Safe Guard Easy

Version 1.12

for Windows 95

Pre-Release

Utimaco Safeware AG
Dornbachstr. 30
61440 Oberursel
Telephone: ++49 / 06171 / 917-126
Telefax: ++49 / 06171 / 917-111

No guarantee is made for the correctness of the contents of the manual.

We would be grateful to have indications of any errors. Please inform us if you discover any errors or anything that is not clear.

Utimaco Safeware AG, D-61440 Oberursel, Germany

February 1997

TABLE OF CONTENTS

1 Introduction

2 Preparing for Installation

3 Installation

4 Change Settings and Deinstallation

1. Introduction

Why Safe Guard Easy ?

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

The necessity of safeguarding such data against access from persons who are not authorised is anchored in the Data Protection Act.

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.

Safe Guard Easy for Windows 95 it the ideal way to safeguard oneself against such risks without investing too much time in the implementation of security measures.

With Safe Guard Easy you can achieve the following goals:

- ❑ **Access protection with password**
  Only the system administrator and up to 15 further users have access to the PC.

- ❑ **Data security with encryption**
  Online encryption of your data safeguards you against criminal activity (tapping, sabotage, theft). Even if your PC is stolen, the data cannot be read and therefore cannot be misused.

- ❑ **MBR-Virus protection**
  Here you have a protective mechanism against viruses which infect the partition sector (MBR = **M**aster **B**oot **R**ecord).

If these security precautions are not sufficient, please contact Utimaco Safeware AG for information on integrative software covering all levels of security.

Safe Guard Easy functions

Safe Guard Easy is simple to install and does not require any administration after installation. At the same time Safe Guard Easy fulfills the requirements of the Data Protection Act.

On-line encryption is central to Safe Guard Easy for Windows 95. It is for this reason that this program is suitable chiefly for standalone systems and notebooks.

The security functions of Safe Guard Easy are briefly described below:

Multi-user system

Safe Guard Easy allows up to 16 users access to the system - the system administrator and 15 further users. The system administrator and the users identify and authenticate themselves with their name and password to have full system authorization.

The system administrator has unrestricted rights. He can grant users administration rights. Different rights profile can be assigned to each user.

These are:

- Deinstall (Safe Guard Easy)
- Toggle floppy encryption
- Toggle block device encryption
- Create configuration file
- Change MBR protection
- Change password rules
- Change PBA settings and MBR options
- Change encryption

Access control with PBA

Only an authorised user receive access to the PC. He log-on with his name and a valid password before the operating system is booted (**P**re **B**oot **A**uthentication). The user can change their password at any time.

On-line encryption

Hard disk, floppy and device encryption can be implemented with different keys using different algorithms (XOR, IDEA, BLOWFISH, STEALTH or DES).

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 anew from a code saved on the hard disk and the user password.

The system areas, individual partitions or a maximum of two hard disks can be encrypted on-line.

Blanking the screen

The user can activate the screen blanking either manually by clicking the mouse. It is also possible to set a time interval for automatic screen blanking. If no key is pressed and the mouse is not moved within the number of minutes defined, the screen is automatically blanked. In both cases the password must be entered to activate the screen.

MBR virus protection

The virus protection checks the MBR for changes each time the system is started. If a change is detected, this can indicate a virus or manipulation. You can specify how Safe Guard Easy should react.

Use of the manual

We recommend you to read this manual carefully. This applies to the installation, deinstallation and for making changes to the settings of Safe Guard Easy for Windows 95. The manual is divided into the following chapters:

Chapter 1 Chapter 1 briefly describes the benefits and functions of Safe Guard Easy for Windows 95 and contains general operating instructions on the program.

Chapter 2 The Safe Guard Easy Setup program is described in Chapter 2. The chapter also contains important information which you should follow when installing Safe Guard Easy.

Chapter 3 How to install Safe Guard Easy together with the creation and evaluation of a configuration file is described in Chapter 3.

Chapter 4 Chapter 4 describes changing settings and deinstallation.

Chapter 5 Chapter 5 deals with the *Extras* menu.

Appendix A In Appendix A the error messages are described.

Support, Hotline and Index At the end of the manual you will find information on our Support, Hotline etc. as well as an index.

General operating hints

Setup and administration of Safe Guard Easy menu have the look and feel of Windows 95, both in appearance and in operation. The keyboard and the mouse can be used as input devices.

With the on-line Help system you always have access on the information you require.

If you want to use the use the on-line help, use the *Help* button in the menus. To do this press either the [F1] key or activate the *Help* with a single mouse click. A help text on the current window appears. With [Shift] + [F1] you obtain individual help on the current cursor position.

2. Preparing for installation

Create a backup

Before you start installing Safe Guard Easy, create a backup copy of the original disk. You should then only work with the backup copy.

Note on the terms of the licence

☞ You may install Safe Guard Easy on only one PC. If you use the backup copy to install Safe Guard Easy on several PCs, you violate the licence conditions and render yourself subject to prosecution.

If you want to protect several PCs, a licence must be acquired for each PC.

Note on SGE_READ.TXT

Safe Guard Easy is subject to on-going development. For this reason your version can already contain innovations which were not included when this manual went to print.

As these innovations are described on the disk in the SGE_READ.TXT, you should read these carefully before the installation. You can view the contents of the file with any editor or have them printed.

Recommendation : complete backup

☞ It cannot be ignored that data is lost as a result of an unintentional interruption during encryption (e.g. as a result of a power failure). For this reason we recommend making a complete backup of the hard disk before the Safe Guard Easy installation.

Before installation

If you observe the following tips, you can exclude possible disruption when installing Safe Guard Easy:

- ➩ The PC must be IBM-compatible. Microsoft Windows 95 is required as operating system.
- ➩ For Safe Guard Easy you require between 5 and 20 KB available base memory.
- ➩ If another boot manager is active, you must deactivate it (e.g. OS/2 Boot Manager). The Windows 95 Boot menu can be used.
- ➩ Check for viruses.
- ➩ If software is active which prevents absolute write access to the hard disk, you must deactivate it during installation or deinstallation (e.g. Virus protection). Afterwards it can be reactivated.

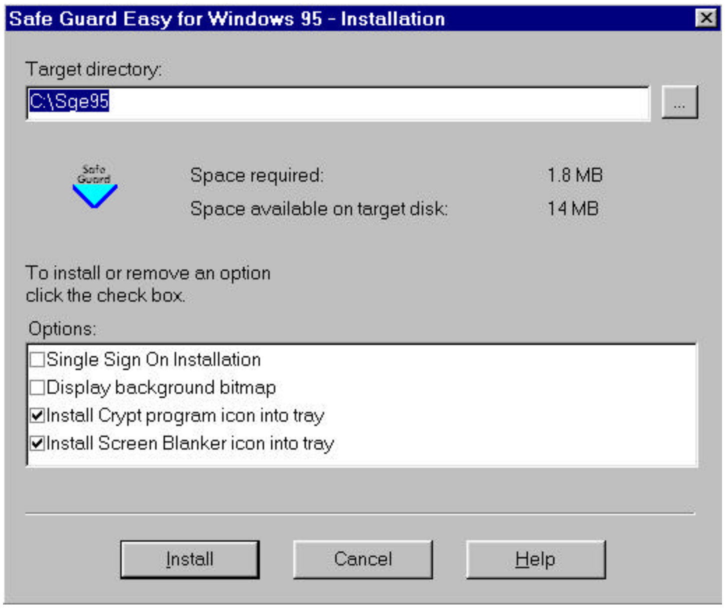
Setup of Safe Guard Easy

Insert the backup of the original Safe Guard Easy for Windows 95 disk in the floppy drive.

Click on the *Start* button and via the *Run* command, execute the Safe Guard Easy for Windows 95 installation program SETUP.EXE. The parameters for SETUP.EXE are displayed when you call up the program as follows:

```
SETUP /?
```

Once it has been called up with the selected parameters, the following dialog box appears:



Safe Guard Easy for Windows 95 - Installation

Target directory: C:\Sge95

Space required: 1.8 MB

Space available on target disk: 14 MB

To install or remove an option click the check box.

Options:

- □ Single Sign On Installation
- □ Display background bitmap
- ☑ Install Crypt program icon into tray
- ☑ Install Screen Blanker icon into tray

Directory

The *Target Directory* field shows the path where Safe Guard Easy for Windows 95 is to be installed. You can change the installation directory by entering another path.

Single Sign On Installation

Using the Single Sign On function, Safe Guard Easy implements the user logon for Windows 95 automatically. The user need only log on to Windows 95 after the first logon in Safe Guard Easy. The password for Windows 95 is then saved in an encrypted file. For every further logon in Safe Guard Easy the logon to Windows 95 is automated.

For Single Sign On it is necessary that the user names in Safe Guard Easy and Windows 95 are identical.

☞ Note that with the two-user system both a user "USER" and a user "SYSTEM" must be defined in Windows 95.

If you tag the *Single Sign On Installation* control box, Safe Guard Easy implements the user logon for Windows 95 automatically.

☞ Do not tag this check box if you want to disable the automatic user logon.

REGSET.EXE can be used to activate SSO in the Registry and REGDEL.EXE to deactivate it. You can also change the SSO setting in the dialog box for changing the password.

Display background bitmap

If you tag this check box, a bitmap will be shown as the background for the SGEADM.EXE program. If you want to use a different bitmap file as the background instead of the default bitmap file, you must enter your selection in the following section of the Registry:

```
HKEY_LOCAL_MACHINE
    SOFTWARE
        UTIMACO
            SGEWIN95
                ADMIN:BACKGROUND.BMP
```

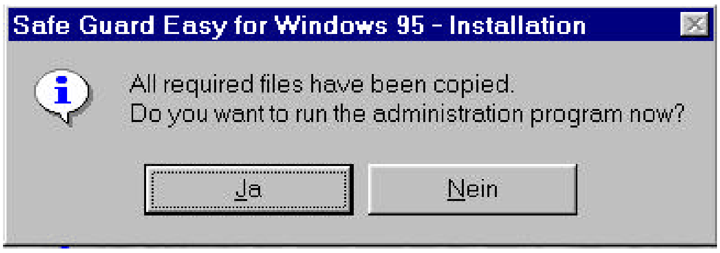
If you do not tag the check box, no background bitmap will appear with the SGEADM.EXE program.

To run the installation, click on the *Install* button.

Further information on the installation process is described in Chapter 3.

3. Installation

Once the Setup program has copied all the necessary files for Safe Guard Easy on your hard disk, the following dialog box appears:



Safe Guard Easy for Windows 95 - Installation

All required files have been copied.
Do you want to run the administration program now?

Enter [Yes] to run the Safe Guard Easy Administration program.

Safe Guard Easy is then installed using this program.

☞ If you answer the question with [No], the Setup program is terminated. You can run the Administration program later in the Windows 95 Start menu, using the section *Programs* submenu (folder) *Safe Guard Easy* or simply click on the icons generated during installation.

There is a difference between the system administrator installation and the automatic installation by the user with a configuration file.

The system administrator can save all the Safe Guard Easy definitions in a configuration file. Using the configuration file users can install Safe Guard Easy independently without knowing the key or the system administrator password. The configuration file contains the users definitions, their rights profiles and the settings for drive encryption.

In the Administration program you must now specify if you want to install Safe Guard Easy on your PC or only want to generate a configuration file.

Install

❶ To install Safe Guard Easy on your PC, open the *Install* menu in the Safe Guard Easy menu bar and run the command *Install*.

Create configuration file

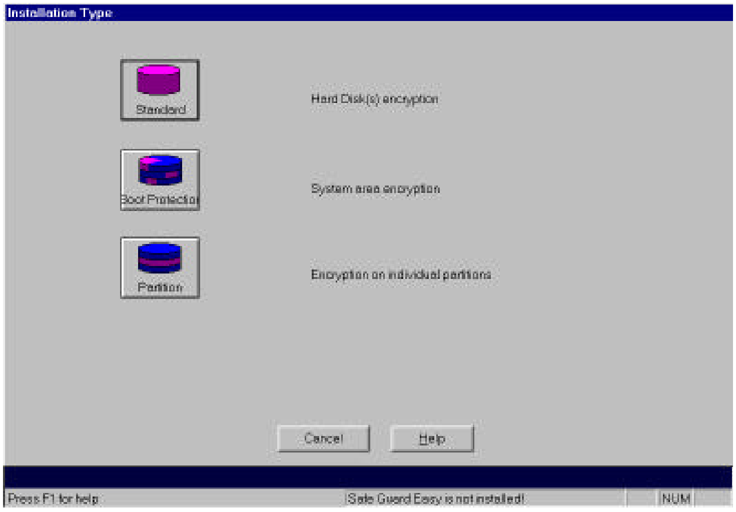
❷ To generate a configuration file open the *File* menu in the Safe Guard Easy menu bar and run the *Create configuration* command.

☞ Even after you have installed Safe Guard Easy on your PC you can still create a configuration file.

The following section describes both the installation of Safe Guard Easy and how to create a configuration file. The two processes are almost identical. However, when creating a configuration file Safe Guard Easy is **not** installed on your PC.

Installation type

Irrespective of the command you select, the **Installation type** dialog field appears:



Installation type

You can choose between three different installation types. The installation procedure varies depending on the choice made.

Select the installation type you require by clicking on one of the four large buttons:

- Standard
- Boot Protection
- Partition

As the procedure for all installation types is very similar, it is only the *Standard* installation type which is described in detail below. This forms the basis for all other installation types.

☞ The descriptions of the other installation types only indicate where these differ significantly from the *Standard* type.

Standard installation type

Hard disks When you select the installation type *Standard,* the hard disks of your PC will be fully encrypted.

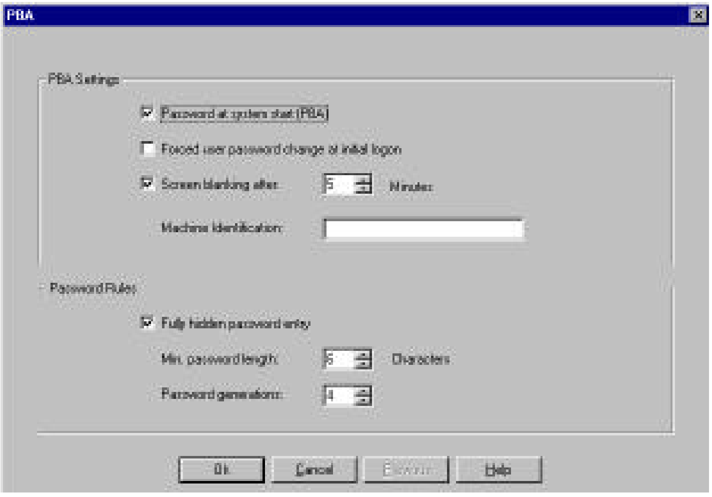
The program automatically recognizes whether your PC has one or several hard disks.

☞ If there are more than two hard disks, the installation is terminated with an appropriate error message.

When hard disk encryption is enabled, the hard disks of the PC are encrypted using the same key.

PBA

When you choose installation type *Standard*, the following dialog box appears:



PBA

PBA Settings

☑ Password at system start (PBA)

□ Forced user password change at initial logon

☑ Screen blanking after: 5 Minutes

Machine identification:

Password Rules

☑ Fully hidden password entry

Min. password length: 5 Characters

Password generations: 4

PBA The PBA settings dialog box enables you to specify the following options:

Password at system start (PBA)

❶ **PBA deactivated:**

If you deactivate the password prompt at the system start, you switch off the PBA function (**P**re **B**oot **A**uthentication) and you are not logged on.

With hard disk and floppy disk encryption, the keys are saved on the hard disk in encrypted form.

☞ When PBA is deactivated, the remaining PBA settings (e.g. screen blanking) are not relevant.

The emergency start

If the PBA function is not switched on when hard disk encryption is active and a system error occurs, you will not be able to boot the system directly from the floppy disk drive.

However, when you boot, a floppy icon appears on the screen for around 5 seconds. If you press the function key [F2] during this time, the password prompt will appear.

Insert a system disk in the floppy disk drive. If floppy disk encryption is not set up, an unencrypted systems disk will do. If floppy disk encryption is set up in Safe Guard Easy, you will need an encrypted systems disk to boot the system. The algorithm and the key must correspond with the floppy disk encryption settings.

Now enter your password and confirm this entry. The PC continues to boot from the floppy disk. The encryption driver is loaded. You are granted access to the system and can carry out any repairs which may have become necessary.

❷ **PBA activated:**

If you enable the PBA function, you increase the level of protection as the keys are not saved. Instead, the passwords are linked to keys and the results of the link are saved on the hard disk.

Reset logon tries

For security reasons, every failed logon results in an exponential increase in the logon time. A logon by the system administrator automatically resets the number of logon tries.

If the system administrator is not available, the time routine can be reset by booting SGEASY from Drive A: and by carrying out the user logon correctly. It can also be reset by means of remote maintenance (see page 3-27).

Select *Reset logon tries* as executable action and pass on the response code which is generated to the user. Once the user has correctly entered this response code, the logon time is reset to normal.

Forced user password change at initial logon

The system administrator defines the users and their passwords in Safe Guard Easy. If you tag this check box, the user will be prompted to change his or her password after the initial logon.

Screen blanking

With screen blanking you can blank the screen and block input via the keyboard or mouse. Programs continue to work unaffected when the screen is blanked. Screen blanking only functions when the PBA function is switched on. When screen blanking is installed, the file SGEBLK32.EXE is automatically copied into the Windows 95 System subdirectory. The settings are controlled by the SGE.VXD file.

Automatic screen blanking

Automatic screen blanking becomes active if no keys have been pressed and the mouse has not been moved for the specified number of minutes.

Screen blanking after ‘n’ minutes

Tag the check box Screen blanking after ‘n’ minutes if you want to activate the automatic screen blanking. This activates the minutes field on the right. Enter the value you require. You can set any value between 1 and 120 minutes.

Manual screen blanking

If you want to take a break from your work, manual screen blanking can be activated by clicking on the screen blanking icon.

Deactivate screen blanking

Screen blanking can be deactivated by entering the correct password. The password must be confirmed with the Enter key. This takes the reader back to the point where the screen blanking was activated. DOS full screens are minimized by Windows 95 and placed in the task bar. They must then be switched back to full screen.

Machine identification

Enter a unique identifier (e.g. PC no.) in the *Machine identification* field. The machine identification is displayed later on PBA logon. This enables the PC to be uniquely identified.

Fully hidden password entry

fully hidden password entry

If you tag the option *Fully hidden password entry*, the password will not appear on the screen when it is entered during logon. The advantage of this is that the length of the password is not revealed. If you deactivate this option, a place holder (*) will appear for each character of the password entry.

Minimum password length

Any number from 1 to 16 can be entered as the value for the minimum password length. The minimum password length specifies the minimum number of characters a new password must have when it is changed by the user.

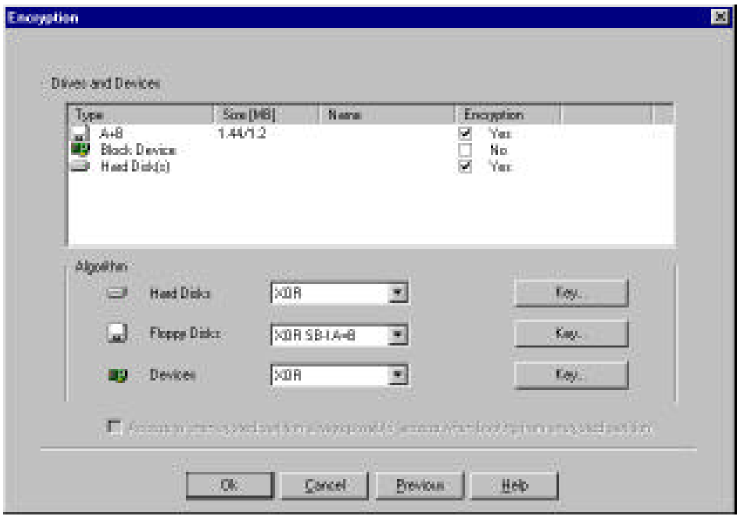
Password generations

The setting *Password generations* is used to specify how many previous passwords are locked when a password is changed. Any number between 1 and 16 can be entered as the value here.

Confirm your settings for the **PBA** dialog field by clicking on the [OK] button.

Encryption

The following dialog field then appears:



Encryption

Drives and Devices

Type	Size [MB]	Name	Encryption
A+B	1.44/1.2		☑ Yes
Block Device			□ No
Hard Disk(s)			☑ Yes

Algorithm

Hard Disks: XOR

Floppy Disks: XOR SB-I A+B

Devices: XOR

Encryption Encryption in Safe Guard Easy is on-line encryption where a choice of various algorithms is available for optimum security and performance.

When the PBA function is not active, the keys are saved on the hard disk in encrypted form. When the PBA function is enabled, the keys are only generated once the password has been entered.

Keys can be selected as required and consist of between 1 and 32 characters. As for the characters, you can enter letters, numbers and other special characters from the letter area of the keybord.The numeric key pad can not be used. Note that a differentiation is made between upper case and lower case letters. It is possible to generate a random key.

Encrypting drives and devices

The *Drives* and *Devices* list field lists all types of data media which you can encrypt. The *Type* column shows the drive or device type, while the *Size* column to the right of this shows the drive capacity.

The *Name* columns shows the label of the partition. However, the label is only displayed if you selected the Partition installation type.

The right-hand column, *Encryption*, shown whether encryption is enabled (yes) or disabled (no) for the selected data medium. The setting can be changed using the check box. Tag all data media you want to encrypt. The relevant current setting will appear to the right of the check box.

Encryption of hard disks

A maximum of two physical hard disks per PC can be encrypted, one hard disk key being used for both.

☞ Encrypting individual partitions of a hard disk is only possible with installation type *Partition* (see page 3-37).

Device encryption

In the default setting, device encryption is not activated as it is only required for encrypting special hardware. This includes external devices (e.g. IOMEGA’s Bernoulli Box or ZIP drives) which read and write by sector and are integrated into the CONFIG.SYS by means of a DEVICE driver.

```
HKEY_LOCAL_MACHINE
    SOFTWARE
        UTIMACO
            SGEWIN95
```

Under Windows 95 device encryption is managed using SGE.VXD. To activate device encryption, the key ‘DeviceEncryption’ must be generated in the following section of the Registry:

ZIP drives

Under this key enter the string ‘DriveLetters’ and assign it the drive letter you assigned to the ZIP drive under Windows 95. It is essential to keep to the syntax for writing ‘DeviceEncryption’ and DriveLetters’.

PCMCIA drives

PCMCIA drives can be encrypted in the same way as ZIP drives.

☞ Note that under Windows 95 the command SGE-DEVC can only be run with the parameters +/- or ON/OFF if there is no ZIP medium in the ZIP drive.

Floppy disk encryption

It is not possible to read unencrypted floppies on a PC with floppy disk encryption enabled. If the floppy disk encryption is enabled, you must reformat the floppy you want to use. The same key applies to all floppy disk drives.

☞ **When floppy disk encryption is active, it is important that you create an encrypted systems disk.**

Encrypted floppies cannot be read in PCs without floppy disk encryption or in PCs with a different floppy key or algorithm.

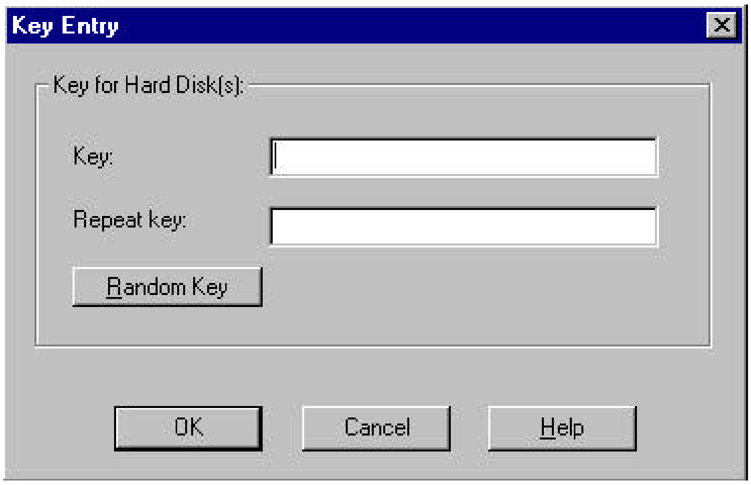
Floppy disk encryption can be toggled

If floppy disk encryption is activated, an option can be set in the user rights enabling you to switch it on and off temporarily.

☞ Note that programs such as MSBackup or Win-Backup, which run directly via the controller, can only save data in unencrypted form even when floppy disk encryption is enabled.

The [key] buttons allow you to define the key for encryption.

The **Key Entry** dialog field appears:



Key entry

The **Key Entry** dialog fields for floppies, hard disks and devices look similar. You must enter a key for each drive type you want to encrypt. Enter the key and repeat your entry.

Only after you have clicked on the OK button to confirm your entry is a check made whether your key entries were identical or trivial. If the key entries are not identical, the entries must be repeated. Trivial keys are strings consisting of one or few characters (e.g. 22222222, aaddaaddaadd, 1h1h1h1h1h1h1h) or which correspond to a sequence of keys on the keyboard (e.g. asdfghjk, lkjhgfds). If you enter a trivial key, you will be advised of the security risk and prompted to define the key again.

The [Random key] button allows you to generate the key via Safe Guard Easy.

☞ Make sure that the key is kept secret.

The encryption algorithms

The algorithms available to you are XOR, STEALTH, IDEA, DES and BLOWFISH. The speed and level of security provided by these algorithms varies considerably.

☞ Please note that due to export or license restrictions some of the algorithms listed are not contained in all product versions. These are indicated with an asterisk.

A brief description of the algorithms should help you to select the right one.

XOR SB-I A=B:

This is a XOR algorithm which is compatible with the Safe Board I floppy encoder (from version 1.43). It is very fast but not particularly secure.

XOR SB-I:

This is a XOR algorithm which is compatible with the Safe Board I floppy encoder (before version 1.43). It is very fast but not particularly secure.

DES:

The DES algorithm with 16 iterations is relatively slow but very secure. Its key length is 56 bit.

DES SB-II:

The DES SB-II algorithm is compatible with the Safe Board II and III floppy disk encryption and to the floppy disk encryption of Safe Board X II and II with old key management.

IDEA:

The IDEA algorithm is new. It is not very fast but offers a very high degree of security (*Patent rights of Ascom Tech Ltd. given in EP, JP, US. IDEA(tm) is a trademark of Ascom Tech Ltd*.).

STEALTH-40:

This algorithm is about as fast as XOR but significantly more secure (*STEALTH Encryption Copyright (c) 1994 Intelligence Quotient International Limited. All rights reserved. Patents pending. STEALTH encryption is a trademark of Intelligence Quotient International Limited*).

BLOWFISH-16:

The Blowfish-16 algorithm is relatively new and fast. At present there are no precise details available about how secure it is. However, it is considerably more secure than the XOR algorithm or STEALTH-40.

BLOWFISH-8:

The Blowfish algorithm reduced to 8 iterations. Here too there are not yet any precise details available about the level of security offered. It is, however, considerably more secure than the XOR algorithm.

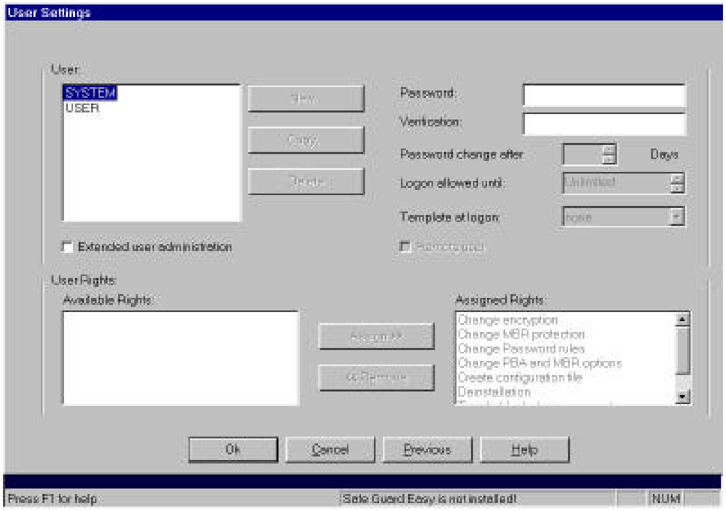
Choose the algorithm you prefer for the encryption.

☞ The function “Access to plain text partitions not always possible (data exchange when booting from encrypted partition)” can only be set in installation type Twin-Boot.

Confirm your settings for the **Encryption** dialog field by clicking on the [OK] button.

Defining the users

The users are defined using the User settings dialog field.



User Settings

User:
- SYSTEM
- USER

Password:

Verification:

Password change after: Days

Logon allowed until: Unlimited

Template at logon: none

□ Extended user administration

□ Remote user

User Rights:

Available Rights:

Assigned Rights:
- Change encryption
- Change MBR protection
- Change Password rules
- Change PBA and MBR options
- Create configuration file
- Deinstallation

Press F1 for help | Safe Guard Easy is not installed! | NUM

Extended user administration

Two- or multi-user system

Safe Guard Easy distinguishes between a two-user system and a multi-user system. If you do not tag the *Extended user administration* check box, you configure Safe Guard Easy as a two-user system, where only the password is required for the logon. If you do tag this box, you can define up to 15 additional users in addition to the system administrator.

☞ In the multi-user system the user name also has to be entered when logging on.

☞ If you specify the two-user system setting, the options "*Template at logon* " and "*Logon allowed until*" are inactive and are not available.

The system administrator

Irrespective of the setting for *Extended user administration*, the user SYSTEM always exists. Its name cannot be changed. As system administrator, SYSTEM has all rights in the system.

SYSTEM defines all other users and assigns or withdraws their rights so that certain administrative activities can be carried out or locked.

The system administrator can transfer individual rights to other users. A detailed description of the individual rights can be found in the "User rights" section of this chapter.

User settings

Existing users are listed alphabetically in the *Users* list field. If you want to change the settings for a user, select the user from the list or click on the user's name.

If you have selected the option *Extended user administration*, you can define a different rights profile for each user.

Defining the passwords

You must define the password for the system administrator and for all further users. You can specify that the passwords are changed after the initial logon. It is important to note that the system administrator password may not be used for other users. The reason for this is that in the two-user system logon is performed using only the password. It would then be impossible to distinguish between the user and the system administrator.

Note the following password rules:

❶ A password consists of a maximum of sixteen characters, and it is possible for the system administrator to specify a minimum length for passwords (see **PBA** dialog field). The minimum length for the system administrator password is six characters, while the other passwords may have less than six characters.

❷ You may only use characters from the alphabet block of the keyboard (letters, numbers and special characters). The numerical block and the function keys may not be used here.

❸ A distinction is made between upper case and lower case letters.

❹ The passwords must not be trivial (e.g.: 11111111, asasasasas, oiuztrew or 987654321).

❺ In both the two-user system and the multi-user system the system administrator password must be different from the user password.

System administrator password

The system administrator needs a password for authentication in the user logon.

To define a new password for the system administrator, tag the user SYSTEM in the user list.

Password

Enter the system administrator password in the entry field.

☞ The password must consist of at least six characters.

Verification

Repeat the password entry in this field.

☞ **Do not forget the system administration password. If you forget, you cannot deinstall Safe Guard Easy or change settings. Exception: You have applied the corresponding rights to a user.**

User password

The user needs a password for authentication at log-on. To set this select the required user from the list.

In the entry field enter the password for the user. You must comply with the password rules which have been defined. Repeat your entry in the relevant field.

Notes on dealing with passwords

For the initial logon in Safe Guard Easy each user must be given their password. Inform the user that the password must be changed at the first logon and that it should not be forgotten. You can require a password change using the option *Forced password change at initial logon* in the dialog box **PBA Settings**. If Safe Guard Easy was installed using a configuration file, the user is prompted automatically to change the password at logon.

Change password at logon

To change their password, the user must press the [F10] key after entering the (old) password. The user then enters the new password in an entry box and repeats the entry. If the entry is correct, the new password is valid from the next logon.

Menu item Change password

A user authorized to run the Safe Guard Easy Administration program, can define a new password in the *Change password* menu item (see page 5-2).

If the user forgets their password, the system administrator or another authorized user can assign a new password (cf. “Change settings”).

☞ If the system administrator forgets their password, then they do not have access to the system as system administrator any more. As a result they can neither deinstall nor modify Safe Guard Easy. However the system administrator can log on as a user, if the user tells him the password. In this case the system administrator only has user rights.

Password change after ‘n’ days

User must change password

Here the number of days which pass before the user must change their password can be entered. You can enter values between 0 and 365 days. If you enter the value “0", the user is not forced to change the password.

If a number not equal to “0" is entered, the user is prompted to change the password after the number of days entered. After this point the user can only access the system with a new password.

☞ This setting does not apply to the system administrator.

Logon allowed until ‘dd.mm.yyyy’

Limit user access

You can enter a date after which the user cannot log on to the system. This setting does not apply to the system administrator. The entry must be in the ‘dd.mm.yyyy’ data format (e.g. 31.12.1999). After this date the user can no longer access the system.

☞ This setting does not apply to the system administrator and can only be set with the multi-user system.

Template at logon

If you have set the multi-user system, you can define a template. This template contains the user rights defined by the system administrator. If you have defined less than 15 users, additional users can log on to Safe Guard Easy using this template until the number of 15 (including the template) has been reached.

Each new user who logs on to Safe Guard Easy via a template, receives the rights in Safe Guard Easy defined in the template.

The following settings are possible for a template:

❶ **none**
If you select the none entry in the *Template* box, then a user, not a template, is created.

❷ **rename**
If you select the rename entry in the *Template* box, only one other user can log on to Safe Guard Easy with this template. The template is no longer available as it has been replaced by this user.

❸ **copy**
With the copy setting in the Template box any number of users can log on using this template until the total number of users logged on reaches 15.

Remote maintenance

Using remote maintenance a user can obtain special rights on a temporary basis. These are assigned by the system administrator.

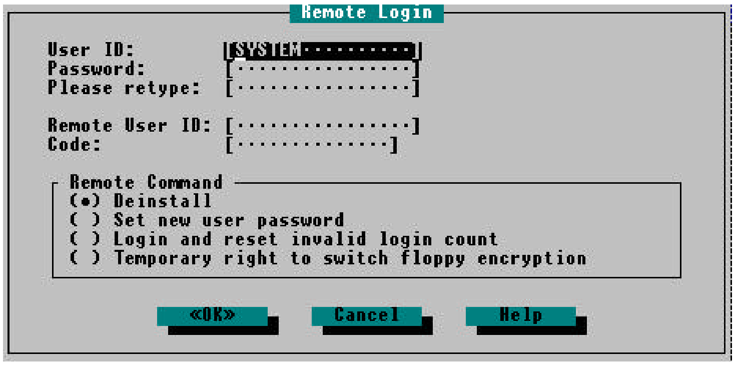
☞ For remote maintenance it is necessary that both systems are configured in an identical manner. In addition the system administrator must be registered on the foreign system with the relevant rights.

☞ The response code is only valid during the period the user is logged on. On each new logon (prompt) a new code must be generated.

Remote maintenance functions as follows.

❶ The user starts Safe Guard Easy. The user enters the user name and presses the [F9] function key in the password entry box. A fourteen character code (the challenge) is then displayed. This code is then given to the system administrator (e.g. by telephone of by fax) together with the user name.

❷ The system administrator/remote user now starts the SGEREMT.EXE program. The following dialog box appears:



```
User ID:        [SYSTEM··········]
Password:       [················]
Please retype:  [················]

Remote User ID: [················]
Code:           [··············]

 Remote Command
 (•) Deinstall
 ( ) Set new user password
 ( ) Login and reset invalid login count
 ( ) Temporary right to switch floppy encryption
```

❸ In this box the system administrator/remote user enters his/her password, the challenge and the name of the user. For a two-user system “USER” is entered as *Remote User ID*.

☞ For the system administrator with or without a user ID who deletes the *User ID* box or leaves it empty, a response code only 30 bytes long is generated.

The action to be run is then selected by the user. The entries in the dialog box are then confirmed with [OK].

❹ The response code is now calculated and displayed. It is this code that the system administrator gives to the user (by phone or by fax).

❺ The user enters the response code and then obtains the rights to his/her system assigned by the system administrator.

Note on remote maintenance:

☞ A user can also press [F9] in the PBA logon mask in the field for the password entry, after they have entered the user name. A challenge is then displayed with which special rights can be granted with remote maintenance. However the right to deinstall Safe Guard Easy cannot be granted in this way.

User rights

The system administrator can assign special rights to the user to which normally only the system administrator is allowed. These include:

Available rights

Change user
Deinstallation
Change floppy encryption
Change device encryption
Create configuration file
Change MBR protection
Change password rules
Change PBA and MBR options
Change encryption

In the **Available rights** list the above rights which are not available to the user by default are listed. The rights in the ***Assign rights*** list are allowed for the user selected.

Tag the rights you want the user to receive. Then press the [*Assign*> >]button to move the rights into the **Assigned rights** list.

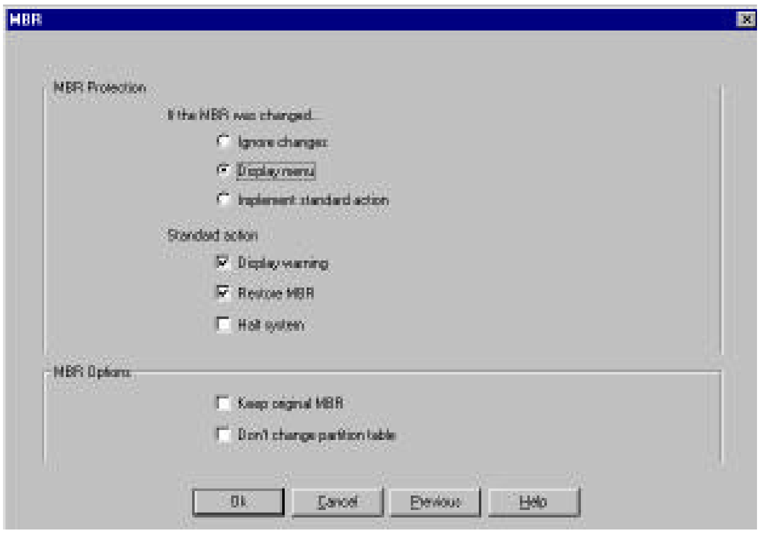
In the same way you can move the rights back to the list on the left by using the [< < *Remove*] button.

☞ Note the possible impact on your security environment.

Confirm the entries in the User Settings dialog box by pressing the [*OK*] button.

MBR Virus Protection

The **MBR** dialog box is then displayed:



MBR

MBR Protection

If the MBR was changed...

○ Ignore changes
● Display menu
○ Implement standard action

Standard action

☑ Display warning
☑ Restore MBR
☐ Halt system

MBR Options

☐ Keep original MBR
☐ Don't change partition table

MBR protection offers a protective mechanism against viruses which infect the partition sector (MBR). Unless you have set *Ignore changes* under *If the MBR was changed ...*, the MBR is checked for changes every time the system is booted.

Ignore changes

With this setting, changes to the MBR are accepted. The boot process is not terminated.

Display menu

With this option checked, a menu is displayed if the MBR is changed. The following actions can be selected:

- Default setting
- Restore
- Ignore
- Accept

With *Default setting* the user selects the standard settings. With *Restore* the backup copy is used for restoration. With *Ignore* the change is skipped and with *Accept* the current MBR is accepted.

☞ 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.

Implement standard action

This runs the standard action defined in the next section.

Display warning

If this option is tagged, a warning is displayed if the MBR has been changed. This warning must be acknowledged.

Restore MBR

With the *Restore MBR* setting, the MBR is automatically restored from a backup copy. Depending on the situation, the system is rebooted in order to remove a potential virus from memory.

Halt system

If the *Halt system* option is selected, a message is displayed after logon and the system is halted. This does not apply when the system administrator logs in.

Keep original MBR

This setting can be used with COMPAQ notebooks to boot the maintenance partition by pressing [F10], even when Safe Guard Easy is installed.

Don’t change partition table

With Safe Guard Easy all the FAT partitions are hidden on protected disks in order to make them invisible when booting with a system diskette.

As there are hardware and software configurations which cannot cope with changes of the partition table, you can enable the *Don’t change partition table* option. This is necessary with notebooks in ‘Suspend-To-Disk’ mode.

Confirm the entries in the *MBR Protection* by pressing the [*OK*] button.

This completes the installation of Safe Guard Easy. You can check the entries made. To do this select [*Check*]. If you select [*Cancel*], the installation or the creation of a configuration file is aborted.

If you have made the definitions in the *Create configuration menu item, then the* [*Save*] button is available to create a configuration file.

If this occurred in the *Install* menu item, you can now select the [*Installation*] button. After making this selection, you are prompted whether you want to restart Windows 95.

Select [*No*] if applications which have not be saved are active in the background.

☞ In this case encryption begins the next time Windows 95 is started.

Otherwise select [*Yes*]. Windows 95 is then restarted and Safe Guard Easy starts the encryption process. Once the encryption is completed, the PC is automatically rebooted. If the PBA option is enabled, the Safe Guard Easy logon mask then appears.

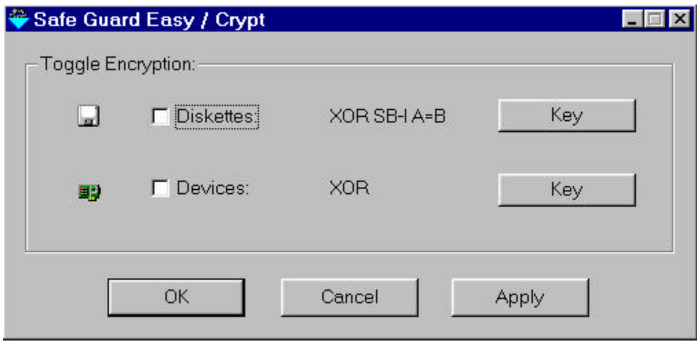
After installation

When Safe Guard Easy is installed, a folder is created in which there are icons for the administration of Safe Guard Easy (SGEADM), for toggling the floppy and device encryption (SGECRYPT) and for screen blanking (SGEBLANK).

SGEADM After double clicking on SGEADM you are placed in the logon mask. There a check is made if you are authorized to start Safe Guard Easy to make changes. Without the relevant rights you are denied entry.

SGEBLANK With a double click on SGEBLANK screen blanking is activated manually. This is a good idea if you suddenly want to leave your work place and want to lock the PC without ending the program.

SGECRYPT After calling SGECRYPT the following dialog box appears:



Safe Guard Easy / Crypt

Toggle Encryption:

□ Diskettes: XOR SB-I A=B

□ Devices: XOR

Whether a user is authorized to toggle diskette or device encryption depends on whether these rights were assigned in the Safe Guard Easy user definition. If the user has been granted a right, it appears in the relevant box (and vice versa).

The following situations are possible:

❶ The boxes for toggling encryption are enabled.

The user can enable/disable the diskette and/or device encryption. A tick in the check box indicates that encryption is enabled.

❷ The boxes for toggling encryption are not enabled.

The user has no influence on encrypting diskettes and/or devices. However a tick in a check box indicates that encryption is enabled, while an empty check box indicates that it is not activated.

☞ The right to toggle the encryption of diskettes or devices is defined on a user-specific basis. In the Safe Guard Easy default setting these rights are locked.

Other installation types

Other installation types are described below:

Installation type Boot Protection

If you decide on the *Boot Protection* installation type, select a Safe Guard Easy configuration where only the system areas (boot area, FAT and Root) of all the logical drives are encrypted. In this way there is no noticeable loss of performance when reading and writing.

With this installation type the *PBA Function* is preset. It thus offers a high level of security in respect to access protection. However unauthorized access to data on the physical level (sector) cannot be prevented.

After selection of the *Boot Protection* installation type, the installation proceeds as the *Standard* installation type. Please continue reading from page 3-3.

In the **Encryption** dialog box (page 3-11) the activation of hard disk encryption cannot be changed. You must thus define the hard disk key. It is used to encrypt the system areas. All other settings can be changed.

☞ The encryption of the system areas generally requires only a few seconds.

Installation type Partition

If your hard disk has several partitions and you do not want to encrypt all the partitions, you should select the *Partition* installation type. Here you can choose which partitions you want to encrypt.

The PC can only be accessed by entering the password (with *Extended user administration* the user name must also be entered). You can store your confidential data in the encrypted partition in order to protect them against unauthorized access. You can work in the unencrypted partition without any loss of performance.

After selecting the *Partition* menu item, the installation is as the *Standard* installation type. However in the *Encryption* dialog box you also see logical drives in addition to devices and disks. Please continue reading from page 3-3.

Installation using a configuration file

With the help of a configuration file it is possible to install the same configuration of Safe Guard Easy on several PCs. It also means that Safe Guard Easy can be installed by one person who may not know either the key or the system administrator password.

☞ Note that configuration files may only be used to create as many Safe Guard Easy versions as you have Safe Guard Easy licences. Any attempt to create more versions would constitute a breach of the licence regulations!

Before you can install Safe Guard Easy using a configuration file, you have to generate the configuration file.

Create configuration file

Once you have called up this menu item, the procedure is the same as for the installation of Safe Guard Easy. See pages 3-3 ff. for further details.

Once you have entered all of the installation details, a dialog box will appear, enabling you to specify the drive, the directory and the file name of the configuration file. CFG is proposed as extension. Other extensions can also be selected.

You can generate several configuration files. Select file names which indicate the configuration in question.

If a user who does not know the key or the system password installs Safe Guard Easy using a configuration file at a later stage, you must save the configuration file on the installation disk.

Installation by the user

If a user who does not know the key or passwords wants to install Safe Guard Easy, the installation disk must contain the relevant configuration file. There are two different possibilities here:

❶ The Safe Guard Easy for Windows 95 files are not on the hard disk. The user must enter the following command:

```
SETUP /DIR <Inst-Dir> a:\ <Name config-
    file>
```

After this command, the Safe Guard Easy files are first copied onto the hard disk. The installation is then implemented on the basis of the configuration file. The user only has to follow the screen messages.

❷ The Safe Guard Easy for Windows 95 files are already on the hard disk without Safe Guard Easy being installed. The user must enter the following command:

```
SGEADM <Name of configuration file>
```

After this command, the installation is implemented on the basis of the configuration file. The user only has to follow the screen messages.

After the automatic warm boot, Safe Guard Easy for Windows 95 is installed. The user logon appears. The user must already have been given a password. When the user first logs on, the user must change his or her password.

Installation by the system administrator

As system administrator, you can implement the installation of Safe Guard Easy in the same way as the user. However, if the Safe Guard Easy files are already on the hard disk, you can also start up Safe Guard Easy and then call up the menu item *Load configuration file*.

4. Change Settings and Deinstallation

In this chapter the menu items *Change settings* and *Deinstallation* which are part of the *Installation* menu are described. These menu items can only be run by a user who has the right to do so.

Change settings

The *Change settings* menu item is in the *Installation* menu. In it the system administration can make targeted changes of the current Safe Guard Easy settings. The changes which are possible depend on the existing setting. It is not possible to select a different installation type. To do this Safe Guard Easy must be deinstalled and then reinstalled.

When you call *Change settings*, you are placed in the installation dialog boxes. In the respective boxes, lists and check boxes the values defined in the installation are displayed. For reasons of security, passwords and keys are not displayed.

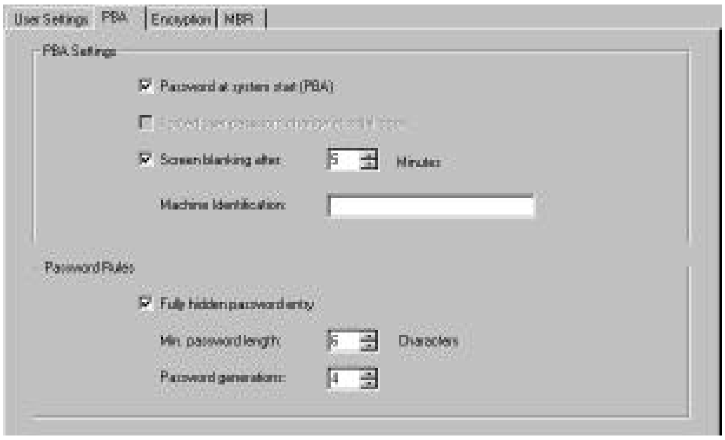
☞ The changes you make in the dialog boxes are only saved when you exit Safe Guard Easy.

For this a dialog box appears in which you are prompted whether you want to save the changes to the settings. Only when you confirm this dialog box are the changes made. Otherwise the Safe Guard Easy configuration remains unchanged.

☞ Note that for reasons of security that you should back up the settings of the system kernel after each change (see Chapter 5).

The dialog boxes are described below. The explanation is restricted to notes which you should observe when making changes. For an exact description on the individual fields refer to Chapter 3.

PBA



PBA Settings

☑ Password at system start (PBA)

□ [illegible]

☑ Screen blanking after: 5 Minutes

Machine Identification:

Password Rules

☑ Fully hidden password entry

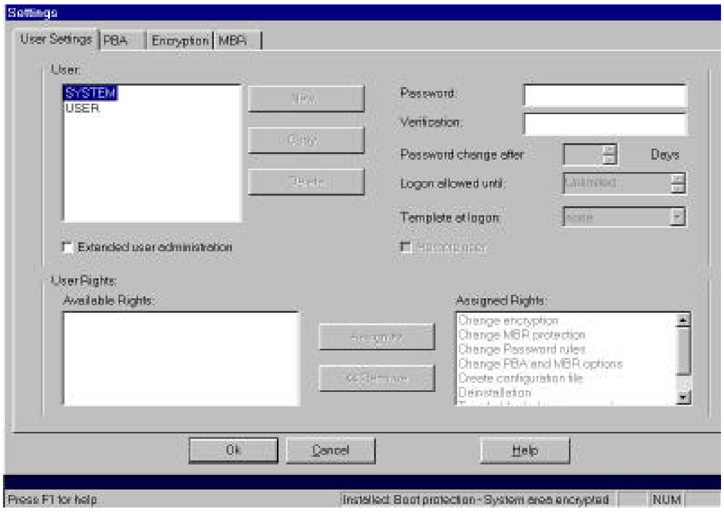
Min. password length: 6 Characters

Password generations: 4

In the PBA dialog box you can change the PBA settings and the password rules. For a description of the individual boxes, refer to page 3-5.

☞ If you remove the tag in the *Password at system start (PBA)* control box, the PBA function is disabled the next time the system is started. This also means the keys required are saved on the hard disk.

User settings



SYSTEM
USER

Logon allowed until: Unlimited

Template at logon: None

Assigned Rights:
- Change encryption
- Change MBR protection
- Change Password rules
- Change PBA and MBR options
- Create configuration file
- Deinstallation

Press F1 for help | Installed: Boot protection - System area encrypted | NUM

In this dialog box you can change the existing entries of the user profile. For a description on the individual boxes, refer to 3-19.

You can define new users, copy or remove existing ones and change the profile of existing users as you require.

If you change the tag in the *Extended user administration* check box, you switch between the two-user and the multi-user system. After the next system start the new conditions apply.

If you switch from a multi-user to a two-user system, no users are deleted internally. This means that should the multi-user system be reset at a later date, the defined users are still available.

It is only necessary to define the password if there has been a change of user or if a user has forgotten the password. If you change the user password, the user must log on with the new password at the next logon. This is why you must inform him/her of the new password.

☞ At each logon a user can change the password himself. To do so he must confirm the password with [F10] instead of [Return]. A dialog box then appears in which he can enter the new password.

If a user forgets his password and the system administrator is not available, the user can define his password himself under the supervision of the system administrator.

This can be done by means of remote maintenance (see page 3-27). For this the user presses the [F9] key in the logon screen, instead of entering the password.

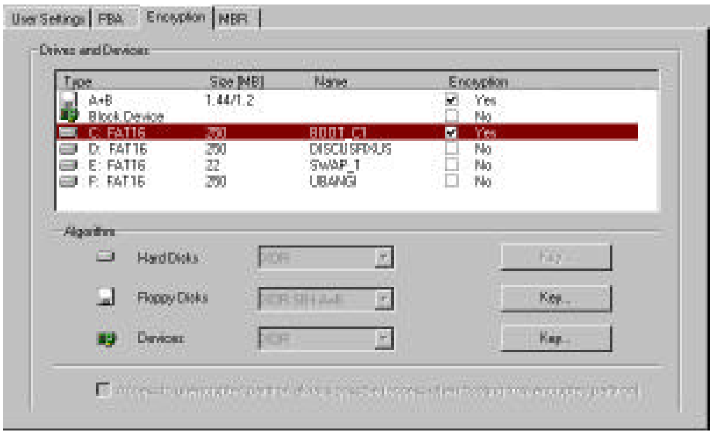
Select the action *Set new user password* and tell the user the response code which was generated. When the response code is entered correctly, the user is placed in the mask in which he can define the password himself.

Inform the user that he must not forget his password.

☞ If the system administrator forgets the system password, it is not possible to log on as system administrator. Changing settings and deinstallation can then only be implemented by users who have been assigned these rights.

Change the settings in the other boxes and lists as required. They become effective at the next system start.

Encryption



Type	Size [MB]	Name	Encryption
A+B	1.44/1.2		☑ Yes
Block Device			□ No
C: FAT16	250	BOOT_C1	☑ Yes
D: FAT16	250	DISCUSFXUS	□ No
E: FAT16	22	SWAP_1	□ No
F: FAT16	250	UBANGI	□ No

Hard Disks: XOR

Floppy Disks: XOR-SIH A-4

Devices: XOR

The Encryption dialog indicates which drives and devices are encrypted and which algorithms are used for this. The keys are not shown in the boxes. For a detailed description refer to page 3-11.

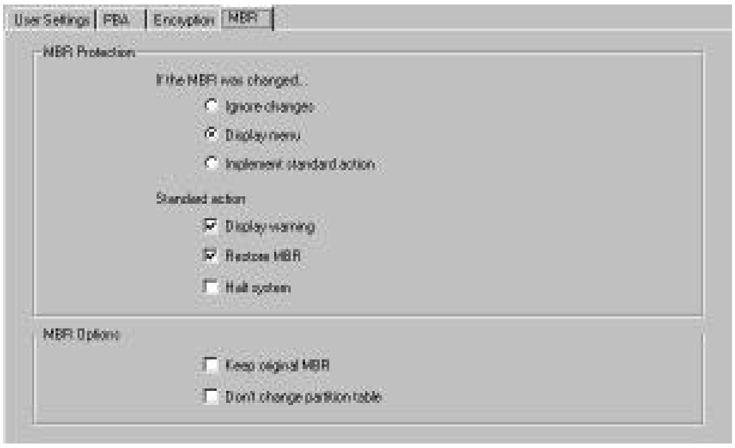
☞ For hard disks it is not possible to change either the algorithm or the key. For this Safe Guard Easy must first be deinstalled.

If you want to encrypt a unencrypted hard disk, this is implemented directly after the changes are saved. A warm boot then occurs.

For floppy drives or block devices you can define a new key. However, floppies or devices with the old settings can no longer be read.

Change the settings as you require. They become effective after the next system start.

MBR



MBR Protection

If the MBR was changed...

○ Ignore changes
● Display menu
○ Implement standard action

Standard action

☑ Display warning
☑ Restore MBR
☐ Halt system

MBR Options

☐ Keep original MBR
☐ Don't change partition table

In this dialog box the current settings on the MBR virus protection are displayed. Change these settings as required. They become effective after the next system start. For a detailed description, refer to page 3-30.

Deinstallation of Safe Guard Easy

Only the system administrator and users authorized to do so can deinstall Safe Guard Easy. An exception here is remote deinstallation, where a user can carry out the deinstallation guided by a system administratior who is not physically present.

☞ Before deinstalling Safe Guard Easy we recommend a complete hard disk backup.

Menu item ***Deinstall***

The *Deinstallation* menu item is only active if Safe Guard Easy is installed on the system. When you call *Deinstallation* a dialog box with a confirmation prompt appears. If you answer [No], you are returned to the main menu. With [Yes] Safe Guard Easy is deinstalled and an automatic warm boot implemented.

Remote deinstallation

This way of deinstalling Safe Guard Easy is only sensible if the system administrator is not present. Here supervised by the system administrator the user is empowered to deinstall Safe Guard Easy. For this it is necessary that the user and the system administrator can communicate either by telephone or by fax. The procedure for remote deinstallation is described on 3-27.

5. The *Extras* Menu

The *Extras* menu contains only two menu items:

❑ Change password

❑ Back up system kernel

In *Change password* the user can redefine his password without calling the user administration.

Backing up the system kernel on the other hand makes it possible to restore the system kernel after a system malfunction.

If Safe Guard Easy detects a malfunction and there is a current backup of the system kernel, you can restore the system kernel under DOS.

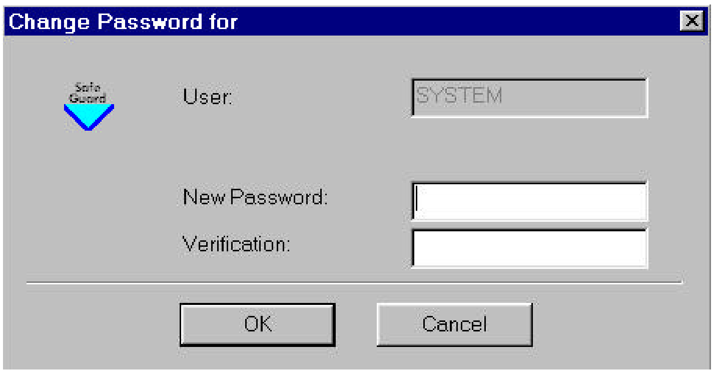
If there is no current backup of the system kernel, you can also try under DOS to repair the system kernel.

These two options on Safe Guard Easy malfunctions are explained at the end of the chapter in the section *Remove system errors*. The two menu items are described first.

Change password

Every user can define a new password in the *Change password* menu item, without calling the User administration.

After calling *Change password*, the following dialog box appears:



Enter the new password. In doing so observe the password rules. Repeat the password entry in the corresponding box. Confirm the entry. The new password is valid from the next logon.

If your entries were not identical or if they violated password rules, an error message appears. In this case, repeat the entries.

Backup system kernel

With this function the entire system kernel (drivers for Safe Guard Easy and the Master Boot Record) is backed up in a file. This backup is specific to the individual system.

☞ A backup file for restoring the system kernel can be used only on the PC where it was created. The menu item *Backup system kernel* is only active if Safe Guard Easy does not detect any malfunction.

When it is called a dialog box appears in which you set the drive and directory where the backup file should be saved. In the *File name* box, name the file where the system kernel should be saved. The extension proposed SVF can be changed. You can create several backup files of the system kernel.

When you confirm the dialog box, a backup file is saved. A message indicating that this is done then appears. When you confirm it, you are placed back into the Safe Guard Easy main menu.

In addition with the SGEBACK.EXE program you can back up the system kernel from the command line, without starting the Safe Guard Easy Administration program:

```
SGEBACK <Target file>
```

As the screen messages are taken from the text file, the SGEASY.HLP file must be in the directory being called.

☞ After the installation and each time the Safe Guard Easy settings are changed, the system kernel should be backed up again. A backup file for restoring the system kernel can only be used on the PC where it was created.

Removing system errors

If your PC with an encrypted hard disk has a system error, the drivers cannot be found. As a consequence the PC cannot boot. In this case you must boot from drive A: and call Safe Guard Easy from the floppy drive. The password prompt cannot be used.

As Safe Guard Easy has detected a system error, the *Extras* menu has two new menu items, *Restore system kernel* and *Repair*. With these functions you can try to eliminate the system malfunction. As the screen messages are taken from the text file, the file SGEASY.HLP must be in the directory being called.

☞ The following functions may not be run if Safe Guard Easy has been deinstalled.

Restore system kernel

With this function you can restore the system kernel from a 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.

☞ These functions 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.

Boot from drive A:. Start Safe Guard Easy from the floppy drive. When you call the *Restore system kernel* menu in *Extras,* a dialog box appears in which you can specify the drive, the directory and the backup file.

For security reasons the current system password is prompted before the actual restoration. This prevents a driver with an unknown system password from being loaded. The restoration of the system kernel then begins.

Both the driver and the Master Boot Record are restored. A message then appears informing you if the restoration was successful or not.

Repair

With *Repair* you can try to eliminate a system error.

☞ 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.

Boot from drive A:. Start Safe Guard Easy from the floppy drive. If you call the *Repair* menu item in the *Extras* menu, a diagnostic routine attempts to localise the system kernel and to reactivate it. This can take several minutes. The progress is shown in a percentage bar. A message then appears informing you if the repair was successful or not.

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

A. Error messages

All the error messages have the following format:

```
(Fatal) error SGEnnn: <text>
```

‘SGE’ is the Safe Guard Easy product-ID, and ‘nnn’ a three-figure error number.

The error numbers are divided into the following groups:

000-099: (not currently in use)

100-199: product-specific errors

200-299: hardware and firmware errors

300-399: system errors

400-499: system kernel

500-599: errors with utilities such as SGEFLPY or SGE-DEVC

600-899: (not currently in use)

900-989: reserved

990-998: initialisation errors

999: unknown errors

Error messages

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

After each error message (typed in bold) the cause of the error is explained and the steps required to eliminate the error are given.

Product-specific errors

100 **Different version of Safe Guard Easy or CRYPTON DOS already installed.**

Can only occur if an attempt was made to evaluate a configuration file via command line.

101 **Cannot read configuration file**

The file indicated cannot be found, opened or read.

102 **Invalid configuration file**

The file indicated exists, but it is not a configuration file or it was damaged.

103 **Cannot write configuration file**

The disk is full, the drive is not ready or similar.

104 Currently installed driver is inconsistent

The check made at the program start indicated that the driver or the MBR is damaged. In the Recovery pulldown menu call the menu item Restore system kernel or Repair.

105 System kernel already installed

Safe Guard Easy has already been installed.

106 This program cannot be run under X.

This software uses functions which could lead to interference or data loss in multi-tasking environments.

107 Cannot write backup file

The disk is full, the directory is full, the file is read-only.

108 Cannot read backup file

The file indicated cannot be found, opened or read.

109 Invalid backup file

The file indicated can be read, but it is not a backup file or it is logically damaged.

110 Cannot install a second boot partition on disk 0

The “Twin Boot” installation automatically creates a second primary DOS-partition on disk 0, if one does not already exist. This is only possible by converting a logical drive or by using available hard disk areas (outside of all partitions).

111 Cannot install Boot Manager via OS/2

The Boot Manager supplied with OS/2 is not compatible with the system kernel or would not function as expected after installation. In addition, this product is not intended for operation under OS/2.

112 Earlier version of Safe Guard Easy or C:CRYPT already installed

Safe Guard Easy 1.x or C:CRYPT must be deinstalled before you can install Safe Guard Easy 2.00.

113 Last installation / deinstallation / change not closed

As the last installation / deinstallation / change was not closed properly, it must be implemented again.

114 Not enough contiguous space on the boot partition

Before installation you must ensure that the boot partition has enough contiguous memory.

115 No access on the system kernel partition

This error message appears if booting does not take place from the installation partition, but from the floppy drive.

116 No resource files found

There is no resource file (*.RES) in the product directory, although it is essential for Safe Guard Easy. Copy all resource files of the original diskette into the product directory.

117 Cannot open resource file

At least one resource file was found in the product directory. However, it cannot be opened. The file is possibly damaged or locked (e.g. on a network).

Check the file system with SCANDISK or CHKDSK. Also check the product directory if there are foreign files with the ‘RES’ extension. Remove them.

If the problem is still not solved after a warm boot, then you must reinstall Safe Guard Easy.

118 Invalid or defective resource file

The resource file found cannot be read or has an unknown format. This file is possibly damaged or originates from a different version.

Check the file system with SCANDISK or CHKDSK. Also check the product directory if there are foreign files with the 'RES' extension. Remove them.

If the problem is still not solved after a warm boot, then you must reinstall Safe Guard Easy.

119 Algorithm not found

The module for the algorithm selected cannot be found. This can occur on an upgrade version, if you have used an algorithm which is not supported in the new version (e.g. FEAL) in the version you have installed.

If your existing version is installed with a FEAL algorithm, you must first deinstall Safe Guard Easy. Then install the new version.

Hardware and company-specific errors

200 Cannot analyze hard disk structure

Possible causes: there are either no hard disks or more than 2 hard disks in the system, hard disk parameters are incorrect, disk incorrect or not partitioned, disk defective or similar.

201 Hard disk read failure

Direct reading of the disk not possible or only partially possible.

202 Hard disk write failure

Direct writing of the disk not possible or only partially possible.

203 Invalid partition table on disk 0

The software cannot be installed on this system, usually on grounds of compatibility. The installation is aborted to prevent damage.

204 Incompatible ROM BIOS

The software cannot be installed on this system, usually on grounds of compatibility. The installation is aborted to prevent damage.

205 Invalid boot sector

A partition was found in the disk analysis, which was entered as DOS partition. However its boot sector contains contradictory or invalid information. This can also be the case, if the partition is created, but not formatted.

206 Cannot lock volume

Safe Guard Easy attempts to gain exclusive access on the drive but is prevented by another program.

System-specific errors

The error messages 300 to 312 are critical errors.

See DOS manual.

300 Medium write protected

301 Unknown unit

302 Drive X not ready

303 Unknown command

304 CRC error

305 Bad request

306 Seek error

307 Unknown media type

308 Sector not found

309 Printer out of paper

310 Write error

311 Read error

312 General error

320 Out of memory

Please ensure that there is enough memory for the installation program. If necessary, deinstall any programs loaded resident.

321 Divide trap at program address <address>

Actually this error should not occur. If it does occur, it is essential to note the address. Without an address it is not possible to understand the problem.

322 Batch overrun

An internal error occurred. Please call the hotline.

System kernel errors

400 Kernel load error

It was not possible to integrate the driver at the system start. Possible causes are: physical defect of the hard disk in the area of the driver; manipulation of the partition sector.

401 Invalid kernel

The kernel area could be read, but seems changed. Possible causes: kernel was overwritten (unlikely); partition sector has been changed.

402 Hard disk 0 read failure

The boot sector of the active partition can not be read.

403 No valid MBR on disk 0

Partition sector contains no partition or no active partition.

404 Module load failure

An additional module could not be loaded.

Errors with utilities such as SGEFLPY or SGEDEVC

500 Encryption driver not installed

A Safe Guard Easy program was called, but Safe Guard Easy is not installed. To start the program, Safe Guard Easy must be installed.

501 Incorrect encryption driver version

A Safe Guard Easy program was installed, but the wrong version of Safe Guard Easy is installed. To start the program the right Safe Guard Easy version must be installed.

502 Invalid command line argument(s)

Incorrect parameter given to the program.

Initialisation error

990 Cannot access language file

Access error on the language file.

991 Integrity check failure

Error on integrity test. Possibly a file was changed.

Unknown errors

999 Unknown error

Can also occur with other undefined numbers. For this reason this classification.

H. Hotline & Support

We are happy to support you in all matters relating to our products. Maintenance agreements are available which regulate support and updates as well as enabling access to our mailbox. Our training seminars are open to all users. Please ask for our training program.

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

Normal use of the hotline is available free of charge. But only call the hotline after a study of the manual and extensive trial and error have not produced a solution for your problem. Prepare for the call with our hotline. You require:

- Model and type of your PC, how it is equipped and size of the main and disk memory.
- Operating system and its release status
- Name of the Utimaco product and its release status

You can reach the free hotline on the following number:

0180-521 32 45

INDEX