SOPHOS

SafeGuard® LAN Crypt 3.71 Client
User manual

Document date: December 2010

Contents

1 Overview

1.1 What is SafeGuard LAN Crypt?

SafeGuard LAN Crypt is a product for transparent file encryption. It has been developed to enable confidential file exchange for groups of trusted users in large organizations.

In contrast to other file encryption products, SafeGuard LAN Crypt works without user interaction, supporting the role of a security officer who is also able to restrict the access rights of the system administrator by LAN Crypt-encrypted files. A Master Security Officer can delegate the right to administer SafeGuard LAN Crypt. This way they can establish a hierarchy of Security Officers, which meets the security requirements of any company.

Every time a user moves a file into a trusted directory, the file is encrypted on their computer. And every time another trusted user in the same group reads the file from this directory, it is transferred to them in encrypted form. The file is only decrypted on its recipient's computer. It may be modified there and encrypted again before being transferred back to the encrypted directory.

Encrypted files are not assigned to individual users. Any user who has the correct key can access an encrypted file. This allows administrators to create logical user groups which are able to share encrypted files. This can be compared to a bunch of keys in use in everyday life. SafeGuard LAN Crypt provides users and user groups with a bunch of keys that can be used for different doors or safes.

Unauthorized users may be able to access these encrypted files (only from workstations without SafeGuard LAN Crypt), but without SafeGuard LAN Crypt authorization, they cannot read them.

This means a file is never at risk even if no access protection is defined for the system itself, if the network is attacked, or even if employees do not obey the organization's security policy.

If you need to protect your intellectual property stored in files from unauthorized access in the LAN, on file servers, on local hard disks or on removable media, SafeGuard LAN Crypt should be the product of your choice.

1.2 Data protection using SafeGuard LAN Crypt

SafeGuard LAN Crypt guarantees that sensitive files can be stored securely on file servers and workstations. The data is transmitted securely over LAN or WAN networks, as encryption and decryption are performed in RAM on the client workstation. There is no need to install special security software on the file server itself.

The policy files include all the rules, access rights and keys required for transparent encryption. Before a user can encrypt/decrypt data using the SafeGuard LAN Crypt software installed on the client workstation, they need to be able to access the policy file. The policy file is secured via a certificate. For accessing the policy file, a user has to own the private key of the appropriate certificate.

All encryption/decryption tasks run transparently on the client workstation with minimal user interaction.

SafeGuard LAN Crypt allows trusted users to be organized into different trusted groups by defining different rights for directories and files. These rights are grouped into encryption profiles for the users. The user can access the policy file containing the encryption profile by owning the private key assigned to the certificate.

All SafeGuard LAN Crypt users whose policy file contains the same encryption profile are members of a trusted group. They do not need to worry about encryption or key exchange. They only have to be able to access the policy files to have their data encrypted or decrypted transparently, as soon as they open or close it.

As the encryption profiles are distributed via policy files, all organizational forms can be mapped from a centralized LAN model, in which users are administered centrally, to a remote model in which users work on notebooks.

SafeGuard LAN Crypt Administration and Windows Administration

A separate administration computer is used to configure SafeGuard LAN Crypt and administer encryption profiles. To draw a clear distinction between Windows administration and SafeGuard LAN Crypt administration, the role of a security officer is established. The security officer defines encryption profiles in policy files to specify which encrypted data is to be stored in particular directories, and who is allowed to access this data. After creating the policy files on the administration station, the security officer deploys them.

A standard Windows tool, the Microsoft Management Console (MMC), is used to administer SafeGuard LAN Crypt. The SafeGuard LAN Crypt Administration user interface consists of snap-ins for the MMC. SafeGuard LAN Crypt Administration stores most of the objects to be administered (user data, keys, encryption paths, etc.) in their own databases.

There are two major benefits to using this database approach instead of just Windows tools such as Active Directory:

- System administration and security administration can be kept strictly separate. This is because SafeGuard LAN Crypt uses a dedicated database, and is totally independent of system administration. The SafeGuard LAN Crypt database is encrypted and therefore protected against unauthorized access. In addition, this database prevents the SafeGuard LAN Crypt system from being changed unintentionally (e.g. if the system administrator deletes a required security object).
- On the other hand, it is often not a good idea to allow people who are not system administrators to change the system configuration. It is obvious that assigning permission to write data for system administration is a real problem. This is another good reason for storing SafeGuard LAN Crypt-specific data in a separate database.

The path to the policy files (from the user's point of view) and other non-security-relevant settings are distributed by means of operating system mechanisms (e.g. Active Directory or the central configuration file, `ntconfig.pol`).

To provide the best possible protection, SafeGuard LAN Crypt's functions are divided into two parts:

- **SafeGuard LAN Crypt User functions**

  SafeGuard LAN Crypt user functions include the encryption and decryption information for data.
  This information is required for everyday tasks using SafeGuard LAN Crypt. As soon as a user is permitted to access the encryption information, the files are encrypted and decrypted transparently. No further user interaction is required.
  In addition, SafeGuard LAN Crypt has a range of display functions that allow the user to view "their" encryption profile.

- **Safe Guard LAN Crypt Security Officer functions**

  SafeGuard LAN Crypt Administration has functions that are reserved for security officers.
  A Security Officer certificate is a prerequisite for creating encryption profiles, and administering existing encryption profiles.
  The SafeGuard LAN Crypt Administration component can be installed separately from the user application, since only a security officer should be able to access it.
  When you install SafeGuard LAN Crypt you can select the components you require (only Administration, only the User application, or both).

1.3 Transparent encryption

For the user, transparent encryption means that all data stored in an encrypted form (in encrypted directories or drives) is automatically decrypted in the main memory when opened by an application. When the file is saved, it is again encrypted automatically.

- All files for which there is an encryption rule are encrypted automatically.

- If files are copied or moved into an encrypted directory, they are encrypted according to the encryption rule that is valid for this directory. You can, of course, define different encryption rules for different file extensions or names in the same directory. Encryption is governed solely by encryption rules - it does not depend on directories!
- When renaming encrypted files, they remain encrypted (unless there is no, or no other, encryption rule for the new file name/file extension).
- When the user copies or moves encrypted files to a location where the current encryption rule is no longer valid, the system automatically decrypts these files.
- If the Administrator has activated *Persistent Encryption*, files also remain encrypted if they are moved (in Windows Explorer) to a location in which no encryption rule applies. This function has no effect if files are copied or moved outside Windows Explorer (for example, from the command line) and the files will be decrypted.
- When the user copies or moves encrypted files to a location where the current encryption rule is no longer valid, but a different one is present, the system first decrypts these files and then encrypts them again.
- Transparent encryption takes place for all file operations. As all the tasks run in the background, users will be unaware of these processes while working with encrypted data.

Note: SafeGuard LAN Crypt does not encrypt files for which **NTFS compression** or **EFS encryption** is used under the Windows NTFS file system. However, the Initial Encryption Wizard can decompress and decrypt NTFS compressed and/or EFS encrypted files respectively during initial encryption, provided that an encryption rule exists for these files. Afterwards, SafeGuard LAN Crypt will encrypt the files according to the encryption rules applying.

The security officer defines whether a user is entitled to decompress NTFS compressed files or to decrypt EFS encrypted files if necessary.

1.3.1 Access to encrypted data

If a user’s profile does not contain a key or encryption rule for a particular directory in the encryption policy, they cannot access the encrypted data in this directory. They cannot read, copy, move, rename, etc. encrypted files in this directory.

If the user owns the key used to encrypt these files, they can access them, even if their encryption profile does not contain an encryption rule for these files.

Note: When storing files which have only been opened with the available key (no encryption rules for these files), these files may be set up in an unencrypted form. This happens because applications create temporary files, delete the source file and then rename the temporary file. As the new file does not have an encryption rule, it is created in an unencrypted form. To avoid this such a program has to be registered as „program with special behavior when saving files“ (see *Programs with specific behavior when saving files* on page 22).

1.3.2 Renaming or moving directories

For performance reasons, SafeGuard LAN Crypt does not change the encryption status when it uses Windows Explorer to move entire folders within a disk drive. This means that the folders are not encrypted, decrypted or re-encrypted when they are moved.

If the files in these folders have already been encrypted, they stay that way even though they will now have a new folder name or be stored in a new location. If the user has the corresponding key, they can access and work with these files as usual.

The exception to this is when folders or files are moved to a different partition or USB memory medium for which no encryption rules have been implemented. If *persistent encryption* is not active, the files are decrypted when they are moved to these types of media, as before. However, if the administrator has activated the *persistent encryption* function, these files will remain encrypted.

Persistent encryption has no effect if files are copied or moved outside Windows Explorer (for example, from the command line), and the files will be decrypted.

Moving over SafeGuard LAN Crypt

However, SafeGuard LAN Crypt supports the secure movement of files and directories. When you move files over SafeGuard LAN Crypt, the files and directories are encrypted, decrypted or re-encrypted as required, according to the current encryption rules at the new storage location. Afterwards, the source files are securely deleted.

To access this function, select the **Move over SGLC** command from the Windows Explorer context menu. A dialog appears in which you can specify where the files are to be moved to.

1.3.3 Explicit file decryption

To decrypt a file, simply copy or move it to a directory without encryption rules. The file is decrypted automatically.

However:

- the correct encryption profile must be loaded.
- you must have the right key.
- the active encryption profile does not include an encryption rule for the new location.
- and *persistent encryption* is not active.

Note: SafeGuard LAN Crypt can also encrypt offline folders in Windows. However, in this case problems may arise when it is used together with virus scanners. The Readme file supplied with the SGLC Client will give you more specific information about known problems with virus scanners.

1.3.4 Deleting encrypted files - Recycle Bin

If your encryption profile is loaded, you can delete any encrypted file for which you own the key.

Note: Deleting files actually means you move them to the Windows Recycle Bin. To provide the highest level of security, files encrypted by SafeGuard LAN Crypt remain encrypted in the Recycle Bin. The key used to encrypt a file must be available in the active profile before you can finally delete the file. If the key is not available, an error message appears and you cannot remove the files from your system.

In some situations, encryption rules may have been modified after a file was moved to the Recycle Bin. In this case, the old key must be available in the active profile before you can finally delete this file.

1.3.5 Files/directories excluded from encryption

The following files and directories are automatically excluded from encryption (even if an encryption rule has been defined for them):

- Files in the SafeGuard LAN Crypt installation directory
- Files in the Windows installation directory
- Local Cache

1.3.6 SafeGuard LAN Crypt and SafeGuard Enterprise

This version of SafeGuard LAN Crypt can be used in parallel with SafeGuard Enterprise. For example SafeGuard Data Exchange can be used to encrypt all data on removable media and SafeGuard LAN Crypt for encrypting all files on network shares.

The SafeGuard LAN *Client status* dialog displays all encryption rules, which are valid on the computer. In general SafeGuard Enterprise Data Exchange rules are applied first and then the SafeGuard LAN Crypt rules are applied. Prioritization can be changed.

Re-encrypting files encrypted by SafeGuard Enterprise Data Exchange

The *Initial Encryption Wizard* allows to re-encrypt files, which have been encrypted using SafeGuard Data Exchange but the SafeGuard Enterprise encryption rule does not apply anymore. Such files do exist for example if the encryption rule was removed but the files have not been decrypted explicitly. In this case the option **Re-encrypt files in accordance with profile** can be selected in the Initial Encryption Wizard, which will re-encrypt these files according to the SafeGuard LAN Crypt encryption rules.

1.3.7 Loading the policy file

SafeGuard LAN Crypt standard behavior

When a user logs on to Windows, their cached profile will be loaded first. SafeGuard LAN Crypt then checks whether a new policy file is available for the user by establishing a connection to the specified location of the policy file (network drive). If a new policy file is found there, the cached user profile will be updated.

This approach has the advantage that the user can start working with encrypted files while SafeGuard LAN Crypt checks whether a new version of the policy file exists.

If the network drive is not accessible, the user works with the cached user profile until it can be updated.

Note: SafeGuard LAN Crypt verifies the certificates of the user and the (master) security officer. If the certificates contain a ”CRL Distribution point” and no valid CRL is present in the system, Windows tries to import the CRL from the specified address. If a firewall is installed you may see a message that a program (loadprof.exe) is trying to establish a connection to the Internet. In some cases also the download of the user profile may cause this message.

Behavior defined by security officers

The security officer can modify the standard behavior using central settings. Security officers can specify for how long the cached policy will be valid on client computers. Furthermore they can define update intervals for the policy files. The settings defined by the security officer are shown in the *Profile* tab of the *Client Status* dialog (see *The Client status dialog* on page 21).

Within the time period defined here the policy file is valid on the client and the user can access encrypted data, even if there is no connection to the file location of the policy file.

When the specified time period expires SafeGuard LAN Crypt tries to load the policy file from the network drive to update it again. If this is not possible, the policy file will be unloaded. The user can no longer access encrypted data. The policy file will only be updated and loaded again, when a valid policy file is available (for example at the next logon with a connection to the client location for policy files). The user can access encrypted data again. The counter for the duration of cache storage is reset.

By specifying the duration of cache storage you can on the one hand ensure that the client computers are provided with up-to-date policy files in regular intervals and that users use up-to-date policies at all times. On the other hand you can prevent users from working with the same policy files for an unlimited time period since a user can continue working with a cached version of the policy file for an unlimited time period, if this option is set to *not configured*.

The counter for the permitted duration of cache storage will be reset in the following situations:

- The storage location of the policy files is accessible and a valid policy file was transferred to the client (e.g. at user logon or triggered by a specified update interval), however, the policy file is not new compared to the existing one.
- A new policy file is available and has been loaded successfully.

The counter for the permitted duration of cache storage will NOT be reset in the following situations:

- The client computer tries to receive a new policy file. However, the storage location of the policy files is not accessible.
- A new policy file was transferred. However, it could not be loaded due to an error.
- A new policy file is available. However, it requires a new certificate. The user does not have this certificate or is not able to load it.

If updating the policy file fails, the expiry time of the cached policy file will be displayed in a balloon tooltip on the client computer. The user can then initiate a manual update via the SafeGuard LAN Crypt Tray Icon (*see Load encryption rules/Update encryption rules* on page 19).

Policy files are not cached

Security officers can also specify that the policy file will not be cached. This means that users receive their user profiles when logging on, if the file location of policy file is accessible. If it is not accessible or an error occurs when loading the profile, the user cannot access encrypted files.

Clients from version 3.12

This functionality is not available for older client versions. However, clients from version 3.12 can be operated with SafeGuard LAN Crypt Administration version 3.60. Clients of this type show the following behavior when loading policy files:
The client will always try to load the policy file from the specified file location. If this location is not accessible, a cached version of the policy file will be loaded. This cached policy file does not have an expiry date and will not be updated until a newer version has been loaded successfully. Furthermore, it is not possible to define an update interval for the policies. Cached policy files remain valid until the file location specified for policy files is accessible and the cached policy file is replaced by a policy file from this location.

1.4 System requirements

1.4.1 Platforms

SafeGuard LAN Crypt Client is available for the following operating systems:

- Windows XP SP2 32bit
- Windows XP SP3 32bit
- Windows Vista Ultimate SP1 32bit
- Windows Vista Enterprise SP1 32bit
- Windows Vista Business SP1 32bit
- Windows Vista Ultimate SP2 32bit
- Windows Vista Enterprise SP2 32bit
- Windows Vista Business SP2 32bit
- Windows 7 Professional 32bit
- Windows 7 Enterprise 32bit
- Windows 7 Ultimate 32bit
- Windows 7 Professional 64bit
- Windows 7 Enterprise 64bit
- Windows 7 Ultimate 64bit

1.4.2 Firewall

After a user logs on, Safeguard LAN Crypt tries to load the SafeGuard LAN Crypt user profile. At the same time, it verifies the user and (M)SO certificate. If the certificates contain a "CRL Distribution point" and no valid CRL is present in the system, Windows tries to import the CRL from the specified address. If a firewall is installed you may see a message that a program (loadprof.exe) is trying to establish a connection to the Internet.

1.5 SafeGuard LAN Crypt und SafeGuard Enterprise

- SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise 5.35.4 and higher can coexist on the same computer and are fully compatible.
- SafeGuard LAN Crypt with versions below 3.7x and SafeGuard Enterprise 5.4x cannot coexist on one computer.
  If you are trying to install SafeGuard Enterprise 5.4x on a computer with an already installed SafeGuard LAN Crypt of version 3.6x or below, the setup will be cancelled and a respective error message will be displayed.

- SafeGuard LAN Crypt 3.7x and SafeGuard Enterprise with version below 5.35.4 cannot coexist on one computer.
  If you are trying to install SafeGuard LAN Crypt 3.7x on a computer with an already installed SafeGuard Enterprise of versions below 5.35.4, the setup will be cancelled and a respective error message will be displayed.

2 Installation

Note: SafeGuard LAN Crypt can only be installed with Windows administrator privileges.

1. Doule click on one of the **.msi** files in the `Install` directory of your installation CD.)
   - **sglc_x64.msi** for installation on a 64bit operating system **ou**
   - **sglc.msi** for installation on a 32bit operating system

   Click **Next**.

2. The *License Agreement* dialog is displayed.
   Please select **I accept the license agreement** in the *License Agreement* dialog. Otherwise, it is not possible to install SafeGuard LAN Crypt! Click **Next**.

3. The *Destination Folder* dialog is displayed.
   Select where to install SafeGuard LAN Crypt. Click **Next**.

4. The *Select Installation Type* dialog is displayed.
   In this dialog, you select which components of SafeGuard LAN Crypt are to be installed.

- **Typical:**
  Installs the most commonly used of SafeGuard LAN Crypt Client's application functions

- **Complete:**
  Complete client installation

- **Custom:**
  Lets the user select the different components.

  Select **Custom** and click **Next**.

  The following components can be installed:

- **Client Installation**
  - Shell Extensions

    Installs the SafeGuard LAN Crypt Explorer Extensions.
    SafeGuard LAN Crypt adds entries to the Windows Explorer which allow the initial encryption of files and directories, the explicit encryption/decryption of files and directories and makes it easy for you to check the encryption state of your data. These entries are displayed in the context menus of the drives, directories and files. In addition, an *Encryption information* tab is added to the Windows *Properties* page.

  - **User Application**

    Installs the SafeGuard LAN Crypt user application.
    An icon in the Windows Taskbar represents the SafeGuard LAN Crypt user application.

A key icon displays the state of SafeGuard LAN Crypt.
The application provides users with these functions (right-hand mouse click to access them):

- Load/Update encryption rules

- Clear encryption rules

- Deactivate/Activate encryption

- Show profile

- Client status

- Initial encryption

- Close

- About

- **Client API**

  API for automating tasks on the SafeGuard LAN Crypt client.

5. Select which components are to be installed and click **Next**.
6. Check your entries again and click **Next** to start the installation.
7. If the installation is successful, a dialog appears in which you can click the **Finish** button to close the installation process.

Note: Restart the system to load the driver so that all the settings will be accepted!

2.1 Unattended installation

Unattended installation means you can install SafeGuard LAN Crypt automatically on a large number of computers.
The `Install` directory of your installation CD includes the `.msi`-file that is required for unattended installation of the client components.

2.1.1 Components to install

The following list shows all the components that are to be installed and the way they have to be specified for an unattended installation.

The keywords (Courier, bold) represent the way the components have to be specified under ADDLOCAL= when an unattended installation is run. Component names are case-sensitive.

ADDLOCAL=ALL installs all available components.

Shell Extensions - **`ShellExtensions`**

User Application - **`UserApplication`**

Client API - **`ClientAPI`**

2.1.2 Command Line Syntax

To perform an unattended installation you must run `msiexec` with certain parameters.

Mandatory parameters:
`/I`
Specifies the installation package to be installed.

`/QN`
Installation without user interaction (unattended setup)

Name of the **`.msi`** file:
`sglc.msi` for 32bit operating systems
`sglc_x64.msi` for 64bit operating systems

Syntax:

```
msiexec /i <path>\sglc.msi | sglc_x64.msi /qn
ADDLOCAL=<component1>,<component2>,...
```

Optional parameter:
`/L* <path + filename>`
Logs all warnings and all error messages in the location specified under `<path + filename>`.

EXAMPLE:

```
msiexec /i C:\Install\sglc.msi /qn ADDLOCAL=ALL
```

A complete installation of SafeGuard LAN Crypt (32bit) is performed. The program is installed in the default installation directory (`<System drive>:\Program Files\Sophos`). The `msi` file is located in the `Install` directory on the C drive.

3 Deinstallation

SafeGuard LAN Crypt Client may only be deinstalled if you have Windows administrator privileges.

Please note that encrypted files can no longer be decrypted after SafeGuard LAN Crypt Client has been deinstalled!

Notice: Do not install SafeGuard LAN Crypt Client again immediately after you have deinstalled it. You must reboot the machine at least once before you install it again.

4 Terminal Server

This version of SafeGuard LAN Crypt supports Windows Terminal Servers and Citrix Terminal Servers.

4.1 System requirements

4.1.1 Platforms

SafeGuard LAN Crypt Client is available for the following operating systems:

- Windows Server 2003 R2 SP2 32bit with Terminal Server services
- Windows Server 2008 R2 64bit with Terminal Server services
- Citrix Presentation Server 4.5 32bit with Hotfix Rollup Pack 3 on Windows Server 2003 R2 SP2 32bit
- Citrix XenApp 6 on Windows Server 2008 R2 64bit

4.1.2 Firewall

After a user logs on, Safeguard LAN Crypt tries to load the SafeGuard LAN Crypt user profile. At the same time, it verifies the user and (M)SO certificate. If the certificates contain a "CRL Distribution point" and no valid CRL is present in the system, Windows tries to import the CRL from the specified address. If a firewall is installed you may see a message that a program (loadprof.exe) is trying to establish a connection to the Internet.

4.2 Installation

In general the installation procedure has to be carried out the same way as in non Terminal Server environments (see chapter *Installation*).

For installation on a Terminal Server use the **`sglcts.msi`** or **`sglcts_x64.msi`** installation package.

Important:

- When installing on a Terminal Server please use a local logon session with administrative rights to install LAN Crypt.
- In case Citrix Presentation Server or Citrix XenApp will be used please install these before SafeGuard LAN Crypt.

4.3 Restrictions

Citrix

- Encryption in combination with Citrix Client Drive Redirection is not supported.
- Citrix Streamed Applications are not supported.

5 SafeGuard LAN Crypt User Application

In everyday use, SafeGuard LAN Crypt requires hardly any user interaction. A number of improvements have been made to the new SafeGuard LAN Crypt Client so that users can work with their files more securely and effectively. The SafeGuard LAN Crypt Client actively supports its users when they encrypt and decrypt data.

5.1 Logon to SafeGuard LAN Crypt

When you log on to SafeGuard LAN Crypt, the encryption profile, which is stored in policy files, is loaded onto the client machine. The encryption profile can only be loaded, if the user owns the corresponding certificate.

SafeGuard LAN Crypt encryption profiles are created by a security officer, in accordance with the company's security policy, and then stored in policy files. When they log on to the network, client machines find out where these policy files are stored. The system administrator makes these settings. The path to the policy files is written to a client machine's registry. SafeGuard LAN Crypt loads the policy files from this directory and checks, whether the user is allowed to load it, by verifying the user's certificate.

5.1.1 Logon with token

You can also log on to SafeGuard LAN Crypt using a token. A prerequisite for this logon method is that the user's SafeGuard LAN Crypt user certificate is stored on the token. If the user certificate is found on a token connected to the system, the user will be logged on.

When using tokens for logging on, SafeGuard LAN Crypt may try to load a policy file before the token can be identified by the operating system.

In this case, a message will be displayed indicating that the user certificate could not be found, although the token is connected to the system.

The user has to load the policy file manually via the user application in the toolbar > Load encryption rules. Thereby, the token will be identified and the user will be logged on.

5.2 Certificates

Before they can access their encryption profile, the corresponding certificate must be available on a user's machine. The Security Officer has the task of distributing these certificates to the users. Users then import the certificate to their own machines.

If the certificates are available at the first logon, the entire process runs without any user interaction.

SafeGuard LAN Crypt also has an option for importing certificates automatically, when the encryption profile is loaded for the first time. In this case, the security officer configures the system in such a way that SafeGuard LAN Crypt can find a certificate file during logon and starts importing the certificate automatically. The user is prompted once to enter the PIN for the PKCS#12 key file.

Note: The Security Officer is responsible for distributing the PIN required to import a certificate automatically to the users.

The certificate is checked every time the encryption profile is loaded. If a valid certificate is found, the user is logged on to SafeGuard LAN Crypt. If no valid certificate is found, the user is not able to work with encrypted data.

Note: If a user attempts to log on to SafeGuard LAN Crypt and their logon fails, they receive an error message to tell them why they were unable to log on. For a list of the various error messages see *Appendix: Error messages displayed when the profile is loading* on page 35.

Special encryption rules included in the SafeGuard LAN Crypt encryption profiles give users access to encrypted data. These rules define exactly which files in particular directories have to be encrypted by each key. A user's encryption profile only needs to be loaded and encryption and decryption takes place in the background (transparently). The user is unaware of the encryption/ decryption tasks being performed.

Note: CA certificates are only accepted if they are held by "Trusted Root Certification Authorities". However, the SGLC software does import any CA certificates that might be held in PKCS#12 key files, together with the user certificates in the "Personal - Certificates" folder. To prevent an error message appearing, you must move the CA certificates to "Trusted Root Certification Authorities" manually.

5.3 User application

A key icon in the Windows Taskbar shows the state of SafeGuard LAN Crypt:

- **Green means:**
  Encryption rules loaded, transparent encryption activated.
- **Yellow means:**
  Encryption rules loaded, transparent encryption deactivated.
- **Red means:**
  No profile loaded.

Users can access these functions in the application (by right-clicking):

- Load encryption rules/Update encryption rules
- Clear encryption rules

- Deactivate/Activate encryption
- Show profile
- Client status
- Initial encryption
- Close
- About

5.3.1 User menu

The SafeGuard LAN Crypt user menu is represented by an icon in the Windows task bar. This icon changes according to the current status of SafeGuard LAN Crypt.

Note: The menu commands available depend on the configuration of the SafeGuard LAN Crypt Client.
The security officer defines the configuration centrally.

Right-click the icon to open the SafeGuard LAN Crypt user menu offering the following commands:

- **Load encryption rules/Update encryption rules**
  This command loads the currently valid encryption rules. This is important if the profile has been changed during runtime.

- **Clear encryption rules**
  Encrypted data cannot be accessed, if the encryption rules are cleared. This is a security function that secures encrypted data against unauthorized access when the workstation is unattended. Of course, this function only makes sense if the usage of the private key is secured by a password. Otherwise, the profile could be reloaded by using the **Load encryption rules** command.

- **Deactivate/Activate Encryption**
  Toggles transparent encryption on and off.
  Deactivating encryption is used if files are to remain encrypted when they are moved or copied to a folder where no encryption rule is valid. With active encryption, the files would be decrypted if they were copied to this type of folder.
  If, for example, an encrypted file is attached to an e-mail, it would be decrypted automatically, if transparent encryption were active. If transparent encryption is deactivated, the encrypted file can be sent as an e-mail attachment.

Note: If the administrator has activated the **persistent encryption** function, encrypted files remain encrypted even if they are copied or moved to a location for which no encryption rule has been specified, via Windows Explorer. Persistent encryption has no effect if files are copied or moved, but not with Windows Explorer (for example, from the command line) and the files will be decrypted.

- **Show profile**

  Displays the encryption rules and the keys contained in the encryption information in two tabs.
  The *Active encryption rules* tab page lists the rules that apply to the user who is currently logged on. In addition, the user can also select the *Display Ignore Rules* and *Display Exclude Rules* options to view these encryption rules.
  The *Available keys* tab page lists all the keys that are available to the current user.

- **Client status**

  The **Client status** function uses seven tabs to display detailed information about the current status of the SafeGuard LAN Crypt Client.

- **Initial encryption**

  Starts the wizard that will encrypt the selected file for the first time (for details see *Initial encryption and explicit encryption* on page 22).

- **Close**

  Closes the SafeGuard LAN Crypt User Application.

- **About**

  Displays information about your current version of SafeGuard LAN Crypt.

Note: The **Close** command only closes the SafeGuard LAN Crypt User Application. SafeGuard LAN Crypt remains in its current status! This means that transparent encryption/decryption continues. Closing the User Application does not protect your files against unauthorized access (e.g. when you leave your workstation).

5.3.2 The Client status dialog

You can also start the **Client status** dialog from Start/All Programs/Sophos/SafeGuard LAN Crypt/Client status. The *Client status* function includes eight tabs which provide useful information about, for example, the current encryption rules:

Here you will see this information:

- **Status**

  Indicates whether the user profile has been loaded and encryption is active. Furthermore, this tab shows detailed information on the policy file (creation date, security officer who created the file etc.).
  If the user profile has been loaded, encryption is also active. However, the encryption can also be (temporarily) disabled when the user profile has been loaded (*see Deactivate/Activate Encryption* on page 19).

- **Settings**

  Provides information on the settings which currently apply to the client. These settings are defined centrally by the security officer and refer to encryption, system tray icon and the settings for the Initial Encryption Wizard. Among other details this tab shows whether persistent encryption has been activated as well as the menu commands to be available on the client computers.

- **Profile**

  This tab shows the settings for the user profile centrally defined by the security officer.

- **Certificates**

  Shows details about the user certificate (issuer, serial number, validity) and also the rules that apply to the client for checking the certificate.

- **Keys**

  Shows information on all keys available for the currently loaded profile.

- **Rules**

  Lists all the encryption rules that apply to the current user. By clicking checkboxes you can also display the exclude rules and the encryption rules of other SafeGuard products.

- **Unhandled**

  This provides information about unhandled applications, disk drives and devices as well as the *Ignore rules* of all installed SafeGuard products.

  SafeGuard LAN Crypt treats certain applications as „unhandled applications“ by default. These application are also shown on this tab.

- **Applications**

  This tab shows programs which require a special approach by SafeGuard LAN Crypt due to their behavior.

  Programs with specific behavior when saving files

  The security officer has specified these programs here because they show a special behavior due to their behavior when saving files. In order for these programs to work properly, SafeGuard LAN Crypt has to use a special approach on them.

  Antivirus software

  For scanning encrypted files, antivirus software requires the key used for encrypting the files. The antivirus software specified by the security officer in this tab has access to all keys and is therefore able to also check encrypted files.

- **Import/Export buttons**

  Use the *Import* button to import SafeGuard LAN Crypt settings from an XML file, or the *Export* button to export the current client settings to an XML file.

5.4 Initial encryption and explicit encryption

After SafeGuard LAN Crypt has been installed, initial encryption needs to be performed. During this process, all files are encrypted using the loaded encryption profile. This initial encryption can be performed using

- the SafeGuard LAN Crypt system tray icon
- SafeGuard LAN Crypt Explorer extensions (see *Explorer extensions* on page 30) or
- the `sglcinit.exe` tool that also supports Unattended mode (see below).

In addition to performing the initial encryption of entire folders, the `sglcinit.exe` command line tool, together with the Explorer extensions, can also be used to encrypt, decrypt and re-encrypt individual files.

Targeted explicit encryption, decryption or re-encryption might be necessary in these cases:

- If plain (unencrypted) files are located in a directory for which an encryption rule exists.
- If encrypted files are located in a directory for which no encryption rule exists.
- If files in an encrypted directory are encrypted with the wrong key.
- If the encryption rules in the encryption profile have changed.
- If files are encrypted with several keys.

5.4.1 The Initial Encryption Wizard

The tool for initial encryption, `sglcinit.exe`, offers a wizard with a graphical user interface. This wizard supports

- encrypting, decrypting and re-encrypting files
- checking the encryption status of files.

You can start this wizard in a number of ways:

- by clicking the Systray icon
- by going to Start/All Programs/Sophos/SafeGuard LAN Crypt/Initial encryption
- by double-clicking on `sglcinit.exe` in C:\Program Files\Sophos\SafeGuard LAN Crypt\

Note: The encryption, decryption and re-encryption processes are always only performed in accordance with the encryption profile. That is why you have to load an encryption profile.

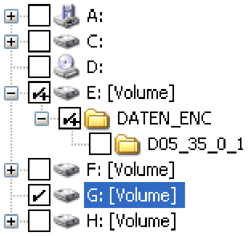
5.4.1.1 Performing initial encryption

1. After starting the wizard, select the **Perform initial encryption** option in *Step 1 / 5*.
2. After clicking **Next**, you can define how files are to be handled in *Step 2 / 5*.

- **Encrypt files in accordance with profile**
  If you select this option, the files will be encrypted according to the rules contained in the user's profile (default setting). If the system finds already encrypted files, they will be ignored.
- **Re-encrypt files in accordance with profile**
  If you select this option, files encrypted with a different key than the one defined in the profile will (also) be decrypted and encrypted with the correct key.
  A prerequisite for this procedure is that the key which has been used for encrypting the file(s) in the first place is contained in the user's profile.
  This option allows to re-encrypt files, which have been encrypted using SafeGuard Data Exchange but the SafeGuard Enterprise encryption rule does not apply anymore. Such files do exist for example if the encryption rule was removed but the files have not been decrypted explicitly. In this case an option can be activated in the *Initial Encryption Wizard*, which will re-encrypt these files according to the SafeGuard LAN Crypt encryption rules.

Already encrypted files can be decrypted if there is no (longer) an encryption rule applying to them (see *Decrypting files* on page 26).

3. After clicking **Next**, you can define which folders are to be encrypted/re-encrypted via a directory tree structure in *Step 3 / 5*.



☐ A:
☐ C:
☐ D:
☑ E: [Volume]
☑ DATEN_ENC
☐ D05_35_0_1
☐ F: [Volume]
☑ G: [Volume]
☐ H: [Volume]

Selected folders are marked by a tick. A + sign indicates that the folder contains subfolders which will not be processed, i.e. files in these subfolders will not be encrypted/re-encrypted.

By pressing the **Profile Rules** button you can automatically select all directories for which encryption files are contained in the user's profile.

When you press the **Advanced** button further settings for initial encryption become available:

Note: The settings which can be changed by the user depend on the configuration of the SafeGuard LAN Crypt Client. The security officer defines the configuration centrally.

- **Decrypt EFS encrypted files if necessary**
  If you select this option, the wizard decrypts EFS encrypted files and encrypts them again, if an encryption rule applies to them.
  If you do not select this option, the Initial Encryption Wizard will ignore EFS encrypted files. They will not be re-encrypted by SafeGuard LAN Crypt, even if an encryption rule has been specified for them.

- **Decompress NTFS compressed files if necessary**
  If you select this option, the wizard decompresses NTFS compressed files and encrypts them, if an encryption rules applies to them.
  If you do not select this option, the Initial Encryption Wizard will ignore NTFS compressed files. They will not be encrypted, even if an encryption rule has been specified for them.

- **Decrypt/re-encrypt files encrypted with several keys**
  If you select this option, the wizard decrypts files encrypted with several keys and encryptst them again, if an encryption rule applies to them. Afterwards, the files are encrypted with one key only.
  This option is only available if **Encrypt files in accordance with profile** or **Re-encrypt files in accordance with profile** was selected in step2/5. Otherwise this option is greyed out.

- **Only include the following files:**
  If you specify file types here (e.g., .txt, .doc, etc.), the initial encryption wizard only processes files of the specified type. This setting only applies to files for which an encryption rule exists.
  If there are files of different types in the directory, they will not be processed during initial encryption. They will only be encrypted when the user opens and saves them. To specify several file types, use a list separated by semicolons.

4. After clicking **Next**, you can define which files are to be included in the initial encryption report in *Step 4 / 5*. For the initial encryption report the user can select between the following options:

   - **Report errors only**
     The status report will only include files for which errors occurred during encryption.
   - **Report modified files and errors**
     The status report will include all files which have been modified and for which errors occurred during encryption.
   - **Report all files**
     The status report will include all files.

5. After clicking **Next**, the **Result** of the encryption and the **keyname** of the key used will be shown for each file in *Step 5 / 5*.

   In case encryption should have failed for individual files, you can immediately try again to encrypt those file by pressing the **Retry** button.

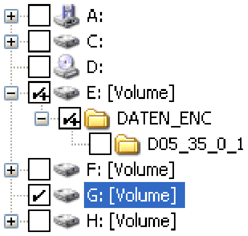
   You can sort the results alphabetically by clicking the column header. Furthermore, you can save the status report as an XML file at a file location of your choice (**Export** button). Using the status report you can later retry to encrypt the files for which encryption has failed.

   After clicking **Finish**, the wizard will be closed.

5.4.1.2 Verifying encryption state

1. After starting the wizard, select the **Verify encryption states** option in *Step 1 / 5*.

2. After clicking **Next**, you can define for which folders the encryption status is to be verified in *Step 2 / 5*.



Selected folders are marked by a tick. A + sign indicates, that the folder contains subfolders which will not be processed, and therefore the encryption state is not checked.

By pressing the **Profile Rules** button you can automatically select all directories for which encryption rules are contained in the user's profile.

By pressing the **Advanced** button you can restrict the verification to specific file types:

- **Include only the following file types:**
  If you specify specific file types here (e.g. .txt, .doc, etc.), only files of the specified type will be checked.
  If a directory also contains files of a different type (which has not been specified here), they will not be taken into account. To specify several file types, use a list separated by semicolons.

3. After clicking **Next**, the **Result** of the verification and the **keyname** of the key used will be shown for each file in *Step 3 / 5*.

   You can sort the results alphabetically by clicking the column header. Furthermore, you can save the status report as an XML file at a file location of your choice (**Export** button).

   After clicking **Finish**, the wizard will be closed.

5.4.1.3 Decrypting files

Files encrypted by SafeGuard LAN Crypt can be decrypted, if there are no longer any encryption rules applying to them. If initial encryption was required to be performed again, for example due to modified encryption rules in the user's profile, the files for which encryption rules no longer exist can be decrypted via this wizard.

To decrypt files, select the **Perform initial encryption** in *Step 1 / 5* of the wizard and the **Decrypt files with selected keys** option under *Decryption* in *Step 2 / 5*.

Afterwards you can select the keys. Only files encrypted with the keys selected will be decrypted. However, they will only be decrypted, if there is no longer any encryption rule applying to them.

Note: SafeGuard LAN Crypt only decrypts files for which no encryption rule applies.

Example:
The Initial Encryption Wizard is started because the user profile has been changed. To ensure that all files have the intended encryption state after closing the Initial Encryption Wizard, proceed as follows:

- **Enable** *Encrypt files in accordance with profile*
  All files are encrypted according to the new encryption rules.

- **Enable** *Re-Encrypt files in accordance with profile*
  If files are to be encrypted with a different key according to the new rules, the will be re-encrypted.

- **Enable** *Decrypt files with selected keys* and select **all** keys.
  Encrypted files, for which no longer any encryption rule exists, will be decrypted. SafeGuard LAN Crypt only decrypts files for which no encryption rule exists. Therefore, selecting all keys will not cause any problems.

After completing the process successfully and closing the wizard, all files have the correct encryption state.

Explicitly decrypting files can be of importance, if persistent encryption is activated. In this case, files will not be automatically encrypted when they are copied/moved from a directory for which an encryption rule applies to a directory without any encryption rule.

5.4.2 Initial encryption in Unattended mode

If you want to run the `sglcinit.exe` tool in Unattended mode, you must call sglcinit.exe from the command line with specific parameters, from the folder in which it is located (for example, C:\Program Files\Sophos\SafeGuard LAN Crypt\).

Command line syntax:

```
SGLCInit <Startpfad | %Profile>[/S]
{-DIgnoreDirectory}[/Tv][/Te][/Tr][/Td]
[/Tdk {GUID}][/Dc][/De][/Dm][+FFiletype][/V1|/V2|/V3] [/X][/LLogfile]
```

Parameter:

- `Start path`

  This results in either a single file that is to be encrypted, decrypted or re-encrypted (for example, C:\Data\sale.doc), or a folder in which encryption, decryption or re-encryption is to be performed (for example, D:\Data). The default setting is for subfolders not to be included in this process!

- `%Profile`

  This processes all the rules in the loaded encryption profile with the absolute path. Encrypts/ decrypts or re-encrypts files if necessary.

Note: Before a file can be decrypted, the profile must contain an EXCLUDE rule for it.

- `/S`

  Includes all subfolders from the start path.

- `/h` or `/?`

  Opens a window which displays help about the syntax used in sglcinit.exe.

- `-D`*`IgnoreDirectory`*

  Ignore this folder.

- `/Tv`

  Task mode: v = Shows the encryption status of the files.

- `/Te`

  Task mode: e = encrypts files, if necessary, in accordance with the encryption profile.

- `/Tr`

  Task mode: r = re-encrypts files, if necessary, in accordance with the encryption profile.

- `/Td`

  Task mode: d = decrypts files, if necessary, in accordance with the encryption profile.

- `/Tdk`

  Task mode: dk= decrypts the files that were encrypted using the pre-defined keys. You must enter the GUID for the keys.

Note: All task mode parameters can be used together in one command call.

- `/Dc`

  This option decompresses NTFS compressed files and encrypts them afterwards.
  If this option is not set, NTFS compressed files are ignored.

- `/De`

  This option decrypts EFS encrypted files and encrypts them again afterwards.
  If this option is not set, EFS encrypted files are ignored.

- `/Dm`

  This option decrypts files encrypted with several keys and encrypts them again afterwards. As a result, the files are encrypted with one key only.

- `+F`*file type*

  If you specify file types with this option (e.g., +Ftxt+Fdoc), only files of the relevant type are processed. This setting only affects files for which an encryption rule exists.
  If a directory also contains files of a different file type, that is not specified with this option, they are not taken into account during initial encryption. They will only be encrypted when the user opens and saves them.

- `/V1`

  Verbose mode 1: Only error messages are displayed.

- `/V2`

  Verbose mode 2: Outputs the files that are to be encrypted/decrypted/re-encrypted and error messages.

- `/V3`

  Verbose mode 3: Outputs all files.

- `/E`

  Stop on error.

- `/X`

  Initial encryption without displaying a window

- `/LLogfile`

  Output is also stored in the file.

Note: The /Td parameter should only be combined with %Profile when the files you want to decrypt are listed in the profile with an exclude rule. Otherwise you should use /Td together with the start path.

Example:

```
sglcinit.exe %PROFILE -DC:\ignore /S /Te /Tdk {1234ABCD-1234-1234-
1234-1234ABCD} {5678EFGH-5678-5678-5678-5678EFGH} /V1 /
LC:\logfile.xml
```

5.5 Explorer extensions

The SafeGuard LAN Crypt Explorer Extensions offer the following features:

- Initial encryption of files and directories
- Explicit encryption and decryption of files and folders
- Easy control of the encryption state of your data

SafeGuard LAN Crypt adds menu options to Windows Explorer. They appear in the context menus for drives, folders and files. In addition, a tab is added to the Windows Properties window for files. This new tab contains information about the encryption status.

You can right click on a file or directory to display the entry **SafeGuard LAN Crypt** in its context menu. Keys in different colors show the encryption state of the file:

- **Green Key**
  The file is encrypted and the user has access to the key.
- **Red Key**
  The file is encrypted and the user does not have access to the key.
- **Gray Key**
  A gray key indicates that the file is plain (unencrypted) but should be encrypted in accordance with an encryption rule in the loaded profile.
- **Yellow Key**
  If a yellow key is displayed, the file is encrypted, but the transparent encryption is currently deactivated.

Note: For files with the offline attribute (i.e., files that do not exist physically), the system does not show any key symbols.

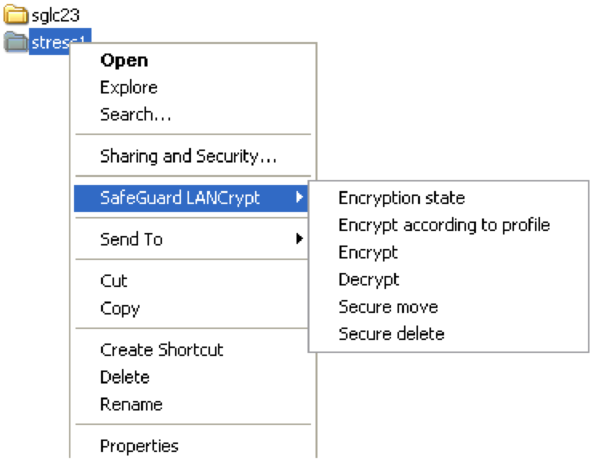
When you click the **SafeGuard LAN Crypt** entry in the context menu, the system displays a submenu containing more entries. These entries will vary, depending on whether a file or directory has been selected and also on the encryption state of the file.

Note: Key symbols are also added to folders and files in the Windows Explorer. Keys in different colors show the encryption state of the file:

- **Green Key**
  The file is encrypted and the user has access to the key.
- **Red Key**
  The file is encrypted and the user does not have access to the key.
- **Gray Key**
  A gray key indicates that the file is plain (unencrypted) but should be encrypted in accordance with an encryption rule in the loaded profile.

- **Yellow Key with question mark**
  The user does not have sufficent access rights so SafeGuard LAN Crypt is not able to determine the encryption state.

The following entries may be displayed in this menu:



For directories

- **Encryption state**

  If you click this entry you display a list of all files in this directory and their encryption state (colored keys). Only files on the first directory level are displayed. To display files in a subdirectory, first go to that subdirectory. In Explorer folders for which an encryption rule is present are identified by their key icon.

- **Encrypt according to profile**

  Encrypts all files in the directory according to the loaded encryption profile. Subdirectories with an existing encryption rule are also included in the encryption.
  A progress bar shows you how long the initial encryption is likely to take. You can also see the total number of files in the folder and how many of them have already been encrypted. You can also see the path of the file that is currently being encrypted.

- **Encrypt**

  Encrypts all files in the directory, using a key available in the active encryption profile. A list of the available keys is displayed, from which the key to be used to encrypt all files can be selected.

- **Decrypt**

  Decrypts all files in the first directory level. Therefore, all relevant keys need to be available in the active encryption profile. If a key is missing, the files that use that key remain encrypted.

- **Secure move**

  When moving a folder via SafeGuard LAN Crypt, files contained in this folder are encrypted, decrypted or re-encrypted at the new location according to the encryption rules applying. The source files are wiped after being moved.

- **Secure delete**

  Using this command, the storage locations of the files are overwritten several times. The files cannot be restored via the Windows Recycle Bin.

For individual files:

- **Encryption state**

  Shows the file's encryption status. For encrypted files, a popup information box shows the key used to encrypt them along with additional information about whether the user is entitled to use this key.
  If another user is logged on, but is not entitled to use this key, the GUID appears in the infobox instead of the key name.
  You can identify encrypted files in Explorer by the small green key icon shown next to them.
  If the user clicks on *Folder Options/View/More Options* they can specify whether or not the file encryption status and the folder encryption status are to be displayed for their profile. The changes they make to these settings do not become effective until they log off and then log on again.

- **Encryption according to profile**

  Encrypts a file in accordance with the currently loaded encryption profile. This entry only appears in the Context menu if a file's encryption status does not match the encryption profile.

- **Encrypt**

  Use this to encrypt a specific individual file. A list of the available keys is displayed, from which the key to be used for encryption can be selected.

- **Decrypt**

  Decrypts the selected file. Therefore, the correct key needs to be available in the active encryption profile, or else the file remains encrypted.

- **Secure move**

  This command is used to encrypt, decrypt or re-encrypt files according to the loaded encryption rules, when files are moved to a new location. The source files are wiped after being moved.

- **Secure delete**

  Using this command, the storage locations of the files are overwritten several times. The files cannot be restored via the Windows Recycle Bin.

Note: Active encryption rules always take priority over explicit encryption/decryption that has been performed using the **Encrypt/Decrypt** command. If you are trying to encrypt/decrypt files for which an encryption rule defines something different, your command will not be executed and an error message will be displayed.
The following situations cause an error message when the user tries to encrypt files using the context menu:

- the directory contains files which are encrypted using an unknown key
- the user tries to encrypt/decrypt a file in contradiction of its encryption rule (e.g. a different key than the one used in the encryption rule is selected)

5.5.1 Encryption information

In addition, an *Encryption State* tab is added to the Windows *Property* dialog. This tab displays information about the encrypted file.

5.6 Deactivating/activating transparent encryption

If transparent encryption is deactivated in the SafeGuard LAN Crypt User menu, the consequence is that the files that are accessed after deactivation of transparent encryption will no longer be encrypted and decrypted automatically. Newly-generated files also remain unencrypted, even if the user's encryption profile includes an encryption rule for them.

Note: The consequences of deactivating transparent encryption may be important if encrypted files should normally stay encrypted when they are copied/moved to a location without encryption rules (e.g. if encrypted files should be attached to an e-mail, or copied to a CD). According to the philosophy of SafeGuard LAN Crypt, these files would be decrypted when copied/moved to this folder.

In contrast, if the administrator has activated the *persistent encryption* function, files automatically remain encrypted even if they are moved to a folder using the Windows Explorer for which no encryption rule is present. If persistent encryption is used in the cases described above, it is no longer necessary to deactivate transparent encryption first. Persistent encryption ensures that files remain encrypted even if they are moved to another folder by mistake or if the user has forgotten to deactivate encryption before moving or copying them. You must reboot the client computer before changes to the status of persistent encryption (active or not active) come into effect.

Note: If persistent encryption is active and a user moves or copies a file into a folder to which an ignore or exclude rule applies, they receive a warning message that this will result in the file being decrypted.

5.6.1 Transparent encryption and file-compression tools

File-compression tools open files, read the file contents and compress it. If transparent decryption/encryption is enabled, file-compression tools will receive the decrypted files and the files will be compressed. The files in the resulting archive are no longer encrypted.

If the archive is stored in a directory for which no encryption rule exists, all files are now stored in plain.

Even if persistent encryption is enabled, the files will not be compressed in encrypted form as persistent encryption only refers to copying/moving files in Windows Explorer.

To ensure that files will be compressed in encrypted form by file-compression tools, transparent encryption has to be deactivated during the use of those tools.

Another way to ensure that files are compressed in an encrypted format is to define file-compression tools as Unhandled Applications. This has to be done by the security officer.

5.7 Compatibility with older versions

If you want to run the new SafeGuard LAN Crypt 3.71 software alongside older versions, you must take these points into consideration:

- The SafeGuard LAN Crypt 3.71 Client can only load profiles that were created with Version 3.60 of SafeGuard LAN Crypt Administration.
- Older SafeGuard LAN Crypt Clients can use profiles and rules created with Version 3.60. (However, there are some exceptions to this, for example, rules created with Japanese Unicode, because this function is not supported prior to version 3.60).
- SafeGuard LAN Crypt Clients older than version 3.50 cannot read files that are encrypted with the 3.50 or higher Client versions.The new Client can also be configured in such a way that it can be used to encrypt files that are in the old format.
- However, the new SafeGuard LAN Crypt 3.71 Client can read files that were encrypted with older clients.

5.8 Uninstalling the Client

You uninstall the SGLC Client in the Control Panel, in Windows:
Select Start/Control Panel/Add or Remove Programs and then select the entry for *SafeGuard LAN Crypt Client*. Then click *Remove*.

In both cases you will then need to reboot your computer to make the changes effective.

Note: Any files that have been encrypted with SafeGuard LAN Crypt cannot be decrypted, once the SGLC Client has been uninstalled.

5.9 Appendix: Error messages displayed when the profile is loading

If problems occur while the profile is loading, the SGLC Client warns the user by displaying one of the following error messages, to tell them the cause:

- User certificate not found.
- LAN Crypt Security Officer certificate not found!
- Problem loading the certificates - process interrupted ...
- Error while checking the user certificate.
- User certificate expired or not yet valid.
- LAN Crypt Security Officer certificate expired or not yet valid.
- User certificate removed.
- LAN Crypt Security Officer certificate has been cancelled.
- Error while checking the LAN Crypt Security Officer certificate.
- Cannot copy User profile "%s" into local cache folder "%s"!
- Error while loading the Key Management key.
- This version of the policy file is not supported.
- Could not find or check certificate issuer.
- Could not find or check master certification location of certificate.
- Revocation status of certificate is unknown. CRL not found or expired.
- The user certificate does not have the necessary key usage extensions.
- The user certificate has extensions that are not supported.
- The user certificate is linked with the Microsoft Base Cryptographic Service Provider, which is not supported.
- The PIN entered may be incorrect!
- Could not find or check LAN Crypt Security Officer certificate issuer.
- Could not find or check master certification location of LAN Crypt Security Officer certificate.
- Revocation status of the LAN Crypt Security Officer certificate is unknown. CRL not found or expired.
- The LAN Crypt Security Officer certificate does not have the necessary key usage extensions.
- The LAN Crypt Security Officer certificate has extensions that are not supported.
- Cannot decrypt policy file.
- Failed to download the policy file.

6 Legal Notices

You will find copyright information on third party suppliers in the file entitled *3rd_Party_Software.rtf* in your product directory.

7 Technical Support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk forum at http://community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at http://www.sophos.com/support/
- Download the product documentation at http://www.sophos.com/support/docs/
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.