SafeGuard® LAN Crypt

Version 1.0

for Windows ® NT 4.0

Confidential Data Storage
in Global Organisations

Utimaco Safeware AG, D-61440 Oberursel

Utimaco Safe Concept GmbH, A-4020 Linz

User Handbook 1st Edition, December 1998

TABLE OF CONTENTS

Overview **Chapter 1**

Definitions 1-3

Introduction 1-6

Application examples 1-7

Enterprise Distribution Concept 1-10

Most important features 1-22

SafeGuard LAN Crypt Administration 1-24

Encryption 1-31

Encryption algorithms 1-32

Support and hotline 1-36

Installation **Chapter 2**

General 2-2

System requirements 2-3

Installation/update 2-4

Installation from disk 2-5

Installation from network to PC 2-11

Script-driven installation 2-13

Key Management **Chapter 3**

Structure of the key file 3-2

The file header 3-6

User Functions **Chapter 4**

SafeGuard LAN Crypt User Menu 4-2

Logon to SafeGuard LAN Crypt 4-6

Change user password 4-8

Switch key file 4-10

Encryption dialog 4-11

Initial encryption 4-15

Decrypt files 4-16

Delete file 4-17

Rename directories 4-18

Status display in Windows NT Explorer 4-19

Exit SafeGuard LAN Crypt 4-21

Administration Chapter 5

SafeGuard LAN Crypt User menu 5-4

SafeGuard LAN Crypt key file 5-6

First steps: default.tre 5-7

Change security administrator password 5-9

Administration dialog 5-12

Create a key file 5-15

Switch key file 5-17

Generate new key 5-18

Import key 5-21

Encryption rules 5-23

Hierarchy of encryption rules 5-24

Edit entries 5-26

Define encryption rules 5-28

Passwords 5-30

The specimen file demo.tre 5-33

Encrypted CD-ROMs **Appendix A**

General A-2

Create encrypted CD-ROM A-3

Prepare the files A-4

Initial encryption of the files A-5

Write CD-ROM A-7

E-Mail **Appendix B**

General B-2

Send e-mail B-3

Receive e-mail B-6

Backup **Appendix C**

General C-2

Backup on floppy disks C-3

Restore data from floppy disk C-6

Backup using backup software C-9

Restore data with backup software C-10

Tips & Hints **Appendix D**

Autosave-functions D-2

FTP server D-3

File attributes D-4

NTFS attribute D-5

Compressed files D-6

Registry-Entries **Appendix E**

Registry-entries E-2

Chapter 1

Overview

Contents:

- Definitions
- Introduction
- Application examples
- Enterprise Distribution Concept
- The most important characteristics
- SafeGuard LAN Crypt Administration
- Encryption algorithms
- Support and hotline

Increasingly sensitive data are saved and processed on servers in network environments and on local PCs. The confidentiality of these data must be safeguarded.

In many networks (LANs) there are dangers which are generally unknown and often underestimated. Modern network systems generally protect the data saved centrally on the server very well. But there are still large gaps. SafeGuard LAN Crypt can close these gaps.

This chapter provides a general overview on the structure and functions of SafeGuard LAN Crypt. Read this chapter prior to installation to familiarise yourself with the SafeGuard LAN Crypt product philosophy. This is important so that you can use the broad range of SafeGuard LAN Crypt applications to the full.

Definitions

The specialised terms used in this handbook are explained in brief below.

- **Security officer**

The security officer generates a master key file with all the keys required (Admin keys) for the organisation. For distribution purposes the security officer makes copies of the master key files (templates).

The template only contains the subset of the key which is made available to the relevant security administrator.

The security officer should be a trustworthy person. He should not have access to the confidential data of the company.

- **Security administrator**

The security administrators create the user key files. Into these files you import the keys needed by the individual users using the templates provided by the security officer.

◆ Master key file

The master key file is the key file created by the security officer. It contains all the keys which are valid in the company, but no encryption rules.

◆ Template

A template is part of the master key file. It contains valid keys only for a defined area (e.g. Personnel Department).

◆ Key File

The SafeGuard LAN Crypt key file contains the information needed for the application. It contains password references, keys and encryption rules.

Key files are stored in encrypted form and can only be edited by the SafeGuard LAN Crypt Administration.

◆ Admin key

The admin key is specified by the security officer when creating the master key file. The data key saved in the file header is encrypted using the valid admin key.

- **Data key**

The data key is generated at the initial encryption of a file using random algorithms. It is used to encrypt data and is saved in the file header together with the admin key in encrypted form.

- **System key**

The system key is generated for each key file using random algorithms. It is used to encrypt profiles and keys in the key file.

- **File header**

Every file encrypted by SafeGuard LAN Crypt has an approx. 4 KB file header. The data key valid for this file is saved in encrypted form in the file header . The symbolic name of the admin key is in the file header as plain text.

For the explanation on the way individual keys are combined, see the chapter “Key Management”.

Introduction

SafeGuard LAN Crypt encrypts selected files in LAN/WAN environments and on local PC (on hard disk, CD-ROM, removable media and floppy disk).

If the data are on a server, they are transferred to the PC or workstation in encrypted form. They remain completely encrypted on the server and in the network. Decryption takes place only in the main memory of the PC or the workstation.

The encryption program is loaded resident. This means it can only be removed from the PC memory at a reboot. However, it can be deactivated at any time when the user (temporarily) disables the encryption or logs off from SafeGuard LAN Crypt.

Application examples

Problem

System administrators have unrestricted access to personal information at Board level or from the Personnel Department. Due to their activities the rights of the system administrators cannot be restricted. System administrators need their rights to maintain the system and to make backups.

Application example: Field sales

Field sales staff regularly receive sensitive information, such as price lists, terms and conditions, product information. Using encrypted CDs, the data can be generated on one master data carrier for all involved and then distributed appropriately.
Each authorised user or each authorised department then can access its data with the key which has been assigned. The other areas of the CD cannot be accessed. Encryption safeguards the integrity and confidentiality of sensitive data. In addition costs are considerably lower.

Application examples: Outsourcing

A company places the administration of his IT landscape in the hands of an external service provider. By taking on the responsibility for network administration, the service provider guarantees the permanent availability of all data relevant to the company.Generally this includes very sensitive information. If disseminated in an improper manner, this would result in great damage. In general an organisational agreement is made with the service provider that he may not read confidential data. Using SafeGuard LAN Crypt the company can ensure technically that the updating and maintenance of the data infrastructure is guaranteed without it being possible to view sensitive.

Application example: Group concept

The company management prepares confidential data which has to be processed by third parties. Executives pass on confidential documents to their assistants, to the Personnel Department or to outsiders.

By using SafeGuard LAN Crypt to implement a group concept, confidential documents can be processed by different groups/employees without individuals having access to all the keys of the other group members.With this concept trusted interfaces between various hierarchy levels can be created. Using prescribed directories encrypted documents can be transferred between persons having different hierarchy levels (Board/Assistants). Nonetheless each person retains his own private data in his own directory with his own keys.

Enterprise Distribution Concept

In designing SafeGuard LAN Crypt, corporate objectives and interests predominated.

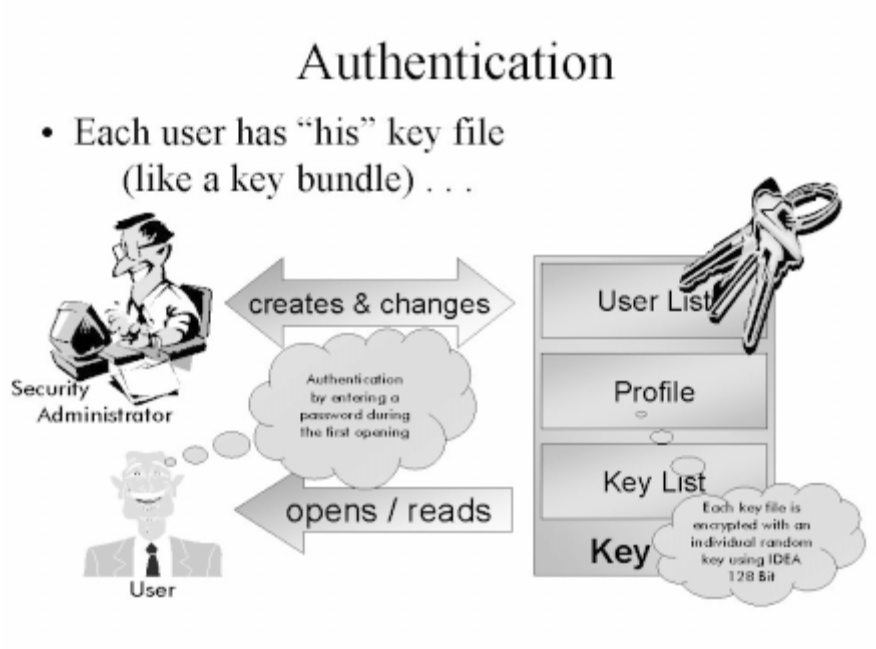
The company provides its employees with individual, user-specific encryption. But the encryption of private documents should not be used against the interests of the company. The individual encryption of documents should be used in this area to safeguard the private sphere of an employee in the company.

However the company as institution always retains ultimate control over the data. For the company defines the security concept, names the security officer and is thus responsible for the separation and distribution of key knowledge and key use.

Solution

The solution of Utimaco enables user-specific encryption at file level. For this the user must have physical access to the files or data media. At the same time each user has his own private files and commonly used data.

User authentication and data encryption occur directly at the workplace. Passwords and/or keys are not transferred via the network and thus cannot be intercepted.



With its integrated access control SafeGuard LAN Crypt not only prevents access to confidential documents by persons outside the circle of users, but also access to confidential documents by unauthorised persons in the circle of users.

Access is denied if a SafeGuard LAN Crypt user attempts to read a document for which he does not have the appropriate key. Manipulation of confidential data, deliberate or accidental is thus excluded.

With an individually assigned key bundle, the so-called key file, each user controls not only his own but also commonly used keys. Each user can encrypt and save documents, thus making these documents accessible only for himself. However, he can also encrypt documents which can be read and changed by several persons specified by the security officer.

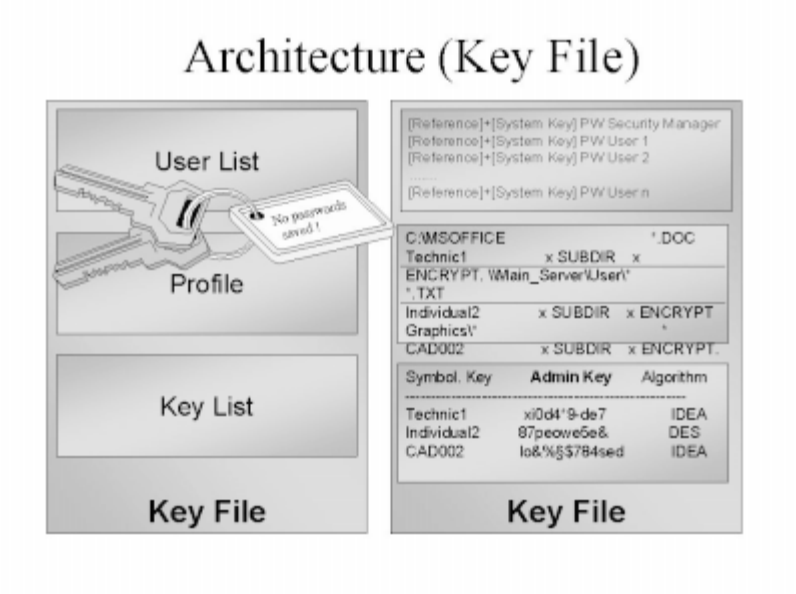
The security concept is based on a multilevel key management method using secure encryption (128 bit IDEA) and random keys.

User authentication and the specification of encrypted files can be accessed is done using the key bundle, the key file. All authorised, i.e. authenticated users of a key file have the same rights. There cannot be any hierarchies in the key bundle. Hierarchies are mapped by the linking of keys to various key files.

As with a real key bundle, access to encrypted documents is made possible only with the possession of a key. The key files contain all the relevant information for the user to work with encrypted documents.

In addition to the key bundle, the key files also contain a list of the authorised users (user list) together with the addresses of all confidential documents (profile: a list of all directories/drives with encrypted files).

The security administrator, a trusted person to administer the key files (not the system administrator) generates and changes the key files, while the user can only open them and read them.



For each authorised user of the relevant key file the user list contains two encrypted entries - a reference value (value with known contents which cannot be changed) and a system key (a randomly generated key, individual for each key file) .

The entries are not saved in plain text, but are encrypted with the password of the corresponding user using IDEA.

The key list is the equivalent of the key bundle, i.e. all the keys (admin keys) which the authorised user can use are saved here. The use of symbolic names and hiding the real key values represents a separation between the security administrator and the security officer.

The security administrator generates the individual key files for the user and assigns them keys and profiles. In doing so he does not know the actual key values, operating only with symbolic names.

The security officer is a trusted person within the organisation. He defines the key values and gives them to the security administrators by means of the so-called master key files. Only the security officer knows the "real" key, but he does not generally have physical access to the data.

Application

User logon and authentication takes place the first time a key file is accessed and can be linked to the logon to the operating systems.

The encryption of all files, directories and drives in line with the profiles is transparent and occurs in the background without the user being aware of it. All applications on the user desktop only obtain data in plain text.

In certain cases this may be undesirable. For example, it should be possible to make backups in encrypted form or to append encrypted documents to an e-mail.

With the normal functioning of file encryption, the e-mail client would read the document in plain text and have no possibility of leaving it encrypted. By definition the data filter installed with the file encryption ensures that all read/write accesses on confidential data are encrypted/decrypted.

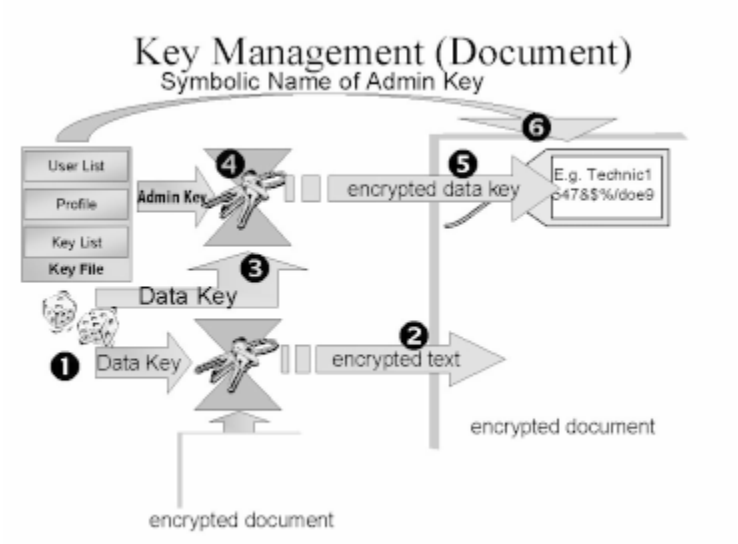
To avoid this the SafeGuard LAN Crypt file filter can be deactivated, without disabling the access protection. This means that the encrypted document remains encrypted in spite of a permitted access and can then be appended in encrypted form to an e-mail or be saved as part of a backup.

Encryption

The data, a Word document, for example, are encrypted with an individual, completely randomly generated key (data key) using an algorithm specified by the security officer (algorithms which can be used are XOR, DES and IDEA).

In the encrypted document SafeGuard LAN Crypt also generates a data block in which reference information is stored (file header).

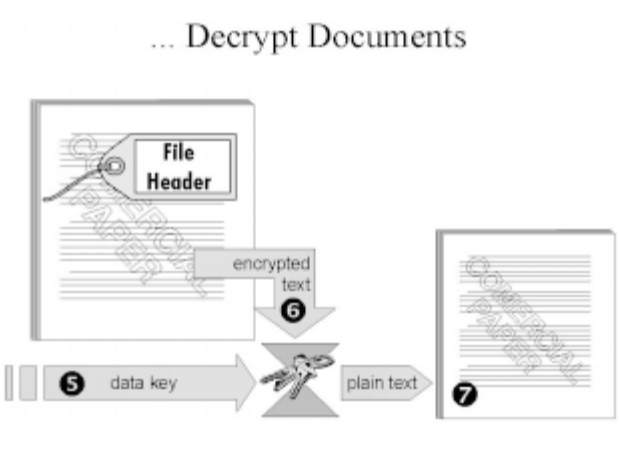
In this file header the symbolic name of the admin key and the data key encrypted with this admin key are saved. The admin key is specified by the security officer when creating the master key files.



Decryption

The user logs on once when opening his key file, typically at the same time as the operating system logon.When opening encrypted documents no further authentication is necessary. When opening the key file the system key is formed on the basis of the correct password and is used to decrypt the profiles and the key bundle (admin keys).

When accessing an encrypted document the entry in the file header shows which symbolic key was used for encryption. Via the file name SafeGuard LAN Crypt now can check for the authorised user in his opened key file (key bundle) and calculate the actual key value (admin key).



Using the admin key the actual data key is obtained and used by the file filter to decrypt the document.

This procedure takes place in the main memory of the user PC, and takes only a fraction of a second so that the user is not aware of it.

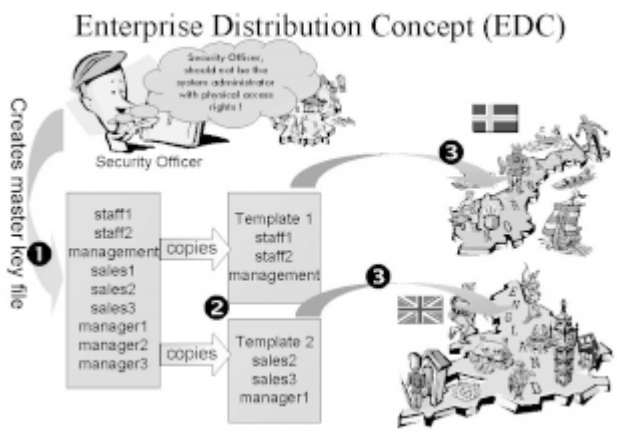
Enterprise Distribution Concept (EDC)

The Enterprise Distribution Concept ensures that key generation and rights administration in the network can (and should) be separated in terms of persons. The keys are generated by a security officer. This can be both an internal person or institute, or an external service provider such as a Trust Center.

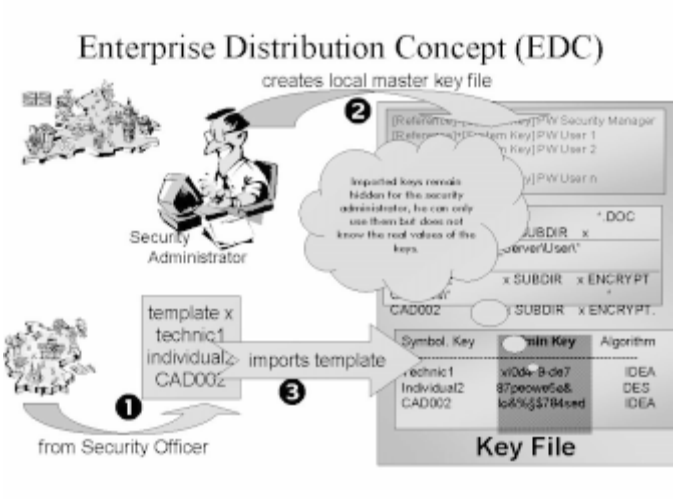
The security officer needs neither technical knowledge nor supervisor rights in the network. This ensures the complete separation between the knowledge of the key values (key knowledge) and the use of these keys (key application) by the security administrator.

The security officer generates a master key file with the necessary keys (admin keys) for the organisation. For distribution purposes the security officer creates individual "copies" of the key file (templates). These templates contain only those keys relevant for the department or subsidiary. They are then made available to the security administrator.

The security administrators, organised if necessary on a regional basis (e.g. in subsidiaries), in their turn create new key files, into which they import the templates they are sent.



The imported keys (admin keys) remain hidden to the security administrator. All he sees are the symbolic names. These enable him to make the profile allocations. This also demonstrates the separation between key knowledge and key application.



Most important features

- **Strong transparent encryption**
  Strong transparent encryption of all data to be protected by SafeGuard LAN Crypt.

- **Enterprise Distribution Concept**
  On a corporate basis a security officer defines the keys to be used, without accessing the resources to be protected.

- **Common use of resources**
  With the header method used in SafeGuard LAN Crypt, several users can access encrypted resources in line with their rights.

- **User-friendly**
  For the user SafeGuard LAN Crypt is largely transparent. After logon no user intervention is necessary in day-to-day work.

- **Easy to administer**
  In the SafeGuard LAN Crypt Administration dialog keys and encryption rules (user rights) can be effectively defined without much administration.

- **Encryption switch**
  The transparent encryption can be temporarily disabled in order for data to be sent in encrypted form (e.g. via e-mail or disk).

- **Remote accesses**
  As file encryption/decryption takes place in the working memory of the workstation or PC, it is not possible to make a remote access to encrypted files without the relevant key, even if the key file is open.

- **Integrated access protection**
  If SafeGuard LAN Crypt is used across the whole network manipulation of files protected by SafeGuard LAN Crypt for users without rights is impossible. This is because SafeGuard LAN Crypt prevents any access apart from the defined authorisation.

SafeGuard LAN Crypt Administration

To secure the best possible protection SafeGuard LAN Crypt Administration is divided into two areas:

- **User mode:**
  Functions which the user can access (encryption dialog). Here the

- **Administrator mode:**
  Functions reserved for the security administrator (creating key files, defining encryption rules).The Administrator mode contains not only the administration dialog but also the encryption dialog. Here dialog keys can be generated, encryption rules defined and passwords issued for key files.

Security administratorpassword

It is only possible to get into the Administrator mode by logging on as security administrator. This means that it is necessary to have the security administrator password for a key file.

It is only possible to create key files in Administrator mode.

Key files

A SafeGuard LAN Crypt key files comprises SafeGuard LAN Crypt keys, information for the initial encryption (encryption rules), codes for the valid passwords and system key.With a key file different user rights for file encryption/decryption, directories and drives can be allocated.

The encryption rules define quite clearly which directories/files are encrypted with which keys.

The key file (comparable with a key bundle) is very important in Safeguard LAN Crypt, holding the keys to encrypt/decrypt files. Without the valid key, access to an encrypted file is impossible.

As a key file can contain several keys, it is possible to form user groups by allocating the keys required.

For each key file there is a security administrator password and one or more user passwords. It is necessary to be logged onto a key file with a security administrator password to have the rights to define keys and encryption rules, thus determining access rights.

The contents of a key file are saved in encrypted form to ensure that the contents cannot be read (see Chapter "Key Management").

default.tre

By default SafeGuard LAN Crypt is supplied with the key file *default.tre*. This allows the security administrator to get to know the software (password for *default.tre:* system - please note the syntax). After the first logon with the standard password, the security administrator password should be changed.

Password

To start SafeGuard LAN Crypt you require a password for a key file. The key file contains the information required for encryption (encryption rules) and the key you require.

Before starting your work with SafeGuard LAN Crypt, you need a password from the security administrator.

You should change your password after your receive it. Treat your password in a confidential manner. It should not get into the hands of a system administrator.

A password can also contain figures and special characters. In this way you can ensure that your password cannot be guessed.

Access rights

Together with the users the security administrator defines the key file which grants them various access rights. For example an employee of the Accounting Department can obtain access both to Personnel data as well as Accounting data, while an employee of the Personnel Department only has access to personnel data.

These access rights are realised by the possession of keys.

Encryption rules

Encryption rules describe exactly which file(s) are to be encrypted in which directory using which keys.

Encryption is not possible without such a profile. Only those files can be encrypted/decrypted for which there is an encryption rules entry in the active key file.

Logon

The SafeGuard LAN Crypt logon dialog is presented automatically each time there is a Windows NT logon (see Chapter “Installation”). The user enters his password for his key file and so obtains access to the encrypted files.

As file encryption/decryption takes place automatically and without any noticeable time lag, the user is not aware that the process is taking place.

If the user does not log on to a key file when booting (by aborting the logon procedure), he does not obtain access to encrypted files. Of course, it is possible to log on manually to SafeGuard LAN Crypt during a session.

User menu

Once the user has logged on to a key file, he can use the SafeGuard LAN Crypt User menu. He can open it by clicking with the right mouse key on the SafeGuard LAN Crypt icon in the Windows task bar.It allows the simple control of LAN Crypt functions such as logon/logoff to the key file, enabling/disabling encryption, exiting SafeGuard LAN Crypt and starting the SafeGuard LAN Crypt Administration.

Working with SafeGuard LAN Crypt

In the daily work with SafeGuard LAN Crypt you log on to SafeGuard LAN Crypt after booting the workstation or PC and then work in your applications as normal.

To access encrypted files with application programs, the key file must be opened.

As file encryption/decryption takes place automatically and without any noticeable time lag, you are not aware that the process is taking place.

You only need work in the SafeGuard LAN Crypt Encryption dialog:

- After installing SafeGuard LAN Crypt to encrypt existing file.If you do not implement an initial encryption, the files are only encrypted when you open them for the first time to process them. New files are encrypted in line with the encryption rules.

- If the encryption rules are changed in your key file. You must then implement an initial encryption to encrypt the files in line with the new rules.

- In certain exceptional cases, when, for example, a user who does not use SafeGuard LAN Crypt, copies files into one of your encrypted directories.The files would remain unencrypted until you open them the first time to process them. If, however, you implement an initial encryption, the files are then immediately encrypted in line with encryption rules.

If you implement an initial encryption at regular intervals, you can ensure that are the files are encrypted in line with your encryption rules.

Deactivating SafeGuard LAN Crypt

You can deactivate SafeGuard LAN Crypt at any time by logging off from the SafeGuard LAN Crypt application.

By temporarily logging off from SafeGuard LAN Crypt, in work breaks, for example, you can protect the contents of your files against unauthorised access. For as long as you are logged on to your key file, anyone who can access your PC can also access your confidential data, even when you are not there.

However, remote accesses are not possible without the relevant keys.

Encryption

Data encryption under SafeGuard LAN Crypt is largely automated.

The keys for encryption are located in the key file. There are precise encryption rules for each key. These state which files (directories) are to be encrypted with which keys.

The user can only encrypt or decrypt such files (directories) where there is an entry in the encryption rules.

To implement an initial encryption all that the user needs to do is to tag the files or directories in the SafeGuard LAN Crypt encryption dialog and to activate the encryption switch [Init]. SafeGuard LAN Crypt then encrypts the data in line with the encryption rules.

It is also possible to encrypt individual files using the Context menu (right mouse key) in Explorer.

Encryption algorithms

SafeGuard LAN Crypt uses the following encryption algorithms.

- **XOR**

The XOR algorithm is very fast, but cannot be regarded as secure.

- **DES**

DES (Data Encryption Standard) was developed in 1970. DES is a block encryption which operates with 64-bit plain text blocks and a 56-bit key.DES works with 16 iterations (rounds) and is thus relatively slow. According to the state-of-the-art, the DES algorithm can no longer be regarded as secure.

- **IDEA**

IDEA (International Data Encryption Algorithm) was developed in 1990. IDEA is a block encryption which operates with 64-bit plain text blocks and a 128-bit key.This algorithm can be implemented very efficiently, even with very slow processors. According to the state-of-the-art IDEA is regarded as the most secure symmetric encryption algorithm.

Encrypt, Decrypt, Recrypt

In SafeGuard LAN Crypt encryption takes place in a transparent way. This means:

All files where encryption rules apply are automatically encrypted.

If files are copied or moved into a directory for which there are encryption regulations, they are automatically encrypted using the relevant key. It is quite possible that different encryption rules apply in a single directory. In SafeGuard LAN Crypt data encryption is not directory-specific, but it is implemented in line with the given encryption rules. This means that different keys can apply for different files in one directory.If files with specific encryption rules are renamed they remain encrypted with the key specified in the rules, provided they still comply with these rules (e.g. *.TXT).

If files are copied or moved into a place where the encryption regulations do not apply, they are automatically decrypted.

If files encrypted in line with encryption rules are copied or moved to a place where the previous rules no longer apply, but where there are new encryption rules which apply to these data, the data is first decrypted, and then re-encrypted in line with the new encryption rules.

Transparent encryption applies to all file operations (including renaming, etc.). As all processes run in the

background the user is not aware of the encryption procedure in his daily work.

Transparent encryption

For the user this means that all data saved in encrypted form (in encrypted directories or in encrypted drives) are automatically decrypted in the working memory as soon as they are called up for processing. If the data are then saved in this directory, then the same process occurs in reverse. This makes a remote access to these files impossible without SafeGuard LAN Crypt.Access to encrypted files.

Accessing encrypted files

If there is no key nor encryption rules for directory C:\1998, then the user of this key file cannot access the encrypted files in this directory. He cannot open, copy, move or rename, etc. the files.

Decrypting files

An explicit file decryption of the files is not necessary in SafeGuard LAN Crypt. In line with the concept of transparent encryption, all you need do is to copy or move the files from the encrypted directory into an unencrypted one (a directory for which there are no encryption rules in the current key file). The files are automatically decrypted.

If another user, with encryption regulations in his key file for the copied or moved file, accesses this directory, the file will be re-encrypted. You cannot open this file any more.

If you have encryption regulations in your key file for the directory into which you are copying or moving the file, the file is "recrypted" in line with the encryption rules for this directory.

Support and hotline

We are happy to support you in all matters regarding our products. Maintenance contracts are available which regulate support and updates as well as access to our mailbox. Our training seminars are available to all users. Please request our training schedule.

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

Normal use of the hotline is available without charge. But only call the hotline after having carefully consulted the manual and after extensive trial and error does not provide a solution for your problem. Prepare the following information before calling our hotline. You need:

- PC model and type, as well as features such as RAM and disk memory
- Operating system and its release status
- Name of the Utimaco products and its release status

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

Http://www.utimaco.com

Chapter 2

Installation

Contents:

- General
- System requirements
- Installation/update
- Installation from disk
- Installation from network from the PC
- Script-based installation

General

Before you install SafeGuard LAN Crypt, you should read and print out the file *README.TXT*. Place a printout in the manual. It may contain information and explanations that became available after the manual went to print.

The SafeGuard LAN Crypt installation packet consists of 4 disks. Installation disks 1-3 contain the SafeGuard LAN Crypt software. Disk 4 (key files) contains two key files (*default.tre*, *demo.tre*). To simplify the installation procedure various key files can be created and saved on this disk before the SafeGuard LAN Crypt software is passed on to the end user.

It is also possible to provide the end user with an "Unattended" setup (see also script-driven installation).

With the relevant password the individual users can access their key file.

The files *default.tre* and *demo.tre* should be deleted. At the very least the Security Administrator password should be changed! The Standard Security Administrator password is generally known. This then allows any user access to SafeGuard LAN Crypt administration functions.

System requirements

SafeGuard LAN Crypt operates on all IBM-compatible PCs and requires:

- Processor 80486 or higher.
- At least 32 MB RAM.
- 5 MB free hard disk memory for SafeGuard LAN Crypt 10 MB for the JAVA Virtual Machine.
- Graphics card with at least 256 colours.
- Operating system: Windows NT 4.0 with Service Pack 0, 1 or 3Service Pack 2 is not supported

Installation/update

If you already have a version of SafeGuard LAN Crypt installed on your system, but would like to install a new version, you must first completely deinstall SafeGuard LAN Crypt.

You require administrator rights to install or deinstall SafeGuard LAN Crypt .

If SafeGuard LAN Crypt finds an existing version on the hard disk of your computer after starting the installation program, a message appears informing you of this.

You are prompted to start the deinstallations. If you respond with **[OK]**, SafeGuard LAN Crypt is deinstalled. Then re-start the installation program.

Please note that files which are still encrypted at deinstallation are not automatically decrypted. This can result in it not being possible to reconstruct the files, as the relevant key is no longer available.We recommend decrypting all files before deinstallation in order to encrypt them later.

The installation program must always be booted on the PC on which you want to install SafeGuard LAN Crypt. It is not permitted to install SafeGuard LAN Crypt from PC A into a released directory on PC B.

Installation from disk

1. Insert Disk1 (Setup) in disk drive A: to install SafeGuard LAN Crypt on the hard disk.

2. Select **Run** from the Windows Start menu and enter A:\Setup in the text field. Then confirm with **[OK]**.

3. Welcome dialog of the SafeGuard LAN Crypt installation.

   Click on **[Cancel]** to exit the installation or **[Continue]** to install SafeGuard LAN Crypt.

4. Click on **[More]**

   The SafeGuard LAN Crypt Information dialog is opened. Additional information and explanations are displayed. Recent software changes which were included when the handbook went to press are documented here.

5. Click on **[More]**

6. The dialog **Select target path** is opened.

Icon bar

At the bottom of every SafeGuard LAN Crypt installation dialog you find an icon bar. It contains the button **[Back]**, **[More]** and **[Cancel]**.

[Back] returns you to the previous dialog

[More] takes you to the next dialog

[Cancel] ends the setup program without installing SafeGuard LAN Crypt.

Select the drive and directory where you want to install SafeGuard LAN Crypt.The default setting for the target folder is:

C:\SafeGuard\SGLC

Browse button

If you want to select a different directory, click on **[Browse]**. In the **Drives** box select the drive where you want to install SafeGuard LAN Crypt.

In the **Directories** window select a directory. Your selection appears on the text line **Path**.

7. Click **[OK]** and then on **[More]**.

The **Select directory** window is opened.

Common components

SafeGuard products uses common files which are copied into a directory. If you use various SafeGuard products, the common components are only installed once.

The **Select program folder** dialog is opened.

8. Confirm the default folder or select another folder. You can enter the name of the folder directly in the text line or select a folder using [Browse].

9. Click **[OK]** and then on **[More]**.

   The **Password echo characters** dialog is opened. Choose whether the password should be echoed when the password is entered (*).

10. Tag your selection and click **[More]**.

11. The **File size correction** dialog is opened.

    In this dialog you can select if and in what form a file size correction should be made.

SafeGuard LAN Crypt adds a 4 KB header to encrypted files, resulting in a change of the file size. But some programs only operate with original file sizes. SafeGuard LAN Crypt can correct the file size.

Following options are available:

- **File size correction in line with profiles**
  This is the recommended default setting. If you select this option, all files corresponding to the SafeGuard LAN Crypt profiles of the currently loaded key file are corrected (4 KB are subtracted).

This correction is implemented with all files which correspond to the profile and which are larger than 4 KB! Should the file not be encrypted, although this should not be the case according to the profile, incorrect size indications can be made in some cases.

- **Always implement file size correction**
  Recommended if problems in using specific applications occur with other settings.

SafeGuard LAN Crypt checks all files to see if a size correction is necessary. Here it is irrelevant if the corresponding key file is loaded.For making a size correction, every single file in your system must be opened. This is naturally very time-consuming and can impair system performance.

- **No file size correction**
  Recommended only for specific applications (e.g. backup of encrypted files). Can result in functional problems when using certain applications.

  SafeGuard LAN Crypt does not implement any file size correction.

12. Tag the option you require and click **[More]**.

If your computer has been instituted for more than one user, a further dialog appears at this point. Here you can enter for which users SafeGuard LAN Crypt should be automatically started immediately after the system start (open the logon dialog).

The following options are available:

- Start SafeGuard LAN Crypt
- For all users
- Only for current user
- Start automatically for current and all new users
- No automatic start

13. Tag the option you require and click **[More]**.

SafeGuard LAN Crypt again shows you the current settings. If you want to make changes, click **[Back]**.

If you now want to start the copy procedure, click **[More]**.

SafeGuard LAN Crypt now starts copying the files on your hard disk. Before the installation is com-

pleted, the **Select default key file** dialog is opened.

Here you can select which key file is displayed by default in the logon dialog. This is very useful if key files have already been defined on the local PC before the installation.

If the installation has been successfully competed, you are prompted to reboot your computer in order to use SafeGuard LAN Crypt.

14. Tag **Yes, reboot PC now** and click **[Exit]**.After restarting Windows and the correct Windows logon, the logon dialog appears. You can log on to SafeGuard LAN Crypt with the default.tre file or that key file entered in the Select default key file dialog.

    If you want to complete the SafeGuard LAN Crypt installation later, tag **No, reboot PC later** and click **[Exit]**.

You can only use SafeGuard LAN Crypt after rebooting your PC!

Installation from network to PC

If you do not install SafeGuard LAN Crypt from disk, but use software located on a server, proceed as follows:

For this the contents of the SafeGuard LAN Crypt Disk 1 must have been copied into a directory *Disk1*, the contents of Disk 2 into a directory *Disk2*, the contents of Disk 3 into a directory *Disk3* and the contents of Disk 4 into a directory *Keyfiles*.

1. Log onto the network and switch into the directory where SafeGuard LAN Crypt is located on the server.

2. Switch into the directory Disk1 and start the installation program with Setup.

   The SafeGuard LAN Crypt Welcome dialog appears.

3. Carefully read the information and click on **[More]**.

4. The SafeGuard LAN Crypt Information dialog is opened.

   More detailed information and explanations are shown. Recent changes to the program which

could not be incorporated when the handbook went into print are documented here.

5. Click **[More]**.

   The Select target path dialog is opened. Enter the drive where you want to install SafeGuard LAN Crypt.

   e.g. *C:\SafeGuard\SGLC*

Proceed as described in the section "Installation from disk".

Script-driven installation

The SafeGuard LAN Crypt installation can also be automated (unattended), so that no user intervention is necessary.

Call setup routine

To start the automatic installations, the setup program must be called with the following parameters:

-s	Indicates that no user entries should occur
-F1Script file	Indicates where the installation can locate the necessary script file. (Full path is necessary!)
-F2	Log file Indicates where the installation should generate the Log file. (Full path is necessary!)

Example: Setup -s -f1c:\setup\sglc.iss -f2c:\log\install.log

In this case the script-driven installation which uses the script file sglc.iss is used. This file is located in the folder *c:\setup*.

The installation creates an installation log *install.log* in the folder *c:\log*.

Installation script

The installation script is a file in which those data necessary for controlling the installation are saved.

On the first installation disk there is an example script called *SGLC.ISS*. Before making a script-based installation we recommend making a backup of this file. You should then adjust the example script to individual requirements.

The script is a normal text file in INI format. Thus there is a range of sections which are marked by square brackets. Most of the sections correspond to an entry mask in the user-driven installation.

(e.g. [SdSelectFolder-0] = Select Folder). Each section consists of several values in the form of "Value=X".

They should be adjusted to individual requirements by changing the following values:

1. Target path

Indicates the path on the target PC where SafeGuard LAN Crypt should be installed.

Section: [SdAskDestPath-0].

Value: szDir=required path

2. Folder

Indicates the folder where SafeGuard LAN Crypt programs should be stored.

Section: [SdSelectFolder-0]

Value: szFolder=name of required folder

3. Echo characters

Indicates on password entry whether there is an echo (*) or not.

Section: [AskOptions-0]

Value: Sel-0=1
Sel-1=0

If "*" is wanted as echo character for password entry, or

Value: Sel-0=0
Sel-1=1

If no echo character is wanted for password entry.

4. File size correction

Indicates how the file size should be corrected.

Section: [DlgAskOptionsEx-0]

Value: Option=0

If the file size should be corrected in line with profiles, or

Value: Option=1

If the file size should always be corrected, or

Value: Option=2

If the file size should not be corrected.

5. Automatic logon

Indicates the users for whom the logon program should be automatically started.

Section: [AskOptions-1]

Value: Sel-0=1
Sel-1=0
Sel-1=0
Sel-1=0

If the logon program should be automatically started for all users or

Value: Sel-0=0
Sel-1=1
Sel-1=0
Sel-1=0

If the logon program should be automatically started for the current user, or

Value: Sel-0=0
Sel-1=0
Sel-1=1
Sel-1=0

If the logon program should be automatically started for the current and all newly created users, or

Value: Sel-0=0
Sel-1=0
Sel-1=0
Sel-1=1

If the logon program should not be automatically started.

6. Standard key file

Indicates which key file the logon proposes as default.

Section: [DlgGetFileEx-0]

Value: File=key file (including complete path)

7. Reboot

Indicates if the PC should be rebooted after the installation, thus immediately activating SafeGuard LAN Crypt .

Section: [SdFinishReboot-0]

Value: BootOption=0

If no reboot should take place, or

Value: BootOption=3

If a reboot should take place.

Please note that only the values described in 1 to 7 may be changed as shown. Other changes in the script file cause the script-driven installation to function incorrectly.

Log file

The result of the script-driven installation is entered in the log file. Using the -f2 parameter it can be specified when calling Setup.exe.

Possible entries:

0	No error
1	General error
2	Illegal mode
3	Data required not found in Setup.iss
4	Insufficient memory
5	File does not exist
6	Script file cannot be generated
7	Log file cannot be written
8	Illegal path for script file
9	List type invalid (internal error)
10	Data type invalid (internal error)
11	Unknown error at installation
12	Dialog order not valid
51	Folder cannot be created
52	No access to file or folder
53	Invalid option selected.

Chapter 3

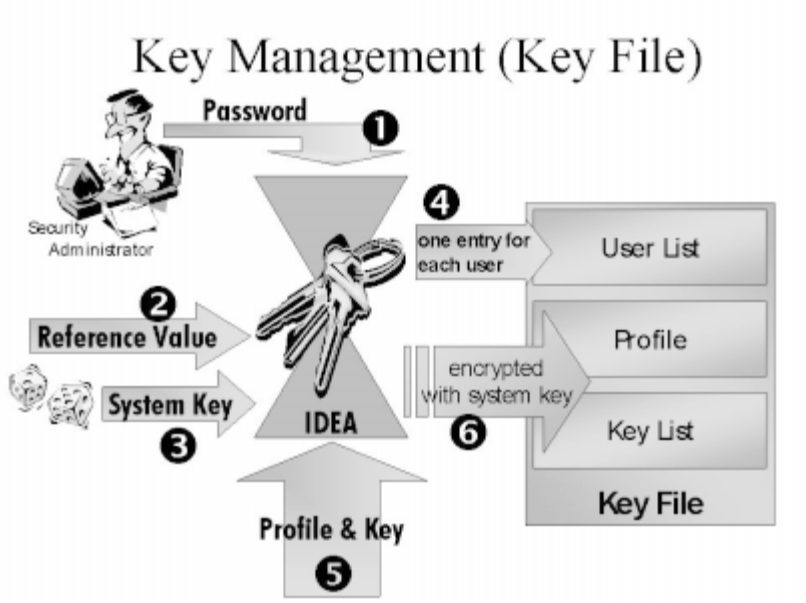
Key Management

Contents:

- Structure of the key file
- The file header

Structure of the key file

The illustration below represents an overview of the key management used in SafeGuard LAN Crypt. For detailled explanations refer to the following pages.



In SafeGuard LAN Crypt neither security administrator nor user passwords are saved in the key file or in the data files to be encrypted.

To verify correct logon to SafeGuard LAN Crypt, the following procedure is used.

1. When creating a new key file an administrator password for this key file is entered by the SafeGuard LAN Crypt security administrator .

2. Using this password the "Reference Value" 2, specific to SafeGuard LAN Crypt, is encrypted with the "IDEA" algorithm. The result of this encryption is saved in the SafeGuard LAN Crypt key file.

3. For each key file the "System Key" 3 is generated uniquely using a a random generator and also encrypted with the relevant password.

4. For each user of a SafeGuard LAN Crypt an entry with the code generated under 1 and 2 and the system key encrypted with the password is saved in the key file 3.

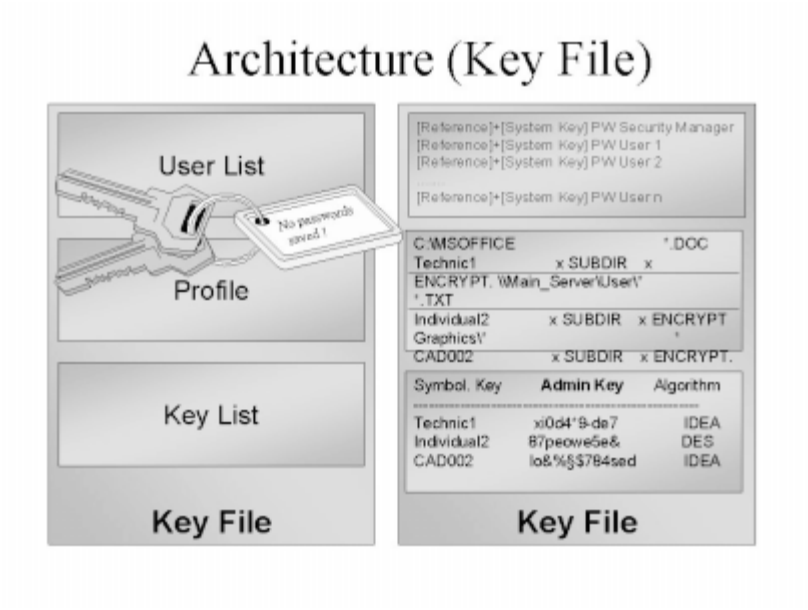
5. The profiles and keys set by the security administrator of the key file are also encrypted using the system key described under 3 and saved in the key file as shown in item 6. The procedure described above is also used when creating user passwords.

The advantage of this method is that profile and key need only appear once in a key file, as every user can access the system key using his password.

The SafeGuard LAN Crypt logon functions as follows (irrespective of whether you log on as user or Security Administrator). SafeGuard LAN Crypt encrypts the above reference value using the password entered and then checks if the result saved in the key file is identical to the result of the current encryption. Only if both values are identical is logon possible. Otherwise the message "Wrong password" appears.

The “IDEA” algorithm is used for all encryption affecting the key file and the SafeGuard LAN Crypt file headers.

The structure of the SafeGuard LAN Crypt key file is shown in the diagram below.



The file header

Every file encrypted with SafeGuard LAN Crypt receives an approx. 4 KB file header. This file header contains the random key generated for the respective file in encrypted form.The random key is encrypted with the key specified in the Administration mask and thus can be calculated only after a correct logon by SafeGuard LAN Crypt.

If a file encrypted with SafeGuard LAN Crypt is opened on a PC where SafeGuard LAN Crypt is not installed, the user can see from the file header that the file is encrypted and that it is not damaged. The file header contains the following entry:

SafeGuard LAN Crypt
Copyright (C) 1998 Utimaco Safeware AG

ENCRYPTED FILE

The name of the key used (e.g. "DOCUMENTS") is then shown in plain text.

The actual document is displayed in encrypted form.

Chapter 4

User Functions

Contents:

- SafeGuard LAN Crypt User menu
- Logon to SafeGuard LAN Crypt
- Change user password
- Switch key file
- Encryption dialog
- Initial encryption
- Decrypt files
- Delete files
- Rename directories
- Status in Windows NT Explorer
- Exit SafeGuard LAN Crypt

SafeGuard LAN Crypt User Menu

At installation, the program containing the logon/log-off and the user menu (LcLogn.exe) is entered in the registration database. This results in the logon being activated at every Windows NT user logon. At the same time an icon has been integrated in the Windows task bar which shows a red traffic light before a valid logon.

If you remove this entry from the registration database or if the option "no automatic start" was selected during installation, you must start the SafeGuard LAN Crypt logon manually.

If you are logged on to a key file, and thus have access to your encrypted data, the SafeGuard LAN Crypt "traffic light" icon in the Windows task bar shifts from red to green.

The User menu offers the user the option of enabling or disabling the transparent encryption, of starting the Administration program and of calling up various information on SafeGuard LAN Crypt.

If SafeGuard LAN Crypt Administration is started by a user logged on to a key file without administration rights, the encryption dialog is presented.

Open Open the SafeGuard LAN Crypt User menu by right clicking with the mouse on the SafeGuard icon in the Windows task bar.

Start Start the SafeGuard LAN Crypt Administration with the command **Start Administration** from the User menu or by double clicking the icon in the Windows task bar.

Menu items in the User menu

About SafeGuard LAN Crypt

Displays information on your SafeGuard LAN Crypt software version and copyright information.

Logon

Allows you to log on to another key file or allows you a new logon once you have logged off from SafeGuard LAN Crypt.

Logoff

With this command you can log off the from the currently active key file. Use this SafeGuard LAN Crypt security function if you leave your workplace and the computer is not shut down.

If you do not log off from your key file, the transparent encryption/decryption is active and an unauthorised user can easily access the encrypted data on your computer.

If you are logged off from your key file, you cannot access your encrypted data

Encryption on

This command switches encryption on or off. This function is important if you want, for example to copy encrypted files.

If an encrypted file is copied/moved with enabled transparent encryption to a place where there are no encryption rules, it is automatically decrypted. If transparent encryption/decryption is disabled, the file can be copied/moved to any place in encrypted state.

With this function encrypted files can also be sent (e.g. e-mail or on disk) without their being decrypted.When encryption is disabled the SafeGuard LAN Crypt icon in the Windows task bar shows a yellow "traffic light" icon.

This SafeGuard LAN Crypt behaviour is a control of the restricted access control (no profile link!). On a file access with disabled encryption, a check is made whether the relevant key is in the key file. The files need not correspond to the profiles of the key file to be manipulated (copied, moved, etc.).

When automatic encryption/decryption is disabled, encryption can be done using the Explorer extension or the Administration program.

Info on current key file

Displays information on active key file.

Start Administration

Starts SafeGuard LAN Crypt Administration in line with the rights of the active key file where the logon has been made.

Exit

Exits the SafeGuard LAN Crypt application. The SafeGuard LAN Crypt icon is removed from the Windows task bar. To access the User menu again you need to restart SafeGuard LAN Crypt.

Logon to SafeGuard LAN Crypt

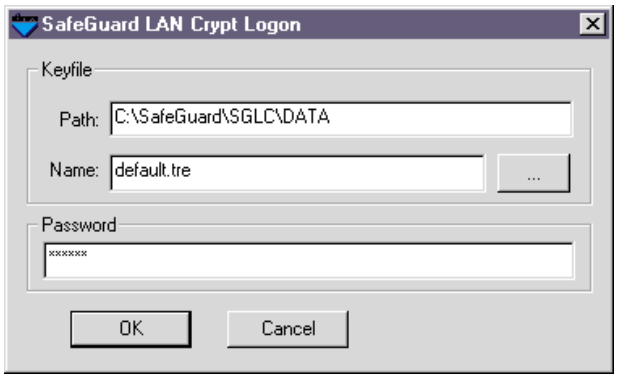
If the automatic start of SafeGuard LAN Crypt was chosen at installation for all users, you can start immediately at 3.

If SafeGuard LAN Crypt was installed with the option "No automatic start", proceed as follows.

1. Click on the **Start** button in the Windows task bar.

2. Select the SafeGuard LAN Crypt folder (or the one in which you entered at installation) and click **SafeGuard LAN Crypt logon**.

   The **SafeGuard LAN Crypt logon** dialog is opened.



3. In the key file section, enter the **Path and Name** of the key file you want to open or click on the File selection switch to the right of the **Name** text field.You can now select a key file from the list. Tag the relevant key file and select **[Open]**. The name of the key file appears in the text field Key file.

4. Now enter your password for the key file in the **Password** text field.

   The entry is not displayed or represented by (*) on the screen. Click **[OK]**. The logon to SafeGuard LAN Crypt is implemented. The SafeGuard LAN Crypt icon appears as a green "traffic light" in the Windows task bar.

If you position the mouse pointer above the SafeGuard LAN Crypt icon in the Windows task bar, the name of the active key file is shown.

In order to activate the automatic logon at a later point, you can create a link to the SafeGuard LAN Crypt logon.
SafeGuard LAN Crypt is started with the program file "C:\SafeGuard\SGLC\BIN\LCLOGN.EXE".

Change user password

If you are logged on as user to a SafeGuard LAN Crypt key file, you can change your user password.

Open the SafeGuard LAN Crypt user menu by clikking with the right mouse key on the icon in the Windows task bar and selecting **Start Administration**.

The **SafeGuard LAN Crypt encryption** dialog is opened.

1. Click **Password** and then on **Other user password**. The **Other password** dialog box is opened.
2. Enter the password you want to change in the **Old password** text line.
3. Enter your new password in the text line Password. The password does not appear on the screen!
4. To avoid errors and typos, you must re-enter the password in the **Repeat** text field.
5. Confirm with **[OK]**.

You change the user password in this way. The key file to which you logged on with the old password remains active. The next time log on with the new password.

A double click on the SafeGuard LAN Crypt icon in the Windows task bar opens the encryption dialog.

Switch key file

SafeGuard LAN Crypt can only manage one key file. This means that it is not possible for several key files to be open at the same time.

If you have passwords for several key files, you can however change the key files.

Tip

If you use several key files, you should contact your security administrator to combine all the keys you need in one key file.

You can confirm to which key file you are currently logged on by placing the mouse pointer on the SafeGuard LAN Crypt icon in the Windows task bar.

Key file info

To change the key file, you need not log off from the active key file. All you need do is to log on to a new key file for which you have a password.

To do this select **Logon** from the SafeGuard LAN Crypt User menu. The selected key file becomes active immediately and encrypts/decrypts your data.

Encryption dialog

Encryption of files and directories

In line with the concept of transparent encryption, SafeGuard LAN Crypt directories and files are encrypted as per the encryption profiles as soon as they are opened.

Transparent encryption is started as soon as you log on to a key file.

Tip

Nevertheless, we recommend first encrypting all files which correspond to the profile entries before starting work with SafeGuard LAN Crypt.Files which are not opened while the user is logged on to a key file remain unencrypted, even though they should be encrypted according to the profile entries.

In spite of using SafeGuard LAN Crypt it is thus possible for unauthorised users to manipulate or delete your files.

To avoid this security risk, you should initially encrypt your files in the SafeGuard LAN Crypt

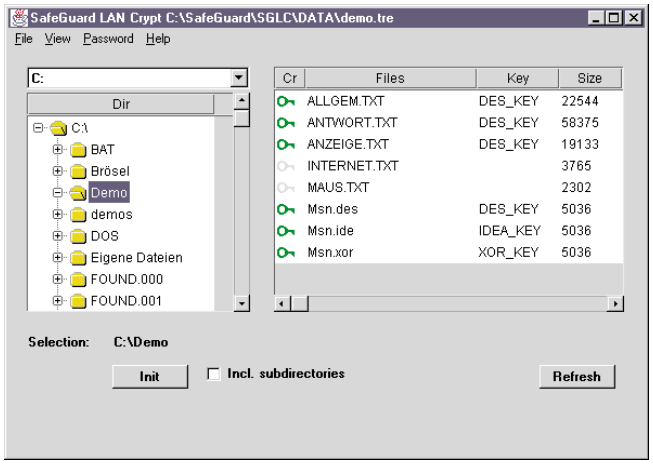
With the SafeGuard LAN Crypt encryption you can explicitly encrypt individual files or directories or even entire drives.

Example If you tag drive C: in the SafeGuard LAN Crypt encryption dialog, select the **With subdirectories** option and then click on **[Init.]**, all the files in this drive for which there are encryption rules in your key file are encrypted. For example, all files with the file extension "txt" (encryption rules=*C:*.txt*).

Which data are encrypted depends on the encryption rules defined in your key file. You can only encrypt files for which there are encryption rules in your key file. All other data remains unencrypted.

You have no access to encrypted data for which there are no encryption rules in your key file.

To encrypt your data, you must switch into the SafeGuard LAN Crypt encryption dialog.



If a key Mydir_key with the profile *C:\Mydir *.** has been defined in the Administrator dialog, then all files in this directory are encrypted with the key Mydir_key when you click the **[Init]** button.

You can only define keys and encryption rules if you are logged on to a key file with a security administrator password.

As soon as you save encrypted files on servers or in a "cached" directory, they can be accessed by other computers when SafeGuard LAN Crypt is not active. The file remains encrypted, so that its contents cannot be read. However, it can be manipulated. This can result in data being destroyed.

Encryption status

In the SafeGuard LAN Crypt encryption dialog you can see the encryption status of the files at all times.

The file list displays the current encryption status of the files.

- Column **E**
  shows in the form of a key if the file is currently encrypted.

Green key The file is encrypted in line with the profile entry.

Red key The file is encrypted with a key which is not in one's own key file.

Grey key The file is not encrypted although it should be encrypted according to the profile entry.

Very rarely the encryption status cannot be detected as the relevant files locked due to a system process. In this case, a red question mark precedes the file.

- Column **File:**
  contains the file and directory names.

- Column **Key:**
  displays which key was used to encrypt the file.

- Column **Size:**
  displays the file size.

Initial encryption

Open the encryption dialog by double clicking on the SafeGuard LAN Crypt icon in the Windows task bar.

1. Select one file or a complete directory using the Drive selection of the Directory display or the File list.

2. Tag the drive/directory/file you want.

   If you tag only one file, encryption relates only to this file.

   If you tag a complete directory, encryption relates to the complete directory.

Note the **Selection** text line. Here you can see which directory or which individual file the action **Init** would relate to.

3. Using the **[Subdir]** switch, check if the encryption should include all subdirectories

   If the switch is tagged with a tick, all the subdirectories are included in the encryption, if these are to be encrypted according to the encryption rules.

4. Click the **[Init]** button.

SafeGuard LAN Crypt encrypts the files in line with the encryption rules defined in your key file.

Decrypt files

No explicit file decryption is necessary in SafeGuard LAN Crypt.

To decrypt your data you must move or copy the relevant files from the encrypted directory into a directory for which no encryption rules have been defined.

The files are automatically decrypted.

If another user whose key files contain encryption rules for the copied or moved file accesses this directory, the file is reencrypted. You can no longer open this file.

If your key file contains encryption rules for the directory into which you are copying or moving the file, the file is "recrypted" in line with the encryption rules for this directory.

Delete file

If you are logged on the relevant key file, you can delete SafeGuard LAN Crypt encrypted files as any other file.

Note

At deletion, files are placed in the Windows NT recycle bin. Files encrypted with SafeGuard LAN Crypt remain fully encrypted.

As "normal" deletion (File/Delete or [DEL]) of directories moves the entire directory (cf. rename and move directories) into the Windows NT recycle bin, this type of deletion (putting into the recycle bin) is not possible for entire directories. The contents of the directory must first be deleted and then the directory deleted. There are no restrictions on final deletion [SHIFT+DEL]. Empty directories can be renamed or moved without restriction.

Rename directories

If SafeGuard LAN Crypt is installed on your system renaming and moving directories which are not empty is only possible by creating a new

Example The directory *C:\Data* should be renamed to *C:\Data_1*.

1. Create a new directoryC:\Data_1.
2. Copy all files from C:\Data toC:\Data_1.
3. Delete from C:\Data.

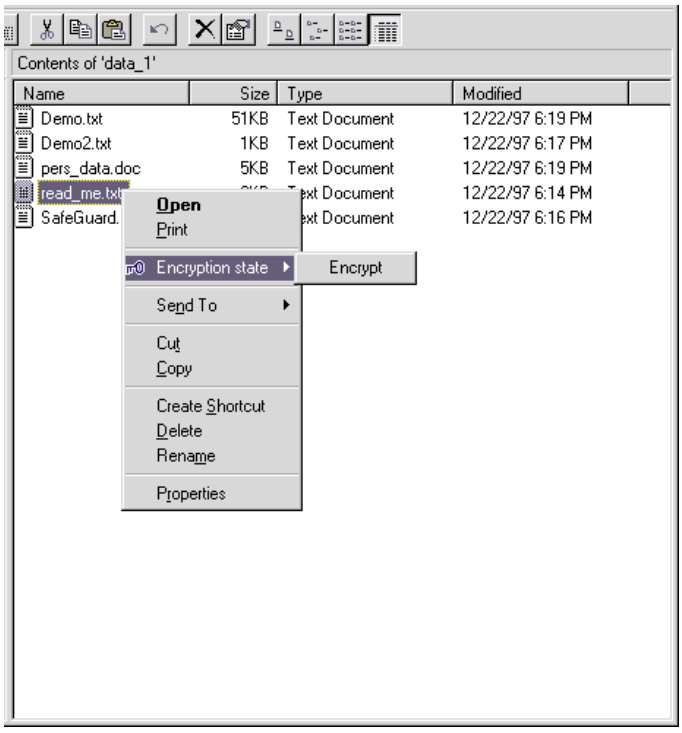
With directory structures this is the only way to ensure that all files are always correctly encrypted.

As "normal" deletion (File/Delete or [DEL]) of directories moves the entire directory (cf. rename and move directories) into the Windows NT recycle bin, this type of deletion (putting into the recycle bin) is not possible for entire directories. The contents of the directory must first be deleted and then the directory deleted. There are no restrictions on final deletion [SHIFT+DEL]. Empty directories can be renamed or moved without restriction.

Status display in Windows NT Explorer

You can monitor the encryption status of your files at all times.

If you right click on a file in Explorer with the mouse, a context menu appears with the menu item **Encryption status**.



Greenkey If this menu item is tagged with a grey key, this file has been encrypted by SafeGuard LAN Crypt. However, you can still open it. You are thus logged on to a key file which has encryption rules for the relevant file.

Red key However, if this file is tagged with a red key, you have no access to this file.

This can be because you have logged off from your key file (red SafeGuard LAN Crypt icon in the task bar). If this is not the case, your key file does not contain any encryption rules granting you access to this file. You cannot open the file.

Greykey The grey key means that this file should actually be encrypted according to the encryption rules, but is not. This can occur when you log off from SafeGuard LAN Crypt and then copy a file into a encrypted directory. Even if encryption is disabled, a grey key can precede many files.

Encrypt file In this case move the mouse pointer over the menu entry **Encryption status**. A fly out menu appears.

Click on **Encrypt**. (You must be logged on to a key file.) The file will be encrypted in line with the encryption rules.

You obtain additional information if you click on Properties in the context menu. The **LAN Crypt Info** tab informs you which files you can access.

Exit SafeGuard LAN Crypt

Generally it is not necessary to close SafeGuard LAN Crypt purposely. The program is automatically closed when shutting down the computer.

However, with LAN Crypt you can temporarily log off from a key file during a session or even exit the program completely.

In both cases you have no access to your encrypted data!

The temporary logoff from a SafeGuard LAN Crypt key file can be used to protect your computer against unauthorised access while you leave your work place.

If you did not log off from your key file in this case, any unauthorised user could access your data.

Logoff

To log off from the active key file, select **Logoff** from the SafeGuard LAN Crypt User menu.

The SafeGuard LAN Crypt icon in the Windows task bar shows red traffic lights. This means that you cannot access any encrypted data. Log on again to a key file by using the **Logon** command from the SafeGuard LAN Crypt User menu.

Exit

To exit the program, select **Exit** from the SafeGuard LAN Crypt User menu. The icon in the Windows task bar no longer appears.

You can no longer access encrypted data. If you again want to log on to a key file, select **Logon** in the SafeGuard LAN Crypt folder.

Chapter 5

Administration

Contents:

- SafeGuard LAN Crypt user menu
- SafeGuard LAN Crypt key file
- First steps in SafeGuard LAN Crypt
- Change security administrator password
- Administration dialog
- Create/switch a key file
- Generate/import key
- Encryption rules/hierarchy
- Edit/define entries
- Passwords
- The specimen file *demo.tre*

In SafeGuard LAN Crypt the administrator function is of central importance.

Only in administrator mode is it possible to:

- create a new key file
- generate a new key
- specify encryption rules
- issue passwords for key files.

As SafeGuard LAN Crypt security administrator you can define different file accesses for individual users of SafeGuard LAN Crypt.

For example, an employee in the Accounting Department can receive access to both personnel and accounting data, while an employee in the Personnel Department only has access to personnel data.

Equal access rights are realised by, for example, allocating different users passwords for the same key file.

By defining specific profiles, it is possible to deliberately specify overlaps of access rights. This is done, for example, by saving a specific key with the corresponding profile (path for encryption) in the key file which otherwise contains different access rights.

Before you start the definition of the key files, you should first determine:

- Which drives/directories/files should be encrypted?
- Who should have access to which encrypted data? (passwords)
- Which data should the individual user be able to access? (rights profile)

SafeGuard LAN Crypt User menu

The program containing the logon/logoff and the user menu (LcLogn.exe) is entered into the registration database at installation. This results in the logon being activated at each user logon. At the same time an icon is integrated into the Windows task bar showing a red traffic light before a valid logon.

If you remove this entry from the registration database or select the option "no automatic start" during installation, you must start the SafeGuard LAN Crypt logon manually.

If you have logged on to a key file and thus obtained access to your encrypted data, the “traffic lights” icon placed by SafeGuard LAN Crypt in the Windows task bar changes from red to green.

With the user menu, the user can toggle the transparent encryption, start the administration program and call up information on SafeGuard LAN Crypt.

The SafeGuard LAN Crypt Administration program comprises an encryption and an administration dialog.

If the SafeGuard LAN Crypt Administration is started by a user logged on to the key file with the Security Administrator password, the Administration dialog is opened.

In this dialog the security administrator can generate

- **new key files,**
- **keys and**
- **encryption rules**

and issue/modify the necessary

- **passwords**

If you are logged on to a key file with the user password, you have no access to the SafeGuard LAN Crypt Administration dialog.

SafeGuard LAN Crypt key file

In the SafeGuard LAN Crypt key file, the keys and the encryption rules defining the user access rights are saved.

The SafeGuard LAN Crypt key file automatically receives the file extension .tre (e.g. *default.tre*).

You can save a key file in any directory.

There is a dialog field for easy selection and saving of keys. You can open it by clicking the button next to the relevant text field for the file name.

To create a key file for a user, the following steps are necessary:

1. Generate new empty key file.
2. Generate / import the key for the new key file.
3. Define the profile entries for the new key file.
4. Add a password for the user.

First steps: default.tre

SafeGuard LAN Crypt is supplied with a key file called *default.tre*. This key file is assigned to the Security Administrator password system. Note how the password is written!

The key file default.tre is completely empty except for the administrator password. It is necessary to allow initial logon to a key file after the SafeGuard LAN Crypt installation.

The first time you log on to SafeGuard LAN Crypt select the file default.tre and log on to this key file with the Security Administrator password.

As soon as you are logged on to the *default.tre* file, you can create new key files. The *default.tre* file is no longer necessary.

You can leave it on your system (to use it, for example, as standard key file), you can rename it and use it as user key file or you can delete it.

If you decide to leave the key file *default.tre* on your system, you should change the security administrator password!

Ensure that you always have a key file available which you can use to log on to SafeGuard LAN Crypt with its security administrator password.

If you create a key file, the first thing you must do is to enter the security administrator password. This ensures that it is impossible to create a key file without a security administrator password.

Once you have logged on to a key file with the security administrator password, you can create new key files and modify existing ones.

After starting SafeGuard LAN Crypt Administration, you can edit key files. You can do this by switching the key file. This means that it is not essential to be logged on to a key file to edit it.
When you close the administration dialog, you are still logged on to the key file that was active when starting the Administration.

To edit the key files use only the SafeGuard LAN Crypt Administration. If you open a key file with another application, an editor for example, and then save it, it can no longer be used by SafeGuard LAN Crypt.

However, renaming key files does not impair SafeGuard LAN Crypt functionality.

Change security administrator password

With the security administrator password, you can access every key file generated using this password. To ensure the highest level of security, this password must be kept confidential.

After you have logged on to SafeGuard LAN Crypt for the first time using the key file default.tre, and you want to keep this file, you must change the security administrator password.

Anyone who can log on to a key file with a security administrator password can generate any number of key files.

Requirement If you want to change the security administrator password of a key file, you must be logged on to a key file with the security administrator password.

1. Start the SafeGuard LAN Crypt Administration by double clicking the SafeGuard LAN Crypt icon in the Windows task bar.

   The dialog **Open key file** appears.

2. Select the key file whose security administrator password you want to change and enter the relevant security administrator password. The Administration dialog is opened.

3. From the **Password** menu, select **Other admin password**.

   The dialog field **Other administrator password** appears.

4. In the **Old password** text line enter the security administrator password you want to change. Enter your new security administrator password in the text line password. The password is not displayed on the screen! To avoid errors and typos, you must re-enter your password in the text line **Repeat**.

5. Confirm with **[OK]**.

6. Save the key file with the new password using **Save** in the menu **File**.

   If you want to save the key file under a new name, select **Save as** . You can now edit the key file saved with **Save as** in the Administration dialog (path and file name appear in the key file text field).

   When you exit SafeGuard LAN Crypt Administration, the key file to which you logged on before starting the Administration remains active.

7. Exit SafeGuard LAN Crypt and log on with the new security administrator password.

Delegate security administrator rights

It is possible to allocate groups of key files different security administrator passwords, thus delegating the right of creating and changing key files.

In this case please note that you can only define keys and edit profile entries when you are logged on to the key file with the security administrator password.

With a normal password you can only access the SafeGuard LAN Crypt encryption dialog.

To ensure the highest level of security, the security administrator password must be kept confidential!

Administration dialog

The SafeGuard LAN Crypt Administration dialog supports the administration and editing of SafeGuard LAN Crypt key files. The SafeGuard LAN Crypt key files contain

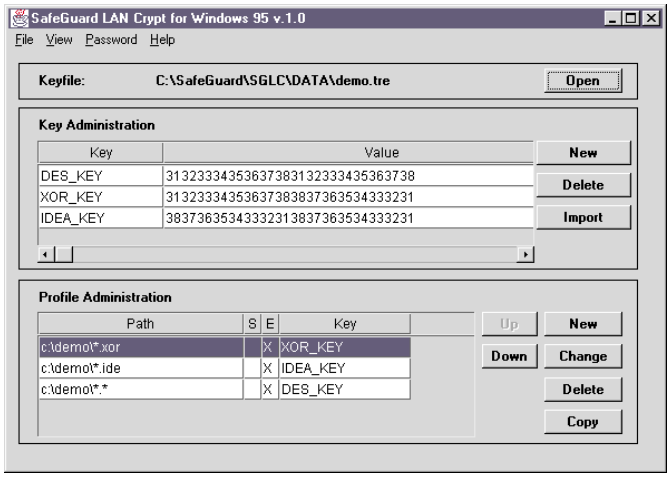
- a code for the security administrator password
- a code for the user password(s)
- the SafeGuard LAN Crypt keys and
- the SafeGuard LAN Crypt encryption rules.

The SafeGuard LAN Crypt encryption rules are profile entries, describing user access rights to specific files.

When you start the SafeGuard LAN Crypt Administration and are logged on to a key file with the security administrator password, the Administration dialog is opened.

If you are logged on as user to a key file, you have no access to the Administration dialog.

When you start the SafeGuard LAN Crypt Administration, the encryption dialog is opened.



The Administration dialog consists of three different areas with different functions:

- Key file
- Key administration
- Encryption rules

Key file

In the **Key file** section the name and path of the currently edited key file are displayed. These need not be the currently active key file!

With the **Open** button you can load another key file for editing.

Not that when you exit SafeGuard LAN Crypt Administration, the key file to which you have logged on before starting the administration remains active.

Key administration

The sections **Key administration** supporting the generation and import of SafeGuard LAN Crypt keys. All keys saved in the key file are listed in the table.

Encryption rules

In the sections **encryption rules** you can specify which data are to be encrypted. All encryption rules you create are displayed in the table.

Create a key file

To create a new key file you must be logged on to a SafeGuard LAN Crypt key file with the Security Administrator password.

1. Log on to any SafeGuard LAN Crypt key file with a security administrator password.

2. Start the SafeGuard LAN Crypt Administration by double clicking on the SafeGuard LAN Crypt icon in the Windows task bar.

   For security reasons, a user who starts the SafeGuard LAN Crypt Administration with administrator rights must re-enter the security administrator password.

3. In the dialog **Open key file** enter the security administrator password. The Administration dialog is opened.

4. Select **New** in the **File** menu. The dialog window **New key file** is opened. In the **File name** text field enter a name with the file extension .tre ein and click **Save**.

   The dialog field **New key file** is opened.

5. In the **Password** text field enter the security administrator password for the new key files. To avoid typos you must re-enter the new security administrator password in the **Repeat** text field. Click **[OK]**. With **[Cancel]** you exit the dialog field without a new key file being generated.

   The new, empty key file is created.Name and path of the key file appear in the Key file text field.

6. Save the new key file using **Save** from the Menu file. If you have opened and edited a new key file, but have not saved it, a message appears informing you of this when you log off from SafeGuard LAN Crypt. You are prompted to save the changes.

Changes in a key file only become active after they have been saved and you log on again to this key file.

Once you have created a new key file you can start adding the SafeGuard LAN Crypt key.

Switch key file

When you are logged on to SafeGuard LAN Crypt as security administrator, you can edit the different key files in the Administration dialog.To switch the key file it is not necessary to log off and then log on again, as was the case with the user function.

1. Click **[Open]** in the Key file section of the Administration dialog. The window **Open key file** appears.

2. Enter the Path and Name of the key file you want to open or click the file selection switch and select a key file.

3. Enter the security administrator password for the selected key file in the Password text line.

   The password does not appear on the screen.

4. Click **[OK]**.

   The selected key file is displayed in the **Key file** section of the Administration dialog.

When you have made the changes, save the key file using **Save** from the menu **File**.

Generate new key

A SafeGuard LAN Crypt key comprises three components:

- **A name which can be selected as required**

To ensure a good overview, we recommend using the name of the owner or the owner group.

- **A specific value**

The minimum length of the value is 16 characters. The maximum length is 32 characters. If you enter a shorter value, this will automatically be filled to reach the minimum length of 16 characters.

- **An encryption algorithm (XOR; DES; IDEA)**

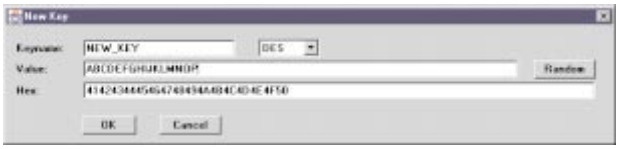
To create a new key you must have logged on to the SafeGuard LAN Crypt key file with the security administrator password.

1. Log on to the SafeGuard LAN Crypt key file with the security administrator password .

2. Switch with the command **Administration** from the **View** menu in the SafeGuard LAN Crypt Administration dialog.

3. In the Key Administration section, click on the **[New]** button.

   The **New key** window is opened.



4. In the **Name** text field enter the name for new key. In the drop down menu select an Algorithm (XOR; DES; IDEA) .

5. In the text field **Value** or **Hex** (hexadecimal) enter a character string. Depending on the column in which you enter the new value, SafeGuard LAN Crypt supplements the other value automatically.

   You can click on the **[Random]** button to have SafeGuard LAN Crypt enter a value for the key. Confirm with **[OK]**.

The new key is displayed in the table in the key administration dialog.

6. Save the key file.

You can add keys by repeating the procedure.

You can remove the key by tagging it and clicking on **[Delete]**.

You can save the new keys using **Save** from the **File** menu in the current SafeGuard LAN Crypt key file, or create a new key file with **Save as**.

The keys appear in the Administration dialog. Here you can define profiles for the initial encryption.

Import key

With the Import function you can add keys to a key file.

You can add the key of any other key file to the active key file.

Keys can be imported with the security administrator- or the user password.

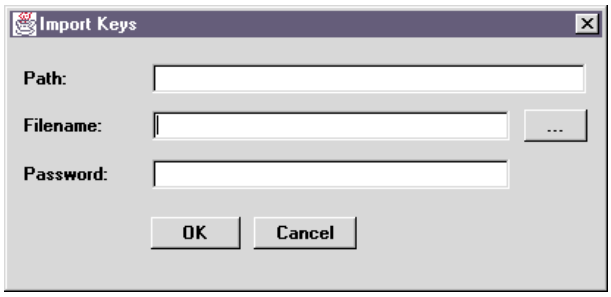
When you import keys with the user password, thier values are not displayed in the Administration dialog. If the key is imported with the security administrator password, only those key values are displayed which are also visible in the file from which they are imported.

This function is helpful if you want to grant user B the same access rights as user A. In this case all you need do is to import the key from user A's key file and save it in user B's key file.Of course the corresponding encryption rules to the keys must be defined in both key files.

If you want to import keys:

1. Click the **[Import]** button in the SafeGuard LAN Crypt Administration dialog.

   The dialog window **Import key** appears.



2. Enter the Path and File name of the key file whose key you want to import or click the file selection switch and select a key file.

3. Enter the security administrator password or a user password for the selected key file.

4. Confirm with **[OK]**.

   The keys are imported and displayed in the key table in the Administration dialog.

5. Save the changed key file.

Encryption rules

To have a file encrypted or decrypted by SafeGuard LAN Crypt, encryption rules are necessary. Encryption rules are profiles which specify precisely which file(s) should be encrypted under which path and with which key.

Files for which no encryption rules have been defined, cannot be encrypted.

For this reason these encryption rules must be defined in the SafeGuard LAN Crypt administration dialog. These profiles make it possible to allocate users different access rights.

A user without a profile entry for encrypted files in directory X cannot access these data.

The encryption rules in a key file are displayed in the profile table in the Encryption Rules section in the Administration dialog.

Hierarchy of encryption rules

SafeGuard LAN Crypt treats the profile entries in order (downwards) in the encryption rules list. In this way you can even exclude individual files or file groups from encryption.

To do so you must define encryption rules which exclude the relevant files from encryption. You do so in the **New encryption rules** dialog field. Here you deactivate the check box **Encryption** which is enabled by default.

Observe the hierarchy! An exclusion rule must precede the encryption rules. Once a directory as a whole has been encrypted, exclusions have no impact. This also applies to the rules which state that specific file groups (or subdirectories) are to be encrypted using a different key.

Example

In this example all files with the .TXT extension are excluded from encryption.

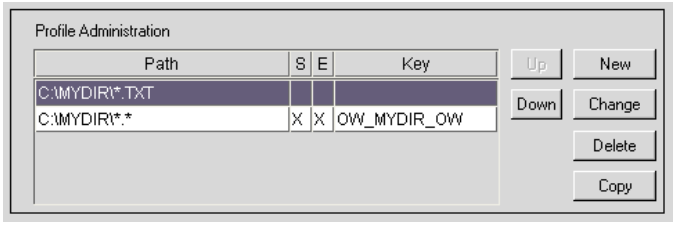
The encryption rules which define that all files with the .txt extension are excluded from encryption precede the encryption rules which define encryption.

- **First:**
  Entry C:\MYDIR*.TXT(no encryption, no key!) excludes all files with the TXT extension.

- **Second:**
  Entry C:\MYDIR*.Encrypts the directory MYDIR including all the subdirectories with the key OW_MYDIRKEY_OW.

Edit entries

The buttons **[Up]**, **[Down]**, **[Copy]**, **[Delete]** are tools for creating encryption rules.



Up — With the **[Up]** button you move encryption rules up one line.

Down — With the **[Down]** button you move encryption rules down one line.

Copy — The **[Copy]** simplifies defining encryption rules.

It can be used if you want to encrypted all the files in a directory, but want to use different keys to do so.In this case you need only create one entry, copy it and make the relevant changes (e.g. file extension or key).

If you want to copy an entry, tag it in the profile table and click **[Copy]**. The dialog **Copy encryption rules** appears. You can change the copied entry in this dialog.

If you then click on **[OK]**, the entry is appended to the end of the profile table.

If you make a change, for example, the file extension .xls to .txt, define a new entry for the key file, without having to re-enter the whole path again.

With the **[Delete]** button you can remove a profile entry from the profile table.

Tag the relevant line and click **[Delete]**. The entry is removed from the profile table.

Once you have defined key and profile entries, you must add a user password to the key file. This allows the user to log on to the SafeGuard LAN Crypt key file.

Define encryption rules

To define encryption rules you must be in the SafeGuard LAN Crypt Administration dialog.

1. Click the **[New]** button in the Encryption rules. Section. The New encryption rules window opens.

2. In the text field **Path** enter the path of the file(s) / directories you want to encrypt or click the file selection switch and select the files or directories you want to encrypt there.You can use the joker (*) and wildcard (?) in the path entry. The drive entry is optional. However, if it is not entered, the path of the profile entry applies to all available drives.

3. Select a key from the pull-down menu. All available keys in the active key file are listed.

4. Activate the switch [With subdirectories], if you want to include all subdirectories in the encryption (tick = enabled).

   The switch **[Encrypt]** is enabled by default. If you deactivate it, the files entered in **Path** are not encrypted. This is relevant, if you want to exclude specific files from encryption . (Hierarchy of the profile entries)

5. Click **[OK]**.

   The new encryption rules appear in the profile table in the **Encryption rules** section of the Administration dialog.

6. Save the new profile entry using **Save** in the relevant key file.

   In the profile table in the **Encryption rules** section of the Administration dialog all the encryption rules in the opened key file are displayed.

Column Path The **Path** column specifies a file or a file mask.

Column S The **S** column shows if the **Encrypt subdirectories** option applies for this profile entry.

Column E The **E** column shows if Encryption is enabled.

ColumnKey The **Key** column specifies the key used. No key means no encryption.

Passwords

Issuing passwords is a fundamental security function of SafeGuard LAN Crypt.

A password allows you to open a key file and thus to log on to the SafeGuard LAN Crypt application.

Several passwords can be assigned for one key file. This means that several users can use a key file with the same access rights.

To allocate a password to a key file, switch into the SafeGuard LAN Crypt Administration dialog (only possible if you are logged on to SafeGuard LAN Crypt with security administrator rights).

Add user password to key file

To add a user password you must be logged on to the SafeGuard LAN Crypt key file with the security administrator password.

1. With Administration switch from the View menu into the SafeGuard LAN Crypt Administration dialog.

2. Select the **Password** menu.

3. Click **[New password]**.

The dialog window **New password** opens.

4. Enter the new password.

   The password does not appear on the screen. In order to avoid errors and typos, you must re-enter the password in the Repeat text field.

5. Click **[OK]**.

6. Save the key file with the new password using Save from the File menu. If you want to save the key file under another name, select Save as.

You can issue several different passwords for a key file.

Changes only become active after being saved and after a new log on.

Delete a user password

If a user password is no longer needed, or if a user should no longer be able to access specific data, you can delete the user password.

1. With Administration switch from the **View** menu in the SafeGuard LAN Crypt Administration dialog.
2. Select **Password** in the **Action** menu.
3. Select **Delete** password.

   The dialog field **Delete password** is opened.
4. Enter the password you want to delete.

   The password is not displayed on the screen.
5. To avoid errors and typos you must re-enter the password in the text field Repeat.
6. Click **[OK]**.
7. Save the key file using **Save** from the **File** menu. If you want to save the key file under another name, select **Save as**.

Changes only become active after being saved and after a new log on.

The specimen file demo.tre

SafeGuard LAN Crypt deliverables include a second key file called *demo.tre*. This file is for demonstration purposes only. It shows how a key file can be organised and how the encryption profiles can be used.

Demo.tre has been allocated two passwords:

- Security administrator password **system**
- User password **user**.

Change the security administrator password or delete the file *demo.tre* before distributing the software to end users. Otherwise any user can log on to SafeGuard LAN Crypt with administrator rights using the password **system**.

Log on to the key file demo.tre with both passwords to see the effect of the logon with the security administrator or user password on the SafeGuard LAN Crypt Administration.

If you log on with the user password to the key file, only the encryption dialog is available.

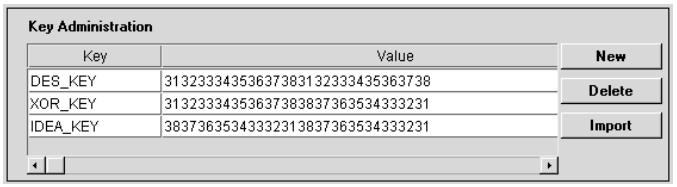
If, however, you log on with the security administrator password to the key file, you can edit the key file(s) in the Administration dialog.

The Administration dialog

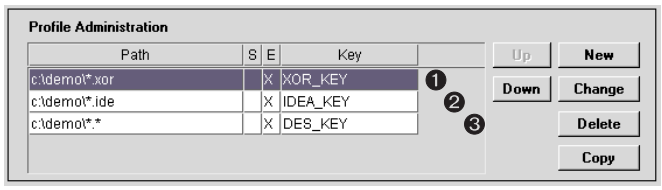
The dialog field comprises three section:

In the **Key file** section you can see which key file is currently open. With the **[Open]** button, you can load another file for editing.

In the **Key administration** section there is a list of the keys saved in the key file. With the **[New]**, **[Delete]** and **[Import]** buttons you can edit the SafeGuard LAN Crypt keys.



The valid profiles for encryption are listed in the Encryption rules section. You should pay particular attention to the order of the profiles.



In this example the encryption of the data in the directory *C:\demo* has been organised as follows:

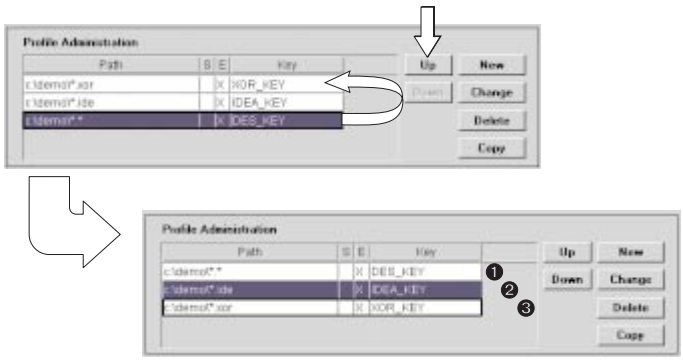
The profiles are processed according to the position in the table!

1. **Entry 1**
   All files with the .xor extension are encrypted with the key XOR_KEY.

2. **Entry 2**
   All files with the .ide extension are encrypted with the key IDEA_KEY.

3. **Entry 3**
   All other files are encrypted with key DES_KEY.

If you now changed the encryptions profile order, by putting the last profile at the beginning of the table, the result would be quite different.



1. Entry 1
   ALL (!) files in the demo directory are encrypted with the key DES_KEY.

2. Entry 2
   has no effect, as all files are encrypted.

3. Entry 3
   has no effect for the same reason.

Appendix A

Encrypted CD-ROMs

- General
- Create encrypted CD-ROMs

General

With SafeGuard LAN Crypt you can work with encrypted CD-ROM media. This offers functions which make it possible to create company-wide CD-ROM media (master), while at the same time ensuring that each department can only use the data relevant for its department.

Tip

The data are encrypted on the CD-ROM using different keys. Each department has the required keys and so can read the necessary data from the CD-ROM. Without a key it is not possible to access data from other departments. SafeGuard LAN Crypt denies access since a key or correct encryption rules have not been defined.

Create encrypted CD-ROM

To create encrypted CD-ROM, it is first necessary to put together all the data and programs required. The security officer must determine which files and directories are to be encrypted with which keys in order to safeguard data confidentiality and to ensure that the individual user can also access data relevant to his work.

For the initial data encryption the security officer creates a key file with the necessary keys and in which the encryption rules for the initial encryption are defined.

Please note that the key file for the initial encryption contains all the keys required for the CD-ROM (master). This key file must not be made available to third parties. Otherwise they will be able to read the whole of the CD-ROM.

Prepare the files

The files to be saved on the CD-ROM being created must first be saved on a hard disk or another suitable data medium where write accesses are possible.

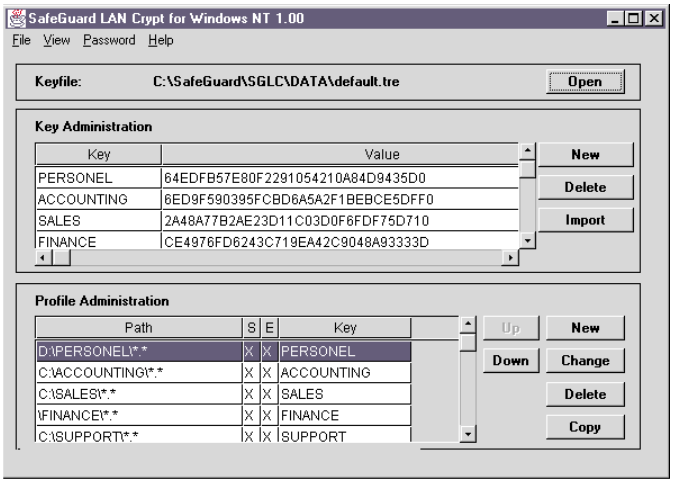
Once all the data have been saved in the appropriate structure on the data medium, the initial encryption can take place with the key file made provided by the security officer for this purpose.

Initial encryption of the files

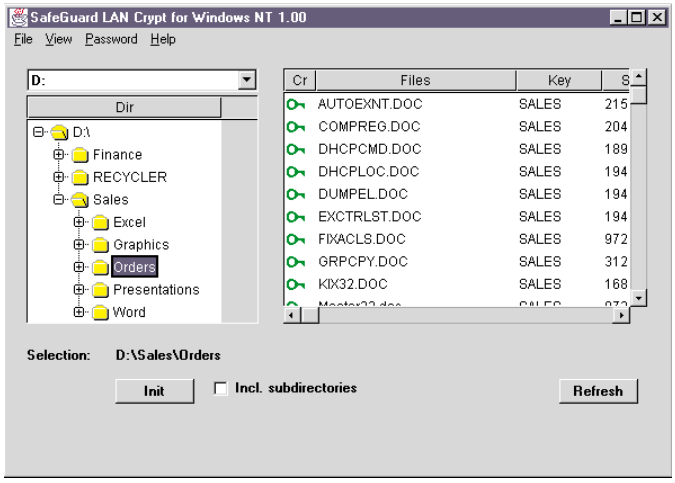
To implement the initial encryption SafeGuard LAN Crypt must be installed on the PC accessing the files to be encrypted. In SafeGuard LAN Crypt the key file prepared for the initial encryption is opened.

Tip

To implement the initial encryption you need not have the security administrator password. Initial encryption can take place with a SafeGuard LAN Crypt user password.



The initial encryption of the files should be done using the SafeGuard LAN Crypt Administration. This is because the complete directory tree can be encrypted there. When using Windows Explorer for the initial encryption, each individual file must be initially encrypted by right clicking the mouse or opening.



Write CD-ROM

Once all the files are encrypted as required, they can be written onto the CD-ROM.

Remember that you need to be logged on to the key file made for the initial encryption. Otherwise you are denied access to the encrypted files by SafeGuard LAN Crypt.

It is not essential for all files on the CD-ROM to be encrypted. You can save unencrypted areas on a CD-ROM. These can then by accessed by all users. For example, you can store the key files required for decryption on the CD-ROM.

If a user's encryption rules state that all the files and directories on the drives of the CD-ROM must be encrypted, this user cannot read any "normal" plain text CD-ROM when encryption is activated.

Appendix B

E-Mail

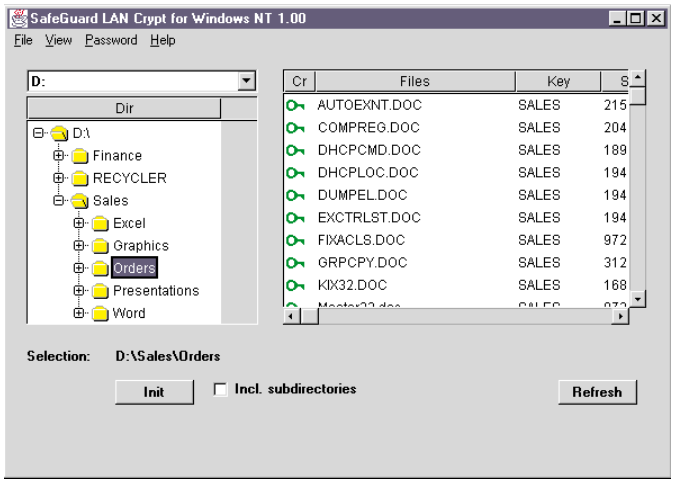
- General
- Send e-mail
- Receive e-mail

General

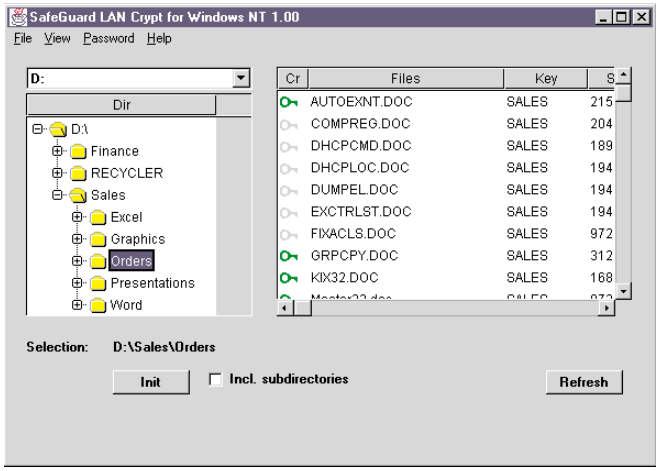
In SafeGuard LAN Crypt it is possible to send encrypted data by e-mail or on data carrier. You have functions which make it possible to provide employees with data without jeopardising data confidentiality.

Send e-mail

To send file attachments in e-mails with SafeGuard LAN Crypt, you must first ensure that the file being send has been initially encrypted. You can check if this is the case by selecting the SafeGuard LAN Crypt Administration dialog and opening the relevant directory in the encryption viewer. If the file shows a "green" key symbol, it has been properly encrypted.



If no icon or a “grey key” precedes the file you want to send, then no encryption rules have been deined for this file or the file has not yet been initially encrypted.



If the file has not been correctly encrypted, you must implement an initial encryption.

Write your e-mail in your comms software as usual. Before you “attach” the file(s) you want to send in encrypted form, you must first temporarily disable encryption in SafeGuard LAN Crypt.

To do this right click the mouse in the Windows task bar on the SafeGuard LAN Crypt Symbol. The Application menu is opened.

Select the **Encryption on** menu item. By clicking this menu item once, the transparent encryption is temporarily deactivated. Now select the relevant command in your comms software to attach the file(s) to your e-mail.

The file(s) will now be attached in encrypted form to your e-mail.

Do not forget to reactivate the encryption. Otherwise all the files you create will be saved in unencrypted form on your data media. To reactivate transparent encryption, select the **[Encryption on]** button from the SafeGuard LAN Crypt Application menu.

Receive e-mail

If you receive an e-mail attachment consisting of a SafeGuard LAN Crypt encrypted file, proceed as follows to decrypt the file.

To separate the encrypted file from your e-mail you must first temporarily disable the encryption. To do this select the menu item **Encryption on**. Click once on this menu item to temporarily disable the transparent encryption.

In your comms software now select the relevant command to separate the file from your e-mail.

The file is now saved in encrypted form on your data carrier. To decrypt the file, copy or move the file into a directory encrypted with the same key as the file received.

Do not forget to reactivate the encryption. Otherwise all the files you create will be saved in unencrypted form on your data media. To reactivate transparent encryption, select the **[Encryption on]** button from the SafeGuard LAN Crypt Application menu.

Appendix C

Backup

- General
- Backup on diskette
- Data restoration from diskette
- Data back up with backup software
- Data restoration with backup software

General

SafeGuard LAN Crypt can protect your data against attacks from unauthorised persons. However, there is no protection against damage to data resulting from program crashes or hardware damage. For this reason you should save your data at regular intervals.

Depending on the backup method it is possible to back up files encrypted by SafeGuard LAN Crypt in encrypted form or in plain text.

Backup on floppy disks

With SafeGuard LAN Crypt you can back up your data on floppy disks in both unencrypted and encrypted form. You can use standard disks as backup medium, i.e. 3.5" floppy disks as well as ZIP, JAZ or removable media, as long as you do not make your backup using backup software.

Unencrypted data backup

To back up data in plain text on a backup media (see above), simply copy them on the relevant backup medium, in Windows Explorer for example.

When creating the backup you must be logged on to SafeGuard LAN Crypt. Only those files which correspond to the profiles in the current key file can be baked up. You have no access to other files encrypted with SafeGuard LAN Crypt.

Encrypted data backup

To back up encrypted data on a backup media (diskette, ZIP, etc.), you must be logged on to a SafeGuard LAN Crypt key file, containing the relevant encryption rules for the files being backed up.

Before the backup the transparent encryption must be temporarily disabled. To do this select the menu item **Encryption on** from the SafeGuard LAN Crypt Application menu.

A single click on this menu item temporarily disables the transparent encryption. Now select the files you want to back up and copy them to the target data medium.

The files are now written to the target data medium in encrypted form.

Do not forget to reactivate the encryption. Otherwise all the files you create will be saved in unencrypted form on your data media. To reactivate transparent encryption, select the **[Encryption on]** button from the SafeGuard LAN Crypt Application menu.

During the data backup you must be logged on to SafeGuard LAN Crypt. Only those files which correspond to the profiles in the current key file can be backed up. You have no access to other files encrypted with SafeGuard LAN Crypt.

Restore data from floppy disk

With SafeGuard LAN Crypt you can back up your data on floppy disks in both unencrypted and encrypted form. You can use standard disks as backup medium, i.e. 3.5" floppy disks as well as ZIP, JAZ or removable media, as long as you do not create your backup using backup software.

Restore unencrypted data

To restore data in plain text from a backup medium (see above), simply copy them from the corresponding backup medium into your target drive, using Windows Explorer for example.

If SafeGuard LAN Crypt is enabled when restoring the data and if there are automatic encryption rules for the target directory, the files are automatically saved in the target directory in encrypted form.

Restore encrypted data

To restore encrypted data, you must be logged on to a SafeGuard LAN Crypt key file containing the relevant encryption rules for the files being restored.

Before the backup the transparent encryption must be temporarily disabled. To do this select the menu item **Encryption on** from the SafeGuard LAN Crypt Application menu.

A single click on this menu item temporarily disables the transparent encryption. Now select the files you want to back up and copy them to the target data medium.

The files are now written to the target data medium in encrypted form.

Do not forget to reactivate the encryption. Otherwise all the files you create will be saved in unencrypted form on your data media. To reactivate transparent encryption, select the **[Encryption on]** button from the SafeGuard LAN Crypt Application menu.

Backup using backup software

Files encrypted with SafeGuard LAN Crypt encrypted can be backed up using backup software. This can be done locally and using LAN/WAN links.

Data can be backed up on removable media (ZIP, JAZ, etc.) or on DAT streamer. As most backup programs access the local data media using other mechanisms, the files encrypted with SafeGuard LAN Crypt are backed up by these programs in encrypted form. Here it is irrelevant if a user is logged on to SafeGuard LAN Crypt or not. This thus ensures a central backup of data created in the company.

With most backup programs it is possible to compare the backed up files after backup with the source files (Verify). Here there can be differences as some backup programs do not react correctly to the changed file size which occurs in SafeGuard LAN Crypt (see File size correction).

Restore data with backup software

Files backed up in one backup can be restored using the restore functions of the relevant backup software.

Note that files which are used when the restoration is made cannot be overwritten.

Tip

With most backup programs it is possible to compare the backed up files after restoration with the source files (Verify). Here there can be differences as some backup programs do not react correctly to the changed file size which occurs in SafeGuard LAN Crypt (see File size correction).

Appendix D

Tips & Hints

- Autosave functions
- FTP-Server
- File attributes
- NTFS attributes
- Zipped files

Autosave-functions

Many software products offer autosave functions so that the user need not make regular interim saves of data during work.

When autosave functions are activated in conjunction with SafeGuard LAN Crypt it is possible that encrypted files are destroyed. This is because the relevant autosave functions remain active during work breaks when you are logged off from SafeGuard LAN Crypt.

Ensure that no documents are open when you log off from SafeGuard LAN Crypt during work breaks. Otherwise files can be destroyed as a result of automatic saving of data.

FTP server

SafeGuard LAN Crypt can only be used on Windows NT workstation and on Windows NT servers.

If SafeGuard LAN Crypt is used on Windows NT servers which also function as FTP servers, please note the following:

To secure FTP accesses with SafeGuard LAN Crypt, an initial encryption of the files in the FTP release directory is made. To ensure that only authorised users can access the data on the FTP servers, SafeGuard LAN Crypt on the FTP server must be exited.

This is necessary as FTP accesses can also be run on the server. In addition all "cached" accesses should be removed. This is because the data is in plain text, depending on the type of access.

Encrypt the files which are to be accessed using FTP services on a workstation and save them on the FTP server in encrypted form.

File attributes

- Read only attribute

Files where the read-only attribute is set cannot be encrypted transparently. If a file operation (rename, copy ...) makes transparent encryption of such files necessary, the operation is prevented by denying access. In this case encrypt the relevant file manually using the Administration program or Windows Explorer. Once the ReadOnly attribute is removed (ATTENTION: Only possible with disabled transparent encryption) transparent encryption functions again.

NTFS attribute

In Windows NT it is possible to restrict by granting access rights on files and directories using advanced "NTFS Attributes". If access rights on files are limited using NTFS attributes, problems can occur when encrypting these files.

If a user/group only has reading rights on a file, the file cannot be encrypted by SafeGuard LAN Crypt encrypted, as this is a dual read/write operation.

Compressed files

With Windows NT you can automatically compress files and directories on data carriers.

Please note that compressed files cannot be encrypted.

You must decompress these files to encrypt them. It is not possible to copy or move them into a directory where encryption rules apply.

Appendix E

Registry-Entries

Registry-entries

The behaviour of SafeGuard LAN Crypt can be changed by changing certain entries in the Windows registration.

In **KeyHKEY_LOCAL_MACHINE\Software\Utimaco\Safe Guard LAN Crypt**:

- Defaultkeyfile

The name of the key file is entered here which is displayed by default in the first user logon. This entry can be replaced by another key file (with complete path).

- Language

The language used by SafeGuard LAN Crypt is entered here. Legal values are DE (German) and UK (English).

- PW_HIDDEN

For password entries this entry controls if a "*" is used as echo character or if there is no echo.

NO means echo character "*"

YES means no echo.

In the key

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Utimaco\SGLCDRV:

- AllowRecycleRen

NO means that moving complete directories into the recycle bin is not allowed if they are not empty.

YES means that moving complete directories into the recycle bin is allowed. In this case no decryption, encryption and recryption takes place.

- DirSizeCorrection

Files encrypted with SafeGuard LAN Crypt are preceded with a 4KB header. In many cases it is necessary and advisable to correct the file size, i.e. subtract the 4KB header size to display the original size of the data used. For this data size correction there are three strategies:

The entry ALWAYS means that a check is made on every file whether it is encrypted or not. If it is, the header size is subtracted. This setting can have a negative impact on performance. This is why we do not recommend it.

The entry PROFILES means that a correction takes place in line with the encryption profile. The header size is always subtracted if a file should be encrypted according to the profile.

We recommend using this setting.

The NONE setting means that the header size is never corrected. This setting can result in problems with certain applications. This is why we recommend using this setting only in special cases (e.g. backup of encrypted files). Please note that the changes in Registry settings are only activated on the next reboot of the PC.

Please note that no changes, other than those described in this chapter, may be made to Registry settings. Otherwise the functionality of SafeGuard LAN Crypt is impaired. This can result in data losses.

INDEX

A

Access control 1-12
Access protection 1-23
  Deactivation 1-15
Access rights 1-27
Admin key 1-3, 1-4, 1-18
  Name (File Header) 1-5
Administration dialog 5-12
  Encryption rules 5-14
  Key administration 5-14
  Key file section 5-14
Administrator mode 1-24, 5-2
Administrator password 1-24, 5-9
Algorithm 1-32
  DES 1-32
  IDEA 1-32
  XOR 1-32
AllowRecycleRen 10-3
Application examples 1-7
  Field sales 1-7
  Outsourcing 1-8
Authentication 1-11
Automatic logon 2-17

B

Backup data 1-15
Backup on diskette
  encrypted 8-4
  JAZ 8-3
  removable media 8-3
  unencrypted 8-3
  ZIP 8-3
Backup using backup software
  DAT-Streamer 8-9
  File size correction 8-9
  verify 8-9

C

CD encryption 1-7
CD-ROM, create
  Initial encryption 6-5
  prepare Files 6-4
  write data carier 6-7
Central backup 8-9

D

Data key 1-5, 1-18
  File header 1-5
Decryption 1-17, 1-33
  of files 1-34, 4-16
Default key file 10-2
default.tre 1-26
  First steps 5-7
Delete files 4-17
demo.tre 5-33
Directories
  Deleting 4-18
  Renaming 4-18
DirSizeCorrection 10-4

E

E-mail
  append 7-3
  receive 7-6
  send 7-3
Encrypted data backup 1-15
Encrypted e-mail 1-15
Encryption 1-16, 4-11
  Activation 4-4
  Deactivation 4-4
  Initial encryption 4-15
Encryption dialog 4-11
Encryption rules 1-27
  Defining 5-28
  Editing 5-26
  Hierarchy 5-24
Encryption status 4-14
  Explorer 4-19
Enterprise Distribution Concept 1-10
Examples
  demo.tre 5-33
  Hierarchy 5-25
Exit 4-5, 4-21

F

File attributes
  read-only attribute 9-4
File header 1-5, 1-16, 3-6
File size correction 8-9, 8-10
FTP-Server 9-3

I

Initial encryption 1-5, 4-15
Installation 2-2
Installation script 2-14
Integrated access protection 1-23

K

Key file 1-4, 1-13, 4-4, 5-6
  Components 1-25
  Create 5-15
  Creation 5-15
  Definition 5-3, 5-5
  Import 5-21
  Information 4-5
  Structure 3-2
  Switching 4-10

L

Language 10-2
Log file 2-19
Logoff 4-3, 4-21
Logon 4-3, 4-6

M

Many 9-2
Master key file 1-3, 1-4

N

NTFS attributes 9-5

P

Password 1-26
  Change administrator password 5-9
  Change user password 4-8
  Characters 1-26
Password 5-30

PW_HIDDEN 10-3

R

Random algorithms
  Data key 1-5
  System key 1-5
Random key 1-12
Recrypt 1-33
Recycle bin 4-17
Registry-entries 10-2
Remote access 1-23, 1-34
Restore data from diskette
  encrypted 8-7
  JAZ 8-6
  removable media 8-6
  unencrypted 8-6
  ZIP 8-6

S

Script-driven installation 2-2
Security administrator 1-3
Security concept 1-12
security officer 6-3
Security officer 1-3
Solution concept 1-11
Standard key file 2-18, 3-3
Start Administration 4-5
System key 1-5
System requirements 2-3

T

Template 1-3, 1-4, 1-20
Transparent encryption 1-22

U

Unattended setup 2-2, 2-13
Update 2-4
Use of resources 1-22, 3-3
User menu 4-2, 4-3
User mode 1-24
User password
  Deleting 5-30, 5-32

Z

Zipped files 9-6