conpal LAN Crypt

Persistent
Highly secure
Scalable

Client help

Product version: 3.97
Document date: May 2019

Contents

1 What is SafeGuard LAN Crypt?

SafeGuard LAN Crypt enables confidential file exchange, using transparent file encryption, for groups of trusted users in large organizations. SafeGuard LAN Crypt works without user interaction. It supports the role of a security officer (SO) who is able to restrict the access rights to SafeGuard LAN Crypt-encrypted files. A master security officer (MSO) can delegate the right to administer SafeGuard LAN Crypt. You can establish a hierarchy of security officers (SOs), to meet the security requirements of your company.

Encrypted files are not assigned to individual users. Any user who has the correct key can work with an encrypted file. This allows administrators to create logical user groups that 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.

Every time a user moves a file into a directory, that has been defined as an encrypted directory, the file is encrypted on their computer. Every time another trusted user in the same group reads the same file from this directory, it is transferred to them in encrypted form. The file is only decrypted on the recipient's computer. The user can modify it there. The file is encrypted again before being transferred back to the encrypted directory.

Unauthorized users may be able to access these encrypted files (only from workstations without SafeGuard LAN Crypt), but without SafeGuard LAN Crypt authorization, they can only see the encrypted content. 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.

1.1 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 or decryption is performed in the RAM on the client workstation. All encryption or decryption tasks run transparently on the client workstation with minimal user interaction. There is no need to install special security software on the file server itself.

A Security Officer can define different access rights for directories and files. These rights are grouped into encryption profiles for the users. Encryption profiles are distributed via policy files. Policy files include all the rules, access rights and keys required for transparent encryption. The policy file is secured via a certificate. Before a user can start working with encrypted data using the SafeGuard LAN Crypt software installed on the client workstation, they need to be able to access the policy file. The user can access the policy file containing the encryption profile by owning the private key assigned to the certificate.

SafeGuard LAN Crypt allows trusted users to be organized into different trusted groups. 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. All organizational forms can be mapped using trusted groups from a centralized LAN model, in which users are administered centrally, to a remote model in which users work on notebooks.

1.2 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. See the SafeGuard LAN Crypt release notes for information on the supported versions.

The SafeGuard LAN Crypt **Client status** dialog displays all encryption rules, which are valid on the computer, see The Client status dialog *(page 19)*. In general SafeGuard Enterprise Data Exchange rules are applied first and then the SafeGuard LAN Crypt rules are applied. Prioritization can be changed.

Note: For **Persistent Encryption**, always the setting of SafeGuard Enterprise applies. This cannot 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, see The Initial Encryption Wizard *(page 10)*. 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.

2 Encryption

2.1 Transparent encryption

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

Encryption is governed solely by encryption rules - it does not depend on directories. Encryption works as follows:

- 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. The security officer can define different encryption rules for different file extensions or names in the same directory.
- When renaming encrypted files, they remain encrypted (unless there is no, or no other, encryption rule for the new file name/file extension).
- When a user copies or moves encrypted files to a location where the current encryption rule is no longer valid, these files are decrypted.

  Note: An exception to this is when a user moves files from one directory to another on the same network share. In this case the files remain encrypted although no encryption rule is valid.

- If the security officer has activated **Persistent Encryption**, files also remain encrypted if they are moved to a location for which no encryption rule applies.
- When a user copies or moves encrypted files to a location where a different encryption rule is valid, the files are decrypted and then encrypted again using the key defined for this location.

2.1.1 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 The Client status dialog *(page 19)*.

2.1.2 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. However, if the security officer has activated the **Persistent Encryption function**, these files remain encrypted.

Secure Move

SafeGuard LAN Crypt supports the secure movement of files and directories. When the user moves files using 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 **SafeGuard LAN Crypt** > **Secure Move** command from the Windows Explorer context menu.

2.1.3 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.
- the user must have the right key.
- the active encryption profile does not include an encryption rule for the new location.
- **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. Release notes supplied with the SafeGuard LAN Crypt Client will give you more specific information about known problems with virus scanners.

2.1.4 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 they 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. For emptying the Recycle Bin no key is necessary.

2.1.5 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
- Policyfile cache

Location is specified in SafeGuard LAN Crypt Administration and displayed on the **Profile** tab of the **Status** dialog.

- Root directory of the System drive. Subfolders are not excluded
- Indexed Locations (search-ms)

2.1.6 Persistent Encryption

For SafeGuard LAN Crypt a security officer can configure **Persistent Encryption**. Files usually only remain encrypted for as long as they are subject to an encryption rule.

For example, if a user copies an encrypted file into a folder for which no encryption rule has been defined, the file will be decrypted in the target folder. By activating **Persistent Encryption** you can ensure that files remain encrypted even when they are moved or copied.

To avoid unintended creation of plain copies of encrypted files, copies of encrypted files will be created encrypted even if created in locations not covered by an encryption rule.

Security officers can disable this behavior in SafeGuard LAN Crypt Configuration. If disabled, files are unencrypted when they are copied/moved to a location not covered by an encryption rule.

For **Persistent Encryption** the following rules apply:

- The SafeGuard LAN Crypt driver only keeps the name of the file without any path information. Only this name can be used for comparison and therefore will only catch situations where the name of the source and the target file is identical. If the file is renamed during the copy operation, the resulting file is considered to be a 'different' file and thus not subject to the **Persistent Encryption**.
- When a user saves an encrypted file with **Save As** under a different file name in a location not covered by an encryption rule, the file will be unencrypted.
- Information about files is kept for a limited time only. If the operation takes too long (more than 15 seconds), the newly created file is considered to be a different, independent file and thus not subject to the **Persistent Encryption**.

2.1.6.1 Persistent Encryption vs. encryption rule

Persistent Encryption tries to ensure that an encrypted file retains its encryption state, for example its original encryption key. This works well if the file is relocated to a folder with no applicable encryption policy. If the file is copied or moved to a location where an encryption policy applies, the encryption policy has higher priority and thus overrules **Persistent Encryption**. The file is encrypted with the key defined in the encryption rule and not with the original encryption key

2.1.6.2 Persistent Encryption vs. Ignore path rule

An Ignore path rule overrides **Persistent Encryption**. This means that encrypted files that are copied to a folder with an applicable Ignore path are decrypted.

An Ignore path rule is primarily used for files that are accessed very frequently, and for files that do not have a particular reason to be encrypted. This improves system performance.

2.1.6.3 Persistent Encryption vs. Exclude path rule

An Exclude path rule overrides **Persistent Encryption**. This means encrypted files that are copied to a folder with an applicable Exclude path are decrypted.

2.1.7 Limitations on Persistent Encryption

Persistent Encryption has some limitations. These are:

Files that are supposed to remain plain are encrypted

- **Unencrypted files are copied to multiple locations with and without applying encryption rules**

If an unencrypted file is copied to several locations at the same time, with one location having an encryption rule applied, all copies of that file might be encrypted too.

If an unencrypted file is copied to an encrypted location the file is added to the encryption tool's internal list. When a second copy of the file is created, the encryption tool finds the file name in its list and also encrypts the second copy.

- **Create a file with the same name after accessing an encrypted file**

  If an encrypted file is opened (accessed) and a new file with the same name is created shortly afterwards, the newly created file is encrypted with the same key as the first file.

  Note: This only applies if the same application/thread is used for reading the encrypted file as well as creating the new one.

  For example: In Windows Explorer right-click in a folder with an encryption rule and click **New** > **New Textdocument**. Immediately right-click in a folder without an encryption rule and click **New** > New Textdocument. The second file is also encrypted.

Files are not encrypted

- **Multiple copies of a file are created**

  If copies of an encrypted file are created in the same folder as the original file, these copies are not encrypted. Since the created copies have different file names (for example doc.txt vs. doc - Copy.txt) the matching of the file name fails and therefore they are not encrypted by Persistent Encryption.

2.1.8 Client API and encryption tags for DLP products

If a Data Loss Prevention (DLP) product identifies data that needs to be encrypted, it can use the SafeGuard LAN Crypt Client API to encrypt these files. In **SafeGuard LAN Crypt Administration**, you can define different encryption tags that specify the SafeGuard LAN Crypt key to be used. The Client API can use these predefined encryption tags in order to apply special keys for different content. For example, the encryption tag **<CONFIDENTIAL>** to encrypt all files that are categorized as confidential by your DLP product.

2.2 Deactivating/activating transparent encryption

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

Note: Deactivating transparent encryption can have consequences if encrypted files should normally stay encrypted when they are copied or moved to a location without encryption rules (e.g. if encrypted files are attached to an e-mail, or copied to a CD). These files will now be decrypted when copied or moved to a location without encryption rules.

If you have activated the **Persistent Encryption** function, files automatically remain encrypted even if they are moved to a folder for which no encryption rule is present. If **Persistent Encryption** is used, you don't need 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, this will result in the file being decrypted.

2.3 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 stored files are decrypted.

If **Persistent Encryption** is enabled, the files will not be compressed in encrypted form.

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.

Alternatively, the security officer can define file-compression tools as Unhandled Applications to ensure that files stay encrypted when they are compressed.

2.4 Initial encryption and explicit encryption

After SafeGuard LAN Crypt has been installed, you need to perform initial encryption process. 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, see User application *(page 18)*
- SafeGuard LAN Crypt Explorer extensions, see Explorer extensions *(page 20)*
- the **sglcinit.exe** tool, which also supports Unattended mode, Initial encryption in Unattended mode *(page 14)*.

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.

2.4.1 The Initial Encryption Wizard

The initial encryption tool, **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

- by clicking the Systray icon or
- by going to Start/All Programs/Sophos/SafeGuard LAN Crypt/Initial encryption or
- by launching it from the Windows 8/Windows 2012 Start screen or
- by double-clicking on sglcinit.exe in the SafeGuard LAN Crypt Program folder.

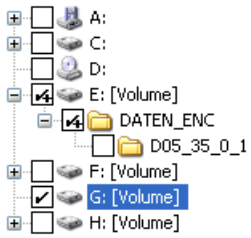
Note: The encryption, decryption and re-encryption processes are always performed in accordance with the encryption profile. That is why you have to load an encryption profile.

2.4.1.1 Performing initial encryption

1. Start the wizard, see User menu *(page 18)*.
2. Select the Perform initial encryption option in Step 1 / 5.
3. Click **Next**.
4. Now define how files are to be handled in Step 2 / 5.
   a. **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.
   b. **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.

   Note: 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 you 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 you can choose to re-encrypt these files using the Initial Encryption Wizard. This will re-encrypt these files according to the SafeGuard LAN Crypt encryption rules.
5. Click **Next**.
6. Select which folders are to be encrypted/re-encrypted via a directory tree structure in Step 3 / 5:



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.

Click **Profile Rules** to automatically select all the directories for which the user's profile contains encryption rules.

Click **Advanced** to access extra options:

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**

  Select this option to decrypt and re-encrypt EFS encrypted files. Note an encryption rule must apply 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**

  Select this option to decompress NTFS compressed files and encrypt them. Note an encryption rule must apply 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**

Select this option to re-encrypt files that were encrypted with several keys. The files are encrypted with one key only. Note an encryption rules must apply to them.

This option is only available if **Encrypt files in accordance with profile** or **Re-encrypt files in accordance with profile** was selected in step 2/5. Otherwise this option is greyed out.

- **Include only the following file types:**

Select the file types to which you want to restrict the initial encryption process (for example .docx, .rtf). 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.

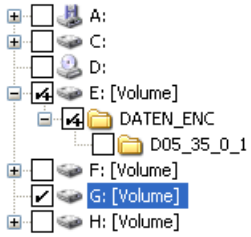
7. Click **Next**.
8. Now define which files are to be included in the initial encryption report in Step 4 / 5. For the initial encryption report the user can select between the following options:
   a. **Report errors only**
   The status report will only include files for which errors occurred during encryption.
   b. **Report modified files and errors**
   The status report will include all files which have been modified and for which errors occurred during encryption.
   c. **Report all files**
   The status report will include all files.
9. Click **Next**.
   The **Result** of the encryption, the **keyname** of the key used and the encryption algorithm will be shown for each file in Step 5 / 5.

   In case encryption has 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.
10. Click **Finish**.
    The wizard will be closed.

2.4.1.2 Verifying encryption state

1. Start the wizard.
2. Select the **Verify encryption states** option in Step 1 / 5
3. Click **Next**.
4. Select the folders you want to verify in Step 2/5.



5. Select folders by marking with a tick.

   A + sign indicates, that the folder contains subfolders which will not be processed, and therefore the encryption state is not checked.

Click **Profile Rules** to automatically select all the directories for which the user's profile contains encryption rules.

Click **Advanced** to 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.

6. Click **Next**.

   The **Result** of the verification, the **keyname** of the key used and the encryption algorithm will be shown for each file in Step 3 / 5

   You can sort the results alphabetically by clicking the column header.

   Click **Export** to save the status report. as an XML file at a file location of your choice.

7. Click **Finish**.
   The wizard will be closed.

2.4.1.3 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:

1. Select **Perform initial encryption** in Step 1 / 5 of the wizard.
2. Under **Decryption** in Step 2 / 5, select **Decrypt files with selected keys**.
3. 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:

1. Enable **Encrypt files in accordance with profile**.

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

   If files are to be encrypted with a different key according to the new rules, they will be re-encrypted.
3. Enable **Decrypt files with selected keys** and then 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 decrypted when they are copied/moved from a directory for which an encryption rule applies to a directory without any encryption rule.

2.4.2 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 <startpath | %Profile>[/S]
{-DIgnoreDirectory}[/Tv][/Te][/Tr][/Td]
[/Tdk {GUID}][/Dc][/De][/Dm][+FFiletype][/V1|/V2|/V3|/V4] [/X]
[/LLogfile]
```

Parameters:

- **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**

  Processes all rules with an absolute path in the loaded encryption profile. 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.

- **-DIgnoreDirectory**

  Ignores this folder

- **/Tv**

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

- **/Te**

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

- **/Tr**

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

- **/Td**

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

- /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.

- **+Ffile 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.

- **/V0**

  Verbose mode 0: No reporting.

- **/V1**

  Verbose mode 1: Lists error messages.

- **/V2**

  Verbose mode 2: Lists modified files.

- **/V3**

  Verbose mode 3: Lists all files.

- **/V4**

  Verbose mode 4: Lists plain files.

- **/E**

  Stop on error

- **/X**

  Initial encryption without displaying a window

- **/LLogfile**

  Writes output to the specified 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.

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

sglcinit.exe D:\data /S /V4

Lists all plain files in D:\data and its subfolders.

3 Policies

3.1 Certificates

Before users can access their encryption profile, the corresponding certificate must be available on the computer. The security officer distributes 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 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 so 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 users attempt 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.

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.

3.2 Loading the policy file

SafeGuard LAN Crypt default behavior

When a user logs on to Windows, their cached profile is loaded first. SafeGuard LAN Crypt 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 or web server via http/https). If a new policy file is found, the cached user profile is updated.

The user can start working with encrypted files while SafeGuard LAN Crypt checks whether a new version of the policy file exists. If the specified location 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 default behavior using central settings. Security officers can specify for how long the cached policy is valid on client computers. 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 *(page 19)*.

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 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 is unloaded. The user can no longer access encrypted data.

The policy file is 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 the security officers can 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. They can prevent users from working with the same policy files for an unlimited time period. Note if this option is set to **not configured** a user can continue working with a cached version of the policy file for an unlimited time period.

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 User menu *(page 18)*.

Policy files are not cached

A security officer can specify that the policy file will not be cached. This means that users receive their 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.

3.3 Logon to SafeGuard LAN Crypt

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. An encryption profile can only be loaded, if the user owns the corresponding certificate.

The path to the policy files is written to a client machine's registry by the system administrator. When a user logs on to SafeGuard LAN Crypt, the encryption profile, which is stored in policy files, is loaded onto the client machine. SafeGuard LAN Crypt loads the policy files from the defined directory and checks, whether the user is allowed to load it, by verifying the user's certificate.

Logon with token

Users 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 is 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 is 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**. The token is identified and the user is logged on. To avoid this, a delay for loading the profiles can be specified in **SafeGuard LAN Crypt Configuration** (setting **Delay when loading profiles**).

4 User application

The status of SafeGuard LAN Crypt is represented by a key icon in the Windows task bar.

- **Green** means:

  Encryption rules loaded, transparent encryption activated.
- **Yellow** means:

  Encryption rules loaded, transparent encryption deactivated.
- **Red** means:

  No profile loaded.

4.1 User menu

Right-click on the key icon to open the SafeGuard LAN Crypt user menu offering the following options:

- **Load encryption rules/Update encryption rules**
- **Clear encryption rules**
- **Deactivate/Activate encryption**
- **Show profile**
- **Client status**
- **Initial encryption**
- **Close**
- **About**

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

- **Load encryption rules/Update encryption rules**

  This option loads the currently valid encryption rules. This is important if the profile has been changed during runtime.
- **Clear encryption rules**

  This option prevents access to encrypted data. This is a security option that secures encrypted data against unauthorized access when the workstation is unattended. Note the use of the private key must be secured with 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.
- **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 Show Ignore Rules, Show Exclude Rules and Show encryption tags 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** option uses several tabs to display detailed information about the current status of the SafeGuard LAN Crypt Client, see The Client status dialog *(page 19)*.

- **Initial encryption**

  Starts the wizard that will encrypt all files using the loaded encryption profile, see Initial encryption and explicit encryption *(page 10)*.

- **Close**

  Closes the SafeGuard LAN Crypt User Application.

- **About**

  Displays information about your current version of SafeGuard LAN Crypt

Note: The **Close** option 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).

4.2 The Client status dialog

The **Client status** option displays several tabs that provide information on the encryption settings for a user's machine. These are:

- **Status**

  This tab shows whether the user profile has been loaded and encryption is active. It also displays 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 User menu *(page 18)*, command **Deactivate/Activate encryption**.

- **Settings**

  This tab provides information on the settings that currently apply to the client. These settings are defined centrally 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 options to be available on the client computers.

- **Profile**

  This tab shows the settings for the user profile.

- **Certificates**

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

- **Keys**

  This tab shows information on all keys available for the currently loaded profile.

- **Rules**

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

- **Unhandled**

  This tab 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 that require a special approach by SafeGuard LAN Crypt due to their behavior.

  - **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.

- **Client API**

  This tab shows the settings for the Client API and list all applications that are allowed to use it.

- **Trusted Vendors**

  If Client API access is restricted to applications signed by trusted vendors, these vendors must be registered in SafeGuard LAN Crypt Administration. All registered trusted vendors and corresponding certificate information are listed on this tab.

- **Export** button

  Use the **Export** button to export the current client settings to an XML file.

  This way, support teams can be easily provided with important configuration information.

4.3 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.

- **Yellow Key with question mark**

  The user does not have sufficient access rights so SafeGuard LAN Crypt is not able to determine the encryption state.

Note: For files with the offline attribute (e.g., 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 sub-menu 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**

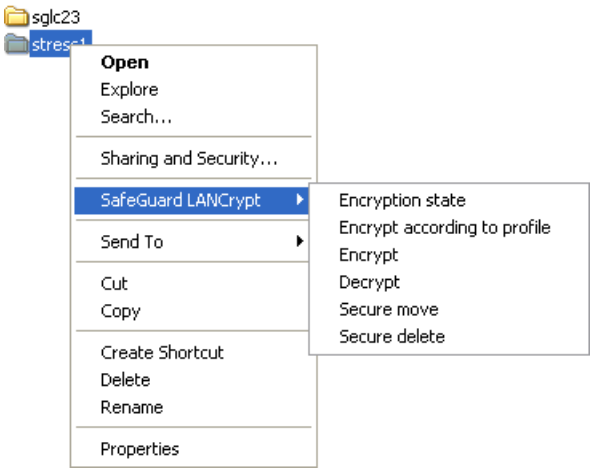
  The file is encrypted and the user has access to the key.
- **Red Key**

  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 sufficient access rights so SafeGuard LAN Crypt is not able to determine the encryption state.

The following entries may be displayed in this menu:



4.3.1 Menu options for directories

- **Encryption state**

  This option displays 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**

  This option encrypts all the 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**

  This option encrypts all the 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**

This option decrypts all the files on 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**

  This option writes over the storage locations of the files several times. The files cannot be restored via the Windows Recycle Bin.

4.3.2 Menu options for individual files

- **Encryption state**

  This option 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**, 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.

- **Encrypt according to profile**

  This option 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**

  This option encrypts the selected file. A list of the available keys is displayed, from which the key to be used for encryption can be selected.

- **Decrypt**

  This option decrypts the selected file. The correct key needs to be available in the active encryption profile, or else the file remains encrypted.

- **Secure move**

  This option encrypts, decrypts or re-encrypts the selected file according to the loaded encryption rules, when files are moved to a new location. The selected source file is deleted after being moved.

- **Secure delete**

  This option writes over the storage locations of the selected file several times. The file cannot be restored via the Windows Recycle Bin.

Note: Active encryption rules always take priority. If the user tries to encrypt/decrypt files for which an encryption rule defines something different, their command is not executed and an error message is displayed.

The following situations cause an error message when a user tries to encrypt files using the menu options:

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

4.3.3 Encryption information

In the **Properties** dialog, the **Encryption state** tab displays information about the encrypted file.

5 Terminal Server

This version of SafeGuard LAN Crypt supports Windows Terminal Servers and Citrix Terminal Servers. For details on the supported versions refer to the SafeGuard LAN Crypt release notes.

5.1 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.

5.2 Installation on a Terminal Server environment

In general the installation procedure has to be carried out the same way as in non Terminal Server environments, see Installation and upgrade *(page 24)*.

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

Note:

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

5.3 Restrictions

Citrix

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

- Citrix Streamed Applications are not supported.

6 Installation and upgrade

Note: SafeGuard LAN Crypt can only be installed with Windows administrator privileges. For upgrading from older versions simply install the new client version.

1. Double-click on one of the .msi files in the Install folder of your unzipped installation package.
   a. sglc_x64.msi for installation on a 64bit operating system or
   b. sglc.msi for installation on a 32bit operating system.

2. Click **Next**.
   The **License Agreement** dialog is displayed.

3. Select **I accept the license agreement** in the **License Agreement** dialog. Otherwise, it is not possible to install SafeGuard LAN Crypt!

4. Click **Next**.
   The **Destination Folder** dialog is displayed.

5. Select where to install SafeGuard LAN Crypt.

6. Click **Next**.
   The **Select Installation Type** dialog is displayed.

7. In this dialog, you select which components of SafeGuard LAN Crypt are to be installed.
   a. **Typical**: Installs the most commonly used application functions of SafeGuard LAN Crypt Client.
   b. **Complete**: Complete client installation
   c. **Custom**: Lets the user select the different components.

8. 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 Applications**

       Installs the SafeGuard LAN Crypt user application, see User application *(page 18)*.

     - **Client API**

       Used to access SafeGuard File Encryption functionality through an API.

       Note: You must install the Client API to enable DLP products to access data using the SafeGuard LAN Crypt Client API.

9. Select which components are to be installed and click **Next**.

10. Check your entries again and click **Next** to start the installation.

11. If the installation is successful, a dialog appears in which you can click the **Finish** button to complete the installation process.

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

6.1 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.

6.2 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**

6.3 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 parameters

/Lvx* <path + filename>

Logs the complete installation procedure in the location specified under <path + filename>.

NOOVERLAY=1

Disables overlay icons for files and folders.

Note: Users can enable overlay icons after installation. If the users click on **Folder Options > View** 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.

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.

6.4 Removing SafeGuard LAN Crypt Client

You can only remove the SafeGuard LAN Crypt Client if you have Windows administrator privileges.

Go to **Control Panel** > **Programs** > **Programs and Features**, uninstall the client and reboot your computer.

Note: Encrypted files can no longer be decrypted after SafeGuard LAN Crypt Client has been removed.

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

7 Technical support

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

- At https://support.conpal.de registered customers with active maintenance contracts get access to downloads, documentation and knowledge items.
- Download the client product documentation at

  https://docs.lancrypt.com/de/client/sglc_397_hdeu.pdf in German language, at
  https://docs.lancrypt.com/en/client/sglc_397_heng.pdf in English language and at
  https://docs.lancrypt.com/fr/client/sglc_397_hfra.pdf in French language.
- Download the admin product documentation at

  https://docs.lancrypt.com/de/admin/sglc_397_ahdeu.pdf in German language, at
  https://docs.lancrypt.com/en/admin/sglc_397_aheng.pdf in English language and at
  https://docs.lancrypt.com/fr/admin/sglc_397_ahfra.pdf in French language.
- As a registered maintenance customer send an email to support@conpal.de , including your conpal software version number(s), operating system(s) and patch level(s), and the text of any error messages.

8 Legal notices

You find copyright information on third party suppliers in the *3rd Party Software* document in your product directory.