SafeGuard® Easy

Version 3.1

Data protection by encryption

Windows® 95/98,
Windows® NT 4.0, Windows® 2000,
Windows® XP

utimaco®
safeware

Imprint

Fon	+49 (6171) 88-0
Fax	+49 (6171) 88-1010
Internet	www.utimaco.com
E-Mail	info.de@utimaco.de
Author(s)	
Version	1
As of	März 2002
Translation	
Lectorat	

Table of Contents

Table of Contents

Table of Contents

Preliminary Remarks

The change from an industrial to an information society is progressing at an unstoppable pace. Work organization is also changing at rapid speed. In more and more companies, the rigid structures are loosening and jobs are becoming increasingly more mobile. Many employees have exchanged their desks in the company building for a tele-job and now work at home, at changing locations or remote offices.

Desktop-PCs and notebooks have thus become important information and communication media without which the new working world would be unthinkable.

These changes also involve an element of risk, however. Confidential information is often insufficiently protected and this means that it could be misused if it falls into the wrong hands. The damage caused to businesses in this way is often irreparable.

Sensitive company data is only really secure if it is encrypted. SafeGuard Easy closes this security gap for you, thereby offering you effective protection against attacks from the outside.

1 Introduction

Thank you for purchasing our security system SafeGuard Easy and we hope that you will be satisfied with our product. Should you have any comments or suggestions for improvement, then we would be grateful if you informed us of them.

Before starting SafeGuard Easy, please read this manual carefully.

Utimaco Safeware AG reserves the right to modify or amend the manual at any time without prior notification. Utimaco Safeware AG does not assume any liability for printing errors that may cause issue in the future.

To make the manual easier to use, we have marked important areas, information or examples using symbols. The symbols used are explained below:

Here, you will find important information that you should observe in every case.

Here, you will find additional or supplementary information.

Here, you will find an example.

You will frequently encounter text with the following notational conventions in the manual:

`Typewriter text` highlights file names and command names in the body of the manual text.

Italic text indicates menu items and dialogue headings.

<Text in Angle brackets> substitutes individual file names, folders etc.

In [Square brackets] buttons are displayed.

1.1 Support and Hotline

We are happy to support you in all matters regarding our products. For customers with a large userbase support and updates are regulated by maintenance agreements. Our training programs are open to all users. Please ask for our training schedule.

We also offer such services as security consultancy and implementation support. Please ask for our services on offer.

Please call the hotline only after extensive trial and error has not produced a solution for your problem. Prepare yourself for the call to our hotline. You need to have the following information:

- Model and type of your PC, as well as the RAM and hard disk size.
- Operating system and its release status.
- Name of the Utimaco Safeware product and its release status.

Please ask your local Utimaco distributor for the hotline number or visit our homepage:

http://www.utimaco.com

1.2 Organization of the manual

The manual comprises the following chapters:

Chapter 1 shows you in brief the advantages of SafeGuard Easy.

Chapter 2 gives you an overview of the performance spectrum of SafeGuard Easy. In addition to the program's properties, the basic functionalities of SafeGuard Easy is dealt with in more detail. In this way, you will gain an overview of the various areas of application.

In **Chapter 3** you will find out what you have to do to install and uninstall SafeGuard Easy properly.

Chapter 4 tells how to logon to the program.

In **Chapter 5** you will find information about working with the administration program, switching the encryption of floppies and removable media drives, creating configuration files and remote maintenance.

Chapter 6 shows how to remove system errors.

Chapter 7 shows how to upgrade SafeGuard Easy from former versions.

Chapter 8 contains all the error messages.

In **Chapter 9** you find answers to frequently asked questions.

In **Chapter 10** you find the glossary.

1.3 License Note

Any unauthorized duplication of the SafeGuard Easy manual or software will be liable to criminal prosecution.

The terms and conditions of the software license contract apply.

Other license notes:

STEALTH Encryption Copyright (c) 1994 Intelligence Quotient International Limited. All rights reserved. Patents pending. STEALTH encryption is a trade select of Intelligence Quotient International Limited.

Patent rights of Ascom Tech Ltd. given in EP, JP, US. IDEA is a trade select of Ascom Tech Ltd.

Credits:

Special thanks go to Dr. Brian Gladman, whose AES implementation we used as a base for building our AES encryption drivers."

1

2 What can SafeGuard Easy do?

Personal computers often contain personal data, confidential and company information or other sensitive data.

The danger which results from the theft of notebooks should not be underestimated. Highly sensitive client information on a sales representatives notebook could fall into the hands of a competitor resulting in serious damage for the company.

SafeGuard Easy is the ideal way to safeguard oneself against such risks without investing too much time in the implementation of security measures.

How does SafeGuard Easy protect workstations from unauthorised access? The program's essential security features are the drive encryption and the boot protection to prevent access to a workstation by using a external medium.

The biggest advantages of SafeGuard Easy are that the program

- protects the confidentiality of stored data simply but effectively
- can be implemented quickly
- is very user-friendly
- offers a security concept suitable for many different application areas.

SafeGuard Easy is easy to install. For this reason, it is particularly well suited for standalone systems and mobile units such as notebooks.

2.1 Security features

Encryption of drives

The principal item of SafeGuard Easy is the encryption of hard disk drives, floppy drives and removable media drives.

Encryption can be implemented with different keys using different algorithms (AES-128, AES-256, Rijndael-256, IDEA, DES, DES SB-II, Blowfish-8, Blowfish-16, STEALTH-40, XOR und XOR SB-I A=B) . After being defined, the key is encrypted and for reasons of security is not stored in the system. Each time the computer is booted, it is generated new from a code saved on the hard disk and the user password.

The system areas, individual partitions or a maximum of four hard disks can be encrypted SafeGuard Easy supports the following file systems: FAT-12, FAT-16, FAT-32, HPFS, NTFS and NTFS5.

The encryption of floppies and removable media drives provides the advantage that the entire data communication runs completely encrypted from the outside world.

Access control with Pre-Boot Authentication (PBA)

If Pre-Boot Authentication is switched on only SafeGuard Easy users are allowed to logon to a workstation.

Trying to start a workstation whose hard disk is encrypted from an external medium (floppy, removable medium) the hard disk remains encrypted. Starting the system is possible, but the hard disk cannot be accessed.

Boot protection

By using both PBA and boot protection it is not possible to start a workstation from an external medium without knowing the SafeGuard Easy user data.

Additional Functionalities

Multi-User System

SafeGuard Easy allows access to the system for up to 15 users: The user SYSTEM who is usually the system administrator and 14 other users. The user SYSTEM has unrestricted rights. Users identify and authenticate themselves by entering their SafeGuard Easy user name and password which then authorizes them to use the entire system.

Secure Auto Logon (SAL)

If SAL is activated, a user can log onto SafeGuard Easy and the operating system simultaneously by entering the SafeGuard Easy password in the PBA.

Protection of the Master Boot Record (MBR)

Using MBR protection, you can check the MBR for possible changes (e.g. viruses) every time you boot the system. You can determine how SafeGuard Easy is to respond if a change is detected in the MBR.

User Right “Boot from floppy allowed”

Only a user who has been given this authorization can boot a workstation protected with SafeGuard Easy from floppy disk.

Workstation lock

If no key is pressed and the mouse is not moved within the number of minutes defined, the screen is automatically blanked. The workstation can be unlocked by entering the SafeGuard Easy password.

Recording of critical SafeGuard Easy events (Windows NT/2000/XP)

SafeGuard Easy records certain security-relevant events in the event protocol of Windows.

Support of Plug-and Play drives

SafeGuard Easy supports hard disk drives and removable media drives which are connected by plug-and-play mechanism of Windows.

Increased Encryption Performance

First-time encryption is approximately 30% faster than earlier versions.

2.2 System Requirements

To enable you to use SafeGuard Easy efficiently, certain hard and software requirements must be met.

Hardware Requirements

Depending on the selected installation mode SafeGuard Easy requires hard disk memory space of between 5 and 15 MB.

The program can then be run without any problems on an IBM compatible workstation. SafeGuard Easy does not need more additional resources than Windows is using.

Although SafeGuard Easy will run perfectly on the system described, encryption has its price. It is therefore recommended that hardware to be used should exceed the minimum requirements listed.

Supported Operating Systems

SafeGuard Easy requires one of the following operating systems:

- Windows 95B / Windows 95C
- Windows 98/Windows 98 SE
- Windows NT 4.0 Workstation
  Windows NT 4.0 Server
  (incl. Service Pack 3 or higher)
- Windows 2000 Professional
  Windows 2000 Server
  Windows 2000 Advanced Server is *not* supported
- Windows XP Home Edition
  Windows XP Professional Edition

2.3 Notes

In running operation the following points should be considered:

- If the workstation is integrated in a peer-to-peer LAN, then parts of hard disks may not be assigned to other users of this LAN.
- When leaving the workstation for a short time the Windows NT/2000 screen blanking should be enabled (button [Lock workstation]); leaving the workstation for a longer period of time, the pc should be switched off and then rebooted.
- System administrators who start the administration program on the workstation of a logged on user, should close this before leaving the workstation.
- When the recommended installation system configuration is set correctly the logical access on hard disks after booting from floppies is prevented. To achieve additional protection of the system against the discovery of an SafeGuard Easy password with a “Trojan Horse”, the workstation should be protected against booting from floppy by means of a mechanical lock or another internal measure.

Encryption algorithms and keys for hard disk drive encryption cannot be changed once SafeGuard Easy installed.

3 Installing and Deinstalling

3.1 Preparing for Installation

Security Settings

Certain preparations must be made prior to installation:

Please read the following list carefully and ensure that you pay attention to all points.

- Hard disk drive encryption and decryption are protected against power cuts and similar disturbances. As soon as the power is returned, the process continues at the right place without the user having to do anything. Despite this, it is recommended that you backup your data carrier prior to installing SafeGuard Easy.
- Virus scanners should be switched off during installation/deinstallation.
- The partitions of your hard disk should be completely formatted and should have a drive letter assigned.
- Initial installation must be carried out by a user with Windows administrator rights.
- If the boot partition has been converted from FAT to NTFS and the system has not been reset by rebooting, SafeGuard Easy should not be installed. It is possible here that the installation will not be completed because the file system was still FAT at the time of installation while NTFS was found at the time of activation. In this case you have to do a one-time reboot before SafeGuard Easy is installed.

- SafeGuard Easy is being constantly developed further. This means that your version can contain new features which are not included in the manual or online help due to the editorial deadlines. These new changes or features are described in the `Readme.txt` file.

Installation Mode

Initial installation can be done in several ways – either interactively via CD or via a network, or without any user interaction by using a configuration file.

In general, the installation of SafeGuard Easy is carried out in two steps:

- The setup program copies the software onto the workstation's hard disk.
- The settings of SafeGuard Easy are configured during the installation process. You determine the type of installation of SafeGuard Easy here and give details of the general workstation settings, encryption method, user identities/rights and settings for the Master Boot Record's protection.

*To start SafeGuard Easy's installation you have to ensure that Microsoft Windows Installer is activated on your system. The file extension *.msi has to be connected to this application, too. Windows Installer is preinstalled on every workstation using the Windows 2000/XP operating system.*

For further informations about Windows Installer please have a look e.g. at Microsoft's homepage (http://www.microsoft.com).

With interactive installation and installation without user interaction, a warning is given whenever a Non-Dos partition type is found.

All disk packets fit again on single floppy disks. So installation of SafeGuard Easy from floppy disks is possible again.

Note

SafeGuard Easy does not support the Windows XP feature 'Fast User Switching'. After the installation of SafeGuard Easy the Welcome screen is switched off automatically.

3.2 Interactive Installation

Insert the SafeGuard Easy CD-ROM into your CD-ROM drive. If Autorun is activated, it is started from Windows when the CD-ROM is inserted into the drive. If the Autorun function is deactivated on your computer, you can start installation via the Windows Explorer by running `Setup.exe` in the subfolder `\disk1`.

A user who wants to install SafeGuard Easy interactively must have Windows administrator rights because the hard disk has to be accessed here and/or drivers and system services have to be installed which also require administrator rights.

The installation process for the interactive installation of SafeGuard Easy is described now.

First dialog box is opened

Install SafeGuard Easy	Starts installation of SafeGuard Easy
View Readme	Opens the `Readme.txt` file SafeGuard Easy is subject to on-going development. For this reason your version can contain innovations which were not included when this manual went to print or when the online help was being prepared. Such innovations are described in the `Readme.txt` file. Before installation you should therefore read the contents of this file carefully.
View manual	Opens the online manual
Install Acrobat Reader	To view the online PDF documents it is necessary to have Adobe Acrobat Reader installed.
Exit	Installation will be aborted.

The dialog box including the license agreements appears.

If you accept the license agreement, check it and continue. If not, the installation will be terminated.

☞ *Click [Next].*

The SafeGuard Easy *Welcome* dialog box appears.

Please read the information carefully!

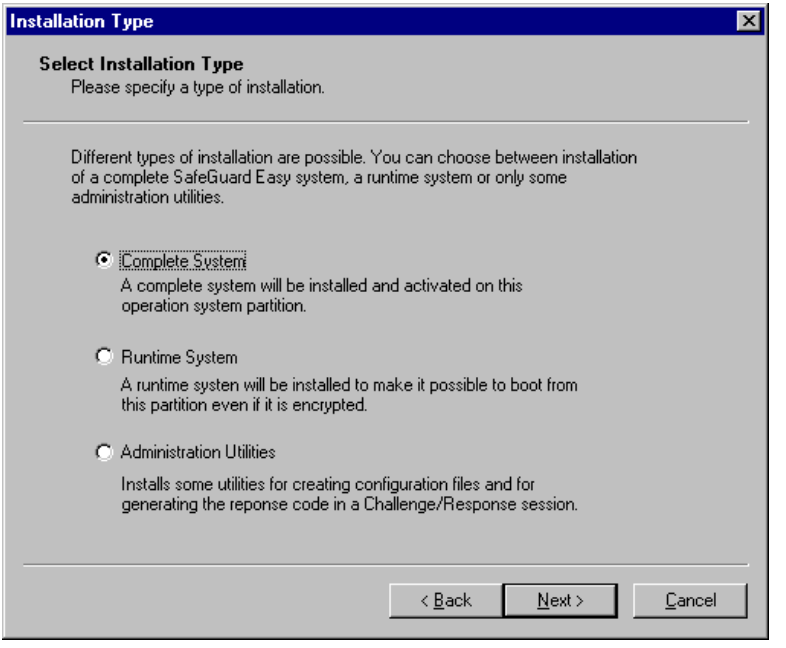
You will find a navigation strip at the bottom margin of every Safe Guard Easy installation dialog box. It contains the buttons

Back, **Next** and **Cancel**.
Back takes you back to the previous dialog box,
Next takes you on to the next dialog box,
Cancel ends the setup program without installing SafeGuard Easy.

☞ *Click [**Next**].*

3.2.1 Installation Type

The dialog box *Select Installation Type* appears.



Three options are available to you here. You can either install the complete system, prepare a minimum configuration or decide whether you only need programs for administration.

- **Complete System**
  The option "Complete System" installs SafeGuard Easy with all available components.

- **Runtime System**
  Runtime system installs programs which are necessary to enable booting from the corresponding partition if a complete version of SafeGuard Easy has been installed on another system partition. Additionally the tool for switching floppy and device encryption (SGECRYPT) is installed.

  Dualboot and Runtime System

  SafeGuard Easy can also be installed on hard disk drives with several Windows installations. To run the operating systems without any problems on one partition install type runtime system has to be installed, on the other one a complete system.

  Please pay attention to the following combinations of operating systems:

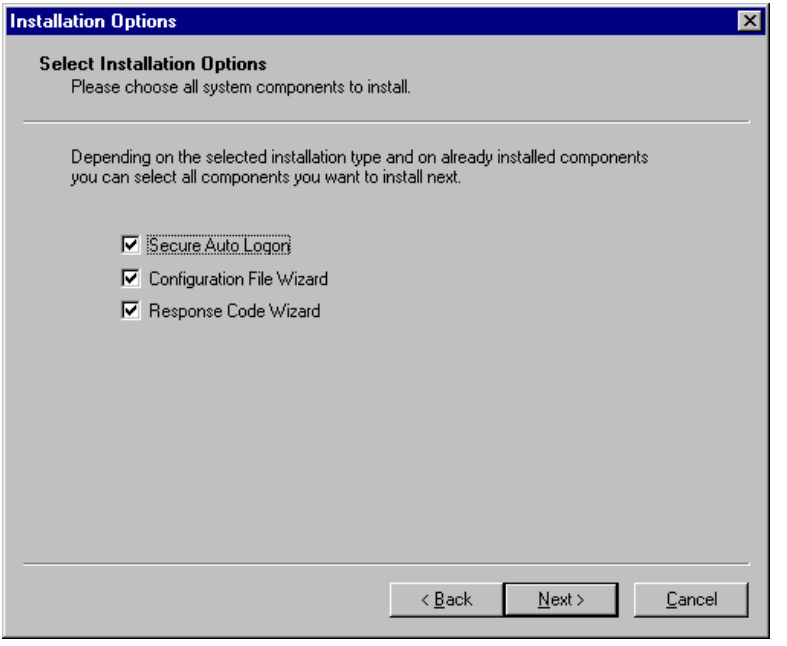
Any combination of **Windows XP** **Windows 2000** **Windows NT**	Determine e.g. a Windows installation for primary installation. Thereafter, boot all non-primary Windows installations in the mode Runtime System. Select a different directory for each installation. Finally, you have to boot your primary Windows installation in order to install SafeGuard Easy there as a Runtime System. Once encryption has been completed, you can then continue to boot all non-primary Windows installations.
Windows 95/98 **combined with** **Windows XP** **Windows 2000** **Windows NT**	Runtime system always has to be installed on the Windows 95/98 partition, Complete System on the Windows NT/2000/XP partition.

- **Administration Utilities**
  If only administrative tasks are to be performed on the destination workstation, it is recommended to install the administrative utilities Response Code Wizard and/or Configuration File Wizard only.

☞ *Click [Next].*

3.2.2 Installation Options

The dialog box *Select Installation Options* appears.



You can now determine which components are to be installed.

You can choose from the following options:

- **Secure Auto Logon** (SAL)

  You should select the option 'Secure Auto Logon' if you want to log on automatically to Windows after logging on to SafeGuard Easy. After entering the Windows access data one time only, a relationship is established between SafeGuard Easy user

and the operating system user. If Pre-Boot Authentication is activated, the user is automatically logged on to Windows after entering his/her SafeGuard Easy user data – without being requested to make any more entries (see page 85).

- **Configuration File Wizard**

  Configuration File Wizard creates configuration files. With the help of these files, SafeGuard Easy can be installed onto a workstation, changed or removed from a computer without any user interaction (see page 92).

- **Response Code Wizard**

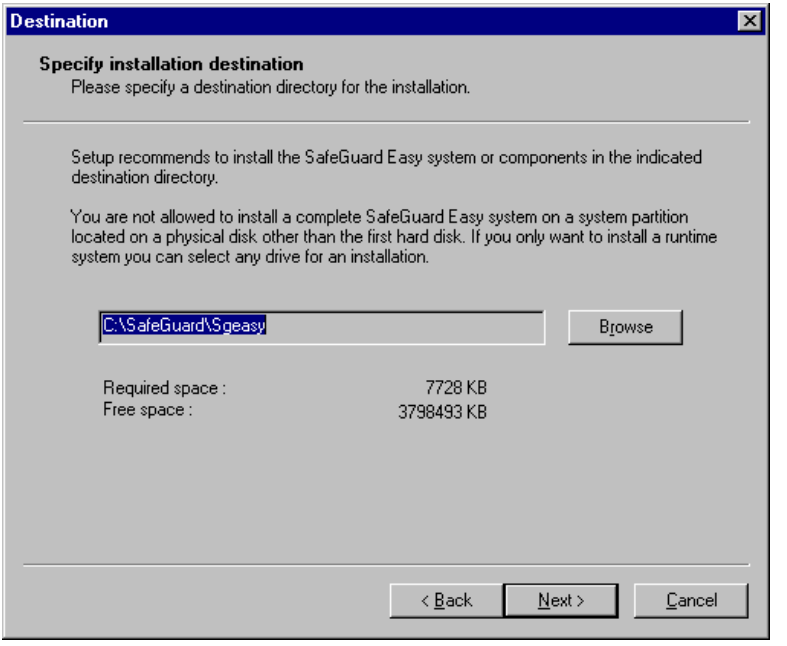
  Selected actions, such as the issuing of a new password without knowing the old one or the deinstallation of SafeGuard Easy can be carried out despite the user and system administrator being in different places (see page 116).

You will find detailed information on the installation options in the corresponding chapters.

☞ *Mark (a tick is displayed) the components that you want to install and click the button [Next].*

3.2.3 Installation destination

The dialog *Specify Installation destination* is displayed.



Select the drive and directory into which SafeGuard Easy is to be installed. The standard setting for the destination folder is `\Safe Guard\Sgeasy`. From here on, the term *<SgeasyPath>* is used for this directory. If you want to select another directory, click the [Browse] button.

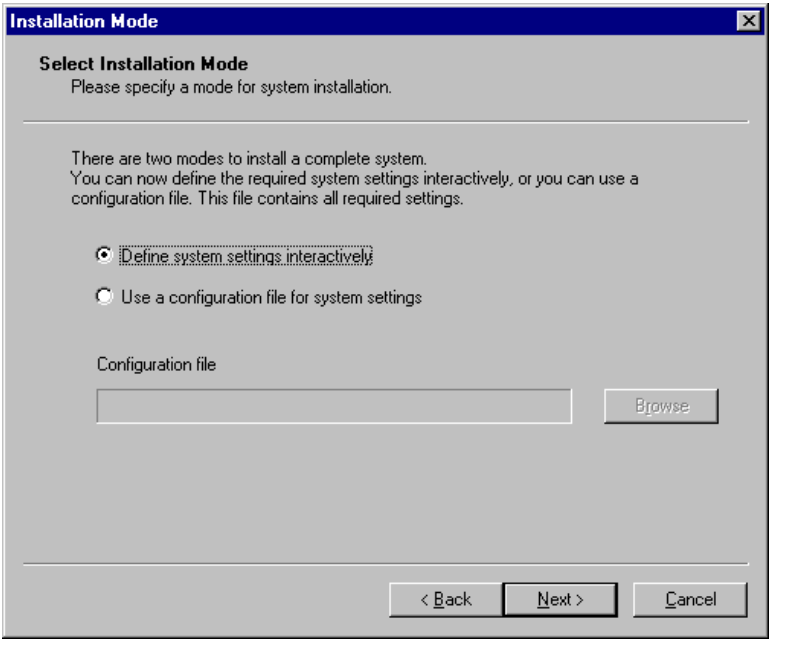
Do not use special characters for the path name!

You should consider disk space requirements when you decide where the SafeGuard Easy directory is to be created.

☞ *Click [Next].*

3.2.4 Installation Mode

The dialog *Select Installation Mode* is displayed.



You can choose between two installation modes:

- **Define system settings interactively**

  You can install SafeGuard Easy onto your computer and choose the settings for the workstation personally. After clicking [Next] the SafeGuard Easy files are copied onto the hard disk. The setup process is then finished and the 'actual' installation procedure begins.

- **Use a configuration file for system settings**

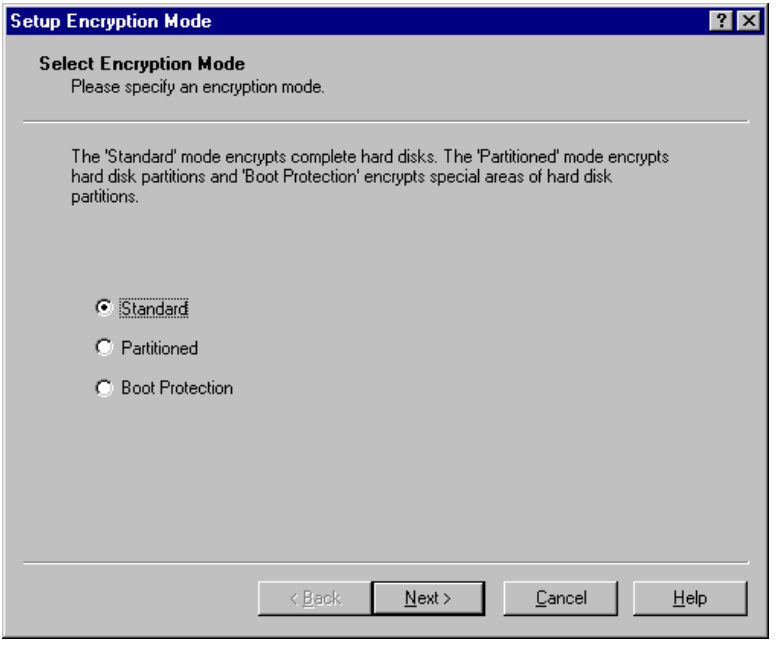
  By using a configuration file, SafeGuard Easy will be installed on your workstation without any user interaction. Click [Browse] to browse for an existing configuration file. How to create a configuration file, please see page 93.

☞ *Tick one of the two installation options.*

If you have selected option “Define system settings interactively” SafeGuard Easy files are now copied into the target directory.

3.2.5 Encryption Mode

If you *Interactive Selection of System Parameters* was selected, the dialog box *Select Encryption Mode* opens.



There are three different encryption modes:

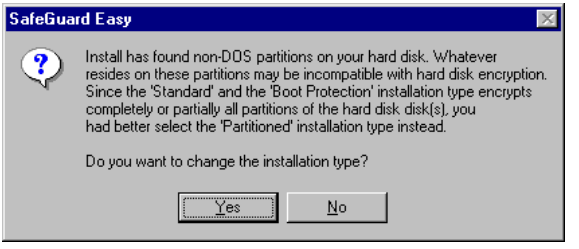
- **Standard**
  All hard disks of your workstation are completely encrypted. SafeGuard Easy recognizes automatically whether your computer has one or more hard disk drives. The program can be installed under Windows onto systems with up to four physical hard disk drives. If more than four hard disks are identified, SafeGuard Easy discontinues installation. Up to eight logical partitions can be present on each of these hard disks.

- **Partitioned**
  In this mode, SafeGuard Easy only applies the encryption to individual partitions. You should select this setting if your hard disk drive(s) has/have several partitions and you do not want to encrypt all of them. You decide which partitions to encrypt later on (see page 51). This encryption type is selected automatically if more than eight partitions are detected.

- **Boot Protection**
  With this type of installation, only the system areas (boot area, FAT, root and NTFS-MFT) for all logical drives are encrypted. The actual data area remains unencrypted. Boot protection means that no unauthorized person can boot the computer from an operating system floppy disk, because this would allow them access to the workstation's hard disk drive. Pre-Boot Authentication should always be activated because without PBA there is no Boot Protection.

Windows 95/98

Operating systems Windows 95/98 only support the file system FAT/FAT 32. If you select the encryption mode *Standard* or *Boot Protection* and a non-DOS partition is detected during installation of SafeGuard Easy for one of these operating systems, the following message box appears:



If you select [Yes], SafeGuard Easy returns to the dialog box Encryption mode and you can select another encryption mode, by clicking [No] installation goes on.

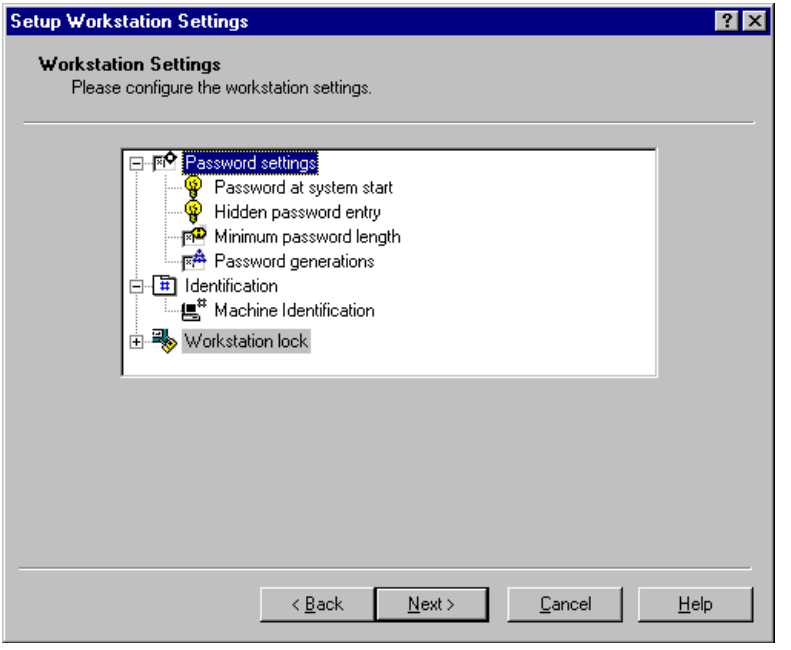
Problems can occur in this case: Two different operating systems are installed on partitions supporting different file systems (e.g. Windows 98 on FAT partition/Windows 2000 on NTFS partition). After installing SafeGuard Easy on the FAT partition, access to the NTFS partition is no longer possible, so Windows 2000 cannot be started anymore.

This scenario is only valid for encryption types *Standard* and *Boot protection*.

☞ *Click [Next].*

3.2.6 Workstation Settings

The dialog box *Workstation Settings* appears.



Password Settings

- **Password at System Start (Pre-Boot Authentication)**
  If PBA is switched on only SafeGuard Easy users are allowed to logon to the workstation.

  PBA is switched on
  A logon screen is displayed before the operating system (Windows or the Boot Manager) is loaded. Windows starts up after

successful authentication with the correct SafeGuard Easy access data.

PBA is switched off
If Pre-Boot Authentication is switched off, logon prior to booting the system is not required. Authentication is then done exclusively via the logon dialog of the operating system.

For further informations about Pre-Boot Authentication see also page 81.

- **Hidden Password Entry**

  Hidden password entry means that, contrary to conventional logon procedures, no place selectors (e.g. the symbol '*') appear when the password is entered. This means, for instance, that others cannot see the number of characters entered. Cursor movement is deactivated, too.

Please inform your users that characters are not displayed in the logon screen. Otherwise misunderstandings can occur if no '' symbols are displayed.*

- **Minimum Password Length**

  The password length is determined in this field. By doing so, you determine the minimum number of characters a password has to have when being entered by the user.

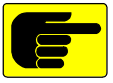
  The number of characters can either be entered directly or it can be increased or decreased by pressing the direction keys. Any value between 1 and 16 can be entered for the password length. As a default value 6 characters are set.

- **Password Generations**

  To prevent users from changing back and forth between a few passwords, you can set the number of password generations to a higher level. Each password is compared with the ones used in the past and rejected if it is identical with one which has already been used. This setting regulates the number of used passwords stored for the purpose of comparison.

  The default setting is 4 password generations. The maximum number of storable passwords already used is 16. You can change the number by clicking the entry field and using the keyboard or with the help of the direction arrows.

  Password generations should be combined with "Password change" (see page 62).



Example:
You have set the number of password generations for the user Miller at four and the number of days after which the user must change his/her password at 30. Mr. Miller has been authenticating himself with the SafeGuard Easy password "Security" up to now. After the deadline has expired, he is requested in the PBA to change his password. He enters "Utimaco" as his new password. 30 days later, he is again requested to change his password when logging on. Mr. Miller enters "Security" and receives an error message telling him that he has already used this password and that he has to choose a new one. Mr. Miller can only use "Security" again after the fourth request to enter a new password (this is why password generations=4).

Machine Identification

The text entered here appears in the PBA logon screen. You can set for example an exact name for your workstation in this field. Thereby enabling you to identify the machine precisely.

Please proceed as follows:

1. Double click on “Identification”.
2. Mark “Machine Identification”.
3. Enter a text (e.g. the name of the computer) in this field. A maximum of 63 characters can be set.
4. A machine name already set within the Windows network settings is transferred automatically.

☞ *Click [Next].*

The machine ID string can contain references to environment variables. These will be expanded at the time of installation. This is especially useful for configuration files that are installed on more than one computer.

Example:

"*This is %USERDOMAIN% booting from %WINDIR%*"

will expand to

"*This is PC1234 booting from C:\WINNT*"

during installation under Windows NT/2000/XP.

Since Windows 95/98 doesn't offer any predefined environment variable containing the computer name, a special variable %COMPUTERNAME% is available on all operating systems to provide a platform-independent way to include the computer name. %COMPUTERNAME% will always expand to the NETBIOS name of the computer.

In addition, the following rules apply:

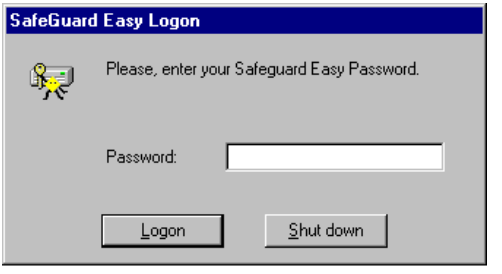
- Undefined variables expand to an empty string.
- If the contents of a variable is too large to fit the machine ID field, it is expanded to "[...]".
- Variable names are case insensitive.
- If you need a percent sign in the string, use the sequence "%%"
- Variable expansion is done once during installation, not every time the computer is booted.

Workstation lock (Windows 95/98)

The workstation lock integrated in SafeGuard Easy for Windows 95/98 is comparable to the Windows NT/2000/XP's screen saver. Both screensaver and workstation lock protect workstations from not authorized access.

Workstation lock is deactivated by entering the SafeGuard Easy password entered at Pre-Boot Authentication (PBA) (Option "Password at system start"). Workstation lock can therefore only be used if PBA is activated.

If workstation lock is switched on the following screen appears:



Switching on

- **Automatically**

  Tag the check box “Workstation lock after ‘n’ minutes” if you want to activate the automatic workstation lock. This activates the minutes field on the right. Enter the value you require. You can set any value between 1 and 59 minutes.

- **Manually**

  If you want to take a break from your work, manual workstation lock can be activated by clicking on the workstation lock icon  in the system tray.

Switching off

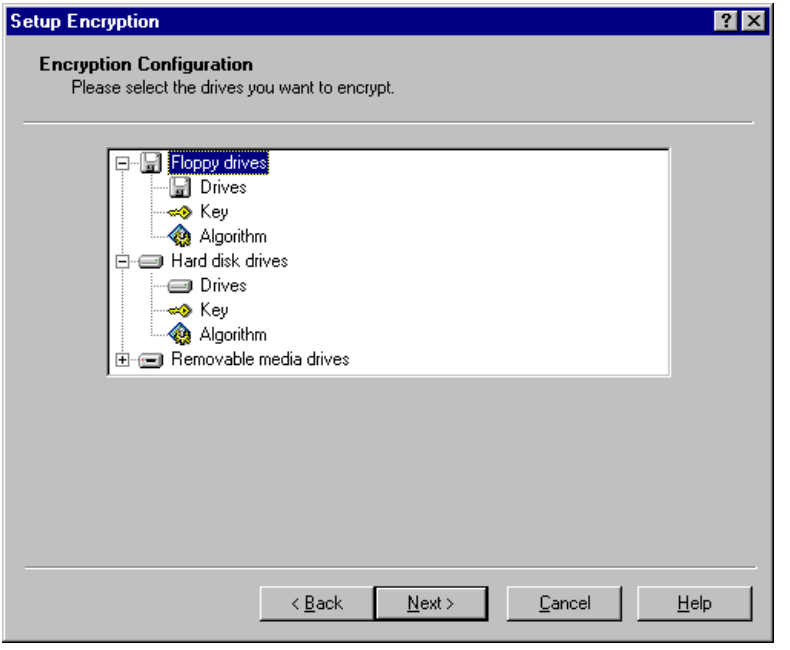
Workstation lock can be deactivated by entering the same SafeGuard Easy password that was entered in the PBA. The password must be confirmed with the [Enter] key. This takes the reader back to the point where the workstation lock was activated. DOS full screens are minimized and placed in the task bar. They must then be switched back to full screen.

If PBA is switched off, workstation lock is switched off, too. Switching on the PBA again, workstation lock has to be activated separately.

To protect your workstation it’s recommended to activate workstation lock.

3.2.7 Encryption Configuration

The dialog box *Encryption Configuration* is displayed.



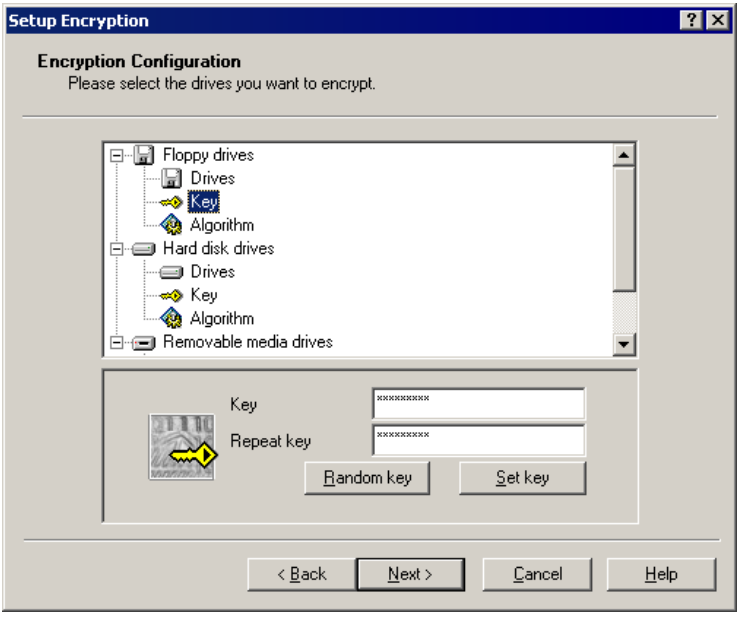
You can encrypt

- Floppy drives
- Hard disk drives / partitions
- Removable media drives

How the various drives are to be encrypted is defined here.

Key

Prior to first-time encryption, you must assign a key. You can set the key for the various drives by clicking the sub-item *Key*.



With all drives, you can either determine a key by yourself or have one generated at random by the system.

How to assign a Key

Click the sub-item *Key*. Once you have entered the correct key or if the random key function was selected, please press the button [Set key] to confirm.

Random Key

The randomized generated key has always a length of 32 Byte (256 Bit). It will then be reduced to the matched length of the respective algorithm. A random key always has a length of 32 bytes (256 bits). It is then reduced to match the length of the selected algorithm. The * symbols in the entry field for the key serve merely as markers.

Length of key

There is no predetermined minimum key length, but the maximum number of characters is 32. Alphanumerical (A-Z; a-z; 0-9) and special characters (°!“”§$%&/()=?’*’-:;^+#-.,) can be used for the key. The numbers on the number pad may not be used. Please ensure that you differentiate between the upper and lower cases, the key is case sensitive.

Trivial key

Newly defined keys (hard disk, floppy,...) are checked for triviality. A trivial key is a character sequence which consists of one or only a few characters (e.g. 22222222, aad daad daadd, 1h1h1h1h1h1h1h) or the sequence of a row of keyboard characters (e.g. asdfghjk, lkjhgfds). If you select a trivial key, a warning is given about the security risk and you may define another key.

Hints

Floppy drives / Removable media drives

- Never give the key to unauthorized persons and keep it in a safe place (particularly recommended for floppy and removable media drives).
- Keys for floppy and removable media drives can be changed once SafeGuard Easy is installed by the user SYSTEM or any user given the right to change encryption settings. Furthermore they can be changed temporarily by using SGEYCRYPT (see page 93), too.
- If encrypted floppies or removable medias need to be shared among the employees, for example, keys should never be generated at random. If the key was created using the random method, it can only be read and/or used on the workstation it was generated.
- You can only assign one key for all floppy drives. This is also valid for removable media drives.

Hard disk drives

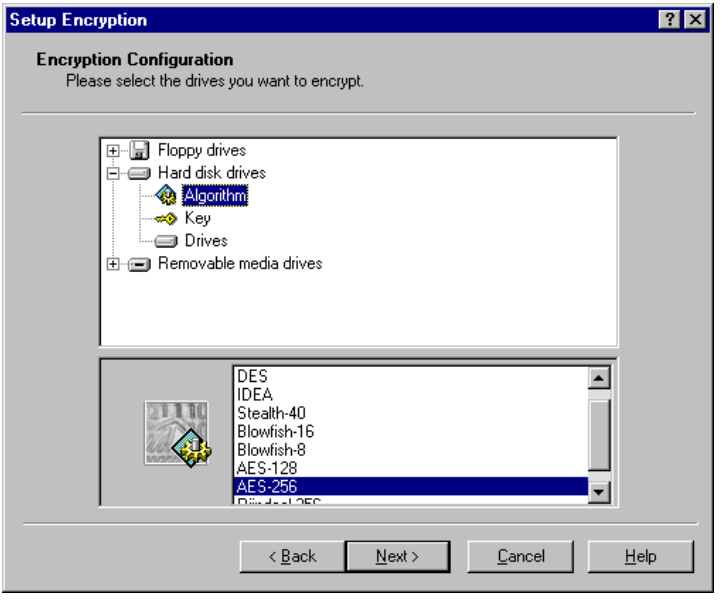
- Keys of hard disk drives/partitions cannot be changed once SafeGuard Easy is installed.
- If SafeGuard Easy is installed interactively workstation by workstation, it's possible to select different keys for each workstation.The generation of random keys for hard disk drives is recommended in particular when installing SafeGuard Easy onto several workstations using a configuration file: a different random key is generated for each computer here despite the same configuration settings. Random key is not trivial and is really generated randomized.
- You can only use one key for all hard disk drives and partitions.

As soon as a hard disk drive is encrypted keys cannot be changed anymore.

See also remarks for floppy drive encryption (page 50), hard disk drive encryption (page 52) and removable media drive encryption (page 54).

SafeGuard Easy's Algorithms

You can set the algorithms for the various drives by clicking the sub-item *Algorithm*.



The various algorithms are measured in particular by the level of security they provide. The more secure a method is, however, the longer the encryption process lasts.

Listed below, you will find all of the algorithms used in SafeGuard Easy along with their corresponding standards or names.

- **AES-128/AES-256**

  The Advanced Encryption Standard (AES) is a new algorithm replacing the Data Encryption Standard (DES) The algorithm Rijndael was selected for AES by the National Institute for Standards and Technology (USA). AES is a very fast and secure encryption algorithm and works with a 128 bit key. AES-256 is equal to AES-128, but uses a 256 bit key.

- **Rijndael**

  Rijndael is a special implementation of the AES 128 bit algorithm but works with a 256 bit key.

- **IDEA (International Data Encryption Algorithm)**

  The symmetrical encryption algorithm developed at the beginning of the 90s works with a 128-bit key. It is regarded as very secure nowadays in regard to the mathematical process involved as well as the key length and it is considered extremely resistant to all crypto analytical attacks. If you want to install a highly secure system, please use IDEA.

  If you want to set up a system with a security level, it's recommended to use IDEA.

- **DES (Data Encryption Standard)**

  DES was developed in the 70s and works with a 56-bit key.

- **Blowfish-16/Blowfish-8**

  Blowfish is a relatively new symmetrical algorithm developed by Bruce Schneier. It uses a 64-bit block coding algorithm and uses a 256-bit key.

  Blowfish - 8 is equal to Blowfish - 16 algorithm but reduced to 8 rounds. There are no precise statements concerning the security of this algorithm either. It is, however, also considerably more secure than XOR. It is freely available and uses a 256-bit key.

  If you want to install a secure system with the lowest possible performance loss, please use Blowfish-16.

- **STEALTH-40**

  This algorithm is roughly as fast as XOR, but considerably more secure. STEALTH-algorithm uses a 48 - 64-bit key.

- **XOR (eXclusive Or opeRation)**

  XOR is a symmetrical algorithm. However, its security level should be regarded as low, however. XOR uses a 64-bit key.

Additionally there are some special floppy drive Algorithms:

- **DES SB-II**

  The algorithm DES SB-II is compatible with the floppy drive coding of SafeBoard II and III and/or the floppy drive encryption of SafeBoard X II and II with the old key management.

- **XOR SB-I A=B**

  See XOR properties. XOR SB-I A=B is compatible with floppy drive encryption from SafeBoard I (from Version 1.43) C:Crypt and Crypton DOS.

Available Algorithms

Drives	Algorithms
Floppy Drives	- AES-128 - AES-256 - Rijndael-256 - IDEA - DES - Blowfish-16 - Blowfish-8 - STEALTH-40 - DES SB-II - XOR SB-I A=B If no other algorithm is selected AES-128 is set by default.
Hard Disk Drives/ Removable Media Drives	- AES-128 - AES-256 - Rijndael-256 - IDEA - DES - Blowfish-16 - Blowfish-8 - STEALTH-40 - XOR If no other algorithm is selected AES-128 is set by default.

Once SafeGuard Easy is installed algorithms cannot be changed anymore.

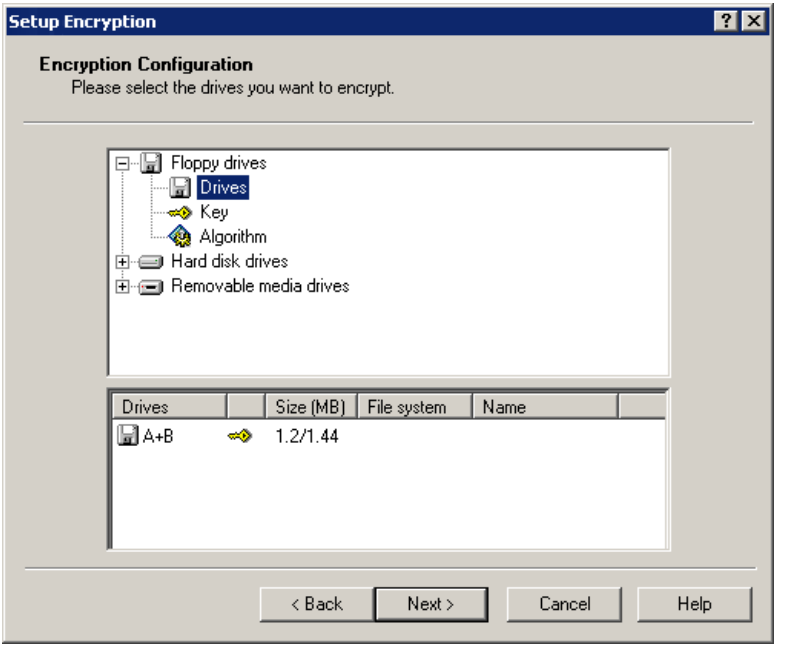
Floppy Drive Encryption

Under *Drives*, you decide if you want to activate the floppy drive encryption.

To avoid problems please read the hints for floppy drive encryption listed on page 50 carefully.

Floppy encryption is switched on/off as follows:

1. Click *Drives.*



2. By double-clicking on the drive letter a key symbol appears that indicates that the drive will be encrypted. The encryption status is valid for all floppy drives.
3. If you want to switch off the encryption double-click the drive letter once again.

Hints

- **Reading encrypted floppies**
  If floppy drive encryption is activated, unencrypted disks cannot be read. For this reason, you have to reformat these in an encrypted drive. By formatting the floppy all data on it are deleted.
- **Create encrypted system disk**
  If floppy drive encryption is activated it's recommended to create an encrypted boot floppy.
- **Exchange of floppies**
  If floppies are exchanged between different workstations, the floppy drives of the workstations in question must be encrypted with identical algorithms and keys. If not, the floppy disks cannot be read.
- **List of floppy drives**
  When there is more than one floppy disk drive this is not shown in the drive list of SafeGuard Easy. It is only possible to encrypt/decrypt all floppy drives. You cannot select them separately.

Hard Disk Drive Encryption

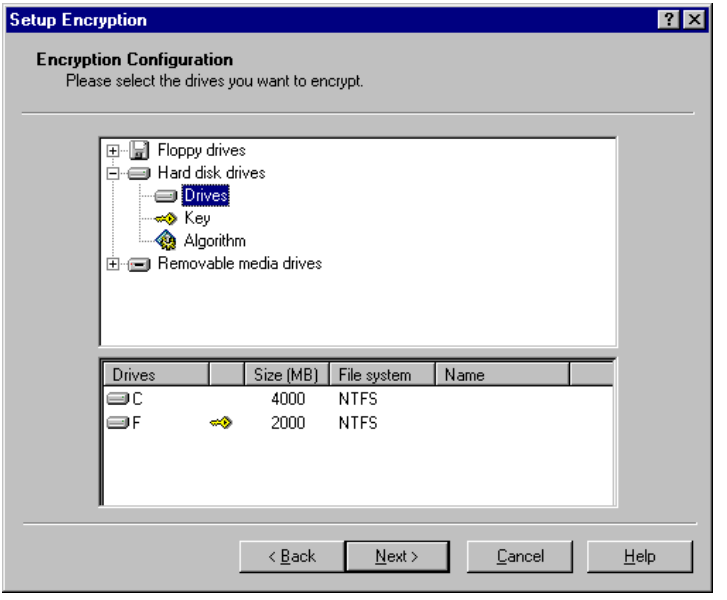
Depending on the encryption mode you have selected (Standard, Partitioned or Boot Protection), you can encrypt either the entire hard disk or only individual partitions.

To avoid problems please read the hints listed on page 52 carefully.

Depending on the encryption mode different view are displayed: “Standard” and “Boot Protection” show you all hard disk drives, with “Partitioned” all found partitions will be displayed.

How to switch on hard disk drive encryption:

1. Click “Drives”.



2. By double clicking a hard disk drive/partition a key symbol appears that symbolizes that the chosen drives/partitions.
3. If you want to switch off the encryption double click the drive again.

Hints

- **Keys and algorithms**
  Only one key and one algorithm can be set for different hard disk drives with complete as well as partitional encryption. Partition D, for example, cannot be encrypted with IDEA while intending to encrypt Partition E simultaneously with XOR.
- **Unformatted areas**
  If a partition has not been firmly assigned to a file system, SafeGuard Easy will not recognize this with the encryption mode "Boot Protection" and the unformatted sub-area of the hard disk will be encrypted too.
- **Number of hard disks**
  SafeGuard Easy recognizes automatically whether your computer has one or more hard disk drives. The program can be installed under Windows onto systems with up to four physical hard disk drives. The number of partitions on a hard disk is limited to eight. If encryption is already done for one hard disk, do not add any further hard disk to your workstation. If a new hard disk drive is to be integrated you first have to remove SafeGuard Easy from the workstation, integrate the new hard disk and install SafeGuard Easy once again.
- **Generating new partitions with an installed SafeGuard Easy**
  Do not change the partitioning of the hard disk after encryption as this can lead to a loss of data.
- **Disable virus scanners**
  During Encryption virus scanners should be disabled

- **Suspend to disk**
  If one hard disk is encrypted suspend to disk mode is not supported.
- **Reboot before installing SafeGuard Easy**
  If you have repartitioned the hard disk, you must reboot the system BEFORE installing SafeGuard Easy.
- **ECVIEW** (***Windows NT/Windows 2000/Windows XP***)
  The program `ECVIEW.EXE` shows the current status of encryption for every hard disk drive encryption process. You can monitor the progress in the left-hand side of the window (percentage scale). The speed at which the encryption is to be done can be adjusted with the help of the regulator. The higher the selected percentage, the faster encryption is done. The speed value of the encryption process isn't stored any longer in the registry. After rebooting the workstation the full speed value is used.
  If very small partitions are being encrypted, or only the system area, it can happen that ECVIEW is not displayed. An entry within the event log of Windows is written once encrypting/decrypting has been completed.

Encryption of Removable Media Drives

In addition to floppy and hard disk drives, removable media drives can be encrypted with SafeGuard Easy.

SafeGuard Easy supports encryption of following removable media drives:

- ZIP drives (no IDE)
- JAZ drives
- MO drives

To avoid problems please read the hints for removable media drive encryption listed on page 54 carefully.

How to switch on/off Removable media drive encryption:

1. Click “Drives”.
2. By double clicking on the removable media drive a key symbol appears that symbolizes that the drive will be encrypted. The encryption status is valid for all removable media drives.
3. If you want to switch off the encryption double click the drive again. The key symbol disappears and the drive will be decrypted.

Hints

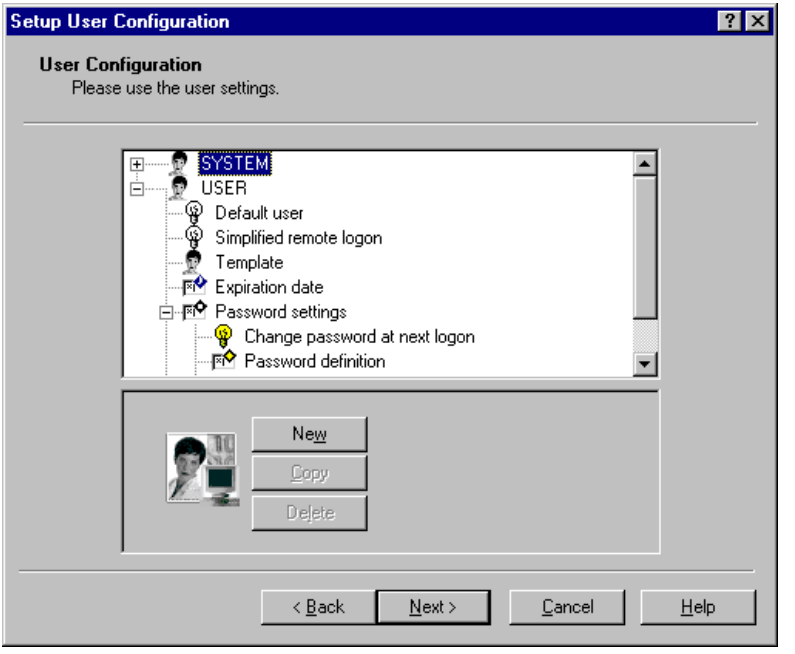
- **Keys and algorithms**
  Only one key and one algorithm can be set for various removable media drives.
- **List of floppy drives**
  It is only possible to encrypt/decrypt all removable drives. You cannot select them separately.
- **Reading encrypted medias**
  If encryption is activated, unencrypted medias cannot be read. For this reason, you have to reformat these in an encrypted drive. By formatting the medium all data on it are deleted. If a removable medium is accessed but cannot be read e.g. because encryption is active and media is plain text a new message appears informing the user that by formatting the medium all data are deleted.

- **Exchange of medias**
  If removable medias are exchanged between different workstations, the drives of the workstations in question must be encrypted with identical algorithms and keys. If not the medias cannot be read.
- **SG Eject** (***Windows NT/Windows 2000/Windows XP***)
  Windows treats removable media drives the same way as hard disk drives unless corresponding software originating from the drive manufacturer is used. If a removable medium drive is encrypted only users with administrative rights for Windows can eject the medium. Without having these rights users are forced to use SG Eject.
  You find SG Eject in the context menu of the removable media drive letter.
- **Change of encryption state**
  Within the SafeGuard Easy administration program the encryption state for each removable media drive can be set separately. By changing the encryption state with SGECRYPT all removable media drives are effected, which means that all removable medias are encrypted or not until system is rebooted.

☞ *If you have done all the settings click [Next].*

3.2.8 User Configuration

The dialog box *User Configuration* appears.



You determine which users may have access to a workstation protected by SafeGuard Easy. One can add new users, modify the data of existing users and remove users no longer required. You can also determine here the SafeGuard Easy users rights and characteristics.

SafeGuard Easy allows up to 15 users access to one system. It is also possible to assign up to 13 additional users as a supplement to the predefined user SYSTEM and USER. The *AUTOUSER appears if "Password at system start" (Pre-Boot Authentication) is switched off.

User SYSTEM
SYSTEM is a special case. No one can delete or administer that user. SYSTEM cannot change the personal settings either. Only the highest security officer of the system should be able to log on with the user ID SYSTEM. Thus only the highest security officer should know the password for the user SYSTEM. He should note the password and deposit it in a safe.

Adding New Users

Click the button [New]. Give the new user a name and press [OK] to confirm that the name has been given correctly. Press [Cancel] to end the process. If the name has already been assigned, an error message to this effect is issued.

Copy Users

The copying of a user who already exists provides the quicker option of creating new users and assigning them the same settings of an already existing user at the same time. Only a new password has to be assigned to the copied user. The copied user can be modified if required.

Select the user whose settings you want to copy by means of a single mouse click and then press the button [Copy]. Give the user a new name and press [OK] to confirm that the name has been changed correctly. You can abort the process by pressing [Cancel]. If the name has already been assigned, an error message to this effect is issued.

Delete Users

Users can also be deleted from the user list.

Select the user that you want to remove and click [Delete].

If you want to run the delete process, press [Yes] to confirm. The action is cancelled by clicking [No]. The removal of a user cannot be reversed.

User Properties

The following properties can be assigned to users:

- **Default User**

  One single SafeGuard Easy user can be set as a default user - except the user SYSTEM. A default user logs on by entering the SafeGuard Easy password only. If other users besides the default user wish to log onto the workstation, they must activate "Extended logon" (see also page 82).

  The user being the default user is marked by a green arrow  .

- **Simplified Remote logon**

  The simplified remote logon is used for logging on to a target system with challenge response. Using the simplified remote logon will result in a short response (see challenge/response page 112).

- **Template**

  The user defined as a template is marked by a changed user icon  . A user template serves as a basic user profile.

  Templates serve a very special purpose and should only be used for this. They are usually used when SafeGuard Easy is to be installed on several computers with the help of a configuration file. If there were no templates, all users would have the same SafeGuard Easy user name on all computers. In many cases, however, this would be in contradiction of corporate organizational guidelines which stipulate that there has to be individual

user names, such as surnames, personnel numbers etc. A SafeGuard Easy user name can then be defined as a template for environments of this kind. This has the result that this SafeGuard Easy user gets a new user name when he/she logs on to the PBA for the first time and is thereby individualized.

A template is implemented as follows:

SafeGuard Easy is installed on a workstation and one SafeGuard Easy user is defined as a template user. The user of this workstation is informed of the access data (user name and password) of the user template. When the user logs on for the first time, he/she must enter this access data at the logon screen. Thereafter, the user is requested to enter his/her new SafeGuard Easy user name and new password which must also be used for identification at the next logon.

A template can either be used to rename or to copy a user.

Rename
If you want to ensure that exactly only one user can logon by using the template, you must designate the attribute "Rename" to the user template. In this case the template is overwritten with the new user data and it is no longer possible to log on with the template's access data.
Copy
The new user name is added to the SafeGuard Easy users but the user template remains as it is. Additional users can log on with the template's access data. A maximum of 13 new users can be added, when SYSTEM and USER are already on the workstation.

For security reasons it is recommended to use the "Rename" template.

- ***AUTOUSER**

  If the PBA is switched off, SafeGuard Easy adds an additional user called "*AUTOUSER".

  By default the *AUTOUSER has no rights. He can be granted the following rights:

  - Change device keys temporarily
  - Change floppy keys temporarily
  - Switch floppy drive encryption
  - Switch removable media drive encryption

  If PBA is switched off all users log on with the *AUTOUSER's profile. By activating the PBA the *AUTOUSER is deleted automatically.

- **Expiration Date**

  The expiration date option enables you to restrict a user's access to the workstation on a predefined date. You can determine a cut-off date by which the user can log on to the system for the last time. This setting does not apply to the user SYSTEM. This setting is best suited for the situation that an employee is only intended to use a workstation for a certain period of time (e.g. summer job). Upon expiry of the date, the employee in question can no longer logon to this workstation.

  Select the checkbox "expiration date". You can now fill in the date by using the keyboard or click the pull-down-menu and change the expiration date within the calendar.

- **Password Settings**

  The identification passwords which a SafeGuard Easy user has to enter during the various logon processes are defined under Password Settings. But users can also change their passwords by

themselves. In addition to this, it is determined here whether a user has to change his/her password within a particular period of time.

Especially the SafeGuard Easy user SYSTEM must give particular thought to his/her password as it is crucial for administration or removal of the program.

– **Change password at next logon**

  The user is forced to change the SafeGuard Easy password in the SafeGuard Easy logon screen when logging on for the first time.To do so, PBA has to be switched on.

– **Password Definition**

  Passwords can consist of all existing letters, figures and special characters (!“”§$%&/()*+;:._-). Figures of the numbering block must not be used. SafeGuard Easy checks if a password is trivial (e.g. “12345” oder “AAABBB”) and displays a warning.
  Enter the password in the top line and once again in the field *Repeat Password*. The repetition is necessary in order to avoid typing errors. A check is made to ensure that the entered strings are identical and an error message is issued if the passwords do not confirm with each other or is too trivial. Please use the reset key to correct entries.
  For security reasons, the entry is only indicated by ‘*’ symbols.

  It is not possible to bypass the *Repeat Password* entry by “copy and paste”.

– **Password Change**

SafeGuard Easy permits a password to be valid for an unlimited period of time. In this case, however, there is a very great risk of it becoming known. In order to minimize the security risk, you can determine a time limit for the validity of the password. Once this date has been reached, the users have to change their passwords after logging on. The time period can be set with the help of the direction keys and via the keyboard. By selecting the date with the mouse once you click on the drop down box and a calendar appears.

Time period can be set from one to 99 days, 90 days are determined by default. After the selected time period a user has to change his / her password.

- **Rights**

All new users do not have any administrative rights to begin with. It's predefined that user SYSTEM has all the rights.

For security reasons, a lot of thought should be given to the rights that are granted to individual users.

Each user may only change the settings of those users who have fewer rights than they do. It also goes without saying that users can only grant the rights, which they themselves have.

You can give users the rights to temporary and permanent settings. Temporary settings are only valid for the duration of one log-on. Once the system has been rebooted or after the next Windows logoff, they are no longer available and system settings are valid again. Permanent rights remain in effect, even after the system has been rebooted.

Select the menu item “Rights”. All assignable rights appear in the lower part of the window. Depending on the previous status, the authorization to be changed is converted to either “Granted” or “Not Granted” by double-clicking the appropriate symbol.

Following rights can be assigned:

– **Change removable media drive key temporarily**
Allows the user to temporarily change the key of removable media drives.

– **Change floppy key temporarily**
Allows the user to temporarily change the floppy key.

– **Switch floppy drive encryption**
Floppy drive encryption can be switched on or off.

– **Switch removable media drive encryption**
Removable media drive encryption can be switched on or off.

– **Change encryption keys**
The user may modify the encryption key of all drives, except hard disk drive is already encrypted.

– **Change encryption settings**
The user can make changes to encryption settings. He/she may, for example, determine which partitions are to be encrypted etc.

– **Change password rules**
Allows users e.g. to define a minimum password length.

– **Change user settings**
Allows users to add, copy or remove other SafeGuard Easy users (except SYSTEM and *AUTOUSER).

– **Remove**
  If you select this box, the user is given the right to remove SafeGuard Easy from his /her workstation.

– **Boot from Floppy allowed**
  A user may boot a system protected with SafeGuard Easy from a floppy disk.

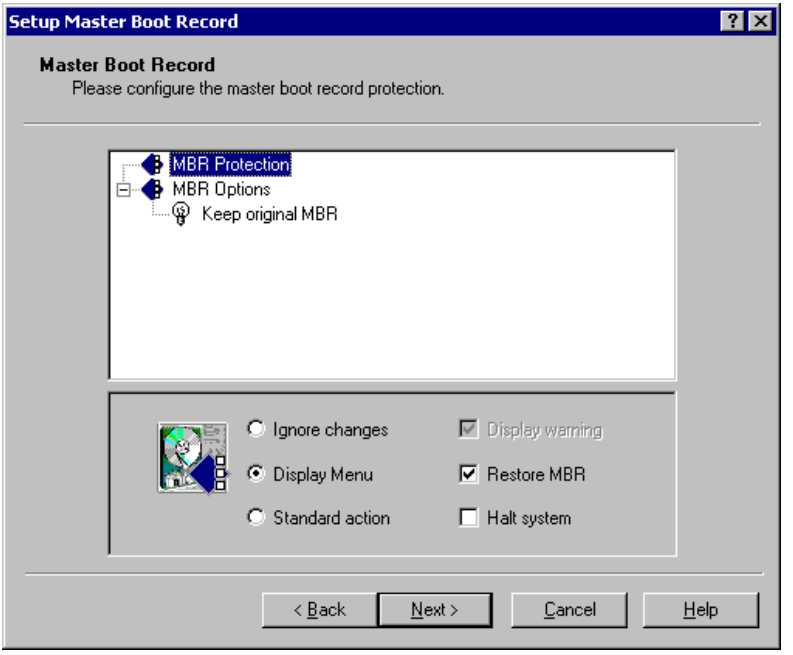
– **Change workstation settings**
  Users can change the workstation settings, e.g. activate/deactivate the password at system start (PBA) etc.

– **Change MBR settings**
  Users may change the defined settings to protect the Master Boot Record.

☞ *Click [Next].*

3.2.9 Master Boot Record

The dialog box *Master Boot Record* appears.



Various information regarding all partition created is stored in the Master Boot Record of the hard disk. Using this information, the system finds out which hard disk drive and/or which partition is used to boot the system. For this reason, it is a popular attacking point for viruses because the BIOS executes the machine code it contains right at the start of the booting process, before the operating system has been loaded. SafeGuard Easy can recognize modifications to the MBR and respond to them in various ways.

MBR-Protection

If a change to the MBR version is established, you can determine how the program is going to respond to these changes.

- **Ignore changes**

  No reaction follows. The original MBR is not restored and the boot process is continued without intervention.

- **Display menu**

  A menu is displayed if the MBR is changed. There the following actions can be selected:

  - Default Action
  - Undo Changes
  - Ignore Changes
  - Keep Changes

  With **Default Action** the "Standard action" is run, with **Undo Changes** the original status of the MBR is restored from the internal backup, with **Ignore Changes** nothing will be done and with **Keep Changes** the current MBR is left as it is and the internal backup is updated. The check takes place before the user logon. The menu only appears after a successful logon. This ensures that it is not possible for an unauthorized user to decide what should happen in such a case.

- **Run standard actions**

  You can select one or more standard actions to check the MBR.

  – **Display warning**
  The user is notified that the MBR created for SafeGuard Easy has been modified. The user must confirm this message by pressing a key.

– **Restore MBR**
The original MBR is restored automatically as a back-up copy without notifying the user. The system then reboots to remove any possible viruses.

– **Halt System**
If the MBR is changed, the system will display a message and halt after logon if the user logs in, the system administrator can logon. It is now no longer possible to boot the workstation and the user is forced to request the assistance of the administrator or support staff.

MBR-Options

With the Master Boot Record-Options you can modify the standard method with which SafeGuard Easy deals with the Master Boot Record. This option was added to provide compatibility with the various BIOS versions of the different hardware manufacturers (e.g. Compaq).

- **Support Compaq Setup partition**
This option leaves the MBR virtually unchanged. This is necessary on certain Compaq Systems (and possibly on others too) to enable access to the setup partition. Click "On" to keep the original MBR. In case you don't want to set this option select "Off". This option can be selected with all encryption modes (Standard, Partitioned, Boot protection).

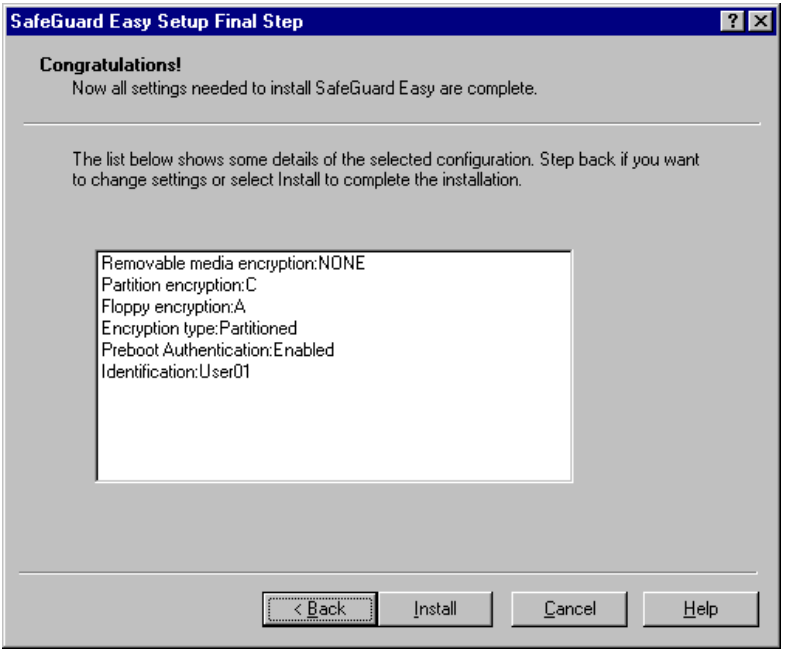
Utimaco recommends to activate this option only if it's necessary. If you do not know your system's reaction please contact Utimaco's hotline.

- **Don't change partition table (Windows 95/98)**
  This option leaves the partition table of the MBR sector on the hard disk unchanged. By default after installation all partitions will be hidden if a system start with a system floppy disk was executed. Some hard-and software configurations could have problems with this functionality which could be avoided by setting this option to ON.

  Because for functional reasons this option is always set for Windows NT, Windows 2000 and Windows XP. Therefore this option is not displayed for these Windows versions.

☞ *Click [Next].*

The dialog box *Congratulations* appears



Interactive Installation is now finished.

The list above shows some details regarding the chosen configuration settings. Click [Back] to change the settings, with [Install] SafeGuard Easy will be activated.

After the installation (and deinstallation) of SafeGuard Easy, the workstation is automatically shut down and restarted. Any applications open at this point in time are also closed without being saved. To avoid the loss of data, it is recommended that you close all active applications before installation / deinstallation.

How it is continued depends on the operating system installed:

Windows XP
Windows 2000/
Windows NT

After the restart, an automatic check of the hard disk drive (CHKDSK) is run. The reason for this is changes made by SafeGuard Easy to the Master Boot Record and the file system. The hard disk does not get damaged, changed etc. After first reboot PBA is inactive. At this time a Windows user only got the *AUTOUSER's rights. As soon as the workstation is shut down and restarted again PBA logon screen appears (if switched on) and a SafeGuard Easy user can logon to the system.

Encryption is done online. Users are able to work at the workstation during the encryption process.

If hard disk encryption is not finished and the workstation is shut down und restarted, the system is always booting directly from hard disk. As long as hard disk encryption has not come to an end, boot from floppy is not possible.
This is also true for the first reboot after encryption has finished.

Windows 95/98

Encryption is not done online. Users are not able to work at the workstation during the encryption process.

When the encryption is finished, the workstation restarts and - when PBA is activated - the SafeGuard Easy logon screen appears.

3.3 Installation from Network

The SafeGuard Easy setup can also be started from a network drive.

The following steps are required here:

1. Create four directories,...`\disk1` to `...\disk4`, on a network drive or insert the installation CD.
2. Logon with Windows administrator rights.
3. Copy the contents of the installation CD into the corresponding directories.
4. Ensure for a network installation that the directory structures are identical and that all files are copied into the corresponding subdirectories 'disk1'... 'disk4' on the network drive. This directory structure is imperative for the correct execution of the installation.

By installing SafeGuard Easy from a released network drive, this drive must be assigned to a special drive name or UNC-path.

You can now install SafeGuard Easy onto every workstation from where the released network drive can be accessed.

☞ *Continue as described in the chapter Installation from a CD.*

3.4 Installation without User Interaction

In addition to the interactive installation method, you can install SafeGuard Easy unattended. You can fully automate the installation process to the extent that no entries have to be made throughout the installation process. To do so, the desired options are entered in advance into a configuration file that is created with the configuration file wizard.

How to run the configuration file Wizard and create a configuration file see pages 93 and 103.

3.5 Deinstallation

The deinstallation of SafeGuard Easy has the following effects:

- All previously encrypted areas of the hard disk(s) are decrypted.
- Pre-Boot Authentication - if installed – is removed.
- The original Windows logon appears again if SAL was installed.
- All SafeGuard Easy files are deleted.
- All SafeGuard Easy registry entries are removed.

Do not attempt to remove SafeGuard Easy by deleting the files. If SafeGuard Easy is not uninstalled correctly registry entries remain. Therefore another installation of SafeGuard Easy may not work. In this case you should reinstall your operating system.

If the SafeGuard Easy Master Boot Record (MBR) on the hard disk is replaced by the standard MBR (FDISK command), the SafeGuard Easy components remain installed on the system.

The names of the files which have to be removed when deinstalling SafeGuard Easy are stored in the file `Sgefiles.dat`. If this file gets lost or modified, SafeGuard Easy cannot be deinstalled.

SafeGuard Easy can be uninstalled by users who have the right to remove the program. By using challenge/response it is possible to uninstall SafeGuard Easy as well even if a user has not have the right to carry out this action.

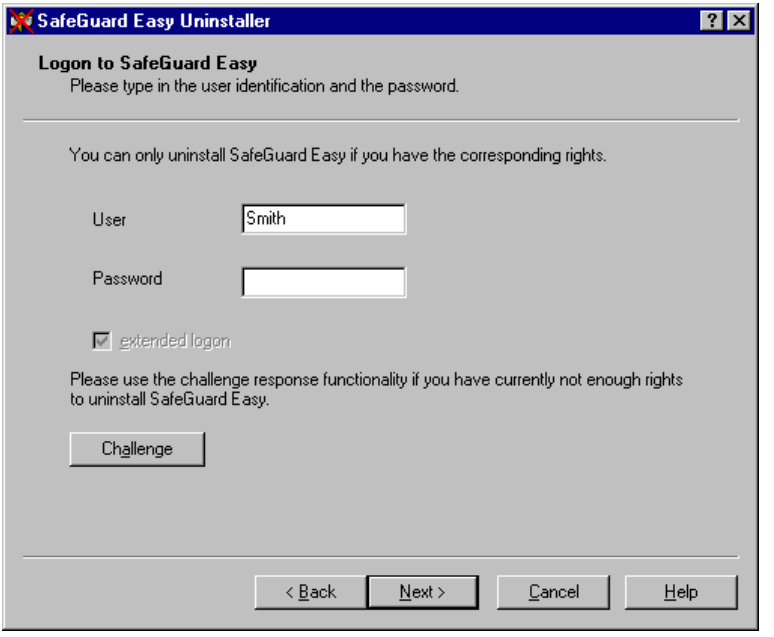
In case SafeGuard Easy should be removed you have these options how to do it:

- **Via Windows' Control panel**

  Click the Windows [Start] button and select Settings, then Control Panel. Double click *Add/Remove programs* (Windows 2000/XP) or *Software* (Windows 95/98/NT). Mark "SafeGuard Easy" and click "Uninstall" to delete the program. In the following dialog box the user who wants to uninstall SafeGuard Easy is prompted to enter his /her correct user ID and password to check the identity. Enter your correct user data. After clicking [Next], SafeGuard Easy will be removed after a reboot.

- **Uninstall via the submenu "Deinstallation"**

  Click the *Start* button in the Windows task bar and select the command *Programs*. Tick the submenu *Deinstallation* in the SafeGuard Easy folder. After the Welcome screen the following dialog box appears:



The user who wants to uninstall the program is prompted to enter his /her SafeGuard Easy user name and password. This user must have the right to remove SafeGuard Easy. After entering the correct user data, click [Next] and confirm the security check. SafeGuard Easy will be removed automatically.

- **Deinstallation with Challenge/Response**

  By using challenge/response a user can be authorized to remove SafeGuard Easy from his/her workstation although he/she has not the right to remove the program (see page 112).

- **Unattended Deinstallation**

  The deinstallation of SafeGuard Easy can be automated with the help of a configuration file. To uninstall SafeGuard Easy without any user interaction, it is necessary to create a configuration file type “Uninstall” and run it.

  How to run a unattended deinstallation see page 106.

To uninstall SafeGuard Easy unattended installation type “Complete” has to be selected. Runtime system and administration utilities installations cannot be removed by an unattended operation.

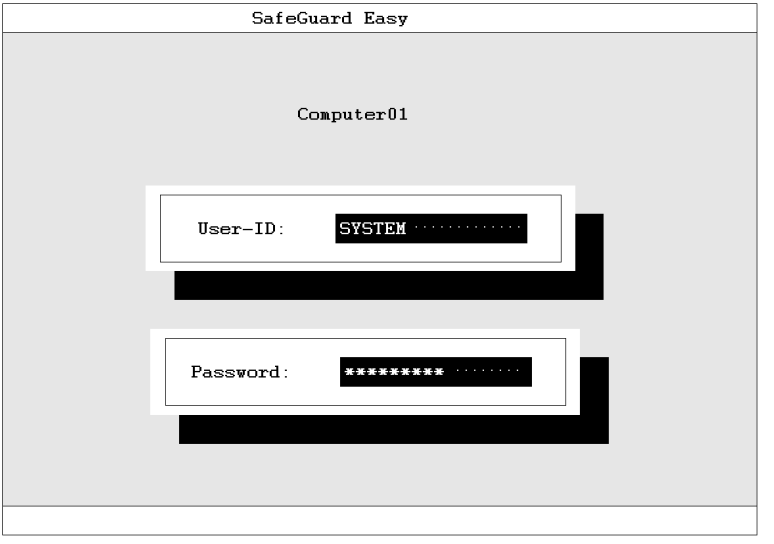
If a system installation was removed partially (e.g. by replacing the SafeGuard Easy MBR sector on the hard disk with a standard MBR sector (FDISK /MBR) or using SGEASY.EXE to decrypt from drive A:) then all SafeGuard Easy components and registry entries remain installed on the operating system partition. Running “Uninstall” from the Start Menu will now remove all these components completely.

4 Logon

SafeGuard Easy is now installed on the workstation. Encryption if activated is done. Next step now is the logon procedure. Whether the SafeGuard Easy logon screen appears or not depends on the setting “Passwort at system start”. To display the SafeGuard Easy logon screen this option has to be activated.

4.1 Pre-Boot Authentication (PBA)

PBA requires authentication before any operating system is started. Pre-Boot Authentication ensures that only registered SafeGuard Easy users can log on to a workstation. If PBA is switched on, before any operating system is loaded or booted, the SafeGuard Easy logon screen is displayed.



The user has to authenticate with his/her SafeGuard Easy user name and password. The PC cannot be booted up without a valid login. Invalid logons cause rapidly increasing response times in the PBA screen.

If Pre-Boot Authentication is not active, the logon is done as usual in the Windows logon screen.

How to enable/disable Pre-Boot Authentication see page 35.

Because of security reasons you should never deactivate the PBA.

4.2 Extended Logon

If a SafeGuard Easy user is set as a default user on a workstation, only the password field i displayed at SafeGuard Easy logon screen and other logon dialog boxes. If you don't want to log as a default user you have to use the "Extended Logon". The extended logon prompts for your SafeGuard Easy user name and password.

At the SafeGuard Easy logon screen you have to press the [**F2**] key. Within the administration and uninstall logon the option "Extended logon" has to be activated to logon with user name and password. In both cases, a field for the entry of the user name appears above the password inquiry line.

The user SYSTEM always has to logon with user name and password.

4.3 Failed Logon

Login can fail if SafeGuard Easy user name is wrong, SafeGuard Easy user password is not correct or user name has expired (see “Expiration date“ on page 60).

Reset a failed Logon

If a user enters his PBA password incorrectly, the waiting period increases after the second logon attempt. The waiting period can be reset by a valid logon.

The waiting period can be reset as follows:

1. Boot the system from drive A and insert the emergency disk.
2. Call the programm `SGEASY.EXE`.
3. Type in the SafeGuard Easy user password.
4. In the following menu select “Cancel”.
5. Reboot the system.

Waiting period is reset.

4.4 Change SafeGuard Easy Password

Users must change their passwords from time to time. A wide range of different settings concerning passwords can be made in the password rules for workstations and users.,

The SafeGuard Easy password can be changed in the SafeGuard Easy PBA logon screen or within the SafeGuard Easy Administration.

SafeGuard Easy logon screen

The user has to enter the valid SafeGuard Easy user name and password and then confirm these entries with [F10]. Then he/she will be requested to assign a new password and confirm it.

SafeGuard Easy Administration

Password can be changed within the “Users” tab. Choose *Password settings - Password* or click Menu *Extras - Password change*.

To apply the new password it has to be saved (Menu *Files - Save Settings*).

4.5 Secure Auto Logon

If SafeGuard Easy was installed with SAL, the system recognizes this when logging on for the first time and the SAL dialog box, which scans the operating system data, appears.

Secure Auto Logon is activated once the user has entered his/her access data to the operating system (user name, password, domain (if needed)).

How it works

Secure Auto Logon (SAL) is a convenience feature which creates a connection between a SafeGuard Easy and a Windows user. If this connection is established users logon simultaneously to the operating system and SafeGuard Easy by entering the SafeGuard Easy access data only. The relationship is stored in an encrypted file (`<Windows Directory>\SYSTEM32\Sgsal.dat`).

It's decided during installation if SAL is activated (see also page 27). You can only use SAL if the option "Password at System Start" (Pre-Boot Authentication) is activated.

Users are not forced to use the Secure Auto Logon. They can ignore this function by clicking [Cancel] in the SAL dialog box. The Windows logon dialog then appears and the Windows user name and password can be entered.

As long as SAL is present on a workstation, the dialog box appears every time the system is booted.

How to change the Windows Password

Windows passwords have to be changed regularly for security reasons. How a newly defined password is integrated into the Secure Auto Logon process, however, depends on the manner in which the user password is changed.

- **Forced Password Change**

  Users are forced to change their operating system passwords because of presettings entered by the administrator.

  If the user has to change his/her password when logging on, notification to this effect is given. SAL is deactivated for this

logon. Once the user has entered his/her new password, a password synchronization process is then run which the user cannot see. When logging on after the password has been changed, the user does not have to re-enter the access data to Windows and Secure Auto Logon is run without notification.

- **User Changes Password** (*Windows NT/2000/XP*)

  If the user presses the keys [CTRL]+[ALT]+[DEL] on his/her keyboard, the password can be altered via "Change password". If the change is made in this way, password synchronization is done automatically and the new data is stored in the file Sgsal.dat. When logging on after a password change, the user does not have to re-enter the access data for Windows and Secure Auto Logon is run without notification.

  If the password is changed via the Windows user administration, there is no automatic password synchronization.When logging on for the first time after the password change, the access data to Windows must be re-entered in the SAL dialog box.

Switching SAL off

An installed Secure Auto Logon can be deactivated by a user with Windows administrator rights subsequently and switched back on again with CHGSAL.EXE from the SafeGuard Easy directory.

To do so, proceed as follows:

1. Start MS Dos mode or call up the Run command in the Windows Start Menu.
2. Switch to the directory SafeGuard Easy is stored (e.g. on a network drive).

3. Enter the following command with the corresponding parameters:

   `CHGSAL.EXE /ON | /OFF [ /? ]`

   `/ON` SAL is activated

   `/OFF` SAL is deactivated

   `/?` Short help

This tool only works if SafeGuard Easy is installed.

If a SafeGuard Easy user who has already made a SAL connection is deleted from a system, this relationship remains if the same user is registered, again. The relationships cannot be removed separately, but completely by removing the file `Sgsal.dat` *within the directory <Windows>/ System32.*

The deactivation of SAL is necessary when, for example, an application is or has already been installed on a computer with smartcard support (e.g. SafeGuard Advanced Security or SafeGuard VPN). In this case, SafeGuard Easy may not be installed with Secure Auto Logon.

With Windows 2000 you get the option "The following user is always logged on". That means that you don't get the usual windows logon screen and therefore you don't get a SAL screen to fill out.

4.6 Compatibility to Logon components of other vendors

To guarantee the best possible security Utimaco Logon components ensure that they are always the first Windows logon component called by the operating system. Should anything change the call order the Utimaco Logon will automatically reinstate itself as the first component to be called.

If as a result logging on to Windows becomes impossible or Windows does not respond any more after logging on, there are two possible ways to undo the changes introduced by the logon component:

- To define the logon component that is to be called by Utimaco logon component manually, press and hold the [F8] key when the system first switches from the blue text display to the (yet empty) desktop.
- If [F8] is not pressed, a dialog box will appear. The user must define the logon component that is to be called by the Utimaco logon component, either the original Microsoft logon component or a third-party logon component. This dialog will reappear at each login until the user disables it. After that, the current logon component setting remains. Selecting the original Microsoft component will ensure that the logon is done correctly but may disable some features of the third-party product. Due to a lack of standardization it is not always possible to run an arbitrary set of different Windows logon components together.

For bigger rollouts it is possible to suppress this user interaction. To do so the administrator has to assure that before the reboot after the installation of the new logon component the registry value "ForceKnownGina" in key "HKLM\Software\Utimaco\ SGLogon" is set from 0 to the value 1 (new logon component will be called by SafeGuard Logon Extensions). As an alternative setting this value to 2 will force the use of the original Microsoft component even if other software is installed.

5 Working with SafeGuard Easy

Now you are logged on. Via the Windows [Start] menu you can select the following SafeGuard Easy components:

Administration

You can change the current settings of SafeGuard Easy in the Administration. Changes to the existing settings can only be made by those users who are authorized to make changes.

Switch Floppy and Device Encryption

The program SGECRYPT permits users to switch encryption of floppies and removable media devices and temporarily use own keys.

Configuration File Wizard

With the Configuration File Wizard configuration file with predetermined settings (rights etc.) can be created and installed onto a user's workstation without being able to interfere with the installation process.

Response Code Wizard

With the Response Code Wizard, you are given a user-friendly tool which allows a user to execute certain actions despite being in another place.

Emergency wizard

This wizard creates the emergency disk and a kernel backup.

5.1 SafeGuard Easy Administration

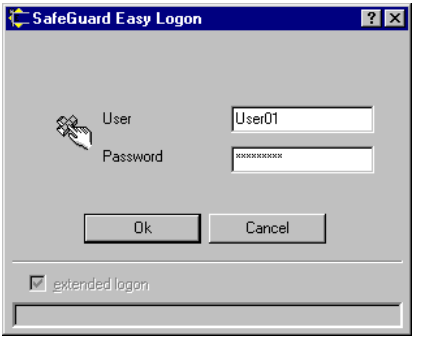
How to start SafeGuard Easy's administration program:

- Click the following one after the other in the Windows Start Menu: Programs - *<SafeGuard Easy folder>* - Administration

- or -

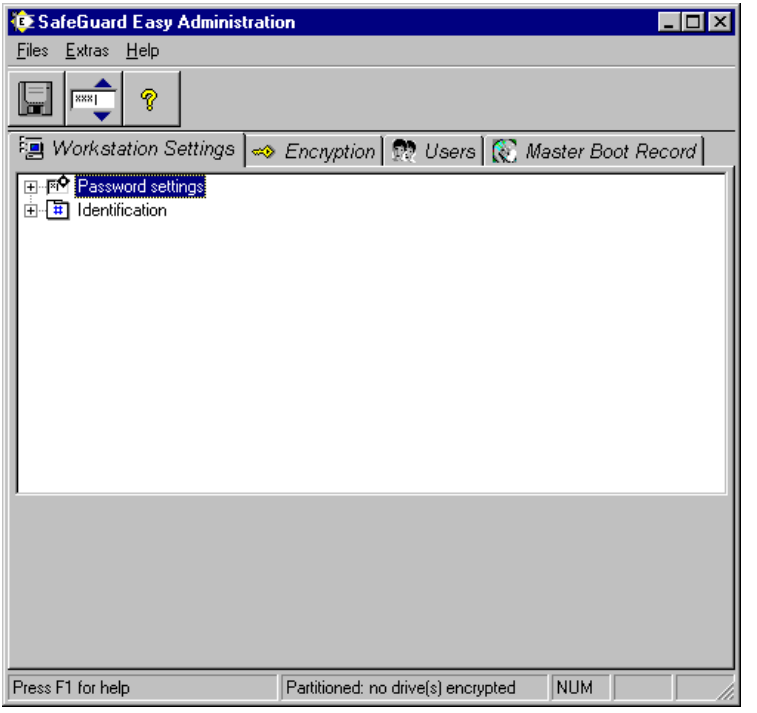
- start the program `SGEADM.EXE` in the SafeGuard Easy directory selected during installation.

You are then placed in the logon screen of the administration.



The number of logon tries is restricted to five. The system has to be re-booted to try another logon.

After entering the correct user data SafeGuard Easy administration appears.


SafeGuard Easy Administration
Files Extras Help
Workstation Settings
Encryption
Users
Master Boot Record
Password settings
Identification
Press F1 for help
Partitioned: no drive(s) encrypted
NUM

Menus

With the following table you get an overview about the Menus within the administration and the associated functionalities.

Files	Save Settings Exit
Extras	Change Password
Help	Content Index About

Toolbar

This table shows on the left hand side you the icons with their corresponding meaning on he right.

	Save Settings
	Change Password
	Help

Tabs

Within the administration tabs you can change the SafeGuard Easy configuration. The various settings correspond to the settings that can be chosen during installation.

- *Workstation Settings* tab (see page 35)
- *Users* tab (see page 56)
- *Encryption* tab (see page 41)
- *Master Boot Record* tab (see page 65)

Only authorized user can make changes.

To activate changes within the SafeGuard Easy configuration in some cases a reboot is necessary. If a user who is logged on to SafeGuard Easy in the PBA and changes the settings regarding his / her user profile, a reboot is necessary in following cases:

- Tab "Workstation settings" - Hidden password entry
- Tab "User" - Right "Change user settings"

In these cases a message is shown. The user can decide, whether to restart the workstation immediately or later.

5.2 Switch Floppy and Device Encryption

To have a workstation completely secured it's recommended to encrypt all drives. But sometimes it's useful to have he possibility to switch encryption of floppy and removable media drives. The program SGECRYPT permits users to switch encryption of floppy drives and removable media drives (devices) and use own keys temporarily. If a SafeGuard Easy user is allowed to do so depends on his/her user rights that have been given in the "User" tab.

To avoid problems please read the hints for removable media drive encryption listed on page 95 carefully.

Necessary user rights

A user has to be given at least one of the following rights to use SGECRYPT (see page 62):

- Change removable media drive key temporarily

- Change floppy key temporarily

- Switch floppy drive encryption

- Switch removable media drive encryption

These rights determine if a user may switch encryption or not or he / she can set a temporary key for a one-time logon in case encryption is activated.

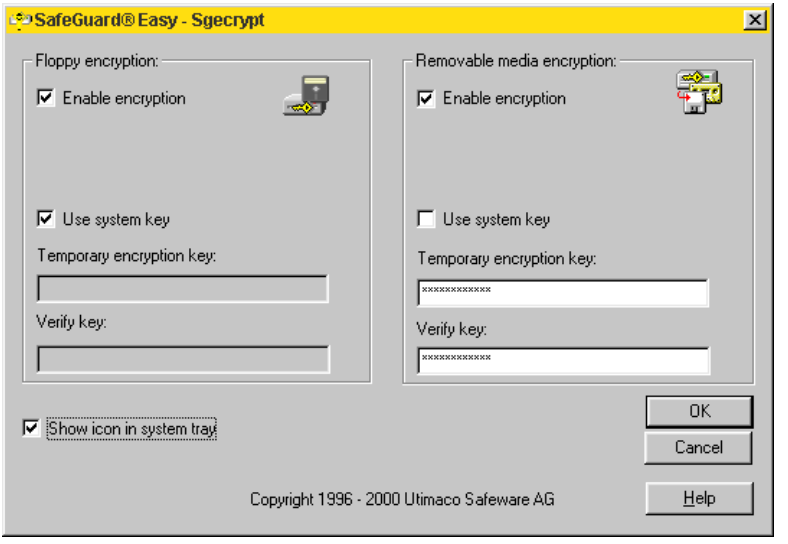
Starting SGECRYPT

There are different ways to start SGECRYPT:

- Click the following one after the other in the Windows Start Menu: `Programs - SafeGuard Easy - Floppy and device encryption.`

- Start the program `SGECRYPT.EXE` in the SafeGuard Easy-directory.
- Right-click the icon  in the system tray and select “Floppy and device encryption”.

SGECRYPT dialog box appears.



Enable Encryption	Enable/Disable encryption for one logon.
Use system key	The key predefined for floppy and removable media drive encryption is named as system key.
Temporary encryption key	A temporary key only lasts for one logon. After reboot it is removed and replaced by the system key.
Show icon in the system tray	Activates/Deactivates SGECRYPT icon in the system tray.

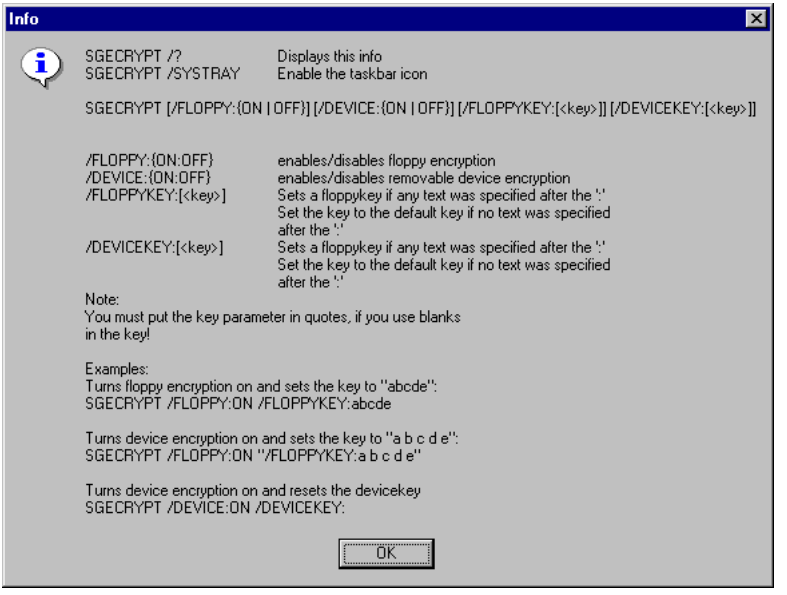
Temporary settings (encryption/key) are reset after the Windows user logged off. Then the system settings are valid once again.

To enable a system key, one must be set at the workstation and encryption for floppy disks and/or removable media drives must be switched on. If not, a user with the necessary administration rights can apply the system key subsequently.

SGECRYPT can also be started from the command line.

Enter the following to inquire about possible parameters:

<SgeasyPath>\SGECRYPT /?



Hints:

- A removable media drive is encrypted by the key as well as the algorithm. Please find out which algorithms for floppy and/or removable media drives are being used at each workstation.

  Example: Floppies of your computer are encrypted with a DES algorithm. You store important data on a floppy disk so that you can call it up again on another computer. If the floppy drive of this workstation is encrypted with IDEA, access to the data will be denied.

- Attention must be paid if encrypted floppies/removable medias should be read within a not encrypted drive and vice versa. If you insert a encrypted floppy/removable medium in a not encrypted drive a message will be prompted that the file system of your is not correct. By formatting because of this message all files stored are going to be deleted. If a removable media/floppy is accessed but cannot be read e.g. because encryption is active a new message appears informing the user that by formatting the floppy all data are deleted.
- The right to switch the encryption of floppies and/or removable media drives on/off in the SafeGuard Easy administration is effective immediately, while the granting of new rights for SGECRYPT only takes effect after rebooting.
- Within the SafeGuard Easy administration the encryption state for each removable media drive can be set separately. By changing the encryption state with SGECRYPT all removable media drives are effected, which means that all removable medias are encrypted or not until system is rebooted.

5.3 Central Configuration

Administrators can determine the entire configuration of the security mechanisms prior to distributing the software in order to install this solution throughout the company simply and without any further user intervention via so-called configuration files.

5.3.1 What is a Configuration File?

By using a configuration file you can install or remove SafeGuard Easy unattended. Already existing installations can be changed unattended, too.

You can predetermine in a configuration file all of data necessary for one of these operations. A configuration file is created by using the *Configuration File Wizard*.

The configuration file can then be used for installation in batch operations. It is not dependent on a particular system, which means that it can also be used on systems other than the one on which it was generated on. Only the SafeGuard Easy version used on the various systems has to be identical.

When creating a configuration file, SafeGuard Easy is not installed on your computer.

5.3.2 Creating a Configuration File

A configuration file can only be created using the *Configuration File Wizard*. Once the required settings and requirements have been made in the individual steps of the Wizard, a configuration file is created.

How to start the *Configuration File Wizard*:

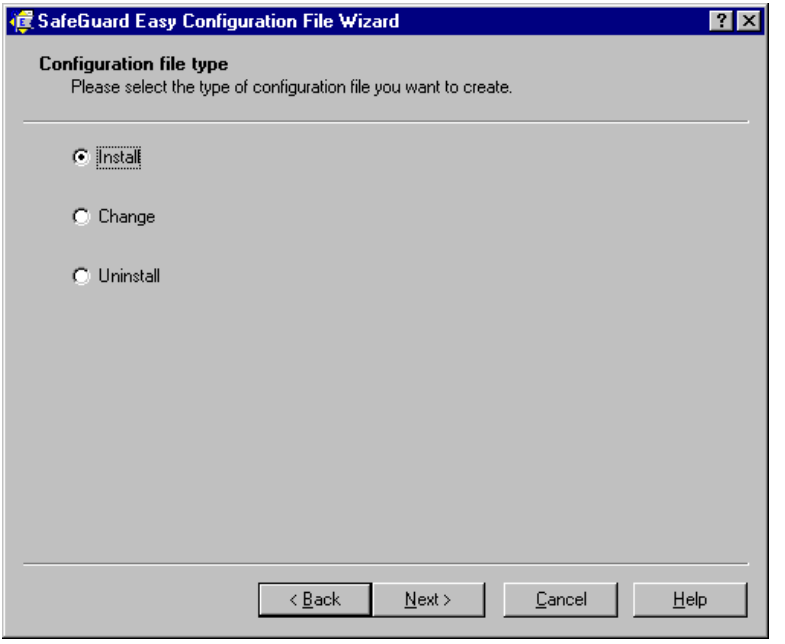
- Click the following one after the other in the Windows Start Menu: `Programs - SafeGuard Easy - Configuration File Wizard`

- or -

- start the program `CFGWIZ.EXE` in the SafeGuard Easy directory that was selected during the installation.

After the welcome screen has appeared, you are guided through the wizard step by step.

1. After the Welcome screen the dialog box *Configuration File Type* appears.



You can select from among the following file types here:

- **Install**

  If you want to install SafeGuard Easy unattended you have to create a configuration file with the attribute “Install”. By running this file SafeGuard Easy will be installed on a workstation.

- **Change**

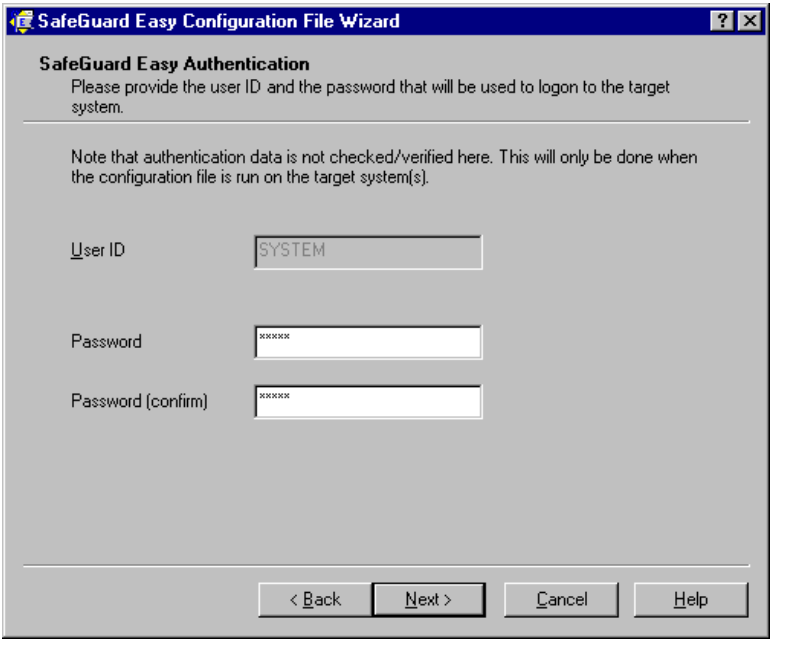
  If you want to change an existing SafeGuard Easy installation/ configuration you must select this option.

- **Uninstall**

  If you want to uninstall SafeGuard Easy unattended you have to create a configuration file with the attribute "Uninstall". By running this file SafeGuard Easy is removed from the workstation.

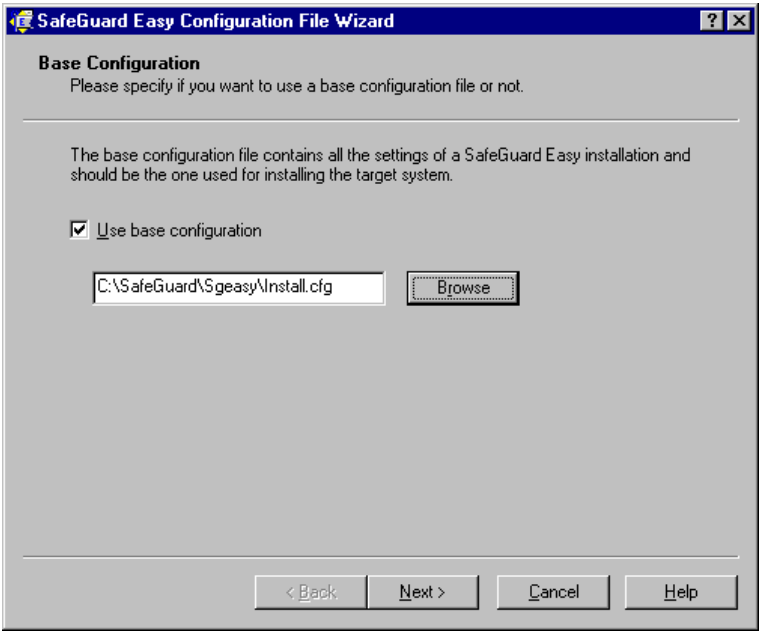
☞ *Choose a configuration file type and click [Next].*

2a. With the file type "Uninstall" the dialog box *SafeGuard Easy Authentication* appears.



After SYSTEM password has been entered and confirmed, the *Configuration File Wizard* jumps onto the dialog *Target Directory* (step 6).

2b. With the file types “Install” and “Change” the dialog box *Base Configuration* appears.



You can decide if you want to choose the settings of an already existent configuration file as the basis for your new configuration file.

As a base configuration only an “Install” configuration file can be used.

- **File Type Install**

  Without base configuration
  If configuration file type "Install" was chosen, you can create a new configuration file without any preconditions.

  With base configuration
  Configuration file type "Install with base configuration" loads the settings of the base configuration file. You can change the settings of this base configuration file. Additionally it's possible to advise a new file name to the changed base configuration file and save it.

- **File Type Change**

  Without base configuration
  It's possible to change the configuration of already existing workstations provided that configuration of the target workstation is known.

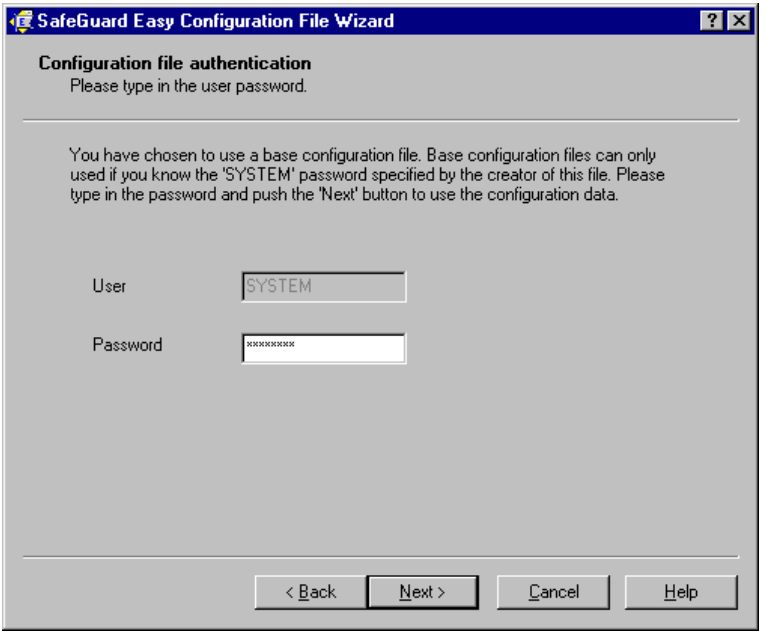
  With base configuration
  To avoid having to re-install the system, you can now create a new configuration file which makes the desired changes based on the settings of the configuration which already exists.

  If you want to use an existing configuration file, select the checkbox "Use Basic Configuration". Click the [Browse] button and select the file (e.g. "Install.CFG") from the appropriate directory.

☞ *If a base configuration file is used, Step 3 appears otherwise the wizard jumps to Step 4.*

☞ *Click [Next].*

3. If a base configuration file is selected the dialog box *Configuration file authentication* appears.

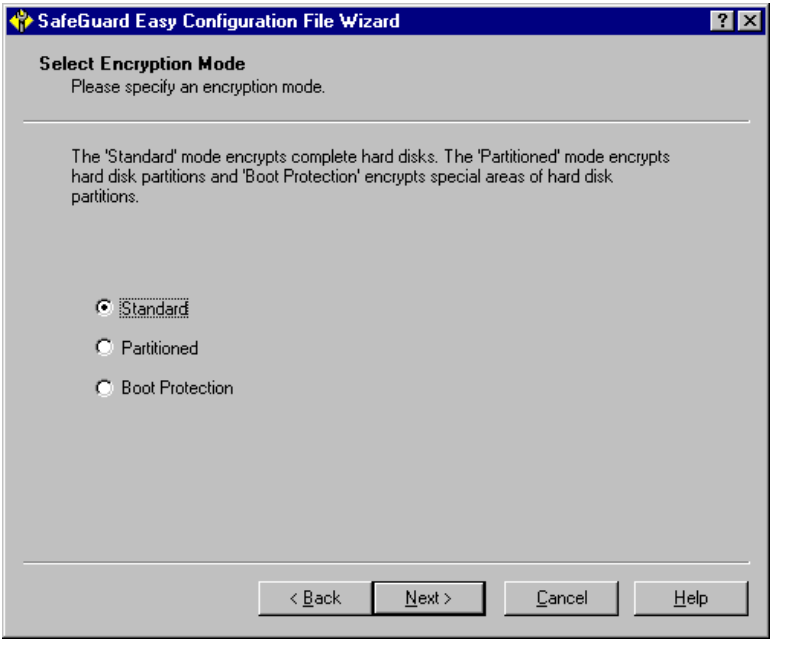


You must enter access data of the SafeGuard Easy user SYSTEM who had created the base configuration file.

If a configuration file without base configuration is to be created the *Configuration File Wizard* jumps to step *Encryption Mode* (file type "Install") or *workstation settings* (file type "Change").

☞ *Click [Next].*

4. **The encryption mode for encrypting the hard disk of your workstation is defined in the dialog box *Select Encryption Mode*.**



The dialog box only appears if file type “Install” was selected. To find detailed descriptions see page 32.

☞ *Click [Next].*

5. **The dialog boxes following now are *Workstation Settings*, *Users*, *Encryption* and *Master Boot Record*.**

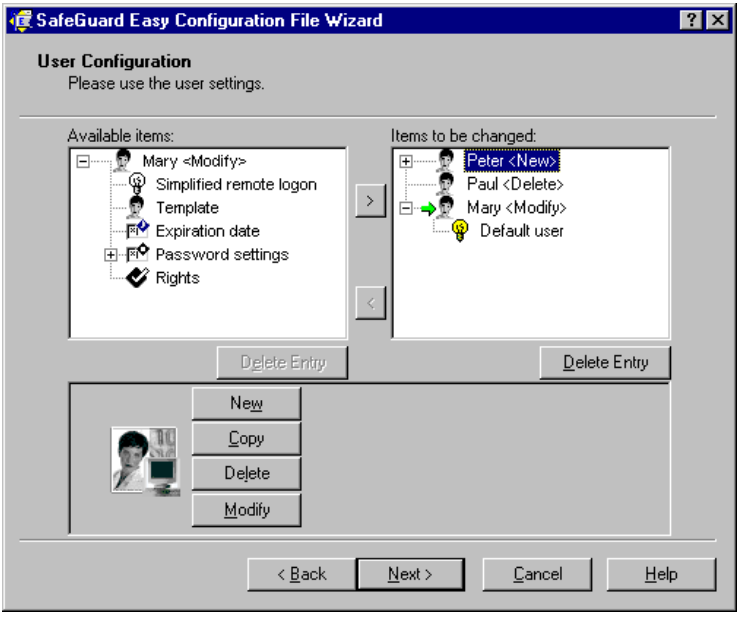
Select the settings SafeGuard Easy is to be installed. To find detailed descriptions see the corresponding chapters.

- **File type "Install"**

  If you choose configuration file type "Install" (with or without base configuration) you can determine the configuration file step by step - comparable to installation and administration.

- **File type "Change"**

  If you've selected configuration file type "Change" (with or without base configuration) a divided screen appears.



Under “Available items” in the Workstation, Encryption, User and Master Boot Record dialog boxes you’ll find the default SafeGuard Easy settings. If base configuration was set on the left-hand side (“Available items”) you can see the settings predefined in this base configuration file. Select the settings you want to change and afterwards press the arrow-button. The selected setting is now transferred onto the right (“Items to be changed”) and changes can be made. To remove select the setting on the right and move it to the left-hand side. Changes done before are now deleted.

Changed functionalities

By using a configuration file with the attribute “change without base configuration” please note the functionality of the [New], [Copy], [Delete] button and the additional [Modify] button in the user tab.

[**New**]**:** After clicking [New] you have to type in a new user name. A new SafeGuard Easy user is created when the configuration file is run (see user “Peter”).

[**Copy**]**:** Mark an already existing user. Afterwards click the [Copy] button an define a new user name. A new SafeGuard Easy user having all the settings of the copied user is generated (see user “Peter”).

[**Delete**]**:** By clicking [Delete] you create a user that is to be removed on the target system (see user “Paul”).

[**Modify**]**:** With [Modify] you can change the profile of a existing user on the target system (see user “Mary”).

[Delete Entry] removes a user profile from the list.

☞ *Click [Next].*

6. The dialog *Target Directory* appears.

You can determine in the dialog box *Destination of configuration files* the path in which you want to store the configuration file.

Please note remarks regarding file type “Change” with base configuration file:

By clicking [Save] you're asked if you want to replace the existing base configuration file. If you do so by clicking [Yes] all changes stored in the change file will be overwritten into the existing base configuration. By clicking [No] only the change configuration file is created. The base file remains the same. By changing the name of the base configuration the original base file remains and a new one including base and change file informations will be created.

It's recommended here to create a new base configuration file in order to retain your original base configuration file.

To avoid problems it’s recommended to write down the characteristics of the configuration file settings.

Editing a Configuration file

Configuration file type “Install” can be edited, whereas already existing “change” and “uninstall” file types cannot be changed later on.

How to edit a configuration file:

1. Start the *Configuration File Wizard*.
2. Select configuration file type “install”.
3. In the dialog box *Base configuration* call up the install-file to be changed.
4. Click [Next] and the configuration file will be loaded.

5. Now settings regarding Workstation settings, User, Encryption and Master Boot Record are displayed and can be changed.

Trying to open up a “change” or “uninstall” file a error message is displayed.

5.3.3 Run a Configuration File

To activate predefined settings, the configuration file has to be run. How to run the configuration file depends on the configuration file type.

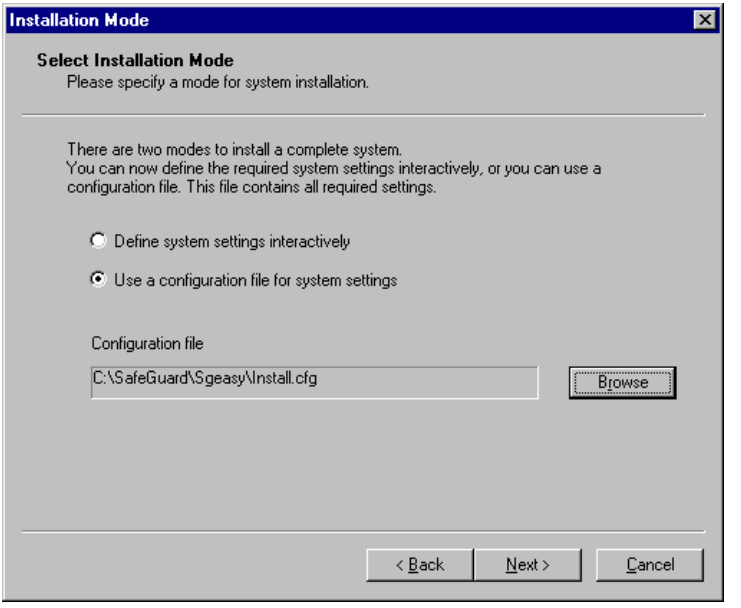
Run File Type “Install”

File type “Install” is to be run during the installation of SafeGuard Easy within the dialog *Select Installation Mode* or by using a response file.

If SafeGuard Easy was installed with an “install” configuration file on a workstation, no further configuration file with type “install” can be run on this machine.

Run during installation

During the installation of SafeGuard Easy the dialog box *Select installation mode* appears (see page 30).



Click “Use a configuration file for system settings”, select the drive and directory for the desired configuration file. Click [Browse] and select the configuration file. After clicking [Next], SafeGuard Easy is installed with the settings determined in the configuration file without any further user interaction. To find out how to create a configuration file, please see page 98.

Run with a response file

To install SafeGuard Easy without any user interaction, it is necessary to create a configuration file with the attribute “install” (see page 98). This configuration file has to be included into a response file (see page 111).

The response file is run as follows:

1. Start MS Dos mode or call up the Run command in the Windows Start Menu.
2. Switch to the directory where SafeGuard Easy is stored (e.g. a network drive).
3. Enter the command

   `SETUP.EXE /f:`*<Path and name of response file>*

   in the command line and then click [OK].

Example:

An unattended installation of SafeGuard Easy can e.g. be started with

```
C:\SGEasy\Disk1\SETUP.EXE /f:D:\Install.txt
```

With this command, the response file is now called up and SafeGuard Easy is installed without any user interaction.

With an unattended installation the settings will be activated after a second reboot.

The parameters for `SETUP.EXE` are displayed when you call up the program as follows:

```
SETUP.EXE /?
```

Run File Type “Change” and “Uninstall”

Configuration file type “Change” and “uninstall” are run by the program `EXECCFG.exe`.

They are run as follows:

1. Start MS Dos mode or call up the Run command in the Windows Start Menu.
2. Switch to the directory SafeGuard Easy configuration file is stored (e.g. a network drive).
3. Enter the command

   `EXECCFG.EXE /f:`<*Path and name of configuration file*>

   in the command line and then click [OK].

Parameters regarding `EXECCFG.EXE` are displayed with the command

```
EXECCFG.EXE /?
```

Additionally `EXECCFG` supports the parameter `/Reboot` to issue a shutdown after the defined configuration file is executed successfully.

Example:

```
C:\SGEasy\EXECCFG /f:D:\Deinstall.cfg /Reboot
```

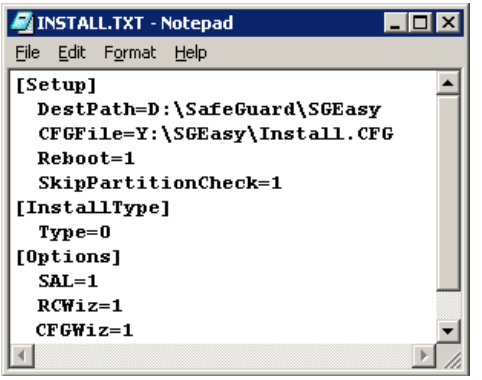
With this command, a configuration file is now called up and SafeGuard Easy is removed without any user interaction and a reboot is issued.

5.3.4 Creating a Response File

To automate SafeGuard Easy installation, a file has to be created with which the setup procedure can be controlled.

A response file can be created with a text editor (Notepad, Edit etc.) and stored with a file name of your choice. It has to be available in ASCII format and can be modified by the administrator at any time.

A response file (named e.g. `Install.txt`) to install SafeGuard Easy could look like this:



With this sample file SafeGuard Easy is installed with Secure Auto Logon, *Response Code Wizard* and *Configuration File Wizard*. The target directory of the SafeGuard Easy installation and source of the configuration file are given by the parameters `DestPath` and `CFGFile`. If a non-dos partition is detected during installation, installation will be continued (`SkipPartitionCheck`). After SafeGuard Easy has been installed the system will be automatically rebooted (`Reboot`).

Parameters of a Response File

Please note that entries in square brackets must be taken over into the response file in precisely the same form.

[Setup]

`NoSgeGinaSystem=1`

Surpresses the installation of the Utimaco SafeGuard GINA.

CAUTION !
WE DO NOT RECOMMAND TO USE THIS FEATURE !

If you do not install the Utimaco-Gina some features of SafeGuard Easy will not be available after installation:

- no display of the encryption/decryption process dialog if the user is not logged on (for Windows NT/2000/XP)
- no automatic restore of permanent settings (encryption, key) for floppy disk drives and removable disk drives if user logged off.
- SAL (Secure auto logon) will not work.
- workstation lock will not work (for Windows 95/98)

THE UTIMACO-GINA SYSTEM IS AN IMPORTANT FUNCTIONAL PART OF SAFEGUARD EASY AND WILL BECOME EVEN MORE IMPORTANT IN THE FUTURE TO REALIZE NEW FUNTIONALITIES. IF THE GINA IS NOT INSTALLED SOME OF THESE FUNTIONALITIES WILL NOT BE AVAILABLE AFTER MIGRATION TO A NEW VERSION OF SAFEGUARD EASY ! THE MISSING GINA COULD EVEN INJURE A FUTURE MIGRATION !

`CFGFile=<Path>`	Enter the name of the configuration file and the path, which contains the configuration file. This command line is only required with complete installations.
`DestPath=<Path>`	Path SafeGuard Easy is to be installed. Ensure that the path details are correct and written in full.
`Reboot=<0,1>`	Determines how the system is to react after the successful installation of SafeGuard Easy. There will be no restart without an Reboot command in the response file. 0 = No Restart 1 = Restart
`SkipPartitionCheck=<0,1>`	Determines how the system is to react if a non-dos-partition is recognized during installation. 0 = Installation will be aborted 1 = Installation will be continued
`DisableEDWizAutostart =<0,1>`	Determines, if the emergency disk wizard is to be started after installation. 0 = Wizard is started automatically (Default setting!) 1 = Wizard will not be started
`SgeKernelInstDrive= <drive name>`	Defines the drive, the SafeGuard Easy system kernel data are stored on To define the kernel installation drive can be helpful for example if you will restore the Windows system partition with tools like GHOST and this operation would remove the SafeGuard Easy Kernel because it is always stored on the system partition. `e.g. SgeKernelInstDrive=C` **Note: This feature is only available for Windows NT/2000/XP !**

[InstallType]

`Type=<0,1,2>`	Defines the installation type of SafeGuard Easy. 0 = Complete System 1 = Runtime System 2 = Administration utilities To do an unattended installation [Install Type] has to be Type=0 (=complete installation).

[Options]

`CfgWiz=<0,1>`
`SAL=<0,1>`
`RCWiz=<0,1>`
	CfgWiz = Configuration file wizard
	SAL = Secure Auto Logon
	RCWiz = Response code wizard
	0 = Option won't be installed
	1 = Option will be installed
	
	Depending on the installation type the following options can be installed:
	Complete System: CfgWiz, SAL, RCWiz
	Runtime system: none
	Administration utilities: CfgWiz, RCWiz

5.4 Remote Help

Remote help allows remote help for workstations protected by SafeGuard Easy. It serves to help users out of emergency situations. using remote maintenance a user can obtain special rights on a temporary basis. The following rights can be assigned:

- Uninstall SafeGuard Easy
- Set new user password
- One-time logon
- Temporarily grant right to switch floppy encryption

Remote help is done by using challenge/response.

The user who needs help has to create a challenge code. The challenge code is displayed to the user on his/her PC as an ASCII character string (14 characters). The user who can assign certain rights (e.g. the SafeGuard Easy administrator) creates a response code. After exchanging the codes the right is assigned to the user who needs it.

5.4.1 Creating a Challenge Code

Depending on the action to be executed, a challenge code is created in different ways:

Set new user password
One-time logon
Temporarily grant right to switch floppy encryption

Starting the system with PBA the user has to enter his/her user name at the PBA, switch into the password field and then press [F9]. The challenge code then is displayed.

Starting the system without PBA a green floppy disk symbol appears in the top left-hand corner of the screen for a few seconds when booting the computer,. The user has to press [F2] during this period. The PBA logon dialog box appears.The user has to enter his/her user name at the PBA, switch into the password filed and then press [F9]. The challenge code then is displayed.

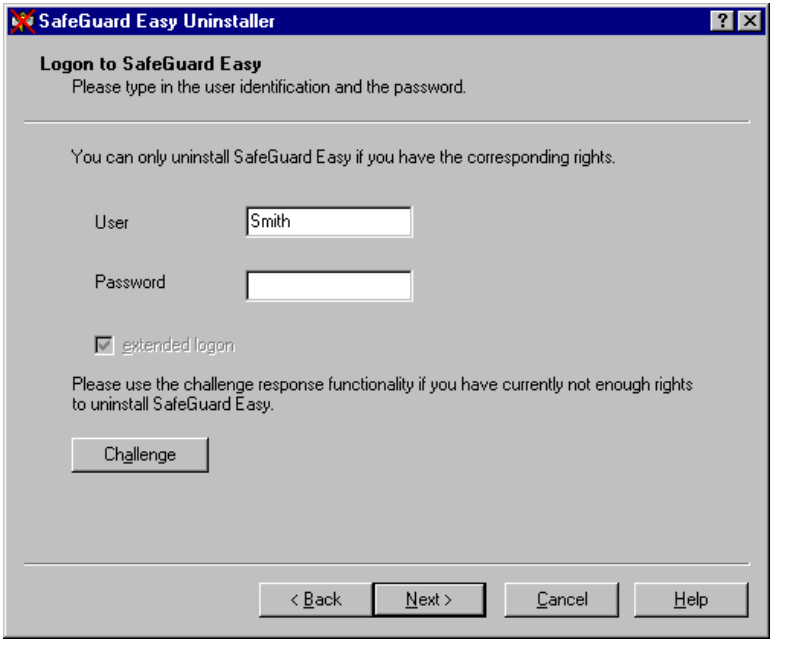
The challenge code is displayed to the user on his/her pc as an ASCII character string (14 characters).

Deinstallation

With the challenge/response procedure the user can be authorized to remove SafeGuard Easy from his/her workstation.

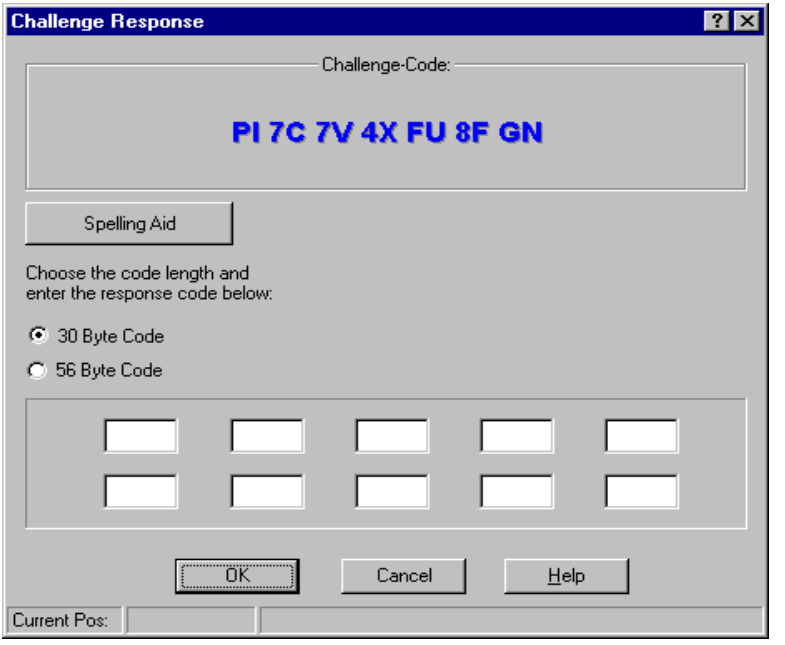
In the Windows-Start menu the user has to choose `Programs - SafeGuard Easy - Uninstall`.

The dialog box *Logon to SafeGuard Easy* pops up and the user has to enter his user ID.



If only the password field is activated click “Extended Logon”.

To initiate the challenge/response procedure the user has to press the [Challenge] button. The challenge code is displayed to the user on his/her PC.



Deinstallation cannot be started within the SafeGuard Easy logon screen. It can only be started once the user has logged on to the machine.

5.4.2 Create a Response Code

To generate a response code, the user must be registered as a SafeGuard Easy user at the workstation of the remote user.

The user creating the response code must have at least the same rights as the remote user. Additionally to allow a user running remote commands the user creating the response needs one of the following rights:

Remote Command	User right
Uninstall	Remove
Set new user password	Change user settings
One-time logon	Change user settings
Temporarily grant right to switch floppy encryption	Switch floppy drive encryption

To run a challenge/response process, SafeGuard Easy does NOT have to be installed on the computer on which the response is generated. It is sufficient if the administration tools, including the Response Code Wizard, are installed there.

A response code that entitles a user to execute a particular action, is created by using the *Response Code Wizard*.

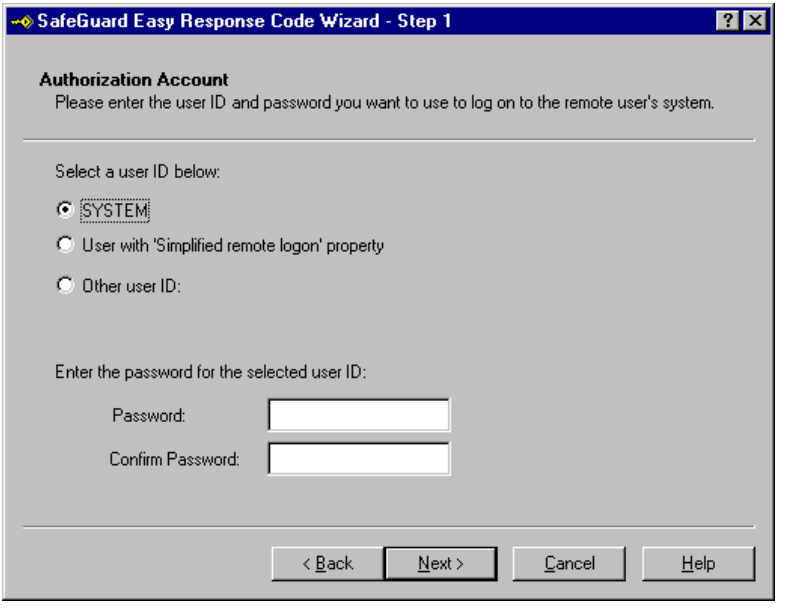
How to start the *Response Code Wizard* can be started as follows:

- Click the following one after the other in the Windows Start Menu: `Programs - SafeGuard Easy - Response Code Wizard`.

  -or-

- start the program `SGREMT32.EXE` in the SafeGuard Easy directory selected during installation.

1. After the Welcome screen the dialog box *Authorization Account* appears.



The user generating the response code must have a user account with the corresponding rights on the remote user's computer.

The following options are available here:

SYSTEM	The user SYSTEM is pre-set on every workstation fitted with SafeGuard Easy and it cannot be changed. It is used as the user name of the SafeGuard Easy System administrator.
User with 'simplified remote logon' property	Logon of that user with the characteristic "Simplified remote logon". Users who have this right are determined under "User Settings". This user has to have at least all rights of the local user on the target workstation.
Other user ID	Any SafeGuard Easy user that is registered on the target system.

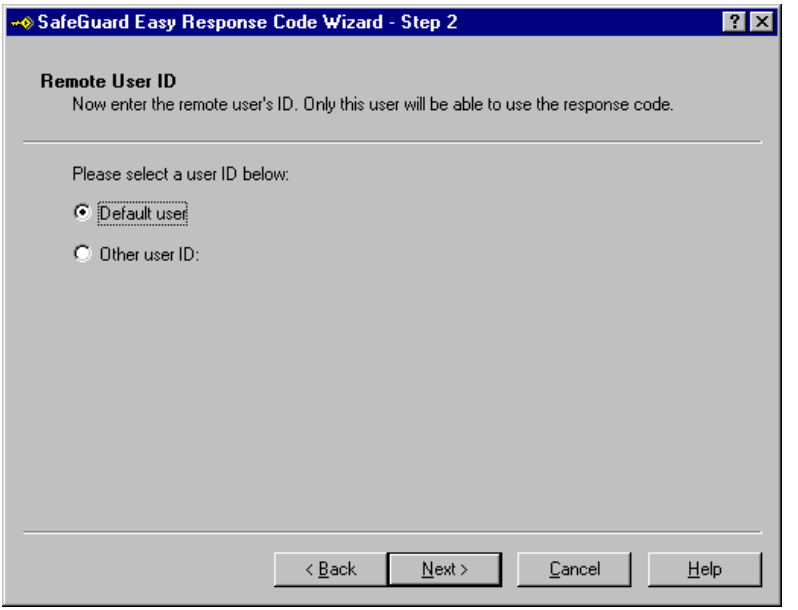
If the logon is done either by SYSTEM or the user with the 'simplified remote logon' property, a short response (30 characters) is generated, other user ID generates a long response (56 characters).

The reason for the different number of characters is as follows: Choosing the user ID "SYSTEM" or "simplified remote logon" only the corresponding passwords are taken into consideration when generating a response (short response=30 characters). With "Other user ID", the Response Code Wizard includes the user identification in the generation process, this increases the number of characters to 56.

Once you have selected the appropriate user ID, please enter the corresponding password in the field **Password** and confirm it in the next field.

☞ *Please proceed by clicking [Next].*

2. The dialog *Remote User-ID* appears.

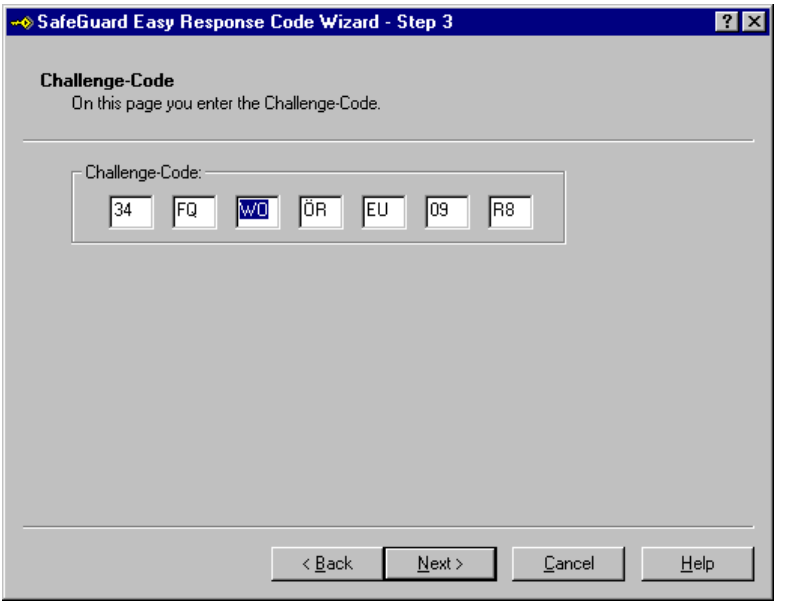


Within the dialog box *Remote User-ID* the user name of the user asking for help. There are two options.

Default User	User is registered on the target system as default user and logs on by entering his/her SafeGuard Easy password only. Accordingly he/she does not know the corresponding user name.
Other user ID	User logs on by entering his/her SafeGuard Easy user name and password. Therefore he/she knows the user name.

☞ *Please proceed by clicking [Next].*

3. The dialog *Challenge Code* is displayed.

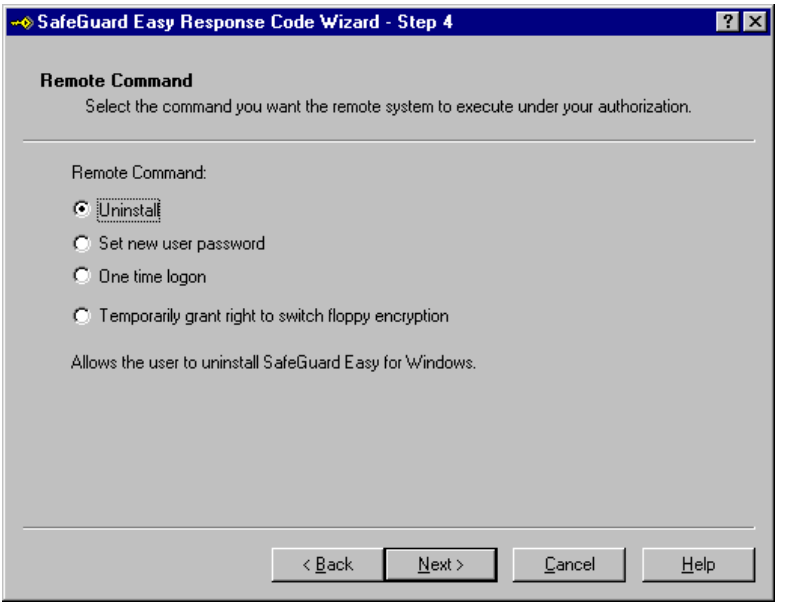


The challenge code is displayed to the user on the target system as an ASCII character string. This string consists of 14 characters divided into pairs.

The challenge code is to be entered into the fields.

☞ *Once you have entered the sequence of characters correctly, you can proceed by clicking [Next].*

4. The dialog box *Remote Command* is displayed.



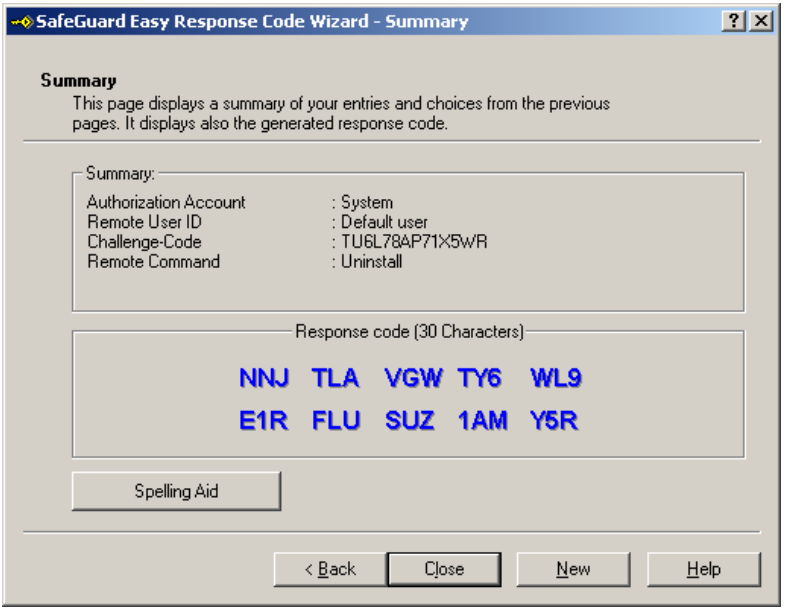
Remote command determines the actions to be executed.

Uninstall	The user is authorized to remove SafeGuard Easy from his/her workstation. This type of removal is only required if the system administrator is not on site.
Set new user password	If a user has forgotten his/her password or waiting period at PBA has increased enormously with the help of a Challenge Response wizard, the user can define a new password in the PBA without knowing his old one. The SYSTEM password cannot be reset by challenge/response.

One time logon	If another user wants to execute an action on a workstation (e.g. installation of new software packages by an external technician), he/she is granted access to the computer in question for one session only. The external user is logged on with the *AUTOUSER's rights.
Temporarily grant right to switch floppy encryption	A user is authorized to switch the floppy drive encryption on or off for a one time logon. The key for the floppy drive must be already set.

☞ *Proceed by clicking [Next].*

5. The dialog box *Summary* appears.



In the final screen you will receive a complete overview of the settings you have selected in the preceding dialog boxes of the *Response Code Wizard*. The Authorization Account, Remote User ID, challenge code and Remote Command are listed once again in Summary on one page so that you can verify once again the correctness of the listed data.

Response Code

The response code field displays the generated response. That code must be given to the user. The user then enters the response code in his/her PC and is logged on once the data has been verified.

Please note that the response code is only valid once, a new one is generated with every request.

Spelling Aid

If you press the button [Spelling Aid], a window appears which is split into three columns, each with one of the following headings. Under Position, you can see the position taken up by each character within the code. In this way, inquiries can be answered immediately without investing a great deal of time (such as counting the positions). You can see which character to enter under the heading with the same name. Alphabetic indicates the word with which the characters can be "linked" in order to avoid confusion. As a rule, first names are used, the first letters of which are then entered into the code fields.

☞ *If all of the entries are correct and the inquiring user was able to execute the necessary actions, the Response Code Wizard is closed by clicking [Close]. If you wan to make some changes in previous steps click [Back]. With [New] all entries are deleted and a new response code can be created.*

5.5 Entries in the Event Log Protocol

The following SafeGuard Easy events are entered into the Windows NT/2000/XP event log protocol:

- Successful/ failed installation
- Failed uninstall
- Successful/ failed execution of a configuration file (attribute “Change”)
- Beginning/completion of the encryption/decryption process
- Completion of the encryption/decryption process

To view the entries click the following one after the other in the Windows Start Menu: `Programs > Settings > Control Panel > Administrative Tools > Event Viewer.`

Under “System Log” you find the SafeGuard Easy entries within the “Source” field. By double clicking one of these SafeGuard Easy events the dialog box “Event properties” pops up. Within “Description” the corresponding SafeGuard Easy event is displayed.

Following events can be displayed within the event log:

Message Id=24
Installation of SafeGuard Easy was completed successfully.

Message Id=25
The first phase of the uninstall procedure of SafeGuard Easy was completed successfully.

Message Id=203
All required encryption/decryption completed successfully.

Message Id=204
The encryption/decryption process was started successfully.

Message Id=1167
Execution of the configuration file *[filename]* failed.

Message Id=307
The execution of the configuration file *[filename*] has been completed successfully.

Message Id=1098
Installation of SafeGuard Easy has failed.

Message Id=1099
Uninstall of SafeGuard Easy has failed.

6 Removing System Errors

If your computer displays a SafeGuard Easy system error with an encrypted hard disk drive, this means in almost all cases that the system kernel of SafeGuard Easy cannot be found.

Occurring errors are corrected with an emergency disk. Using the emergency disk you can

- restore the saved system kernel,
- repair the system kernel,
- decrypt encrypted areas and remove the PBA.

6.1 Emergency Disk/Kernel backup

If your PC has a system error, you need an emergency disk, that contains the emergency tools and the backed up current system kernel. This emergency disk is created by using the emergency wizard.

The emergency wizard starts unattended when the workstation reboots for the first time after SafeGuard Easy was installed. It's possible to save the kernel later, too.

Utimaco recommends to backup the kernel of every workstation regularly.

How to start the emergency wizard:

- Click the following one after the other in the Windows Start Menu: `Programs - SafeGuard Easy - Emergency Wizard`

- or -

- start the program `EDWizard.EXE` in the SafeGuard Easy directory that was selected during the installation.

1. If you want to create a kernel backup, the *Choice* dialog box appears.

Create kernel backup only	A kernel backup is done only.

Create kernel backup and copy the SafeGuard Easy emergency tools	Kernel and the following files are copied: - `SGEASY.EXE` - `Sgeasy.hmf` - `Sgecrypt.mod` - `Sgenls.mod` - `Sgekrnl.mod`

2. The *Path Info* dialog box appears.

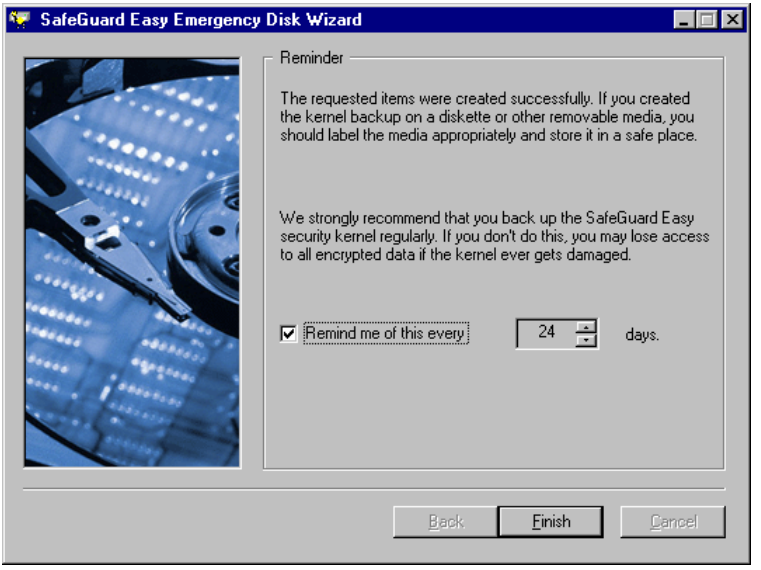
Here you can select the directory, where the target files (kernel backup and SGE emergency disk tools, if selected) should be copied.

You can also define a name for your kernel backup file. The names of the emergency disk tools are always the same, and should not be changed.

If you have created several backup files, you should ensure that the file name indicates the backup status.

*The system kernel can only be backed up to a **non** encrypted floppy/removable medium.*

3. The Reminder dialog box appears.



At this point you will be asked if you want the Emergency Disk Wizard starting automatically or not. In the former case you can also specify the frequency in days at which the wizard will start each time after a successful kernel backup.

On this window and independently of the start mode you can always enable/disable the automatic start of the Emergency Disk Wizard. The frequency can only be set and has just a sense if the automatic start is enable.

Hints

- **Backup kernel**
  Encryption (floppy or removable medium) is switched off during kernel backup.
- **Emergency files**
  The emergency files
  - `SGEASY.EXE`
  - `Sgeasy.hmf`
  - `Sgecrypt.mod`
  - `Sgenls.mod`
  - `Sgekrnl.mod`

  are stored on the SafeGuard Easy installation CD or the program's installation directory.
- **Backup from command line**
  In addition with the `SGEBACK.EXE` program you can back up the system kernel from the command line, without starting the SafeGuard Easy administration:
  `SGEBACK` <*Target file*>
- **Location of kernel**
  If the Windows boot partition is not located on the first hard drive, the SafeGuard Easy system kernel is automatically stored on the C: partition during installation. This partition should therefore not be formatted after installation because it contains the most important Windows information (system kernel, driver etc.). If it is formatted after the installation of SafeGuard Easy, then the system has to be re-installed.

6.2 Recover kernel

To eliminate system errors please proceed as follows:

1. Boot the system from drive A and insert the emergency disk.
2. Call the program `SGEASY.EXE`.
3. A menu with **Restore**, **Repair** and **Uninstall** appears.

By using this functions you can try to remove system errors.

If the kernel is not damaged option "Uninstall" is active and also SafeGuard Easy password check appears. Otherwise only the options "Restore" and "Repair" are active.

Once SafeGuard Easy is installed and the hard disk drive is encrypted running `SGEASY.EXE` *will cause an error message. The program's reaction is correct because only one encrypted partition is enough for this message to appear. Confirm the error message with [OK] and the menu with "Restore", "Repair" and "Uninstall" is displayed.*

6.2.1 Restore Kernel

With this function you can restore the system kernel from a kernel backup file in the case of a system malfunction. Naturally this assumes that you have backed up the system kernel at an earlier point in time.

How to backup the kernel see page 129.

Without a backup the kernel cannot be restored. Restore kernel may not be executed if the backup file does not correspond with the latest status. This applies if the encryption status of the hard disk(s) was changed between saving the system kernel and the restoration.

To restore the kernel that way a user has to know the SafeGuard Easy SYSTEM password. For security reasons the password should never be given to a user. Without knowing the SYSTEM password a user can restore the kernel by using the challenge/response procedure (see page 138).

To restore the kernel please proceed as follows:

1. Boot the system from drive A and insert the emergency disk.
2. Call the programm `SGEASY.EXE`
3. In the following menu select “Restore”.
4. A dialog box appears in which you can specify the drive, the directory and the backup file.
5. Click [OK].
6. Enter the SafeGuard Easy SYSTEM password.

If the data is correct, restoring of the system kernel then begins and the kernel is restored to the status of the last kernel backup.

6.2.2 Repair Kernel

Select **Repair** if you do not have a current backup of the system kernel.

This function is only necessary if there is no backup of the system kernel or if the backup file does not correspond to the latest status of the system kernel. This applies if the encryption status of the hard disk(s) was changed between backing up the system kernel and the occurrence of the system error.

To repair the kernel proceed as follows.

1. Boot the system from drive A and insert the emergency disk.
2. Call the programm `SGEASY.EXE`.
3. In the following menu select “Repair”.

A diagnostic routine attempts to localize the system kernel and to repair it. This can take several minutes. A message then appears informing you if the repair was successful or not.

*The attempt to avoid a system error using the **Repair** menu item is not always successful. For this reason you should always have a current backup of the system kernel.*

6.2.3 Deinstallation after System Error

If the system error cannot be eliminated either with **Restore** or **Repair**, the option **Uninstall** has to be used.

To uninstall SafeGuard Easy after a system error a user has to have the right to remove SafeGuard Easy from a workstation. If not the removal can be done by using the challenge/response procedure (see page 138).

Please proceed as follows:

1. Boot the system from drive A and insert the emergency disk.
2. Call the programm `SGEASY.EXE`.
3. In the following menu select “Uninstall”.
4. Type in the SafeGuard Easy user password.

After that, encrypted files on the hard disk will be decrypted and two automatic reboots will be carried out.

After an emergency uninstall SafeGuard Easy folder and icons remain. They will be completely removed by clicking the “uninstall” command in the SafeGuard Easy folder again. After that, SafeGuard Easy is uninstalled completely. In addition, you should carry out a volume check in Windows. For further information refer to your Windows documentation.

6.3 Removing System Errors with Challenge/ Response

Until the SafeGuard Easy SYSTEM password (”Restore Kernel”) or the user password (”Uninstall”) is required, the user goes on as described. Because he / she does not know the SYSTEM password to restore the kernel or has not the right to uninstall, the user initiates the challenge/ response procedure by pressing [F9]. The challenge code is displayed. The user gives the challenge code to the SafeGuard Easy administrator (e.g. by phone).

To generate a response code the SafeGuard Easy administrator has to proceed as follows:

1. Start the *Response Code Wizard*.
2. He/she selects the user name SYSTEM and types in the SYSTEM password in the dialog box *Authorization account*.
3. Click [Next].
4. The dialog box *Remote user ID* appears. Various entries has to be made:
   - **Restore:**
     Other user ID: “USER”
   - **Deinstall:**
     - Other user ID: <*SafeGuard Easy user name* >
     or
     - Default user
5. Click [Next].
6. In the next step, the administrator enters the challenge code he/ she was given.

7. Click [Next].
8. As the *Remote Command* the administrator selects
   – **Restore:** One-time logon
   Deinstall: Uninstall
9. By clicking [Next] the response code is created.

The response code is displayed in the dialog box *Summary* as an ASCII character string (30 or 56 characters in groups of three). SafeGuard Easy administrator now informs the user about the created response code that has to be entered on the target machine.

If the result is valid, the entered response is accepted and the user is subsequently entitled to execute the action authorized by the administrator.

6.4 Emergency Start

If a system error occurs, you can carry out an emergency start, to regain access to your PC.

Encrypted/not encrypted system disk

If floppy encryption is enabled you must use an encrypted system disk. The algorithm and key of the system disk must be identical with the settings of the workstation encryption for the floppy drive. This means that if the floppy drive was encrypted with the algorithm IDEA and the key "Utimaco", the system disk must have these properties too. If floppy encryption is disabled, an unencrypted system disk will suffice.

To implement the emergency start you have to distinguish if SafeGuard Easy is installed with the PBA option switched on or off.

Without PBA

If a system error occurs and PBA is switched off by activated hard disk encryption, you cannot boot the system from drive A. If PBA is switched off, a green floppy icon appears in the top left of the screen for five seconds when booting. If you press the [**F2**] key in this time, the PBA logon screen appears. Insert a system disk in the floppy drive. Afterwards enter your SafeGuard Easy password in the PBA logon screen and confirm your entry. The PC then boots from the floppy. You obtain access to the system and do any repairs which may be necessary.

With PBA

If SafeGuard Easy is installed with the PBA option, wait until the password prompt appears. Insert a system disk in the floppy drive. Afterwards enter your SafeGuard Easy password in the PBA logon screen and confirm your entry. The PC then boots from the disk. You obtain access to the system and do any repairs which may be necessary.

7 Migration

If you have already installed a previous version of SafeGuard Easy on your workstation, you can easily run a system update. Parameters already set (user name, user password etc.) are maintained here.

To run a migration it´s necessary to have one of the following Safe Guard Easy versions already installed:

- Windows 2000: Version 1.0 and Version 3.0
- Windows NT: Versions 1.02 (incl. all Service Packs), 1.15 (incl. Service Release 1)
- Windows 95: all versions
- Windows 98: all Versions

SafeGuard Easy Windows 95/98
SafeGuard Easy Windows NT v1.01 und 1.02

Please note that when the system is updated, a person defined as a user in the previous version automatically migrates to become a default user in the new version of SafeGuard Easy.

A migration can be run either during installation or unattended by using a response file.

To migrate previous versions to present SafeGuard Easy the so-called *Migration Wizard* is used. Within the *Migration Wizard* the SafeGuard Easy user SYSTEM creates a migration file (Sgemig.cfg). The file con-

tains the user SYSTEM's access data in order to open the existing SafeGuard Easy kernel and create a new one. The file can also be used on systems other than the one on which it was generated. Only the SafeGuard Easy version used on the various systems has to be identical.

To run the migration file on different workstations it has to be included into a response file. The response file afterwards has to be executed on every workstation.

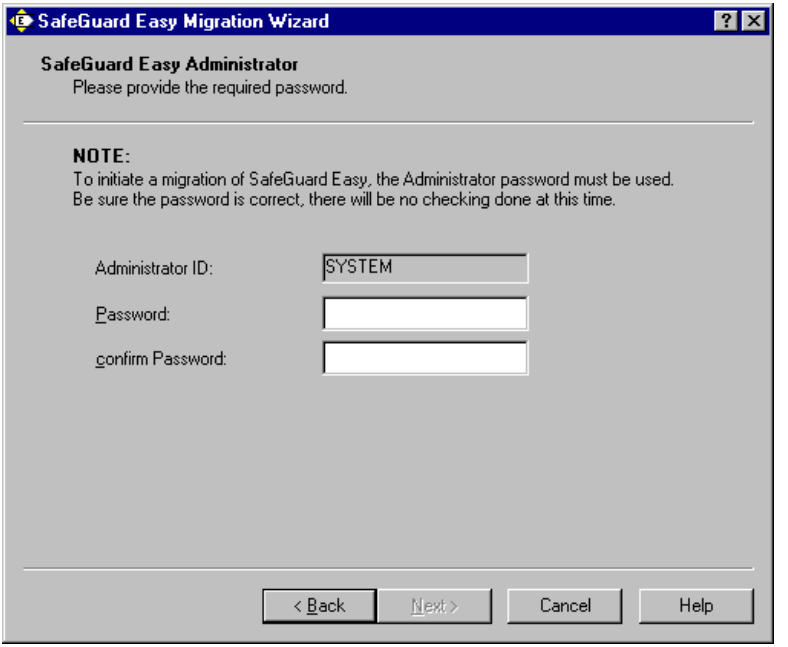
Configuration File Wizard and Response Code Wizard are not installed automatically during a migration. They can be activated later on.

Please note that when the system is updated, the person defined as "USER" in the previous version automatically migrates to become a default user in the new version of SafeGuard Easy.

7.1 Interactive Migration during Installation

If SafeGuard Easy detects an older version of the program on the workstation, a dialog is displayed. After confirming that dialog the *Migration Wizard* is started.

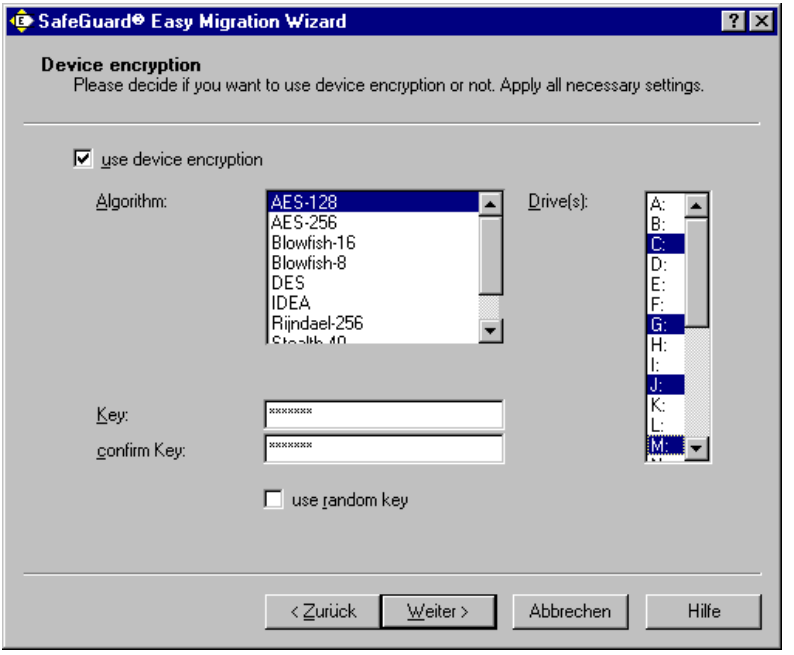
1. The dialog *SafeGuard Easy Administrator* is opened.



If you are logged on as the SafeGuard Easy user SYTEM, the field Administrator-ID displays the user name. The field cannot be edited. Enter the SYSTEM password and confirm it.

☞ *If all the information is correct, you can proceed by clicking [Next].*

2. The dialog box *Device Encryption* is displayed (only for SafeGuard Easy 1.01 and 1.02 for Windows NT).



In versions 1.01 and 1.02 for Windows NT, it was not possible to encrypt removable media drives (such as ZIP drives). In this dialog box you can add this feature.

Use device encryption	Device encryption is activated
Algorithm	Select the algorithm you want to encrypt the removable media drives with.

Drive(s)	Determine which drive letters are to be designated to the removable media drives.
Key	Enter key
use random key	Random key is used

Please note the hints regarding the encryption of removable media drives listed on page 54.

☞ *If all the information is correct, you can proceed by clicking [Next].*

3. The dialog box *Target directory* appears.

You can determine in the dialog box Destination folder the path in which you want to store the migration file. The program recognizes the directory in which the SafeGuard Easy previous version was stored and sets this path as the standard. The standard name for the file is `SGEMIG.CFG`.

By clicking the [Browse] button, you can decide for yourself the drive and directory in which the file is to be stored.

☞ *If all the information is correct, you can proceed by clicking [Next].*

4. The dialog box *Summary* appears.

In conclusion, you are given a complete overview of the settings you have selected in the previous dialogues of the *Migration Wizard*.

If these do not comply with the settings you require you can click the button [Back] to go back to the place in the Wizard where you want to make changes.

☞ *When you click [Next], the migration will be started and also the migration file will be created.*

All files of the new version of SafeGuard Easy are copied into a temporary directory. Please note that the older version of SafeGuard Easy is not yet replaced here. Once the update process has been completed, the system is rebooted. After reboot the Windows logon process is suppressed and the new program files of SafeGuard Easy are copied into the previous version´s directory and replace them. All registry entries and files no longer required are removed. The system shuts down automatically. The next time the system is booted, the new version is installed.

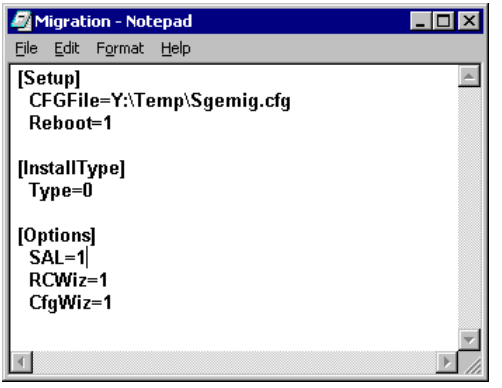
7.2 Unattended Migration with a Response File

In order to migrate older versions of SafeGuard Easy you have to create

- the migration file `Sgemig.cfg` with the *Migration Wizard*
- a response file with a text editor

The Migration Wizard will be installed if during the program´s installation either install type “complete“ or “administration utilities“ and the configuration file wizard was selected.
Migration Wizard is started by running the application `WIZLDR.EXE`.

A response file to run a migration (named e.g. `Migration.txt`) could look like this:



If the response file `Migration.txt` is run,

- all informations regarding migration are read from the file `Sgemig.cfg` in the directory `Y:\Temp`

- SafeGuard Easy will be installed completely (`Type=0`).

- Secure Auto Logon, Response Code Wizard and Configuration File Wizard (`SAL=1, RCWiz=1, CfgWiz=1`) are installed.

- the system is rebooted after running the response file (`Reboot=1`).

A response file for an unattended migration is performed as follows:

1. Call up the SafeGuard Easy setup program via the RUN command in the Windows Start Menu.
2. Switch to the SafeGuard Easy directory.
3. Enter the command

   `SETUP.EXE /u /f:`<*Path and name of response file*>

   in the command line and then click [OK].

Example:

An unattended migration can be run as follows:

```
C:\SGEasy\Disk1\SETUP.EXE /u /f:D:\Migration.txt
```

The response file is called up with this command and the migration of SafeGuard Easy is automated.

The parameters for `SETUP.EXE` are displayed when you call up the program as follows:

```
SETUP.EXE /?
```

For further information concerning the parameters of a response file refer to chapter “Creating a response file” on page 107.

Completely unattended migration of SafeGuard Easy is currently only possible with a deactivated Pre-Boot Authentication.

8 Error Messages

The list of error messages is sorted according to error numbers. As each SafeGuard Easy error message is displayed with an error number, you can find the description required easily.

Overview

All the error messages have the following format: SGEnnnn: <text>

'SGE' is the SafeGuard Easy product-ID, and 'nnnn' a four-figure error number.

The error numbers are divided into the following groups:

0100-0199: Product specific errors

0200-0999: Hardware errors

1000-1029: API errors

1030-1059: File errors

1060-1099: Installation errors

1100-1169: Common errors

1170-1199: MESSAGE Control errors

1200-1209: Key errors

1220-1239: IPC errors

1240-1259: Drive errors

1260-1269: Service errors

1271-1299: REGISTRY errors

1300-1319: CRAREA errors

1400-1805: Other errors

Product Specific Errors

0100: Different version of SafeGuard Easy or Crypton already installed.
Wrong driver / kernel version

0101: Cannot read configuration file.
Error reading config file

0102: Invalid configuration file.
Wrong Configuration file

0103: Cannot write configuration file.
Error in writing Configuration file

0104: Currently installed driver is inconsistent.
Error for read/wrong driver or MBR data

0105: Driver already installed.

0106: This program cannot be run under &0.
Error multi task environment

0107: Cannot write backup file.
Error in writing backup file

0108: Cannot read backup file.
Error read or wrong backup file

0109: Invalid backup file.
Wrong backup file

0110: Cannot install a second boot partition on disk.

0111: Cannot install on top of OS/2 Boot Manager.
Boot partition is an OS/2 boot manager partition

0112: Earlier version of SafeGuard Easy or C:CRYPT already installed.
Earlier version was found

0113: Last install, deinstall, or update not complete.
Error setting install flag on MBR

0114: Not enough contiguous free disk space on boot partition.
No driver space allocation possible

0115: Cannot access the driver boot partition.
No access to driver partition

0116: No resource files found.
No resource file is bad news

0117: Cannot open resource file.
Error in opening resource file

0118: Bad or unreadable resource file.
Error in opening resource from resource file

0119: Missing algorithm module.
No three algorithm modules for driver are selected

0120: Missing kernel module.
No all five kernel modules are ready

0121: Missing PBA module.
No PBA module found

0122: Cannot create *AUTOUSER.
*AUTOUSER can't be added

Hardware Errors

0200: Cannot analyze hard disk structure.
Error no disk structure (not partitioned)

0201: Hard disk read failure.
Error read hard disk

0202: Hard disk write failure.
Error write hard disk

0203: Invalid partition table on disk 0.
Error invalid partition table (e.g. more than 1 partition is active; descriptor is not 0xaa55)

0204: Incompatible ROM BIOS.
Error incompatible BIOS

0205: Invalid boot sector.
Error verifying disk data with boot sector -> boot sector is bad

0206: Cannot lock volume.
Error can't lock hard disk

0300: Disk write protected.

0301: Unknown unit.

0302: Drive *[drive name]* not ready.

0303: Unknown command.

0304: Data CRC error.

0305: Bad request structure length.

0306: Seek error.

0307: Unknown media type.

0308: Sector not found.

0309: Printer out of paper.

0310: Write fault.

0311: Read fault.

0312: General failure.

0320: Out of memory.
Error by allocation of memory, no memory available

0321: Divide trap at program address &0.
Error divide by 0, routine is changed with original int 0 trap

0322: Runtime stack overflow.
Error by alternate stack overflow handler

0500: Encryption driver not installed.
No driver or no active driver found

0500: Incorrect encryption driver version.
Wrong driver, installed version is older than

0502: Invalid command line argument(s).
If we have invalid command line arguments

0503: No encryption key defined.
No key is defined

0999: Unknown error.
Error is unknown, place for all other errors

API Errors

1001: No subsystem active.
SGE subsystem is not active

1002: No key was specified.
Invalid status change made

1003: Invalid or missing encryption algorithm.
Invalid encryption algorithm

1004: Internal error in subsystem detected.
At least default error of api substystem

1005: Subsystem has reported an I/O error.
I/O to subsystem has failed

1006: The access to the kernel has failed.
By reads in all system settings stored in SGE kernel

1007: Already logged in to the API.
Multiple open calls are not allowed

1008: An invalid user was defined.
Invalid user or user table full (e.g. free entry for *AUTOUSER)

1009: Assign defined rights to user is not allowed.
The rights of the user doesn't correspond to the current user rights

1010: Defined user already exists.
The user is already exists, please choose another user name.

1011: The new password was already used for this user in the past.
The given new password found in history list

File Errors

1031: File *[filename]* cannot be opened.

1032: File *[filename]* cannot be closed.
Error by "Call WNetCloseEnum" to end the enumeration

1033: File *[filename]* cannot be created.
Can't create directory or file

1034: Error writing to file *[filename]*.
File could not be written, write to file list has failed

1035: Error reading from file *[filename]*.
file could not be read, or to get file content properties

1036: Error accessing the file *[filename]*.
No access on file to receive file time and date information

1037: File *[filename]* could not be found.
Defined file can't be found

1038: Invalid path or filename defined.
Defined destination path must be valid

1039: Not enough free space on disk.
Insufficient space for (temporary) files

1040: Hard disk partition is too heavily fragmented.

1041: Invalid file system detected.

1042: Unknown file system detected.

1043: File *[filename]* already exists.
This file exists and could not be overwritten

1044: Corrupted structure of the file system detected.

1045: Invalid entry in file system found.

1046: Request of partition information failed.
Request information about disk to compute size of a cluster failed.

1047: Unknown or invalid file system detected.
Installing is only accepted on FAT or NTFS formatted partitions.

1048: File *[filename]* could not be copied.
Error by copying source file or move kernel file to target with or without including expanding the file

1049: File *[filename]* could not be deleted.
Deletion of file or directory has failed

1052: CRC check for file *[filename]* has failed.
Check of CRC for file has failed

1053: File *[filename]* could not be renamed.
Rename of file (link) has failed

Installation Errors

1061: Invalid installation drive.
No usable partition found

1062: Installation of SafeGuard Easy has failed.
Installation has failed because files copied or file crc or any other is wrong.

1063: SafeGuard Easy system is already installed.
Because avoid a new install if a SGE system is already installed

1064: The CardMan API is not installed.
Uninstall of cm-api-files failed because files registered in the registry but these files are not found on the drive or CARDMANAPI or SCCMNT.EXE in \System32 directory is currently not running.

1065: The Config.sys file is write protected.
By install of the language system used by some 'SharedComponents'

1066: Entry in INI file or config file not found.
Mandatory entry not attended

1067: Installation of the screen saver failed.
For dynamic disks is only install of utilities allowed

1068: The kernel file could not be created.

1069: Config.sys file could not be modified.
Registering SmartCard Administration as 'SharedComponent' has failed

1070: File *[filename]* could not be copied.

1071: No target directory was defined.

1072: Wrong system administrator password was specified.
Wrong administration password given

1073: No system administrator password was defined.

1074: Installation of Master-Gina SGGINA failed.
Installation GINA SGGINA failed

1075: File DEINST.EXE could not be found.

1076: The uninstall procedure terminated abnormally. The following list shows.
Uninstall of some components has failed

1077: Deinstallation of Master-Gina SGGINA failed.
Uninstall GINA SGGINA failed

1078: Installation of Client-Gina GINA failed.
Install GINA client failed

1079: Deinstallation of Client-Gina GINA failed.
Uninstall GINA client failed

1080: Creating a system menu entry has failed.
Creating the defined system menu entry (and directory) has failed

1081: Removing a system menu entry has failed.
Deleting the file link, which will remove the menu item has failed

1082: Entry in INI file not found.
The section for defined packet exists not in INI file

1083: Installation of Cardman API has failed.

1084: Installation initialization file INSTALL.INI was not found.
Can't copy the necessary and compressed INI-file to the target directory

1085: A wrong or unknown installation process ID was reported.
Setup dialog sequence corresponding not to evaluated installation process ID

1086: A complete SafeGuard Easy system is still installed.
Install: a complete SGE system is still installed on this machine,
Uninstall: a complete SGE system is still installed on another partition of this machine

1087: Installation of a SafeGuard Easy system is not allowed.
Installation of a complete SGE system must be defined or there are more than MAX_HARDDISKS on the machine

1088: A required PBA resource file (.MOD) could not be found.
No PBA-module is found

1089: The installation of SafeGuard Easy could not be completed successfully.
The second phase of installation process has failed (CRAREA.DAT signaled there are s occurred)

1090: Wrong version of operating system found.
Operation system WINNT required

1091: Wrong version of operating system found.
Operation system WIN95/WIN98 required

1092: The uninstall procedure cannot be started because one or more SafeGuard Easy components are currently not running.

1093: This process cannot be executed because an encryption operation is currently running. Please wait until all encryption operations are completed and start this program again.
Encryption state of some drives is sets to running

1094: Uninstallation process is running. Administration is no longer allowed.
No change of settings is allowed if UNINSTALL process is already started

1095: Maximum number of hard disks exceeded.
For complete system installation the maximum number of hard disks may not be exceeded

1096: Some non-DOS partitions were found which would be encrypted next using this install type. Therefore we recommend to choose install type 'Partitioned'.
If install type is 'STANDARD' or 'BOOPTROTECTION' and a none DOS partition was detected no installation is allowed

Common Errors

1101: Self check failed.
Invalid call of functions because data not initialized or handle for current system data not defined

1102: Help system could not be initialized.

1103: Class could not be registered.
Internal error occurred, but the most entries occur because the wrong current system data

1104: The partition configuration information is inconsistent.
Can't find partition info or clearly partition data

1105: Invalid or wrong parameter defined.
Invalid parameter

1106: No or not enough parameters were defined.
Missing parameter in command line, If Update process is required or parameter /U must have been defined in SETUP command line

1107: Unknown parameter defined.

1108: Not enough memory available.
Not enough memory

1109: Module *[module name]* could not be loaded.
Dll-module can't be loaded

1110: Dialog could not be created.
Can't load dialog resources

1111: Dialog could not be initialized.
Error on initializations dialogs

1112: Thread could not be created.
The additional start of a thread is failed

1113: Window could not be created.
A dialog window or a message window can't be created

1114: You need administrator rights to install or uninstall.
Create a registry key will fail if user do not have necessary rights

1115: Desktop could not be opened.
By open the desktop on logon

1116: Desktop could not be switched.

1117: Log file *[filename]* could not be opened.

1118: You cannot run the Uninstall or Administration programs of SafeGuard Easy at the same time.
If Sgeadm.exe is currently running or if Uninst.exe is currently running

1119: Kernel file not found.

1120: Installation of control handler failed.

1121: Unknown environment variable defined.
Unknown evaluated size of complete value entry corresponding to environment variable

1122: Environment variable could not be set.
Append new entry to environment variable value string and write to the registry key failed

1123: Insufficient size of buffer.
Size of any value exceeds buffer size

1124: The dynamic link library '%5' couldn't be loaded.
Loads of any modules has failed

1125: The specified function '%5' couldn't be found.
Function entry could not be load (from dll)

1126: The semaphore '%5' couldn't be opened.

1127: The module '%5' couldn't be freed.

1128: An exception has occurred during execution of a SafeGuard Easy sub system function.
This occurred if "out of memory" detected

1129: A critical error has occurred during the execution of a SafeGuard Easy sub system function.

1130: Allocated memory could not be released.

1131: Function is currently not supported.
The specified function is not supported

1132: Access denied.
Access denied. No system data present or no necessary rights

1133: Start of program *[program name]* has failed.
Process can't be launched because of variously causes

1134: Function or resource is not available.
Algorithm ID is not supported, unknown client defined, no file packet or files defined, smart card not present

1135: Process was aborted by user.
Process was aborted by user

1136: Invalid or wrong entry defined.
Invalid entry in a string or in the INI - file

1137: Changes are not allowed in read mode.
No write access possible

1141: Kernel backup failed.

1144: The logon client 'SgeGina.dll' could not be found. This component provides vital functionality of SafeGuard Easy. Removing or disabling it can cause serious problems that may require you to reinstall SafeGuard Easy.

1145: The service 'SgeCtl.exe' could not be found. This component provides vital basic functionality of SafeGuard Easy. Removing or disabling it can cause serious problems that may require you to reinstall.

1150: Configuration file errors.

1151: Configuration file *[filename]* could not be found.
Defined config file didn't exist at all

1152: No configuration file defined.
Config file is not defined

1153: Invalid configuration file.
Error by get login info defined in configuration file to be executed.

1154: Invalid entry in configuration file found.
Invalid entry in the config file

1155: Configuration file *[file name]* could not be created.

1156: Error in line *[line name]* of the configuration file found.

1157: Execution of configuration file failed.
At executed of any changes of system settings within an active SGE system has failed

1158: The specified configuration file couldn't be found!

1159: An unknown command was found in the configuration file.

1160: An unknown configuration file type was detected.
Type of the config file is unknown (expected: install/uninstall or change)

1161: The type of the configuration file is not valid.
No valid configuration handle is available, wrong config file

1162: Handle for the configuration file could not be created.
Creating an config file handle failed

1163: Configuration file for uninstallation could not be created.
at creating configuration file of type CT_UNINST

1164: Configuration file for installation could not be created.
At creating an install configuration file that is used to install SafeGuard Easy

1165: Configuration file *[filename]* could not be found.
Can't found the defined config file

1166: The type of the configuration file is not valid.

MESSAGE Control Errors

1171: Message ID *[message ID]* not found.
Message string id not found

1172: No control text for control ID found.
Message text control number not found

1173: The Windows [NT/2000] event log couldn't be written.
By building an event report

1174: An invalid file or message link command was found.
Invalid link into the message file

1175: The format of the given message file '*[filename]*' is invalid.
1180: Password errors
1181: No system administrator password defined.
1182: Unknown password.
1183: No password defined.
No password is given

1184: Defined password is too short.
Yield of the checking user password is "too short"

1185: Defined password is too long.
Yield of the checking user password is "too long"

1186: Defined passwords do not match.
The comparison of the two passwords are mismatched

1187: The password contains too many identical characters,
Yield of the checking user password is "trivial"

1188: The same password exists for another user.
yield of the checking user password is "already used"

Key Errors

1201: A hard disk key is not yet defined.
No key for hard drives was defined

1202: A floppy disk key is not yet defined.
No key for floppy disks was defined

1203: A removable disk drive key is not yet defined.
No key for removable disks was defined

1204: Defined key is too long.

1205: Defined key is too short.

1206: The defined keys do not match.
Compare content of the two entry fields yields no matching

1207: No key was defined.

1208: The Boot Protection mode requires a key for hard disk drive encryption
The entry for Key Field missing, because the Boot-Protection mode requires a HD key.

1209: The Standard mode requires a key for hard disk drive encryption
The entry for Key Field missing, because the standard protection mode requires a HD key

1210: The key is trivial. Do you want to enter a different one?
Yield of the checking key is "trivial"

IPC Errors

1221: IPC server could not be started.
The function failed by creating a pipe, by connecting to it or by initializing it ready for connecting

1222: IPC client could not be started.
The function failed by opening a pipe, by reading some specific data or by creating shared memory object containing all relevant data

1223: IPC connection could not established.
The IPC connection can't be found

1224: IPC message could not be fetched.
Get message from IPC connection failed

1225: IPC message could not be posted.

1226: IPC function IPC_SGE_PROCESS_DEF_MSG
Yield of the evaluated message is failed

1227: IPC server could not be closed.
Error by closing IPC server

1228: IPC client could not be closed.
Error by closing IPC client

1229: IPC thread could not be started.

1230: Waiting for IPC message failed.
Error by waiting to receive messages is an timeout reached

1231: IPC communication object not found.

Drive errors

1241: Unknown or invalid drive defined.
An invalid or unknown drive was defined

1242: No more drives found.

1243: Drive I/O operation has failed.
No access to the called device

1244: Reading from a drive has failed.
Error by reading in all the required data from the hard disk

1245: Writing to a drive has failed.
Error by writing data into the hard disk

1246: Start access to a drive has failed.
Access to the drive could not be opened

1247: Drive is not ready.
Device not ready, if this an removable drive then is no media within the drive

1248: Locking a disk drive has failed.

1249: Unlocking a disk drive has failed.

1250: The system partition must be a primary partition.
Failed if option KEEP MBR is defined and the system partition isn't the first partition

1251: Dismount of volume has failed.
This function can only be performed successfully if currently there are no open files on this volume

1252: The first physical disk is not a hard disk.
Function can't reading in the 1st sector of the 1st hard disk, disk invalid

1253: All entries in partition table of MBR sector on the first hard disk are already used. Option 'Keep Original MBR' requires a free, unused partition table entry!
There must be at least one free entry in the partition table to add a new one (entry for our 'pseudo' partition)

Service Errors

1261: Info about a memory object for a system service.
Mapping for service info already exists

1262: Error detected in system service dispatcher.
Service dispatcher can't be run (e.g. invalid entry within the dispatch table)

1263: System service could not be started.
Service cannot start

1264: System service status could not be changed.
Set service status fails because he specified handle is invalid or the specified service status structure is invalid

1265: Handler for system service could not be registered.
This message means that the service name not exists or the service name is invalid

1266: The service initialization function reported an error.

1267: The service information block couldn't be found.

Registry Errors

1271: Entry in the registry could not be opened.
Registry key or value not found

1272: Entry in the registry could not be read.
Registry key entries could not be read

1273: Entry in the registry could not be written.
Registry key entries couldn't be written

1274: Entry in the registry could not be created.
Creating registry key failed

1275: Entry in the registry could not be removed.
Deleting registry entry failed

1276: Entry for system service in the registry.
Open specified service for delete operation fails.

1277: Entry for a system service in the registry.
The creating of an entry for a standalone driver failed

1278: Entry for a system service in the registry.
Delete service operation fails

1279: Entry for a system service in the registry.
Installing actual driver fails because this service already exists

1280: Session Control Manager could not be opened.
Open system control manager to create a service fails

1281: Entry in the registry for a session.

1282: Invalid entry in the registry detected.
The specified string entry was not found in string list

1290: Driver data base file errors.

1291: No more encryption drivers found.
If defined driver or driver list does not exist

1292: Driver database file not found.
Name of file with driver list and number of driver entries can't be found

1293: Error occurred while reading the driver database file.
Read in all entries in driver database file to our driver list fails

1294: Driver database file is empty.
The driver database file is empty

1295: Illegal or invalid entry in driver database file.
Wrong number of driver entries

CRAREA Errors

1301: Installation drive cannot be accessed.
Open access to installation partition or 1st hard disk fails

1302: Request of partition information failed.
Can't get information about installation partition

1303: Access to boot partition failed.
Can't open volume to mark clusters

1304: Invalid process option defined.
Either create area or remove area allowed

1305: Unknown or invalid file system defined.
Only file system FAT, FAT or NTFS are allowed

1306: Difference between type of current file system
Specified file system differences to existing file system

1307: Difference between current and defined cluster size.
Specified cluster size be differences with actually cluster size

1308: Invalid start cluster for kernel area defined.
Specified start cluster is invalid, because this entry is negative

1309: Invalid start sector for kernel area defined.
Specified start sector is invalid, because this entry is negative

1310: Invalid partition type defined.
No valid partition found

1311: No free clusters for kernel found.
No free clusters are found

1312: Clusters could not be marked as 'Used'.
Mark of clusters to be used fails

1313: Clusters could not be marked as 'Good'.
Cluster mark good fails (reserving clusters for installation of SGE)

1314: Clusters could not be marked as 'Unused'.
Now unused clusters marked as good failed

1315: Clusters could not be marked as 'Bad'.
Free clusters can't be marked as bad (reserving clusters for installation of SGE)

1316: Cluster information is corrupt.
Can't find clusters markings bad in list

1317: Area marked as 'Bad' could not be found.
Can't find reserved clusters for installation to be marked bad

1319: MBR sector on 1st hard disk could not be replaced.
Failed write process of the current read original MBR sector must be done via I/O control call to SGE FLT

1331: Invalid size of kernel area defined.
Error by checking if created area for kernel is large enough

Other Errors

1401: The requested object communication area information data already exists.

1402: The object communication area already exists.
Object communication area already exists, normally this function creates the root entry of the information list

1403: The requested object communication area information data already exists.

1404: The object communication area couldn't be found.
An OCA object can't be found (no handle available)

1405: The requested object communication area information data doesn't exist.
An OCA object can't be found (no data available)

1405: Additional object information data found.

1601: The logon failed. Please retry.
The check if the authentication was performed successfully was failed

1602: The SafeGuard Easy subsystem does not allow more than 5 logon attempts. You must restart your computer to start this application again.
Maximal logon counter may not be exceeded to logging on

1603: The start of the SafeGuard Easy logon component has failed.
Logon module (logon counter) can't be either opened or queried logon with challenge code incorrect

1605: The logon to SafeGuard Easy was successful, but you don't have sufficient rights to uninstall the product.
Rights to logged on are not sufficient

1801: The user *[user name]* cannot be created because the maximum count of users has been reached.
MAX_USERS entries are not allowed because we need one free entry to create intern (SGEAPI.DLL) the AUTOUSER user

1802: It is not possible to create, delete or modify the '*AUTOUSER'.
The user tries to create the *AUTOUSER. This is not allowed

1803: The user *[user name]* already exists. Please specify another user identification name.
If there is already a user with that name in the list

1804: The maximum count of users has been exceeded.
Maximal count of users reached

1805: It is not allowed to create or delete the 'SYSTEM' user profile. It is only allowed to modify this profile.
It is only allowed to modify the SuperUser profile

9 FAQ´s

Does SafeGuard Easy cause any loss of performance?

No, SafeGuard Easy does not cause any noticeable performance loss.

How many SafeGuard Easy users can be implemented?

There is a maximum number of 15 users.

Is it possible to assign different rights to the various users?

Yes, every user has his/her own user profile with certain rights.

Is it possible to start a workstation from a floppy disk?

If Pre-Boot Authentication and Boot protection are switched on, booting is not possible for users without the corresponding rights.

Which operating systems are supported by SafeGuard Easy?

Windows 95, Windows 98, Windows NT, Windows 2000 and Windows XP.

Which file systems are supported?

SafeGuard Easy supports FAT-12, FAT-16, FAT-32, HPFS, NTFS and NTFS5.

What can be encrypted with SafeGuard Easy?

Hard disk drive(s). floppy drive(s) and removable media drive(s).

Is a workstation lock (screensaver) available for Windows 95 and Windows 98?

Yes. the screensaver can only be unlocked by entering the SafeGuard Easy password.

Does SafeGuard Easy support a single logon?

Yes.with the secure auto logon (SAL). A user enters the operating system data once. At next logon only the SafeGuard Easy user data has to be entered. Logon to the operating system is done automatically.

Is is it possible just to encrypt partitions of a hard disk?

Yes, not only the whole hard disk, but different partitions or just the system areas can be encrypted.

Is is it possible to encrypt external devices?

Besides encryption of hard disk8s) SafeGuard Easy encrypts floppies and removable medias like IOMEGA ZIP and JAZ Medias.

What algorithms and key lengths uses SafeGuard Easy?

AES (128 or 256 Bit), Rijndael (256 Bit), IDEA (128 Bit), BLOWFISH-8/-16 (256 Bit), STEALTH-40 (48 to 64 Bit), XOR (64 Bit).

Is it possible to use defragmenters or virus scanners on a hard disk drive after SafeGuard Easy has been installed?

Yes, defragmenters and virus scanners will work.

Does SafeGuard Easy support special characters in passwords?

Yes.

Is it possible to set a expiration date for a SafeGuard Easy password?

Yes. After a defined period of time a password expires and a new one has to be defined.

What happens if a user has forgotten his password?

By using remote help a user can be assigned a password.

What happens in hibernation mode?

Encryption modes “Boot protection” or “Partitioned”:

If the ***systemroot partition is not encrypted*** and the system hibernates it will return to the point from where it hibernated when it resumes.

Encryption mode “Standard” with all partitions encrypted or with the install type “Partitioned”:

If the ***systemroot partition is encrypted*** and the system hibernates it will ***not*** return to the point from where it hibernated when it resumes. This means, that all changes in open applications will be lost, when they had not been saved before hibernation.

Does SafeGuard Easy cause any loss of performance?

No, SafeGuard Easy does not cause any noticeable performance loss.

10 Glossary

Authentication	Confirms a predefined identity.
Boot Protection	Prevents the system from being booted from a medium other than the hard drive. While it is possible to boot the system with a system disk, access to the hard drive is denied.
Challenge/Response	Transfer process for the mutual authentication of users. The communications partner replies to the challenge with a response code.
Data Encryption	Conversion of information into encrypted form using a defined key. The data can only be made legible again by using the right key. There are two different methods: symmetrical and asymmetrical encryption.
Function Separation	SafeGuard Easy recognizes two types of user: the System Administrator and the user.
Master Boot Record	The Master Boot Record is located in the first sector of the hard disk. All of the important information regarding booting the system is stored here.
Online Encryption	Work can continue without interruption while encryption is in progress.
Encryption Algorithm	Method of encrypting data. Encryption algorithms differ in the level of security they provide and in the speed of the throughput. Various encryption algorithms are available for encrypting data under SafeGuard Easy.

Confidentiality of Data	Encryption provides protection against unauthorized access to data.

Index

Index

Index

P

R

S

T

U

Index