand=50
/Autoexp=90
```

Utilities supporting this option:

- SDWCREAT.EXE

/Autoshrink = NN

Specifies when a volume should be automatically shrunk. The new volume size will be calculated to maintain approximately the selected minimum amount of free space in-side the volume. For example, if the threshold is set to 10 percent, the volume size will be reduced if less than 10-percent of the volume is filled up. It will be reduced to approximately 10 times the amount of used space, so that the volume is about 10-percent full. The volume will never be reduced below the size set when the volume was created or last manually resized. The auto-shrink feature is useful only to automatically reduce the size of a volume which was previously automatically expanded.

Examples:

```
/Autoshrink=50
/Autoshrink=90
```

Utilities supporting this option:

- SDWCREAT.EXE

/AUTOSIzenotify = [ON | OFF]

This option is used in conjunction with /AUTOEXPAND to specify if the user should be notified each time SafeHouse determines that it should automatically expand a volume. The default is OFF.

Examples:

```
/Autosizenotify=on
/Autosizenotify=1
```

Utilities supporting this option:

- SDWCREAT.EXE

/USEPASSWORDDLL

Specifies that the current volume password should be obtained by calling a special DLL instead of prompting with a dialog box. The DLL must conform to the SafeHouse password pass-through API. This feature is intended to assist in the deployment and maintenance of SafeHouse. Please contact PC Dynamics for further information and sample DLL source code (available to qualified site license clients only).

When creating volumes, the password provided by the DLL will be the new password for the volume.

Windows will expect to find the password DLL named SAFPWD32.DLL in the same SafeHouse directory containing the map or create volume utility.

Examples:

```
/usepassworddll
```

Utilities supporting this option:

- SDWCREAT.EXE
- SDWMAP32.EXE

/READONLY

Specifies that a volume is being mapped in read-only mode. The mapping utility will not attempt to update the volume's file header with the timestamp for this access, nor will it allow any disk write operations to take place on the volume drive data.

Examples:

```
/readonly
```

Utilities supporting this option:

- SDWMAP32.EXE

/Expires = NNN

Specifies that the password for the encrypted volume is to expire every NNN days. Valid values are from 1 to 999 days. For example, a volume with this option set to 1 would require that the password be changed the first time it is mapped each day. A setting of 30 would require password changes once a month.

Once a password has expired, users will be required to change the password before being allowed to map the respective volume to a drive letter. The only exception to this rule is when a grace period is allowed. See /GRACE option.

Examples:

```
/Expires=30
/E=90
/e=5
```

Utilities supporting this option:

- SDWCREAT.EXE

/STOP

Specifies that the volume monitor program should terminate and remove itself from memory. This option is intended for use by administrative deployment and maintenance scripts.

Examples:

```
/stop
```

Utilities supporting this option:

- SDWMON32.EXE
- SDWTRAY.EXE

/Grace = NNN

Specifies the number of days after a password expires during which users will still be allowed to access encrypted volumes without first selecting a new password. This option is only meaningful when password expirations are enforced. Valid values are from 1 to 999 days.

In the absence of a grace period, volumes with expired passwords will be inaccessible until the passwords are changed.

Examples:

```
/Grace=10
/G=5
/g=30
```

Utilities supporting this option:

- SDWCREAT.EXE

/Expandableto = NNN

This option is used to specify the expansion limit in megabytes of the volume being created. Values are automatically rounded up to the next power of 2 (100 becomes 128). Specifying 0 prevents the volume from being expanded in the future.

The default value is the same size as the create size rounded up to the next power of 2. For example, a 70 MB volume by default would be expandable to 128MB. A 60 MB volume could be expanded to 64 MB.

Examples:

```
/Expand=100
```

```
/expandableto=500
```

Utilities supporting this option:

- SDWCREAT.EXE

/Quickexpand = [ON | OFF]

This option allows you to specify that the new disk space added to a volume file should not be zeroed during the expansion process.

The default is OFF, meaning that all new space added to the volume will be preset to zeros.

Examples:

```
/Quick=on
/quickexpand=1
/q=true
```

Utilities supporting this option:

- SDWCREAT.EXE

/Expandvolume = filepath

This parameter to the expand volume utility is used to specify the volume file to expand in advance on the command line. The volume filename must be a fully-qualified filepath starting with a drive letter.

Examples:

```
/Expandvolume="c:\myfile.sdsk"
/e=c:\myfile.sdsk
```

Utilities supporting this option:

- SDWEXPAN.EXE

/Changekeys = d:\filename.ext

This parameter is used to specify the volume filename in advance on the command line when modifying the ActivCard keys associated with an encrypted volume.

The volume filename specified must be a fully-qualified filepath starting with a drive letter.

Examples:

```
/changekeys="c:\myfile.sdsk"
```

```
/c=c:\myfile.sdsk
```

Utilities supporting this option:

- SDWACTIV.EXE

/SHORTCUT = [ON | OFF]

The option allows you to specify that when creating a volume a corresponding desktop shortcut should be created. The default is ON.

Examples:

```
/shortcut=yes
/shortcut=off
```

Utilities supporting this option:

- SDWCREAT.EXE

/MInpassword = NN

Specifies the minimum length for volume passwords. The default value is 1. Valid numbers range between 1 and 255. See also /MAXPASSWORD.

Examples:

```
/MI=8
/minpassword=5
```

Utilities supporting this option:

- SDWCREAT.EXE

/MAxpassword = NN

Specifies the maximum length for volume passwords. The default value is 255. Valid numbers range from 1 to 255. See also /MINPASSWORD.

Examples:

```
/MA=8
/maxpass=10
/maxpassword=12
```

Utilities supporting this option:

- SDWCREAT.EXE

/Activcard ="1234 1234 1234 1234"

Specifies that the encrypted volume being created will require ActivCard authentication before access is granted. The service key for the ActivCard must be provided either as a 16-digit hex number without quotes or spaces, or as a quoted string with spaces allowed.

The Windows create volume utility allows up to 5 ActivCards to be associated with a volume. Use of this command line option allows only the first key to be set. Keys 2 through 5 may be set only using the Change SafeHouse ActivCards wizard.

Examples:

```
/A=1234123412341234
/ActivCard="1234 ABCD 4567 ABCD"
/a="abcd 1234 abcd 1234"
```

Utilities supporting this option:

- SDWACTIV.EXE
- SDWCREAT.EXE

/Map [=d:\filename.ext]

Specifies in advance on the command line that the desired operation is to map a drive volume. The /MAP is optional, and may also be specified without a volume filename.

The most common use of this option is for Windows map icons. Create an icon or Windows shortcut for the SDWMAP32.EXE utility and specify /MAP as the only command line parameter. This will force the utility to execute in "map" mode instead of asking if you'd like to map or unmap. The default setup program for SafeHouse automatically creates map and unmap icons for you using this technique.

If you include the optional volume filename with this switch, the mapping utility will initially display the description of the named file in the drop-down list box. This is useful when you work with more than one encrypted volume since it allows you to setup specific mapping icons for each of the volumes.

The filename must be enclosed in quotes if it contains spaces.

Examples:

```
/Map
/m=c:\test.sdsk
```

Utilities supporting this option:

- SDWMAP32.EXE

/Drive = d

Specifies the target virtual drive letter for mapping and unmapping.

If you do not specify the drive letter in advance on the command line, the map utility will default to the letter of the last drive mapped. If you frequently work with multiple encrypted volumes, you can set up an icon (shortcut) to reference the drive/volume pairings you prefer.

Examples:

```
/Drive=S
/d=j
/drive=e
```

Utilities supporting this option:

- SDWMAP32.EXE

/Unmap [=d | =ALL]

Specifies in advance on the command line that the desired operation is to unmap a drive. This option may be specified without a drive parameter.

Using /Unmap without any additional parameters to SDWMAP32.EXE forces the program to come up in "unmap" mode.

Tip

- Try SDWMAP32 /unmap /go /silent for a quick way to unmap a volume from Windows without seeing a dialog box.

Examples:

```
/Unmap=D
/u=all
/u=s
/unmap
```

Utilities supporting this option:

- SDWMAP32.EXE

/CHangepassword = d:\filename.ext

Specifies in advance on the command line the name of the volume to have its password changed.

Examples:

```
/Change="c:\test.sdsk"
/CH=c:\mydrive.sdsk
/changepass=d:\active.sdsk
```

Utilities supporting this option:

- SDWCHANG.EXE

/Newpassword = "mypassword"

Specifies in advance on the command line the new password to be set during a password change operation. If this parameter is not supplied, you will be prompted automatically for your new password and then asked to confirm.

Examples:

```
/Newpass="sail$away"
/N="my_new_password"
/n="telephone.rope"
```

Utilities supporting this option:

- SDWCHANG.EXE

/GO [=ON | OFF]

Causes the utility to immediately begin the requested procedure without waiting for any further user input. This option is frequently paired with /SILENT to run invisibly and unattended in the background.

If you specify /GO without including all the normally-required parameters for a utility, you will still be presented with a dialog box prompting for the missing items.

Examples:

```
/GO
/go
/go=on
```

Utilities supporting this option:

- SDWACTIV.EXE
- SDWCHANG.EXE
- SDWCREAT.EXE
- SDWEXPAN.EXE
- SDWMAP32.EXE

/SILENT

Specifies that the utility should run invisibly without displaying any banners, dialogs or message boxes to the user. This option is frequently combined with the /GO option.

Examples:

```
/Silent
/silent
```

Utilities supporting this option:

- SDWACTIV.EXE
- SDWCHANG.EXE
- SDWCREAT.EXE
- SDWEXPAN.EXE
- SDWMAP32.EXE

DEPLOYHLP.EXE

This utility is used by administrators to create customized versions of the standard SafeHouse installer. Using this tool, the SafeHouse installer can be modified to include files branded for administrative password recovery, as well as numerous other preferences for a corporate deployment. See the SafeHouse User's Guide for more information.

Notes:

- This program runs only on Windows NT/2000/XP. Resulting setup files run on all SafeHouse-compatible platforms.
- Deployment of this file may be disabled for corporate roll-outs.

SAFDSK95.VXD

VxD files are used by Windows 95/98/Me to communicate with hardware devices and virtualized hardware devices.

SAFDSKNT.SYS

On Windows NT and Windows 2000/XP, .SYS files are drivers that are typically used to communicate with hardware or virtualized hardware devices.

SDWBRAND.EXE

The SDWBRAND.EXE utility is used by administrators to embed a special key into certain SafeHouse files to facilitate administrative password recovery. Please see the SafeHouse User`s Guide for more information on this topic.

Note:

- Deployment of this file may be disabled for corporate roll-outs using the DEPLOYHLP.EXE utility.

SDWULOCK.EXE

The SDWULOCK.EXE utility is used by administrators during a remote password recovory procedure. See the SafeHouse User's Guide for more information on this topic.

Note:

- Deployment of this file may be disabled for corporate roll-outs using the DEPLOYHLP.EXE utility.

Table of Contents

Using SafeHouse

Using the SafeHouse System Tray Utility

SafeHouse Utilities Reference

/Force

Specifies that when volumes are unmapped that standard alerts warning about open files should be suppressed. This option is valid only in combination with the /unmap option. Normally, SafeHouse will display a warning dialog message if it detects that a volume being unmapped has open files. However, in some cases, these open files can be safely ignored. One such example is that on Windows NT/2000/XP, the standard Windows Explorer windows showing the contents of directories each hold a file open and therefore unnecessarily trigger an alert. An example of an alert that should not be ignored is when using a word processor to edit a document residing on a SafeHouse volume, and forgetting to save and close the document prior to unmapping the volume.

Examples:

```
/force
```

Utilities supporting this option:

- SDWMAP32.EXE

/REMovable

This option is used to change the drive letter mode used for mapping encrypted volumes. By default, SafeHouse makes mapped volumes appear to Windows as another fixed disk drive. The benefit to the default mode is that you get secure encrypted recycle bins for deleted files inside your SafeHouse volumes. This is useful if you frequently need to recover files after deleting them. A side effect of the default mode that is not always desirable is that Windows will sometimes pop up an Explorer window upon mapping. This is a new "feature" of Windows that is included in some of the newer versions and updates to the operating system.

By specifying the /REMOVABLE option during mapping, SafeHouse will make the new volume appear as a removable drive to Windows. Although the operational differences between the modes are very subtle, sometimes they are enough to help with certain problems you are trying to work around. For example, Windows will not automatically pop up Explorer windows for removable drives. Other changes to be aware of are that removable drives do not get recycle bins and show up marked as "removable" under MyComputer. Prior to SafeHouse 2.00, all volumes were mapped as removable drives.

If you are experiencing undesirable Explorer windows being displayed after mapping SafeHouse volumes, try adding this command line option to your mapping shortcuts. Alternatively, you can make this change for all mappings by creating a *config.ini* file in your SafeHouse program directory that contains the following two lines:

```
[SDWMAP32]
removable=1
```

The sample *config.ini* file shown above instructs SafeHouse to map all volumes as removable without you needing to add the /REMOVABLE option to all of your mapping shortcuts. This file must be placed in your SafeHouse program directory; typically named *C:\Program Files\SafeHouse*. To make this easier for you, this file is available for downloading in the support section of the SafeHouse web site.

Examples:

```
/removable
```

Utilities supporting this option:

- SDWMAP32.EXE

SDWTRAY.EXE

This utility provides quick and convenient access from the system tray to all essential SafeHouse features. The SafeHouse setup program configures this tray utility to run automatically each time Windows starts. You can disable or re-enable this feature by running the program and using the checkbox on the About property sheet page.

Optional command line parameters:

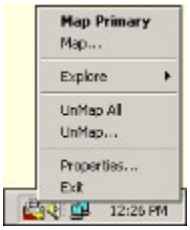
The upper case letters in the option list below indicate the required minimum number of characters needed by this utility to recognize the respective option.

- /STOP

Introduction

The SafeHouse System Tray utility is a one-stop control panel for all essential SafeHouse tasks. When it is running, you will see its "lock" icon in the system tray as shown in the picture below. The default action taken by the SafeHouse installer is to configure this utility to run automatically each time Windows starts. This way, you always have quick access to the product features you use most often.

You can display the context menu by right clicking on the lock icon. Double-clicking the icon with your left mouse button automatically invokes the **bold** menu item without first displaying the menu.



Map Primary

Select this item (or double-click the tray icon) for one-step mapping of your primary volume. Your primary volume is the one you use most often. Other than that, there is no other difference between your primary volume and any other volume you may have created. The Map property page contains fields for setting up your primary volume and corresponding mapping options.

If you select this menu item when your primary volume is already mapped to a drive letter, for your convenience, the Explorer window for the volume will be displayed without prompting you for a password.

Map…

Select this item to map a volume that is not your primary volume. A dialog will be displayed so that you can select the desired volume file and enter your password. Preference settings are available on the Map property page.

Explore

This item displays a submenu of mapped volumes and lets you choose one of the volumes to explore. When you make a selection, the standard Windows Explorer window will be launched showing the contents of the selected drive letter or volume.

UnMap All

Select this item to immediately unmap all SafeHouse volumes without displaying a dialog. SafeHouse volumes are unmapped automatically when you log off or shut down your PC. This option is needed only when you wish to quickly unmap everything without logging off. Preference settings are available on the UnMap property page.

UnMap…

Select this item to display a dialog showing the currently mapped drive letters so that you may pick one to unmap. Preference settings are available on the UnMap property page.

Properties…

Select this option to launch the property sheet dialog containing preference settings and easy access buttons for common SafeHouse tools.

- Map Property Page
- UnMap Property Page
- Tools Property Page
- Volumes Property Page

Exit

Terminates the system tray utility. This does not affect whether it will or not run automatically the next time you start Windows. If you wish to make such an adjustment, please see the corresponding topic below.

Running the Tray Utility automatically when Windows Starts

By default, the SafeHouse setup program configures the system tray utility to run automatically each time you start Windows. You can disable this feature by right clicking on the icon, choosing "Properties…", and then clicking the About tab. The About tab contains a checkbox that lets you control whether or not this utility will be run at startup.

To run the task tray utility when you have not chosen to have it run automatically at startup requires that you invoke the program manually. You can do this using the "System Tray Utility" menu option found along with all the other SafeHouse utility menu links

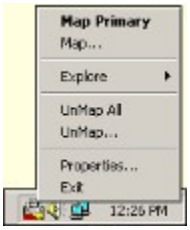
in the Windows Start menu.

Map Property Page

The Map property page is used to set preferences for displaying the SafeHouse Map dialog when it is run from the tray utility. These preferences do not affect how the Map dialog is displayed when run from other menus or shortcuts you may have created.

This property sheet contains two grouped frames of settings. The top group is for your "primary" volume. This is the volume you used most often. These settings correspond to the "Map Primary" right-click menu option for the tray utility as shown in the picture below. The checkbox options for Sound, Explore and Removable correspond to command line options available when running the stand-alone Map dialog from a standard Windows shortcut.

The second group of settings allows you to set preferences for when you choose to display the Map dialog for any volume other than your primary volume. This is done by choosing the second item from the top on the right-click menu as seen below. The checkbox settings have identical meanings to those available in the first group.



UnMap Property Page

The UnMap property page allows you to set preferences for displaying the SafeHouse UnMap dialog when it is run from the tray utility. These preferences do not affect how the UnMap dialog is displayed when run from other menus or shortcuts you may have created.

The option to "force" an UnMap action to complete can be used to prevent the display of a standard message box informing you that you may have open files on a drive being unmapped. Normally you would never want to unmap a drive when it has open files; however, a quirk in Explorer causes this message to appear even when you don't actually have any open files when you attempt to unmap while the Explorer window for a mapped drive is showing. When this is the case, it is safe to ignore the message. Closing the Explorer window for the mapped drive before unmapping also prevents the message from being displayed.

Tools Property Page

This page contains buttons for each of the essential SafeHouse utilities. Running these utilities from here by clicking the buttons is the same as running them individually from the SafeHouse program menu.

Volumes Property Page

The Volumes property page lists the SafeHouse volumes that are currently mapped to Windows drive letters. Right clicking on the icons for listed volumes displays a menu of possible actions.

Please remember that you cannot change passwords or resize volumes when they are mapped. This is why you will not find these actions available on this page. If you wish to change a password or resize a volume, please unmap the volume and display the Tools property page in order to perform the desired functions.