PC DYNAMICS, INC.

Information Security Products

Guide to Using SafeHouse™ Drive Encryption

PC DYNAMICS, INCORPORATED

Guide to Using SafeHouse Drive Encryption

31332 Via Colinas, Suite 102 • Westlake Village, CA 91362
Phone 818.889.1741 • Fax 818.889.1014
http://www.pcdynamics.com

Version 2.10

Revised 12/3/01

License Agreement

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THIS SOFTWARE PACKAGE. IF YOU DO NOT AGREE WITH THEM, PLEASE DISCONTINUE USE OF THE PRODUCT.

PC Dynamics, Inc., provides this program and licenses its use under the terms and conditions stated herein. You assume responsibility for the selection of the program to achieve your intended results, and for the installation, use and results obtained from the program.

LICENSE AGREEMENT

This agreement gives you the right to:

a. use the program on a single machine;

b. copy the program into any machine readable or printed form for backup or modification purposes in keeping with your use of the program on the single machine;

c. modify the program and/or merge it into another program for your use on the single machine (any portion of this program merged into another program will continue to be subject to the terms and conditions of this Agreement.); and,

d. transfer the program and license to another party if the other party agrees to accept the terms and conditions of this Agreement. If you transfer the program, you must at the same time either transfer all copies whether in printed or machine-readable form to the same party or destroy any copies not transferred; this includes all modifications and portions of the program contained or merged into other programs.

YOU MAY NOT USE, COPY, MODIFY, OR TRANSFER THE PROGRAM, OR ANY COPY, MODIFICATION OR MERGED PORTION, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS LICENSE.

IF YOU TRANSFER POSSESSION OF ANY COPY, MODIFICATION OR MERGED PORTION OF THE PROGRAM TO ANOTHER PARTY, YOUR LICENSE IS AUTOMATICALLY TERMINATED.

TERM

The license is effective until terminated. You may terminate it at any time by destroying the program and all copies, modifications and merged portions of the program in any form. The license also terminates upon conditions set forth elsewhere in this Agreement or if you fail to comply with any term or condition of this Agreement. Upon termination, you agree to destroy the program together with all copies, modifications and merged portions in any form.

LIMITED WARRANTY

THE PROGRAM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU (AND NOT PC DYNAMICS, INC., OR AN AUTHORIZED PERSONAL COMPUTER DEALER) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR OR CORRECTION.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

PC Dynamics, Inc., does not warrant that the functions contained in the program will meet your requirements or that the operation of the program will be uninterrupted or error-free.

LIMITATIONS OF REMEDIES

IN NO EVENT WILL PC DYNAMICS, INC., BE LIABLE TO YOU FOR ANY DAMAGES INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PROGRAM EVEN IF PC DYNAMICS, INC., OR AN AUTHORIZED PC DYNAMICS, INC., DEALER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

GENERAL

You may not sublicense, assign or transfer the license or the program except as expressly provided in this Agreement. Any attempt otherwise to sublicense, assign, or transfer any of the rights or obligations hereunder is void.

This Agreement will be governed by the laws of the State of California.

Should you have any questions concerning this Agreement, you may contact PC Dynamics, Inc., by writing to PC Dynamics, Inc., 31332 Via Colinas, Suite #102, Westlake Village, CA 91362.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT AND THAT YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN US WHICH SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS BETWEEN US RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

If your company purchased a multi-user site license for this product, the terms of the Site License Agreement or purchase contract may supersede this license.

Table of Contents

Chapter 1

Introducing SafeHouse

Your hard drive is full of confidential files. You want protection, but it needs to be simple to use. Can such a product exist?

Appears as a new drive letter!

SafeHouse provides transparent "*on-the-fly*" encryption for your notebook or desktop personal computer. Using SafeHouse, you can allocate portions of your existing hard drives to be reserved for encrypted data. 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 virtual drive that you can do with a normal hard drive; only that with SafeHouse, the encrypted volumes require password authentication before the files become accessible.

2048 Gigabytes!

SafeHouse encrypted volumes can range in size from 2 Kilobytes to 2048 Gigabytes when using NT/2000/XP. The maximum size for Win9x/Me is 4GB. The only other limitation is the size of your hard drive. Volumes are *mapped* to a standard Windows drive letter in a single step. Just type your secret password and the entire contents of your encrypted volume will be instantly available. No waiting! When you're done, either click the *unmap* icon or turn off your PC. Unlike many competing products, protected files are never temporarily decrypted and stored back to disk, meaning that the secrecy of your data will not be compromised if you forget to re-encrypt, unmap or unexpectedly lose power to your PC.

Why is SafeHouse Encryption Important?

Industry analysts predict that 1 in 14 notebook PCs will be stolen.

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

Consider the consequences of your files getting into the wrong hands. You could lose business, be sued, or even worse, be fired from your job! With SafeHouse being so easy to use, you can now continue being the quintessential PC *"road warrior"* without ever having to risk the integrity, safety and security of your data due to being overwhelmed by cumbersome security software.

Individuals and organizations may use SafeHouse outside of the U.S. by observing the export guidelines presented in Appendix A.

SafeHouse Includes Blowfish, Twofish, Rijndael, DES and Triple DES Encryption

SafeHouse includes support for the very best encryption algorithms available in a commercial product. Many of the supported ciphers are offered in several different key strengths to meet the widest possible range of environmental and regulatory requirements. The longest key currently supported by SafeHouse is 448 bits, however, some demonstration and export versions of the software support only smaller keys.

The Rijndael and Twofish algorithms are new to this version of SafeHouse. Both are extremely fast, support 128- and 256-bit keys, and are well-respected in the industry. Rijndael was selected in October, 2000, by NIST to become the new Advanced Encryption Standard **(AES)** and is destined to replace **DES** as the predominant encryption algorithm used by the U.S. Government. Twofish was also a finalist in the **AES** competition and is best known for its exceptionally-fast speed.

How strong is a 128-bit key? For starters, a 128-bit key has 3.4×10^{38} possible keys. That's 10^{21} times stronger than a 56-bit **DES** key. The famous "DES Cracker" machines built in the late 1990's could recover a 56-bit key in a matter of hours. If this time could subsequently be reduced to one second (meaning trying 2^{55} keys per second), then it would take that same machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit key. To put this into perspective, the universe is believed to be less than 20 billion years old. Of course, if you need something stronger, SafeHouse still has you covered; offering two 256-bit ciphers and another at 448-bits.

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

SafeHouse 2.00 for Windows requires:

- Windows 95, 98, Me, NT 3.51, NT 4, XP or Windows 2000
- 486 or Pentium CPU
- Approximately 2-5MB available hard disk space

Visit PC Dynamics' web site.

www.pcdynamics.com

This version of SafeHouse is compatible with all 32-bit versions of Windows. The setup program automatically detects your operating environment and installs the appropriate suite of code and drivers. If you upgrade your PC to NT/2000/XP after installing SafeHouse on Windows 9x/Me, you will need to run the SafeHouse setup program again to allow the installer to adjust the software driver configuration.

SafeHouse virtual encrypted volumes may reside on local hard drives, removable media such as diskettes and ZIP disks, and additionally on most network servers. Volumes may also be transferred to CD ROMs, CD-R and CD-RW media.

Key Product Features

SafeHouse is a powerful product and includes many features to help you protect your sensitive data. The most-important features are listed below.

- Be up and running within 5 minutes. No need to repartition drives.
- Compatible with Windows 95, 98, Me, NT, XP and Windows 2000.
- Looks and works like a new Windows drive letter.
- Supports Blowfish, Twofish, Rijndael, DES and Triple DES encryption.
- Lightning-fast access using highly-optimized 32-bit device drivers.
- Encryption is transparent. No need to remember to encrypt/decrypt.
- Volumes as large as 2048GB on NT/2000/XP; 4GB max on Win9x/Me.
- Volumes can be resized either on demand, or automatically when mapped.
- Native support for FAT12, FAT16 and FAT32 internal volume formats.
- On NT/2000/XP, volumes can be manually reformatted to use NTFS.
- Up to 10 volumes may be mapped at the same time; even more on NT.
- No limit to the number of volumes that can reside on a single hard drive.
- Supports mandatory password lengths, expirations and grace periods.
- Optional administrative key recovery using public/private keys.
- Drive monitor suspends access during power-management sleep modes.
- Encrypted volumes can reside on local drives, CDs and network servers.
- Command-line API supports scripting and silent program execution.
- Encrypted volume files can be securely backed up to tape or other media.
- Includes support for X.9 handheld hardware authentication devices.
- The full-strength version may be exported to over 23 countries.

What's New in Version 2

SafeHouse version 2 introduces several new features, improvements and refinements; the most-significant of which are listed below. The SafeHouse volume file format has not changed, which allows volumes created with previous versions of SafeHouse to be compatible with this new version.

- Improved support for Windows Me and Windows 2000. Windows XP is supported starting with SafeHouse v2.10.
- The maximum size of an encrypted SafeHouse volume has been increased to 2048GB when using NT/2000/XP and 4GB for 98/Me. The previous limit was 2 GB.
- The internal volume disk format now supports the FAT32 format in addition to FAT12 and FAT16 which were previously supported. Volumes can also be created without a file system and later be formatted with **NTFS** using the standard hard disk formatting utilities which come with Windows.
- Volumes can be compacted (shrunk). Previously, only expansion was supported.
- The Twofish encryption algorithm is available in both 128- and 256-bit strengths.
- The new Advanced Encryption Standard algorithm (**AES**), Rijndael, is supported in both 128- and 256-bit strengths.
- A variety of changes have been made to the SafeHouse utility wizards to make them easier to use.
- The file extension for SafeHouse volumes has changed from **.DSK** to **.SDSK** in order to be compatible with the new *System File Protection* feature introduced by Microsoft inWindows Me. This change is implemented on all Windows platforms. You must manually rename your volumes to use the **.SDSK** extension if they were created with a prior version of SafeHouse since the SafeHouse utilities will scan only for this extension.
- Volumes with the read-only attribute are treated as write-protected media.
- SafeHouse no longer includes 16-bit utilities and drivers to support running on PC-DOS, MS-DOS or Windows 3.1.

Important Notice Regarding our Shareware Version

PC Dynamics publishes a reduced-strength Shareware version of SafeHouse which is freely-distributed on the Internet. The primary differences between this Shareware version and our standard retail version are highlighted below.

- The maximum encryption key strength is limited to 40 bits, which allows our evaluation version to avoid most export controls.
- Several of the stronger encryption algorithms found in our retail product are completely omitted. This includes: Twofish, Rijndael and Triple DES.
- Only a few specific passwords can be used. When creating volumes or subsequently changing volume passwords, the utility wizards for the Shareware version will accept only the following case-sensitive passwords: *safehouse*, *password*, *pass*, *one*, *two*, *three*, *four*, *five, six* and *seven.*. The retail version allows you to choose your own passwords or passphrases up to 255 characters.

Upgrading from the Shareware Version to the Retail Version

If you are upgrading SafeHouse from the Shareware version to the full-strength retail version, please know the following:

- You may install the retail version of SafeHouse over the evaluation version without uninstalling the old version. The installer is smart enough to make the appropriate adjustments.
- You must reboot your PC after completing the retail install to load up the new device drivers (drivers load only during system startup).
- Volume files are not automatically converted to full-strength encryption since this would pose a substantial risk to your data in the event of a system failure. You must create new volume files after completing the upgrade and copy your personal files from the old volumes to the new ones by mapping both at the same time and using standard Windows Explorer drag-and-drop file copy procedures.

Corporate Site License Evaluations

If you are evaluating SafeHouse for a large corporate environment, please see our web site or contact our sales department to obtain an evaluation copy of SafeHouse which does not have the aforementioned restrictions.

Chapter 2

Software Installation

In a nutshell, run SETUP and the installation wizard will step you through the entire process. Files are not encrypted during installation.

SafeHouse is easy to install. The **SETUP** program included on the distribution diskette or within the Internet download does all the work. Encryption is not performed at this time. After creating a new directory for SafeHouse and copying over a group of files, the installation wizard will offer you the option to install its device driver and create your first empty encrypted volume. The "create volume" wizard optionally run by **SETUP** is the exact same one you can run separately anytime after completing the installation. The 32-bit Windows device drivers required by SafeHouse are installed automatically by the setup program.

To install SafeHouse for Windows:

1. Insert your SafeHouse diskette into your **A:** drive.
2. Select *RUN* from the *Start* menu.
3. Type **A:\SETUP** and press **OK**.
4. Follow the on-screen instructions.

Running SETUP does not encrypt your data files.

If during the installation you have questions about the volume creation wizard, please refer to the corresponding section of this manual for step-by-step instructions.

See also:
- Creating SafeHouse Encrypted Volumes

The instructions above assume you are installing from a floppy diskette. If you are instead installing from an Internet download file, you may run **SETUP** by executing the downloaded file. SafeHouse files available on the Internet may have a variety of names; however, they are all self-extracting installers which work identically to that distributed on diskette or CD ROM.

NOTE: See the next page for an important note on changes made to volume filenames.

The SafeHouse Volume File Extension is Now .SDSK

Starting with SafeHouse version 2.00, the standard file extension used for encrypted volumes is **.SDSK**. Prior versions of SafeHouse used **.DSK**. This change was required to ensure that SafeHouse volume files would remain compatible with Microsoft's new *System File Protection* features introduced in Windows Me, and likely to also be included in all future versions of Windows.

You Must Rename Your Existing Volume Files

If you are using SafeHouse for the first time, this change will not affect you. However, if you are upgrading from a previous version of SafeHouse and have existing volume files which you intend to keep, then you must rename these volume files to use the new **.SDSK** file extension. This is a simple procedure which can be accomplished by using Explorer to display the folder containing your volume files and then right-clicking on these files to display their pop-up menus. Choose ***Rename*** and type in the new extension.

The SafeHouse utility wizards will only allow you to work with volumes having the **.SDSK** extension. Volumes with the old extension will not be shown in any of the volume-selection drop-down lists. Don't worry, files not renamed will not be deleted.

Why was this Change Necessary?

Microsoft's new System File Protection (**SFP**) feature, first introduced in Windows Me, attempts to maintain the integrity and stability of your system by making backup copies of certain files automatically as you work or make changes to your system configuration. The files affected by this feature are determined by file extension. For some uknown reason, Microsoft placed our **.DSK** extension on the list of files needing protection. This resulted in an extreme performance problem for SafeHouse because Windows would make a complete hidden backup copy of volumes each time they were mapped. Since many of our customers are using large volume files (1 to 2GB), this meant having to wait several minutes for Windows to make copies before gaining access to encrypted data. By changing to the **.SDSK** extension, this problem is avoided.

Turn Off the Read-Only Attribute on Previously-Created SafeHouse Volume Files

Starting with version 2.00, volume files with the Windows read-only file attribute set will be treated as write-protected media when mapped. You must use Explorer to manually turn off this attribute on volumes created with previous versions of SafeHouse if you wish to write to them since this attribute was previously set by default for all volumes.

Chapter 3

Getting Started with SafeHouse

SafeHouse drive encryption is automatic and transparent. To your programs, it looks just like another Windows drive letter.

SafeHouse does not require you to change your working habits. Once you've installed the software onto your PC, you can be up and running in just a few minutes. Easy Windows wizards are available for each task you might need to perform while using encrypted volumes. Each wizard has its own icon installed into your Windows *Start* menu. Using SafeHouse is so easy, in fact, that you may not need to read beyond this chapter.

The following programs and icons are installed automatically by **SETUP**:

Filename	*Desktop Icon*
README.TXT	Readme File
SDWCREAT.EXE	Create SafeHouse Volume
SDWMAP32.EXE	Map or UnMap a SafeHouse Volume
SDWCHANG.EXE	Change SafeHouse Password
SDWEXPAN.EXE	Resize SafeHouse Volume
SDWMON32.EXE	SafeHouse Volume Monitor
SDWACTIV.EXE	Change SafeHouse ActivCards
SDWSHOW.EXE	Show Volume Properties
SDW.HLP	SafeHouse Online Help
SAFEHOUSE.PDF	SafeHouse User's Guide in Acrobat format
SDWULOCK.EXE	Remote Recovery (for administrators only)
SDWBRAND.EXE	Brand SafeHouse (for administrators only)
DEPLOYHLP.EXE	Deployment Tool (for administrators only)
REMOVE.EXE	None. Run directly or from Windows control panel.

Each of these wizards or files is self-explanatory. However, if you need more information, complete details can be found in later chapters of this user's guide. Context-sensitive online help is also available for all SafeHouse utilities.

Why use Separate Wizards Instead of a Single Big Application

We are sometimes asked why SafeHouse is implemented using separate wizards instead of having a single do-everything application. The reason we chose this approach is that in real-life use of this software, you will only be mapping and unmapping volumes on a daily basis. All the other product features, as important as they may be, will be used infrequently. We felt that it was important to make your daily routine as streamlined as possible. Running the wizards from the *Start* menu seemed very natural.

Figure 1. Simple Volume Mapping.

Most SafeHouse users prefer to create volume-mapping shortcuts directly on their Windows desktop. This makes it easy to gain access to confidential files without the overhead of launching a full-blown application. Clicking on the mapping shortcut displays a simple password dialog similar to the one shown to the left. Most of the other wizards are run from the Windows *Start* menu.

Another reason for implementing SafeHouse as a series of separate wizards is that a great number of our clients purchase corporate site licenses and prefer to deploy only specific portions of the product to some users.

Overview of 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 drivers are 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 designated 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", or 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.

Encrypted Volumes

SafeHouse encrypted volumes can reside in any directory of your local hard drive. The default action taken by SafeHouse is to create volumes in your root directory using a **.SDSK** file extension. You can also create volumes on network servers, floppy disks and most any other removable media.

Volume sizes can range from just a few kilobytes all the way up to 2048GB or the maximum available space on your hard drive when you are using Windows NT/2000/XP. The maximum size for Win9x/Me is 4GB due to a limitation of the FAT32 file format. You'll be asked to choose an initial size for your volumes when they are first created. Afterwards, you can change their sizes as often as desired within their configuration limits using the ***Resize SafeHouse Volume*** utility wizard. The wizard will let you know what the limits are.

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, which is currently fixed at 10 for Windows 95, 98 and Me. On Windows NT/2000/XP, the number of mapped drives is limited only by the number of available Windows drive letters.

Passwords, Protections, and Access Controls

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 between 1 and 255 characters long and to select from one of the available encryption methods. The **Blowfish**, **Twofish** and **Rijndael** algorithms are considered to be the most secure and are strongly recommended for most commercial environments.

ActivCard handheld X.9 security devices are optional and may be purchased separately.

The next level of protection offered by SafeHouse is to configure your volumes to require *ActivCard* authentication. ActivCards are small handheld devices which serve to uniquely identify the individuals who possess them. These devices, sometimes referred to as security *tokens*, are sold separately and are available from a variety of security resellers. By having your volumes require ActivCard authentication, users must both know the volume's password and have possession of their ActivCard and its corresponding **PIN** code to retrieve your encrypted data. This extra level of protection is completely optional. The ActivCard support in SafeHouse conforms to the X.9 specification.

Each SafeHouse 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 that they will be unable to make a duplicate while it's in their possession.

Getting Ready for SafeHouse

Before using SafeHouse for the first time, you must create an empty volume to store your encrypted files. This step is usually accomplished during the setup process. However, if you didn't run the complete setup program, you will need to perform this task before going any further.

If you did not run the ***Create SafeHouse Volume*** wizard during setup, you must first:

- Create an empty SafeHouse disk volume by running the ***Create SafeHouse Volume*** wizard. You will find a corresponding icon on your Windows Start menu in the SafeHouse program group.

Working with SafeHouse Encrypted Volumes

Using SafeHouse drive encryption on a daily basis usually involves only a few extra steps beyond what you are currently doing. SafeHouse's encrypted disk volumes appear to Windows and to your application programs as another Windows drive letter. As such, you can do most anything with a SafeHouse volume as you could with any other drive. This includes creating, reading, writing, copying, deleting and renaming files, as well as all drag-and-drop actions supported by your desktop manager.

If you are using SafeHouse with the Windows Explorer or other file manager, you should note that right-clicking on a SafeHouse volume file provides quick access to most of the volume administration wizards described below. These are the wizards are also accessible from your Windows *Start* menu.

Daily SafeHouse tasks:

- Map your SafeHouse volume to a Windows drive letter.
- UnMap the volume when done or turn off your PC.

From time to time, you may also wish to:

- Change your volume's password.
- Resize your volume.

Setup installs icons for each of these tasks onto your Windows desktop.

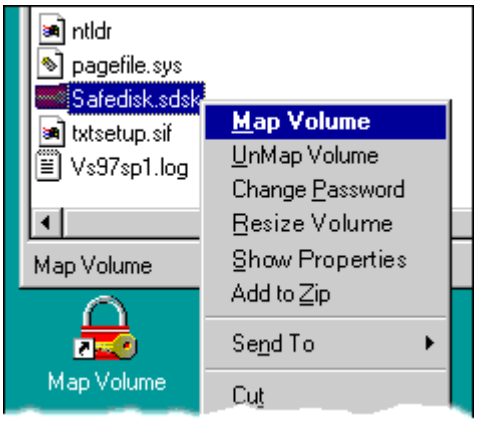


Figure 2. Right-clicking in Windows Explorer

Figure 2 shows the new selections added to the right-click pop-up menu for SafeHouse volumes. These menu items invoke the same wizards as found in your Windows Start menu.

The "Map Volume" shortcut appearing in the lower left portion of the image shows a typical desktop shortcut used for one-step volume mapping.

Mapping Volumes to a Drive Letter

You must be authenticated each time you map a volume to a drive letter.

Once you've created a SafeHouse volume, you must associate the volume file with one of the Windows drive letters reserved for SafeHouse before working with the encrypted files contained within the volume. This process is called *mapping*.

Figure 3. Mapping a SafeHouse Volume

Mapping is accomplished using the ***Map SafeHouse Volume*** wizard as shown here. Simply enter your secret password and press **Enter**. The other controls on the screen can usually be left as they are.

Provided that the password is correct, you will then be authenticated for access to the files contained within the volume. You do not need to supply your password for access to individual files.

A single password is used for access to all files within a volume.

After mapping the volume to a drive letter, you can work with that drive letter as you would any other normal drive. In fact, to Windows, it is a normal drive. When you're done working with the files on the encrypted volume, either *unmap* or shut down your PC to disassociate the volume from the drive letter. This ensures that nobody else will gain access to your data. Unmapping is automatic after an unexpected loss of power.

UnMapping Volumes

Unmapping disconnects a volume from its corresponding Windows drive letter. An unmapped volume cannot be accessed. Not by you, nor anyone else. It's a good idea to unmap active volumes whenever you expect to leave your PC unattended. Turning off your PC forces an implied unmap and is perfectly safe for SafeHouse. Be careful, however, as most applications and Windows itself do not take kindly to an abrupt loss of power. We are only letting you know that such will not compromise your security.

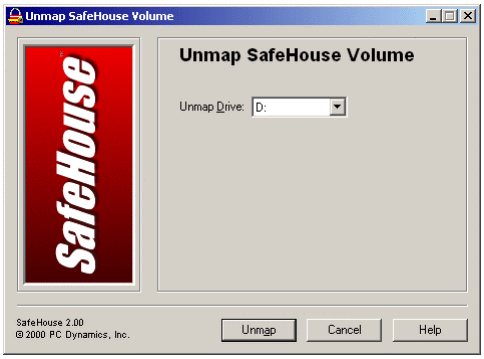


Figure 4. Unmapping a Volume

Unmapping is accomplished using the ***Un-Map SafeHouse Volume*** wizard shown here. Unless you're working with multiple mapped volumes at the same time, the drive letter will always be correct. Just press **Enter**.

You might want to consider using a good password-protected screen saver for times when unmapping wouldn't be appropriate.

TIP: You can modify your unmap icon to unmap all mapped volumes at the same time without displaying the dialog by changing the command line parameters for the unmap icon to **/unmap=all /go /silent /sound**. Click the icon and you'll hear a confirmation sound.

Changing Volume Passwords

Try to avoid passwords which include parts of your name, names of your children, pets or birthdays.

All volumes require a password for authentication. The initial password for each volume is established when the volume is created. Afterwards, you can change the password as often as desired. You can even force regular password changes for a volume by specifying the appropriate options during create.

Consider using a simple phrase instead of single words.

Figure 5. Change Volume Password

Password changes are accomplished using the ***Change SafeHouse Password*** wizard. You can run this program either directly from its icon, or by selecting the corresponding button on the map volume dialog.

It's a good idea to change passwords every 30 to 60 days. SafeHouse can enforce regular password changes if instructed to do so.

NOTE: Remember your passwords. PC Dynamics cannot help you recover lost passwords.

An often overlooked aspect of using strong encryption is that using weak passwords can easily compromise your security; even when using algorithms supporting long key

lengths. Please do not use short passwords! Short passwords are more-easily guessed by intruders. Equally important is not choosing passwords that have specific meaning to your life such as the name of your pet, child, a birth date, etc. Intruders know that most people tend to choose short familiar passwords because they are easy to remember. Easy for you, and easy for them too. If your data is important enough to require strong encryption, you'll be much safer using a multi-word passphrase instead of a single word or a few numbers. If you pick your passphrases wisely, the will still be easy to remember. For example, "*I hate to eat small green bugs.*" would make a nice one.

Increasing or Shrinking the Size of a Volume

Volumes reside on their respective host drives (normally C:\) as a single large file. The create volume wizard pre-allocates only the amount of space specified as the initial volume size. To increase the size of a volume up to its expansion limit, you must use one of the supplied wizard utilities. You may increase a volume's size as often as desired. Volume compaction (shrinking) is also supported.

Figure 6. Increase Volume Size

You may increase the size of a volume at anytime using the ***Resize SafeHouse Volume*** wizard. After first authenticating yourself for access to the volume by supplying your password, you will see the wizard page shown in Figure 6.

Set the new size within the allowable range and press the Next button to display the final page and complete the operation.

TIP: For maximum performance, optimize (defragment) your host drive (C:) after expanding.

Viewing or Changing a Volume's Properties

You may view or change a volume's properties, such as its description and password restrictions, by running the ***Show Volume Properties*** wizard shown in Figure 7.

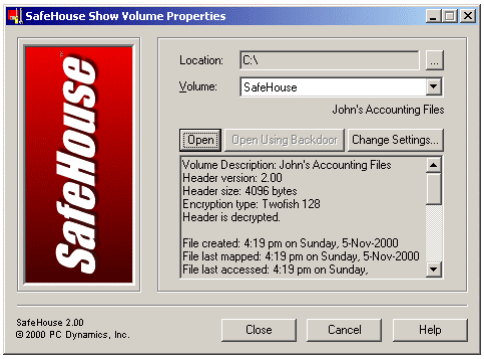


Figure 7. Show Volume Properties

Some of the information available for viewing is kept hidden until you authenticate yourself using the Open button.

Authentication is always required before you will be allowed to make any changes to the property settings.

Chapter 4

Using SafeHouse

SafeHouse has a Windows wizard for just about anything you'll ever need to do with encrypted volumes. This chapter contains a thorough description of each wizard along with a few tips and tricks to make using SafeHouse easier than ever.

SafeHouse ships with a variety of Windows wizards to perform all essential tasks and maintenance on encrypted volumes. The **SETUP** program automatically installs icons into your Windows *Start* menu for each of these utilities. For the most part, these utilities are self-explanatory and do not require any special instructions. However, for the sake of completeness, this chapter describes each utility in detail along with some helpful tips which should assist you in fine tuning your final configuration.

Creating SafeHouse Encrypted Volumes

See also:
- SDWCREAT.EXE

SafeHouse uses large encrypted volumes to store protected data. An encrypted volume is simply a large file which contains enough space to hold all your sensitive documents. Internally, the file contains a format that is designed to be fast, efficient and secure with regard to safeguarding your critical information. In addition to holding your data, the volume file contains a set of properties which determine the security rules governing access to its contents.

You may create as many volumes as desired. If you are just getting started with SafeHouse, we recommend creating one or two temporary volumes which can be used for testing and getting familiar with some of the product's features.

TIP: Volumes which are no longer needed may be deleted using Windows Explorer.

This is the same create wizard that can be run from SETUP.

Figure 8. Create Volume Wizard

The ***Create SafeHouse Volume*** wizard is used to create a new empty volume. You will find an icon for this utility in the *Start* menu or program group installed for SafeHouse during setup.

This wizard will ask you a variety of questions about how you want to configure and control access to your files, and then builds a volume file which meets those requirements.

SafeHouse volumes can reside in any local disk directory, on diskettes, and on most network servers.

Figure 9. Volume Filename and Description

Every volume file must have a name, description and location. By default, volume files are usually stored in your root directory; or alternatively, in the last directory remembered from a previous SafeHouse operation. If you need to change the *Location* directory, use the [...] directory browse button to choose a new location.

The *Description* can be any text you choose. This will be the brief description of the volume that is displayed under the volume's filename whenever the volume is selected in any of the SafeHouse utility wizards. The *Description* is stored within the volume file and may be different from the volume's given filename.

TIP: SafeHouse volumes are fully compatible with most types of removable media. This includes floppies, optical disks, zip disks, and CD-RW, as well as CD-R media in read-write mode. Simply point the *Location* to that drive. Most network servers are also supported.

The SDSK volume file extension is required for all SafeHouse utility wizards.

The *Filename* is the name of the file within the *Location* directory. The file extension is supplied for you and is always **.SDSK** so that the file will be found when searching for SafeHouse volumes. Do not type the extension as part of the filename. You will be warned if you choose a name that already exists.

About Volume Extensions

Please note that previous versions of SafeHouse used **.DSK** for the standard volume extension. Starting with version 2.00, the extension has been changed to **.SDSK** and the old extension is no longer supported. You must rename any previously-created volume files to use this new extension. This change was necessary to maintain compatibility with the new system recovery features added to Windows.

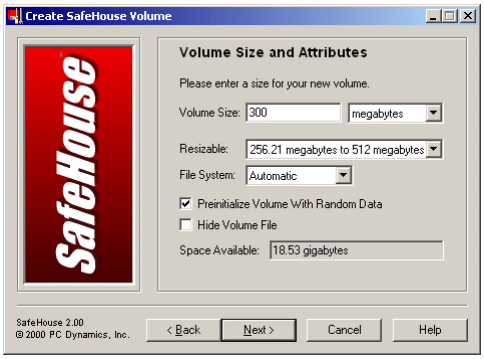


Figure 10. Volume Size and Attributes

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 2KB to 2048GB on NT/2000/XP; otherwise the maximum is 4GB. 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 absolutely 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.

TIP: Creating a volume which is excessively large for small amounts of data is overkill and will result in a lot of wasted hard disk space. Also, most people save only data and document files to encrypted volumes as there is generally no security benefit to saving program files.

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 presented 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** in this version of SafeHouse is 2048GB when the host drive is formatted using **NTFS** (NT4/2000/XP), and 4GB when the host drive is formatted using **FAT32**. **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** or reformatted to **NTFS** cannot be subsequently resized since SafeHouse will not know which file system you are using.

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.

The *Hide Volume File* checkbox is used to set the hidden file attribute for the volume after it is created. Hiding the file makes its existence a little less obvious; however, not all disk managers will suppress listing the volume. The read-only file attribute is set automatically for all volumes, yet here again, this flag is not always respected by certain file management programs.

Volumes can expand or shrink automatically.

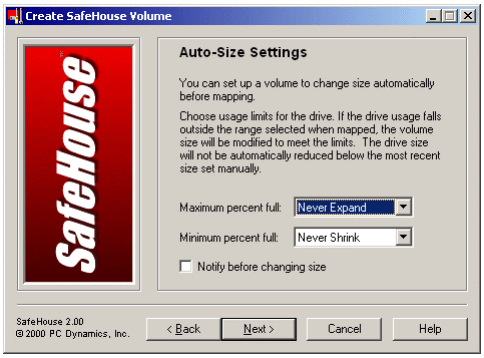


Figure 11. Automatic Resize Limits

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.

The Blowfish, Twofish and Rijndael ciphers are considered to be the strongest.

Figure 12. Encryption Type

On this next wizard page you are asked to choose the method of encryption. Different versions of SafeHouse may offer different choices of algorithms. Press the ***Help*** button to see a detailed explanation for each of the available algorithms.

If you are working in a commercial environment and strong security is important, we recommend that you select either **Blowfish**, **Twofish** or **Rijndael** encryption using a 128-bit or greater length key. All three algorithms are very-well respected. The retail version of SafeHouse defaults to selecting the Twofish algorithm since it is the fastest.

TIP: The SafeHouse administrative key recovery feature works on key sizes up to 128 bits.

SafeHouse still offers **DES** and **Triple DES** encryption due to their use in legacy applications; however, **DES** is now believed to be vulnerable to attack due to its small key size (56-bits); and **Triple DES**, although significantly stronger than standard **DES**, is an order of magnitude slower than some of the newer competing algorithms.

TIP: You cannot change the encryption method of a volume after it has been created. If you later determine that a different algorithm is required, you will need to create a new volume with the desired algorithm, then mount both volumes simultaneously and copy all files to the new volume.

Optional Hardware authentication devices must be purchased separately.

Figure 13. Protection Level

Depending upon your version of SafeHouse, you may be offered several choices of protection levels. This is what determines what will be required of you to access, or *map*, the volume.

At the very minimum, a password is always required. You will be given an opportunity to choose your password and its properties on a subsequent wizard page.

For a higher level of protection, SafeHouse supports certain hardware authentication devices, such as the *ActivCard* handheld X.9 authentication token. Support for other devices may be added in the future. If you in-

dicate that extra authentication or identification will be required, the wizard will ask you to supply some additional information about the device's characteristics.

TIP: Good security is based upon something you know and something you have. This double layer of protection safeguards you from snooped passwords and stolen hardware because neither one will work alone.

The *Password Only* option is the default choice as it does not require the support of additional hardware. Most SafeHouse users find that password-only authentication is very suitable and appropriate for typical corporate environments.

Figure 14. Password Properties

Passwords are from 1 to 255 characters in length.

On this screen you are asked to choose your initial password along with several of its properties. The properties you establish here will be enforced on future password changes.

By default, passwords may be from 1 to 255 characters in length and can consist of letters, numbers, spaces and symbols. Passwords are case sensitive.

You may optionally force frequent password changes by enabling the *Enforce Password Expiration* group and setting the number of days between mandatory changes and the grace period after which the volume will not be usable until the password is actually changed. Within the grace period, you will receive a warning that requests that you change your password immediately.

Special Note to Shareware Users

Please note that the Shareware version of SafeHouse has restrictions placed on password choices. The Shareware version will accept only the following case-sensitive passwords: *safehouse*, *password*, *pass*, *one*, *two*, *three*, *four*, *five*, *six* and *seven*. If you choose a password other than one of these, the wizard will alert you when you attempt to move on to the next page. Although this restriction on passwords is certainly suitable for testing, it is important to know that intruders would have only to test a maximum of these ten passwords in order to gain access to volumes protected using the Shareware version. This restriction is imposed to encourage paid software registrations.

ActivCard security tokens must be purchased separately.

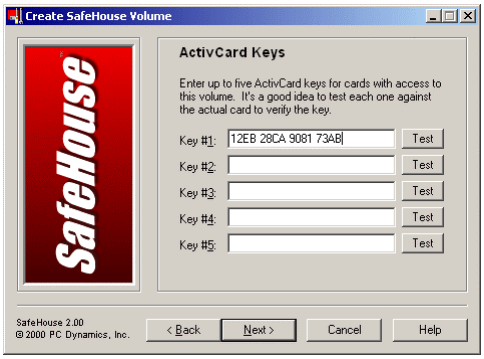


Figure 15. ActivCard Keys

If you had indicated previously that your volume will require *ActivCard* token authentication, this page will be presented to obtain the keys for up to five devices.

After you enter each key, we strongly suggest using the corresponding ***Test*** button to run through a simulated authentication. This will ensure that the key you entered actually does match the device.

TIP: The procedure for authenticating yourself to SafeHouse using an ActivCard is presented in Appendix C.

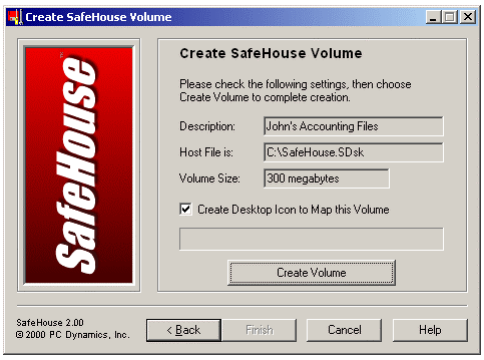


Figure 16. Final Wizard Page

On this final wizard page you are given one last opportunity to review some of your choices before actually creating the volume.

Press the ***Create Volume*** button to create the volume file on your hard drive. The meter bar will indicate the progress as the operation is performed. In most cases, this step should take less than a minute.

The *Create Desktop Icon to Map this Volume* checkbox is used to instruct the wizard to create a Windows desktop shortcut specifically referencing this volume. Volumes mapped using shortcuts such as the one created by this option will use the simplified password dialog shown in Figure 1. Shortcuts can also be created by the ***Map SafeHouse Volulme*** wizard.

When done, press ***Finish*** to exit.

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

Mapping and UnMapping SafeHouse Volumes

See also:
- SDWMAP32.EXE

Mapping and unmapping SafeHouse volumes will be the tasks you perform most often. Mapping a volume is the process of authenticating yourself using a password and

associating the contents of the volume with an available Windows drive letter. Unmapping is the process for making the volume inaccessible. Because you'll perform these tasks often, SafeHouse provides several options which should help make mapping and unmapping more convenient, efficient and automatic.

Mapping and unmapping are performed using the same utility. What you see in the dialog box depends upon the command line options associated with your desktop icons. The SafeHouse **SETUP** program automatically creates two icons for the **SDWMAP32.EXE** utility; one for mapping, the other for unmapping. Both icons run the same program, but since each has a different set of command line options, the behavior of the program will be adjusted accordingly.

When you map a SafeHouse volume, the volume's file is located on your host drive and passed along to SafeHouse's device driver, which is in charge of opening the file and making its contents appear to Windows as a standard removable hard drive. Once mapped, you can do anything with the drive that you could do with any other disk drive. This includes reading, writing, copying, renaming, deleting, dragging, dropping, or just about anything else your file manager is capable of. As far as Windows is concerned, the mapped volume is just another hard drive. Of course, all this assumes that you are able to provide the correct password for accessing the volume.

Mapping is required in order to access an encrypted volume.

Figure 17. Map SafeHouse Volume

Run the ***Map SafeHouse Volume*** utility to gain access to your encrypted data.

Select the target volume, enter your password, then press the ***Map*** button.

If your PC has sound support, you will hear a simple confirmation sound to signify that the mapping was successful.

The *Read Only* checkbox is used to indicate that you wish to map the volume only for reading. When this option is checked, any attempt to write to the volume will result in a Windows error message similar to the one you see when you attempt to copy files to a write-protected floppy diskette. You should also know that SafeHouse honors the read-only file attribute on the volume file. If you map a volume that has this attribute set, then the *Read Only* checkbox will be automatically set and disabled to prevent inadvertent writing to the volume. Volumes residing on CD will also behave this way.

Use the *Change* button as a convenient means to launch the ***Change SafeHouse Password*** wizard. This is especially useful when your password has expired.

Figure 18. Simple volume mapping.

The *Create Shortcut* button is used to instruct the wizard to create an icon on your desktop with command line options configured to match the settings currently shown in the wizard. Clicking on this icon, or shortcut, will present you with the simplified password dialog shown in Figure 18. Many users find this more convenient than using the full mapping wizard each time they wish to map a volume.

TIP: You can double-click the background of this dialog to instruct SafeHouse to reveal the characters of your password as you type them. This is often useful when using long passwords. Double-clicking a second time hides your password. This setting is remem-bered between sessions and is also available by clicking on the window caption.

Mapping Volumes on Network Servers

SafeHouse volumes can be mapped for writing only by one person at a time. If you wish to have multiple users access a volume simultaneously over a network, then all users must check the *Read Only* option. If the first user maps with write access, then all subsequent network map requests will be denied. Similarly, if any users have mapped the volume for read-only access, any attempt to map for writing will be denied.

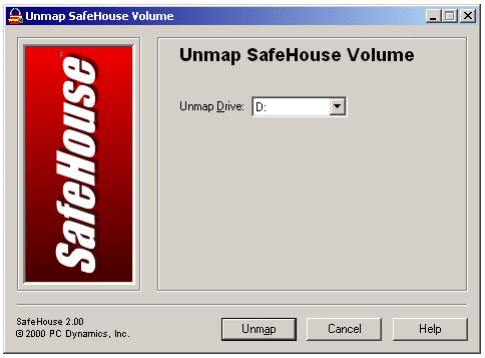


Figure 19. UnMap SafeHouse Volume

Run the ***UnMap SafeHouse Volume*** utility to make a previously mapped volume inaccessible.

Choose the letter of the drive to unmap and press the ***UnMap*** button.

If your PC has a sound card, you will hear a short sound to signify a successful operation.

TIP: SafeHouse volumes are unmapped automatically when you turn off your PC. This includes both normal and abrupt shutdowns, including inadvertent loss of power.

Once you've become accustomed to mapping and unmapping, there are some things you can do to automate these tasks since they are performed so often. First, consider dragging a copy of the ***Map SafeHouse Volume*** icon into your Windows *Startup Group*. Doing this will cause SafeHouse to be run automatically each time you start Windows. You'll be prompted for your password and granted instant access to your data without needing to perform any additional steps.

Another popular thing to do is to place shortcuts for common tasks directly onto your desktop. The SafeHouse **SETUP** program can do this for you if you so choose.

If you really want to get fancy, you can use a few optional command-line parameters to customize certain icons and shortcuts. By specifying volume filenames, drive letters and other information directly on the command line for your icons, you can automate just about anything you'll ever want to do within SafeHouse.

You may want to try combining some of these tricks. For example, create an icon in your *Startup Group* which runs **SDWMAP32.EXE** with the command line parameters set to **/map=c:\safehouse.sdsk /drive=d: /sound /go** for instant volume mapping each time you start your PC. SafeHouse will recognize that the only thing that's missing is the password and prompt you using a simplified dialog box similar to the one shown in Figure 18. Of course, you'll need to make the appropriate substitutions in this example for your actual volume filename and drive letter. A variation of this would be to create desktop mapping icons for each volume that you use frequently. The same can be done for unmapping and password changes.

Another trick is to create an unmap icon to unmap all mapped volumes at the same time without displaying a dialog. This is accomplished by changing the command line parameters for the unmap icon to **/unmap=all /go /silent /sound**.

TIP: SafeHouse remembers the last volume filename referenced in any of its wizards to fill in as the default target volume on your next operation. You can override this default if necessary.

Please refer to Chapter 5 for a complete reference of supported command options and their meanings.

Changing SafeHouse Volume Passwords

See also:
- SDWCHANG.EXE

All volumes require a password for authentication. The initial password for each volume is established when the volume is created. Afterwards, you can change the password as often as desired. You can even force regular password changes for a volume by specifying the appropriate options when the volume is created.

In order to change a volume's password, you must provide both the old password and the new password. The new password will be checked to ensure that it meets the minimum and maximum length criteria that was established when the volume was created.

Due to the way SafeHouse uses passwords and encryption keys, your authentication password is never stored on disk or in the volume file; not even in encrypted format. This is important, because your data is safeguarded against programmer attacks. Fur-

ther, since password changes do not entail re-encrypting your data, you do not have to wait around for the changes to take place. All password changes are instantaneous.

This dialog can also be displayed using a button on the map volume wizard.

Figure 20. Change Volume Password

Password changes are accomplished using the ***Change SafeHouse Password*** wizard. You can run this program either directly from its icon, or by selecting the corresponding button on the *map volume* dialog.

It's generally a good practice to change your volume passwords every 30 to 60 days.

NOTE: Remember your passwords. PC Dynamics cannot help you recover lost passwords.

Resizing SafeHouse Volumes

See also:
- SDWEXPAN.EXE

As your SafeHouse encrypted volumes begin to fill up with data, you will likely want to make them bigger using the ***Resize SafeHouse Volume*** wizard. Volumes can be expanded or compacted (shrunk) as often as desired within the size limits established when the volume was created. You do not need to keep track of the size limits for your volume. The wizard will present you with the allowable range. If you've enabled automatic risizing for your volumes, this step may be unnecessary.

To change the size of a volume, you must first authenticate yourself using your password , and possibly, an optional hardware device if such a device is usually required for *mapping* the volume to a drive letter. Once authenticated, you simply indicate the new size for the volume and let the wizard make the required changes. This process usually takes less than a minute. Please note that volumes that have been manually reformatted to **NTFS** on Windows NT/2000/XP cannot be resized.

Figure 21. Resize SafeHouse Volume

Run the ***Resize SafeHouse Volume*** wizard to increase a volume's size.

On the initial wizard page, select the target volume and enter your password, then press the ***Next*** button.

The maximum size is set when the volume is created.

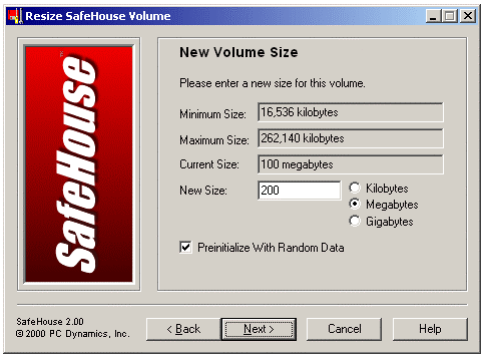


Figure 22. New Volume Size

The *Maximum Size, Minimum Size* and *Current Size* fields can be used to help you choose a new size that's within the allowable range for the volume.

The maximum will be either the expansion limit for the volume that was set when the volume was created, or the amount of remaining hard drive space left on your host drive, whichever is smaller.

The minimum size will be either the minimum volume size limit established when the volume was created or the smallest size that can be accommodated based on file allocations within the volume. To achieve the smallest possible volume size, first map the volume and run a drive optimizer on it.

The *Preinitialize with Random Data* checkbox instructs SafeHouse to fill the newly-allocated space with random data to make it more difficult for intruders to determine which areas of the virtual volume contain live data.

Figure 23. New Volume Size

The final wizard page is where the actual expansion or compaction is performed. Press the ***Expand Volume*** button (or Shrink Volume) when you are ready to begin. The time needed depends on the choices you've made; however, it is usually no longer than one minute.

TIP: For maximum performance, optimize (defragment) your host drive (C:) after expanding.

If you would like to make a volume smaller, it is recommended that you map the volume to a drive letter and run the Windows drive optimizer on it in order to free up as much space as possible at the end of the virtual volume. By doing this, you will maximize the amount of hard drive space able to be reclaimed since SafeHouse does not itself attempt to shift files toward the front of the virtual disk as part of this process.

Changing ActivCard Keys for SafeHouse Volumes

See also:
- SDWACTIV.EXE

If you feel your data warrants extra protection beyond the use of simple passwords, you might consider using an *ActivCard* authentication token as an additional step for gaining access to your encrypted volume. *ActivCards* look like small handheld calculators which are about the size of a credit card. Each one contains a unique service key which acts like a "secret" serial number. By adding *ActivCard* to your authentication process, access to your data will require both a password and possession of the *ActivCard*. The procedure for authenticating yourself with an *ActivCard* is described in Appendix C.

The primary benefit of the *ActivCard* authentication token is that since both the password and token are required to access a volume, if either one is stolen, your data is still safe because one isn't good without the other. This also means that you can lend a friend or coworker an *ActivCard* token to gain access to a specific encrypted volume, and revoke their right to access the volume simply by asking them to return the token.

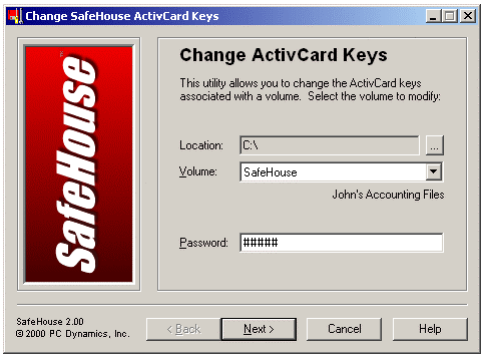


Figure 24. Change ActivCard Service Keys

Run the ***Change SafeHouse ActivCards*** wizard to add, edit or delete *ActivCard* service keys.

On the initial wizard page, select the target volume and enter your password, then press the ***Next*** button.

You might notice that the screen shown below is very similar to the *ActivCard* service key screen which appears within the create volume wizard. This is because SafeHouse allows you to initialize these keys from either utility. Once a volume is created, either with or without using ActivCard authentication, any further maintenance of the *ActivCard* keys requires using the ***Change SafeHouse ActivCards*** wizard.

SafeHouse supports up to 5 ActivCards.

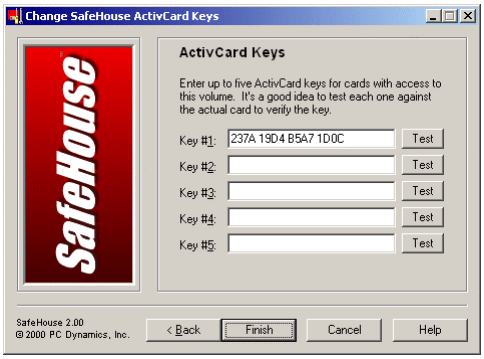


Figure 25. Enter Service Keys

Fill in up to five *ActivCard* service keys to be associated with the volume. All keys have the same priority.

Test each key to verify your entry.

Press ***Finish*** to exit the wizard.

The ***Test*** button next to each service key field performs a simulated *ActivCard* challenge/response authentication as described in Appendix C of this manual. It is very important to perform this sanity check because typing in a wrong number could lock you out of your own data. By performing this test, you will know for sure that the service key you input does indeed match the secret service key contained within your *ActivCard*.

To eliminate the need for *ActivCard* authentication on a volume once such has initially been established, run this wizard and set all the key fields to blanks. From then on, your volume will be accessible using only a password.

Visit http://www.activcard.com for more information about ActivCard devices.

Viewing and Changing 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 as explained in Chapter 6.

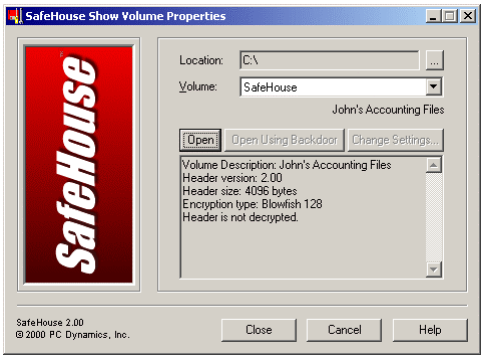


Figure 26. Show Volume Properties

This screen shows the information presented prior to authentication. After authentication, many more items will be listed in the scrolling window.

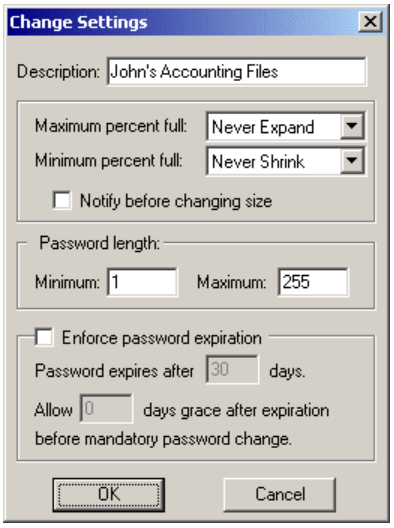


Figure 27. Change Volume Properties

Once you are authenticated, press the ***Change Settings*** button to display this dialog which allows you to make various adjustments to your volume's properties.

The meanings of these fields are the same as described previously for the ***Create SafeHouse Volume*** wizard.

Using the SafeHouse Volume Monitor

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.

Figure 28. SafeHouse Volume Monitor

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.

Removing SafeHouse from your PC

See also:
- REMOVE.EXE

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.

It is important to note that removing SafeHouse from your PC does not routinely remove or delete your encrypted volume files; provided, that is, that you do not keep your volumes in the SafeHouse programs directory. Volume files are treated similarly to word processing documents, whereby you are allowed to remove or change your word processor without having all your documents deleted in the process.

Automatically Removing SafeHouse

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

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

2. Run the **REMOVE.EXE** wizard utility located in your SafeHouse directory by double-clicking its icon from within your program manager. This same utility may also be launched using the Control Panel's ***Add/Remove Programs*** applet.

Manually Removing SafeHouse

If for some reason you find it necessary to manually remove SafeHouse from your PC, please follow these steps:

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

2. Delete the files and directory entry on your hard drive for SafeHouse. This directory is frequently named **C:\Program Files\SafeHouse**.

3. Delete your SafeHouse encrypted volumes. These volumes are usually located in your root directory and have **.SDSK** extensions. Note that some volume files may be marked as hidden.

4. Use **REGEDIT** to remove the registry entries for SafeHouse these keys: HKEY_LOCAL_MACHINE\Software\PC Dynamics\SafeHouse16 and HKEY_CURRENT_USER\Software\PC Dynamics\SafeHouse16

PC Dynamics strongly recommends against trying to modify the registry by hand unless your are extremely familiar with making these kinds of changes. Please make every effort to use the **REMOVE.EXE** utility.

Chapter 5

Commands and Options Reference

Can a software product really be complete without a bunch of command line slash options? Not this one. But that doesn't mean you need to read about them. Unless you're a programmer, skip over this section.

SafeHouse includes a rich set of commands and options to assist you in automating various tasks which you perform often. If you're running Windows, the SafeHouse wizards are your best bet for working with encrypted volumes. However, if you're a programmer or have a need for extensive command automation, this chapter contains the complete command syntax and options reference.

Use command line options to customize the behavior of the Windows wizards.

Listed below are the Windows programs used for working with SafeHouse encrypted volumes.

Almost every wizard fill-in field has a corresponding command line slash option.

SDWCREAT.EXE	Windows wizard to create encrypted volumes.
SDWCHANG.EXE	Windows wizard to change encrypted volume passwords.
SDWMAP32.EXE	Windows wizard to map and unmap encrypted volumes to Windows drive letters.
SDWACTIV.EXE	Windows wizard to change the ActivCard service keys for volumes.
SDWSHOW.EXE	Windows utility to show information about volume files.
SDWMON32.EXE	Windows program to disable volumes on idle timeouts.
SDWEXPAN.EXE	Windows wizard to resize volumes.

Common Command Line Options

Listed below is the complete set of command-line parameters for working with Safe-House encrypted volumes. Not all parameters are valid for all commands. Command parameters are not case sensitive. Complete descriptions, syntax and examples for each option are presented later in this chapter.

Long filenames must be enclosed in quotations. Additionally, 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**.

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

Parameters requiring embedded spaces must be enclosed in double quotes.

Slash Option	*Description*
/Activcard	Specifies an ActivCard service key.
/AUTOExpand	Specifies how full a volume must be before it is expanded.
/AUTOSHrink	Specifies a threshold for automatically shrinking a volume.
/AUTOSIzenotify	Specified if the user is notified when a volume will be expanded.
/Changekeys	Identifies the filename for a volume to change ActivCard service keys.
/CHangepassword	Identifies the filename for a volume to change passwords.
/CReate	Identifies the name of a volume to be created.
/DEscription	Specifies the long name description of a volume being created.
/Drive	Specifies the DOS drive letter associated with a volume.
/ENcryption	Specifies the encryption method.
/EXPANdableto	Specifies the maximum expansion limit of a volume.
/Expandvolume	Identifies the filename for a volume to have its size increased.
/EXPIres	Specifies the number of days between forced password changes.
/EXPLORE	Launch Explorer window for volume after mapping.
/FILESYSTEM	Specifies the hard drive format internal to a volume.
/FINISH	Complete command without user interaction if possible.

Command options are not case sensitive.

/FORCE	Force unmap even though some files may be open.
/GO	Automatically begin processing command without user interaction if possible.
/Grace	Specifies the grace period on forced password changes.
/HIdden	Set the Windows hidden file attribute on created volumes.
/Map	Map volume to a Windows drive letter.
/MAxpassword	Sets the maximum length of a password.
/MInpassword	Sets the minimum length of a password.
/Newpassword	Specifies a new password.
/Password	Specifies a current password.
/Quickcreate	Force rapid create mode.
/Quickexpand	Force rapid expand mode.
/READONLY	Force read-only mode for volume mapping.
/REMovable	Map as removable drive instead of fixed disk.
/SHELL	Right-click menu system use only.
/SHORTCUT	Force or prevent creating mapping shortcut
/SILENT	Complete command silently in background.
/SIze	Specifies the size of a volume.
/SOUND	Enables use of WAV sound support
/STOP	Remove SDWMON32.EXE from memory.
/Unmap	Unmap a currently mapped volume.
/USEPASSWORDDLL	Use DLL API to get password instead of dialog box.

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.

Using the SafeHouse CONFIG.INI File

This DAT file saves your preferences.

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 parameters. 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 INI file:

Parameters must follow the name=value standard for INI files.

Example: GO=1

```
[SDWMAP32]
      map=c:\mydisk.sdsk

[SDWCREAT]
      description=My Confidential Files
      expandableto=128
      quickcreate=1

[SDWEXPAN]

[SDWACTIV]
```

Restricting Available Encryption Algorithms

It is often desirable in corporate environments to restrict the use of certain encryption algorithms. You can prevent one or more encryption algorithms from appearing in the create volume encryption selection list by creating a section named **[ENCRYPTION]** in your **CONFIG.INI** file and including a reference for each algorithm that should not be presented to the user as an available choice. The required syntax is shown below.

```
[ENCRYPTION]
      DES=0
      BF32=0
```

Encryption codes supported by this feature: DES, DES40, FAST, BF32, BF48, BF56,BF128, BF448, TDES128, TDES168, RJ128, RJ256, 2F128 and 2F256. These codes have identical meanings to the codes described for the **/Encryption** option.

SDWCREAT.EXE

Icon: ***Create SafeHouse Volume***

See also:
- Creating SafeHouse Encrypted Volumes

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.

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:

/SOUND
/SILENT
/GO
/FINISH
/Create
/DEscription
/Password
/Size
/ENcryption
/Hidden
/Quickcreate
/EXPIres
/Grace
/MInpassword
/MAxpassword
/ActivCard
/EXPAndableto
/AUTOExpand
/AUTOSHrink
/AUTOSIzenotify
/FILESYSTEM
/SHORTCUT

SDWMAP32.EXE

Icons: ***Map SafeHouse Volume*** *and* ***UnMap SafeHouse Volume***

See also:
- Mapping and UnMapping SafeHouse 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:

/SOUND
/SILENT
/GO
/Password
/Map
/Unmap
/Drive
/READONLY
/REMovable
/FORCE

SDWCHANG.EXE

Icon: ***Change SafeHouse Password***

See also:

- Changing SafeHouse Volume Passwords

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

/Changepassword
/SOUND
/SILENT
/GO
/Password
/Newpassword

SDWEXPAN.EXE

Icon: ***Resize SafeHouse Volume***

See also:

- Increasing Volume Size

This utility is used to change the size of an encrypted 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:

/SOUND
/SILENT

/GO
/FINISH
/Expandvolume
/Password
/Size
/Quickexpand

SDWACTIV.EXE

Icon: ***Change SafeHouse ActivCards***

See also:
- Changing ActivCard Keys

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

/SOUND
/SILENT
/GO
/Changekeys
/Password
/Activcard

SDWSHOW.EXE

Icon: ***Show Volume Information***

This utility is used to display various volume information, attributes and properties. Certain public information is available at all times and does not require a password. Other more sensitive information is only displayed after the volume's password is provided.

This program also allows certain volume policy changes for the policies originally established with the create volume wizard. Such includes minimum and maximum password lengths, expiration times and automatic volume expansion parameters.

Optional command line parameters:

None

SDWMON32.EXE

Icon: ***SafeHouse Volume Monitor***

This utility can be used to automatically disable access to mapped encrypted volumes after a specified idle timeout. Once disabled, the volume's password will be required to regain access to the drive.

This program automatically attaches itself to the RUN= registry setting. It will run transparently in the background each time Windows is started.

Optional command line parameters:

/STOP

REMOVE.EXE

Icon: ***None***

This utility is run to completely remove SafeHouse from your system. You may run this program by double-clicking its name or icon within your desktop manager or using the Control Panel's *Add/Remove Programs* applet.

The **REMOVE.EXE** program will display a series of wizard pages offering to:

- Delete all SafeHouse program files and corresponding disk directory.
- Remove your Windows Start menu shortcuts.

Optional command line parameters:

None

Command Line Options

This section describes each of the command line options supported by the various SafeHouse utilities. The options are listed in alphabetical order.

Please note that not all options are meaningful to all SafeHouse executables. However, the naming, syntax and purpose of options are consistent across all the utilities.

TIP: When specifying options, you need only supply enough letters to be unique amongst the other options supported by the corresponding utility. Names are not case sensitive.

/Activcard

/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:

SDWCREAT.EXE
SDWACTIV.EXE

/Autoexpand

/Autoexpand=NN

Specifies if the volume being created should be expanded automatically each time it is mapped if it is filled beyond the threshold percentage. For example, specifying 75 will cause SafeHouse to try to keep the volume at least 25% free. The free space check and potential volume expansion occurs only during the mapping process. The maximum lifetime size of a volume is still restricted to the maximum size specified during create.

Examples:

/Autoexpand=50
/Autoexpand=90

Utilities supporting this option:

SDWCREAT.EXE

/Autoshrink

/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 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 ap-

proximately 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

/Autosizenotify= ON | OFF

Specifies if the user should be notified when SafeHouse is about to automatically expand or compact a volume. The default is not to notify the user.

Examples:

/Autosizenotify=Y

Utilities supporting this option:

SDWCREAT.EXE

/Changekeys

/Changekeys=filepath

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

/Changepassword

/CHangepassword=d:\filename.ext

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

Examples:

/Change=”c:\documents\test.sdsk”
/CH=c:\mydrive.sdsk
/changepass=d:\active.sdsk

Utilities supporting this option:

SDWCHANG.EXE

/Create

/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 icon. This parameter is optional.

The target filename must be a fully-qualified filepath beginning with a drive letter. By convention, encrypted volumes must 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

/DEscription="My Volume Description"

Allows you to specify the long internal name or description of an encrypted volume in advance on the command line. This parameter is optional. If the description contains spaces, then it must be surrounded by quotes.

Examples:

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

Utilities supporting this option:

SDWCREAT.EXE

/Drive

/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:

SDWMAP.EXE

/Encryption

/ENcryption= DES | DES40 | FAST | BF32 | BF48 | BF56 | BF128 | BF448 | TDES128 | TDES168 | RJ128| RJ256 | 2F128 | 2F256

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 that do not support long keys). This parameter is optional.

Blowfish (BF32, BF48, BF56, BF128, BF448)

Blowfish is fast, supports long keys, and is well-respected in the industry. Blowfish runs nearly 20x faster than **DES**. SafeHouse offers several different Blowfish key lengths: 32, 48, 56, 128 and 448. Each version runs at the same speed. The various key lengths are required for compliance with certain export control laws. The 448-bit version is not supported by SafeHouse's administrative key recovery features.

Twofish (2F128, 2F256)

Twofish was designed by the same scientist who invented Blowfish. Although it has not been around as long as Blowfish nor subjected to the same level of scientific scrutiny, it was a finalist in the NIST competition for choosing a new national encryption standard and is generally regarded as being superior to Blowfish in quality and speed. Twofish is available in two strengths: 128 and 256 bits. Only the 128-bit key size is compatible with SafeHouse's administrative key recovery features.

Rijndael (RJ128, RJ256)

The Rijndael algorithm was selected by NIST in October, 2000, to become the new official Advanced Encryption Standard **(AES)** for use within the U.S. Government. Rijndael is available in two strengths: 128 and 256 bits. Unlike Blowfish and Twofish, this algorithm takes longer to process at higher key strengths. The 256-bit version is approximately 40% slower than the 128-bit version. Only the 128-bit version is compatible with SafeHouse's administrative password recovery features.

DES

DES stands for **Data Encryption Standard**. This algorithm has been around for over 25 years and is now believed to be vulnerable to attack since its key size is only 56 bits.

DES40

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 to certain restricted countries. **DES40** runs at the same speed as normal **DES(56).**

Triple DES (TDES128, TDES168)

Triple DES is three rounds of **DES**. Each round uses a different permutation of your password. The algorithm is secure, yet very slow. Only the 128-bit version is compatible with SafeHouse's key recovery features. Blowfish, Twofish and Rijndael are usually better choices than **triple DES** when you have the opportunity to make a choice.

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. It should be noted that this algorithm was originally developed a decade ago when PCs were much slower and **DES** introduced a significant performance impact on the system. **FAST** is included here primarily for legacy support. New SafeHouse users are encouraged to consider using Twofish or Blowfish as a replacement.

Examples:

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

Utilities supporting this option:

SDWCREAT.EXE

/Expandableto

/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

/Expandvolume

/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

/Expires

/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

/Explore

/Explore

Use this option to automatically launch the Windows Explorer shell window for the volume after mapping an encrypted volume to a drive letter. SafeHouse normally defaults to adding this option to your drive mapping shortcuts, however, if you are getting extra popup windows, then remove this option. The reason it is possible to see two popup windows after mapping a drive is that newer versions of Windows detect when new fixed disks are introduced and automatically display a corresponding Explorer window. By not including this SafeHouse option, you eliminate one of the windows. Please note that Windows does not automatically pop up an Explorer window when volumes are mapped using the **/REMOVABLE** option. If you are trying to prevent any windows from showing up, remove the **/EXPLORE** option and use **/REMOVABLE**.

Examples:

/Explore

Utilities supporting this option:

SDWMAP32.EXE

/Filesystem

/Filesystem= AUTO | FAT12 | FAT16 | FAT32 | NONE

Use this option to specify the internal file system format of a volume when it is being created. If you specify **AUTO**, then SafeHouse will choose the best format based upon your operating system and volume size requirements.

Examples:

/Filesystem=AUTO
/Filesystem=FAT32

Utilities supporting this option:

SDWCREAT.EXE

/Finish

/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.

See also:

- /Go option
- /Silent option

Examples:

/Finish

Utilities supporting this option:

SDWCREAT.EXE
SDWEXPAN.EXE

/Force

/Force=[Yes | No]

Specifies that the standard alert displayed by SafeHouse when unmapping volumes with open files should be suppressed. By default, for safety, SafeHouse will present a warning when unmapping volumes with open files; however, sometimes this message may be undesirable. By using this option in combination with **/UNMAP**, these messages can be suppressed. This option is often useful on Windows NT/2000 since Explorer holds an open file whenever a directory window is showing, hence unnecessarily triggering this alert.

Examples:

/force

Utilities supporting this option:

SDWMAP32.EXE

/Go

/GO [=ON | OFF]

See also:
- /Silent option
- /Finish option

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:

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

/Grace

/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

/Hidden

/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 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

/Map

/Map [=d:\filename.ext]
Specifies in advance on the command line that the desired operation is to map a drive volume. The **/MAP** parameter 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.

Examples:

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

Utilities supporting this option:

SDWMAP32.EXE

/Maxpassword

/MAxpassword=NN

See also:
- /Minpassword option

Specifies the maximum length for volume passwords. The default value is **255**. Valid numbers range from **1** to **255**.

Examples:

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

Utilities supporting this option:

SDWCREAT.EXE

/Minpassword

/MInpassword=NN

See also:
- /Maxpassword option

Specifies the minimum length for volume passwords. The default value is **1**. Valid numbers range between **1** and **255**.

Examples:

/MI=8
/minpassword=5

Utilities supporting this option:

SDWCREAT.EXE

/Newpassword

/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. The quotes are required.

It should be noted that this command line feature is provided primarily to support scripting and silent program execution. Care should be taken to make sure that live passwords are not stored in easily-accessible scripts.

Examples:

/Newpass="sail$away"
/N="my new password"
/n="telephone.rope"

Utilities supporting this option:

SDWCHANG.EXE

/Password

/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 shortcuts since such would allow easy access for intruders.

SafeHouse utilities will prompt for unspecified passwords.

By default, passwords are between **1** and **255** characters and may include letters, numbers and punctuation symbols. The quotes 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="2345 my secret"
/P="birds.nest"
/pass="saved by the bell"

Utilities supporting this option:

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

/Quickcreate

/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

/Quickexpand

/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:

SDWEXPAN.EXE

/READONLY

/READONLY

This option is used to indicate to SafeHouse that you wish to map a volume for read-only access. This has two primary results. First, SafeHouse will not attempt to write timestamp information back to the volume file; and second, SafeHouse will not place an exclusive file lock on the file which otherwise would prevent the volume from being shared by more than one user at the same time over a local area network. This op-

tion is sometimes required when creating mapping shortcuts for volume files residing on CD ROMs or making volumes accessible to more than one user at a time.

Examples:

/READONLY

Utilities supporting this option:

SDWMAP32.EXE

/REMovable

/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:

CONFIG.INI Sample:

```
[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*. You can download this file from the SafeHouse web site by clicking on the following link:

http://www.pcdynamics.com/SafeHouse/config.ini

Examples:

/REMOVABLE

Utilities supporting this option:

SDWMAP32.EXE

/Shell

/SHELL

This option is used to inform the utilities that they are being run from the Explorer shell's right-click menu. This allows the programs to make slight adjustments in their behavior and messages. Normal shortcuts should not specify this option.

Examples:

/Shell

Utilities supporting this option:

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

/Shortcut

/SHORTCUT= [ON | OFF]

Specified whether or not a volume mapping shortcut will be created on your desktop when running the create volume utility. The default state is **ON**.

Examples:

/ SHORTCUT =YES
/SHORTCUT=no

Utilities supporting this option:

SDWCREAT.EXE

/Silent

/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.

See also:

- /Go option
- /Finish option

Examples:

/Silent
/silent

Utilities supporting this option:

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

/Size

/Size=NNN [MB]

Default values are assumed to be KB

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 size is 4 Gigabytes.

The maximum supported volume size is 4 Gigabytes (4,000MB) 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

NOTE: **SDWEXPAN.EXE** also has a **/Size** option, but the meaning is slightly different. When resizing volumes, the **/Size** parameter is used to specify the new size of the volume in megabytes.

/Sound

/SOUND [=ON | OFF]

You will find a variety of sound files in your SafeHouse disk directory.

Enables or disables playing of sounds upon command completion. Separate sound 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.

Sound File	*Description*
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 SDWMAP.EXE after successfully mapping a volume.
SDWMF.WAV	Played by SDWMAP.EXE after failing to map a volume.
SDWUS.WAV	Played by SDWMAP.EXE after successfully unmapping a volume.
SDWUF.WAV	Played by SDWMAP.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.

Several example sounds are installed automatically by setup.

Examples:

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

Utilities supporting this option:

SDWCREAT.EXE
SDWMAP32.EXE
SDWCHANG.EXE
SDWEXPAN.EXE

/Stop

/STOP

This option is used to force the volume monitor program to terminate and remove itself from memory.

Examples:

/Stop

Utilities supporting this option:

SDWMON32.EXE

/Unmap

/Unmap [=d | =ALL]

Specifies in advance on the command line that the desired operation is to unmap a drive. This parameter is optional. It may also 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=d: /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

/Usepassworddll

/Usepassworddll

Specifies that the program should query a special DLL API interface to obtain the volume password instead of displaying a dialog. The password provider DLL must always be named **SAFPWD32.DLL**. Please contact PC Dynamics or check our web site for specifications on this interface and sample DLL source code. This information is made available only to qualified site license customers.

Examples:

/Usepassworddll

Utilities supporting this option:

SDWMAP32.EXE
SDWCREAT.EXE

Chapter 6

SafeHouse Administration

SafeHouse contains a variety of features to aid administrators in deployment and password recovery. If you're in charge of setting up SafeHouse throughout your company, be sure to read this chapter.

SafeHouse includes a number of features designed to help administrators configure, deploy and support its software. If you are a system administrator or otherwise charged with deploying SafeHouse throughout your company, the information contained within this chapter will prove to be invaluable as you begin the process of enterprise deployment. If you are not in charge of administering SafeHouse, or you are running a single-user system, you can skip this chapter.

NOTE: This feature is not available for key lengths above 128 bits.

Administrative Domains

One of the first decisions you will need to make as the overall SafeHouse administrator is the determination of your *administrative domains*. A domain is a territory. In a small company with just a few dozen PCs located within a single building, you may decide that your entire company will operate as a single SafeHouse domain. In larger companies, it may be easier to establish domains by geographic regions, or possibly by departments and job classifications. If your company already has a security department or structured software administration, your SafeHouse domains should be chosen to conform to your existing hierarchies.

Administrative domains segregate classes of users.

The purpose of administrative domains is to establish manageable groups of users and to segregate the features and files made available to those groups. The most obvious use of domains is for encrypted volume password recovery. An administrator is assigned to each domain and authorized to help users recover their lost passwords. Since each domain should have its own unique administrator password, a barrier exists which prevents administrators from recovering passwords outside of their respective territories. The benefit of this approach is that you could empower the sales manager

to recover passwords for anyone within his department, however, this same manager would not be able to recover passwords for people in the accounting department. Additionally, the company support center could be empowered to recover any password, subject to your security policies, when department managers are not available.

The second purpose of domains is to establish separate security policies for various groups of users. For example, your normal policy on passwords might require a minimum of eight characters, however, senior executives might be required to use twelve characters because the information on their PCs is more sensitive.

Once you've chosen your domains you'll need to generate a set of SafeHouse files to distribute to the users within those domains. Each domain requires its own set of marked files. We generally refer to this process as *branding*. Branded files contain the special information needed to allow administrators to recover lost passwords.

Branding SafeHouse Files for Password Recovery

Branding is the process of marking, or updating, the original set of SafeHouse distribution files with special keys and administrative messages. Not all files need branding. At present, only **SDWLIB.DLL** gets updated. This file is then deployed in place of the non-branded version when installing SafeHouse throughout your organization.

Before you begin branding files you must perform a normal SafeHouse install which includes the administrative components. The administrator's tools are only needed on the administrator's PC. Normal users do not need any of these extra utilities, although it doesn't do any harm for them to be available.

If you will be using more than one administration domain, you should save copies of the non-branded version of **SDWLIB.DLL** to a temporary directory so that you can retrieve fresh copies before each branding procedure. You will need to run the branding wizard on the non-branded version of this file once for each domain to be created.

Figure 29. Brand SafeHouse Files

The branding wizard is run using the ***Brand SafeHouse*** icon. The first screen summarizes what's about to take place. Context-sensitive help is available at every step.

The files to be branded must reside in the same directory as the branding wizard. The default action during installation is to copy all files to **C:\Program Files\SafeHouse** which complies with the requirement.

Select ***Next*** to begin.

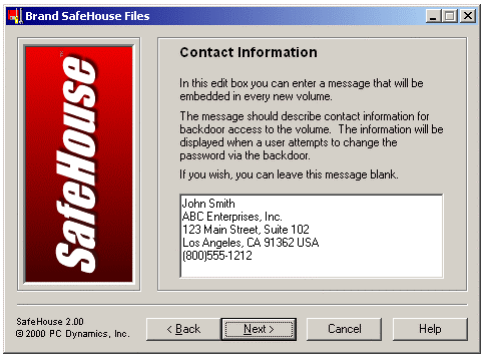


Figure 30. Contact Information

The first piece of information you are asked to provide is the administrative contact and description for the target domain. At the very minimum, you should include a name, phone number and domain identifier.

The message you enter here is embedded into every encrypted volume created with the branded fileset. It can be displayed by users at any time using an option built into the ***Change SafeHouse Password*** utility.

The contact information message can be any format you desire. The maximum length is 128 characters. An example of this sample being displayed for a user can be seen in the next section under password recovery. Use of this field is completely optional.

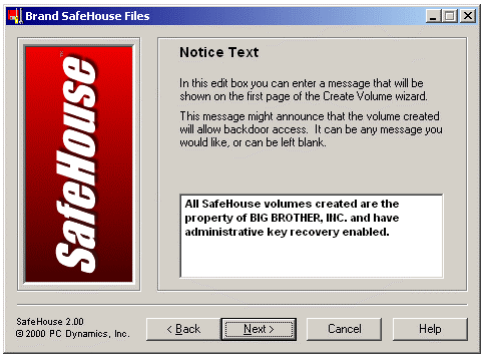


Figure 31. Notice Text Input

The next wizard page allows you to enter a multi-line text message which will be displayed on the first page of the ***Create SafeHouse Volume*** wizard.

You may enter any text up to 128 characters long. If you do not wish to display a special message during volume creation, leave this field blank.

Figure 32. Notice Text Display

This screen capture shows how the first page of the create volume wizard would look after being branded with the sample message shown above.

Figure 33. Administrative Passphrase

You are next asked to choose an administrator's *passphrase*. A passphrase is simply another word for password. We recommend that you create a normal sentence with proper punctuation which is at least 24 characters long.

Your passphrase is case sensitive and can be any combination of text, letters, numbers and punctuation. The maximum length is 999 characters.

Please be sure to write down your passphrase exactly as you typed it into this edit field. If you created an exceptionally long passphrase, you might find it convenient to copy it to the Windows clipboard and paste it into a text file created with **NOTEPAD**.

Your passphrase must remain secret. Anyone with knowledge of this phrase will be capable of accessing the encrypted volume content for all volumes created with this branded fileset.

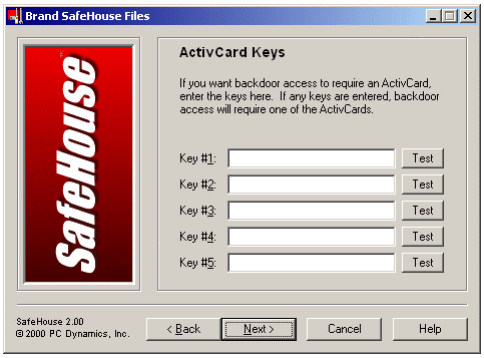


Figure 34. Optional ActivCard Keys

An optional feature for password recovery allows you to require that all recoveries be authenticated with an ActivCard challenge-response security token. By requiring ActivCard authentication in addition to the administrator's passphrase, you are protected from passphrase breaches which might be caused by disgruntled administrators. Leave these fields blank if you choose not to require the use of ActivCards.

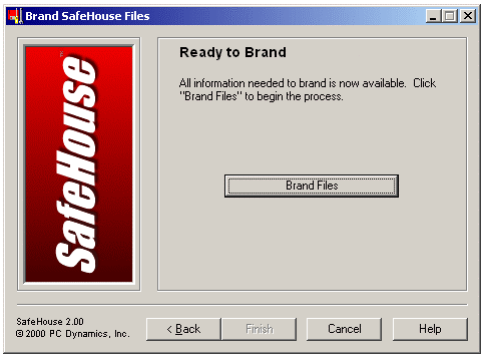


Figure 35. Final Screen

This is the final screen. If you are satisfied with all of your previous answers, press the ***Brand Files*** button to perform the file updates.

Before deploying your branded files, you should first check your messages and test the password recovery features as described in the next section.

Recovering Lost Passwords

Password recovery requires that you deploy branded SafeHouse files.

Administrators can recover lost passwords for encrypted volumes created using branded SafeHouse utilities as described in the previous section. If you lose the password for an unbranded encrypted volume, the password is lost forever. Please do not call PC Dynamics for help when this happens as we do not have any alternative capability to recover your lost passwords.

Before going much further, it is important to note that you cannot actually recover a specific lost password; but rather, you can recover from losing your password by choosing a new one. By using technique known as computing message digests, SafeHouse can determine if you enter the correct password without actually knowing the true password. The most obvious benefit of this technique is that hackers won't be able to find your passwords using disk scanning utilities. Another important benefit is that administrators cannot secretly snoop out passwords since the recovery process forces a password change, which would in turn alert the primary owner of the encrypted volume.

Administrator contact information lets users know where to go for help.

Figure 36. Backdoor Access

Password recovery begins by running the ***Change SafeHouse Password*** utility. You will find an option on the dialog's *System Menu* named ***Backdoor***. Choosing this item displays a message box similar to the one shown here on the left. If this item is dimmed, then the volume is not branded and password recovery is therefore not available.

TIP: The System Menu is displayed by clicking small icon located on the left-hand side of the wizard's caption bar.

One of the first things you should notice is that the contact information you entered during the branding process appears within this message box. This makes it easy for stranded users to find out who to call in case of emergency. This same information can also be used to help support personnel determine your administrative domain.

Pressing the button on this message box displays the initial recovery dialog.

SafeHouse supports two modes of password recovery. *Local recovery* requires that the administrator have direct access to the encrypted volume. This usually means being in close physical proximity to the troubled PC. *Remote recovery* allows administrators to as-

sist users over the telephone. Both methods have the same result and are equally secure. The primary difference is that remote recovery requires a few extra steps in order to avoid disclosing the administrator's password over the phone.

Local Password Recovery

Passwords can be recovered locally in less than 60 seconds.

Local password recovery requires that the administrator be able to walk up to the PC and type in their administrator's password. This is by far the most convenient of the two recovery methods.

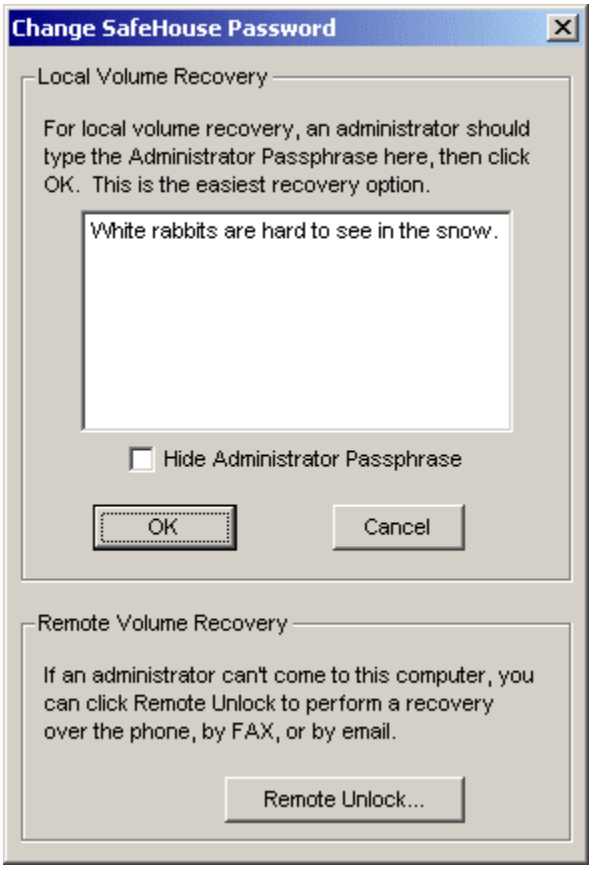


Figure 37. Local Key Recovery

The dialog shown here is the one displayed when you click the **OK** button on the *Backdoor* message box.

Enter the administrator's passphrase, or password, exactly as specified during the branding process. Then press **OK**.

Assuming the correct passphrase was provided, a message box is displayed informing you that the volume's password has successfully been changed to "password" (all lower case) and that you should immediately choose a new password.

That's it. You're done!

Please note that if ActivCard authentication for password recovery was specified during the branding process, then the administrator performing the recovery must have a corresponding ActivCard and respond correctly to an additional authentication dialog.

TIP: Some people find it convenient to use the Windows clipboard to paste long passwords into the edit field.

Remote Password Recovery

Never give your administrator's password over the phone.

Remote password recovery is used when the administrator is unable to directly access the troubled PC. The remote recovery dialog (below) is displayed by pressing the ***Remote Recovery*** button on the initial backdoor dialog as seen in the photo above.

The reason this procedure is slightly more involved than the local recovery method is that it is imperative that the administrator's password be kept secret. Without this second method, the administrator would have to disclose their password to the troubled user over the phone. It would then be possible for that user to access the encrypted volumes for all other users within their same domain.

The remote recovery procedure incorporated into SafeHouse employs the use of public/private key algorithms. You may already be familiar with these algorithms if you spend a lot of time on the Internet. The primary benefit of this technique is that only public information is openly exchanged. There is no need for secrecy as the troubled user and administrator perform the recovery.

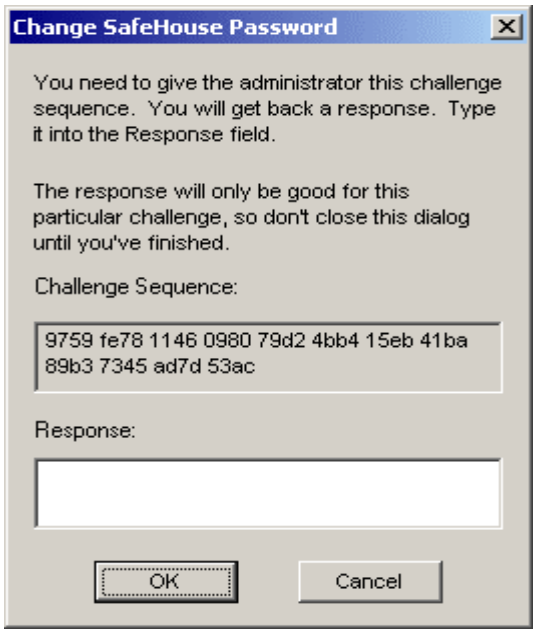


Figure 38. Remote Recovery for User

The first step in a remote recovery is to display this dialog window as described above.

The *Challenge Sequence* numbers are generated automatically by the program and must be communicated to the administrator. These numbers are always formatted as twelve four-digit values.

The administrator responds by providing a corresponding sequence of numbers which are entered into the *Response* field. Response values are presented as four four-digit values. Press **OK** to accept the response.

Please note that if ActivCard authentication for password recovery was specified during the branding process, then the administrator performing the recovery must have a corresponding ActivCard and respond correctly to an additional authentication dialog. Since only the troubled user has access to the PC, the ActivCard authentication must be done over the phone by voice between the user and the administrator. This does not present a security breach due to the algorithms employed by the ActivCard.

Remote Recovery from the Administrator's Perspective

When recovering passwords over the phone, it is necessary for the administrator to use a special utility designed just for this purpose. The **SDWULOCK.EXE** program is usually invoked using the ***Remote Password Recovery*** icon installed automatically by **SETUP** when administration components are selected. It is not necessary for normal users to have this utility. Further, this utility is completely useless without the administrator's password.

The administrator begins by entering their administrator's passphrase into the top edit field. This is the same passphrase selected during the branding process.

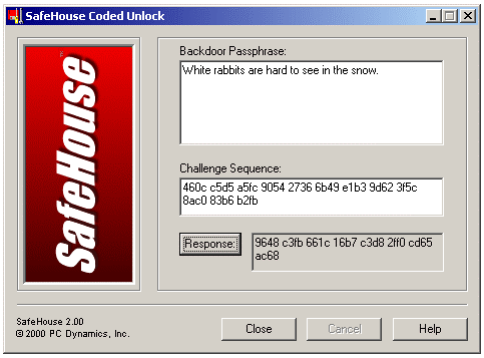


Figure 39. Admin Remote Recovery

Next, the *Challenge Sequence* field must be filled in with the values communicated by the troubled user. These numbers are always formatted as twelve four-digit values.

Press the ***Response*** button to generate the corresponding return codes which will be formatted as four four-digit values. These numbers must be communicated back to the user and input into their open dialog window.

Appropriate error messages are displayed if incorrect values are detected.

Note: The challenge digits generated by the user's program are one-time values. If the dialog window on the user's side is closed before entering the corresponding response codes, you will need to start over with new challenge sequence numbers.

Deploying SafeHouse throughout your Company

The **SETUP.EXE** program used to install SafeHouse can be customized using the SafeHouse ***Deployment Tool***. This file is named **DEPLOYHLP.EXE** and is included with all standard SafeHouse distributions.

Note: The deployment utility requires Windows NT, 2000 or XP. Installs run on all platforms.

The purpose of the deployment tool is to help administrators create customized versions of the standard SafeHouse installer that contain corporate default settings, preferences and custom files required to support features such as administrative password recovery. The deployment tool is implemented as a Windows wizard utility which is run using the shortcut located on the SafeHouse menu.

DEPLOYHLP.EXE must be run by administrators on Windows NT, 2000 or XP. The original SafeHouse **SETUP.EXE** or equivalent download installer program must be available as well since that file will be copied and then modified to include your custom settings. The wizard pages displayed by this utility contain full explanations of the choices and options available to you. Try running the tool a few times to get a feel for how it works before creating your final distributable installer. The resulting installer will run on all Windows platforms.

Silent Installs

Starting with SafeHouse 2.10, silent installs are supported by specifying **/silent** on the installer command line. This provides some flexibility when creating enterprise deployment scripts. When this option is specified, the SafeHouse installer does not automatically create an initial encrypted volume since such would require interaction with the user. If an initial volume is desired, you should create it in your deployment script after the standard installer finishes by calling the **SDWCREAT.EXE** program with an appropriate set of command line options.

Appendix A

Export Rules

New rules effective October 19, 2000, allow SafeHouse to be exported to the European Union plus 8 additional countries.

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 Australia, 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 immediately after submitting a commodity classification request to BXA, rather than waiting for the review and classification to be completed.

Please Visit our Web Site

Please refer to PC Dynamics' web site for the most up-to-date information on current export controls governing the distribution of SafeHouse.

http://www.pcdynamics.com/safehouse

Appendix B

Scripting and Exit Codes

The SafeHouse wizards can be scripted or run using custom shell programs written in Visual Basic or C++.

All of the standard SafeHouse utility wizards support being run from batch files **(.BAT)**, Windows Scripting Host scripts **(.VBS)**, Windows NT command files **(.CMD)** and custom-designed C++ or Visual Basic applications. In any of these environments, the wizards can be instructed to display fully- or partially-completed dialogs, or to not display any user interface at all and perform their tasks silently without a window. You can specify how you want the utilities to behave by using the command line options described in Chapter 5.

TIP: Running the SafeHouse utilities silently without a window requires using the /SILENT and /GO command line options in addition to the usual parameters required by each utility.

The SafeHouse utilities are designed to return a variety of process exit codes. These codes allow custom-created applications to silently perform a SafeHouse task and receive a return value indicating the success or failure status of the operation. Unfortunately, these codes are not available when using batch files or Windows Scripting Host scripts.

If you are an experienced programmer and require this fine level of control over SafeHouse, the accompanying table of exit codes and C++ sample program will help you to design specialized applications which can call upon the SafeHouse utilities to perform important tasks. Please note that even though we make this information available (because it is frequently requested), PC Dynamics will not generally provide programming assistance to you unless you have purchased an Enterprise Site License.

The sample C++ program is a command-line utility which takes a program name and variable list of arguments provided on the command line and creates a corresponding Win32 process. The sample waits for the child process to finish and then retrieves its exit code and writes it to the screen. In a real-world application, the child process would be one of the SafeHouse utilities. In fact, the sample can actually be used to run any of the SafeHouse utilities provides a convenient shell for experimentation.

SafeHouse Win32 Process Exit Codes

Listed below are the Win32 process exit or error codes returned by the SafeHouse utilities.

Code	*Description*
0	No error.
1	Canceled.
2	<Not Used>
3	Unknown error.
4	Internal error.
5	Invalid error code.
20	Disk error.
51	Your password has expired. You have X days left to change it.
100	Initialization failure.
101	Out of memory.
102	The SAFEDISK driver is not installed.
103	The SAFEDISK driver is not the right version.
104	Protected/Real mode failure.
110	Volume filename missing
111	Volume filename formatted incorrectly.
112	Volume cannot reside on map drive.
113	Volume file not found.
114	Cannot open volume file.
115	Cannot write to volume file.
116	Volume is not a SAFEDISK volume.
117	Volume is already in use.
118	Volume and SAFEDISK driver are incompatible versions.
119	Volume uses unsupported encryption algorithm.
120	Volume file resides on incompatible drive.
121	Volume file has been damaged and is unmappable.
122	Unable to lock volume file for mapping.
123	Unable to lock host drive for mapping.
124	Unable to lock SafeDisk drive for mapping.
125	Unable to communicate with compressed host drive.
130	Target drive missing.
131	Target drive is not a SAFEDISK drive.
132	Target drive is already in use.
133	No drive specified, but all drives are currently mapped.
134	There are files open on the target drive.
135	Cannot unmap drive - drives must be mapped and unmapped in the same VM.

Code	*Description*
140	Password missing.
141	Password is invalid length or contains invalid characters.
142	Incorrect password.
143	Password has expired, please change it before mapping this host file.
144	Verify password does not match original.
145	New password is not different.
150	Incorrect ActivCard response.
160	Lockbox file not found.
161	Cannot open lockbox file.
162	No valid password found in lockbox.
170	Filename is missing.
171	File already exists.
172	Size is missing.
173	Size is too large. Not enough space to create file.
174	Size is too large. Drives must be less than 2048 mb.
175	Size is too small, or expand limit is too large.
176	Size is larger than supported by the operating system.
180	Cannot change drive letters, invalid starting drive letter.
181	Cannot change drive letters, a SAFEDISK drive is mapped.
182	Cannot change drive letters, Windows is running.
184	Cannot change drive letters, a requested drive letter is in use.
190	Invalid size for drive expansion.

Sample C++ Application to Run a Program and Retrieve its Process Exit Code

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <string.h>
#include <windows.h>


int main(int argc, char *argv[])
{
	LPSTR cmdline, cmdargs;

	cmdline = GetCommandLine(); // program to run is specified on the command line

	// the returned string above includes the name of ourself, so advance past

	if (argc > 1 &&  (cmdargs = strstr(cmdline, argv[1])) != NULL)  {
		printf("Executing command: %s\n", cmdargs);

		PROCESS_INFORMATION ProcessInfo;
		STARTUPINFO StartupInfo;

		FillMemory(&StartupInfo,sizeof(StartupInfo),0);
		StartupInfo.cb = sizeof(StartupInfo);
		DWORD dwExitCode;

		if (CreateProcess(

			NULL,	// application to run defaults to using command line
			cmdargs, // command line args
			NULL,	// process attributes, cannot be inherited.
			NULL,	// thread atribs, cannot be inherited
			FALSE,	// new process does not inherit any handles from us
			CREATE_DEFAULT_ERROR_MODE | CREATE_NEW_CONSOLE |
					NORMAL_PRIORITY_CLASS,   // create flags
			NULL,	// default environment
			NULL,	// current directory is same as ours
			&StartupInfo,
			&ProcessInfo
			)) {

			printf("Waiting for process to terminate...\n");

			while (1) {
				GetExitCodeProcess(ProcessInfo.hProcess, &dwExitCode);
				if (dwExitCode == STILL_ACTIVE)
					Sleep(100);
				else
					break;
			}

			printf("\nProcess Exit Code: %d\n", dwExitCode);

		} else
			printf ("Create Process failed with error code %d.\n", GetLastError());
	} else
		printf ("Something is wrong.\n");

	return (0);
}
```

Appendix C

ActivCard Authentication for SafeHouse Volumes

It's commonly said that good security is based upon something you know, and something you have...

SafeHouse encrypted volumes may optionally be protected using an ActivCard hand-held personal security authenticator. ActivCards may be purchased either directly from ActivCard, Inc., or one of their resellers. By keying your SafeHouse volumes to an ActivCard, you will need both your secret password and possession of the ActivCard to gain access to your files.

See also:
- Creating SafeHouse Volumes
- Changing ActivCard keys

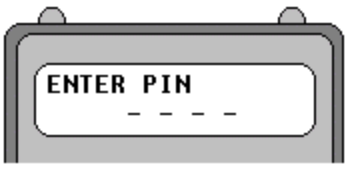
ActivCard security is based upon a technique known as *challenge-response authentication*. During each login or volume mapping, you will be presented with a numeric *challenge*. To be authenticated you must provide the corresponding single-use password *response*. The only way to arrive at the correct response is to use the ActivCard, which operates much like a small credit card size pocket calculator. Each ActivCard is delivered pre-programmed from the factory with a series of unique secret 56-bit *service keys* which guarantees that each card will generate a different set of responses to authentication challenges.

Responding to the ActivCard Authentication Dialog

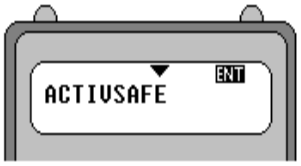
ActivCard authentication dialogs are presented automatically by SafeHouse after first validating your secret volume password.

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. Please follow the steps below to complete this process.

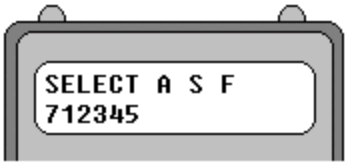
STEP 1. Turn on your ActivCard using the **ON/CE** key.



STEP 2. Enter your private PIN code and press **ENTER**.



STEP 3. Select the ActivCard *Service Name* for this authentication.. 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.



STEP 4. 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.

STEP 5. Press the **AUTH** key for authentication.

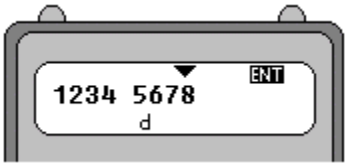
STEP 6. Type the challenge presented in the dialog and press **ENTER**.

Did you know that ActivCard can read the flashing optical patterns?

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.

Note: If you don't get a good transmission, press [ON/CE] to clear, then [AUTH], and try again.



STEP 7. The ActivCard then displays your one-time dynamic password as an eight-digit value. This is the number that must be typed 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.

STEP 8. Press the **OK** button on the SafeHouse dialog to finish.

That's it. You're done.

More Information on ActivCard

To find out more about using and purchasing ActivCards, please contact ActivCard, Inc. or visit their web site at http://www.activcard.com.

Appendix D

Troubleshooting

Having problems? Please look here before contacting PC Dynamics. Did you know you can get answers by email by writing to support@pcdynamics.com?

Problem: One or more Explorer windows are popping up after mapping volumes.

A new feature showing up in Windows and various web updates is that Windows will attempt to detect when new fixed drives are introduced to the system and automatically display an Explorer window showing the drives' contents. This can sometimes compete with SafeHouse's **/explore** option causing two windows to show up, or worse, show a window when you don't want any at all. The first thing to do to work around this event is to remove the **/explore** option from your SafeHouse mapping shortcuts. This prevents SafeHouse from popping up a window when Windows is already doing this for you. Alternatively, you can use the **/removable** option on your mapping shortcut to instruct SafeHouse to mount the volume as a removable disk drive instead of the default fixed disk drive mode. Although the differences between these two modes are subtle, the important difference that helps solve the popup window problem is that Windows does not automatically pop up Explorer windows for removable drives. See the description for the **/removable** option in Chapter 5 for more details on this problem.

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

The first version of SafeHouse that supports Windows XP is 2.10. Earlier versions will have trouble mapping volumes. Additionally, if you install SafeHouse on a Windows 95/98/Me machine and then subsequently upgrade to Windows XP or 2000, you will need to run the SafeHouse installer program again to allow SafeHouse to make some important driver adjustments. You do not need to uninstall SafeHouse and no changes will be made to your volume files. This procedure is necessary because the driver requirements of these operating systems are quite different.

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.

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 designed 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/2000/XP?

SafeHouse volumes appear to Windows NT/2000/XP as normal hard drives. This allows you to use the standard Windows **FORMAT.EXE** program to reformat 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 on the CD already has the read-only attribute set, then SafeHouse will know to automatically map the volume in read-only mode. If you find that this is not the case, you should check the *Read Only* checkbox when using the mapping utility, or alternatively, specify the **/READONLY** option on the **SDWMAP32.EXE** command line.

Problem: SafeHouse cannot write to volumes residing on CD-RW media.

SafeHouse is generally compatible with CD-RW media. If you experience problems, the first thing you might try is mapping the volumes in read-only mode and seeing if the problem is related to writing. If so, it may be a driver compatibility issue.

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 updateable only by the administrator, and the other is a recent 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 product's administrative password recovery feature – which must have been implemented in advance of creating the volume you are unable to access. See Chapter 6.

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.

Index