

c-onpal LAN Crypt



smart
highly secure
persistent

Admin help

Product version: 3.97
Document date: May 2019

Contents

1 What is SafeGuard LAN Crypt?	7
1.1 Data protection using SafeGuard LAN Crypt.....	8
1.2 Transparent encryption.....	9
1.2.1 Accessing encrypted data.....	9
1.2.2 Renaming or moving directories.....	9
1.2.3 Explicit file decryption.....	10
1.2.4 Deleting encrypted files - Windows Recycle Bin.....	10
1.2.5 Files/directories excluded from encryption.....	10
1.2.6 Persistent Encryption.....	11
1.3 Architecture.....	12
1.3.1 SafeGuard LAN Crypt Administration.....	13
1.3.2 SafeGuard LAN Crypt Client.....	14
2 Getting started	15
2.1 Certificates.....	15
2.1.1 Security levels.....	15
2.1.2 Certificate verification.....	17
2.1.3 Smartcard readers.....	17
2.2 Installation.....	17
2.3 Unattended installation.....	18
2.3.1 Components to install.....	18
2.3.2 Command Line Syntax.....	18
2.4 Upgrading.....	19
2.4.1 Installing the new version.....	19
2.4.2 Upgrading the existing SafeGuard LAN Crypt database structure.....	19
2.4.3 Upgrade wizard.....	20
2.4.4 Server logon credentials for versions below 3.61.....	20
3 Administration	21
3.1 Required steps.....	22
3.2 Preparations for administering SafeGuard LAN Crypt.....	22
3.2.1 Installing the supplied database system.....	23
3.2.2 Adding a data source (ODBC).....	24
3.2.3 Creating tables in the SafeGuard database.....	25
3.3 Master Security Officers.....	25
3.4 Administration: overview.....	26

3.4.1 Confirmations.....	26
3.4.2 User settings.....	27
3.5 Central settings.....	28
3.5.1 The Algorithms tab.....	28
3.5.2 The Keys tab.....	29
3.5.3 The Certificates tab.....	29
3.5.4 The Resolving Rules tab.....	30
3.5.5 The Server tab.....	32
3.5.6 The Directories tab.....	34
3.5.7 The Regions tab.....	37
3.5.8 The Configurations tab.....	37
3.5.9 The Additional Authorization tab.....	38
3.5.10 The Recovery Keys tab.....	39
3.5.11 The Database tab.....	40
3.5.12 The Database tab.....	41
3.5.13 The Antivirus tab.....	42
3.5.14 The Client API tab.....	42
3.5.15 The Trusted Vendors tab.....	43
3.5.16 The Other Settings tab.....	43
3.6 Displaying all SafeGuard LAN Crypt keys.....	43
3.6.1 Finding keys.....	44
3.7 Showing selected users and certificates.....	44
3.8 Creating a Security Officer.....	45
3.8.1 Granting/editing global permissions.....	47
3.8.2 Permissions for changing the settings for a Security Officer.....	48
3.8.3 All rights for groups/OUs of a specific Security Officer.....	50
3.8.4 Changing or renewing MSO or SO certificates.....	50
3.9 Logging on to Administration.....	51
3.10 Importing groups and users.....	51
3.10.1 Importing groups and users from a file.....	52
3.10.2 Icons in the Administration system.....	54
3.10.3 Selecting import source.....	54
3.10.4 Preparing for transfer into the SafeGuard LAN Crypt Database.....	55
3.11 Assigning SOs to organizational units.....	59
3.11.1 Parent group of a user.....	60
3.11.2 Allowing a Security Officer to see and edit groups.....	60

3.11.3 Granting the SO permissions to process the groups.....	62
3.12 Properties of groups.....	63
3.12.1 The Properties tab.....	63
3.12.2 The Member of tab.....	64
3.12.3 Adding SOs.....	65
3.13 Properties of users.....	65
3.14 Security environment design.....	66
3.15 Generating keys.....	66
3.15.1 Specific keys.....	68
3.15.2 Importing Keys.....	69
3.15.3 Making Keys Active/inactive.....	69
3.15.4 Relations between keys.....	69
3.15.5 Removing keys from a group.....	70
3.15.6 Deleting keys from the database.....	70
3.15.7 Editing keys.....	71
3.16 Encryption rules.....	71
3.16.1 Encryption paths.....	72
3.16.2 Keys.....	73
3.16.3 The sequence of encryption rules.....	73
3.16.4 Generating encryption rules.....	73
3.16.5 Find a specific key.....	75
3.17 Encryption tags.....	76
3.18 Assigning certificates.....	77
3.18.1 Assigning a certificate to a user.....	77
3.18.2 Generating and assigning SafeGuard LAN Crypt certificates.....	78
3.18.3 Certificate Assignment Wizard.....	79
3.19 Providing encryption rules - generating policy files.....	82
3.19.1 Creating (resolving) policy files for an entire group or selected users.....	82
3.19.2 Selected provision via the Certificate snap-in.....	83
3.19.3 Clearing profiles.....	84
3.20 Database logging.....	84
3.20.1 Settings.....	85
3.20.2 Logged events.....	85
3.20.3 Viewing and exporting entries.....	85
3.20.4 Filtering events.....	86
3.20.5 Archiving, deleting, checking entries.....	86
4 SafeGuard LAN Crypt Configuration.....	88

4.1 Client settings.....	88
4.1.1 Allow Encrypt/Decrypt.....	88
4.1.2 Ignore during Certificate Verification.....	88
4.1.3 Use Novell Name.....	89
4.1.4 Resolve all environment variables.....	89
4.1.5 Enabled Menu Entries.....	89
4.1.6 Default Ignore Rules.....	90
4.1.7 Security Officer Certificate Client Location.....	90
4.1.8 Keyfile Client Location.....	90
4.1.9 Policyfile Client Location.....	90
4.1.10 Policyfile Cache Directory.....	91
4.1.11 Delay when loading profiles.....	91
4.1.12 File types for the Initial Encryption Wizard.....	91
4.1.13 Cached Policyfile lifetime.....	92
4.1.14 NTFS Decompress Files.....	93
4.1.15 EFS Decrypt Files.....	93
4.1.16 Profile Update Interval.....	93
4.1.17 Silent mode if user profile is missing.....	94
4.1.18 Silent mode if user profile is missing.....	94
4.1.19 Persistent Encryption.....	94
4.1.20 Strong private key protection.....	94
4.1.21 CSPs and Algorithms.....	94
4.2 Server Settings.....	94
4.2.1 Strong private key protection.....	95
4.2.2 SQL Dialect.....	95
4.2.3 Database Owner.....	95
4.2.4 ODBC Data Source.....	95
4.2.5 Ignore during Certificate Verification.....	95
4.2.6 Hash Algorithm.....	95
4.2.7 Check certificate extensions.....	96
4.3 Unhandled Drives, Unhandled Application, Unhandled Devices.....	96
4.3.1 Adding ignored disk drives.....	96
4.3.2 Adding ignored applications.....	96
4.3.3 Adding ignored devices.....	97
4.4 Programs with specific behavior when saving files.....	97
5 APPENDIX.....	99

5.1 Logging.....	99
5.2 Permissions.....	100
5.2.1 Global permissions.....	100
5.2.2 Permissions for changing the settings for a Security Officer.....	101
5.2.3 SO permissions for processing the groups.....	102
6 Technical support.....	103
7 Legal notices.....	104

1 What is SafeGuard LAN Crypt?

SafeGuard LAN Crypt provides transparent file encryption. It was developed to enable users within large organizations to exchange data confidentially. In this situation, encrypted files can be stored locally on the user's hard disk or on a removable medium or even on network drives.

The encryption process is completely transparent for users. It takes place automatically when the files are created or saved. These files are also decrypted transparently when their data is read. This process is performed by a filter driver that is integrated in the file system on a Windows computer. The SafeGuard LAN Crypt filter driver works in a similar fashion to a virus scanner: it identifies which files are to be accessed and performs the appropriate encryption or decryption operation on them.

Whenever a user moves a file into a trusted directory, the file is encrypted on that user's computer, and each time another trusted user, who is a member of the same group, reads the file from this directory, it is transferred to this user in encrypted form. The file is not decrypted until it reaches the target computer, where the user can change it. Then it is encrypted again before being returned to the encrypted directory.

Encrypted files are not "assigned" to individual users. Any user who has the right key can access the encrypted file. This allows administrators to create logical user groups whose members can share encrypted files. This process can be compared with a bunch of keys, just like you use in daily life: SafeGuard LAN Crypt provides users and user groups with a bunch of keys, and the individual keys can be used to open different doors or safes.

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

As a result, a file is always protected, even if no access protection is defined for the file system itself, if the network is attacked, or the employees do not comply with the organization's security policy.

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

The Security Officer (SO) can specify which files and folders are to be protected by SafeGuard LAN Crypt, centrally, by defining one or more encryption rules. For example, to ensure that all Word documents are protected, the SO would define the rule *.doc. As soon as this rule was rolled out across a client system as part of a policy file, all Word documents would be encrypted, no matter where they are stored. If required, more than one encryption rule can be combined to form an encryption profile.

In this example, three different rules have been brought together in one encryption profile.

Rule	Key	Description
*.doc	Key1	This encrypts all Word documents with key1, no matter where they are stored.
D:\Data*.*	Key2	This encrypts all the files in the specified folder with key2.
\\Server1\Share1\Personal*.xls	Key3	This encrypts all the Excel files in the specified server folder with key3.

With SafeGuard LAN Crypt the SO can define very complex rules to ensure that only the actual data they require is encrypted in very specific locations. These rules are rolled out in policy files that can be stored on a file server or in the Netlogon folder on a Windows Domain Controller. The Security Officer can create a tailored policy for each individual user at the click of a button. This policy contains all the keys and rules that apply to that user.

The SO uses the SafeGuard LAN Crypt Administration graphical user interface to generate and administer these policy files. In turn, this uses the Microsoft Management Console (MMC) as its interface. The Snap-Ins provide the Security Officer with a range of tools to make their tasks easier.

The policy files are encrypted separately, by means of certificates, for every single user. This process involves the Public Key Infrastructure (PKI) already present in the organization. Alternatively, the SO can also create the certificates themselves by using SafeGuard LAN Crypt.

The SafeGuard LAN Crypt administration data is then stored in an SQL database. Of course, all important data records and especially the key data are encrypted in the SQL database. Because the database used here is not dependent on the system administration functionality, the security and system administration functions can be kept strictly separate. SafeGuard LAN Crypt can also be used to configure different SO roles whose permissions can be restricted to suit specific tasks in specific areas.

The Master Security Officer (MSO) is the only person who always has every permission. In addition, an SO is also able to delegate the permissions required to administer SafeGuard LAN Crypt and therefore build up an administrative hierarchy to suit the organizational structure of their own company.

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 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 manage profiles. To draw a clear distinction between Windows administration and SafeGuard LAN Crypt administration, the role of a security officer must be 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.

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).

1.2 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 RAM when opened by an application. When the file is saved, it is automatically encrypted again.

- Every file for which there is an encryption rule is encrypted automatically.
- If files are copied or moved to an encrypted directory, they are encrypted in accordance with the encryption rule that applies to that directory. You can, of course, also define different encryption rules for different file extensions or names in the same directory. Encryption is not specific to directories. It depends entirely on encryption rules!
- When encrypted files are renamed, they remain encrypted (provided there is not a different encryption rule, or no encryption rule, for the new file name/file extension).
- If you copy or move encrypted files to a location where the current encryption rule is no longer valid, they remain encrypted, as persistent encryption is enabled by default.
- If you copy or move encrypted files to a location where the current encryption rule is no longer valid, but a different encryption rule is valid, these files are first decrypted and then encrypted again according to the new encryption rule.
- Transparent encryption is applied to all file operations. The user remains completely unaware of these processes while working with encrypted data, because they all run in the background.
- Persistent encryption can prevent a user decrypting files by mistake when they copy or move them to a different folder for which no encryption rule has been defined, with Explorer. However, this mechanism does not come into play if the file is copied or moved with another function instead of Explorer.

1.2.1 Accessing encrypted data

If the user does not own the appropriate key, they are not permitted to access the encrypted data in a directory. The user cannot read, copy, move, rename, or in any other way interact with the encrypted files in this directory.

However, the user can access such files if they own the key used to encrypt them, even if their user's encryption profile does not contain an encryption rule for these files.

Note: When files that have only been opened with the available key are stored (no encryption rules for these files), they may be saved as unencrypted data. This happens with applications that create a temporary file, delete the source file and then rename the temporary file, when they save it. As there is no encryption rule for the new file, it is saved as unencrypted data.

1.2.2 Renaming or moving directories

For performance reasons, SafeGuard LAN Crypt does not change the encryption status when complete directories are moved using Windows Explorer. This means that no encryption, decryption or re-encryption is carried out when a directory is moved.

If files were encrypted, they remain encrypted in the new directory or in the new storage location. If the user owns the appropriate key, they can work with these files as usual.

Moving files and directories securely

SafeGuard LAN Crypt can also move files and directories securely. In this case, the files and directories are encrypted, decrypted or re-encrypted as required, in accordance with the current encryption rules. The source files are securely deleted ("wiped") after they have been moved.

You access this function via the **Secure Moving** command in the Windows Explorer context menu. In a dialog, you select the location to which the files are to be moved.

1.2.3 Explicit file decryption

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

However, this is only the case if

- an appropriate encryption profile has been loaded
- the user has the right key
- no encryption rule for the new location exists in the active encryption profile.
- persistent encryption is switched off.

1.2.4 Deleting encrypted files - Windows 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. For emptying the Recycle Bin no key is necessary.

1.2.5 Files/directories excluded from encryption

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

- Files in the SafeGuard LAN Crypt installation directory
- Files in the Windows installation directory
- Policyfilecache

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)

1.2.6 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 behaviour in SafeGuard LAN Crypt Configuration. If disabled, files are created in plain 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 plain text.
- 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.

1.2.6.1 Persistent Encryption vs. encryption rule

As mentioned above, Persistent Encryption tries to ensure that an encrypted file retains its encryption state, for example its original encryption key. This works perfectly fine if the file is relocated to a folder with no applicable encryption policy. But 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 will end up encrypted with the key defined in the encryption rule and not with the one that was originally used.

1.2.6.2 Persistent Encryption vs. Ignore path rule

An Ignore path rule also overrides Persistent Encryption, thus ensuring that encrypted files which are copied to a folder with an applicable Ignore path are stored in plain!

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

1.2.6.3 Persistent Encryption vs. Exclude path rule

An Exclude path rule also overrides Persistent Encryption, thus ensuring that encrypted files that are copied to a folder with an applicable Exclude path are stored in plain!

1.2.6.4 Limitations on Persistent Encryption

Due to technical reasons Persistent Encryption has some limitations or in other words the actual result of Persistent Encryption might not always meet the expectations of the user. Here are some common scenarios where the Persistent Encryption falls short.

Files that are supposed to remain plain are encrypted

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

If a plain file is copied to several locations at the same time, with one having an encryption rule applied, the other copies of that file might be encrypted too, although the original file is not encrypted. If the file is copied to an encrypted location in the first place, the file is added to the drivers internal list. When the second copy is created anywhere else, the driver does find the file name in its list and therefore encrypts the second copy, too.

- **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 will be encrypted with the same key as the file that was opened first.

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

A common use case: In Windows Explorer right-click in a folder with encryption rule and click **New > New Textdocument**. Immediately right-click in a folder without encryption rule and

click **New > New Textdocument**. The second file will be encrypted, too.

Files are not encrypted

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

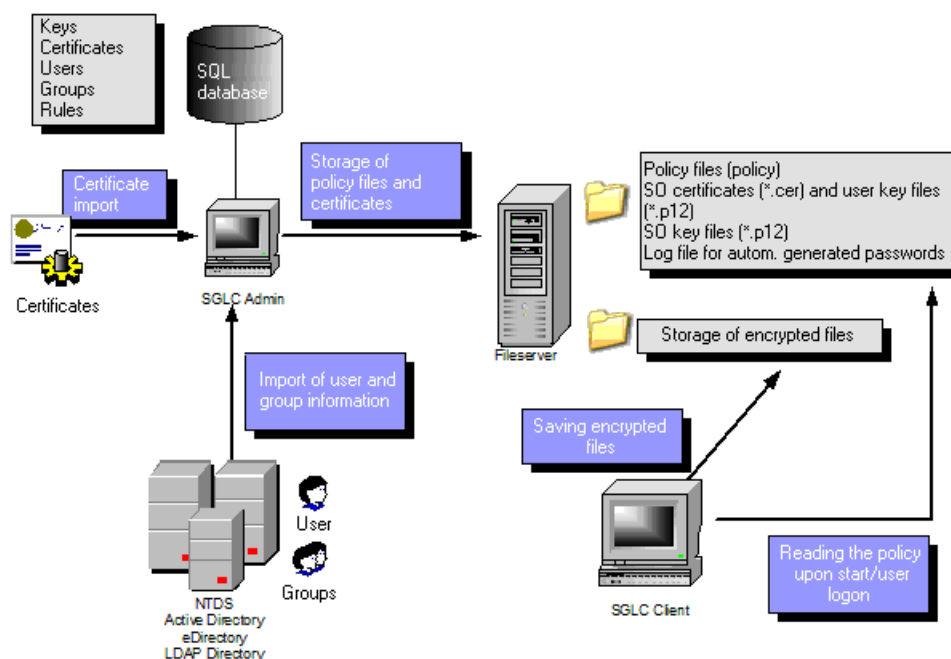
If copies of an encrypted file are created in the same folder as the original file, these copies are not encrypted. Since the created copies have different file names (for example doc.txt vs. doc - Copy.txt) the matching of the file name fails and therefore they are not encrypted by Persistent Encryption.

1.2.6.5 Client API and encryption tags for DLP products

If a 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.

1.3 Architecture

SafeGuard LAN Crypt consists of two components: SafeGuard LAN Crypt Administration and SafeGuard LAN Crypt Client. These two components are usually installed on a regular workstation computer with an operating system such as Windows XP, Windows Vista or Windows 7. Security Officers use SafeGuard LAN Crypt Administration to define and distribute encryption profiles. This figure shows how individual components interact with each other and how SafeGuard LAN Crypt is integrated in a corporate network.



1.3.1 SafeGuard LAN Crypt Administration

The administration components contain the tools required for the central administration of SafeGuard LAN Crypt and are used by one or more Security Officers. They are usually installed on one or more workstation computers running Windows XP, Windows Vista or Windows 7 as their operating system. They can also be installed on a Windows 2003 server system if you want to perform central administration tasks with Windows Terminal Services or Citrix MetaFrame. This is particularly useful in larger environments and especially where sites are distributed to different geographical locations. In such situations, SGLC Administration is accessed via the Remote Desktop (RDP) or Independent Computing Architecture (ICA) protocol.

As the maximum level of security and confidentiality of the data you want to protect can only be guaranteed if SGLC Administration and the system administration operate independently of each other, SGLC has separate user and group administration functionality. To make everyday tasks easier, the users and groups managed by SafeGuard LAN Crypt can be imported from existing Active Directory or from another LDAP-based Directory.

SafeGuard LAN Crypt Administration requires an SQL database so that it can store configuration data and manage SGLC users and groups. This database can be installed locally on the administration system if the Microsoft Express Edition is being used. In larger installations that have a number of Security Officers we recommend that you use a central database system with a structure similar to a Microsoft SQL or Oracle Server.

Security Officers are responsible for defining the security policy used in their organization. They specify the policies and ensure that they are implemented, modified and adhered to correctly. Smaller companies will usually manage with just one Security Officer. Larger organizations often have several Security Officers who usually work at departmental or site level and are organized into a hierarchy. SafeGuard LAN Crypt can also represent and reflect the various hierarchy levels involved in this situation. At the top of the hierarchy stands one or more Master Security Officers: they must be present when the SafeGuard LAN Crypt database is generated. These officers define the first policies and decide whether the two person rule (two people necessary for authentication) is to be used for actions that impact security issues. Each Security Officer is assigned particular administrative permissions which define their fundamental rights. Their area of responsibility can also be limited to a few user groups by Access Control Lists (ACLs).

SafeGuard LAN Crypt uses Key Encryption Keys (KEKs) to administer access rights for users. These are encrypted and stored in the SQL database and, like all database contents, are protected from being changed with MAC and hash values. Administration tasks are arranged in such a way that a Security Officer can only ever know the name of a key and not its actual value. This means they can work with key objects and create encryption rules. The flexibility of permission control procedures mean that a wide range of scenarios can be covered. For example, a Section Head can define keys and assign folders. In the next work step, a central Security Officer can generate the encryption profile. As a result, the keys remain under central control.

SafeGuard LAN Crypt recognizes two automatically-generated key types: user keys and group keys. User keys are generated for individual users and can be used for generic encryption rules, such as the encryption of home directories or

local or temporary folders. Each user has precisely one user key. If data protected by a user key has to be recovered in an emergency, the Security Officer must assign this specific key to another user. This type of recovery requires a special administrative permission and can be linked with a "two person rule" (approval by a second person) to ensure that it is not misused. A similar concept is also available for user groups: this is the group key.

The policy files include all the rules, access rights and keys required for transparent encryption. Before a user is able to encrypt/decrypt data using the SafeGuard LAN Crypt software installed on the client workstation, they first need to access the encryption information stored in a policy file. In this situation the policy files are stored either on a file server or in a domain controller's Netlogon share.

Note: You do not need to install SafeGuard LAN Crypt components on file servers or domain controllers.

The policy file is protected against unauthorized access by a certificate. Only the owner of the certificate has access to the private key belonging to the certificate, and can therefore use this certificate to access the relevant encryption information. If self-signed certificates are being used these are also stored on a fileserver and the user will require read access rights, to enable them to use the certificates. SafeGuard LAN Crypt also supports the use of certificates stored on smartcards, USB tokens or suitable hardware boards.

Note: You can use SafeGuard LAN Crypt without having to use smartcards or tokens to store certificates.

The paths to the policy files (from the user's point of view) and other SafeGuard LAN Crypt settings are identified by mechanisms in the operating system.

A SafeGuard LAN Crypt trusted group consists of a number of users with the same encryption profile. Policy files for every single user are generated in Administration. All SafeGuard LAN Crypt users who have the same profile stored in their policy file are members of an authorization group. They do not need to worry about encryption or key exchange. They only have to be able to access the policy file to have their data encrypted or decrypted transparently, as soon as they close or open it.

1.3.2 SafeGuard LAN Crypt Client

The SafeGuard LAN Crypt Client is installed on the Windows systems (PCs, workstations, notebooks, terminal servers) on which you want encryption to be performed. In addition to the filter driver required for encryption and decryption, the client component has a range of other optional components:

- Explorer extensions for initial and explicit encryption
- A user application for loading and deleting encryption rules as well as activating and deactivating encryption
- A user application for displaying all the settings and rules that are active on the client. This is for example important in support cases.
- A user application for initial encryption
- Token support so that token-based certificates can be used to access stored encryption information

The client component first loads the profile created by the Security Officer. It then decrypts this profile and derives from it the encryption rules that apply to the user who is currently logged on. These are then applied by the installed filter driver. Before a user can access their encryption profile, the certificate assigned to them must either already be present on their computer or be loadable from a file server or a Netlogon share. These certificates must first be provided by a Security Officer, and then imported by the user who requires them. SafeGuard LAN Crypt also has an option that imports certificates automatically the first time a user profile is loaded.

In this situation, the user is prompted to enter a PIN before this certificate is imported. They must first be given this PIN by the Security Administrator. The certificate is checked every time the encryption profile is loaded. If the certificate is valid, the user can log on to SafeGuard LAN Crypt. If no valid certificate is present, the user cannot access the encrypted data. If the certificate is stored on an SGLC Client-supported hardware-based token, the user does not need to take any further actions once the token is unblocked: encryption and decryption are performed automatically.

2 Getting started

2.1 Certificates

SafeGuard LAN Crypt uses certificates and public/private key pairs to secure encryption information stored in policy files. Only the owner of a certificate can access the private key that belongs to that certificate and is therefore able to use it to access the encryption information.

Which certificates can be used and where do they come from:

- A company either has its own Public Key Infrastructure (PKI) or uses a Trust Center to create certificates for the users. In this case, existing certificates can be used.
- Alternatively, the SafeGuard LAN Crypt Administration component can generate self-signed certificates. These certificates can only be used by SafeGuard LAN Crypt! The certificates also have a Critical Extension to show applications that they must not be used. These are simple certificates (comparable to Class-1 certificates) which comply with the X.509 standard. In SafeGuard LAN Crypt you can configure whether a critical extension is added to a newly generated certificate or not.

Note: In certain situations other applications will ignore these Critical Extensions on SafeGuard LAN Crypt certificates. This will then cause problems with these self-signed certificates. In such cases you must explicitly deactivate all the areas of use for SafeGuard LAN Crypt certificates with the Microsoft Management Console's certificate snap-in to prevent these certificates from being used in other applications.

The certificates are assigned to the users within the SafeGuard Administration component.

Important information about how to use certificates:

- SafeGuard LAN Crypt only uses the Microsoft Crypto API for certificate functionality.
- SafeGuard LAN Crypt supports all Cryptographic Service Providers (CSPs) that comply with certain standards (e.g. RSA key length at least 1024 bits). They include, among others, the Microsoft Enhanced CSP.

Note: The Microsoft Standard CSP (Microsoft Base CSP) cannot be used.

If you have any questions about the compatibility of other CSPs, please contact the support team.

2.1.1 Security levels

As SafeGuard LAN Crypt aims to provide the highest possible security, it is necessary to use strong CSPs such as the Microsoft Strong Cryptographic Service Provider. These CSPs allow the use of keys that are up to 16384 bits long and provide strong encryption algorithms (such as 3DES).

You will also need to activate the following option when importing a certificate using the *certificate import wizard*:

Enable strong private key protection

You will be prompted to enter the password every time the private key is used by an application. After you click **Finish** in the **Certificate import wizard**, the **Importing a new private exchange key** dialog is displayed. Click on **Set Security Level**, to set the security level again:

- **High**

If you select **High**, you will need to enter a password to confirm that you are using a private key. In the next dialog box, enter a new password.

- **Medium**

If you select **Medium**, the system displays a prompt in which you are asked to confirm the use of a private key by clicking **OK**.

Highest Security Level with Automatically-Imported Private Exchange Keys (.p12, .pfx)

SafeGuard LAN Crypt allows you to import certificates automatically. To use the medium or high security level with the private keys belonging to these certificates, you must set the Strong private key protection option in the SafeGuard LAN Crypt Configuration to yes.

If this option is not activated, the security level "low" is automatically used for the imported certificates.

In this way, you can ensure that certificates with a high security level are compulsory and can be implemented within a company-wide security policy:

Note: If the highest security level is being used, SafeGuard LAN Crypt users must enter the password for the private key once, at the Windows logon prompt, and again manually, each time an encryption rule is loaded.

Smartcard

If certificates stored on smartcards are used, the password only has to be entered once. As long as the smartcard remains in the card reader there is no need to enter the password again

We recommend that you set this option to "high" before starting SafeGuard LAN Crypt Administration for the first time. If not, the initial Master Security Officer's certificate is used without security level "high", when it is created by SafeGuard LAN Crypt, and not, for example, imported from a smartcard.

Note: Windows caches PINs for 24 hours by default. Using software certificates may cause security problems when you log on to SafeGuard LAN Crypt Administration and when additional authorization is provided. We strongly recommend that you deactivate this feature. To do so, set these values:

"PrivKeyCacheMaxItems"=dword:00000000

"PrivKeyCachePurgeIntervalSeconds"=dword:00000000

under the key

KEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography

If you do this the PINs will not be cached.

Preconditions for using certificates with SafeGuard LAN Crypt

- The certificate must include a public key.
- The private key for the assigned certificate must be available before a user can access the encryption profile.
- Only certificates stored in **User Configuration** in the Personal Certificates, Other People and Active Directory User Object certificate stores, and in **Local Computers** in the Personal Certificates certificate store, are listed by SafeGuard LAN Crypt. SafeGuard LAN Crypt ignores certificates that are stored in other locations! You can use the Certificate Management Console snap-in to import and organize certificates.
- Only the public key is used to "associate" a certificate with SafeGuard LAN Crypt's encryption information. You do not need to know the private key. The private key remains the property of the certificate's owner, who is the only person who can access the encryption information.

We recommend that you have the certificates available and ready to use before you start installing SafeGuard LAN Crypt. The certificates then appear in the *Certificates* dialog immediately after SafeGuard LAN Crypt has been installed, and can be used right away.

Note: SafeGuard LAN Crypt does not administer certificates. However, you can do so using your company's own PKI infrastructure or by using trust centers.

2.1.2 Certificate verification

SafeGuard LAN Crypt carries out extended certificate verification. This means that certificates are not accepted until their entire certificate chain (evaluation of a **C**ertificate **R**evocation **L**ist) has been checked.

Extended certificate verification is carried out for these certificates:

- For certificates which are provided when a Master Security Officer is created. Only certificates which pass the entire check are displayed.
- For certificates which are created after a recovery key has been used to assign a new certificate to a Security Officer. Only certificates which pass the entire check are displayed.
- For certificates which are used by Security Officers to log on to the SafeGuard LAN Crypt database. If the certificates cannot be checked, access is denied.
- For certificates which are used for additional authorizations.

These are the preconditions for extended certificate verification:

- The certificate being used must include a CRL. Some PKIs allow you to define a CRL in the certificate itself. If a CRL has been defined, the list is evaluated. You may need to download a CRL from the issuer via the network for this purpose. If the certificate cannot be verified, the encryption profile is not loaded.
- A CRL has been loaded into the local certificate store.

Note: You may need a network connection before you can evaluate a CRL. If this connection cannot be established, access will be denied, even though the certificate itself may be valid.

2.1.3 Smartcard readers

As the use of certificates is handled by using Cryptographic Service Providers (CSPs), smartcards are supported automatically when a smartcard CSP is used. You can therefore handle access to encryption information by using certificates on smartcards.

If you want to use certificates on smartcards, ensure that the smartcard reader and an appropriate Cryptographic Service Provider are installed correctly!

2.2 Installation

You can only install SafeGuard LAN Crypt if you have Windows Administrator privileges.

1. Go to the Install directory of your unzipped installation package and double-click on the .msi file.
An installation wizard guides you as you install SafeGuard LAN Crypt, which is a very simple process. Click **Next**.
2. The **License Agreement** dialog is displayed. Select **I accept the license agreement** in the **License Agreement** dialog. If you do not do this, you will not be able to install SafeGuard LAN Crypt! Click **Next**.
3. The **Destination Folder** dialog appears. Select where you want to install SafeGuard LAN Crypt. Click **Next**.

4. The **Select Installation Type** dialog is displayed. In this dialog, you can select which SafeGuard LAN Crypt components are to be installed. Select **Custom** and then click **Next**.

The following components can be installed:

- **Administration**

Installs the SafeGuard LAN Crypt Administration.

- **Scripting API**

Installs the SafeGuard LAN Crypt Scripting API required for using scripts to administer the product.

5. Select which components are to be installed and click **Next**.
6. After having checked your settings, click **Next** in the **Ready to Install the Application** dialog. The installation process starts.
7. If the installation is successful, a dialog box appears. In it, click **Finish** to complete the installation.
8. To accept all the settings, reboot the computer! This loads the drivers.

2.3 Unattended installation

Unattended installation means you can install SafeGuard LAN Crypt automatically on a large number of computers. The **Install** directory contains the **sglccadm.msi** file required for an unattended installation.

2.3.1 Components to install

The following list shows which components must be installed and the way in which you specify them for an unattended installation.

The keywords represent the way the components have to be specified under **ADDLOCAL=** when you run an unattended installation. Component names are case-sensitive.

SafeGuard LAN Crypt Administration - **Administration**

Scripting API - **ScriptingAPI**

Note: If you do not specify a component, a complete installation will be performed.

2.3.2 Command Line Syntax

To perform an unattended installation you must run **msiexec** with specific parameters.

Mandatory parameters

- **/I:** Specifies which installation package is to be installed.
- Name of the .msi file: **sglccadm.msi**
- **/QN:** Installation without user interaction (unattended setup)

Syntax: **msiexec /i <path>\sglccadm.msi /qn**

Optional parameter

- **/Lxv <path + filename>**: Logs the complete installation procedure in the location specified under **<path + filename>**.

Example

```
msiexec /i C:\Install\sglcam.msi /qn
```

This carries out a complete installation of SafeGuard LAN Crypt. The program is installed in the default installation directory (**<System drive>\Program Files\Sophos**). The **.msi** file is located in the **\Install** directory of drive C.

2.4 Upgrading

For upgrading older versions to this version of SafeGuard LAN Crypt Administration the following steps are necessary:

- Installing the new version
- Upgrading the existing database
- Running the upgrade wizard
- Entering new server credentials in case you upgrade from a version older than 3.61.

Note: The first logon after upgrading has to be performed by a Master Security Officer.

2.4.1 Installing the new version

Install the new version as described.

Note: Make sure that all instances of SafeGuard LAN Crypt Administration are closed before you install the new version.

2.4.2 Upgrading the existing SafeGuard LAN Crypt database structure

Using the command line tool **Tool CreateTables.exe** you can upgrade the structure of the tables in your SafeGuard LAN Crypt database. The tool is available in the **\Install** directory of your installation package.

Note: Logon to the database has to be performed with privileges that allow creation and modification of the database schema.

Command line syntax

```
CreateTables <ODBCName[.OwnerName]> <SQL dialect> <action>
```

CreateTables.exe offers the following parameters for creating tables in other configurations:

- **ODBCname:** The name used for the ODBC data source.
- **OwnerName:** For the database to be addressed correctly, the database owner has to be specified for Oracle databases. The owner has to be specified in CAPITALS.
- **SQL dialect:**

- **m**: Microsoft SQL Server
- **o**: Oracle 9 or higher
- Actions:
 - **u**: Update of the database structure.
- Examples:
 - **CreateTables SGLCSQLServer m u**
 - **CreateTables SGLCSQLServer.SGLC o u**

2.4.3 Upgrade wizard

After upgrading the database an upgrade wizard guides you through the necessary steps to complete the upgrade. The wizard is launched after the first logon to the upgraded administration.

Note: Only a Master Security Officer is allowed to perform the first logon after upgrading the administration. If you do not have the appropriate rights a message will be displayed. The steps to complete the upgrade may vary depending on the version you upgraded.

In the wizard, you perform the following steps:

- Entering a location name.
- Verifying and - if necessary - correcting the database integrity. Information on corrected errors will be displayed.
- Creating a new recovery key.

After you completed the wizard administration is ready to use.

2.4.4 Server logon credentials for versions below 3.61

After upgrading, the logon credentials have to be entered again under **Central settings** on the **Server** page. If you use a Microsoft directory service, do as follows:

- Enter the domain name under **Domain or Server Name**.
- Enter the **User Name** as **user name@domain name**.

3 Administration

SafeGuard LAN Crypt Administration integrates seamlessly in Microsoft's Management Console (MMC) and offers a Security Officer a trustworthy user interface with typical MMC functionality. The Administration Console was developed to enable users to benefit from existing Windows replication tools. This not only helps to achieve high levels of efficiency but also reduces the total costs of ownership (TCO), since customers who have a large number of workstations usually only want to implement one system for administering them.

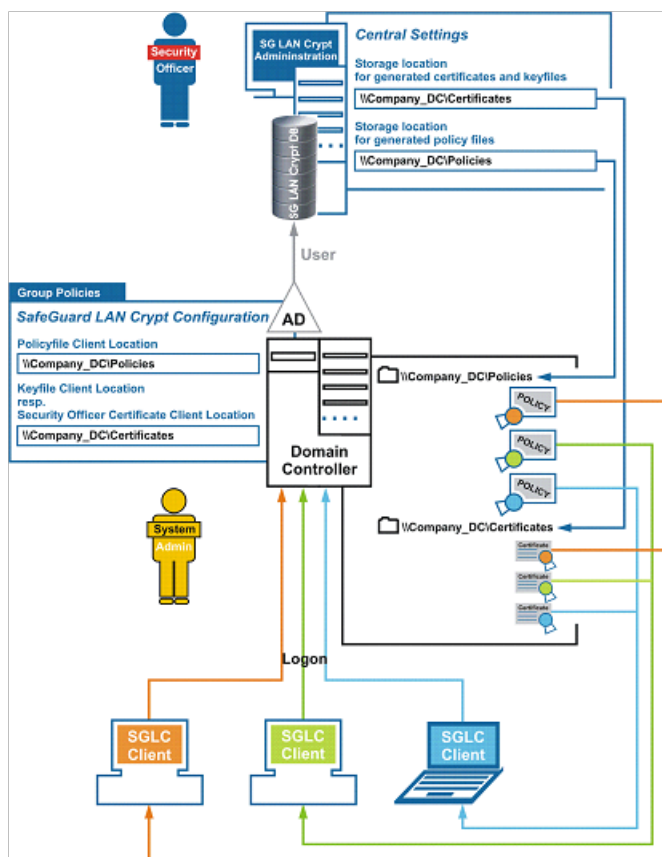
The SafeGuard LAN Crypt Administration Console is usually installed on a separate machine, from where the required directory services and the SafeGuard LAN Crypt database can be accessed.

SafeGuard LAN Crypt uses the concept of Security Officers. Initially there is one **Master Security Officer** who installs the Administration Console. During installation the Master Security Officer must specify where the certificates and key files (the public part of the Security Officer's certificate and .p12 files containing the user certificates which have to be imported on the client machines) generated for users are to be saved. After installation you must specify where the policy files generated for the users are to be saved. Policy files containing the encryption rules are generated for each user.

Certificates, .p12 files and policy files are automatically imported by the clients from the specified storage location at a later point in time.

The clients must therefore be able to access these directories. The **Master Security Officer** and the **System Administrator** must work together to define these directories (usually shared network folders).

Clients can use group policies when they log on to a domain controller to find out how to access these files. The System Administrator specifies the storage locations in the SafeGuard LAN Crypt Configuration Console. SafeGuard LAN Crypt is configured in the group policy object that is valid for the users.



SafeGuard LAN Crypt clients do not need to connect to the SafeGuard LAN Crypt database. The information required for finding certificates, .p12 files and policy files can be found at logon in group policies. These files are then automatically transferred to the clients.

To import a certificate, a user must have a password. In the case of certificates generated by SafeGuard LAN Crypt, the `p12pwlog.csv` file contains the passwords and can be used, for example, to create a PIN letter.

3.1 Required steps

- Preparations:
 - Optional: install the supplied database system
 - Add data source (ODBC)
 - Create database tables (**CreateTables.exe**)
- **System Administrator**: Define settings in the SafeGuard LAN Crypt Configuration console.
- Create initial Master Security Officer
- Define storage locations
 - for certificates and key files generated by SafeGuard LAN Crypt

Note: The user certificates (.p12 files) and the public part of the Security Officer's certificate are imported from this directory by the Clients. A directory that has been defined together with the System Administrator should therefore already be available (network share).
 - for SO certificates generated by SafeGuard LAN Crypt
 - for the password log file, which contains the passwords that were automatically generated for the key files
- Define central (core) settings

Here you define where the policy files generated for users are to be stored. Work together with the **System Administrator** to do this.

Note: If you are using an Oracle database and access the database from Administration Consoles on different machines, you should now also specify the code page settings (see The Database tab on page 53 XXX).
- Create additional Master Security Officers
- Define rights for Security Officers
- Import objects (Organizational Units, groups, users) from the directory service (e.g. Active Directory)
- Assign Security Officers to the organizational units and define their rights
- Create keys
- Create encryption rules
- Generate or assign certificates
- Generate policy files

3.2 Preparations for administering SafeGuard LAN Crypt

After installation, you must work through the following steps before you can start administering SafeGuard LAN Crypt:

- Optional: install database management system

This is only necessary if your database system does not include a database you want to use for administering SafeGuard LAN Crypt. To cover this eventuality, SafeGuard LAN Crypt has its own freely usable database system that you can use for administration. This is the Microsoft SQL Server 2008 R2 Express Edition. In addition, SafeGuard LAN Crypt supports the following database systems:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2005 Express
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008 R2 Express
- Oracle9i
- Oracle10g
- Oracle11

Note: If you are using an Oracle database, you must install the Oracle client before you can use SafeGuard LAN Crypt Administration. If you select the "runtime" variant of the Oracle client you must also install the Oracle ODBC driver. SafeGuard LAN Crypt does not support Microsoft ODBC for Oracle. Make sure that you do not use any of the manufacturer's reserved key words when you generate database objects.

- Specifying a data source (ODBC)

If you want to use your own database system, you must know the access data for the database you want to use so that you can specify the data source.

- Creating database tables

After specifying the data source you have to create the SafeGuard LAN Crypt tables in the database using the tool provided with your software (CreateTables.exe).

3.2.1 Installing the supplied database system

The following description refers to the Microsoft SQL Server 2008 R2 Express Edition. For this example description, the defaults of this version have been used as far as possible.

To install the database system, do as follows:

1. In the Install directory of your unzipped installation package, double-click the file **SQLEXP32_x86_ENU.exe**.

Note: If you use a 64 bit operating system download the 64 bit version of Microsoft SQL Server 2008 R2 Express Edition from www.microsoft.com.

2. Accept the license agreement and click **Next**.
3. The installation files are extracted and the installation wizard starts.
4. Follow the installation wizard instructions and accept all defaults.

- **Defaults:** The following descriptions of preparatory steps refer to these defaults. If you make any changes (authentication method, database instance), you have to take them into account when specifying the data source and creating the database tables.

- **Database authentication:** By default, the Express Edition uses Windows authentication. A prerequisite for using Windows authentication is that the user who logs on to the database has Windows administrator rights.
- **Master database:** By default, the existing master database is used when specifying the data source. In general, we recommend NOT to use the master database since it may cause problems when upgrading the Express Edition or the SQL Server version.

You can create a separate database for SafeGuard LAN Crypt and specify it when adding the data source. For the Microsoft SQL Server 2008 R2 Express Edition you can create a database by using the following command on the command line:

```
osql -E -S .\SQLEXPRESS -Q "CREATE DATABASE <name_of_the_database>"
```

A database with the specified name using Windows authentication is created.

With parameter **-U**, for example, you can specify a user name for authentication. To see all parameters, **type osql -?**.

You can also download Microsoft SQL Server 2008 R2 Management Studio Express, which is available for free, and use it to create a separate database.

In the next step, a data source has to be specified so that SafeGuard LAN Crypt can use the database system.

3.2.2 Adding a data source (ODBC)

Note: The data source has to be added with the 32 bit ODBC Data Source Administrator, which is also available on 64 bit systems. If you use a 64 bit system, start the ODBC Data Source Administrator by clicking Start\All Programs\Sophos \SafeGuard LAN Crypt \ODBC Data Source Administrator (x86). This ensures that the correct version is launched.

Specify a data source so that SafeGuard LAN Crypt can use the database via the data management system. To do so, use the ODBC data source administrator.

ODBC (Open Database Connectivity) allows data to be accessed on a wide variety of database management systems. For example, if you have a program for accessing data in an SQL database, ODBC lets you use the same program to access data in another, different database. To do this, you must add "drivers" to the system. ODBC supports you when you are adding and configuring these drivers.

To add a data source:

1. Select Start\Settings\Control Panel\Administrative Tools\Data Sources (ODBC). The ODBC Data Source Administrator opens.
2. Select the **System DSN** tab and click **Add**.
A list now appears to which you can add data sources, each with its own System DSN (system data source name). These data sources are saved locally on a computer but are not assigned to any particular user: any user who has the appropriate rights can use a System DSN.
3. Select **SQL Server** as the driver for which you want to create the data source and click **Finish**.

Note: If SQL Server Native Client is available in the list, select this entry.

4. A dialog now appears in which you enter the SGLCSQLServer name to reference the data source.
You configure the data source reference name in SafeGuard LAN Crypt configuration. The default setting is SGLCSQLServer. If you want to use a different name, enter it in the configuration.

Note: The name of the ODBC source is case-sensitive! Here you must enter names in exactly the same way as they were specified in SafeGuard LAN Crypt configuration. You must enter the names in the configuration before running the SafeGuard LAN Crypt Administration Console for the first time.

5. In the Server field, select the server you want to use to establish the connection and click **Next**.
6. Accept the default settings in the next dialog. If you accept the option **With Windows NT authentication using the network login ID** you specify that Windows user data is to be used to log on to the database system. You do not need to enter a password. Click **Next**.
7. Accept the default settings in the next dialog.

As a result, the existing master database is used. However, if you have generated your own database, select it here.

8. In the next dialog, accept the default settings and click **Finish**.

3.2.3 Creating tables in the SafeGuard database

Using the command line tool `CreateTables.exe` you create the required tables in your SafeGuard LAN Crypt database. The tool is available in the `Install` directory of your unzipped installation package.

Note: Logon to the database has to be performed with privileges that allow creation and modification of the database schema.

To create the table in your database, enter the following on the command line: **CreateTables SGLCSQLServer m c**.

If you have used the defaults during installation, configuration of the database system is now complete. You can now start SafeGuard LAN Crypt Administration.

3.2.3.1 CreateTables command line syntax

CreateTables <ODBCName[.OwnerName]> <SQL dialect> <Action>

CreateTables.exe offers the following parameters for creating the tables in different configurations:

- **ODBCName:** The name used for the ODBC data source.
- **OwnerName:** For the database to be addressed correctly, the database owner has to be specified for Oracle databases. The owner has to be specified in CAPITALS.
- SQL Dialect:
 - **m:** Microsoft SQL Server
 - **o:** Oracle 9 or higher
- Actions:
 - **c:** Create all tables
- Examples:
 - **CreateTables SGLCSQLServer m c**
 - **CreateTables SGLCSQLServer.SGLC o c**

3.3 Master Security Officers

SafeGuard LAN Crypt uses the concept of Security Officers. Initially there is one Master Security Officer, who can delegate tasks later on by creating additional Security Officers and assigning them specific rights for the administration of SafeGuard LAN Crypt. The first Master Security Officer may even create additional Master Security Officers.

ACLs are used to define the rights assigned to the Security Officers created by a Master Security Officer. Individual Security Officers can then be assigned to different organizational units in central Administration. Their rights then apply exclusively to the organizational unit to which they have been assigned. These rights are inherited downwards in the organizational hierarchy until other rights are assigned.

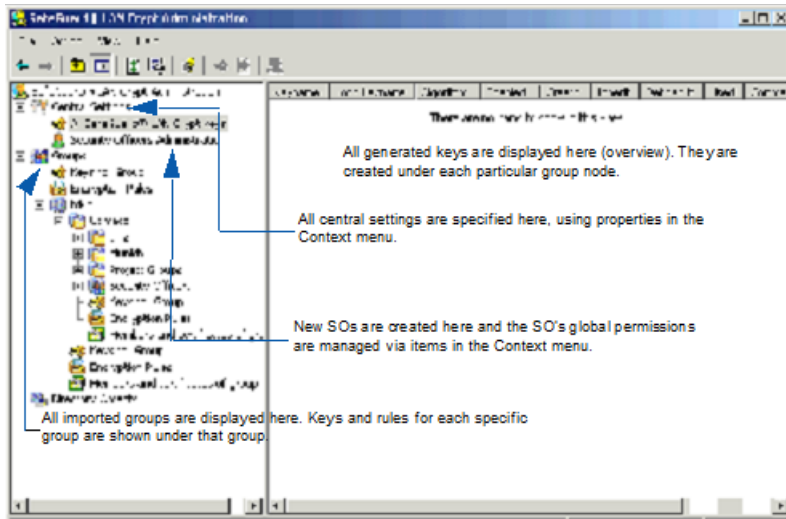
After you have set up the database system and the data source, the next step, when SafeGuard LAN Crypt Administration Console runs for the first time, is to create an initial Master Security Officer. A Master Security Officer always has all existing rights.

Notice: When creating the initial Master Security Officer, you must also define the storage location for the certificates and key files generated by SafeGuard LAN Crypt. The public part of the Security Officer's certificate, which is needed by the clients, is also stored there. User certificates (.p12 files) are also imported from this directory later on. The directory you defined with the System Administrator should already be available (network share).

All settings made when creating the initial Master Security officer can be changed at a later point in time under *Central Settings* in the SafeGuard LAN Crypt Administration Console.

3.4 Administration: overview

When SafeGuard LAN Crypt is installed, the **SGLCAdmin.msc** file is saved to the SafeGuard LAN Crypt installation folder. Click this entry, via the Windows Start menu (**Start > Programs > ...**) to open a window in the Management Console that displays only those snap-ins required for the SafeGuard LAN Crypt Administration



Console.

You can also add the snap-in for the SafeGuard LAN Crypt Administration Console to the Management Console's normal view (File\Add/Remove Snap-In - SafeGuard LAN Crypt Administration). Even when you add the snap-in you still need the password for the SafeGuard LAN Crypt administration database.

Who is logged on

The status bar shows which Security Officer is currently logged on. You can also see whether they are a Master Security Officer or a Security Officer.

Administration Console tool bar

Many of SafeGuard LAN Crypt's functions appear as icons in the Administration Console Tool bar. The function and number of icons in the tool bar depend on which tab is selected at any particular time.

You can also select all the functions that appear as these icons from the relevant context menu.

Right-click the **SafeGuard LAN Crypt Administration** tab to display the node's properties and modify them if required. You will find a description of these properties in the following sections.

3.4.1 Confirmations

In the SafeGuard LAN Crypt Administration Console you can specify actions that are required to be confirmed prior to execution. To do this, click **Properties** in the context menu for the **SafeGuard LAN Crypt Administration** root node. A dialog displays these options.

If you select an action, you must confirm that you want to perform it before it is carried out. The action is not carried out until you have confirmed it.

- Confirm creating group reference

Adding a group reference to a different group has to be confirmed. Select group > right-hand mouse button > **Copy** > select different group > right-hand mouse button > **Paste** > **Confirmation**.

Note: All **Copy**, **Cut** and **Paste** operations can either be done by using the context menu or by using the Drag&Drop or Drag&Drop + CTRL functionality.

- Confirm creating group reference

Creating a reference to an existing group has to be confirmed.

- Confirm move group to other group

Moving of a group to a different group has to be confirmed.

- Confirm delete group from database

Deleting of a group has to be confirmed.

- Confirm remove shortcut from group

Deleting of a group reference has to be confirmed.

- Confirm remove all shortcuts from group

If there is a reference to a group in a different group, e.g. in group1 and group2 there is a link to group3, deleting this reference has to be confirmed. (select group3 > right-hand mouse button > select **Remove Links**).

- Confirm remove keys from group

Deleting of keys, which was used in an encryption rule and have been deactivated afterwards, has to be confirmed. Used keys are marked in the Administration and reside in the database also if they have been removed from a group. Keys which have not been used yet, will also be deleted from the database if they are removed from a group.

- Confirm attaching key to groupKeys which was used in an encryption rule and have been removed from all groups reside in the database and are displayed under **Central Settings > All SafeGuard LAN Crypt Keys**. From there they can be re-assigned to a group via Drag&Drop. This action has to be confirmed.

- Confirm creating key reference in group

Inserting a link to a key in a group (e.g. by dragging and dropping it from one group to a different group) has to be confirmed. Keys are always copied or a link to them is inserted. Cutting keys is not possible.

- Confirm remove key reference from group

Removing a link to a key from a group has to be confirmed.

Which Security Officer is logged on

This dialog also shows which Security Officer is currently logged on. The Security Officer's name is displayed at the bottom of the dialog. The status bar of the SafeGuard LAN Crypt Administration also shows which Security Officer is currently logged on.

3.4.2 User settings

The **User Settings** tab is where you can influence how information is displayed in SafeGuard LAN Crypt Administration.

You can activate the following options:

- **Add domain name to each group name**, to display the relationship between SafeGuard LAN Crypt groups and domains in SafeGuard LAN Crypt Administration. This option is especially useful if SafeGuard LAN Crypt is to be used for several different domains.
- **Show "Selected users and certificates"**, to display all users (and their certificates) that have been imported into SafeGuard LAN Crypt under the *Central Settings* node. You should be aware that it will take several minutes to display

all the users and certificates in larger installations. You must then restart SafeGuard LAN Crypt Administration so that the changes you made in the **Show "Selected users and certificates"** option become effective.

- **Show parents of users**, to display a particular user's parent group under the node **Members and certificates for group**. This enables you to see at a glance whether the SafeGuard LAN Crypt database contains any users that are not assigned to any group. You must then restart SafeGuard LAN Crypt Administration so that the changes you made in the **Display user parent** option become effective.

- **Disable caching of user lists**

To improve performance, SafeGuard LAN Crypt usually creates user lists in the background and also continues creating them when a user toggles to a different node in Administration. The results of these lists are buffered so that no database access is required when the list is called again. This saves a lot of time if large lists are involved. However, in environments with several parallel SafeGuard LAN Crypt administrators (terminal servers), this may sometimes lead to increased memory requirements. To prevent this, simply activate this option. As a result, the lists are not buffered and the list will not continue being created when the user leaves the node or changes to a different one. We recommend you only use this option if you are actually experiencing problems with memory capacity. Changes to the database made in the same session are not automatically transferred to a list. You can update the changes at any time by pressing F5.

Note: Any changes to settings mentioned above are not stored in the database. They are personal settings which are saved for every user in the Microsoft Management Console snap-in.

3.5 Central settings

In the **Central settings** tab you can define different properties for SafeGuard LAN Crypt Administration, centrally.

To do so, click **Properties** in the context menu for the **Central settings** node. Alternatively, select this and click the **Properties** icon in the SGLC Administration Tool bar. You can then view these properties in a number of tabs and modify them if necessary.

Note:

The Additional Authorization tab, the Recovery Key tab and the Regions tab can only be displayed by Master Security Officers. The Server tab and the Configuration tab can only be displayed by Security Officers who do have the global right Change Configuration. The global right Change Configuration is also required for changing the paths on the Directories tab. Only Master Security Officers can make changes in the **Algorithm** tab, the Certificates tab and the Resolving rules tab.

3.5.1 The Algorithms tab

SafeGuard LAN Crypt has these encryption algorithms:

- AES-128
- AES-256
- 3DES
- DES (not recommended)
- IDEA
- XOR (not recommended)

Select the algorithms you want to use. The algorithms you select here can be used later on when you generate different keys.

Note: If these settings are changed later (for example, if DES is removed from the list of available algorithms), none of the keys that have already been generated or the data encrypted with them is affected. If an algorithm is affected it is simply not available when you generate a new key later on.

Default algorithm

Here you select which default algorithm is to be used to automatically generate user and group keys.

3.5.2 The Keys tab

Keys

Problems with duplicated internal key names may occur when several SafeGuard LAN Crypt installations are combined into one, for example due to a company or departmental merger. For this reason every key is identified by its own Global Unique ID (GUID). The GUID is usually generated randomly by SafeGuard LAN Crypt and cannot be changed afterwards.

However, if files that have been encrypted with SafeGuard LAN Crypt are to be exchanged between two companies, you will need a method that allows you to generate a common key. This is the only way of ensuring that a file encrypted with, for example, the CRYPTOKEY key from company A can be decrypted by company B. Before this can happen, company B must also generate a key called CRYPTOKEY which has the same settings as the key from company A. This also contains the key's GUID.

To handle this situation, SafeGuard LAN Crypt has an option which allows you to enter the GUID manually when you generate a new key. To enable this, simply activate the **Allow Security Officers to define the GUID for newly created keys (default is a random GUID)** option.

Key value

If you activate the **Only Security Officers with the 'Generate profile' right can generate keys (keys without a value are not permitted)** option you can ensure that only Security Officers who have the **Create key** and **Generate profile** rights are able to generate keys (name and value).

SafeGuard LAN Crypt allows you to generate keys that do not have a value. These keys can be used without any restrictions in the Administration console. Their values are generated when you generate the policy files for users. However, this may cause problems if you use a distributed database system. For example: If policy files, which contain keys without a value (generated manually without a value, <GROUPKEY> are generated in a replication-time-window in different sites. If policy files are generated in each site a different value would be generated for the key. As a result you would have one key with two different values.

If the **Only Security Officers with the 'Generate profile' right can generate keys (keys without a value are not permitted)** option is activated (keys without a value are not permitted), only Security Officers who have the **Generate key** and **Generate profile** right can generate keys. They can no longer generate keys that do not have a value. If the Security Officer does not assign a value to a key when it is created, this value is generated automatically when the key is saved.

For group keys, whose values are generated when policy files are generated, the values are also generated immediately when they are used to create an encryption rule.

If this option is active, Security Officers who do not have the **Create Profiles** right cannot generate keys.

They are also unable to use group keys (<GROUPKEY> in encryption rules.

Note: The **Only Security Officers with the 'Generate profile' right can generate keys (keys without a value are not permitted)** option does not influence how user-specific keys (<USERKEY> are used in encryption rules!

3.5.3 The Certificates tab

Here you can specify key length (1024, 2048, 4096 Bit) and validity for new certificates generated by SafeGuard LAN Crypt.

Under Friendly name for newly created certificates you can specify a name for certificates created by SafeGuard LAN Crypt. All certificates get this name and can therefore easily be identified as SafeGuard LAN Crypt certificates.

If you activate the **Add critical extensions to newly created certificates** option, a critical extension that indicates to other applications that they must not use these certificates, is added to newly created certificates.

You can also specify a warning period, in days, within which the system displays a warning (if the rules are canceled, or by marking certificates yellow in the list).

3.5.4 The Resolving Rules tab

Skip users that have no valid certificate when resolving

In this section "cancellation" means "ignoring" when referring to rules. Select this option if you want the system to ignore users to whom no certificate has been assigned, when generating policy files. As a result, no policy files are generated for these users.

Note: If a user is created, and this option is selected, and no certificate has yet been assigned to the user, the system does not display a warning if it is unable to create policy files for this user when resolving (applying) the encryption rules.

Select how the rules should be ordered on the client:

Note: This setting is only applied to clients of version 3.90 or higher.

Here you can choose from three different sorting methods. Sort method 3 is the default method which is used by Client versions below 3.90:

- **Sort method 1**

1. Ignore rules
2. Exclude rules
3. Encryption rules

- **Sort method 2**

1. Ignore rules
2. Exclude rules
3. Encryption rules specified as absolute paths without wildcards
4. Encryption rules specified as absolute paths with wildcards not including sub-folders
5. Encryption rules specified as absolute paths with wildcards including sub-folders
6. All other encryption rules

An absolute path is either a UNC path (begins with double backslash) or **<drive letter>:**.

For example: `\\server\share*.*` or `c:\encrypt*.*`.

- **Sort method 3 (default)**

Sort method 3 does not distinguish between ignore, exclude and encryption rules.

The rules are sorted in the following order:

1. All absolute paths without wildcards
2. All absolute paths with wildcards not including sub-folders
3. All absolute paths with wildcards including sub-folders
4. All other rules

An absolute path is either a UNC path (begins with a double backslash) or **<drive letter>:**.

For example: `\\server\share*.*` or `c:\encrypt*.*`.

Within one of the above sections (for example: Sort method 3 - All other rules), the rules are ordered depending on how precise the path definition is.

The order is as follows:

1. UNC paths
2. Paths starting with <drive letter>: Here the backslash after the drive letter is not considered.
3. All other paths

Additionally:

- Paths with more backslashes are listed before paths with fewer backslashes
- Paths without wildcards are listed before paths with *. and *.* wildcards

Note: Changes to this option become effective on the clients after new profiles have been generated and distributed.

Select which encryption format should be used by the SafeGuard LAN Crypt Client

Here you can configure which file encryption mode is used by the clients. SafeGuard LAN Crypt supports the following encryption modes:

- CBC format (versions 3.50 or higher)

This format is used by client versions 3.50 and higher. These clients can read files encrypted in OFB mode (legacy format). The file encryption mode for new files is CBC.

- XTS-AES format (versions 3.90 or higher)

This format can be used by client versions 3.90 and higher. These clients can read files encrypted in OFB and CBC mode. File encryption mode for new files is XTS-AES. This mode will only be used for AES keys. If a file is encrypted with a key using another algorithm, CBC encryption mode is used instead.

For client versions below 3.90 only the following configuration is valid:

CBC format for encryption with the optional usage of Legacy format as „old encryption format“. All other settings are ignored by these clients. They use CBC or Legacy format by default.

Use this encryption file format until a defined date

During an upgrade process an old encryption mode can be configured. This old encryption mode is active until a specified date. Starting with this date all clients must be migrated to support the configured file encryption mode. Otherwise new clients create encrypted files using the configured mode, but these files cannot be read by older clients.

Depending on the setting for the encryption format to be used, the following formats can be selected here:

- Legacy format (versions 2.x, 3.0x, 3.1x)
- CBC format (version 3.50 or higher)

is only available if XTS-AES is configured as encryption file format.

CBC requires a client version 3.90 or higher. Older clients evaluate the **Use this encryption file format until a defined date** setting only, if **Legacy format** is selected.

You must specify the date until which the old format is used to encrypt files. After this date, or if the option is cleared, the files are written with the new encryption format. Any changes to this option are only effective on the clients after new profiles have been generated and distributed.

After all clients have been updated we recommend that you perform initial encryption with the initial encryption tool. You thereby ensure that only the new SafeGuard LAN Crypt encryption format is used.

This change becomes effective the next time the encryption rules are resolved.

3.5.5 The Server tab

To import groups and users from a server, SafeGuard LAN Crypt requires the logon information for that server. You must enter this information in the Server tab. Click **Add** to open another dialog, which has three tabs: **Details**, **Preferences** and **Certificates**

3.5.5.1 Server details: Password logon

1. Enter the Domain or Server Name, User Name and the appropriate Password. To prevent duplicate entries, please also enter an alternative name as an Alias for the server in case several names can be used to access the same server.

Note: If you use a Microsoft directory service, do as follows:

- Enter the domain name under **Domain or Server Name**.
- Enter the **user name** as **user name@domain**.

Note:

The user name must be entered in LDAP syntax (canonical name) to import objects from a non-Microsoft directory service.

Example: **cn=admin,O=techops**

2. Specify the API to be used. Select **<Microsoft>** or **<other>** from the drop-down list. The placeholder **<other>** stands for all non-Microsoft APIs.
3. Specify the LDAP authentication method to be used for accessing the server. SafeGuard LAN Crypt offers these methods:
 - Password (LDAP)
 - Password (LDAP with SSL)
4. Click **OK**.

The server is shown in the table on the **Server** tab.

Error message upon logon failure:

If SafeGuard LAN Crypt cannot perform the logon to the server successfully, an error message will be displayed in the SafeGuard LAN Crypt Administration.

3.5.5.2 Server details: Anonymous logon

1. Enter the **Server Name**. To prevent duplicate entries, please also enter an alternative name as an Alias for the server in case several names can be used to access the same server.
2. Specify the API to be used. Select **<Microsoft>** or **<other>** from the drop-down list. The placeholder **<other>** stands for all non-Microsoft APIs.
3. Specify the LDAP authentication method to be used for accessing the server. SafeGuard LAN Crypt offers these methods for anonymous logon:
 - **Anonymous (LDAP)**
 - **Anonymous (LDAP with SSL)**
4. Click **OK**.

The server is shown in the table on the **Server** tab.

Error message upon logon failure

If SafeGuard LAN Crypt cannot perform the logon to the server successfully, an error message will be displayed in the SafeGuard LAN Crypt Administration.

3.5.5.3 Preferences

Identification of an Object

SafeGuard LAN Crypt uses a precise, unchanging GUID (Global Unique ID) to identify imported objects in the Active Directory. This GUID is also used to synchronize the database and directory service, because, for example, the names of individual single objects can change, to ensure that updates in the Active Directory are mirrored in the database, and that no new object is generated in the database because of a new name in the Active Directory.

However, some other directory services do not use this type of ID. In this case SafeGuard LAN Crypt provides another way of unambiguously identifying objects. SafeGuard LAN Crypt can be configured so that certain LDAP attributes are used to uniquely identify the objects. You configure these attributes in SafeGuard LAN Crypt administration.

The settings **<standard>** and **<other>** are always available. Usually the **<standard>** setting will be sufficient for the server, to which the setting refers. The attributes evaluated by the **<standard>** setting always appear below **<standard>**. In this way you can show which attributes are evaluated in the default setting. You can also assign a specific attribute if all these attributes are already present in the directory service concerned. Use **<other>** to specify an attribute other than those that are already displayed.

Note: If you enter an attribute here, make sure that it contains data that will unambiguously identify the object.

- **Object GUID**

Here you specify which attribute is used for identification. If you leave the setting at **<standard>**, both attributes, GUID and objectGUID are evaluated. If you want to use another LDAP attribute to identify the objects, select **<other>** under **Object GUID** and enter the name of the LDAP attribute in the entry field beside it. This attribute must contain data that will unambiguously identify the object.

- **GUID attribute has a binary value**

This option only affects how the GUID appears in the object **Properties** dialogs. To display these correctly, activate this option if the GUID you use has a binary value. If you are not sure what to do, activate this option.

3.5.5.4 Attributes for Users

- **Username Attribute**

This setting only affects how users are displayed in the SafeGuard LAN Crypt Administration Console. The users are displayed in a group's **Properties** dialog and in the **User and Certificates** snap-in. You can select one of the existing attributes or enter an LDAP attribute by selecting **<other>**. **<standard>** evaluates (CN and SN).

- **Logonname attribute**

Special meaning that is attached to the attribute for the logon name. SafeGuard LAN Crypt names the policy files after the user logon name. A user can only logon if their logon name and policy file name are identical. Here you can specify, which LDAP attribute is used to define the user's logon name. **<Standard>** evaluates **SAMAccountName**, **userPrincipalName** and **UID**. If two or three of these attributes are already present in the directory service, you can select the one which defines the user's logon name. Select **<other>** to specify another directory service attribute that contains the logon name.

Note:

If the name in the attribute contains the @character, SafeGuard LAN Crypt cuts off the name at this point. This may cause problems, for example, if e-mail addresses are used.

- **Attribute for E-Mail Address**

This attribute is added to self-generated certificates.

- **Attribute for comment**

Like the e-mail address, this attribute can be used to identify user objects. This is especially useful if the user name and the logon name cannot be used by the wizard to identify objects when certificates are being assigned. At this point you can enter the name of the attribute that the wizard is to use to identify the correct user when certificates are being assigned.

Note:

If empty attributes are imported during synchronisation (for example due to the fact that an attribute was deleted in the AD), SafeGuard LAN Crypt comments are not affected. Existing entries are maintained. New attribute contents overwrite existing comments. If you select **<Standard>** comments are not imported.

3.5.5.5 Certificates

On the **Certificates** tab, specify whether the certificates that were assigned to the user in the LDAP directory, are to be transferred when the user is imported into the SafeGuard LAN Crypt database. You then no longer need to assign certificates for these users in the SafeGuard LAN Crypt Administration Console. Here you can also specify an attribute which contains the user's certificate.

Note: Certificates assigned this way are not checked (expiration time, on a CRL, etc.)!

Activate the

- **Automatically passing certificates when importing users**

option, if certificates from the LDAP directory are to be automatically imported and assigned to the user when they are imported to the SafeGuard LAN Crypt database.

<Standard> evaluates **userCertificate** and **userCertificate; binary**. Click **<other>** to specify another attribute that contains the certificate.

When you click **OK** SafeGuard LAN Crypt transfers the logon information to the servers list. You can also edit or delete these details in this list.

3.5.6 The Directories tab

Note: The settings you make here are always saved in the current configuration record for the SO. If no configuration records have yet been created, the system uses the **<DEFAULT CONFIGURATION>** configuration record.

Storage location for generated policy files

You must specify where the policy files generated for the users are to be saved.

Enter the storage location (usually a network drive that has been shared with the user) in the input field. The folder you enter here must already be present!

Note:

Check that the user can access this folder, as the generated POL (policy) files are loaded or copied from it when the user logs on.

You must also specify the storage location for the policy files from the client's point of view. You will find this setting under SafeGuard LAN Crypt Configuration.

Policy file options - specifying policy file format

If you use different SafeGuard Client versions, you have to make sure that all of your SafeGuard Clients can read the generated policy files. SafeGuard LAN Crypt supports different policy file formats:

- Create legacy policy files (.pol) SafeGuard LAN Crypt Client versions older than 3.12.1
- Create legacy policy files (.pol.bz2) (default) SafeGuard LAN Crypt Client versions older than 3.90
- Create new policy files (.xml.bz2) SafeGuard LAN Crypt Client version 3.90 or higher

Select the format that covers all of your clients.

Note: In case your client cannot read the received policies a corresponding message is displayed. After you have changed the setting you have to build the policy files and distribute them to the clients so that the clients can make use of the new policy files.

Create additional policy files based on Novell name

If you activate this option, SafeGuard LAN Crypt generates two policy files for each user. One file has the Novell logon name and the other has the Windows user name. The contents of these files is identical.

Using the Novell logon name must also be specified in LAN Crypt Configuration/Client Settings before you can use it to log on.

Note: This setting affects the way in which profiles are deleted in the SafeGuard LAN Crypt Administration Console. The process for deleting profiles is similar to the one for creating profiles. If the Novell logon name is to be used here (two policy files are created), both profiles are deleted if this setting is not changed. Deleting means to generate empty policy files here. If the setting is changed at runtime, it may occur that, although two policy files have been created, only the one with the Windows user name is deleted. This is because the setting has been deactivated, and therefore only the policy file with the Windows user name is deleted. The Novell policy file remains in the defined storage location and can theoretically be used for logging on. The system behaves in a similar way, if **Compress policy files** is activated. In this case up to four policy files are generated for each user.

Please keep this in mind and, if necessary, coordinate with the system administrator.

Storage location for generated certificates and key files (*.p12)

If required, SafeGuard LAN Crypt can generate self-signed certificates. These certificates (.p12 files) are generated when the certificates are assigned to users.

The location to which these files are to be saved has to be specified in the Directories tab.

The public part of the Security Officer's certificate (.cer), which is used to secure the administration database, is also saved here.

The key files (.p12) and the public part of the Security Officer's certificate must be made available to the users.

To do this in SafeGuard LAN Crypt Configuration, specify the folder in which SafeGuard LAN Crypt is to search for a .p12 file for the user, if the private key for the policy file is not present. The same applies to the public part of the Security Officer's certificate.

So that SafeGuard LAN Crypt automatically recognizes the user key files, the file names must match the user's logon name ("**Logonname.p12**").

When SafeGuard LAN Crypt finds the correct file, it displays a PIN dialog. You must send a PIN letter to tell the user this PIN (which is in the password log file). The certificate and associated key are automatically imported after the user enters the PIN.

If SafeGuard LAN Crypt finds a .cer file that contains the public part of the Security Officer's certificate, it automatically imports it.

Note: You must set the appropriate paths in SafeGuard LAN Crypt Configuration before you can use this functionality.

Alternatively you can distribute the key files for the users and the public part of the Administrator certificate manually. If you do this, make sure that the clients import both of them.

Note: The clients have to import the public part of the certificate of the particular Security Officer who generated the policy files. If you change the path on which the .cer files of the Security Officers and the .p12 files of the users are stored, after you have created Security Officers, you must copy their .cer files to the new location. Otherwise the public parts of the Security Officers certificates will not be found.

Default password for user key files

In SafeGuard LAN Crypt you can define a uniform password for all user key files.

To do this, copy a file that contains the password you want (up to 32 characters) to the same directory that contains the password log file (see Logfile for passwords of keyfiles on page 47 xxx).

The file containing the password has to have the same name as the corresponding password log file (default name: p12pwlog.csv) but has to have the file extension .pwd (similar to the default name of the password log file: p12pwlog.pwd). If the system finds this type of file, all generated user key files will have this password.

In this file, if you enter ***logonname*** as the keyword, instead of the default password, the current logon name will be used as the password.

Note: .p12 files for Security Officers are ALWAYS given a random password because they have higher security.

Storage location for generated Security Officer certificates (*.p12)

SafeGuard LAN Crypt stores Security Officer certificates in .p12 files, for example, as backups. Here you can specify the folder to which they are saved.

Note: Because they involve sensitive data it is vital that you protect them against unauthorized access!

Logfile for passwords of keyfiles

Here you can specify the storage location and name for the log file for the generated PKCS#12 files (default name: p12pwlog.csv). This file contains the passwords for the generated PKCS#12 files and can be used, for example, to create a PIN letter.

The .csv file contains the following information (the keywords in brackets represent the column headers in the .csv file):

- Date of generation (**CreateDate**)
- Time of generation (**CreateTime**)
- Expiration Date (**ExpirationDate**)
- Exact time when validity ends (**ExpirationTime**)
- User name (**Name**)
- Logon name (**Logonname**)
- E-mail address (**EMail**)
- Generation mode (**Mode**). Possible values are:
 - <GUI> certificate was generated in the user's **Properties** dialog.<SO> certificate of an SO. Was generated when the SO was created.<WIZARD> certificate was generated using the Certificate Assignment Wizard.
- File name (**FileName**)
- Password (**Password**)

Note:

You should protect this file and under no circumstances save it in the same folder as the POL files.

If the user who is assigning certificates has no file system right to change the password log file, SafeGuard LAN Crypt will not be able to generate certificates.

3.5.7 The Regions tab

In SafeGuard LAN Crypt you can set up regions to make key administration easier and less complex. Each region is assigned to a specific Security Officer who is then responsible for it. When this Security Officer generates keys, the system automatically adds the prefix for this region at the beginning of the key names. As a result you can always see the administrative unit for which each key was generated. This approach is particularly useful in distributed environments.

Enter the name and prefix for the regions in the appropriate input fields. Click **Add** to add a new region to the list of existing regions. You can select the regions displayed here when you create a Security Officer.

To change or delete an existing region, select it and then click **Edit** or **Delete**.

Note:

You can only delete a region if it is not assigned to a Security Officer.

3.5.8 The Configurations tab

On this tab you can generate particular configuration records for the individual regions, and then assign them to a Security Officer.

The configuration records contain all the details that can be entered on the *Directories* tab:

- the storage location for generated policy files
- the storage location for generated certificates and key files
- the storage location for generated Security Officer certificates
- the storage location and name of the password log file
- the options for the policy files

The configuration records are always assigned to an existing region. Usually, an SO assigned to a region can only ever use the configuration records that have been generated for this region. The exception is the **<DEFAULT CONFIGURATION>** configuration record, which can be used in every region.

By using one particular configuration for one organizational unit (region) you easily ensure that the correct paths can be set for one or more Security Officers, and that all SOs always use the same paths to save the generated files.

Changes on the **Directories** tab are always saved in the currently-assigned configuration record.

Note:

The global right Change Configuration specifies whether an SO is permitted to change their own configuration settings. If an SO does not have this right, they can only use the selected paths. If an SO changes an existing configuration record, they also change the configuration for all the SOs who are also assigned to this configuration.

3.5.8.1 Generating a configuration record

1. Select an existing region, for which you want to create the configuration record, or select **<no region>** to create a configuration record to which SOs who are not in a region can be assigned.

2. In **New Name** enter a name for the new configuration record.
3. Select an existing configuration record in the list. The system copies this configuration record and saves it with the new name. Click **Copy**.
4. If you want to edit the configuration record, select it and click **Edit**.
5. You see a dialog which is the same as the Directories dialog in Properties. Here, enter the appropriate paths and define the policy file options. Click **OK**.
6. The system now displays the new configuration record in the list, in the appropriate region, and you can use it to create more SOs. To change the configuration (and the region) of an existing configuration record, select the Properties tab for the particular SO.
7. You can create as many additional configuration records as you require.

3.5.9 The Additional Authorization tab

In SafeGuard LAN Crypt you can define that particular actions require additional authorization by least one more Security Officer. Additional authorization can be required for the following actions:

Actions	Necessary permissions
Change Additional Authorization Settings	Can only be performed by a Master Security Officer.
Change Recovery Key	Can only be performed by a Master Security Officer.
The following actions can only be performed by SOs who have the global right to authorize operations and have the right to perform the action. IMPORTANT: Please note that having only the global right to provide an additional authorization may not be enough in some situations. The Security Officer providing the additional authorization must have the corresponding right for this specific object.	
Changing Global Settings	Requires the global right Change Configuration . The system prompts for authorization when you make changes on the Algorithms, Certificates, Regions, Directories, Keys, Antivirus software, Resolving rules, Server, Configuration , and Other Settings tabs. Only Master Security Officers can authorize changes to the Algorithms, Certificates, Keys, Resolving rules, Regions , and Other Settings tabs!
Create Security Officer	Requires the global right Create SOs
Change Access Control Lists	Requires the global right Change global rights and the corresponding group or SO-specific rights.
Change Permissions	Requires the global right Change ACLs .
Assign Certificate	Requires the global right Assign Certificate and the corresponding group-specific rights.
Use or group-specific keys editing	Requires the global right Use specific keys . Specifying additional authorization for using specific keys does not affect the use of the placeholders <userkey> or <groupkey>. It only restricts handling (displaying/using/ editing) an actual specific key.
Administer Groups	Requires the global right Change Groups and the corresponding group-specific rights.
Administer Users	Requires the global right Change Users and the corresponding group-specific rights.
Manage Logging	Requires the global right Read Logging Entries and Manage Logging
Create rules	This requires the global right Generate Rule along with the corresponding group-specific right.
Create Move Keys	Requires the global right Create Key along with the corresponding group-specific right.
Create Profiles	Requires the global right Generate Profiles as well as the corresponding group-specific right.
Display Value	Requires the global right Read Key . Additional authorization is required when checking the Display Key value option in a key's properties dialog.

If an additional authorization is necessary for one of these actions, you must specify how many Security Officers are required for that action.

To do this, select that action. When you double-click the selected action, a dialog opens in which you can specify how many Security Officers are required. When you click **OK** SafeGuard LAN Crypt updates the list on the **Additional Authorization** tab.

A message is displayed if the system recognizes that the required number of Security Officers is not available.

Note: The system cannot precisely find out how many Security Officers are actually available. The number you require may not actually be available even though the message does not appear. For example, a Security Officer's rights may have been changed afterwards or a Security Officer may have been deleted.

If you are informed that the required Security Officers are not available and you specify that at least one additional Security Officer is required when defining the number of required Security Officers and you confirm your setting with **OK** and close the dialog, the setting will nevertheless be adopted due to technical reasons. This will lead to a situation where actions requiring additional authorization can no longer be carried out as the necessary Security Officers are not available. If this setting is specified for the **Change additional authorization settings** option, the settings in this dialog can no longer be modified. The setting can only be changed by generating a recovery key (see *Cancelling additional authorization*)

A similar situation can be caused by deleting Security Officers as the system does not check whether the required number of Security Officers for additional authorization is still available after deleting a Security Officer. SafeGuard LAN Crypt only ensures that a Master Security Officer exists in the system.

Note: If you do not use tokens for additional authorization, we recommend to set **Strong private key protection** to **Yes**.

Providing additional authorization

If additional authorization has been specified for an action, the additional authorization wizard runs when that action is selected. This wizard prompts for authorization by at least one more Master Security Officer. You can select the relevant Master Security Officer in a dialog. If SafeGuard LAN Crypt uses this Security Officer's certificate to authenticate them successfully, the required action can be performed.

If several Security Officers have the same certificate, this certificate can only be used once in one authorization run. Any other SO to whom this certificate is assigned is removed from the list of SOs.

Note: The dialog in which you select a Security Officer has an option that allows you to restrict the display to SOs in one particular region. Security Officers who are not assigned to any region are always displayed in the list.

Cancelling additional authorization

An additional authorization for an action usually applies for the entire duration of one SafeGuard LAN Crypt Administration session. Click the **Cancel authorization** button in the Administration tool bar, to delete the relevant information, so that an additional authorization is required the next time the action is performed in the same session.

Waiving additional authorization

If the configuration causes a situation, where too few Security Officers are present to provide additional authorization for an action, you can use the recovery key to reset the number of Security Officers required to change the additional authorization settings to 0.

To do this, click **Assign Certificate** in the logon dialog. This runs a wizard that allows you to reset the number of additional Security Officers required to 0. For details see below.

3.5.10 The Recovery Keys tab

In SafeGuard LAN Crypt you can generate a recovery key. You can use this key to assign a new certificate to a Security Officer when they log on to the SafeGuard LAN Crypt Database (click the "Assign certificate" button), if their certificate is, for example, damaged and can no longer be used. Using the recovery key, you can also reset the number of additional Security Officers required for changing the settings for additional authorisation to 0.

A recovery key can be split into several parts and you can specify how many parts are necessary to assign a new certificate. The individual parts of the recovery key can be distributed to different Security Officers. The owners of the individual parts must be present when the recovery key is used, and use a wizard to present the parts of the key. The (parts of the) recovery key can be entered manually or loaded from a file.

To generate a recovery key, click the **Generate recovery key** button on the Recovery Keys tab. This runs the wizard used to generate the recovery key.

Using the drop-down menus, select how many parts the key is to contain and how many of them are necessary for using the recovery key. In our example the key is to have three parts, of which at least two are needed to assign a new Security Officer certificate during logon. Click **Next**.

For each part of the key the Wizard displays a dialog in which you can specify whether the partial key is saved in a file or displayed on screen so you can write it down. Once all parts have been processed, the Wizard closes.

On the Recovery Key page, next to Default Recovery Key, you can see how many parts the key contains (in our example, 3) and how many of these parts are necessary, when they are used (in our example, 2).

Note:

When you generate and distribute the parts of the recovery key, remember that they involve extremely sensitive data. It is essential that you protect the Recovery Key against unauthorized access.

You can only ever use the most recently-generated recovery key. Previously-generated recovery keys are no longer valid and cannot be used to assign a certificate.

Using the recovery key

If it is no longer possible to log on to the database (e.g. because a certificate has expired), click **Assign certificate**, in the logon dialog, to start the *Recovery Key Wizard*.

If a dialog informs you that the certificate cannot be used, after you have selected a Security Officer, you can start the wizard from there.

Follow the instructions on the screen.

This wizard contains a dialog in which you can reset to 0 the number of Security Officers needed to change the settings for additional authorization.

This ensures that no situation can arise in which additional authorization is no longer possible because there are no Security Officers who can perform it.

If you activate this option, a single Security Officer can change the settings for additional authorization afterwards.

3.5.11 The Database tab

Note: This setting is only necessary if you use an Oracle database, which is accessed over Administration Consoles on different machines. The setting can only be made by a Master Security Officer!

Oracle's National Language Support (NLS) converts text for the user so that it is always displayed in the same way, no matter which character set is used, even if the characters' numeric encoding is different because of the different character sets (example: WE8MSWIN1252: ü=FC00, AL16UTF16: ü=7C00).

If text is added to the database and extracted using a different character set, this could lead to errors when calculating the checksum (MAC), as, for example if characters were converted to binary, the binary data would cause problems for the MAC.

To avoid these errors, make sure that the same code page/character set is used on all machines that access the database over the Oracle client.

In the **Database** tab you can specify a character set, which has to be used on all the machines, from which the database is accessed. When starting the Administration Console SafeGuard LAN Crypt checks whether or not the settings of the Oracle client match the settings in the database. If not, a warning is displayed and the Administration Console will not start up.

In the edit field, enter the character set to be used on the Oracle clients to allow a logon to the database. On an Oracle client this setting is in the registry under the value NLS_Lang (**Language.Territory.CharacterSet**, example: **GERMAN_GERMANY.WE8MSWIN1252**).

The character set of the current machine is displayed under **INFO:** in the **Database** tab. Usually this character set must also to be used by all other clients which access the database.

Note:

We recommend that you use only one character set! If you use more than one character set, errors may occur when calculating the checksum (MAC). However, in general, it is possible to use more than one character set. Despite this, you

should only use more than one if the character sets are largely identical and differ only by a few characters. You should identify these characters and not use them for database entries.

Deactivating this check

SafeGuard LAN Crypt allows you to deactivate the character sets check. If the edit field is left blank, no check is performed and it is always possible to log on to the Administration Console. Please be aware, that this may lead to errors, when the checksum (MAC) is calculated.

To prevent errors occurring when a character set is specified (for example typing errors), which may lead to the situation in which the Master Security Officer, who made the setting, can no longer log on to the Administration Console, SafeGuard LAN Crypt checks the data that was entered when you press **Apply** or **OK**. If the specified character set does not match the one currently used on this machine, a message is appears and the character set that is currently valid is added to the edit field. The *Database* tab remains on the screen, to check the data that was entered. If necessary change the settings and press **Apply** or **OK** again.

3.5.12 The Database tab

Note: This setting is only necessary if you use an Oracle database, which is accessed over Administration Consoles on different machines. The setting can only be made by a Master Security Officer!

Oracle's National Language Support (NLS) converts text for the user so that it is always displayed in the same way, no matter which character set is used, even if the characters' numeric encoding is different because of the different character sets (example: WE8MSWIN1252: ü=FC00, AL16UTF16: ü=7C00).

If text is added to the database and extracted using a different character set, this could lead to errors when calculating the checksum (MAC), as, for example if characters were converted to binary, the binary data would cause problems for the MAC.

To avoid these errors, make sure that the same code page/character set is used on all machines that access the database over the Oracle client.

In the **Database** tab you can specify a character set, which has to be used on all the machines, from which the database is accessed. When starting the Administration Console SafeGuard LAN Crypt checks whether or not the settings of the Oracle client match the settings in the database. If not, a warning is displayed and the Administration Console will not start up.

In the edit field, enter the character set to be used on the Oracle clients to allow a logon to the database. On an Oracle client this setting is in the registry under the value NLS_Lang (**Language.Territory.CharacterSet**, example: **GERMAN_GERMANY.WE8MSWIN1252**).

The character set of the current machine is displayed under **INFO**: in the **Database** tab. Usually this character set must also to be used by all other clients which access the database.

Note:

We recommend that you use only one character set! If you use more than one character set, errors may occur when calculating the checksum (MAC). However, in general, it is possible to use more than one character set. Despite this, you should only use more than one if the character sets are largely identical and differ only by a few characters. You should identify these characters and not use them for database entries.

Deactivating this check

SafeGuard LAN Crypt allows you to deactivate the character sets check. If the edit field is left blank, no check is performed and it is always possible to log on to the Administration Console. Please be aware, that this may lead to errors, when the checksum (MAC) is calculated.

To prevent errors occurring when a character set is specified (for example typing errors), which may lead to the situation in which the Master Security Officer, who made the setting, can no longer log on to the Administration Console, SafeGuard LAN Crypt checks the data that was entered when you press **Apply** or **OK**. If the specified character set does not match the one currently used on this machine, a message is appears and the character set that is currently valid is added to the edit field. The *Database* tab remains on the screen, to check the data that was entered. If necessary change the settings and press **Apply** or **OK** again.

3.5.13 The Antivirus tab

For virus scanners to be able to scan files encrypted with SafeGuard LAN Crypt, you have to specify the scanners here. The antivirus software will be granted access to all SafeGuard LAN Crypt keys and will therefore be able to recognize virus signatures in encrypted files. This is not possible without the SafeGuard LAN Crypt keys.

To add a virus scanner, click **Add**. Enter the following data in the dialog displayed:

- A name for the antivirus software (this name is displayed on the **Anti-virus-Software** tab under **Product**)
- The name of the executable of the software performing the scan

Enable the Use Authenticode Verification option.

Note: We recommend using an Authenticode signed virus scanner by all means to specify the scanner here and to enable Authenticode verification. Only this verification ensures that the executable is truly the required executable of the virus scanner and that thus only trustworthy applications have access to the SafeGuard LAN Crypt keys.

After clicking **OK** the antivirus software is displayed in the list. You can add further virus scanners.

3.5.14 The Client API tab

SafeGuard LAN Crypt provides a Client API to allow applications to control the file encryption functionality via a simple command line or a COM-style API. For details please see the Client API documentation in the \DOC folder of your unzipped installation package.

Note: The API has to be selected during installation of the SafeGuard LAN Crypt Client. If you want the Client API to be used on your clients, make sure that it is installed properly.

On the **Client API** tab you specify the settings for the Client API.

- Select **Enable Client API** to make the API available on the client. Applications can now control the file functionality via the COM-style API.
- Select **Enable API access for SafeGuard file encryption command line tool** to allow controlling the file encryption functionality via a simple command line tool.
- **COM-style API only:** by default encryption rules defined in SafeGuard LAN Crypt Administration have priority over encryption tasks performed via the Client API. If you want the „API rules“ to have priority select the **API rules have priority over encryption rules in profile** option. **Note:** SafeGuard LAN Crypt Ignore rules and Exclude rules have the highest priority and cannot be overruled by API rules and the same files/directories are automatically excluded from encryption (see Files/directories excluded from encryption on page 7).

Note: SafeGuard LAN Crypt Ignore rules and Exclude rules have the highest priority and cannot be overruled by API rules and the same files/directories are automatically excluded from encryption (see Files/directories excluded from encryption on page 7 xxx).

Since API access is restricted to allowed applications you have to specify which applications are allowed to use it. To do so

1. click **Add** on the **Client API** tab..
2. Enter the name of the application.
3. Specify the executable which will access the API.
4. If you want Authenticode signed executables only to access the API select the Executable file must be Authenticode signed option.

5. If you want only executables signed by trusted vendors to be used additionally select the **Executable file must be Authenticode signed by a trusted vendor** option. This ensures that only executables are accepted which are signed using the certificate that is registered as **Signature certificate** of a vendor on the **Trusted Vendors** tab.

Note: Trusted vendors have to be registered on the Trusted Vendors tab in the SafeGuard LAN Crypt Preferences.

6. Optionally enter a comment.

After clicking **OK** the application is displayed in the list. You can add further applications.

3.5.15 The Trusted Vendors tab

On the Trusted Vendors tab you can register vendors which are accepted to Authenticode sign an executable to access the Client API.

To add a trusted vendor

1. click **Add** on the Trusted Vendors tab.
2. Enter the name of the vendor.
3. Enter the vendor's signature certificate. If selected on the Client API tab the API will only accept executables which are Authenticode signed using this certificate.
4. Optionally enter a comment.

After clicking **OK** the vendor is displayed in the list. You can add further vendors.

3.5.16 The Other Settings tab

Security officer options

SafeGuard LAN Crypt can be configured to automatically create an ACL with the viewing right for the root group for a newly created Security Officer. Requirement is that the SO has the global permission Administer group or Administer users. This guarantees that the SO can access (view and/or edit) all groups they are responsible for.

If you select the Set group permissions for security officers who are allowed to administer groups or users option, ACLs for the root group are created automatically.

Cryptographic Service Provider options

If **Use key wrapping (default setting)** is selected, the Security Officer data and user profile data will be encrypted using a random session key with the selected algorithm (default 3DES). This sessions key then again is RSA-encrypted with the public key from the certificate.

If you use smartcards, make sure that the smartcards you want to use support the algorithm you selected.

If you deselect this option, data is RSA-encrypted without a session key. Note that this option may not be supported by smartcards.

3.6 Displaying all SafeGuard LAN Crypt keys

By selecting the **All SafeGuard LAN Crypt keys** node you can display an overview of all the keys that are currently being managed by SafeGuard LAN Crypt. You can view the following information here:

- Long key name

- The algorithm used for the key
- Tells you if the key is active
- The person who generated the key (generator)
- Tells you if the key should be inherited
- Tells you for which group the key was generated
- Tells you if the key is in use
- Comment field

Click a column header to sort the table contents in ascending or descending sequence, to find the information you require.

3.6.1 Finding keys

In addition to sorting key information you can also search for a particular key. To do this, right-click **Display all SafeGuard LAN Crypt keys** tab and then select **Find a key** from the context menu.

Note:

The **Find a key** function is also available for the group key tab in every group. To add a key to a group, you also need the right *Copy key* for the group the key is in as well as the right *Create key* for the group the key is to be added to.

This starts a wizard which will help you find the key you want. In step 1 you can specify whether you want to search for the key using its GUID or its name.

Example: `{[56]}%` returns all the keys whose GUIDs start with 5 or 6.

Then click **Next** to search the database for the key you require. If the key is found, step 2 shows you the key's name, its GUID and the group in which it was generated.

If you called the Find a key function from a group key-node in a group, activate the **Assign keys in the current group** option to create a link to the key you found. You can then use a key that was generated in another group in the group that you have currently selected. If you activate this option, click **Next** and then click **Close** in step 3, you will see a special key icon in the node group key of the appropriate current group. You can now use this key in encryption rules.

Note:

If you select the **Assign keys from the current group** option it is only effective if you called the **Find a key** function from the **Group key** tab in a group, and not from the **Display all SafeGuard LAN Crypt keys** tab. Also specific keys can be selected but they will not be assigned to the current group. If your selection contains a specific key a corresponding message will be displayed on the wizard's last page.

3.7 Showing selected users and certificates

The **Selected users and certificates** node is only available, if the **Show "Selected users and certificates"** option is active in the **SafeGuard LAN Crypt Administration** user settings (see User settings on page 35 xxx).

Upon clicking node **Show selected users and certificates** a dialog will be displayed for selecting the users to be shown. As displaying all users can be very time-consuming, SafeGuard LAN Crypt allows you to define search criteria to filter the search process.

Note:

If the system is set to cache user lists, you have to update the display either via the icon shown in the toolbar or by pressing F5 first, to be able to enter new search criteria.

Select option **Display matching users** to activate the input fields for defining your search criteria:

The following user information will be retrieved from the SafeGuard LAN Crypt database

- Logon name
- User name
- Assignment between user and certificate
- Requestor of the certificate
- Serial number of the certificate
- Date from which the certificate is valid
- Date up to which the certificate is valid
- Name of the parent group

You can define search criteria based on these attributes. SafeGuard LAN Crypt searches for defined character strings in the user attributes retrieved.

In the first drop-down list, you can select the attribute(s) on which the search process is to be applied.

In addition you can define whether the selected attribute should correspond to the character string entered (**should be**) or if only users are to be displayed, for whom the selected attribute does not correspond to the character string entered (**must not be**).

In the drop-down list on the right-hand side, you can enter the character string SafeGuard LAN Crypt searches for in the defined attribute.

You can use the following SQL wildcards for entering the character string:

% any character sequence

_ single character (e.g., a__ means search for all names containing three characters and starting with a)

[] single character from a list (e.g., [a-cg]% means search for all names starting with a, b, c or g)

[^]single character not contained in a list (e.g., [^a]% search for all names not starting with a)

You can specify up to three conditions for the search process.

If you enter more than one condition, you can define how these conditions are to be combined (AND/OR).

Right-click **Show selected users and certificates** to use all functions of the certificate snap-in that are available for each individual group (see Assigning certificates on page 105 xxx).

At this point, the certificate assignment wizard is only available to Master Security Officers. If a Security Officer has the appropriate permissions they can use the **Properties** menu to assign a certificate to one specific user.

However, if the Security Officer does not have any permissions for this user, the corresponding icon is displayed.

3.8 Creating a Security Officer

Master Security Officers and entitled Security Officers can create additional Security Officers. These Security Officers can then be assigned to individual organizational units. Initially they are granted global rights that define precisely which tasks they can perform. Once Security Officers have been assigned to an organizational unit (an object in SafeGuard LAN Crypt Administration), ACLs can be used to restrict their rights again to suit this particular object.

Note: If a Security Officer's global rights do not permit them to perform a particular action, an ACL cannot be used to grant them the right for this action.

1. To create a new Security Officer (SO), select the Central settings/Security Officers Administration tab. To open the initial dialog for creating an SO, click **Add new SO...** in the context menu for this node, or click Add new SO... in the **Action** menu.

2. In this dialog enter a name, and if necessary an e-mail address and a comment. Then click **Next**.

Note: The e-mail address is added to the password log file for certificates generated by SafeGuard LAN Crypt. It can, for example, be used to create a PIN letter via e-mail.

3. Now, in the dialog, specify whether the new Security Officer is to be granted the rights for a Master Security Officer. A Master Security Officer always has all existing global rights. Click the **Browse** button to select an existing certificate or have one generated by SafeGuard LAN Crypt.

- **Assigning Certificates using an LDAP source**

SafeGuard LAN Crypt allows certificates to be assigned from Microsoft Active Directory or other LDAP sources.

To do so, select **LDAP** from the drop-down list in the **Choose a certificate** dialog.

An edit field is displayed in which you can enter the URL of the LDAP source. After you click **Refresh** the content of the LDAP source is displayed. Texts in square brackets (e.g. Sub_OU_1) represent the OUs in the LDAP source. To display the certificates of an OU, double-click it. Double-click [...] to go up one level up in the hierarchy.

Select a certificate and click **OK**. The certificate is now assigned to the Security Officer.

Note:

If the LDAP server does not allow an anonymous logon, you must enter the server's logon credentials in the Server tab in the Central settings.

If you use SafeGuard LAN Crypt to generate an encryption certificate, this Security Officer must import the private key to their workstation from the generated .p12 file. If the encryption certificate was assigned from an LDAP directory, the relevant private key must be present on the Security Officer's workstation. The encryption certificate is used for cryptographic access to the symmetrical database key.

4. Alternatively, you can click the second Browsebutton to select an existing signature certificate or have SafeGuard LAN Crypt generate a new one for you.

Note: If you use SafeGuard LAN Crypt to generate a signature certificate, this Security Officer must import the private key to their workstation from the generated .p12 file. If the signature certificate was assigned from an LDAP directory, the relevant private key must already be present on the Security Officer's workstation. The signature certificate is used for signature in the generated profiles and for authentication during extended API logon.

5. If you have defined regions for your Security Officers you can now select a region.

6. If you have created individual **configuration records** for the regions, you can now select one.

Note: The system only displays configurations that have been generated for the selected region.

7. Click **Next**.

8. In the Wizard's last dialog you can specify which actions the Security Officer is to be able to carry out.

All the global rights required for the selected actions will be set automatically. These rights are displayed in the SO's properties (double-click an SO to display them) on the *Global Permissions* tab. The global rights can be edited on this page. In this dialog, if you allow an SO to perform a specific action, they will be automatically granted all the necessary rights for this action.

If a new SO receives the global permission Administer groups or Administer users this way, SafeGuard LAN Crypt automatically creates an ACL with viewing rights for the root group for this Security Officer, provided that the Set group permissions for security officers who are allowed to administer groups or users option is activated. This guarantees that the SO can access (view and/or edit) all groups they are responsible for.

The Set group permissions for security officers who are allowed to administer groups or users option can be activated on the **Other settings** tab in **Central settings**.

9. Click **Finish**.

The new Security Officer is displayed in SafeGuard LAN Crypt Administration.

3.8.1 Granting/editing global permissions

The Security Officer must be granted global rights. If the Security Officer Administration node is selected, all existing Security Officers are displayed in the right-hand console pane. Double-click a Security Officer to open the tabs containing the properties assigned to them.

On the *Global Permissions* tab you grant the Security Officer the "basic rights" needed to administer SafeGuard LAN Crypt. If, when they were created, the SO was already granted the right to perform some actions these necessary rights are already active.

Note: Master Security Officer always has all existing global permissions.

A Security Officer can be granted the following global permissions:

Note: Click **Allow** to select all global permissions at once. Click again to deselect all global permissions.

Permissions	Description
Create Security Officer	The SO has permission to create more SOs.
Create Profiles	The SO has the global permission to run the Profile Resolver and generate policy files for individual users. This global permission is the prerequisite for setting the permission Create Profiles for a specific group for an SO. Create Profiles allows the SO to build profiles for users where the SO has the right Create Profiles for the user's parent group (see Parent group of a user on page 80 xxx). This permission is a prerequisite for assigning values to keys. A user who only has the permission Create Keys can only generate keys without values!
Create Profiles for Members	all This permission requires that the permission Create Profiles is set. This global permission is the prerequisite for setting the permission Create Profiles for all Members for a specific group. Create Profiles for all Members allows a SO to create profiles for all users where the SO has the permission Create Profiles on the parent group of the user or the permission Create Profiles for all Members on one of the groups the user is member of. Note: As the global permission Create Profiles is a prerequisite for Create Profiles for all Members the following applies: If you deactivate the permission Create Profiles, the permission Create Profiles for All Members is deactivated automatically. If you activate the permission Create Profiles for all Members, the permission Create Profiles is automatically activated.
Create Keys	The SO can generate keys in the individual groups. A user with the permission Create Keys on its own can only generate keys without values! Within the Administration Console, keys without a value can be assigned to encryption rules. The value itself is generated when policy files are generated. To generate keys with values manually, the SO must have the Create Profiles permission.
Copy Keys	The SO is allowed to copy keys.
Delete Keys	The SO can delete keys from individual groups.
Read Keys	The SO can see the data for the individual keys for a group.
Create Certificates	The SO can generate certificates for users.
Assign Certificates	The SO is allowed to assign certificates to the users. The SO is allowed to run the wizard for assigning certificates. This global permission is the prerequisite for setting the permission Assign Certificates for a specific group for a SO. Assign Certificates allows the SO to assign certificates to users where the SO has the right Assign Certificates for the user's parent group (see Parent group of a user on page 80).
Assign Certificates to Members	all This permission requires that the permission Assign Certificates is set. This global permission is the prerequisite for setting the permission Assign Certificates to all Members for a specific group. Assign Certificates to all Members allows an SO to assign certificates to all users where the SO has the right Assign Certificates for the parent group of the user or Assign Certificates to all Members for one of the group the user is member of. Note: As the global permission Assign Certificates is a prerequisite for Assign Certificates to all Members, the following applies: If you deactivate the permission Assign Certificates, the permission Assign Certificates to all Members is automatically deactivated. If you activate the permission Assign Certificates to all Members, the permission Assign Certificates is automatically activated.

Permissions	Description
Administer Groups	The SO can make changes in the groups. Adding sub-groups, moving groups, synchronizing groups, deleting groups.
Log in Database	The SO can log on to the SafeGuard LAN Crypt database. The default setting is for this permission is active. With this permission an SO can easily make changes to the database without too much effort (for example, if staff leave the company). This right is not granted to people who are only permitted to act if someone else authorizes their actions. This ensures that these people can only authorize actions that require confirmation, and have no way to make changes in SafeGuard LAN Crypt.
Authorize Operations	The SO can participate in actions that require confirmation.
Administer Users	The SO can add users to a group, remove them from a group, and synchronize groups.
Copy Users	The SO is allowed to add (copy) users to groups. This global permission is the prerequisite for setting the permission Copy User for a specific group for a SO. To add a user to a group, the SO must have the permission Copy User on the parent group of the user.
Create Rules	The SO is allowed to generate encryption rules for the users.
Change Global Permissions	The SO can change the global rights granted to another SO.
Change ACLs	The SO can change the ACL for a group.
Use specific Keys	The SO can use concrete specific keys in encryption rules and can display specific keys in All SafeGuard LAN Crypt keys .
Change Configuration	The SO can change the configuration (paths). This permission is required to display the Configuration tab in the Central settings, and for the SO to be able to make changes in the Directories tab if they are logged on to the database.
Read Logging Entries	The SO can view the settings used for logging and the logged events.
Manage Logging	The SO can change the logging settings. They are permitted to archive, delete and check entries.
Import Directory Objects	The SO can import OUs, groups and users from a directory service and add them to the SafeGuard LAN Crypt database. Before they can import Directory Objects, the SO also needs the Administer Groups permission and the Administer Users permission. These are set automatically when the Importing Directory Objects permission is selected. If an SO does not have this permission, the Directory Objects node (used to import OUs, groups and users) is not displayed in the Administration Console.

When granting global permissions, please note the following points:

- A Security Officer does not have a global permission unless they have been specifically granted it!
- A Security Officer can only change those permissions that they personally possess.
- A Security Officer cannot change an ACL that describes their own permissions.
- Some rights can only be granted if you have another right. When you select this type of permission, the other permission is set automatically.
- SafeGuard LAN Crypt can be configured to automatically create an ACL with viewing rights for the root group for a newly created Security Officer. It is required that the SO has the global permission Administer group or Administer users. This guarantees that the SO can access (view and/or edit) all groups he is responsible for.
This behavior has to be activated on the **Other settings** tab in Central Settings.
- If a Security Officer is changed and receives either the global permission Administer Group or Administer Users and does not have an ACL for the root group, it will be created. The ACL has viewing rights for the group. Existing ACLs are not changed.

Select the global permissions you want to grant to the Security Officer and click **Apply**.

3.8.2 Permissions for changing the settings for a Security Officer

The rights for changing the settings for a Security Officer can be transferred to other Security Officers. A Master Security Officer can always change these settings. This right must be specifically granted to a Security Officer.

The global permissions a particular Security Officer has determine which permissions they can change for other Security Officers.

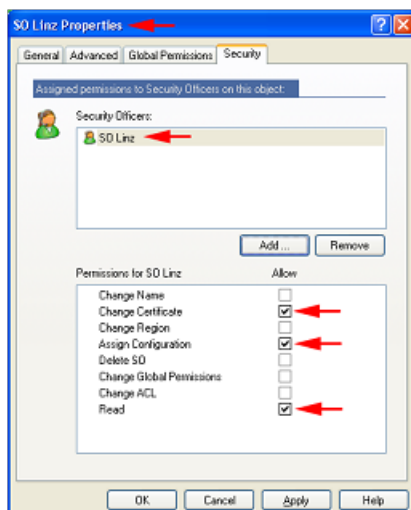
On the Security tab you can define which rights other SOs have for this object (= Security Officer). In the top part of the dialog you can see the SOs that have the right to change the settings for this SO.

1. Click Add to run a wizard for adding a Security Officer. On the first page of the wizard, select the SO you require from the list of existing SOs.
2. Click Next to display the page on which you specify the current SO's right to change this object (the SO whose settings are currently being processed).

Note: Click **Allow** to select all permissions at once. Click again to deselect all global permissions. The global permission settings specify that disabled rights cannot be granted to the Security Officer.

Permissions	Description
Change Name	Allows changes to the name of the SO to whom the permission's owner is assigned.
Change Certificate	Allows changes to the certificate of the SO to whom the owner of the right is assigned.
Change Region	Allows changes to the region prefix of the SO to whom the owner of the right is assigned.
Assign Configuration	Allows changes to the configuration of the SO to whom the owner of the right is assigned.
Delete SO	Allows the SO, to whom the owner of the permission is assigned, to be deleted.
Change Global Permissions	Allows changes to the global permissions of the SO to whom the owner of the permission is assigned.
Change ACL	Allows changes to the global rights of the ACL to whom the owner of the right is assigned.
Read	Displays the SO to whom the owner of the permission is assigned in <i>Central\settings\Security Officer Administration</i> . This is the prerequisite for all rights that allow this SO to be processed. This is set automatically when a right of that type is selected.

You can also grant the Permissions **Change Certificate**, **Assign Configuration** and **Read** to the SO whose properties are defined here. Before this can happen, that SO must be present in the list of SOs that have rights for this object (in this case, that particular SO).



- Read

Displays the SO specified in *Central\Settings\Security Officer Administration*. The SO can see the permissions that have been given to them.

- **Change Certificate**

The prerequisite for this right is "Read" authorization. Allows the SO to change their own certificate.

- **Assign Configuration**

Allows the SO to assign a different configuration to themselves.

Note: Permissions whose checkbox is grayed out cannot be granted because the selected SO does not have the global permissions necessary to do so.

3. Grant the Security Officer the appropriate rights by clicking the checkboxes and then click Finish.

The system now displays the Security Officer in the top pane of the Security page. In the bottom pane of the page an ACL shows the rights of the selected SO.

3.8.3 All rights for groups/OUs of a specific Security Officer

To view the rights of a specific SO for all groups /OUs for which the SO has any right, go to Security Officer Administration and double-click the relevant SO.

In the SO's properties dialog, select the Groups tab. This tab contains two list views:

- The upper list view shows you all groups/OUs for which this SO has rights.
- The second list view shows the corresponding rights of the SO for the selected group/ (OU).

This way you can easily get an overview of all rights a specific SO has for the different groups in your organizational structure.

You cannot change the rights of an SO in this view. Changing rights is only possible in the properties dialog of a group.

Note: Only groups a SO has rights for (allow or deny) are displayed. Groups for which a SO has inherited rights are not displayed.

3.8.4 Changing or renewing MSO or SO certificates

You can change or renew an (M)SO certificate in two ways:

- Via Security Officer Administration
- Using the restoration key

3.8.4.1 Via Security Officer Administration

1. Start SafeGuard LAN Crypt Administration and log on as the MSO. You can also log on as an SO if this SO has the right to change the certificate for the SOs concerned. This can also include the SO themselves if they have the appropriate rights and their certificate is still valid.
2. Switch to the **Central settings** tab and from there go to the **Security Officer Administration** node.
3. Right-click the SO concerned and select the **Properties** entry from the context menu.
4. Go to the **Extended** tab.
5. In **Encryption certificate** click the Search button to select a new encryption certificate for the SO.
6. You can also go to **Signature certificate (optional)** and click **Search** to select new signature certificate for the SO.

Note: You can only change SO signature certificates via **Security Officer Administration**.

3.8.4.2 Using the restoration key

1. Start SafeGuard LAN Crypt Administration.
2. In the SO dialog window, select the (M)SO you require.
3. Click the **Change certificate** button and follow the instructions in the **Restoration key wizard**.

Usually you should use variant 1. Variant 2 is primarily intended to be an alternative method and should be used if no SO with the appropriate rights is able to log on to SafeGuard LAN Crypt Administration.

Note: A prerequisite for variant 2 is that a restoration key exists. No matter which method you use, you must ensure that the profile generated by the SO is regenerated before the old certificate reaches its expiration date. If not, the clients will no longer be able to load the profile. However, you can allow certificates to be assigned with only additional authorization. You must remember that this type of assignment will have an effect when SO certificates are changed. Task step.

3.9 Logging on to Administration

For logging on to the SafeGuard LAN Crypt Administration Console a Security Officer must have the right to log on. Master Security Officers always have this right since they are automatically granted all available rights.

When you run Administration (Start/Programs/Sophos/SafeGuard LAN Crypt/Administration) you see the logon dialog.

All the authorized Security Officers are displayed in the list. If you select the **Show only security officers from a specified region** option, and select that region, only those Security Officers in that region are displayed.

To enable logon, the system must access the private key that belongs to the certificate (software key or a key on a token). After you select the required Security Officer, click **OK** to open the SafeGuard LAN Crypt Administration Console.

Recovery Key

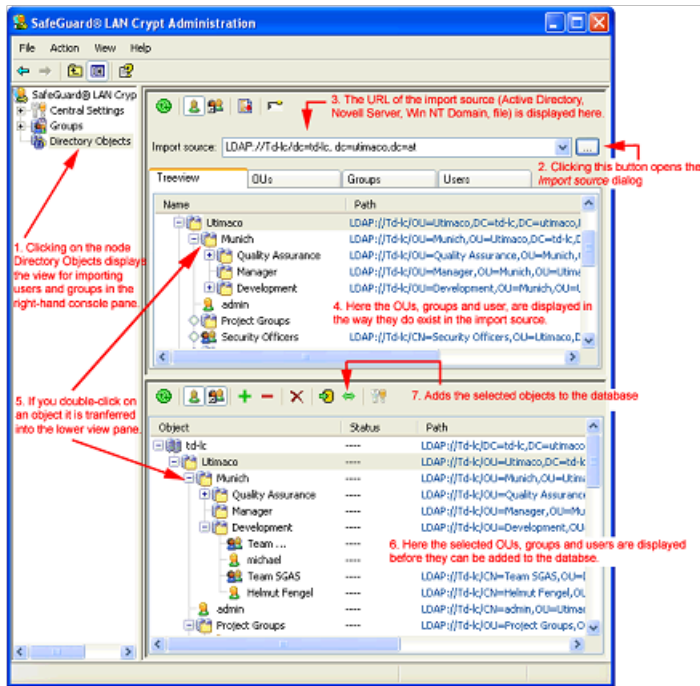
If the key belonging to a Security Officer's certificate has expired, or has been damaged or lost, enter a recovery key to renew the certificate.

Note: If a new certificate is generated during the recovery process, that certificate (and its associated password) are saved to the default path (C:\Documents and Settings\All Users\Documents\Sophos\Admin\) instead of the configured path because at this point no SO-specific configuration is effective.

3.10 Importing groups and users

With SafeGuard LAN Crypt you can import groups and users from directory services that can be accessed via LDAP, from domains, or import them from a manually-created file that contains the groups and users with the particular dependencies.

Click **Directory Objects** to display the dialogs for importing and assembling groups for import into the database, in the right-hand console pane.



Note: If an SO who is logged on cannot display the Directory Objects node it means that they do not have the global permission **Import Directory Objects**. This node only appears in the Administration Console if this SO has this right.

3.10.1 Importing groups and users from a file

Users and groups can be imported from a manually-created file that contains the groups and users with specific dependencies. The imported groups and user are created in the *Groups* node in the SafeGuard LAN Crypt Administration console.

To import users and groups from a file, click **Search file** in the **Import source** dialog. Click the **Search** button and SafeGuard LAN Crypt displays a dialog in which you select the file, from which the users and groups are to be imported (see Selecting import source on page 73 xxx).

The import file is a simple text file with no specific file extension (we suggest you use .lcg as the default extension). The contents of this file have to meet certain requirements.

Import file format

An import file consists of several sections. The sections are separated by an arbitrary number of blank lines.

Each section represents a user or a group.

Each section consists of a header and a fixed number of lines, each starting with a keyword. Lines must end with a new line character. There may be no other new lines between the lines in a section.

The header is the section name in square brackets. The section name is used to define the membership of users and groups.

The keywords define the users and groups data as it appears in their **Properties** dialog.

	Keywords	Description
type=	USER GROUP	
name=		Defines whether the imported object represents a user (USER) or a group (GROUP). Defines a user's logon name. This is displayed under Logonname in the SafeGuard LAN Crypt Administration console.
display=optional		Allows you to define a user name that is not identical to the logon name. This appears as the Username in the SafeGuard LAN Crypt Administration console. If no name is

Keywords	Description
mail=optional	<p>specified here, the logon name entered under name= is displayed under Username in the SafeGuard LAN Crypt Administration console.</p> <p>Allows you to enter the user's e-mail address. This is displayed on the Details tab in the user's properties.</p> <p>Note: The e-mail address is added to the password log file for certificates generated by SafeGuard LAN Crypt. For example, it can be used to create a PIN letter via e-mail.</p>
members=	<p>When groups are used, this defines which users and other groups are members of a particular group. To add a member, enter the section name which identifies the user or the group (e.g. U_BKA,G_Sophos). Enter commas to separate each group member's name from the next.</p>
If you type // at the beginning of a line you can type a comment on that line, anywhere in the import file.	

Note: Entries in the import file are NOT case sensitive (do not distinguish between capitals and lower case letters)!

Example

```
[U_JB1]
```

```
type=USER
```

```
name=JB1
```

```
Display=Jesse Black
```

```
Mail=jb1@company.com
```

```
// my comment .....
```

```
[U_PW1]
```

```
type=USER
```

```
name=PW1
```

```
Mail=pw1@company.com
```

```
[U_JG1]
```

```
type=USER
```

```
name=JG1
```

```
[U_JFU]
```

```
type=USER
```

```
name=JFU
```

```
[G_COMPANY]
```

```
type=GROUP
```

```
name=Company
```

```
members=G_QA,G_Scranton,G_PDM,G_Empty,U_JFU
```

```
// my comment .....
```

```
[G_QA]
```

```
type=GROUP
```

```
name=QA
```

members=U_JB1,U_PW1

[G_PDM]

type=GROUP

name=JG1

members=U_NGR

3.10.2 Icons in the Administration system



Updates the view in the current window.



Shows the users in particular groups.



Also displays the memberships of groups and users in particular groups. Memberships whose object is not directly contained in the group are grayed out.



Moves the selected object into the bottom pane. Has the same effect as double-clicking on the selected object.



Use as new path. You can use this setting to restrict how the structure is displayed. If a node is selected, and you then click this button, the system only displays the structure below the selected node. In addition, the path is added to the drop-down list so that you can quickly toggle to this display again.



Displays the tree structure.



Closes the tree structure.



Deletes a selected object from the view.



Adds the objects displayed in the bottom right-hand pane to the SafeGuard LAN Crypt Database.



Synchronizes the objects displayed in the bottom right-hand pane with the ones already present in the SafeGuard LAN Crypt Database.



Opens the dialog in which you specify the transfer options. You must specify the transfer options before the objects are transferred from the import source.

3.10.3 Selecting import source

You can enter the URL of the server from which the data is to be imported directly in the **Import source** input field (for example, **LDAP://usw-scranton/dc=usw-scranton,dc=company,dc=us** for the Active Directory directory service on the Domain controller **usw-scranton**).

Click the **Search** button and SafeGuard LAN Crypt displays a dialog in which you select the import source.

LDAP://

- **Domain**

If the computer is a member of an Active Directory domain, click this button to display the entire structure of the domain, as stored on the domain controller.

Note: You cannot import built-in groups from the Active Directory. We therefore recommend that you organize users into OUs (organizational units) or groups and import them instead.

- **Search container**

If the computer is a member of an Active Directory domain, and you select **Search container**", the system displays the Browse... button, that you can click to display another dialog. In this dialog you can then select a particular node in the Active Directory structure.

WinNT

- **Computer**

Displays the local groups and users of the computer you are currently logged onto. Usually these groups and users are only used for test purposes.

- **Domain**

If the computer is a member of a Windows NT domain, click this button to display the entire structure of the domain, as stored on the domain controller.

Note:

When using the WinNT protocol the system cannot distinguish between renamed and new users during synchronisation as the WinNT protocol does not assign unique GUIDs to user objects.

FILE://

- **Search file**

To import users and groups from a file, click **Search file** in the **Import source** dialog. Click the **Search** button to select the file from which the users and groups are to be imported. The import file must be of a specific format to enable you to import the users and groups. For information on how to create the import file, see Importing groups and users from a file on page 70 xxx.

Once you have selected an import source, click the **Transfer** button to display the URL to the source, under **Path**.

When you click **OK** SafeGuard LAN Crypt displays the selected data in the top right-hand pane of the console. In this view you can display the selected data in a tree structure, arranged in OUs, groups and users.

Only for LDAP Server

If the administration computer is not a member of a domain, use this procedure to import the groups and users from a server:

1. On the **Server** page, in the **Central Settings**, enter the server's name, and the user name and password.
2. For LDAP or SSL, specify whether the **<Microsoft>** or **<other>** implementation is in use.
3. In the **Import Source** input field enter the address of the server from which the data is to be imported.

3.10.4 Preparing for transfer into the SafeGuard LAN Crypt Database

In the top right-hand console pane you can see the OUs, groups and users, as stored in the import source.

Here you can select which of these displayed OUs, groups or users are to be imported into the SafeGuard LAN Crypt Database. First, move the selected objects into the bottom view pane, where you can then process them again.

Note: If you add an object (node) to the bottom view pane, this does not mean you have added it to the database. You can only group objects in this pane. To transfer them to the database, click **Add to database** or **Synchronize**.

3.10.4.1 Defining data transfer settings

To optimize performance, you can define transfer settings. These transfer settings only affect transfers in the bottom view pane, to let you prepare for transferring the data to the database. Click the transfer settings icon to open a dialog that has three options:

- **Calculate status of objects in the database**

Only applies if entries are already present in the database, i.e. when the database is being synchronized. If this option is selected, you can see the following in the lower view for each object:

- whether it is already present in the database (in the Status column).
- whether the logged-on SO has the right to modify a group (in the Add group column). A red cross shows that the SO does not have the right to add the group. A green tick means that the SO has the right to add the group.
- whether the logged-on SO has the right to add users (in the Add users column). A red cross shows that the SO does not have the right to add users. A green tick means that the SO has the right to add users.

- **Calculate memberships**

If this option is selected, the system also displays the group memberships (groups and users who are not direct members of the individual groups). To distinguish them from direct members they appear as grayed icons.

Note: The system can only calculate the memberships until they are transferred to the database.

- **Sort objects**

Sorting the entries alphabetically in large groups can be very time-consuming, so the entries are usually not sorted. If you want to sort the objects alphabetically, select this option.

Updating the view

If no options were set for transfer, you can perform these actions after the transfer by clicking the **Update** button. Click **Update** to open a dialog with the same options. The update only affects the data in the bottom view pane.

3.10.4.2 Transferring objects into bottom pane

If you double-click a node or select the node and click the **Transfer** button, you transfer the objects in the import source structure into the lower view pane. Before the objects are transferred a dialog appears in which you can specify how the individual containers and objects are to be transferred.

- **Only transfer this object**

Adds the selected object without its contents.

- **Transfer direct members as well**

Adds all objects present in the selected container.

- **Transfer members recursively**

Adds all objects that are present in this container and also all objects that are members and are present in another container. The members are transferred with their entire hierarchy.

Select the option you require and click **OK** to transfer the objects to the bottom view pane so they are ready to add to the SafeGuard LAN Crypt Database.

Before transferring them to the database, you can add more groups to this view (for example, from other sources) and then add everything to the database in one step.

3.10.4.3 Adding data to the database or synchronizing data

Objects are not added to the SafeGuard LAN Crypt Database until they have been grouped in the lower view pane and you click the **Add to database** or **Synchronize** button there.

Note: If you add objects to an existing structure, you must always start by adding them to the database. To do this, click the **Add to database** button. Synchronization is only used if the only change is in the relationships between the objects.

When you click **Add to database**, the system adds the objects and then starts the synchronization process. This begins with a dialog that has three options.

- **Synchronize complete database**

If you select this option the system synchronizes all the entries present in the SafeGuard LAN Crypt Database with the ones in the import source. Changes are displayed in another screen that is shown next.

Select this option, if objects were deleted from the AD and they should also be deleted from the database.

Note: If a complex structure is involved complete synchronization may take a long time.

- **Synchronize only visible entries**

Refers to the selection in the bottom right-hand pane in the Administration Console.

- **Recalculate all relationships**

If you select this option the system recalculates all memberships according to their import source and adds them to the database again. Memberships are even added if they have been switched off in the display in the bottom right-hand console pane (the **Calculate memberships** option in the transfer settings has been switched off).

- **Use visible relationships**

If you select this option, only the relations displayed in the bottom right-hand console pane are added to the database. "Hidden memberships" are not added to the database (**Calculate memberships** is deactivated in the transfer settings).

Note: If this option is used during synchronization, and memberships for objects present in the database are not displayed in the bottom right-hand console pane, any memberships present in the database are deleted.

When you select an option and click **OK** the system displays a dialog that documents synchronization. You must confirm the changes in this dialog.

- **All entries**

Displays all changes in a list. Corresponds to the total number of entries on the other pages.

- **Deleted objects**

Displays objects that have been deleted in the import source (server) since the last synchronization, but are still present in the SafeGuard LAN Crypt Database.

- **New relationships in the directory**

Displays the objects and memberships that have been added to the SafeGuard LAN Crypt Database, or new ones that have been created in the import source (server) since the last synchronization, and have not yet been transferred into the database.

- **Old relationships in the database**

Displays objects and memberships that are still present in the database but are no longer in the import source. For example, groups may have been deleted, or memberships changed on the server.

Note: The synchronization run only evaluates those objects that have been imported at least once from an import source to the database. If objects are deleted in an import source, these changes are only implemented in the database if the Synchronize complete database option is selected. Groups and users added manually in the Administration Console are not evaluated during synchronization and therefore do not appear on these pages.

You can cancel the action for each object listed in this view by clicking on that action (remove the tick). Only the selected actions (the ones with a tick) are performed. Click **OK** to complete the data synchronization run.

Once the OUs (organizational units), groups and users have been imported, the Security Officers responsible for them can be assigned to each OU.

3.10.4.4 Adding groups manually


To add a new group manually, select the node/group to which you want to add the new group, and click **New Group** in the context menu.

Enter a name for the new group in the *Group Name* field and click **OK**. The system now displays the group in the SafeGuard LAN Crypt Administration console.

In the group's **Properties** dialog you can add existing users to the group or create new users.

Unlike imported groups, you can use drag and drop to move manually created groups within the groups hierarchy.

3.10.4.5 Relationships between groups

To create relationships between groups, you can copy a group and insert it in a different group. A group inserted this way is displayed as a shortcut  in the parent group. As a result, the members of the inserted group inherit all keys and encryption rules of the parent group. The prerequisite for inheriting keys is that these keys are defined as inheritable in the parent group. Rights for editing the group are NOT inherited.

Since this group is only inserted in the new place as a shortcut, encryption rules, members, certificates and keys are not shown there. These values are only visible in the "real" group in the hierarchy. The inherited keys can also be used there to create encryption rules.

To add a group to another group via a shortcut

1. Select the relevant group, open its context menu, and select **Copy**.
2. Select the target group, into which you want to insert the group, and click **Insert** in the target group's context menu. You can also create the shortcut by pressing CTRL and dragging and dropping the group onto the target group.
3. The system will prompt you to confirm that you want to add the group. Click **OK** to confirm this.

The group is now displayed as a shortcut under the other group.

In this way you can easily grant all members of one group all the rights of a different group.

For example: if you want to grant the members of Team 1 the same rights as the members of Team 2, for a limited amount of time, (for example so that Team 1 can support Team 2 in a project), you simply add a shortcut to Team 1's group in Team 2's group. Then generate new policy files. Next time the members of Team 1 log on, they have access to Team 2's data. When Team 1 no longer requires the extra rights, you can remove the shortcut from Team 2's group, and generate new policy files again. The members of Team 1 then no longer have access to Team 2's data.

3.10.4.6 Deleting groups

You can delete individual groups/OUs and shortcuts to groups/OUs in the SafeGuard LAN Crypt Administration console.













To delete a group, select **Delete** in that group's context menu. All sub-group and user memberships will be deleted. The users themselves will only be deleted if an OU is deleted in the SafeGuard LAN Crypt Administration console. In this case any memberships of users that might exist in other OUs are also deleted. Keys are NEVER deleted. They remain in the SafeGuard LAN Crypt database. Before the group is deleted, a dialog is displayed in which you must confirm that you want to delete the group.

To delete a shortcut to a group, click **Delete** in the shortcut's context menu. Only the shortcut is deleted. The group itself is not affected. Before you delete a shortcut, a dialog appears that asks you to confirm that you want to do so.

The context menu of the parent group contains the entry **Remove links** that you use to delete a shortcut. Click **Remove links** to delete the all shortcuts to this group. The group itself is not affected.

3.10.4.7 Group icons

The OUs and groups are represented by different icons in the SafeGuard LAN Crypt Administration console, depending on their import source:

	The server icon shows the source from which the OUs and groups have been imported.
	Icons for the shortcut to the server (a link created by copying it)
	Icon for an OU imported from a server.
	Shortcut to an imported OU.
	Icon for a group imported from a server.
	Shortcut to the imported group.
	Icon for a file, from which users and groups have been imported.
	Shortcut to the imported file.
	Icon for a group imported from a file.
	Shortcut to the imported group.
	Group that was added manually.
	Shortcut to a group that was added manually.

3.11 Assigning SOs to organizational units

After OUs, groups and users have been imported into SafeGuard LAN Crypt Administration, Master Security Officers can assign individual SOs to the various organizational units.

The SO can then use the rights they have been given to process the organizational units to which they have been assigned.

To ensure that a Security Officer can only edit the organizational unit for which they are responsible, the Master Security Officer can "hide" the other nodes from this Security Officer. This means that the node is visible but cannot be edited.

If the Security Officer logs on to SafeGuard LAN Crypt Administration, they can only see the part of the organizational structure for which they are responsible.

3.11.1 Parent group of a user

A user in SafeGuard LAN Crypt can be a member of more than one group, but has one dedicated group that is their parent group:

- When importing the user through LDAP, the parent group is the OU the user belongs to.
- When importing the user through a file, the parent group is the group the user is member of, as defined in the file.
- When creating a new user through the group properties dialog, the parent group is the group from which the group properties dialog was opened.

In the SafeGuard LAN Crypt Administration console, the parent group is shown as a column in the Selected Users and Certificates node or as a column in the Members and Certificates of Group node (when configured on the User Settings tab, see User settings on page 35 xxx).

The parent group of a user impacts the evaluation of rights in the following situations:

- Viewing the properties of a user: SOs can view the properties of a user when they have the right Read and Visible for the parent group of the user.
- Modifying the properties of a user: SOs can modify the properties of a user when they have the global permission Administer Users and the rights Add User and Delete User on the parent group of the user.
- Creating Profiles: If Create Profiles is set for a group for a SO, the SO is allowed to build profiles for all members of the group, where the group is also the parent object of the group. The SO is not allowed to create profiles for users who are only members of the group and have a different parent group. This requires the right Create Profiles for all Members.
- Assigning Certificates: If Assign Certificates is set for a group, the SO is allowed to assign certificates to all members of the group, where the group is also the parent object of the group. The SO is not allowed to assign certificates to users who are only members of the group and have a different parent group. This requires the right Assign Certificates to all Members.
- Copying Users: When a SO wants to add a user to a group by using properties dialog of a group (on the tab Members with the Add button), the SO must have the right Copy Users for the parent group of the user.

3.11.2 Allowing a Security Officer to see and edit groups

Context for the current task

1. To permit a Security Officer to see a node in Administration, you must first set the **Visible** right in the base node in the organization structure.
2. To do this, select the base node in the structure and click **Properties** in the context menu to open the **Properties** dialog for this node.
3. Toggle to the **Security** tab and click **Add**. Here you can select the Security Officer you want to assign to process the groups.

Note: Several Security Officers can be assigned to the same group.

4. Click **Next** to display the Permissions dialog for this SO. Here, select the **Visible** permission and then click **Finish**. This permission is inherited downwards through the group hierarchy, which means the SO can now view all groups. If the SO logs on to the database with these settings, they can see the entire Administration structure but cannot edit it.

5. In the next step you can now hide (suppress) the groups in the Administration Console you do not want the SO to see because they have no rights to access them.
6. To do this, select these groups, open their **Properties** dialogs and select the **Security** tab.
7. Here, set **Visible** to **Deny** for the groups that are to be hidden for the SO.

Note:

If an SO has been explicitly refused a right to a hierarchically superior group this right cannot be assigned to a subordinate group. We therefore recommend that you only assign an SO **Read** and **View** permissions to a hierarchically superior group so that they can assign rights to subordinate groups without causing any problems.

SafeGuard LAN Crypt can be configured to automatically create an ACL holding the visible right on the root group for a newly created Security Officer. It is required that the SO has the global permission Administer group or Administer users. This guarantees that the SO can access (view and/or edit) all groups he is responsible for. This behavior has to be activated on the **Other settings** tab in **Central Settings**.

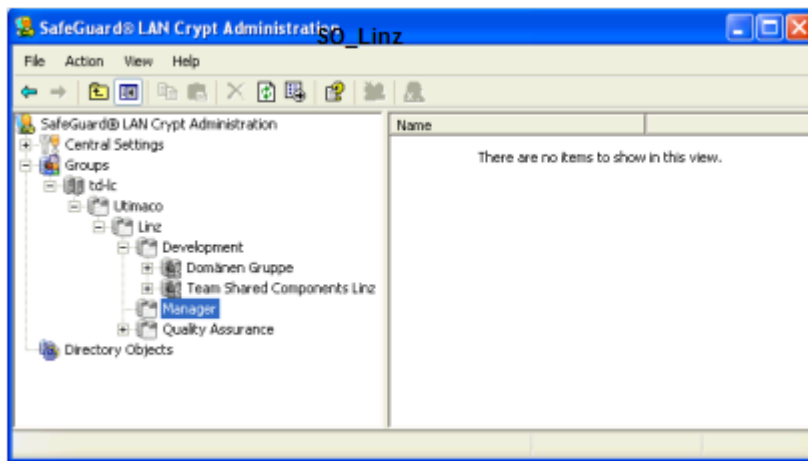
The screenshot shows the 'SafeGuard LAN Crypt Administration Master Security Officer' interface. The 'Munich Properties' dialog box is open, showing the 'Security' tab. The 'Visible' permission is set to 'Deny'. The 'Add Security Officer Wizard' dialog box is also open, showing the 'Permissions' tab. The 'Visible' permission is checked under the 'Deny' column.

The numbering corresponds to the steps in the description:

- 1. Munich Properties dialog box
- 2. Security tab in Munich Properties dialog box
- 3. Security Officers list in Munich Properties dialog box
- 4. Add Security Officer Wizard dialog box
- 5. Permissions list in Add Security Officer Wizard dialog box
- 6. Visible permission in Add Security Officer Wizard dialog box

The numbering corresponds to the steps in the description. Is grayed out, since it is an inherited permission that is being denied here.

When a SO logs on with these settings in place, they see:



Only the groups for which the SO has the **Visible** permission are displayed. These groups are grayed out because, as yet, the SO has no rights to process them.

If both the **Visible** permission and the **Read** permission have been assigned to the SO at the same time, the system would also display the snap-ins for **Encryption rules, Members and certificates for group and Group keys** under the groups. The SO can see the contents of the snap-ins, but cannot change them.

You can use the **Read** permission to give an SO information about other groups without allowing them to edit these groups: the system simply includes that information in the SO's view.

Note: If the SO has also been granted the **Read** permission, you must specifically deny it again to hide the groups again. It is not enough to simply deny the **Visible** permission.

3.11.3 Granting the SO permissions to process the groups

Once you have set up the SO so that they see the groups they are to edit, you can assign them the appropriate permissions.

These permissions are inherited downwards in the organizational hierarchy, and you can deny them in another place, lower down the hierarchy.

1. Select the group for which you want grant rights to the SO, open the **Properties** dialog, and select the Security tab.
2. Under Security Officers you see all the SOs who are assigned to this group. When you select an SO, the system displays their valid authorizations in the lower part of the dialog. Permissions inherited from another group are shown by a gray tick. Permissions that cannot be granted, due to the settings in the global rights, have a checkbox that is completely grayed out.

Note:

The global permissions settings define which permissions can be assigned to a particular SO. Global rights are set when the SO is generated.

Click **Allow/Deny** to allow or deny all the permissions. Click this again to deselect all global permissions. If all rights are selected you can select/deselect them later on as required. The global permission settings define that disabled rights cannot be granted to the Security Officer.

You can assign the following permissions:

Permissions	Description
Create Key	The SO is allowed to generate keys in the group.
Copy Keys	The SO is allowed to copy keys.
Delete Key	The SO is allowed to delete keys.
Create Rules	The SO is allowed to generate encryption rules for the users.
Assign Certificates	The SO is allowed to assign certificates to the users. The SO is allowed to run the wizard for assigning certificates. This permission allows the SO to assign certificates to the users in the group where the group is also the parent group.
Assign Certificates to all Members	This permission requires that the permission Assign Certificates is set. Assign Certificates to all Members allows the SO to assign certificates to all users in the group: users of whom the

Permissions	Description
	group is the parent group and also users who are member of the group and have a different parent group. Note: If you set Assign Certificates to all Members to Allow, the permission Assign Certificates is automatically set to Allow. If you set Assign Certificates to Deny, the permission Assign Certificates to all Members is automatically set to Deny.
Add User	The SO is allowed to add users to the group manually. This permission is a prerequisite for importing/synchronizing groups and users.
Copy User	The SO has the right to add users from this group to another group. This is only allowed for members where this group is also the parent object.
Delete User	SOs is allowed to use the <i>Members and certificates for group</i> snap-in to delete users. This permission is a prerequisite for importing/synchronizing groups and users.
Add Group	The SO is allowed to use a group's context menu to add new groups. This permission is a prerequisite for importing/synchronizing groups and users.
Delete Subgroups	The SO is allowed to delete the sub-groups for this group. This permission is a prerequisite for importing/synchronizing groups and users.
Move Groups	The SO is allowed to move manually-created groups in Administration (with drag and drop). Imported groups cannot be moved. This permission is a prerequisite for importing/synchronizing groups and users.
Change Properties	The SO is allowed to change a group's properties.
Delete Group	The SO is allowed to delete groups. This assumes that the SO has removed the "Delete Subgroups" permission in the group above. This permission is a prerequisite for importing/synchronizing groups and users.
Create Profiles	The SO has the permission to run the Profile Resolver and generate policy files for selected users. Create Profiles allows the SO to build profiles for users in the group where the group is also the parent group.
Create Profiles for all Members	This permission requires that the permission Create Profiles is set. Create Profiles for all Members allows the SO to create profiles for all users in the group: Users of whom the group is the parent group and also users who are members of the group and have a different parent group. Note: If you set Create Profiles for All Members to Allow, the permission Create Profiles is automatically set to Allow. If you set Create Profiles to Deny, the permission Create Profiles for All Members is automatically set to Deny.
Change ACL	The SO is allowed to change the ACL for the group (for example, by adding another SO).
Read	The SO has read rights for this group and can see the contents for the snap-ins. Is set automatically if edit permissions are granted.
Visible	The SO can see the group. Is set in the base node and inherited downwards. If it is refused for the SO, the group is hidden ("Read" must also be denied).

3. Select the permissions you want to assign to the SO. Click **Transfer** to store the settings in the database.
4. If you have assigned other SOs to this group, you can now also set up their permissions. To display the permissions set for the SOs, select them under **Security Officers**.

Note: Changes to the permissions of a SO for a group only become effective after the relevant SO has logged on to the SafeGuard Enterprise LAN Crypt Administration again.

3.12 Properties of groups

The **Properties** dialog for a group (<Group>/Context menu/**Properties**) consists of four tabs in which you can edit the properties for a group.

3.12.1 The Properties tab

The Properties tab displays the

- **Name**
- **DNS Name**
- **GUID**

- **Comment**

for the group.

3.12.2 The Member of tab

In the Member of tab you see the groups that include the current group as a member.

3.12.2.1 Adding/deleting members

In the **Members** tab you can add members to the current group. This list displays all existing users and groups that are members of this group. You can only change the users in this list, not the groups!

- **Add:**

Opens a dialog in which you can select users and then add them to the group.

Displays either all users or you can select specific user groups or individual users, with the help of SQL placeholders.

As displaying all users can be very time-consuming, SafeGuard LAN Crypt allows you to define search criteria to filter the search process.

Select option **Display matching users** to activate the input fields for defining your search criteria:

The following user information will be retrieved from the SafeGuard LAN Crypt database:

- Logon name
- User name
- Assignment between user and certificate
- Requestor of the certificate
- Serial number of the certificate
- Date from which the certificate is valid
- Date up to which the certificate is valid
- Name of the parent group

You can define search criteria based on these attributes. SafeGuard LAN Crypt searches for defined character string in the user attributes retrieved.

In the first drop-down list, you can select the attribute(s) on which the search process is to be applied.

In addition you can define whether the selected attribute should correspond to the character string entered (**should be**) or if only users are to be displayed, for whom the selected attribute does not correspond to the character string entered (**must not be**).

In the drop-down list on the right-hand side, you can enter the character string SafeGuard LAN Crypt searches for in the defined attribute.

You can use the following SQL wildcards for entering the character string:

%any character sequence

_ single character (e.g., a__ means search for all names containing three characters and starting with a)

[] single character from a list (e.g., [a-cg]% means search for all names starting with a, b, c or g)

[^]single character not contained in a list (e.g., [^a]% search for all names not starting with a)

You can specify up to three conditions for the search process

If you enter more than one condition, you can define how these conditions are to be combined (AND/OR).

If you click **OK**, all users whose names are selected in the list are transferred to the current group.

- **New**

Opens a dialog in which you can create a new user.

- **Delete**

Deletes the selected user membership from the current group. If the user is not a member of any other group, they are deleted from the SafeGuard LAN Crypt database.

If the user is a member of more than one group and the current group is the parent group of the user, the resulting action depends on the type of the group:

- if the group is an Organizational Unit or root group and the user is a member of another OU or root group, this OU or root group becomes the parent group of the user. If there is no other OU or root group the user is member of, the user is deleted (similar to Active Directory where a user is deleted, when the OU the user belongs to is deleted).
- if the group is a simple group (not an OU and not a root group), one of the other groups the user belongs to becomes the parent group of the user.

- **Properties**

Displays the properties of the selected user.

Note:

A user can only exist once in a particular container. If you try to create/add a user to a container in which they are already present, a message is displayed informing you that this is not possible. However, more than one user with the same name can be present in the system, as long as they are not in the same container.

3.12.3 Adding SOs

On the **Security** tab, an SO can also add SOs to the current group and assign them rights to the group. The prerequisite for this action is that the SO who wants to add another SO has the **Change ACL** permission.

Note:

If the SO adds SOs to the group, the SO can assign their own permissions (and only those permissions) to those SOs. A SO cannot add themselves to an ACL or edit their rights in an ACL.

3.13 Properties of users

The **Properties** dialog for a user (<user>/Context menu/**Properties**) consists of four tabs in which you can edit the properties for a user.

The Certificates tab

The **Certificates** tab displays all the certificates that are assigned to a user. In this tab you can also create a new SafeGuard LAN Crypt certificate for the user, add a certificate from the certificate store and import a certificate from a file (see Assigning a certificate to a user on page 105 xxx).

The Groups tab

The **Groups** tab displays the groups in which the current user is a member.

The Rules tab

The **Rules** tab displays all the encryption rules for the user. This is a convenient overview of all the encryption rules that are currently valid for a particular user, even if they originate from different groups.

Columns **S**, **X**, **I** show, which kind of rule it is:

- **S** (sub-directories): sub-directories are included in encryption.
- **X** (exclude path): the path is excluded from encryption.
- **I** (ignore path): the folder is ignored by SafeGuard LAN Crypt. For further information, see *Generating encryption rules* on page 100 xxx.

Under **Inherited from** you see the group from which a particular rule has been inherited.

The Details tab

User data is displayed and can be edited in the *Details* tab.

The e-mail address is added to the password log file for certificates generated by SafeGuard LAN Crypt. It can, for example, be used to create a PIN letter via e-mail.

Note: Please be careful when you edit user data. Your changes may have undesirable side effects. For example, if you change the logon name in this tab, the user may no longer be able to access their policy file, because the client uses a different - the old - logon name to search for a policy file.

3.14 Security environment design

SafeGuard LAN Crypt's high degree of flexibility means it can easily be adapted to meet any company's security requirements.

Even so, it is very important that a company-wide security strategy has been defined before you create the SafeGuard LAN Crypt environment.

We usually recommend that you start out with a fairly restrictive security policy because it is easier to liberalize this policy than to make a policy stricter later on in the SafeGuard LAN Crypt system. Making a liberal policy more restrictive could cause security problems that are not easy to solve. To avoid this, it is crucial that a company-wide security policy has been defined before you generate and distribute encryption profiles.

3.15 Generating keys

New keys are generated under the group node for the group in which they are to be used. For each key you can specify whether it is to be inherited downwards in the group hierarchy.

Note:

All existing keys are displayed in General settings \SafeGuard LAN Crypt keys. However, they cannot be processed there. This view is an overview of the keys used in SafeGuard LAN Crypt.

An SO who only has **Create keys** permission and not **Create profile** permissions cannot add a value when generating keys. The value is generated automatically when a key is transmitted to a profile.

A SafeGuard LAN Crypt key consists of the following components:

- **a name**

For the sake of clarity we recommend that the name of the user group is part of the key name. The names you define are especially important because SafeGuard LAN Crypt can also sort keys. SafeGuard LAN Crypt uses specific key names to generate a 16-character key name for internal use. It attaches the prefix for the appropriate region to the beginning of this key name.

- **a key value**

The length of the key depends on which algorithm is used. The key value can be specified either in ANSI characters or in hexadecimal notation (permitted numbers and characters: 0123456789abcdef). The other associated value is updated automatically. You do not need to enter a key value. In this case the value is generated randomly the first time the key is used in a user profile.

- an encryption algorithm

AES-128, AES-256, DES, 3DES, IDEA, XOR

- **a comment** (optional)

- **Key GUID** (optional)

This allows you to enter a key GUID manually so that encrypted files can be exchanged between two different SafeGuard LAN Crypt installations (see The Keys tab on page 37). If this field is empty, the GUID is created automatically

To generate a new key

1. Select **Group keys** under the group for which you want to generate a key.
2. Click the yellow key icon in the tool bar or right-click in the right-hand console pane, to display the context menu, and then click **New key** in this menu.
3. Enter a name for the new key in the top input field. Backslashes (\), slash (/), inverted commas and the & character are not allowed in key names.
SafeGuard LAN Crypt generates a unique, 16-character key name from this name that is used for internal purposes. It also puts the region prefix (if it was specified in the Security Officer properties) at the start of this unique name. The internal name is displayed on the right, next to the drop-down list from which you select the algorithm. You can change the key name at a later point in time, but not the internal name that was generated from it.
4. Select an encryption algorithm from the drop-down list (AES-128, AES-256, DES, 3DES, IDEA, XOR).
Here you can only see the algorithms that you have made available in the Central settings.
5. Specify whether the key can be inherited in the group or not:
 - **No**
The key is not inherited and is therefore only available in the current group.
 - **Once**
The key is inherited in the group(s) in the next hierarchy level below the current group.
 - **Yes**
The key is inherited in all groups in the hierarchy levels below the current group, and is available there for generating encryption rules.
6. Enter a comment for this key in the next input field.
7. If necessary, click the **Enter key GUID manually in {88888888-4444-4444-4444-} format** check box and enter the GUID you require (this is only possible if the **Security officers can define the GUID for new keys** option is

active in **Central settings**). The predefined GUID {88888888-4444-4444-4444-CCCCCCCCCCCC} cannot simply be accepted for use here. You must change it in every case.

8. Enter a hexadecimal value (letters A-F, numbers 0-9) or a character string in the ANSI input field for the key value. The other associated value is updated automatically. Alternatively, click **Random** (recommended) to have SafeGuard LAN Crypt calculate a value.

9. Click **OK**.

The new key is displayed in the Administration Console.

3.15.1 Specific keys

In addition to generating keys manually, user- and group-specific keys can also be used in SafeGuard LAN Crypt.

When keys are assigned to encryption paths, in the list of keys, one **<USERKEY>** key is also always displayed. This is a placeholder for a user-specific key which the system generates automatically for each individual user when it resolves the encryption rules. **<GROUPKEY>**.

You can use **<GROUPKEY>**, in a similar way to the **<USERKEY>**, to generate a common key for all members of a group. The system generates the group key automatically when it resolves the encryption rules.

An example of how **<USERKEY>** could be used is if all users use one network drive, **U:**, which contains one directory per user, and only the appropriate user can access that directory.

The encryption rule used to specify this would look like this: **U:*.* <USERKEY>**

Another example would be to use **<USERKEY>** to encrypt local temporary directories.

User- and group-specific keys do not appear in the default view under **Central Settings/All SafeGuard LAN Crypt keys**, since they usually are not needed. However, if necessary a Master Security Officer or a Security Officer with the global permission **Use specific Keys** can display these keys, so that the data for them becomes visible.

If required, the values of these specific keys can also be displayed in the **Properties** dialog (context menu/**Properties**) of the respective keys.

To display these specific keys, click **Show Specific Keys** in the context menu of the key list. Now only these specific keys are displayed. To return to the default view, click **Show Specific Keys** again.

Note: Specific keys are not removed from the database when the user/group they belong to is deleted. They remain in the database and can be displayed under **Central Settings/All SafeGuard LAN Crypt Keys/Show Specific Keys**.

Re-assigning specific keys

In certain situations you may need to re-assign a user-, or group-specific key to a user or a group

A user is imported from Active Directory into the SafeGuard LAN Crypt Administration Console.

A user-specific key is generated for this user. If you delete the group, of which the user is a member, in the SafeGuard LAN Crypt Administration Console and re-import it, SafeGuard LAN Crypt automatically generates a new user-specific key when it generates the user's policy files.

The user can then no longer access data that was encrypted with the "old" user-specific key.

To overcome situations like this, you can configure SafeGuard LAN Crypt so that specific keys from deleted users/groups can be reassigned.

To do this, add the **DWORD-Value "ShowUserKeyPage"** to the Windows registry with the Data Value **"1"** under the key:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Sophos\SGLANCrypt

You can also make this entry in the Windows registry for a specific user under **HKEY_CURRENT_USER\...**

If this value is found in the Windows registry the tab **Specific key** is added to the **Properties** dialogs (<user/group>/Context menu/**Properties**) for users and groups.

In this tab you can assign specific keys, which are present in the database and are not assigned to a user or group, to specific users and groups.

If a specific key is assigned to a user or a group it is displayed in the **Specific key** tab. If no specific key is displayed you can replace the current key with a different specific key or assign a new key. You can use any keys that are present in the database and have not yet been assigned to a user or a group.

Note: To make changes, a SO must have the **Use specific Keys** permission. If they do not, they have only read access.

Click the **Browse...** button to display a list of all available keys. Select a key and click **OK**.

In the Specific key tab, click **OK**.

If the current specific key was replaced by a different one, it remains in the database as a non-assigned key.

3.15.2 Importing Keys

You can still use the keys produced in versions 2.x in this version of SafeGuard LAN Crypt. To do this, simply import the keys produced in versions 2.x from version 2.x key files.

You can only import keys that are marked as exportable in the key files, if you know the Master ID and the Master Password for the key file and have the corresponding rights to do so. The file may not be write-protected.

To import a key, select the *Group keys* node under the relevant group and click **Import keys from key file** in the context menu.

Select the key file and enter the key file's Master ID in the **Username** field and its Master Password in the **Password** field.

Click **OK**. The keys are displayed in the right-hand console pane.

3.15.3 Making Keys Active/inactive

In SafeGuard LAN Crypt you can toggle an existing key to make it inactive. If you do this, this key is no longer available when you define encryption rules.

However, you can still use this key in encryption rules that are already in use. It remains saved in the Administration Database and you can also activate it again if required.

To toggle a key from inactive to active (and vice versa), select it and click **Passive/Active** in the context menu.


You can recognize a passive key because it has a red key icon at the start of the line.

3.15.4 Relations between keys

In addition to generating keys for the group in which they are to be used, keys can also be made available for the users in a group by creating a relationship (shortcut) to a key in a different group.

For example: If you want to grant the members of a team the same rights as the members of a different team for a limited amount of time, simply add a shortcut to one group's key to the other group. The shortcut to the key can then be used to create encryption rules. If you could not use a shortcut to a key, you would have to create a new group, add the users of both groups to the new one and create new keys and encryption rules, to make this simple data exchange possible. A shortcut to a key provides a fast and easy way of exchanging data.

To add a key to another group via a shortcut, drag it from the *Keys for Group* node of one group into the node of the relevant group. You also can copy the key in the source group and paste it into the target group.

A key imported this way is displayed as a shortcut .

A Security Officer must have these global permissions before they can insert shortcuts to keys:

- **Create Keys**
- **Copy Keys**

In the source group they must also have the group-specific right

- **Copy Keys**

and

- **Create Keys**

in the target group.

To delete a shortcut the Security Officer must have the global and group-specific **Delete Keys** right.

Keys inserted as shortcuts have the following properties:

- They will NOT be inherited, and are therefore only available in the group in which they have been created. NOT in sub-groups.
- If the "original" key is deleted, all shortcuts are also removed.

Note: In the same way as for "normal" group keys, if you remove a reference it does not mean that the rule, in which they have been used, is no longer valid. To remove access to data you must delete the corresponding encryption rule and generate a new policy file. The client must load the new policy file for the first time, to prevent a user from accessing this data.

3.15.5 Removing keys from a group

You can only delete a key from the group in which it was generated. You must deactivate the key before deleting it.

If you delete keys that are in use, they are removed from the group, but remain in the database as unassigned keys and are displayed in **Central settings/All SafeGuard LAN Crypt keys**.

Adding keys again

If you need this key again later (for example, to access an encrypted backup of old data), you can simply drag it from the list of all SafeGuard LAN Crypt keys into the relevant group, where you can use it again. A Security Officer can add a key to any group for which they have the **Create Keys** right. The key is actually added to group; it is not a shortcut.

Note: If you delete a key which has been never used in an encryption rule, it is actually deleted from the database. The key is no longer displayed under All SafeGuard LAN Crypt keys.

3.15.6 Deleting keys from the database

Under the following conditions keys can be actually deleted (under the node **All SafeGuard LAN Crypt keys**) from the database:

- You must be logged on as a Master Security Officer.
- The keys must not be used in any encryption rule.
- The key must not be present in any group.
- The key must not be a specific key assigned to a user or group.

- The key must be deactivated.

3.15.7 Editing keys

After you have generated a key, you can change its name, the type of inheritance specified for it, and the comment.

You can see whether a key was already used in the **used** column in the console.

To change a key, go to the group in which the key was generated and double-click the relevant key name. You see a dialog in which you can change the key.

3.15.7.1 The Properties dialog

The **Properties** dialog displays information about the selected key. In this dialog you can change the long key name and the settings that define whether or not the key can be inherited. You cannot change the 16-character unique key name for internal use that was generated by SafeGuard LAN Crypt.

Note: To edit a key, the Security Officer must have the group-specific **Create Keys** right for the groups in which the key was generated. Keys that do not belong to a particular group cannot be changed.

Double-click a key to display its properties.

The Properties dialog consists of three tabs:

- The **Key** tab displays a key's data. In this tab you can change the long key name and the settings that define whether or not the key can be inherited. Click **Display keyvalue** to display the key's value.
- The **Groups** tab displays all the groups in which the key is available and can be used to create encryption rules.
- The **Rules** tab displays all the encryption rules in which the key is used.

The **Groups** and **Rules** tabs are for information only. No changes can be made here.

3.16 Encryption rules

The SafeGuard LAN Crypt encryption rules define precisely which data can be encrypted with each key. An encryption rule consists of an encryption path and a key.

The encryption rules defined for a group make up one SafeGuard LAN Crypt encryption profile.

The encryption profile for a group can contain different encryption rules, each one used to encrypt a specific type of data.

You can encrypt entire directories (including sub-directories), particular file types (identified by their file extension) and individual files (identified by their file name or parts of a file name).

When you generate the individual encryption rules the system displays all the keys that are present in the group. The SafeGuard LAN Crypt Security Officer can now assign the appropriate keys to define what data a user should be able to access.

Encryption rules are always generated per group. They consist of a path and a key, and are created in the **Encryption Rules and Tags** node. It is easy to generate an encryption rule because you enter the path details, choose a key and select different options in the same dialog.

Encryption rules are always inherited by subordinate groups.

Note: Do not define an encryption rule for the folder "Temporary Internet Files".

3.16.1 Encryption paths

The encryption paths define which data is to be encrypted. You define them in the Encryption Rules and Tags node *under the relevant group node*. They then apply to all users who are present in that group.

Note: Paths to .zip files or compressed folders cannot be used as encryption paths.

Relative paths

SafeGuard LAN Crypt supports relative path definitions. A relative path definition specifies a path to a directory or a file that does not identify the disk drive involved, or the next highest directory in the hierarchy. If you select a relative path definition, the system encrypts each directory that matches that path definition.

You can use relative paths in two ways:

- Entry: `\my_data*.*`

encrypts every **my_data** directory in the ROOT directories.

EXAMPLE

C:\my_data*.*

D:\my_data*.*

Z:\my_data*.*

- Entry:

my_data*.*

encrypts **EVERY my_data** directory.

EXAMPLE

C:\company\my_data*.*

Z:\Departments\development\Team1\my_data*.*

In both cases all files in the my_data directory are encrypted.

If a directory path begins with a backslash, the relative path definition only applies to root directories.

%USERNAME%

SafeGuard LAN Crypt supports the use of the local environment variable %USERNAME% in path definitions. The local environment variable %USERNAME% in path definition is resolved automatically by SafeGuard LAN Crypt. If you also want other environment variables to be resolved, you must define this in SafeGuard LAN Crypt Configuration (see chapter Resolve all environment variables xxx).

Default directory

To facilitate the encryption of user specific folders, SafeGuard LAN Crypt supports the default directories predefined by Windows (for example My Documents, Common Files etc.). The security officer therefore does not have to consider system-specific variations in client configuration. SafeGuard LAN Crypt determines the correct user-specific path in the correct language from the relevant default directory and encrypts the files that are stored in that directory.

To specify further directories in SafeGuard LAN Crypt, enter the relevant ID.

Example: `<0x002f>*.*` This is the directory that contains the administration tools for all users of the computer (CSIDL_COMMON_ADMINTOOLS).

For a list of all possible IDs, refer to: <http://msdn2.microsoft.com/en-us/library/ms649274.aspx>

3.16.2 Keys

You create the keys used to encrypt data before you generate the encryption rules. All available keys for the relevant group are displayed in the dialog in which you create an encryption rule, and you can select them from a list there.

3.16.3 The sequence of encryption rules

When you load the policy files into the client, SafeGuard LAN Crypt sorts the encryption rules according the method you selected on the Resolving rules tab in Centrall Settings:

- Sort method 1
 1. Ignore rules
 2. Exclude rules
 3. Encryption rules
- Sort method 2
 1. Ignore rules
 2. Exclude rules
 3. Encryption rules specified as absolute paths without wildcards
 4. Encryption rules specified as absolute paths with wildcards not including sub-folders
 5. Encryption rules specified as absolute paths with wildcards including sub-folders
 6. All other encryption rules

An absolute path is either a UNC path (begins with double backslash) or **<drive letter>:**.

For example: **\\server\share*.*** or **c:\encrypt*.***.

- Sort method 3 (default)

Sort method 3 does not distinguish between ignore, exclude and encryption rules.

The rules are sorted in the following order:

1. All absolute paths without wildcards
2. All absolute paths with wildcards not including sub-folders
3. All absolute paths with wildcards including sub-folders
4. All other rules

An absolute path is either a UNC path (begins with double backslash) or **<drive letter>:**.

For example: **\\server\share*.*** or **c:\encrypt*.***.

Within one of the above sections (for example: Sort method 3 - All other rules), the rules are ordered depending on how precise the path definition is.

The order is as follows:

1. UNC paths
2. Paths starting with <drive letter>: Here the backslash after the drive letter is not considered.
3. All other paths. Additionally:
 - Paths with more backslashes are listed before paths with fewer backslashes
 - Paths without wildcards are listed before paths with *. and *.* wildcards

3.16.4 Generating encryption rules

1. Right-click **Encryption Rules and Tags** under the relevant group node and click **New encryption rule** in the context menu.

You can also access the New encryption rule command in a context menu which you display by right-clicking in the right-hand console pane. In the right-hand console pane you can see all the encryption rules that have been generated.

2. Enter a relative or absolute path in the input field under Encryption path. You can use jokers (*) and wildcards (?) in file names (but not in the rest of the path) (for example, *.doc). Click the Browse button ("...") to select a path.

Relative paths and programs supporting file or path specifications in 8.3 notation only: If you use programs which only support file or path specifications in 8.3 notation and you want to access encrypted files with file names longer than 8 characters or files in directories with names longer than 8 characters, you must use 8.3 notation to specify the encryption paths. You have to define these encryption rules additionally. If you do not, 32 bit programs will no longer work. Use the **dir /x** command to display the correct 8.3 name of long file names.

3. Three options appear under **Encryption path**:

- **Include subdirectories**
- **Exclude path**
- **Ignore path**

Include subdirectories

Subdirectories are not included in encryption unless specified. To include all subdirectories in encryption, select the **Include subdirectories** option.

Example: **my_data*. * Include subdirectories**

This encryption rule encrypts all the files in:

C:\company\my_data

C:\company\my_data\project NT

C:\company\my_data\project 2000\demo

Exclude path

Here you must define an encryption rule that excludes this data from encryption. To do this, select the **Exclude path** option in the **File encryption** dialog. As a result, the files specified in the encryption rule are not encrypted. By default this option is not selected.

Example: All files with the file extension **.TXT** are to be excluded from encryption.

- First line:
C:\MYDIR*.TXT, Exclude path, no key: excludes all files with the file extension **.TXT** in the **MYDIR** directory from encryption.
- Second line:
C:\MYDIR*. * , Exclude path not selected, encrypts all files in the **MYDIR** (except **.TXT** file) with the specified key.

Ignore path

SafeGuard LAN Crypt includes the **Ignore path** option. SafeGuard LAN Crypt simply ignores files affected by this type of encryption rule.

In contrast to the **Exclude path** option, this also means there is no access control for these files. You can open them (the encrypted contents are displayed), move and delete them, etc. Despite this, the system checks files in directories that are excluded from encryption to see whether or not they are actually encrypted. In this way SafeGuard LAN Crypt can discover whether files in directories of this kind are encrypted or not. You cannot access encrypted data. SafeGuard LAN Crypt simply ignores files in directories for which the **Ignore path** option has been selected! SafeGuard LAN Crypt does not check them, and users can access encrypted files.

This option is primarily used for files that are accessed very frequently, and that there is no particular reason to encrypt. This improves system performance.

4. Select a key from the list.

Encryption path and key form a SafeGuard LAN Crypt encryption rule. The encryption rules you define for the user/group in total form the user's/group's encryption profile.

Note: In the default view, only the placeholders for <USERKEY> and <GROUPKEY> and the keys created by an SO are displayed. With the Specific key button you can search and display the specific keys.

<USERKEY>

One <USERKEY> key is also always included in the key list. This is a placeholder for a user-specific key which the system generates automatically for each individual user when it resolves the encryption rules.

<GROUPKEY>

In the same way as for <USERKEY>, you can use <GROUPKEY> to generate a common key for all members of the group.

Note: When you use <USERKEY> ensure that only the user to whom this key has been assigned accesses the data. Other users cannot decrypt this data!

An example of how <USERKEY> could be used: all users work on the same network drive, U:, which contains one directory per user. Only the appropriate user should be able to access that directory.

An encryption rule to specify this could look like this:

U:*.* <USERKEY> Another example would be to use <USERKEY> to encrypt local temporary directories.

- **Assign a key without path**

The list of defined encryption paths also includes a placeholder called **Assign a key without a path**.

This is used to give users a key that they can use to encrypted data for which there is no encryption path. This may happen, for example, if encrypted files are copied to a location for which no encryption rules have been defined (with encryption deactivated). They can then use this key to access these files with the appropriate key. If a key is created without a path, the system automatically creates a new placeholder to allow other keys without a path to be generated.

5. Select the relevant options.

6. Under **Comment** you can enter a description or information for the encryption rule created.

7. Click **OK**.

The new encryption rule is displayed in the SafeGuard LAN Crypt Administration.

To edit existing encryption keys, select them and click **Properties** in the context menu. You can also double-click the relevant entry.

3.16.5 Find a specific key

Press the Specific key button to launch a wizard for finding specific keys. A key selected in the wizard will be added to the key list and can be used for encryption rules. The key is only added temporarily. If the wizard is run again and different key is selected, the previously added key will be removed from the list.

On the first page, you can define search criteria. The following criteria can be selected from the drop-down list:

- **Key assigned to a user**

Searches for all specific keys assigned to a user. Enter the user name or logon name in the edit field (search condition). To perform a wildcard search, you can use SQL wildcards. For example, "**Board User 1%**" finds all keys assigned to users whose user names or logon names begin with "**Board User 1**").

- **Key assigned to a group**

Searches for all specific keys which are assigned to a group. Enter the name of the group.

- **Key name**

Searches for all specific keys with a certain name. Enter the long name or short name of the key.

- **Key GUID**

Searches for all specific keys with a certain GUID. Enter the GUID of the key.

- **Currently not assigned keys**

Shows all keys which are currently not assigned to a user or group.

The result of the search is shown on the second page

If a key is currently assigned, the user name or group name is shown under Assigned to. The list contains only specific keys, even if non-specific keys match the search criteria.

Select a key and click Finish to add the key to the list in the dialog for creating encryption rules.

3.17 Encryption tags

If a 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.

For example:

SGFEAPI encrypt /Tag:CONFIDENTIAL c:\documents\encrypt.doc

encrypts the encrypt.doc file in the \documents folder using the key associated with the **<CONFIDENTIAL>** tag.

For details please see the Client API documentation in the \DOC folder of your unzipped installation package.

To generate an encryption tag

1. Right-click **Encryption Rules and Tags** under the relevant group node and click **New Encryption Tag** in the context menu.

You can also access the **New Encryption Tag** command in a context menu which you display by right-clicking in the right-hand console pane. In the right-hand console pane you can see all the encryption rules that have been generated.

2. Enter a name for the encryption tag in the input field under **Encryption tag**.

3. Select a key.

Note: In the default view, only the placeholders for **<USERKEY>** and **<GROUPKEY>** and the keys created by an SO are displayed. With the Specific key button you can search and display the specific keys.

<USERKEY>

One **<USERKEY>** key is also always included in the key list. This is a placeholder for a user-specific key which the system generates automatically for each individual user when it resolves the encryption rules.

<GROUPKEY>

In the same way as for <USERKEY>, you can use <GROUPKEY> to generate a common key for all members of the group.

Note: When you use <USERKEY>, ensure that only the user to whom this key has been assigned accesses the data. Other users cannot decrypt this data!

4. Under **Comment** you can enter a description or information for the encryption tag created.
5. Click **OK**.

The new encryption tag is displayed in the SafeGuard LAN Crypt Administration.

To edit existing encryption tags, select them and click **Properties** in the context menu. You can also double-click the relevant entry.

3.18 Assigning certificates

Each profile is protected by its owner's public key. This public key must be assigned to the user in SafeGuard LAN Crypt Administration, via their certificate.

Note: You do not have to perform this step in the sequence described below. You can also do this at an earlier point in time.

We recommend you check that the certificates are already available for use in the certificate store or a directory (for example, LDAP), before you begin assigning them. You can use standard Windows tools to import the certificates into the relevant certificate store.

SafeGuard LAN Crypt has a Certificate Assignment Wizard that assigns certificates automatically.

Note: If a Windows user who assigns a certificate has no right to change the password log file in the file system, no SafeGuard LAN Crypt certificates can be generated.

3.18.1 Assigning a certificate to a user

To assign a certificate, proceed as follows:

1. Select **Members and certificates for group** in the relevant group node. In the right-hand console pane you see a list of all users.
2. Double-click a user, or right-click the user, and then on **Properties** in the context menu. You see the **Properties** dialog.
3. In this dialog you select one of the following options to assign one or more certificates to the user.

- **New**

Click **New** if you want SafeGuard LAN Crypt to generate a new certificate for the user. If no certificates are available, the SafeGuard LAN Crypt Administration Console can even generate certificates itself. However, only SafeGuard LAN Crypt should use these certificates! The certificate it generates is saved as a PKCS#12 file in the default directory.

Note: Any certificate generated in this way must then be distributed to the appropriate user. Otherwise the user will not be able to access their encryption profiles.

- **Import**

If the certificate you require is not yet present in the certificate store, it does not appear in the list of available certificates. In this case click **Import**. The system opens a dialog in which you can select the required certificate. Then click **OK**, and the system assigns the certificate to the user. The import certificate is automatically imported into the certificate store called **Other people**.

Note: Only certificate files whose format is .cer, .crt or .der can be imported. .p12 or .pfx files cannot be imported.

- **Add**

Opens a dialog in which you can assign an existing certificate to a user. In this dialog you see a list of all the certificates present in the certificate store.

Assigning Certificates using an LDAP source

SafeGuard LAN Crypt allows you to assign certificates from an LDAP source. To do this, select **LDAP** from the drop-down list in the **Choose a certificate** dialog.

An edit field appears in which you can enter the URL of the LDAP source. After you click **Refresh** the content of the LDAP source is displayed. Terms in square brackets (e.g. Sub_OU_1]) represent the OUs in the LDAP source. To display an OU's certificates, simply double-click it. Double-click [...] to go up one level up in the hierarchy. Select a certificate and click **OK**. The certificate is now assigned to the Security Officer.

Note:

If the LDAP server does not allow anonymous logon, the logon credentials for the server must be entered as the distinguished name (example: CN= John Doe,O=Marketing) on the Server tab in the Central settings.

If you have a certificate that was assigned from an LDAP directory, the private key belonging to this certificate must be available on the user's workstation.

4. Use one of the options described to select a certificate and click **OK**.

The system displays the certificate in the console pane on the right-hand side next to the user. In the console pane the system displays information about the certificate used (period of validity, serial number, issuer).

Note: The Certificate snap-in is available under each user/group node. Here the system only displays the users that are members of the relevant group.

3.18.2 Generating and assigning SafeGuard LAN Crypt certificates

You use this wizard to generate certificates for **all** users to whom no certificate has yet been assigned, and then automatically assign these certificates to the users.

To open this wizard, click **Generate certificates** in the context menu for each **Members and certificates for group** node or on the appropriate icon in the tool bar.

In the next dialog you specify whether you generate and assign the certificates **in this group only** or **in this group and all subgroups** or **for selected users only**.

For selected users only

This option is only displayed if one or more users are selected. When you click **Members and certificates of group** under the desired group node in the left-hand console pane, the members of the group are displayed in the right-hand console pane. Selecting the users works the same way as in Windows Explorer (select the users with the left-hand mouse button while pressing the SHIFT or CTRL key).

The system generates and assigns the certificates automatically. Click **Finish** to close the wizard.

Note:

The key files (.p12) generated here and the public part of the Security Officer's certificate are saved in the directory specified in the central settings, and must be made available to the users. To set this up, in SafeGuard LAN Crypt Configuration you specify the folder in which SafeGuard LAN Crypt is to search for a .p12 file for the user, if the private key for the policy file is not present. The same applies to the public part of the Security Officer's certificate. The file names must match the user's logon name ("Logon*.p12") so that SafeGuard LAN Crypt can automatically recognize the user key files. When SafeGuard LAN Crypt finds the correct file, it displays a PIN dialog. You must send a PIN letter to tell the user this PIN (which is in the password log file). The certificate and associated key are automatically imported after the user enters the PIN.

If SafeGuard LAN Crypt finds a .cer file that contains the public part of the Security Officer's certificate, it automatically imports it. Alternatively you can distribute the key files for the users and the public part of the Administrator certificate manually. If you do this, make sure that the clients import both of them.

Alternatively you can distribute the key files for the users and the public part of the Administrator certificate manually. If you do this, make sure that the clients import both of them.

3.18.3 Certificate Assignment Wizard

SafeGuard LAN Crypt has a wizard that performs most of the tasks involved in assigning certificates to users. To run the wizard, select **Certificate Assignment Wizard** in the context menu for **Members and certificates for group**.

In the wizard's first dialog, specify whether you assign the certificates to members **in this group only** or **in this group and all subgroups** or **for selected users only**.

For selected users only

This option is only displayed if one or more users are selected. When you click **Members and certificates of group** under the desired group node in the left-hand console pane, the members of the group are displayed in the right-hand console pane. Selecting the users works the same way as in Windows Explorer (select the users with the left-hand mouse button while pressing the SHIFT or Ctrl key).

The wizard supports the assignment of certificates from the following sources:

- Assign certificates from the Active Directory
- Assign certificates from an LDAP directory
- Assign certificates from a file system directory
- Assign certificates from certificate stores

3.18.3.1 Assigning certificates from the Active Directory

Assigning certificates from the Active Directory

To select the **Assign Certificates** option from the Active Directory, enter the DNS address of the Active Directory Server in step 2. Usually this is the domain controller.

If you click **Use Defaults** the system applies the address of the Domain Controller to which you are currently logged on.

To start the wizard, click **Next**. The system imports and assigns the certificates automatically. It displays a message to confirm that it has successfully assigned the certificates. Click **Finish** to close the wizard.

3.18.3.2 Assigning certificates from an LDAP directory

If you select the **Assign Certificates from an LDAP directory** option, you must enter the address of the LDAP directory, from which you want to import the certificates, in step 2.

In **Address**, enter the complete computer name of the LDAP server (for example: Server.MyDomain.com) and specify the relevant port. The standard port for the LDAP server is set by default.

In **DN (Distinguished Name)**, enter the node in the LDAP structure from which the system is to search through the directory. Enter the node in the LDAP directory, using its Distinguished Name (DN). You must not enter the computer name (dc=computername...) here again.

Note: Microsoft AD: The input field must not remain blank. Here you must enter at least the domain and the country.

Example 1: **DC=mydomain,DC=De**

Example 2: **OU=marketing,DC=mydomain,DC=DE**

If you click **Use Defaults**, the system applies the address of the Domain Controller to which you are currently logged on.

To assign the certificates, the system matches the properties of the LDAP user with the SafeGuard LAN Crypt user.

The following LDAP user properties can be used:

- E-mail address
- Common Name
- Full name
- NT 4.0 account name
- User Principal Name
- user-defined attribute

You can specify that these properties match the following SafeGuard LAN Crypt user properties:

- E-mail address
- User name
- Logon name
- Comment

Select the LDAP user property you want each SafeGuard LAN Crypt user property to correspond to. If these properties match, the system imports the LDAP user's certificate and automatically assigns it to the appropriate SafeGuard LAN Crypt user.

Note: To prevent inconsistencies we recommend that you use the e-mail address as an assignment criterion, as it is always unique.

To start the wizard, click **Next**. The system imports and assigns the certificates automatically. It displays a message to confirm that it has successfully assigned the certificates. Click **Finish** to close the wizard.

3.18.3.3 Assigning certificates from a directory

If you select the **Assign certificates from a directory** option, you must enter the address of the directory from which you want to import the certificates, in step 2.

After you specify the directory you see a dialog in which you define the method that SafeGuard LAN Crypt is to use to assign certificates to the users.

- **Username equals filename**

Select this option, if the file names of the certificate files are identical to the user name. All users that correspond to a file name are assigned to the appropriate certificate.

- **User name is in DN**

If the user name is contained in the certificate's Distinguished Name, SafeGuard LAN Crypt can find it and assign the certificate to the appropriate user. SafeGuard LAN Crypt uses a search pattern to identify the user name in the DN.

You can specify this search pattern in the input field under the **User name is in DN** option. The system searches for the user name that appears between the two specified character strings in the DN.

Example:

In the certificate, the user name is always present under **CN=**, (e.g. **CN=JSmith,OU=SafeGuard LAN Crypt**) If you enter **CN=** in the first input field, and **,OU=SafeGuard** in the second input field, SafeGuard LAN Crypt will find the user name that is located between these two character strings (in our example, JSmith). The certificate is automatically assigned to the user.

- **Match as specified in a file**

You can also take the required assignment from a file. For example, the public part of the certificate generated with the SafeGuard Smartcard Administration Console is saved in a file in a pre-defined directory. SafeGuard Smartcard Administration uses these files to generate a file that records which certificate is assigned to each user.

Other PKIs can also generate lists of this kind. This list can, of course, even generate itself.

It must use the following format:

User name;file name

Example:

Guest;Guestcer.cer

HansMeier;Meier.cer

....

The system assigns the certificates in accordance with the assignment in this file.

Click **Next** to start the wizard and automatically assign the certificates.

3.18.3.4 Assigning certificates from certificate stores

If you have selected the **Assign certificates from certificate stores** option, the second step of the wizard prompts you to specify whether it is to generate a list of all available certificates and import them, or whether an existing list is to be imported. SafeGuard LAN Crypt uses this list to assign the certificates.

You can, for example, use the **Import a previously created list** option if assignment has already been started once, but the process was interrupted after the list was generated. The system can then reuse the file that was created here.

If you select the **Create and import a list of all available certificates** option, the system displays this dialog.

Select a name for the list output file.

SafeGuard LAN Crypt creates a list of all certificates available in the certificate stores. This list contains placeholders for the user names to which the certificate is to be assigned.

Example:

******; My; OU=SafeGuard LAN Crypt Certificate, CN=LAN Crypt Admin; 0010-ae671e47...**

******; Root; CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com; 0010-4cad...**

The placeholders (****) can be replaced by the user names.

If the certificate contains the user name, you can use the following option:

- **Try to insert names**

SafeGuard LAN Crypt can try to recognize a user: if the certificate's Distinguished Name contains the user name, SafeGuard LAN Crypt can find it and assign the certificate to the appropriate user. SafeGuard LAN Crypt uses a search pattern to identify the user name in the DN. You specify the search pattern in the input field under the "User name is in DN" option. The system searches for the user name that is found between the two specified character strings in the DN.

Example:

In the certificate, the user name is always present under "CN=" (e.g. **CN=JSmith,OU=SafeGuard LAN Crypt**) If you enter CN= in the first input field, and enter ,OU=SafeGuard in the second input field, SafeGuard LAN Crypt will find the user name that is located between these two character strings (in our example, JSmith). The system replaces the placeholder with the user name and automatically assigns the certificate to the user.

• Open output file for editing with Notepad when finished

If this option is selected the system opens the list of certificates after it has been generated. You can now edit this list. You can replace the placeholder with the user name in the relevant certificates. When you save the list, the system uses the edited version to assign certificates.

Click **Next** to start the wizard and automatically assign the certificates.

3.19 Providing encryption rules - generating policy files

SafeGuard LAN Crypt saves every profile that has been generated (or changed) in its Administration Database. Here they do not yet have any effect on individual users.

To resolve individual profiles and building the policy files, a SafeGuard LAN Crypt Security Officer must run the SafeGuard LAN Crypt Profile Resolver. This generates policy files for each user in accordance with the settings made in the Administration Console. The next time a user logs on, the system loads the new encryption profile.

Note: You must always generate new policy files after you change settings in the SafeGuard LAN Crypt Administration console (added new keys, added new rules, ...). The changes become effective for users, after they load the new policy files onto their machines.

3.19.1 Creating (resolving) policy files for an entire group or selected users

Policy files are created with the Build Profiles Wizard. If more than one user is selected and profile creation is started from the toolbar or from the context menu of users, the wizard is launched.

If a single user and Build /Clear profile is selected from the context menu, the profile is created immediately. A message box informs the Security Officer about the result.

Depending on the view, the wizard is launched from, there are different entry points for the wizard:

• Scope selection (default)**• Collect users and verify certificates:**

If no scope selection is possible or allowed, for example, if profile creation is started for selected users in the node **Selected users and certificates**.

• Profile creation:

If **Clear profile** is started for multiple users. This action cannot be started for an entire group. No certificate checks are necessary.

On the wizard's first page, the scope for the profile creation can be selected. Profiles can be created for:

- users in this group only
- users in this group and all subgroups

- selected users only.

Activate the Resolve changed groups only option to restrict the creation of policy files to the users for whom new policy files are required due to modifications made. The generation of policy files in large organizations can thereby be accelerated.

On the wizard's second page, the progress is displayed, while all user data is collected and the users certificates are verified. After all users have been processed, the next page is displayed.

On the wizard's third page, certificate warnings are displayed. If users do not have a valid certificate assigned or a user's certificate expires soon, the users are displayed on this page. The following certificate warnings and errors are displayed:

- The certificate of the user will expire soon (warning).
- All assigned certificates of the user have expired (error).
- A user does not have a certificate assigned (error).
- The user does not have a certificate assigned and is marked to be skipped (warning).

In case of an error at least one of the options on this page must be selected before profile creation can be continued:

- **Do not warn me again for the users shown in the list**

Skips all users whose certificates have expired or who do not have certificates assigned. These users are skipped during profile creation until new certificates are assigned to them.

- **Always skip users that have no valid certificate assigned**

Ignores all users without a valid certificate. This is a global setting and can also be configured in Central Settings.

Click the **Back** button to return to the wizard's scope selection page.

The wizard's fourth page shows a progress bar while all profiles are created. The wizard can be cancelled, but this only stops profile creation. Policy files which have already been created are not deleted or reverted.

The wizard's fifth and last page displays the number of created profiles. If an error occurred that forced the profile creation to stop, an error message is displayed.

Note:

If you make any changes on the Antivirus tab, the Resolving Rules tab or Other Settings tab in Central Settings, this always results in a change in the policy files of all users. After a change of this type, new policy files for all users have to be created.

3.19.2 Selected provision via the Certificate snap-in

You can also use the Certificate snap-in to provide policy files. You can access it under the **Members and certificates for groups** node and under each group node.

If you use the Certificate snap-in to generate policy files, you can also use these additional functions:

- Select users to whom a certificate is to be assigned. You do not have to generate new policy files for all users. Like in Windows Explorer, you can select several users at the same time (mouse-click + SHIFT or Ctrl).
- The Security Officer immediately sees which users are present in the group.
- The system displays certificate icons next to the user name to show the certificates' status:
 - red means:

the certificate has expired.

- yellow means:

the certificate is running within the configured expiration warning period.

- green means:

everything is OK.


- grey icon means:


either no certificate was assigned to the user, or that user was missed out when the system assigned certificates.

To provide the policy files, select the required users and then click the blue gear icon in the tool bar or on **Build Profile** in the selected user's context menu.

3.19.3 Clearing profiles

You can use the Certificate snap-in to clear the profiles of one or more users. Clearing a profile means generating an empty profile. The user has to log on once to an empty policy file, to overwrite the settings of the current policy file cached on their machine. After that they can no longer access encrypted data.

To clear a profile select the user in the Certificate snap-in and click the **Clear profile for selected user** icon  or click **Clear profile** in the context menu.

You can select several users (select the users with the left mouse button while holding down the SHIFT key) and clear their profiles by clicking the  icon.

Note:

The settings in SafeGuard LAN Crypt Central Settings define how profiles are cleared. The process for deleting profiles is similar to the one for creating profiles. If the Novell name is used (two policy files are created), both profiles will then be deleted if this setting is not changed. If this setting is changed at runtime, it may occur that two policy files have been created, but only the one with the Windows user name is deleted. This is because the Create additional policy files based on Novell name option has been deactivated and therefore only the policy file with the Windows user name is deleted. The Novell policy file remains in the defined storage location and theoretically can be used for logging on. The system behaves in a similar way depending on the selected file format for policy files (.pol/.pol.biz/.xml.bz2). In this case up to four policy files are generated for each user. Please keep this in mind and, if necessary, coordinate with the system administrator.

3.20 Database logging

SafeGuard LAN Crypt logs events that are triggered by the SafeGuard LAN Crypt Administration Console in the SafeGuard LAN Crypt database. With SafeGuard LAN Crypt's logging functions you can specify which events are to be logged, archive events and check log entries.

The global permissions **Read Logging Entries** and **Manage Logging** control how Security Officers access the logging module. These rights can be granted to Security Officers by the Master Security Officer.

Read Logging Entries The SO can see the settings for logging and the logged events.

Manage Logging The SO can change the settings for logging. They are allowed to archive, delete and check entries.

Basic settings for logging can be made in the SafeGuard LAN Crypt Administration Console under the **Logging** node in the **Central Settings**. This node can only be viewed by Security Officers, who have at least the **Read Logging Entries** right.

The basic settings can only be made by a Master Security Officer. They can be given additional security by adding a second level of authorization (scenario **Manage Logging**; requires the global permissions **Read Logging Entries** and **Manage Logging**).

The basic settings also specify which events are to be logged. Only a Master Security Officer can specify this.

Note: Events, which occur before a SO logs on, cannot be logged directly to the database. They are cached, and written to the database after the next successful logon.

3.20.1 Settings

Click **Properties** in the context menu of the **Logging** node to display a dialog in which you make the basic settings.

Settings tab

On this page you specify the period of time after which log entries can be deleted.

When using distributed databases this setting guarantees that entries can be copied to headquarters, before they are deleted at individual sites.

State tab

The **State** tab displays information about the current state of the logging module.

3.20.2 Logged events

If the **Logging** node is selected, all events, which can be logged are displayed in the right-hand console pane. Here you can select which event is to be logged.

Note: Only Master Security Officers can select which events are to be logged.

Click the **Severity** column header to sort the events according to the categories (Emergency, Alert, Error, Warning, Notice, Info).

To select an event to be logged, double-click it, or select it and click the appropriate symbol in the tool bar.



Enables the selected event(s) for logging.



Disables the selected event(s) for logging.

You can select several events at the same time (mouse-click + SHIFT or Ctrl).

After you have selected the events, click the diskette icon in the tool bar to save the settings. However, in each case you will be asked whether you want to save the settings or not, when you leave this view without saving.

3.20.3 Viewing and exporting entries

Note: To view and export entries, a Security Officer must have the global permission **Read Logging Entries**. A Security Officer who has the Read Logging Entries global permission can display entries and export them to a file.

To display the entries, click **View and export entries** in the **Logging** node's context menu or click the icon in the tool bar.



This opens the dialog where you can view and export the logged entries.

This dialog displays all the events that have been selected for logging.

Click the column headers to sort the entries.

Double-click an entry to display details for that entry.

SafeGuard LAN Crypt also has a filter in which you can specify conditions for the displayed entries.

3.20.4 Filtering events

Click the **Filter** button in this dialog to open a second dialog where you can specify a filter for the displayed events.

You can filter events using these constraints:

- **Only show entries of a specified event**

If you select this option, only the entries for the event you selected from the drop-down list are displayed. The list contains all events that can be logged.

- **Only show entries of a specified Security Officer**

If you select this option, you can select a Security Officer from the drop-down list. Then only these events, which were logged when the specified Security Officer was logged on, are displayed. The drop-down list only contains Security Officers for whom entries exist.

- **Only show entries of a specified severity**

If you select this option, you can select a particular level of severity or a range of severity, for which entries should be displayed. **Is less or equal** and **is greater or equal** refers to the number before the severity level.

- **Only show entries from a specified time interval**

If you select this option, you can define a period of time, in which the entries were logged.

- **Only show entries that have specified archive state**

If you select this option, you can specify whether **archived entries only** or **not yet archived entries only** are displayed (entries that have already been archived remain in the database until they are deleted). If this option is not selected, both type of entries are displayed.

- **Only show entries from a specified location**


Select this option to specify a location from which entries are to be displayed. If you are using a distributed database there may be several locations involved. The way in which the database is replicated determines which locations can be displayed.

3.20.5 Archiving, deleting, checking entries

Note: A Security Officer needs the global permission **Manage Logging** before they can archive, delete and check entries.

A Security Officer who has the global permission **Manage Logging** can archive, delete and check logged entries.

Click **Archive, delete and check entries** in the **Logging** node's context menu or click the symbol in the task bar to launch a wizard for carrying out these tasks.

 Launches the wizard to archive, delete and check logged entries.

Archiving entries

To archive entries, select **Archive entries** and click **Next**.

In the next dialog, enter:

- Date and time of the last entry that is to be archived. All entries from that time to the present will be archived.
- The location (if available) to which entries should be archived.
- The name of the file the entries should be written to.

Click **Next**. In the next dialog you can see how many entries have been selected. Click **Next**. When all the entries have been archived, the wizard's last dialog is displayed. Click **Finish** to close the wizard.

Entries that have already been archived remain in the database and can be deleted. Their state is set to **Archived**.

Deleting archived entries

To delete archived entries, select **Delete archived entries** and click **Next**.

In the next dialog, specify:

- Date and time of the last entry that is to be deleted. All entries from that time to the present will be deleted.
Note: The last possible time depends on the minimum age for logged entries, which was specified in the basic settings.
- The location (if available) from which entries are to be deleted.

Click **Next**. In the next dialog you can see how many entries have been selected. Click **Next**. When all entries have been deleted, the wizard's last dialog is displayed. Click **Finish** to close the wizard.

Checking archive integrity

To check the integrity of logged events select **Check archive integrity** and click **Next**.

In the next dialog, select which data you want to check. You can select the entries in the database or archived entries to be checked.

To check entries in a distributed database, select which location's entries are to be checked.

If you want to check an archive, select a file by clicking the **Browse ...** button,

Click **Next**. In the next dialog you can see how many entries have been selected. Click **Next**. When all entries have been checked, the wizard's last dialog is displayed. The result of the integrity check is displayed. If the data has been manipulated, an appropriate warning is displayed.

Click **Finish** to close the wizard.

4 SafeGuard LAN Crypt Configuration

Note: Configuration settings have to be defined with the 32 bit Group Policy Management Editor or the 32 bit Local Group Policy Editor. If you use a 64 bit system, start these editors by clicking on the respective entry under Start\All Programs \Sophos\SafeGuard LAN Crypt. This ensures that the correct version is launched.

The following settings are machine-specific or user-specific settings. To edit these settings, you need administrator rights in the domains or in Active Directory. These settings should only be made by a system administrator.

You select configuration settings in the **LAN Crypt Configuration** node. This node is displayed when you work with system policies in every computeruser node in the Management Console.

In the Active Directory environment, the **LAN Crypt Configuration** node appears in the GPO **Computer Configuration** or **User Configuration/Windows settings/SafeGuard**.

Note: As an alternative you can use the administrative template provided in the \config folder of your unzipped installation package. You may want to use them on computers which do not have SafeGuard LAN Crypt Administration installed.

Usually the configuration settings are intended for machines. However, you can make user-specific settings to assign specific rights to selected users. If a user-specific setting is made, it overrules a machine-specific setting.

If you want to undo a user-specific setting so that a machine-specific setting applies, you must set the status of that setting to **Not Configured**. To do so, select a setting and press the DEL key. In the Management Console, **No** is then displayed in the **Configured** column.

4.1 Client settings

If the **Client Settings** node is selected, the configurable settings are displayed in the right-hand console pane. Double-click an entry to open a dialog in which you can make the settings you require for it.

4.1.1 Allow Encrypt/Decrypt

Any user of SafeGuard LAN Crypt can encrypt or decrypt files by selecting a menu item in the context menu for those files. This means that users can even encrypt files for which no rule has been defined.

If you want to prevent this, you can specify here that this option is not displayed in the context menu for those files.

Allow Encrypt/Decrypt: no

Prevents files, for which no encryption rule has been defined, from being encrypted or decrypted via their context menu.

4.1.2 Ignore during Certificate Verification

In SafeGuard LAN Crypt you can specify whether any errors found when checking user certificates are to be ignored.

This procedure is useful if the validity period of a certificate has expired and no new certificate is yet available. To ensure that a user can continue to access their encryption profile, the period of validity check can be ignored until a new certificate is issued. As a result, the same certificate, which has actually expired, can still be used. Once a new certificate is available, you can cancel **Ignore time invalidity** again.

Note: Ignoring errors that occur during certificate checks always means a reduction in security.

- **Ignore certificate revoked**

If a certificate is on a **Certificate Revocations List**, which is evaluated during logon, it may not actually be used for logging on. Nevertheless, a user can continue to access their encryption profile even if this option is selected.

- **Ignore time invalidity**

Even if the validity period of a certificate has expired, the user can continue to access their encryption profile, if this option is selected.

- **Ignore bad certificate chain**

The user can continue to access their encryption profile even if the public part of the issuer's certificate is not available on the client machine or is kept in the wrong certificate store.

- **Ignore unknown revocation**

When PKIs from some vendors write reasons for the revocation of a certificate to a CRL, they do not comply with common standards. You cannot usually use a certificate if the reason for revocation is not known. However, if this option is selected, the user can continue to access their encryption profile.

Note: Please note that ignoring errors found when checking user certificates usually means compromising the company's security policy.

These settings can also be defined under Server Settings. Certificates are verified out both when a Security Officer logs on to the SafeGuard LAN Crypt Administration Console, and when an additional authorization is performed.

4.1.3 Use Novell Name

Here you specify whether or not the system uses the Novell logon name to find policy files. If you specify that policy files are to be generated with Novell names in the Administration under Central Settings/Directories, SafeGuard LAN Crypt generates two policy files for each user. One file has the Novell logon name and the other has the Windows user name. The contents of these files are identical.

If you log on to a Novell server you must always use the Novell logon name.

If the system settings specify that the Windows user name must be used as the logon name, set **Use Novell Logon Name** to no.

Note:

If a client cannot log on to a Novell server (for example, because the link to the server fails), and the user logs themselves on locally with their Windows user name, the encryption profile is still loaded correctly from the policy file because SafeGuard LAN Crypt can also use the Windows user name to identify the appropriate policy file. In this situation, the file is read from the cache. The cache is as up-to-date as the last Novell network logon.

4.1.4 Resolve all environment variables

SafeGuard LAN Crypt resolves the environment variable **%USERNAME%** for paths.

Here you can specify whether other environment variables are to be resolved in paths.

However, using other environment variables in paths may create problems if users are able to change them. This may result in the path data no longer functioning correctly in the encryption profile.

4.1.5 Enabled Menu Entries

Here you can specify which menu options are visible in the SafeGuard LAN Crypt user menu on a client computer. By default, all menu options are displayed. If you suppress a menu option here, it is not displayed on the client computer. This means that this functionality is also not available on this client. This enables you, for example, to prevent decryption from being switched off (deactivated) on a client computer.

4.1.6 Default Ignore Rules

As the SafeGuard LAN Crypt driver is always loaded when you boot a workstation, all the files have already been checked to if they are encrypted, and therefore also that they have the appropriate access rights, even if no user-specific encryption profile has yet been loaded. This may slow down performance in this phase.

However, if you make a machine-specific setting in SafeGuard LAN Crypt's configuration you can configure the SafeGuard LAN Crypt driver to ignore specific directories until the user's encryption profile has been loaded.

Double-click **Default Ignore Rules** in the **Client Settings** to open a dialog in which you can specify the directories (for example, "**c:*.*;d:*.***") that SafeGuard LAN Crypt's driver is to ignore.

If you enter more than one path, separate each path by a semicolon.

However, if you use this rule you must take into account that SafeGuard LAN Crypt's specific access check will not be carried out until the user's encryption profile is loaded.

Example:

If you enter "**c:*.*;d:*.***" as the Default Ignore Rules, the driver will ignore all directories on the **C** and **D** drives until the user's encryption profile is loaded.

Even if you use SafeGuard LAN Crypt on a terminal server, you can speed up performance by using the Default Ignore Rules setting. If, for example, several users are working on the same terminal server, but only one of them uses SafeGuard LAN Crypt, you can tell the driver to ignore all the other users' sessions. Because no encryption profile has been loaded for them, only the Default Ignore Rules apply to them.

4.1.7 Security Officer Certificate Client Location

To specify the storage location, select **Client Settings** and, in the right-hand console pane, double-click **Security Officer Certificate Client Location**.

After you specify a path, SafeGuard LAN Crypt automatically attempts to import the Security Officer certificate from this directory if the certificate for the relevant user policy file is not present. As a result it imports all (!) .cer files from the directory you have specified.

4.1.8 Keyfile Client Location

To specify the storage location, select *Client Settings* and, in the right-hand console pane, double-click **Keyfile Client Location**.

After you specify a path, SafeGuard LAN Crypt automatically attempts to import a .p12 key file for the user if the private key for the policy file is not present. This file must be called "**logonname*.p12**" so that the system can recognize that it belongs to that particular user.

The two paths described above are not default settings, i.e. the public part of Security Administrator certificates or user certificates are not loaded automatically until the Security Officer has specified the paths.

SafeGuard LAN Crypt Administration stores both the .p12 files for users and the public part of Security Officer certificates in the same directory. However, from the client view, these paths can be configured separately so that either of these functions can be deactivated if necessary. Despite this, these paths are usually the same. If you want the Security Officer certificate and user certificates to be loaded automatically from different directories, you must copy them manually into the relevant directories.

4.1.9 Policyfile Client Location

To specify the storage location, select **Client Settings** and, in the right-hand console pane, double-click **Policyfile Client Location**.

Enter the path for the location of the user-specific policy file. To ensure that clients can access their policy files (for example, on a shared network drive), the path must be entered from the clients' point of view.

This is usually the directory in which they were generated by SafeGuard LAN Crypt. You must follow the UNC (Universal Naming Convention) capitalization rules because no disk drives are associated with these files at this point!

In this setting, you can use the `%LOGONSERVER%` environment variable (for load balancing etc.).

4.1.10 Policyfile Cache Directory

To specify the cache storage location, select *Client Settings* and, in the right-hand console pane, double-click **Policyfile Cache Directory**.

A local copy of the policy file is saved in this directory. This copy is usually loaded from a network directory. The user must have authorization to write data in this local directory. This guarantees that a user's encryption profile is available even if there is no connection to a network.

You can either use one of the storage locations shown in the list or select **<other>** and enter a different one in the input field.

Note:

The storage locations shown in the list are default Windows directories that depend on which operating system you are using. **<Local Application Data>** always refers to a directory on the local machine, whereas any other directories (for example, Roaming Users) may also be present on network drives. If you enter a storage location manually, you must make sure that this directory actually exists on the client computer.

If you want to remove a user from your SafeGuard LAN Crypt environment, please remember that the local copy will still be present on the computer. This user can then use the permissions in this local copy to access data for as long as this copy remains on the computer. To prevent this, you should create an empty policy file for this user. To do so, Clear the policy file and remove the user from all groups.

4.1.11 Delay when loading profiles

Here, you can specify a period of time (in seconds) that will pass before the user profile is loaded. This delay is for example important, if a certificate or a token is used. The delay in loading the profile ensures that the token can be accessed when the certificate is required. Typical value: 20 seconds.

4.1.12 File types for the Initial Encryption Wizard

If you define specific file types here, only the files of the specified type will be processed by the Initial Encryption Wizard. The user cannot change this setting in the initial encryption wizard!

This setting only affects files for which an encryption rule exists.

If a directory contains also other files of a file type specified here, they will not be included in initial encryption. They will only be encrypted when the user opens and saves them again.

If you intend to let the user define this setting themselves in the Initial Encryption Wizard, leave the setting at not configured.

If you specified file types here and you intend to let the user make a selection later, set the setting back to not configured again.

Note: This setting only applies to the Initial Encryption Wizard. If initial encryption is started via the Explorer extension, the setting does not have any effect.

Specify the file types in a list separated by semicolons.

Example: `doc;xls;txt`

4.1.13 *Cached Policyfile lifetime*

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.

If this option is set to **not configured**, the behavior of SafeGuard LAN Crypt is as described.

Using this setting you can change the standard behavior

Note: You can set an option to not configured by selecting it and click Delete in its context menu (right-click). In the **Configured** column, no will be displayed besides the relevant option.

Here you can specify for how long the cached policy will be valid on the client computers.

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 on the policy share.

The time period during which policy files are cached and are therefore valid can be defined in days or weeks.

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. An automatic update will also be carried out according to the update interval settings for the user profile.

Policy files are not cached

If this option is set to **0**, 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 this Administration version. 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 (see Profile Update Interval on page 128 xxx). 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.

4.1.14 NTFS Decompress Files

This setting enables the Initial Encryption Wizard to process NTFS compressed files. If you set the **NTFS Decompress Files** option to **yes**, the wizard decompresses NTFS compressed files and encrypts them, if an applies.

If you set the **NTFS Decompress Files** option to **no**, the Initial Encryption Wizard will ignore NTFS compressed files. They will not be encrypted, even if an encryption rule has been specified for them.

After configuring this option, users cannot change it in the Initial Encryption Wizard! Users can only configure this option themselves in the Initial Encryption Wizard, if it has been set to **not configured** here.

4.1.15 EFS Decrypt Files

This setting enables the Initial Encryption Wizard to process EFS encrypted files. If you set the **EFS Decrypt Files** option to **yes**, the wizard decrypts EFS encrypted files and encrypts them again if a SafeGuard LAN Crypt encryption rule applies.

If you set the **EFS Decrypt Files** option to **no**, 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.

After configuring this option, users cannot change it in the Initial Encryption Wizard! Users can only configure this option themselves in the Initial Encryption Wizard, if it has been set to *not configured* here.

Note:

You can set an option to **not configured** by selecting it and click Delete in its context menu (right-click). In the **Configured** column, **no** will be displayed besides the relevant option.

4.1.16 Profile Update Interval

This setting defines how often SafeGuard LAN Crypt checks for new policy files and updates them if necessary.

For updating policy files SafeGuard LAN Crypt needs access to the network drive on which the policy files are stored. SafeGuard LAN Crypt checks whether a new version of the policy file exists on the network drive and updates the policy file on the client computer if required.

SafeGuard LAN Crypt automatically carries out all steps required for successfully loading the user profile (if necessary, searching for new certificates, verifying new certificates, etc.). The old profile will only be replaced by the new profile and the new profile will only be loaded, if no errors occur during the process. Afterwards, the counter for the duration of cache storage will be reset. If the policy files are identical, the counter will also be reset.

If this option is set to not configured, policy files are not updated.

The update interval can be specified in minutes, hours, days and weeks.

Note: SafeGuard LAN Crypt does not allow any update intervals shorter than 15 minutes. If the option is set to **0**, policy update is disabled.

4.1.17 Silent mode if user profile is missing

SilentModelfUserProfileIsMissing.xml

If the default setting applies, SafeGuard LAN Crypt shows an error message, if the system does not find a user profile.

Here you can specify that this error message is to be suppressed, if no user profile is found.

If you set **Hide error message** to **yes**, the error message will not be displayed.

4.1.18 Silent mode if user profile is missing

SilentModelfUserProfileIsMissing.xml

If the default setting applies, SafeGuard LAN Crypt shows an error message, if the system does not find a user profile.

Here you can specify that this error message is to be suppressed, if no user profile is found.

If you set **Hide error message** to **yes**, the error message will not be displayed.

4.1.19 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 deactivate this function, double-click **Enable Persistent encryption** and select **No** in the list field of **Activate Persist. Encryption**.

4.1.20 Strong private key protection

Here you can specify that the user is prompted for authentication every time the private key is used by SafeGuard LAN Crypt.

4.1.21 CSPs and Algorithms

Here you can specify the CSP and hash algorithm.

For the newest client version only the **CSP to be used for importing a private key** has to be selected.

For clients below version 3.90 **additional** settings have to be configured. You have to select a **CSP to be used for verifying the policy file signature** and a **hash algorithm to be used for signing/verifying the policy file**.

4.2 Server Settings

Note:

You must make these settings for the server. They have no effect on client computers. However, it is vital that you make these server settings before you start the Administration function for the first time.

4.2.1 Strong private key protection

Here you can specify that the user is prompted for authentication every time the private key is used by SafeGuard LAN Crypt.

4.2.2 SQL Dialect

Here you specify the SQL dialect that is to be used for communication with the ODBC data source.

Select:

- MS SQL Server
- Oracle
- Standard SQL

This will then be used in your system configuration.

4.2.3 Database Owner

Here you enter the Database Owner to ensure that the database you are using can be addressed correctly.

For the MS SQL server, the default value "dbo" for the generator must not be changed. This only needs to be changed if you are using an Oracle database.

Note:

If you are using an Oracle database, you must enter the Database Owner here in CAPITAL LETTERS. This must be the same name that was used during the creation of the database tables.

4.2.4 ODBC Data Source

Here you enter the name that is to be used to access the ODBC data source.

SafeGuard LAN Crypt uses SGLCSQLServer as the default name for the ODBC data source. If you want to use a different name, enter it here before you run SafeGuard LAN Crypt Administration for the first time.

Note:

The name for the ODBC data source is case sensitive! The name you enter here must be identical to the name that was entered when the ODBC data source was created. Only 32 bit ODBC data sources can be used.

4.2.5 Ignore during Certificate Verification

Here you can specify which certificate status is to be ignored when a Security Officer logs on or when certificates are assigned in administration console.

4.2.6 Hash Algorithm

The hash algorithm has to be configured in **Client Settings**.

4.2.7 Check certificate extensions

By default, when SafeGuard LAN Crypt assigns certificates from the certificate store, it only uses certificates that have the values **Key Encipherment** and/or **Data Encipherment** set for the "**keyusage**" property.

However, in **Check certificate extensions** you can specify that this check is not carried out, which enables SafeGuard LAN Crypt to use certificates with other properties.

Check extensions: **no** permits the use of certificates with other properties.

Note: However, whether or not these types of certificates can be used with SafeGuard LAN Crypt depends on which CSP you are using. If you decide to switch off this check, ensure that the type of certificate you want to use can actually be used with SafeGuard LAN Crypt.

4.3 Unhandled Drives, Unhandled Application, Unhandled Devices

In SafeGuard LAN Crypt you can specify that drives, applications and devices (network file systems) are to be "unhandled" (ignored) by SafeGuard LAN Crypt's filter driver and therefore excluded from transparent encryption/decryption.

A backup program is an example of an application that might not be handled (known as "unhandled"). If you want backup data to remain encrypted, you can exclude this application from the encryption/decryption process. The data then remains encrypted when it is backed up.

You can significantly improve performance by excluding entire disk drives. If, for example, no encryption is to be performed on the E drive, it can simply be defined as an "ignored drive". Alternatively you could define a rule for this disk drive using the "Ignore encryption rule" option.

When you mark a drive as "unhandled", the filter driver does not process the profile so file operations are performed more quickly.

You will find these settings in the **LAN Crypt configuration** node.

Note: As these are machine-specific settings, they do not come into effect until you restart the client computer.

4.3.1 Adding ignored disk drives

Select **Unhandled Drives** and click **Add unhandled drive(s)** in the context menu.

Select the disk drives you want SafeGuard LAN Crypt to ignore and click **OK**.

4.3.2 Adding ignored applications

Select **Unhandled applications** and click **Add unhandled application** in the context menu.

Typical use:

- Backup programs can be defined as "unhandled" to ensure that they always read and save encrypted data.
- Applications that may cause errors when used simultaneously with SafeGuard LAN Crypt, but which do not require encryption, can usually be excluded from the encryption process.

To specify an unhandled application, you must enter the entire name of its executable file.

Enter the application's name and path (if required) and click **OK**.

4.3.3 Adding ignored devices

Select **Unhandled Devices** and click **Add unhandled device** in the context menu.

The **Unhandled Devices** dialog displays network file systems that you can exclude from the SafeGuard LAN Crypt encryption process. For technical reasons you cannot exclude single network drives here. You can only exclude entire network file systems. The pre-defined devices listed here are:

- Citrix Client Drive Mapping
- Client for Microsoft networks
- Microsoft Client for NetWare
- Multiple UNC Provider
- Novell Client for NetWare

Note: Security officers can exclude individual (network) disk drives from the encryption process by creating an encryption rule for this purpose.

In addition to these standard network file systems, you can also exclude specific devices by entering their device names. This may be useful if file systems from third-party suppliers are being used and you want to exclude them from the encryption process.

Administrators can use tools such as OSR's Device Tree to display the names of file systems currently being used on the system.

Windows Vista and Windows 7

For Windows Vista and Windows 7 only option **Multiple UNC Provider** is considered.

Under Windows Vista and Windows 7 the individual redirectors were replaced by the Multiple UNC Provider. This results in the fact that it is no longer possible to exclude individual network file systems from encryption. Under Windows Vista and Windows 7, either all network file systems can be excluded from encryption or encryption can be enabled for all network file systems.

If option **Multiple UNC Provider** is used, network drives will not be encrypted.

All remaining settings will be ignored under Windows Vista and Windows 7.

4.4 Programs with specific behavior when saving files

Some programs (e.g. Microsoft Office 2007 and higher) use a special approach when saving files. In this case, problems may occur when opening an unencrypted file to which an encryption rule applies (for example due to the fact that no initial encryption has been performed) and saving the file again. Due to the encryption rule applying to the file it would have to be encrypted when it is saved. However, due to the specific behavior of the program when saving the file (creating temporary file - renaming the file --> changing the encryption status) SafeGuard LAN Crypt cannot encrypt the file.

To solve this problem, you can specify these programs here. Using the information specified here SafeGuard LAN Crypt can also encrypt files of this type correctly.

To add a program of this type:

1. Select **Programs with specific behavior when saving files** and click **Add program with specific behavior when saving files** in the context menu.
2. Enter the name of the executable of the program. Example: **WINWORD.EXE**

3. Click **OK**.
4. Repeat these steps for each program you want to add.

The programs requiring special handling by SafeGuard LAN Crypt due to their special behavior when saving files are displayed in the view on the right-hand side.

Note: This problem only occurs when saving a file which was unencrypted when it was opened and has to be encrypted due to an encryption rule applying to it (change of the encryption status).

If you are using Microsoft Office 2007, we strongly recommend specifying the executables of this software here.

5 APPENDIX

5.1 Logging

... Rights for 'SO_Sophos-Linz' added. Allowed: 0x86000000 - Denied: 0x0)...

The values after **Allowed:** and **Denied:** show which rights have actually been modified. You can use the following tables to interpret the values.

Allowed: 0x86000000

ACL for SO: Read 0x80000000
 ACL for SO: Change Certificate 0x02000000
 ACL for SO: Change Region 0x04000000
 Allowed: 0x86000000

	Rights	Values
Create SOs	0x000001	
Generating profiles	0x000002	
Generating keys	0x000004	
Copy Keys	0x000008	
Delete Keys	0x000010	
Reading keys	0x000020	
Generating certificates	0x000040	
Assign Certificates	0x000080	
Change Groups	0x000200	
Logon to Database	0x000400	
Authorize Operations	0x000800	
Change Users	0x001000	
Generating rules	0x002000	
Change global rights	0x004000	
Change ACLs	0x008000	
Use specific Keys	0x010000	
Change Configuration	0x020000	
Read Logging Entries	0x040000	
Manage Logging	0x080000	
Import Directory Objects	0x100000	

Global rights of a Security Officer

	Permissions	Values
Create Key	0x00000001	
Copy Keys	0x00000002	
Delete Key	0x00000004	
Create Rules	0x00000008	
Assign Certificates	0x00000010	
Add User	0x00000020	
Delete User	0x00000040	
Add Group	0x00000080	
Delete Subgroups	0x00000100	
Move Groups	0x00000200	
Change Properties	0x00000400	
Delete Group	0x00000800	
Create Profiles	0x00001000	
Change ACL	0x00002000	
Read	0x00004000	
Visible	0x00008000	

ACL for a group

Permissions	Values
Create Key	0x00000001
Copy Keys	0x00000002
Copy Keys	0x00000004
Create Rules	0x00000008
Assign	0x00000010
Certificat	
Add User	0x00000020
Delete User	0x00000040
Add Group	0x00000080
Delete	0x00000100
Subgroups	
Move Groups	0x00000200
Change	0x00000400
Properties	
Delete Group	0x00008000
Create	0x00001000
Profiles	
Change ACL	0x00002000
Read	0x00004000
Visible	0x00004000

Permissions	Values
Change Name	0x01000000
Change Certificate	0x02000000
Change Region	0x04000000
Assign Configuration	0x08000000
Delete SO	0x10000000
Change Global Permissions	0x20000000
Change ACL	0x40000000
Read	0x80000000

5.2 Permissions

5.2.1 Global permissions

Permissions	Description
Create Security Officer	The SO has permission to create more SOs.
Create Profiles	The SO has the global permission to run the Profile Resolver and generate policy files for individual users. This global permission is the prerequisite for setting the permission „Create Profiles for a specific group“ for a SO. Create Profiles allows the SO to build profiles for users where the SO has the right Create Profiles for the user’s parent group. Owning this permission is a prerequisite for assigning values to keys. A user with the permission Create Keys on its own can only generate keys without values!
Create Profiles for all Members	This permission requires that the permission Create Profiles is set. This global permission is the prerequisite for setting the permission Create Profiles for all Members for a specific group. Create Profiles for all Members allows a SO to create profiles for all users where the SO has the permission Create Profiles on the parent group of the user or the permission Create Profiles for all Members on one of the groups the user is member of. Note: As the global permission Create Profiles is a prerequisite for Create Profiles for all Members the following applies: Deactivating the permission Create Profiles automatically also deactivates the permission Create Profiles for All Members. Activating the permission Create Profiles for all Members automatically activates the permission Create Profiles.
Create Keys	The SO can generate keys in the individual groups. A user with the permission <i>Create Keys</i> on its own can only generate keys without values! Within the Administration Console, keys without a value can be assigned to groups and users. The value itself is generated when policy files are generated. To generate keys with values manually, the SO must have the <i>Create Profiles</i> permission.

Permissions	Description
Copy Keys	The SO is allowed to copy keys.
Delete Keys	The SO can delete keys from individual groups.
Read Keys	The SO can see the data for the individual keys for a group.
Create Certificates	The SO can generate certificates for users.
Assign Certificates	The SO is allowed to assign certificates to the users. The SO is allowed to run the wizard for assigning certificates. This global permission is the prerequisite for setting the permission Assign Certificates for a specific group for a SO. Assign Certificates allows the SO to assign certificates to users where the SO has the right Assign Certificates for the user's parent group.
Assign Certificates to all Members	This permission requires that the permission Assign Certificates is set. This global permission is the prerequisite for setting the permission Assign Certificates to all Members for a specific group. Assign Certificates to all Members allows a SO to assign certificates to all users where the SO has the right Assign Certificates on the parent group of the user or the right Assign Certificates to all Members on one of the group the user is member of. Note: As the global permission Assign Certificates is a prerequisite for Assign Certificates to all Members the following applies: Deactivating the permission Assign Certificates automatically also deactivates the permission Assign Certificates to all Members. Activating the permission Assign Certificates to all Members automatically activates the permission Assign Certificates.
Administer Groups	The SO can make changes in the groups. Adding sub-groups, moving groups, synchronizing groups, deleting groups.
Log in Database	The SO can log on to the SafeGuard LAN Crypt database. The default setting is for this permission is active. With this permission an SO can easily make changes to the database without too much effort (for example, if staff leave the company). This right is not granted to people who are only permitted to act if someone else authorizes their actions. This ensures that these people can only authorize actions that require confirmation, and have no way to make changes in SafeGuard LAN Crypt.
Authorize Operations	The SO can participate in actions that require confirmation.
Administer Users	The SO can add users to a group, remove them from a group, and synchronize groups.
Copy Users	The SO is allowed to add (copy) users to groups. This global permission is the prerequisite for setting the permission Copy User for a specific group for a SO. To add a user to a group, the SO must have the permission Copy User on the parent group of the user.
Create Rules	The SO is allowed to generate encryption rules for the users.
Change Global Permissions	The SO can change the global rights granted to another SO.
Change ACLs	The SO can change the ACL for a group.
Use specific Keys	The SO can use concrete specific keys in encryption rules and can display specific keys in <i>All SafeGuard LAN Crypt keys</i> .
Change Configuration	The SO can change the configuration (paths). This permission is required to display the Configuration tab in the Central settings, and for the SO to be able to make changes in the Directories tab if they are logged on to the database.
Read Logging Entries	The SO can view the settings used for logging and the logged events.
Manage Logging	The SO can change the logging settings. They are permitted to archive, delete and check entries.
Import Directory Objects	The SO can import OUs, groups and users from a directory service and add them to the SafeGuard LAN Crypt database. Before they can import Directory Objects, the SO also needs the <i>Administer Groups</i> permission and the <i>Administer Users</i> permission. These are set automatically when the <i>Importing Directory Objects</i> permission is selected. If an SO does not have this permission, the <i>Directory Objects</i> node (used to import OUs, groups and users) is not displayed in the Administration Console.

5.2.2 Permissions for changing the settings for a Security Officer

Permissions	Description
Change Name	Allows changes to the name of the SO to whom the owner of the permission is assigned.
Change Certificate	Allows changes to the certificate of the SO to whom the owner of the right is assigned.
Change Region	Allows changes to the region prefix of the SO to whom the owner of the right is assigned.
Assign Configuration	Allows changes to the configuration of the SO to whom the owner of the right is assigned.
Delete SO	Allows the SO, to whom the owner of the permission is assigned, to be deleted.

Permissions	Description
Change Global Permissions	Allows changes to the global permissions of the SO to whom the owner of the permission is assigned.
Change ACL	Allows changes to the global rights of the ACL to whom the owner of the right is assigned.
Read	Displays the SO to whom the owner of the permission is assigned in <i>Central settings \Security Officer Administration</i> . This is the prerequisite for all rights that allow the processing of this SO. Is set automatically if a right of that type is selected.

5.2.3 SO permissions for processing the groups

Permissions	Description
Create Key	The SO is allowed to generate keys in the group.
Copy Keys	The SO is allowed to copy keys.
Delete Key	The SO is allowed to delete keys.
Create Rules	The SO is allowed to generate for the users.
Assign Certificates	The SO is allowed to assign certificates to the users. The SO is allowed to run the wizard used to assign certificates. Assign Certificates allows the SO to assign certificates to the users in the group where the group is also the parent group.
Assign Certificates to all Members	This permission requires that the permission Assign Certificates is set. Assign Certificates to all Members allows the SO to assign certificates to all users in the group: users where the group is the parent group of and also users that are member of the group and have a different parent group. Note: Setting Assign Certificates to all Members to Allow automatically sets Assign Certificates to Allow. Setting Assign Certificates to Deny automatically sets Assign Certificates to all Members to Deny.
Add User	The SO is allowed to add users to the group manually. This permission is a prerequisite for importing/synchronizing groups and users.
Copy User	The SO has the right to add users from this group to another group. This is only allowed for the members where this group is also the parent object.
Delete User	SOs is allowed to use the <i>Members and certificates for group</i> snap-in to delete users. This permission is a prerequisite for importing/synchronizing groups and users.
Add Group	The SO is allowed to use a group's context menu to add new groups. This permission is a prerequisite for importing/synchronizing groups and users.
Delete Subgroups	The SO is allowed to delete the sub-groups for this group. This permission is a prerequisite for importing/synchronizing groups and users.
Move Groups	The SO is allowed to move manually-created groups in Administration (with drag and drop). Imported groups cannot be moved. This permission is a prerequisite for importing/synchronizing groups and users.
Change Properties	The SO is allowed to change a group's properties.
Delete Group	The SO is allowed to delete groups. This assumes that the SO has removed the "Delete Subgroups" permission in the group above. This permission is a prerequisite for importing/synchronizing groups and users.
Create Profiles	The SO has the permission to run the Profile Resolver and generate policy files for selected users. Create Profiles allows the SO to build profiles for the users in the group where the group is also the parent group.
Create Profiles for all Members	This permission requires that the permission Create Profiles is set. Create Profiles for all Members allows the SO to create profiles for all users in the group: users where the group is the parent group of and also users that are member of the group and have a different parent group. Note: Setting Create Profiles for All Members to Allow automatically sets Create Profiles to Allow. Setting Create Profiles to Deny automatically sets Create Profiles for All Members to Deny.
Change ACL	The SO is allowed to change the ACL for the group (for example, by adding another SO).
Read	The SO has read rights for this group and can see the contents for the snap-ins. Is set automatically if edit permissions are granted.
Visible	The SO can see the group. Is set in the base node and inherited downwards. If it is refused for the SO, the group is hidden ("Read" must also be denied).

6 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.

7 Legal notices

Copyright © 2018 - 2019 conpal GmbH, 1996 - 2018 Sophos Limited and Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group. conpal, AccessOn and AuthomaticOn are registered trademarks of conpal GmbH.

All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licence where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

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