Creating Trust in
the Digital Society

utimaco®

u.trust

LAN Crypt

Product version: 13.0.1
Document date: August 2026

Table of contents

1 Overview 3

1.1 What is u.trust LAN Crypt? 3

1.2 Data protection using u.trust LAN Crypt 5

1.3 Transparent encryption 7

1.4 Architecture 12

2 Getting started 16

2.1 Certificates 16

2.2 Installation 23

2.3 Unattended installation 25

2.4 Upgrading 27

2.5 Language settings 32

2.6 Uninstallation 33

3 Administration 34

3.1 Required steps 36

3.2 Preparations for administering u.trust LAN Crypt 37

3.3 Master Security Officers 41

3.4 Administration: overview 45

3.5 Central Settings 49

3.6 Displaying All u.trust LAN Crypt keys 81

3.7 Showing selected users and certificates 83

3.8 Creating a Security Officer 85

3.9 Logging on to Administration 99

3.10 Importing groups and users 100

3.11 Assigning Security Officers to organizational units 113

3.12 Properties of groups 120

3.13 Properties of users 124

3.14 Security environment design 127

3.15 Generating keys 127

3.16 Encryption rules 135

3.17 Encryption tags 150

3.18 Assigning certificates 152

3.19 Providing encryption rules - generating policy files 163

3.20 Database logging 168

4 u.trust LAN Crypt Configuration 175
4.1 Client Settings 176
4.2 LAN Crypt Administration Settings 186
4.3 Unhandled Drives, Applications and Devices 188
5 APPENDIX 192
5.1 Logging 192
5.2 Permissions 195
6 Legal notices 202
7 Technical Support 203

1 Overview

1.1 What is u.trust LAN Crypt?

u.trust 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 *u.trust 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: *u.trust 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 *u.trust LAN Crypt*). However, without *u.trust 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, *u.trust LAN Crypt* is your product of choice.

The Security Officer (SO) can specify which files and folders are to be protected by *u.trust LAN Crypt*, centrally, by defining one or more encryption rules. For example, to ensure that all Word documents are protected, the Security Officer would define the rule **.docx*. 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
*.docx	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\HR*.xlsx	Key3	This encrypts all the Excel files in the specified server folder with “Key3”.

With *u.trust LAN Crypt* the Security Officer 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 net logon 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 Security Officer uses the *u.trust 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 protected separately, by means of certificates, for every single user. Thus, among other things, all keys contained in this file are encrypted with the public key of the certificate of the respective user, so that only the authorized user who also has the private key for the certificate used can open this file via the *u.trust LAN Crypt* client application. A **P**ublic **K**ey **I**nfrastructure (PKI) already available in the organization can be used here. Alternatively, the Security Officer can use the option of generating the certificates himself using *u.trust LAN Crypt*.

The *u.trust 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. *u.trust LAN Crypt* can also be used to configure different Security Officer roles whose permissions can be restricted to suit specific tasks in specific areas.

Only the Master Security Officer (MSO) always has all rights. A Master Security Officer is also able to delegate individual tasks and rights for the administration of *u.trust LAN Crypt* to further Security Officers and thus create an administration hierarchy that meets the organizational structure of every company.

1.2 Data protection using u.trust LAN Crypt

u.trust 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.

In order for a user to be able to encrypt and decrypt data with *u.trust LAN Crypt* on his workstation, he must be able to access his policy file. This is done through a network share for the location where the policy file is located. The policy file is encrypted and protected from unauthorized use by a certificate. To be able to use them, the user must have the private key of his certificate and know the password.

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

u.trust 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 *u.trust 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.

Note: Even in normal operation, Windows often swaps parts of the working memory to the hard disk. In some cases, for example in the event of a crash or so-called "blue screens", the entire memory content can even be written to the hard disk. As a result, sensitive information that is otherwise only available in main memory (such as the contents of open documents) could be stored in a file on the hard disk. Hard disk encryption (such as *BitLocker* or *Utimaco DiskEncrypt*) ensures that the content of this often-sensitive data is stored on the hard disk in encrypted form in any case and is thus optimally protected against spying. For this reason, the use of hard disk encryption is recommended as an important basic protection and as a useful addition when using *u.trust LAN Crypt*.

u.trust LAN Crypt supports Windows as well as macOS and for mobile devices Android and iOS / iPadOS.

u.trust LAN Crypt Administration and Windows Administration

A separate administration computer is used to configure *u.trust LAN Crypt* and administer encryption profiles. To draw a clear distinction between Windows administration and *u.trust 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 *u.trust LAN Crypt*. The *u.trust LAN Crypt* Administration user interface consists of snap-ins for the MMC. *u.trust LAN Crypt* Administration stores most of the objects to be administered (user data, keys, encryption paths, etc.) in their own database.

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 *u.trust LAN Crypt* uses a dedicated database and is totally independent of system administration. The keys in the *u.trust LAN Crypt* Administration database are encrypted and thus protected against unauthorized access. In addition, this database prevents the *u.trust 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 *u.trust LAN Crypt*-specific data in a separate database.

To provide the best possible protection, *u.trust LAN Crypt's* functions are divided into two parts:

- ***u.trust LAN Crypt* User functions**

  The *u.trust LAN Crypt* user functions include the encryption and decryption information for data. This information is required for everyday tasks using *u.trust 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, *u.trust LAN Crypt* has a range of display functions that allow the user to view "their" encryption profile, and the keys provided to him.

- ***u.trust LAN Crypt* Security Officer functions**

  The *u.trust LAN Crypt* Administration offers functions that are reserved for a Security Officer. Encryption rules can only be administered if you have a Security Officer certificate. Only then is it possible to create new encryption profiles or manage existing ones, for example.

Both components can be installed separately.

1.3 Transparent encryption

For the user, transparent encryption means that all data stored in an encrypted form (in encrypted folders 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 folder, they are encrypted in accordance with the encryption rule that applies to that folder. You can, of course, also define different encryption rules for different file extensions or names in the same folder. Encryption is not specific to folders. 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 be used to prevent a user from unintentionally decrypting files when copying or moving them to a folder for which no encryption rule exists.

1.3.1 Accessing encrypted data

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

If the user has the key with which the files are encrypted, he can open and work with these files at any time, even if no encryption rule refers to these files in his encryption profile.

1.3.2 Renaming or moving folders

For performance reasons, *u.trust LAN Crypt* does not change the encryption status when complete folders are moved using Windows Explorer. This means that no encryption, decryption, or re-encryption is carried out when a folder is moved or renamed.

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

Note: However, this only applies if there is no encryption rule for the new storage location. If there is, however, the files will be encrypted according to the encryption rule applicable to the new storage location.

Moving files and folders securely: *u.trust LAN Crypt* also enables files and folders to be moved securely. The files are also encrypted, decrypted, or re-encrypted as required in accordance with the applicable encryption rules. The source files are securely deleted ("wiped") after being moved.

This function is available via the **Secure move** entry in the Windows Explorer context menu under the item ***u.trust LAN Crypt***. A dialog can then be used to select the location to which the files are to be moved.

1.3.3 Explicit file decryption

If the **Persistent Encryption** function is deactivated, a file for decryption only needs to be copied or moved to a location or folder for which no encryption rule exists. It will then be automatically decrypted.

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.

1.3.4 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 *u.trust LAN Crypt* remain encrypted in the *Recycle Bin*. For emptying the *Recycle Bin* no key is necessary.

1.3.5 Files / folders excluded from encryption

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

- Files in the *u.trust LAN Crypt* installation folder.
- Files in the Windows installation folder.
- Policy File Cache.

  Location is specified in *u.trust 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).

1.3.6 Persistent Encryption

Files normally remain encrypted by *u.trust LAN Crypt* only as long as they are subject to an encryption policy. Files would therefore be decrypted if they were copied or moved to a folder for which no encryption rule applies.

If you do not want unwanted plaintext copies of encrypted files to be created, **Persistent Encryption** can prevent this. With the **Persistent Encryption** you can ensure that encrypted files are not decrypted when they are moved or copied.

Security Officers or System Administrators can deactivate this behavior in the *u.trust LAN Crypt* configuration via a group policy (GPO) in Windows. By default, this function is already activated in *u.trust LAN Crypt*. If **Persistent Encryption** is deactivated, encrypted files will be decrypted and stored in plain text, when they are copied / moved to a location which is not defined in the encryption rule.

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

- The *u.trust 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**.

1.3.6.1 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.

1.3.6.2 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.

Note: There is no access protection for files in folders that are subject to an **ignore path rule** if the mini filter is used as the encryption driver.

1.3.6.3 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!!

Note: For files in folders that are subject to an **Exclude path rule**, access protection still exists.

1.3.7 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 > Text Document**. Immediately right-click in a folder without encryption rule and click **New > Text Document**. 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**.

1.3.8 Client API and encryption tags for DLP products

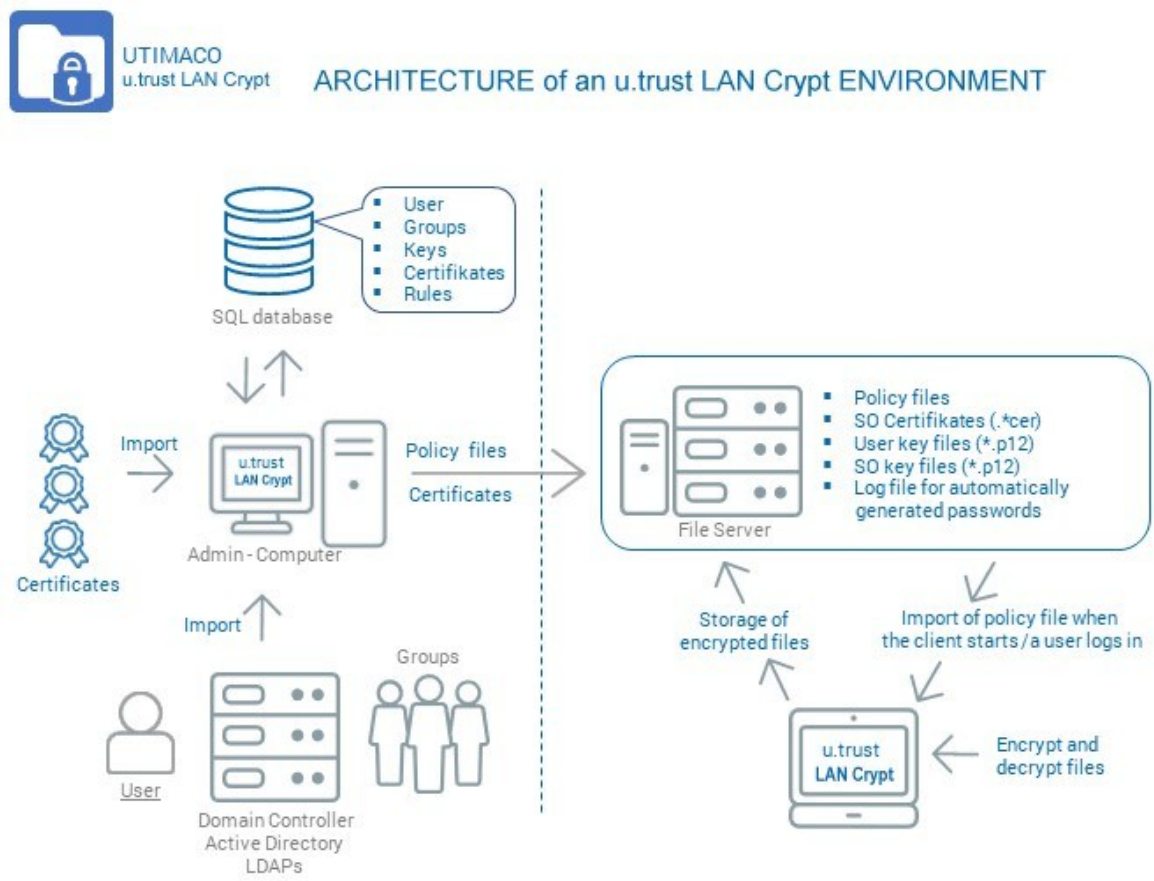
If a DLP product identifies data that needs to be encrypted, it can use the *u.trust LAN Crypt* Client API to encrypt these files. In *u.trust LAN Crypt* Administration, you can define different encryption tags that specify the *u.trust LAN Crypt* key to be used.

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.

1.4 Architecture

u.trust LAN Crypt consists of the two components: The *u.trust LAN Crypt* Administration and the *u.trust LAN Crypt* Client. Both components are typically installed on standard workstation computers with the Windows 11 operating system. Security Officers use *u.trust LAN Crypt* Administration to define and distribute encryption profiles and then make them available to users.

The following figure illustrates the interaction of the individual components and how *u.trust LAN Crypt* is integrated into the company network:



1.4.1 u.trust LAN Crypt Administration

The administrative component contains the necessary tools for the central administration of *u.trust LAN Crypt* and is used by one or more security officers. The installation is typically carried out on one or more workstation computers with Windows 11 as the operating system. Installation on a Windows server system supported by *u.trust LAN Crypt* is also possible if central administration via Windows Terminal Services or Citrix MetaFrame is required. This is particularly recommended in larger environments and especially in distributed locations. The *u.trust LAN Crypt* Administration is then accessed via Remote Desktop (RDP) or Independent Computing Architecture (ICA) protocol. For further information about the supported Windows versions, please refer the *u.trust LAN Crypt* release notes.

Since the maximum security and confidentiality of the data to be protected can only be guaranteed if the *u.trust LAN Crypt* Administration and system administration are independent

of each other, *u.trust LAN Crypt* has separate user and group administration. To make work easier, users and groups managed by *u.trust LAN Crypt* can be imported from an existing Active Directory or another LDAP-based directory.

The *u.trust LAN Crypt* Administration requires an SQL database to store configuration data and to manage *u.trust LAN Crypt* users and groups. The database can be installed locally on the administration system if the Microsoft SQL Server Express Edition is used. For larger installations with several Security Officers, the use of a central database system in the form of a Microsoft SQL or Oracle server is recommended.

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. *u.trust 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 *u.trust LAN Crypt* database is generated. These officers define the first policies and decide whether the Four-eyes-principal rule (two Security Officer 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).

u.trust LAN Crypt uses **K**ey **E**ncryption **K**eys (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 means 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.

u.trust 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 must be recovered in an emergency, the Security Officer must assign this specific key to another user. This type of recovery requires special administrative permission and can be linked with a „Four-eyes-principal 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 (see “*Re-assigning specific keys*“).

Note: For information on an emergency recovery of the *u.trust LAN Crypt* Administration, for example if the certificate of the Master Security Officer is damaged, see Chapter 3.5.10 "*The Recovery Keys tab*" on page 72.

The policy files include all the rules, access rights and keys required for transparent encryption. Before a user can encrypt/decrypt data using the *u.trust 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 Net logon share.

Note: You do not need to install *u.trust LAN Crypt* components on file servers or domain controllers. To facilitate the administration of the *u.trust LAN Crypt* user groups and client computers, however, it can be helpful to install the administrative template files (*.ADMX files) supplied with the admin console on an administrative workstation (RSAT). These enable simple and clear administration of the most important settings for the *u.trust LAN Crypt* clients.

Policy files are stored as BZ2-compressed XML files, which means they are plain text, but contain, among other things, the keys available to the respective user – in encrypted form, of course. To work with them, they must be decrypted using the **P**rofile **E**ncryption **K**ey (PEK).

To do this, the profile loader of the *u.trust LAN Crypt* Client compares the certificates listed in the policy file with the certificates in the certificate store of the logged-in user. If the profile loader finds a match, it transfers the task of extracting the corresponding PEK to the Crypto API. This in turn activates the **C**ryptographic **S**ervice **P**rovider (CSP) or **K**ey **S**torage **P**rovider (KSP) with the associated private key. Depending on the type of provider, the user may be prompted to enter a PIN or password. The policy file is then decrypted and sent to the filter driver.

u.trust LAN Crypt also supports the use of certificates stored on smartcards, USB tokens or suitable hardware boards.

Note: You can use *u.trust 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 *u.trust LAN Crypt* settings are identified by mechanisms in the operating system.

A *u.trust 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 *u.trust 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 must be able to access the policy file to have their data encrypted or decrypted transparently as soon as they close or open it.

1.4.2 u.trust LAN Crypt Client

The *u.trust 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.

After starting the *u.trust LAN Crypt* client, it accesses the folder with its PKCS#12 container (*.P12 file) and its policy file via mechanisms of the operating system (registry settings, group policies). When accessing the PKCS#12 container for the first time, the user must enter a PIN that a Security Officer has given him in a secure way. The user certificate is then stored in the local certificate memory of the operating system, i.e., linked to the loaded Windows profile. The certificate allows access to the encrypted parts of the policy file via the “**P**rofile **E**ncryption **K**ey - PEK”. If the certificate is stored on a hardware-based token supported by the client component, no further user interaction is required for encryption and decryption after the token has been unlocked.

The *u.trust LAN Crypt* Client then loads the policy file with its settings and keys.

2 Getting started

2.1 Certificates

u.trust 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.

Note: Please do not use certificates with a validity of several hundred or even more than a thousand years!

In terms of information security, the validity period of certificates should not exceed a period of 5 years if possible. For CA certificates (**C**ertificate **A**uthority), on the other hand, Utimaco recommends a maximum validity period of 20 years.

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

- A company either has its own **P**ublic **K**ey **I**nfrastructure (PKI) or uses a Trust Center to create certificates for the users. In this case, existing certificates can be used.
- Alternatively, the *u.trust LAN Crypt* Administration component can generate self-signed certificates. These certificates can only be used by *u.trust LAN Crypt*! The certificates also have a Critical Extension (OID) 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 *u.trust LAN Crypt* you can configure whether a critical extension is added to a newly generated certificate or not.

Note: In certain situation other applications will ignore these Critical Extensions on *u.trust 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 *u.trust LAN Crypt* certificates with the Microsoft Management Console's certificate snap-in to prevent these certificates from being used in other applications.

Note: If you set to add a critical extension to newly generated certificates, such a certificate, when you view its certificate information, will display the status: "*A certificate contains an unknown extension that is marked critical*". However, you can safely ignore this information, because *u.trust LAN Crypt* knows the *OID* (object identifier) of its own certificates and therefore recognizes them as valid.

The certificates are assigned to the users within the *u.trust LAN Crypt* Administration component.

Important information about how to use certificates:

- *u.trust LAN Crypt* only uses the Microsoft Crypto API for certificate functionality.
- *u.trust LAN Crypt* version 13.0.1 supports Key **S**torage **P**rovider (KSP).
- *u.trust LAN Crypt* supports all **C**ryptographic **S**ervice **P**roviders (CSPs) that comply with certain standards (e.g., RSA key length at least 2048 bits). They include, among others, the Microsoft Enhanced CSP.

  Note: The Microsoft Standard CSP (Microsoft Base CSP) cannot be used. for self-signed certificates generated by *u.trust LAN Crypt*.

  Note: Please also note that **C**ryptographic **S**ervice **P**roviders (CSP) for key operations by *u.trust LAN Crypt* are now only supported in conjunction with Shims that make them accessible as **K**ey **S**torage **P**roviders (KSP).

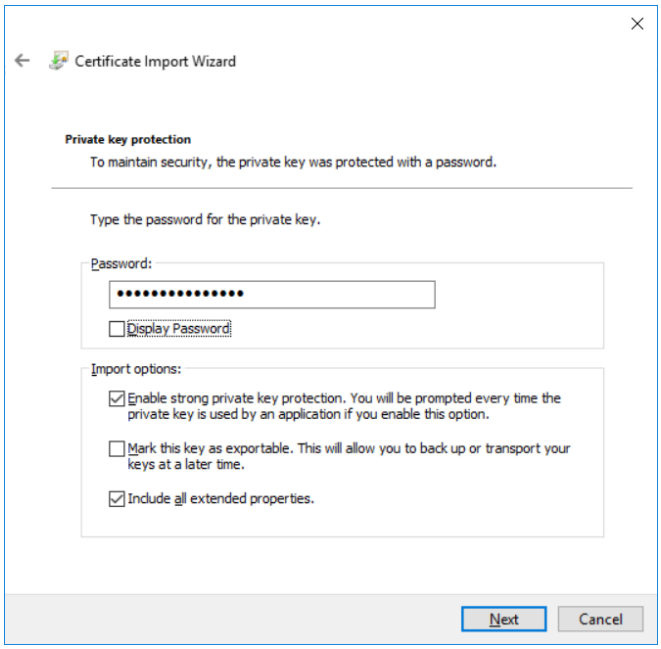
  Note: Please also note that the SHA-1 signature algorithm is no longer supported by Microsoft CSP, because it is no longer considered secure.

If you have any questions about the compatibility of other CSPs or KSPs, please contact the Utimaco support team (see *Technical Support* on page 203).

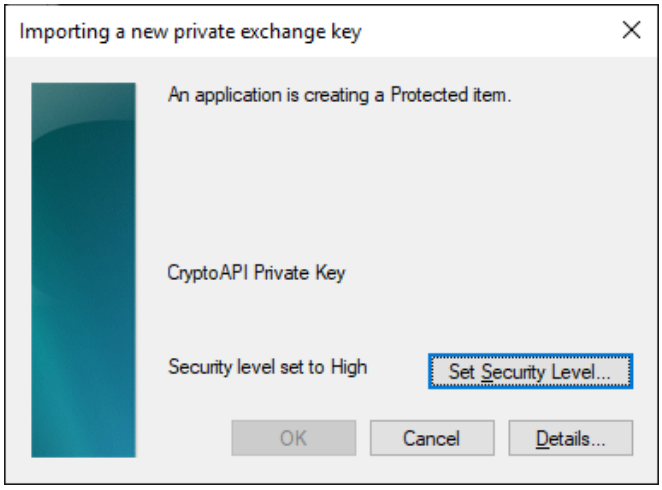
Note: ECC certificates (based on elliptic curve cryptography) are currently not supported by *u.trust LAN Crypt*.

2.1.1 Security levels

As *u.trust LAN Crypt* aims to provide the highest possible security, we recommend setting the security level on "*Enable strong private key protection*", when importing a certificate using the Certificate Import Wizard.



In the two following dialog boxes, click on **Next** and then on **Finish**. 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.

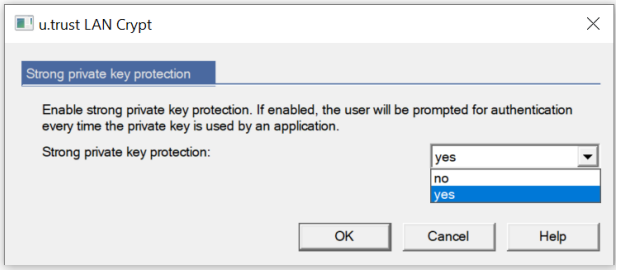
- **Medium**

  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**.

Every time the private key is used by an application, you will be prompted to **enter the password** (high security level) or to click **OK** (medium security level), depending on the security level setting.

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

u.trust 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 *u.trust LAN Crypt* Configuration to **yes**.

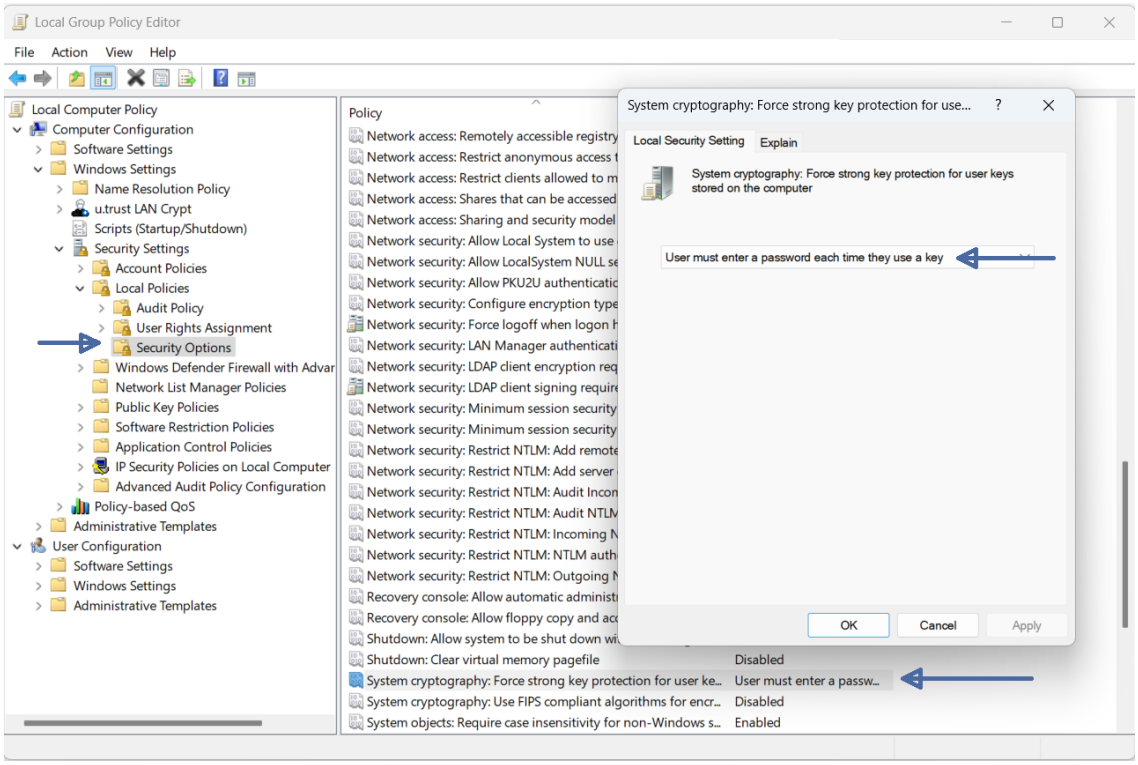


If this option is not activated, the security level “**low**” is automatically used for the imported certificates.

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: For a *u.trust LAN Crypt* user, using the *high security level* means that he has to enter the password for the private key once when logging in and whenever an encryption rule is loaded "manually".

In addition, activate the local Windows group policy "*System cryptography: Enforce strong key protection for user keys stored on the computer*" and select the option "*User must enter a password each time they use a key*". This will always set the security level to "high".



Smartcard:

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

Note: We recommend that you enable the option **Strong private key protection** before starting the *u.trust 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 *u.trust LAN Crypt*, and not, for example, imported from a smartcard.

Note: Windows caches PINs 24 hours by default. Using software certificates may cause security problems when you log on to *u.trust LAN Crypt* Administration and when additional authorization is provided. We strongly recommend that you deactivate this feature.

To do so, set these values:

```
"CachePrivateKeys"=dword:0x00000000
"PrivateKeyLifetimeSeconds"=dword:0x00000000
"PrivKeyCacheMaxItems"=dword:0x00000000
"PrivKeyCachePurgeIntervalSeconds"=dword:0x00000000
```

under the key:

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography
```

as well as the value:

```
"AllowCachePW"=dword:0x00000000
```

under the key:

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography\
Protect
```

If you do this, the PINs will not be cached.

Note: If you set "`CachePrivateKeys`" to "`1`" and "`PrivateKeyLifetimeSeconds`" to a value smaller than "`5`", this **may require a (Master) Security Officer to enter their PIN / Password twice** to access the private key, when the "*Strong private key protection*" setting is enabled.

Preconditions for using certificates with u.trust 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 *u.trust LAN Crypt*. *u.trust 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 *u.trust 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 *u.trust LAN Crypt*. The certificates then appear in the Certificates dialog immediately after *u.trust LAN Crypt* has been installed and can be used right away.

Note: *u.trust 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

u.trust 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 *u.trust 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 **C**ryptographic **S**ervice **P**roviders (CSPs) and **K**ey **S**torage **P**roviders (KSPs), smartcards are supported automatically when a smartcard KSP is used. You can therefore handle access to encryption information by using certificates on smartcards.

Note: If you want to use certificates on smartcards, please make sure that the smartcard reader, the associated middleware, and a corresponding **C**ryptographic **S**ervice **P**rovider (CSP) or **K**ey **S**torage **P**rovider (KSP) are correctly installed and operational!

Note: Please also note that **C**ryptographic **S**ervice **P**roviders (CSP) for key operations by *u.trust LAN Crypt* are now only supported in conjunction with Shims that make them accessible as **K**ey **S**torage **P**roviders (KSP).

2.2 Installation

The installation is typically carried out on one or more workstation computers with Windows 11 as the operating system. Installation on a Windows server system supported by *u.trust LAN Crypt* is also possible if central administration via Windows Terminal Services or Citrix MetaFrame is required.

Note: You can only install *u.trust LAN Crypt* if you have Windows Administrator privileges.

1. Go to the Install directory of your unzipped installation package and double-click on the *LCAdmin.msi* file.

   An installation wizard guides you as you install *u.trust LAN Crypt* Admin, 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 *u.trust LAN Crypt*! Click **Next**.

3. The *Destination Folder* dialog appears.

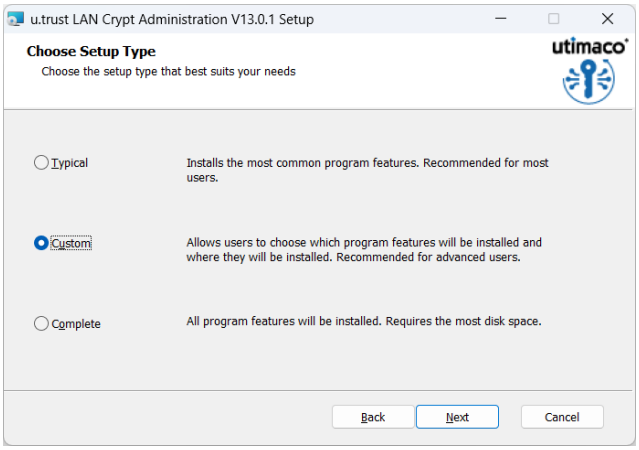
   Select where you want to install *u.trust LAN Crypt*. If you do not change this setting, the installation takes place under:

   ```
   <System Drive>:\Program Files (x86)\Utimaco\u.trust LAN Crypt\Administration\
   ```

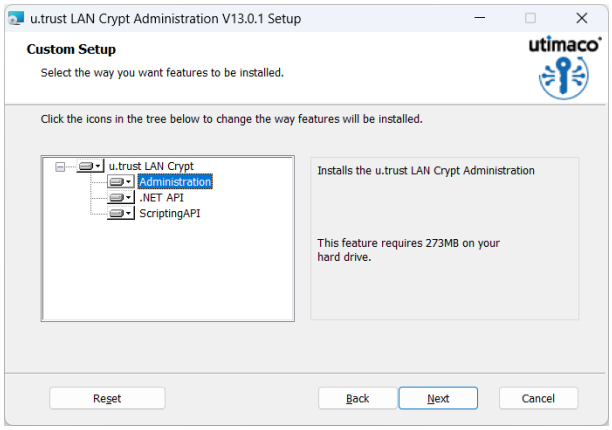
   Click **Next**.

4. The Select *Installation Type* dialog is displayed.

   In this dialog, you can select which *u.trust LAN Crypt* components are to be installed.



If you chose **Custom**, you could choose the components to be installed:



- **Administration**

  Installs the *u.trust LAN Crypt* Administration.

- **ScriptingAPI**

  Installs the *u.trust LAN Crypt* ScriptingAPI required for using scripts to administer the product.

  Note: Unlike in previous versions of *LAN Crypt*, the .NET API is now enabled by default instead of the ScriptingAPI during a custom installation.

- **.NET API**

  Installs the *u.trust LAN Crypt* .NET API required for using .NET based scripts or applications to administer the product. Additionally, sample scripts are also installed.

  Note: As of version 13.0.0, you can install the *u.trust LAN Crypt* .NET API without any additional program functions or components.

  Note: If you receive an error message when using the .NET API, please check if the following package reference is also included in your project:

  ```
  <PackageReference Include="Microsoft.Win32.Registry" Version="5.0.0" />
  ```

  Note: If the *u.trust LAN Crypt* Administration is not installed via the MSI package included in the installation folder, but via a separate installer, the registry key required for the *.NET API* must also be set.

  For the 32-bit .NET API, this must be set as follows:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\conpal\LAN Crypt\Admin\Setup]
  "InstallDir"="C:\\Program Files (x86)\\Utimaco\\u.trust LAN Crypt\\Administration\\"
  ```

  For the 64-bit .NET API, this must be set as follows:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\conpal\LAN Crypt\Admin\Setup]
  "InstallDir"="C:\\Program Files\\Utimaco\\u.trust LAN Crypt\\Administration\\"
  ```

Under "InstallDir" you must enter the path where the DLLs of the *u.trust LAN Crypt* Administration are located. By default, this is one of the paths mentioned above.

If you have **not** installed *u.trust LAN Crypt* in the default path, please note: If you want to use the supplied sample scripts, the paths to the *API DLLs* in the scripts must be adjusted analogously to the changed installation path.

Note: The .Net SDK is only required for using cs scripts / projects, not for Powershell scripts. The *StartFirstHere* sample program is predefined for *.NET Core 8.0* by default.

Please also note: If you want to use the **64-bit version of the .NET API**, a **64-bit ODBC connection to the *LAN Crypt* database** must be established or exist. All associated API library files (DLLs) must be located in the same directory as the application and must be found via the "PATH" environment variable.

This applies to the following files:

- *LCAdminApiNetX64.dll*
- *LCNetApiX64.dll*
- *SGLCScriptApiV4.dll*
- *sglcapi.dll*
- *LCDA.dll*

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

   Note: If you have selected the **Typical** option, only the administration will be installed; if you select **Complete**, the *u.trust LAN Crypt* **ScriptingAPI** and **.NET API** will also be installed.

6. After having checked your settings, click **Install** 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.

2.3 Unattended installation

Unattended installation means you can install *u.trust LAN Crypt* automatically on a large number of computers.

The Install folder contains the LCAdmin.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 indicate how the individual components must be specified under `AddLocal=` if an installation is performed without user interaction. The names of the individual keywords for the components are case-sensitive!

`AddLocal=`**`Administration`**

Installs only the *u.trust LAN Crypt* Administration.

`AddLocal=`**`Administration,ScriptApi`**

In addition to the *u.trust LAN Crypt* Administration the ScriptingAPI will also be installed.

`AddLocal=`**`Aministration,AdminApiDotnet`**

In addition to the *u.trust LAN Crypt* Administration the AdminApi (.NET) will also be installed.

Example:

```
msiexec /i lcadmin.msi /qn AddLocal=Administration
```

In the example only the *u.trust LAN Crypt* Administration will be installed without user interaction.

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

Note: Installing the *.NET API* (*AdminApiDotnet*) also installs sample scripts. By default, the installation is done for 64-bit version under:

```
<Drive>:\Program Files\Utimaco\u.trust LAN Crypt\Administration\Admin API PowerShell Samples\
<Drive>:\Program Files\Utimaco\u.trust LAN Crypt\Administration\Admin API Dotnet Samples\
```

and for 32-bit version under:

```
<Drive>:\Program Files (x86)\Utimaco\u.trust LAN Crypt\Administration\Admin API PowerShell Samples\
<Drive>:\Program Files (x86)\Utimaco\u.trust LAN Crypt\Administration\Admin API Dotnet Samples\
```

Note: See also the further notes for the *.NET API* on page 24.

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.

`/QN`

Installation without user interaction (unattended setup).

Name of the *.msi file: *lcadmin.msi*

Syntax: `msiexec /i <path>\lcadmin.msi /qn`

Optional Parameters:

`/L*xv <path + filename>`

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

Example:

```
msiexec /i C:\Install\lcadmin.msi /qn /L*xv c:\Log\log.txt
```

This carries out a complete installation of *u.trust LAN Crypt*. The program is installed in the default installation directory

(<System drive>:\Program Files (x86)\Utimaco\u.trust LAN Crypt\Administration).

The .msi file is located in the *Install* folder of *u.trust LAN Crypt* installation package.

2.4 Upgrading

For upgrading *LAN Crypt* version 4.2.0 to this version of *u.trust LAN Crypt* Administration, you must first perform an intermediate upgrade to *u.trust LAN Crypt* version 11.0.x (this includes the installation itself and the upgrade of the *LAN Crypt* database). Then install the current *u.trust LAN Crypt* Administration version 13.0.1 and update the existing *LAN Crypt* database using the command line tool `CreateTables.exe`. The steps required for this are described in more detail on the following pages.

Note: If you are using a *LAN Crypt* version older than version 3.90, you must first upgrade to *LAN Crypt* version 3.97 and then to *LAN Crypt* version 4.2.0.

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

2.4.1 Upgrade to the new version

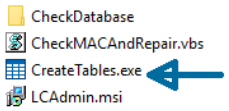
Install the new version as described.

Note: Make sure that all instances of *LAN Crypt* Administration are closed before you install the new version. No other (Master) Security Officers may be connected to the *LAN Crypt* database during the upgrade, as this can lead to inconsistencies in the database!

Note: Please note that **after upgrading *LAN Crypt* Administration to version 13.0.0 or later, mixed operation with previous *LAN Crypt* versions is no longer possible!** All additional *LAN Crypt* administrations must be updated at the same time. **Access to a previous *LAN Crypt* database is not possible with version 13.0.x.** A previous database must first be migrated to the new version before it can be accessed again with LAN Crypt Administration.

2.4.2 Upgrading the existing u.trust LAN Crypt database structure

Using the command line tool `CreateTables.exe` you can upgrade the structure of the tables in your *u.trust LAN Crypt* database. The tool is available in the \Install folder of your installation package.



Note: Before upgrading, create a backup of your *LAN Crypt* database.

For the upgrade of an existing *u.trust LAN Crypt* database structure, Utimaco recommends having this done by the **IT Administration** or a **Database Administrator**, as this requires advanced database permissions (db role: `db_ddladmin`). During the database upgrade by `CreateTables.exe` new tables must be created in the *u.trust LAN Crypt* database and among others DDL triggers must be removed.

Note: Logon to the database must be performed with privileges that *allow creation* and *modification* of the database schema. However, the database roles "`db_datareader`" and "`db_datawriter`" are fully sufficient for Security Officers to use the *u.trust LAN Crypt* Admin Console.

Note: Please note that when updating a *LAN Crypt* database using the `CreateTables.exe` command-line tool on Oracle-managed SQL databases, the *ADMLOGINVIEW*, *USERGROUPVIEW*, *GROUPRULEVIEW*, and *ADMINLISTVIEW* views are deleted and recreated. Database users who connect to the *LAN Crypt* database via ODBC may lose the SELECT privileges for these views. These SELECT privileges must then be reassigned for these users by database owner or database administrator (DBA).

Note: When replicating the *LAN Crypt* database in an Oracle environment, the administrator must ensure that **no triggers** are executed in the target database. A suitable approach is to perform the database replication using *Oracle GoldenGate* and configure the *DBOPTIONS*

parameter with the *SUPPRESSTRIGGERS* flag (this is the default setting). Further information on this topic can be found at:
https://docs.oracle.com/en/middleware/goldengate/core/21.3/reference/dboptions.html#GUID-BA8C0CED-D87F-4106-862E-4AD22D910160

Command line syntex:

```
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 must be specified for Oracle databases. The owner must be specified in CAPITALS. If the default schema of your Microsoft SQL Server does not correspond to "*.dbo"*, you must specify the database owner "*.dbo*" for Microsoft SQL databases.

SQL dialect:

m ... Microsoft SQL Server 2022 or 2025 (incl. Express)

o19 ... Oracle 19 or later

Actions:

u ... Update of the database structure

Example 1:

```
CreateTables SGLCSQLServer.dbo m u
```

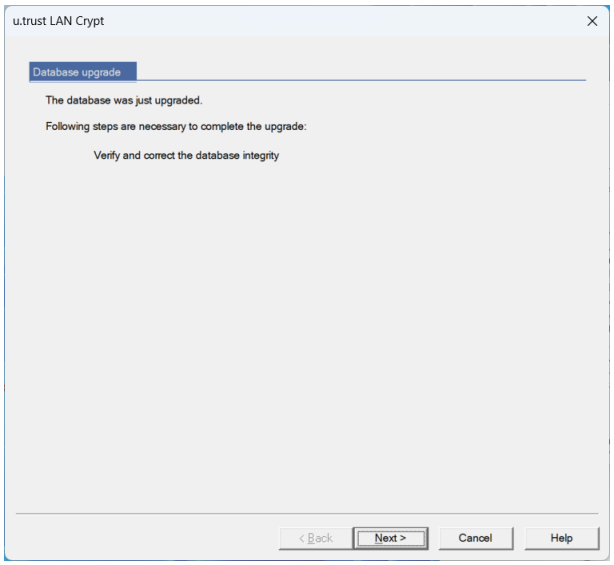
Example 2:

```
CreateTables SGLCSQLServer.SGLC o19 u
```

Note: Please also note that other parameters may need to be set for *CreateTables.exe* if you are installing *u.trust LAN Crypt* Admin for the first time. Further information on this can be found in section 3.2.3 "*Creating tables in the u.trust LAN Crypt database*" on page 100.

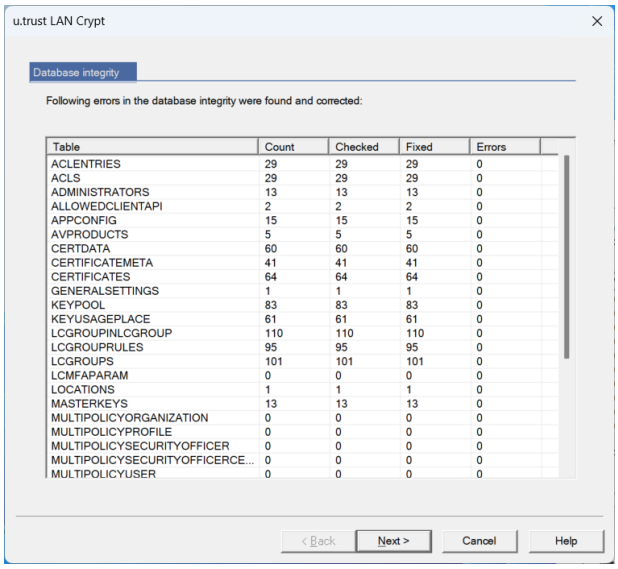
2.4.3 Upgrade Wizard

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.

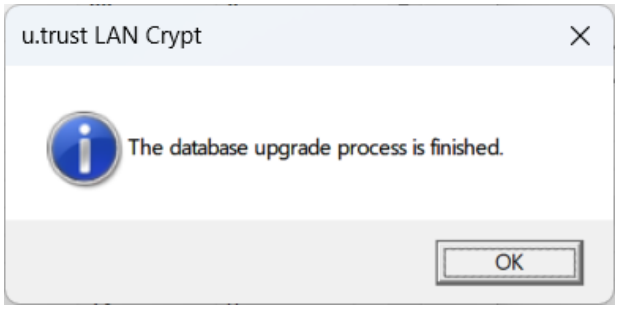


Note: Only a Master Security Officer is authorized to log in to *u.trust LAN Crypt* Administration for the first time after an upgrade. If you do not have the required rights, a corresponding message will be displayed. The steps required to complete the upgrade may vary depending on the version being upgraded from.

The Upgrade Wizard checks the integrity of the *LAN Crypt* database and performs any necessary troubleshooting. It then displays information about any corrected errors and recommends any further actions.

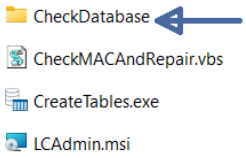


After you complete the wizard administration is ready to use.



2.4.4 Checking and repairing the database

Using the command line tool `CheckDatabase.exe`, you can check the integrity of the *u.trust LAN Crypt* database at any time and if necessary, fix errors. You can find this tool in the *\Install folder* of your *u.trust LAN Crypt* installation package.



Note: A detailed description of the command line tool *CheckDatabase.exe* can be found at: https://help.lancrypt.com/docs/admin/additional-documentation/CheckDatabaseTool/en/

2.5 Language settings

u.trust LAN Crypt Administration supports the following languages:

- English
- French
- German
- Japanese

The language setting of *u.trust LAN Crypt* depends on the current language setting of Windows. If languages are not supported, *u.trust LAN Crypt* displays the dialogs in English by default.

Alternatively, you can set the language for *u.trust LAN Crypt* yourself. To do this, make the following changes in the registry of the computer on which *u.trust LAN Crypt* Administration is installed:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Utimaco\SGLANG]
"LCID"=dword:0x0409
```

for US English language

```
"LCID"=dword:0x40C
```

for French language

```
"LCID"=dword:0x0407
```

for German language

```
"LCID"=dword:0x0411
```

for Japanese Language

Then restart the computer.

The manually set language for *u.trust LAN Crypt* is retained, even if a different language is set or changed in Windows.

2.6 Uninstallation

Note: You can only uninstall *u.trust LAN Crypt* if you have Windows Administrator privileges.

1. Select **Start**, **Settings**, **Apps**.
2. Select **u.trust LAN Crypt Administration** from the list of installed programs.
3. Click **Uninstall** to uninstall the *u.trust LAN Crypt* Administration.
4. If you really want to uninstall the *u.trust LAN Crypt* Administration, confirm the warning message displayed by clicking **OK**.
5. **Restart** the system to complete the uninstallation process.

Note: When uninstalling *u.trust LAN Crypt* the contents of the *u.trust LAN Crypt* Database is preserved. If required, the database must be deleted separately by using operating system tools or the database administration tool. Also, all user specific settings remain on the system (registry keys, group policy settings and so on).

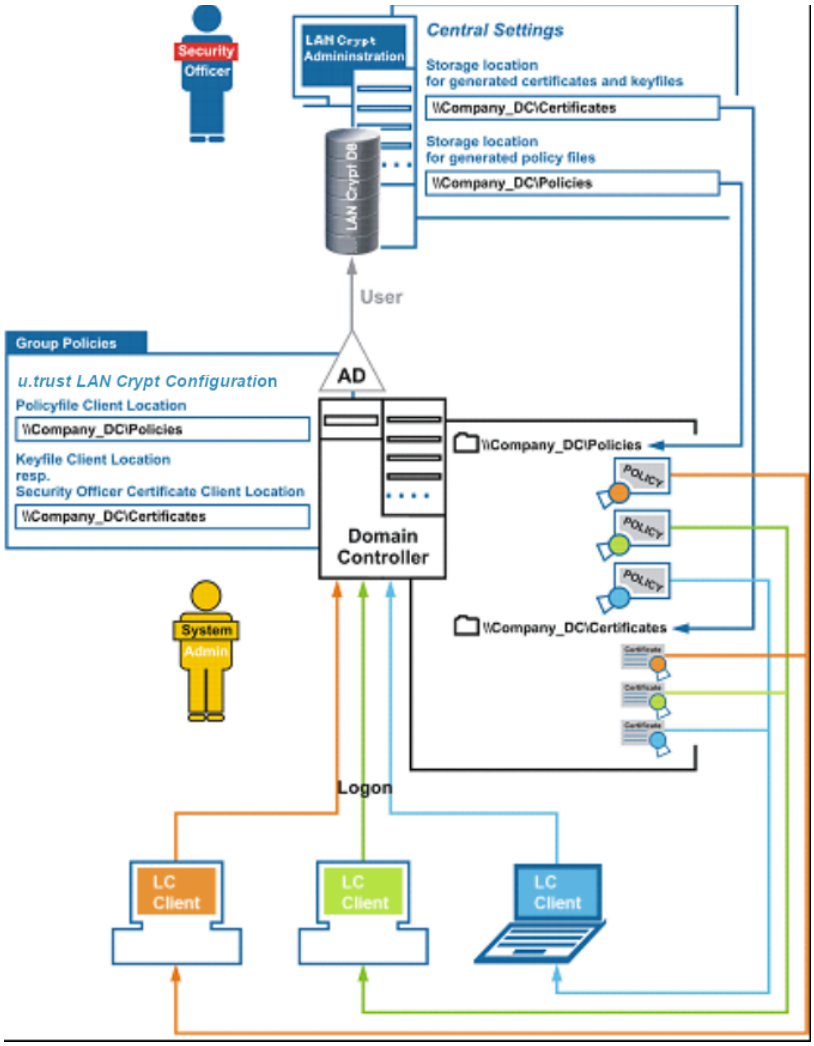
3 Administration

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

u.trust 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 must 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 *u.trust LAN Crypt* Configuration Console. *u.trust LAN Crypt* is configured in the group policy object that is valid for the users.

u.trust LAN Crypt clients do not need to connect to the *u.trust 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 *u.trust LAN Crypt*, the *p12pwlog.csv* file contains the passwords and can be used, for example, to create a PIN letter (e.g. using the “*LCSendP12Password*” tool).

3.1 Required steps

Preparations:

- Optional: Installation of the DBMS (Microsoft or Oracle). Creation of a new database "*LANCRYPT*". The databases prepended in the DBMS should not be used for *u.trust LAN Crypt*!
- Add data source (32-bit ODBC) as system DSN (see chapter 3.2.2).
- Create database tables with `CreateTables` (or extend them during an upgrade).
- **System Administrator**: Define settings in the *u.trust LAN Crypt* configuration console.
- Create initial Master Security Officer.
- Define the storage locations in the Admin Console:
  - for User key files and Security Officer certificates generated by *u.trust LAN Crypt*
  - for Security Officer key files generated by *u.trust LAN Crypt*
  - for the password log file of the automatically generated passwords of the key files (only if the certificates are generated by *u.trust LAN Crypt*)
  - for policy files generated by *u.trust LAN Crypt* (please contact the windows System Administrator to implement these steps)

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 76).

- Create additional (Master) Security Officers
- Define rights for Security Officers
- Import objects (Organizational Units, groups, users) from the directory service (e.g. Active Directory)
- Create *u.trust LAN Crypt* groups and fill them with the objects imported from the directory service (users, groups)
- Assign the *u.trust LAN Crypt* groups and the responsible Security Officer to the individual organizational units or regions, as well as define their rights
- Create keys
- Create encryption rules

  Note: We recommend defining encryption rules only in *u.trust LAN Crypt* groups. Encryption rules in directly imported directory objects represent a security risk and are also prone to errors.
- Generate and assign certificates for the users
- Generate policy files for the users.

3.2 Preparations for administering u.trust LAN Crypt

After installation, you must work through the following steps before you can start administering *u.trust 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 *u.trust LAN Crypt*.

u.trust LAN Crypt supports the following database systems:

- Microsoft SQL Server 2022 or 2025 (incl. Express)
- Oracle 19 or later

  Note: If you are using an Oracle database, you must install the Oracle client before you can use *u.trust LAN Crypt* Administration. If you select the “runtime” variant of the Oracle client, you must also install the Oracle ODBC driver.

  ***u.trust 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 must create the *u.trust LAN Crypt* tables in the database using the tool provided with your software (`CreateTables.exe`).

3.2.1 Installing the database system

The following description refers to the Microsoft SQL Server 2022 Express Edition. For this exemplary description, the default settings of this version have been used as much as possible.

To install the database system, do as follows:

1. Download a current version of Microsoft SQL Server Express (for example, Microsoft SQL Server 2022 Express) from the Microsoft Web site. Then double-click the installation file in the download folder.

   For Microsoft SQL Server 2022 Express, this is SQL2022-SSEI-Expr.exe.

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 the default settings.

Default settings: The following description of preparatory steps refers to the default settings. 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 *u.trust LAN Crypt* and specify it when adding the data source. For the Microsoft SQL Server 2022 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 username for authentication. To see all parameters, type `osql -?`.

You can also use another version of Microsoft SQL Server Express (*u.trust LAN Crypt* Version 13.0.1 supports Microsoft SQL Server Express from version 2022).

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

In the next step, a data source must be specified so that *u.trust LAN Crypt* can use the database system.

3.2.2 Adding a data source (ODBC)

Note: The data source must be added with the 32-bit ODBC Data Source Administrator, which is also available on 64-bit systems. Start the ODBC Data Source Administrator by clicking *Start\u.trust LAN Crypt Administration\ODBC Data Source Administration (x86)*. This ensures that the correct version is launched.

Specify a data source so that *u.trust 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. To secure the connection between the *u.trust LAN Crypt* Administration and the SQL Server, we recommend using "*ODBC Driver 17 for SQL-Server*" or a newer version. This driver enables connection encryption with TLS 1.2 and thus offers increased security. A download is possible via: https://go.microsoft.com/fwlink/?linkid=2120137

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 *u.trust 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 *u.trust LAN Crypt* Configuration. You must enter the names in the configuration before running the *u.trust 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**.

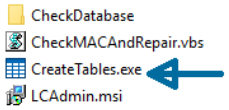
7. Choose as default database the database (e.g. *LANCrypt*) that you have created for *u.trust LAN Crypt* and confirm it.

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

3.2.3 Creating tables in the u.trust LAN Crypt database

Using the command line tool `CreateTables.exe` you create the required tables in your *u.trust 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 tables in your database, do as follows:

If you are using a Microsoft SQL Server, enter the following in the command line:

```
CreateTables SGLCSQLServer.dbo m c
```

If you have used the defaults during installation, configuration of the database system is now complete. You can now start *u.trust 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:

ODBC Name:

The name you used for the ODBC data source.

Owner Name

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. If the default schema of your Microsoft SQL Server does not correspond to "*.dbo"*, you must specify the database owner "*.dbo*" for Microsoft SQL databases.

SQL Dialect:

m ... Microsoft SQL Server 2022 or 2025 (incl. Express)

o19 ... Oracle 19 or later

Actions:

c ... Create all tables

Example 1:

```
CreateTables SGLCSQLServer.dbo m c
```

Example 2:

```
CreateTables SGLCSQLServer.SGLC o19 c
```

3.3 Master Security Officers

u.trust 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 *u.trust 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 *u.trust 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 permissions.

Note: When creating the initial Master Security Officer, you must also define the storage location for the certificates and key files generated by *u.trust LAN Crypt*. The public part of the Security Officer's certificate (*.cer), which is needed by the clients, is also stored there. User certificates (*.p12 files) are also imported from this directory later on. The folder 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 *u.trust LAN Crypt* Administration Console.

3.3.1 Initial Master Security Officer

After the Administration function runs for the first time (*Start, u.trust LAN Crypt Administration, Administration*), and you log on to the database, you see the wizard for creating the initial Master Security Officer.

Enter the data for the initial Master Security Officer. The name you enter here is used as a Common Name in the certificate if you use certificates generated by *u.trust LAN Crypt*. *Email Address* and *Comments* are optional. Click **Next**.

Note: The email address is added to the *password log file* for certificates generated by *u.trust LAN Crypt*. It can, for example, be used to create a PIN letter via email (e.g. using the "*LCSendP12Password*" tool).

In the Wizard's second dialog, specify the storage locations for

- generated certificates (*.cer) and key files (*.p12)
- generated Security Officer certificates and
- the log file for the automatically generated passwords of generated key files.

Storage location for generated certificates and key files

u.trust LAN Crypt can generate self-signed certificates if required. The key files (*.p12) generated for the users in this way contain the private keys as well as the certificates. These are generated when assigning the certificates for the users. The associated storage location must be specified in the second dialog of the assistant. Generally, this is a network share that these files are made available to users.

The public part of the Security Officer certificate (*.cer) is also saved here.

Users must be provided their key files or certificates (*.p12), policy files, and the public portion of the certificate (*.cer file) of the security officer who created and signed the policy files.

This is done for the *u.trust LAN Crypt* Client configuration using group policies or registry settings (if no Active Directory is available or should not be used for security reasons). With these settings the client gets the appropriate access paths. We recommend the use of UNC paths and FQDN names.

If a corresponding "*.cer" file is found that contains the public key of the Security Officer certificate, it is automatically imported.

Note: To use the described functionality, the corresponding paths must be set in the *u.trust LAN Crypt* configuration.

Alternatively, the users' key files and the public part of the Security Officer certificate can be distributed manually. In this case make sure that both are imported by the clients.

Note: The public certificate of the security officer who created the policy files must always be imported by the clients.

If you change the path on which the public certificates (*.cer) of the Security Officers and the key files (*.p12) of the users are stored, e. g. after you have created additional Security Officers, you must copy these files to the new location. Otherwise, the public part of the Security Officers' certificates will not be found by the *u.trust LAN Crypt* clients. The key files for users must also be generated under the new path.

Storage location for generated Security Officer certificates

u.trust 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!

File for password log

The storage location and name for the password log file of the generated PKCS#12 files can be specified here (default name: *p12pwlog.csv*). This file contains the passwords of the generated PKCS#12 key files (*.p12). This can e.g., also be used to create a PIN letter.

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

With *u.trust LAN Crypt* you can easily protect the password log file. To do so, install the Administration and Client on the same computer. After creating the initial Master Security Officer, create an encryption rule that encrypts the password log file, generate a profile for the initial Master Security Officer, and load the profile. The encryption key used should only be available to Master Security Officers and Security Officers that have the right to create certificates.

Note: If you install both *u.trust LAN Crypt* components, *Admin Console* and *Client application* on the same computer, they must be of the same version.

Running the initial encryption wizard will encrypt the password log file. To ensure that the password for the initial Master Security Officer was not compromised while the file was not encrypted, create a new certificate, and assign it to the initial Master Security Officer.

Note: If the Security Officer who is assigning certificates has no file system right to change the password log file, *u.trust LAN Crypt* will not be able to generate certificates.

Click **Next**.

Certificate validity

In the Wizard's third dialog, specify the period of validity for the certificates generated by *u.trust LAN Crypt* and assign an existing certificate, or one generated by *u.trust LAN Crypt*, to the Security Officer.

If you use a certificate generated by *u.trust LAN Crypt*, it is valid for the specified period. All certificates generated after this one also has this period of validity.

The initial Security Officer's certificate

You must select an encryption certificate that will be used to secure the Security Officer's data. Alternatively, you can also select a signature certificate that the Security Officer can use to authenticate themselves to *u.trust LAN Crypt* Administration. If you do not specify a signature certificate, the encryption certificate will also be used as a means of authentication.

Click the **Browse...** button to select an existing certificate or to have *u.trust LAN Crypt* generate a new one. In the next dialog, click **New Certificate**. Select the new certificate from the list and click **OK**.

Note: If you want to use an existing certificate, this certificate must be available. If you are using a software certificate, it must be loaded into the certificate store. If the certificate is saved on a token, the token must be attached to the system. To import a certificate, click **Import Certificate**.

Click **Next**.

In the wizard's fourth dialog you can enter a region with the appropriate prefix. When *u.trust LAN Crypt* generates the key, it attaches this prefix at the beginning of the key name. It always uses the prefix of the region assigned to the Security Officer who generated the key. This prefix makes it clear which administrative unit the key is to be used for. In the **Central Settings** for the Administration Console, you can create additional regions and then assign them to the different Security Officers. This procedure is particularly useful in distributed environments.

You must specify a location. In distributed databases the location is used to clearly assign logged events within *u.trust LAN Crypt* database logging.

You must specify the location even if you are not using a distributed database. This ensures that the entries can be clearly assigned when the database is distributed at a later point in time.

When you click **Finish** *u.trust LAN Crypt* creates the Initial Master Security Officer and displays the logon dialog for *u.trust LAN Crypt* Administration.

Later, all Security Officers that have the right to log on to the *u.trust LAN Crypt* Administration database will be displayed in this dialog.

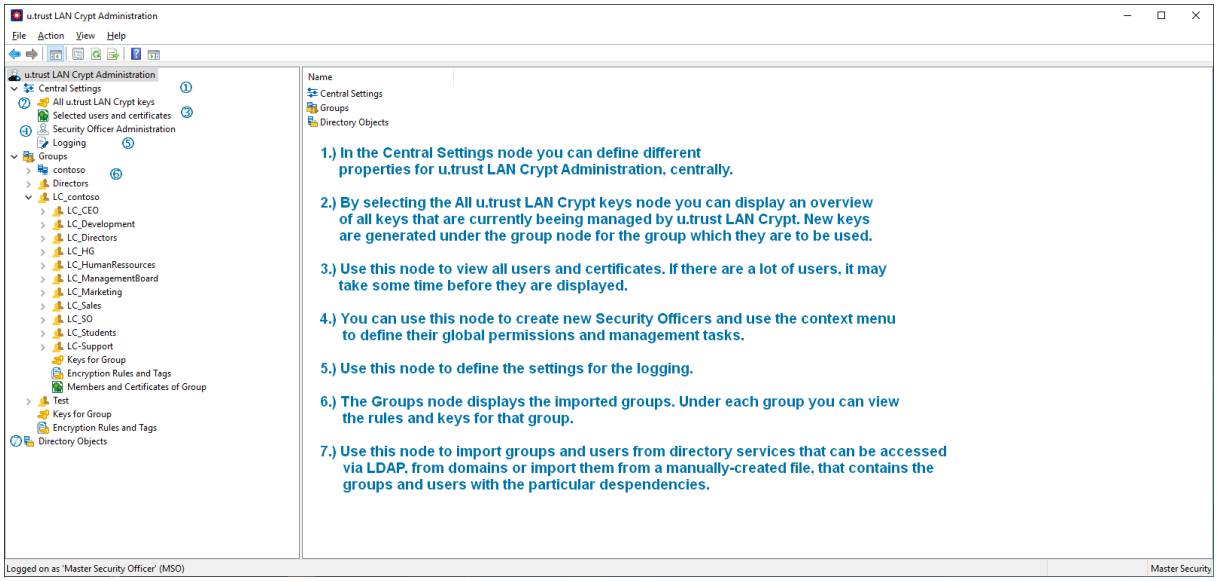
In this dialog, select the newly created Master Security Officer and click **OK**. *u.trust LAN Crypt* Administration Console opens.

Note: After you log on, a dialog appears to tell you that a recovery Key has not yet been generated. If you do not have a recovery key, there is the risk that all your administrative data and all encrypted data will be lost in case of an emergency (for example if you lose a certificate).

This dialog appears every time a Master Security Officer logs on until a recovery key has been generated. If you activate the **Don't warn me again** option, you can prevent this dialog from appearing even if no recovery key has been generated. **To avoid possible data loss, you should generate a recovery key.**

3.4 Administration: overview

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



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

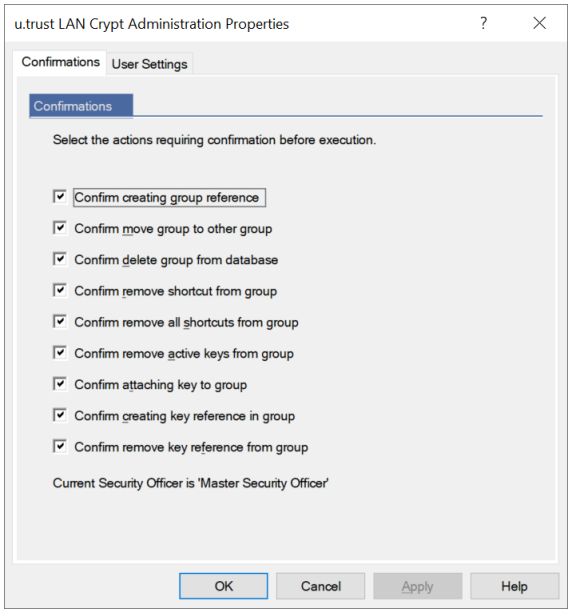
You can also select all the functions that appear as these icons from the relevant context menu.

Right-click the **u.trust 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 *u.trust 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 **u.trust LAN Crypt Administration** root node.

The following dialog displays these actions:



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.

You can make this setting for the following actions:

- **Confirm creating group reference**

  Creating a reference to an existing group has to be confirmed. Select group > right mouse button > copy > select other group > right 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 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 active 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 group**

  Keys which were used in an encryption rule and have been removed from all groups reside in the database and are displayed under the node **Central Settings** / **All 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.

3.4.2 User settings

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

Activate

- *Add domain name to each group name*, to display the relationship between *u.trust LAN Crypt* groups and domains in *u.trust LAN Crypt* Administration. This option is especially useful if *u.trust 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 *u.trust LAN Crypt* under the **Central Settings** node.

  Note: You should be aware that it will take several minutes to display all the users and certificates in larger installations. You must then restart *u.trust LAN Crypt* Administration so that the changes you made in the Show *Selected users and certificates* option become effective.

  Note: Please also note that when upgrading the *u.trust LAN Crypt* Administration, the "*Show selected users and certificates*" option may need to be reactivated.

- 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 *u.trust LAN Crypt* database contains any users that are not assigned to any group. You must then restart *u.trust 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, *u.trust 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 *u.trust 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** node, you can define different properties for *u.trust 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 *u.trust LAN Crypt* 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 permission *Change Configuration*. The global permission *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 Algorithm tab

u.trust LAN Crypt has these encryption algorithms:

- **AES-128**
- **AES-256**
- **3DES** (not recommended)
- **DES** (not recommended)
- **IDEA** (not recommended)
- **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 3DES 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. If you select algorithms that are no longer considered secure, you will receive a corresponding security notice. You can still choose these algorithms.

Default algorithm

Here you select which default algorithm is to be used to automatically generate user and group keys. **AES** with either **256** or alternatively **128-bit key length** is recommended as the standard algorithm because it offers the highest security.

3.5.2 The Keys tab

Problems with duplicated internal key names may occur when several *u.trust 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 *u.trust LAN Crypt* and cannot be changed afterwards.

However, if files that have been encrypted with *u.trust 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 affects the GUID of the key and the encryption algorithm.

To handle this situation *u.trust 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.

Note: Further ways to share keys are also available via *Lc2Go* (see Section 3.15.1 “*Lc2Go Key Import*“ on page 129) or via the *u.trust LAN Crypt API* using the new *multi-policy support* feature.

Note: This setting can only be changed by a Master Security Officer.

Key value

By activating the option **Only Security Officers with the Generate profile right can generate keys (keys without a value are not permitted)** you can ensure that only Security Officers who have the global permissions *Create Keys* and *Create Profiles* can generate keys (name and value). If the Security Officer does not assign a value to the key when creating it, the value will be generated automatically when the key is saved.

If this option is active (the default setting for a new installation), Security Officers who do not have the global *Create Profiles* permission cannot generate keys.

The use of group keys (<GROUPKEY>) in encryption rules also is not possible for these security officers.

Note: If a Security Officer should only generate keys, but no profiles, you can configure this in the permissions of the respective groups (see Chapter 3.11.3 ”*Granting the Security Officer permissions to process the groups*“ on page 116.

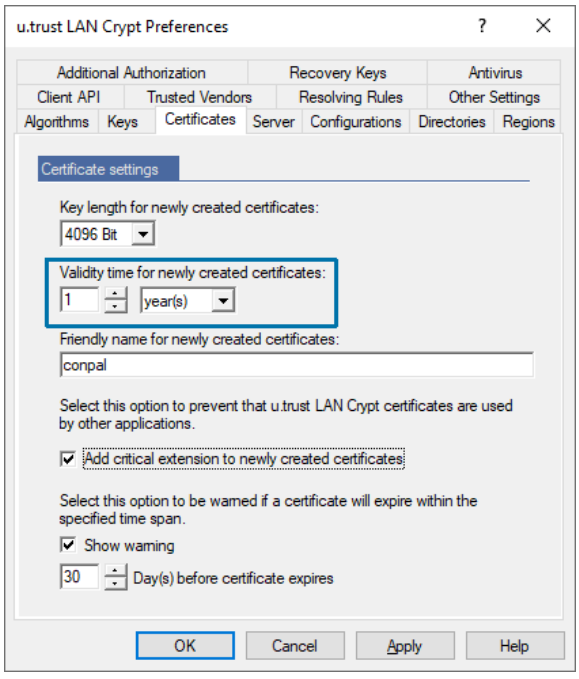
For group keys, whose values are generated when policy files are generated, the values are also generated immediately when they are used to create an encryption rule.

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

Note: In principle, *u.trust LAN Crypt* also offers the option of creating keys without a value. Such keys can be used in the administration without restrictions. However, this can cause problems with distributed databases. An example of the use of a reference to a key would be if policy files are generated in a replication time window at different locations that contain keys without a value (manually created keys without a value, group key <GROUPKEY>). When generating the policy files, a separate value for the key would consequently be generated at each location. The result would be a key with two different values.

3.5.3 The Certificates tab

Here you can specify key length (1024, 2048, 4096 Bit) and validity for new certificates generated by *u.trust LAN Crypt*. A validity time of 1 year for newly created certificates is predefined. You can change this value at any time.



Note: You can set the validity time for newly created certificates between *1 day* and a maximum of 999 years. In terms of information security, however, the validity time should not exceed a period of 5 years if possible. For CA certificates (**C**ertificate **A**uthority), Utimaco recommends a maximum validity time of 20 years.

Note: For certificates assigned to (Master) Security Officers, the validity period **must not extend beyond the year 3100**.

Under *Friendly name for newly created certificates,* you can specify a name for certificates created by *u.trust LAN Crypt*. All certificates get this name and can therefore easily be identified as u.trust 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). For example, if you enter 30 days here, a warning message is displayed approximately one month before the certificate expires that the certificate will soon no longer be valid and must be renewed.

3.5.4 The Resolving Rules tab

Skip users that have no valid certificate when resolving

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 sort methods. *Sort method 3* is the default method which is used by Client versions below 3.90. The sort method could not be changed in LAN Crypt in previous versions and corresponded to sort method 3.

Sort method 3 is therefore considered the default sort method. The following sort methods can be set:

- **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>:\

  Examples of how to use a reference to a key:

  `\\server\share\*.*` or

  `c:\confidential\*.*`

- **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

  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 u.trust LAN Crypt Client

Here you can configure which file encryption mode is used by the clients. *u.trust 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.

- CBC-uIV format (versions 13.0.0 or higher)

  This format can be used by *LAN Crypt* clients from version 13.0.0 or higher. These clients can read files that are encrypted in OFB, CBC and XTS-AES mode. The CBC-uIV encryption mode is used for new files. To increase the security of CBC, a random and therefore unpredictable initialization vector is used in uIV format (**u**npredictable **I**nitialization **V**ector).

Note: You can use the command line tool `encstatus.exe` to check which files are already encrypted with the new *CBC-uIV* format. You will find the command line tool in the installation folder of your extracted *u.trust LAN Crypt* Admin installation package.

You can use `encstatus.exe` to check the encryption mode via the command line as follows:

Example: If you want to check whether and which files in the ”`HR`“ folder on the local drive “`C:`“ are already encrypted with the new *CBC-uIV* format, open the command line on your computer, change to the folder where the command line tool `encstatus.exe` is located, and enter the following command:

```
ENCSTATUS C:\HR /CNM /DCP /XM CBC-uIV /XM CBC /F /S
```

Note: You can find a description of the respective parameters of encstatus.exe by entering `encstatus -h` on the command line.

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 3.50 or higher.
- **XTS-AES format (versions 3.90 or higher)** is only available if CBC-uIV is configured as the encryption format. XTS-AES requires a client version 3.90 or higher. This mode is only used for AES keys.

  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 *u.trust LAN Crypt* encryption format is used.

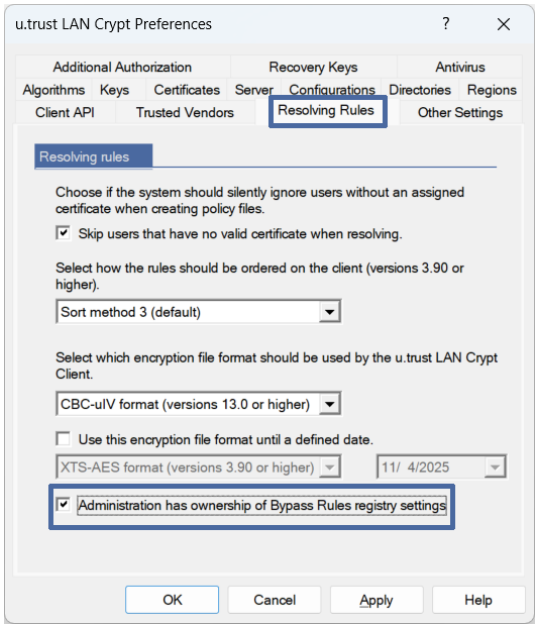
  This change becomes effective the next time the encryption rules are resolved.

  Note: Starting with version 4.0.0, *LAN Crypt* no longer supports writing to files encrypted using the outdated OFB encryption mode. Such files can still be read, but writing is only possible using the newer selected encryption mode. Utimaco strongly recommends re-encrypting all files that are still encrypted with the obsolete OFB encryption mode to (AES) XTS using the Initial Encryption.

  Note: Please be aware that older versions of the *LAN Crypt* Client do not support the CBC-uIV mode. **Before encrypting files to the new CBC-uIV format, it is essential to update all older *LAN Crypt* Clients to the latest version**. The current *LAN Crypt* versions for macOS, iOS, and Android also support the new CBC-uIV format.

Administration has ownership of Bypass Rules registry settings

Bypass Rules are used to disable essential *u.trust LAN Crypt* functions in special scenarios. **Enabling this bypass function affects all clients**. The bypass function is only available for rules via the u.trust *LAN Crypt* Administration if the **Administration is owner for Bypass Rules in the registry** option is enabled (see "*Bypass*" on page 146).



WARNING: Please note that extreme caution is required here! Incorrect settings could, among other things, lead to files being damaged (corrupted). Therefore, the implementation of such rules is critical and should only be done in coordination with Utimaco support.

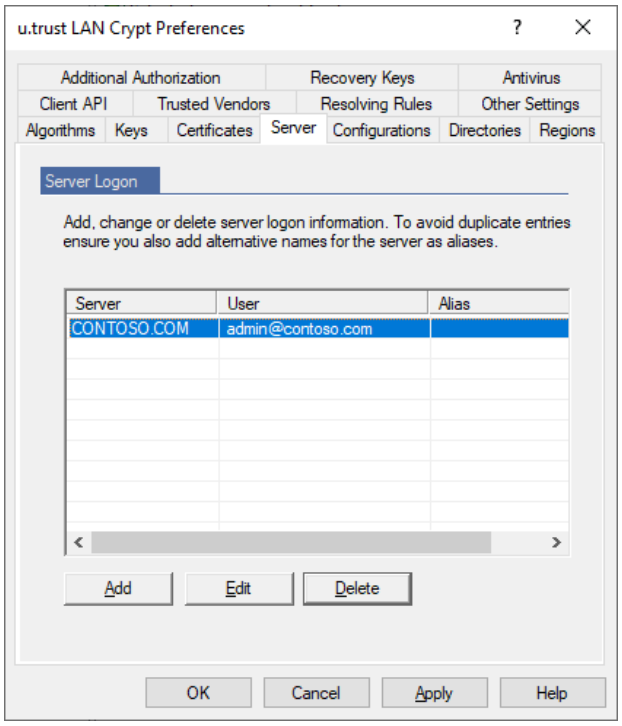
Note: This setting can only be changed by a Master Security Officer.

Note: If **Bypass Rules** were already set by other means via group policy or registry, this new feature would overwrite or delete them.

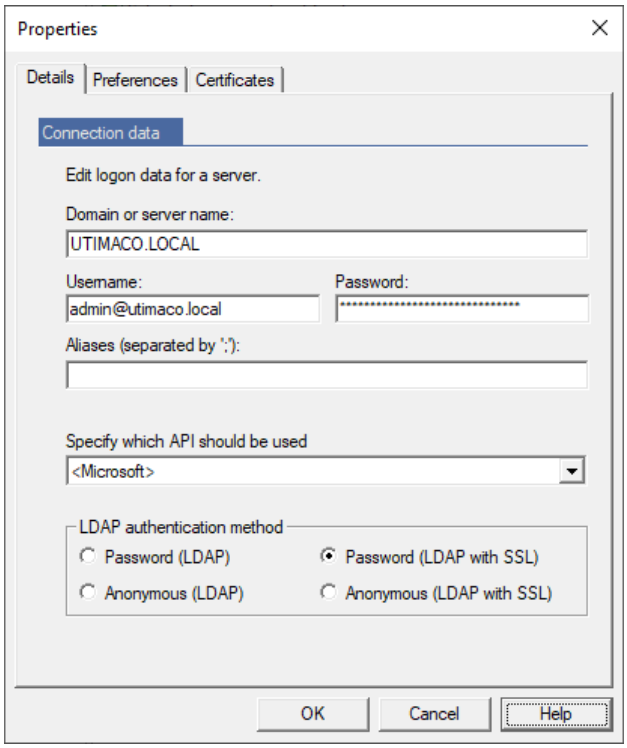
Note: Disabling this feature can only be done after all **Bypass Rules** have been deleted from the configuration to avoid conflicts with other rules.

3.5.5 The Server tab

To import groups and users from a server, *u.trust 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*.



Server details: Password logon

1. Enter the *Domain* or *server name*, *Username,* 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.

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

   - Enter the domain name under *Domain or server name*.
   - Enter the *Username* as username@domain.

     Note: The username must be entered in LDAP syntax (canonical name) to import objects from a non-Microsoft directory service. Example: cn=admin,ou=techops

2. Specify the API to be used.

   Select *<Microsoft>* or *<Novell>* from the drop-down list. The placeholder *<Novell>* stands for all non-Microsoft APIs.

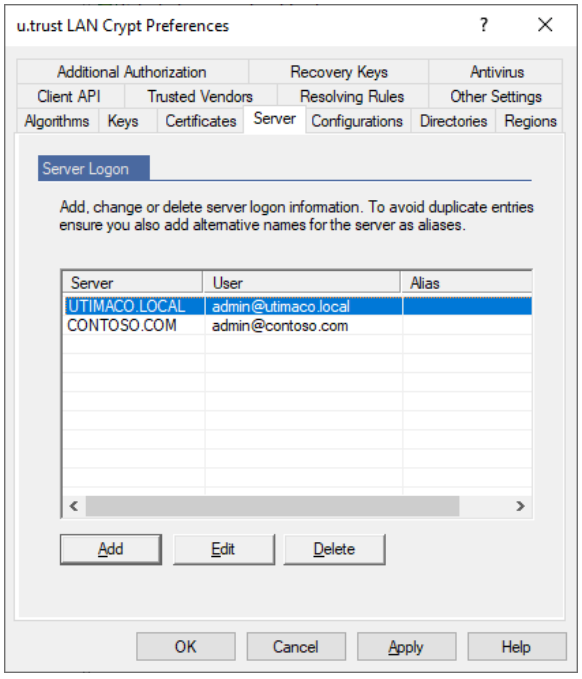
   Note: Import from a Novell Directory service has not been supported since LAN Crypt version 3.90. Other Novell functionalities are now as well not supported and will not be functional in the administration.

3. Specify the LDAP authentication method to be used for accessing the server. *u.trust 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 *u.trust LAN Crypt* cannot perform the logon to the server successfully, an error message will be displayed in the *u.trust LAN Crypt* Administration.

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 *<Novell>* from the drop-down list. The placeholder *<Novell>* stands for all non-Microsoft APIs.

   Note: Import from a Novell Directory service has not been supported since LAN Crypt version 3.90. Other Novell functionalities are now as well not supported and will not be functional in the administration.

3. Specify the LDAP authentication method to be used for accessing the server. *u.trust 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 *u.trust LAN Crypt* cannot perform the logon to the server successfully, an error message will be displayed in the *u.trust LAN Crypt* Administration.

Preferences

Identification of an Object

u.trust LAN Crypt uses a precise, unchanging GUID (**G**lobal **U**nique **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 *u.trust LAN Crypt* provides another way of unambiguously identifying objects. *u.trust LAN Crypt* can be configured so that certain LDAP attributes are used to uniquely identify the objects. You configure these attributes in *u.trust LAN Crypt* Administration.

The settings <*default*> and <*other*> are always available. Usually, the <*default*> setting will be sufficient for the server, to which the setting refers. The attributes evaluated by the <*standard*> setting always appear below <*default*>. 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.

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

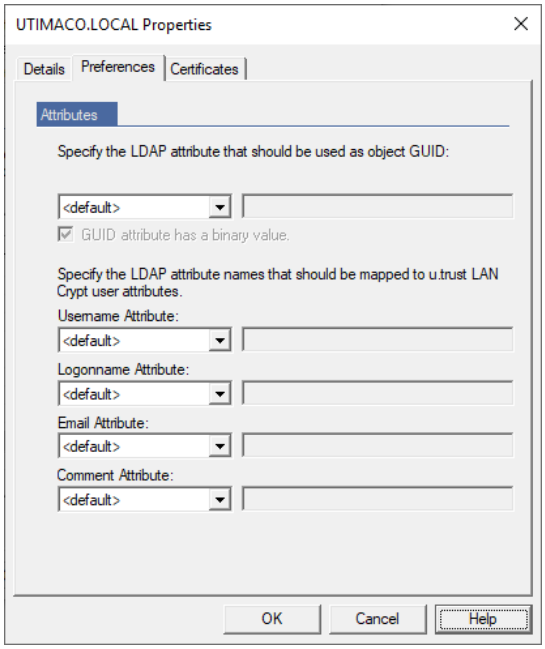
- **Object GUID**

  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 objectGUID 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.



Note: This setting is activated by default. You can only change this setting if you have selected <*other*>.

Attributes for Users

- **Username Attribute**

  This setting only affects how users are displayed in the *u.trust 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>*. *<default>* evaluates (CN and SN).

- **Logonname Attribute**

  Special meaning that is attached to the attribute for the *logon name*. *u.trust 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*.

  <default> 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, *u.trust LAN Crypt* cuts off the name at this point. This may cause problems, for example, if email addresses are used.

- **Email Attribute**

  This email address attribute is added to self-created certificates.

- **Comment Attribute**

  Like the email address, this attribute can be used to identify user objects. This is especially useful if the user's 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 synchronization (for example due to the fact that an attribute was deleted in the AD), *u.trust LAN Crypt* comments are not affected. Existing entries are maintained. New attribute contents overwrite existing comments.

  If you select *<default>*, comments are not imported.

- **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 *u.trust LAN Crypt* database.

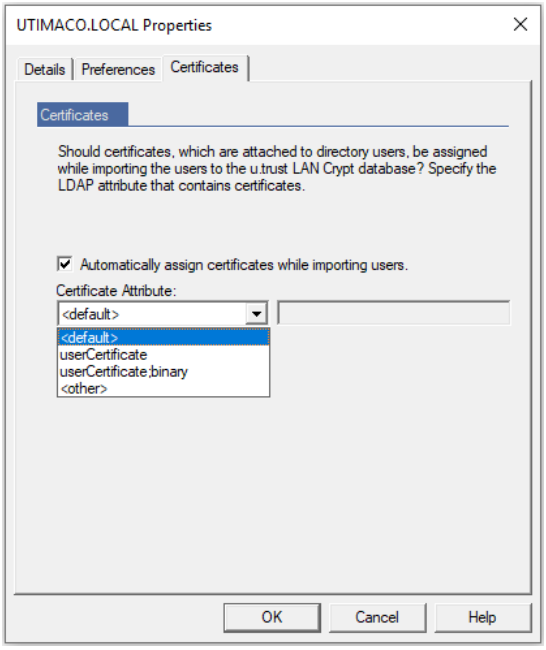
  You do not have to assign certificates to these users in the *u.trust LAN Crypt* Administration Console anymore. Here you can also specify an attribute which contains the user's certificate.

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

Activate the

Automatically assign certificates while 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 *u.trust LAN Crypt* database.



<default> evaluates *userCertificate* and *userCertificate;binary*.

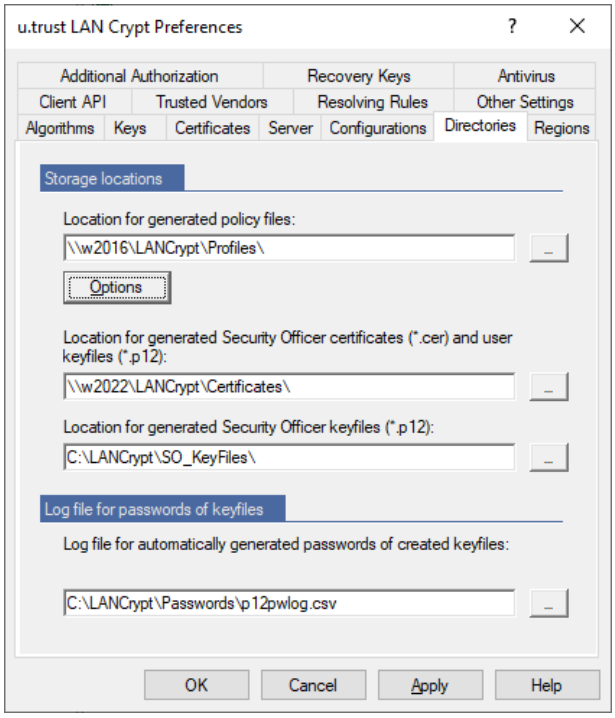
Click *<other>* to specify another attribute that contains the certificate.

When you click **OK** *u.trust 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 Security Officer. If no configuration records have yet been created, the system uses the *<DEFAULT CONFIGURATION>* configuration record.

Note: In the **Central Settings** node on the **Directories** tab, environment variables such as %LOGONSERVER% etc. cannot be used for path specifications.



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.

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

Note: You must also specify the storage location for the policy files from the client's point of view. You will find this setting under the *u.trust LAN Crypt* **Configuration** (see "*Policy file Client Location*" on page 179.

Policy file options - specifying policy file format

If you use different LAN Crypt Client versions, you must make sure that all your LAN Crypt Clients can read the generated policy files.

Note: As of version 4.0.0, *LAN Crypt* no longer supports older policy file formats (such as *"*.pol.bz2*" or "**.pol"*). The current format of the policy files is "**.xml.bz2*". This format is supported by *LAN Crypt* from version 3.90. The file is a compressed XML file. It contains all assigned rules, access rights and keys of the respective user as well as the signature of the Security Officer. The keys contained in the policy file are encrypted with the user's public certificate. If you are using older client versions than 3.97 of LAN Crypt, you must upgrade first to version 3.97, then to version 4.2.0 and then to version 11.0.x before installing version 13.0.1. **Please also note that the format for policy files is predefined and cannot be changed from version 4.0.0.**

Create additional policy files based on Novell name

Note: This function is no longer supported by *u.trust LAN Crypt*.

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

u.trust LAN Crypt can generate self-signed certificates (*.p12 key files) and assign them to the users if required. These certificates are created and assigned in the Admin Console via the node **Selected users and certificates**. Alternatively, this feature is also available through the **Groups** / **Members and Certificates of Group** nodes.

Note: If the node **Selected users and certificates** is not displayed in the Admin Console, check under the node **u.trust LAN Crypt Administration**, after clicking *Properties* in the context menu, whether the option *Show "Selected users and certificates"* is displayed in the **User Settings** tab is activated.

The path where these files should be stored must be specified in the Admin Console in the **Central Settings** node on the **Directories** tab. The clients receive this access path either via a setting in the *u.trust LAN Crypt* group policy ("*Keyfile Client Location*") or via an entry in the registry, for example via a registry file.

The *u.trust LAN Crypt* Client first searches for a matching certificate in the local certificate store of the computer, then (if none was found) in the path defined by GPO or via the registry setting. Also, the public part of the Security Officer certificate (*.cer), is stored by the admin console in this path (GPO setting "*Security Officer Certificate Client Location*").

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

Once *u.trust LAN Crypt* has found the correct file, it will display a PIN dialog. You must then send the user a PIN letter to tell them this PIN (which is in the password log file). To do this, simply use the "*LCSendP12Password*" tool included in the installation package. Once the user has entered the PIN, the certificate and associated key will be imported automatically.

If *u.trust 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 Security Officer certificate manually. If you do this, make sure that the clients import both of them.

Note: The clients must 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 *u.trust 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 60 characters) to the same directory that contains the password log file (see "*Logfile for passwords of key files*" on next page).

The file containing the password must have the same name as the corresponding password log file (default name: p12pwlog.csv) but must 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.

Note: If you are using a "*Default password for user key files*", there must not be multiple key files ("*.p12*") of the same user in the storage location for generated certificates and key files (.p12).

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)

u.trust 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 key files

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 password log 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)
- Email address (EMail)
- Generation mode (Mode). Possible values are:
  <GUI>- certificate was generated in the user's Properties dialog.
  <SO>- certificate of a Security Officer. Was generated when the Security Officer was created.
  <WIZARD>- certificate was generated using the *Certificate Assignment Wizard*.
- Filename (Filename)
- Password (Password)

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

Note: If the Security Officer who is assigning certificates has no file system right to change the password log file, *u.trust LAN Crypt* will not be able to generate certificates.

With *u.trust LAN Crypt* you can easily protect the password log file. To do so, install the Administration and Client on the same computer. After creating the initial Master Security Officer, create an encryption rule that encrypts the password log file, generate a profile for the initial Master Security Officer, and load the profile. The encryption key used should only be available to Master Security Officers and Security Officers that have permission to create certificates.

Note: If you install both *u.trust LAN Crypt* components Admin Console and Client application on the same computer, **they must be of the same version**.

Set password length for key files

The default password length for key files (*.p12 files) is 20 characters. Starting with *u.trust LAN Crypt* version 13.0.0, you can flexibly set the password length for PKCS#12 files (key files containing the certificate and private key) generated by *u.trust LAN Crypt* itself to between 12 and 60 characters, depending on your security requirements.

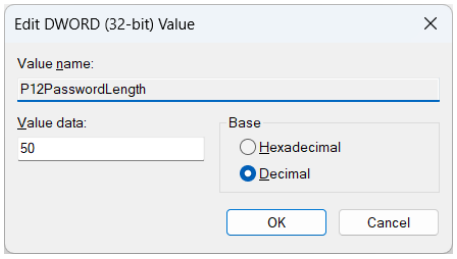
To do this, add the DWORD value named "P12PasswordLength" to the Windows registry under the key

```
[HKLM\SOFTWARE\Policies\Utimaco\SGLANCrypt]
```

Enter a value (decimal) between "12" and "60" here.

Example:

```
"P12PasswordLength"=dword:0x00000032 (50)
```



In the above example, the password for key files was changed to a length of 50 characters.

Note: Restarting the computer is not necessary after changing the password length.

3.5.7 The Regions tab

In *u.trust 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.

You can define regions by clicking *Properties* on the context menu of the **Central Settings** node in the **Regions** tab. The regions displayed here can be assigned to the Security Officers when they are created. You can define a new region by clicking Add. In the *Name for the region* input field, enter an appropriate name (e.g., New York) for the region in question and in the *Prefix for this region* input field, enter the corresponding prefix for the region (e.g., NY). By clicking on the **OK** button, the new region is added to the list of existing regions.

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

Using the **Configurations** tab in the **Central Settings** node, individual configuration sets can be created for each region. A configuration set defined in this way is then only valid for the respective region. The administration of individual regions can be done by selected Security Officers if you assign them to the respective region.

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 user key files
- the storage location for generated Security Officer key files
- 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, a Security Officer 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 Security Officers always use the same paths to save the generated files (e.g., certificates, policy files, password log file).

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

Note: The global permission *Change Configuration* specifies whether a Security Officer is permitted to change their own configuration settings. If a Security Officer does not have this right, they can only use the selected paths.

If a Security Officer changes an existing configuration record, they also change the configuration for all the Security Officers who are also assigned to this configuration!

Generating a configuration record

To generate a configuration record, proceed as follows:

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 Security Officers who are not in a region can be assigned.
2. In *New Name* enter a name for the new configuration record (e.g., New York).
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 Security Officers. To change the configuration (and the region) of an existing configuration record, select the *Properties* tab for the particular Security Officer.
7. You can create as many additional configuration records as you require.

3.5.9 The Additional Authorization tab

In *u.trust 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 Security Officers who have the global permission to authorize operations and have the right to perform the action.

IMPORTANT:

Please note that having only the global permission 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.

Actions	Necessary permissions
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**, **Resolving rules**, **Server**, **Configurations**, 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 permission *Create Security Officers*.
Change Access Control Lists	Requires the global permission *Change ACLs* and the corresponding group or SO-specific rights.
Change Global Permissions	Requires the global permission *Change Global Permissions* and the corresponding group or SO-specific rights.
Assign Certificates	Requires the global permission *Assign Certificates* and the corresponding group-specific rights.
Assign Certificates to all Members	Requires the global permission *Assign Certificates to all Members* and the corresponding group-specific rights.
Use user- or group-specific keys	Requires the global permission *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 permission *Administer Groups* and the corresponding group-specific rights.
Administer Users	Requires the global permission *Administer Users* and the corresponding group-specific rights.
Manage Logging	Requires the global permissions *Read Logging Entries* and *Manage Logging*
Create Rules	This requires the global permission *Create Rules* along with the corresponding group-specific right.
Create or Move Keys	Requires the global permission *Create Keys* along with the corresponding group-specific right.
Create Profiles	Requires the global permission *Create Profiles* as well as the corresponding group-specific permission.
Display Key Value	Requires the global permission *Read Key*. Additional authorization is required when checking the Display Key value option in a key ‘s properties dialog.

Note: If additional authorization is to be required for the execution of certain actions, this setting also applies to the closely related actions.

If 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** *u.trust LAN Crypt* updates the list on the **Additional Authorization** tab within the **Central Settings** node.

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.

Caution: 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 "*Waiving additional authorization*" on next page).

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. *u.trust 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 setting **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 *u.trust 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 Security Officer to whom this certificate is assigned is removed from the list of Security Officers.

Note: The dialog in which you select a Security Officer has an option that allows you to restrict the display to Security Officers 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 *u.trust LAN Crypt* Administration session. Click the **Reset all additional authorizations that are currently granted** 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

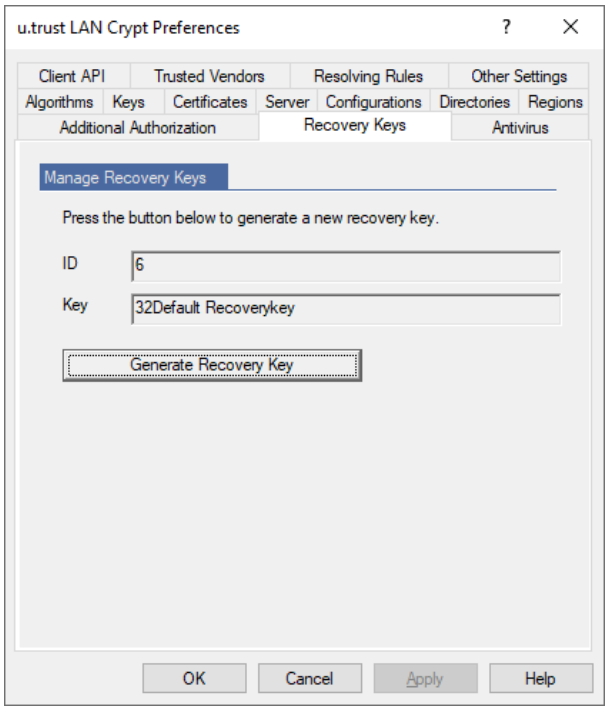
In *u.trust LAN Crypt* you can generate a recovery key. You can use this key to assign a new certificate to a Security Officer when they log on to the *u.trust LAN Crypt* Database (click the “**Assign Certificate**” button), if their certificate is, for example, damaged and can no longer be used. Using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

Alternatively, however, you can (as of *LAN Crypt* Administration version 4.1.0) store the r*ecovery key* on a **KMIP Key Server**.

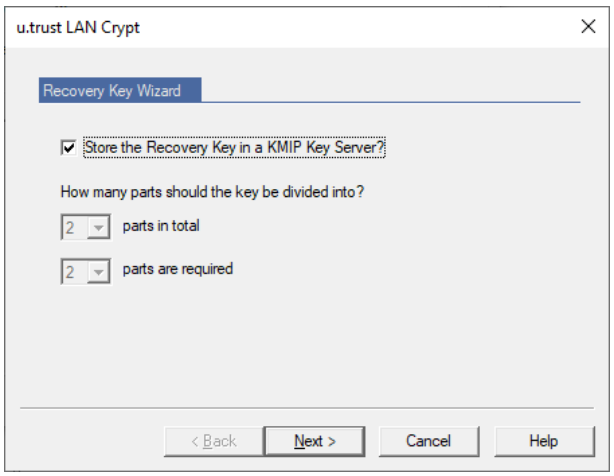
Note: You can use a **KMIP Key Server** (optional) to store the Recovery Key in a particularly secure way. Please also note that *u.trust LAN Crypt* version 13.0.1 currently only supports *Utimaco's* ***E****nterprise* ***S****ecure* ***K****ey* ***M****anager* **(ESKM)**.

To generate a recovery key, open the context menu in the **Central Settings** node of the Admin Console and click *Properties*. In the dialog that appears, switch to the **Recovery Key** tab.



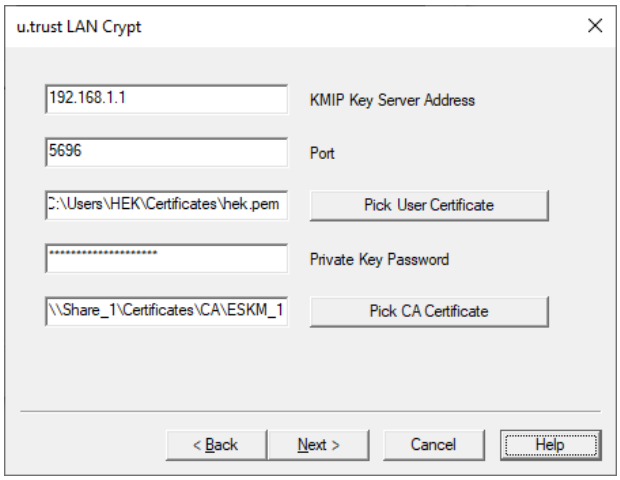
Click on the **Generate Recovery Key** button.

This runs the wizard used to generate the recovery key.



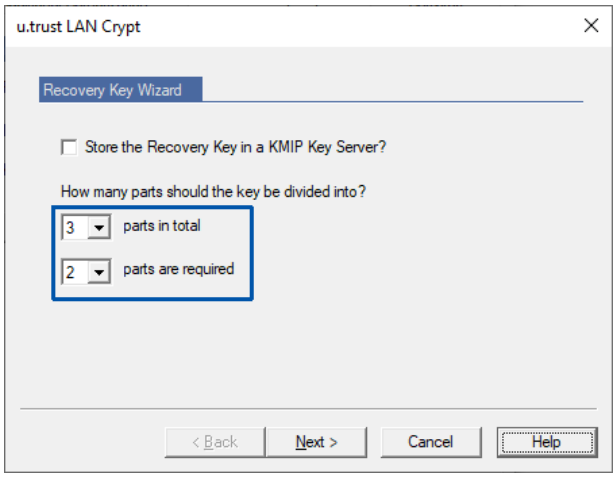
Select either the option **Store the Recovery Key in a KMIP Key Server?** or use the drop-down menus, select how many parts the key is to contain and how many of them are necessary for using the recovery key.

If you have selected the option **Store the Recovery Key on a KMIP Key Server?** and then click **Next**, you must enter the connection data for the **KMIP Key Server** (S*erver Address* and P*ort*) as well as the required certificate details and the password for the private key in the respective input fields.



Then click **Next**. The connection to the **KMIP Key Server** as well as the certificate details are checked and, if successful, the recovery key is stored in a secure manner on the **KMIP Key Server**.

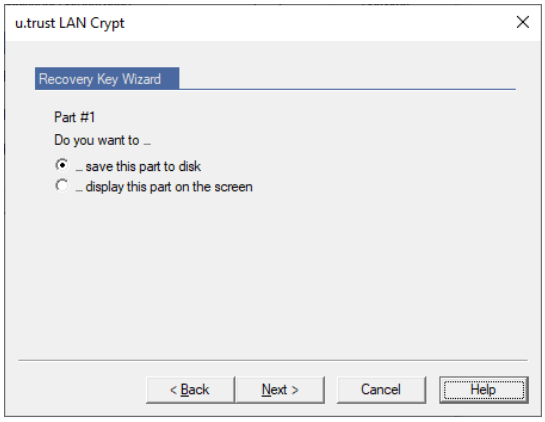
In our example the key is to have three parts, of which at least two are needed to assign a new Security Officer certificate during logon.



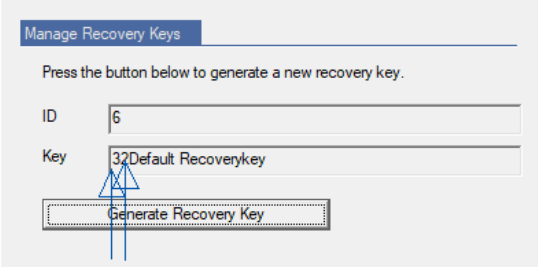
Using the drop-down menus, select how many parts the key is to contain and how many of them are necessary for using the recovery key. In our example the key is to have three parts, of which at least two are needed to assign a new Security Officer certificate during logon.

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.



In the **Recovery Key** tab at the bottom of the table, directly to the left of the "*Default Recovery Key*" entry, you can see how many parts the key consists of (in the example mentioned, 3 parts) and how many parts of these are required for use (in the example mentioned, 2 parts).



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.

Note: 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 *u.trust LAN Crypt* 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.

Depending on which setting was selected for the recovery key (either classic or via a **KMIP Key Server**), the wizard displays the respective dialog required to create a new certificate for the Master Security Officer to allow him access to the *u.trust LAN Crypt* Administration again.

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 *u.trust 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

u.trust 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, *u.trust 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 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 Antivirus tab

For virus scanners to be able to scan files encrypted with *u.trust LAN Crypt*, you have to specify the scanners here. The antivirus software entered there is thus explicitly authorized to access encrypted files and can recognize virus signatures during the scan process even in *u.trust LAN Crypt* encrypted files.

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 **Antivirus** tab under Product).
- The name of the executable file that performs the virus scan.

To prevent virus scanners from delaying the loading process of the *u.trust LAN Crypt* Client policy file, configure the antivirus processes so that they are either already active when the client encryption rules are loaded or include the path to the executable file (*EXE file Name*) that runs the virus scan. You can also use wildcards within the path.

Example:

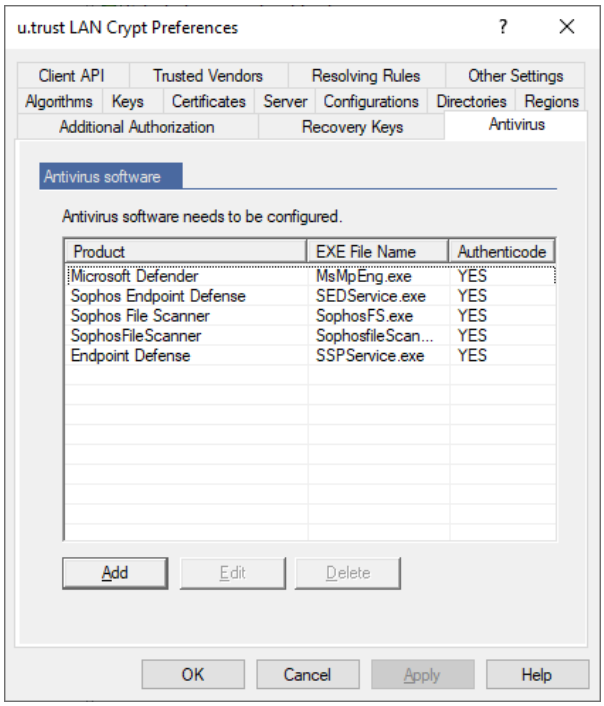
```
C:\ProgramData\Microsoft\Windows Defender\Platform\*\MsMpEng.exe
```

Note: If you do not include the path at this point, it will increase the loading time of the policy file.

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 only trustworthy applications are given the explicitly desired access to encrypted files (see “*The Trusted Vendors tab*” on page 79.

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



3.5.13 The Client API tab

u.trust 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 (PDF) in the "\api" folder of your unzipped installation package.

Note: The API has to be selected during installation of the *u.trust 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 LAN Crypt file encryption command line tool** to allow controlling the file encryption functionality via a simple command line tool.
- **API rules have priority over encryption rules**: by default, encryption rules defined in *u.trust 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: u.trust LAN Crypt **Ignore rules** and **Exclude rules** have the highest priority and cannot be overruled by API rules and the same files/folders are automatically excluded from encryption (see "*Files/folders excluded from encryption*" on page 9).

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. Specify the name of the application which is allowed to use the client API.
3. Specify the executable which is accessing the *u.trust LAN Crypt* Client 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.
6. Optionally enter a comment.

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

3.5.14 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.

3.5.15 The Other Settings tab

Security Officer options

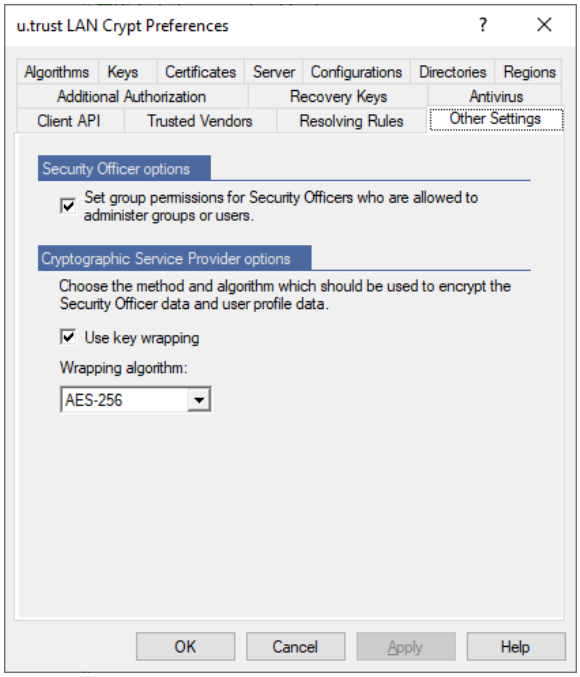
u.trust LAN Crypt can be configured to automatically create an ACL with the viewing right for the root group for a newly created Security Officer. Requirement is that the Security Officer has the global permission *Administer groups* or *Administer users*. This guarantees that the Security Officer can 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.

Note: If you then want to remove a Security Officer from a group, you can only do this in the root group, the main **Groups** node, as the permissions are 'inherited' by all subgroups below it.

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 *AES-128*). This session 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 or middleware.

Note: If the selected algorithm is not supported, users receive an error message when loading the policy file. In this case, change the algorithm or select an appropriate algorithm that is supported by the smartcard or middleware you are using.

3.6 Displaying All u.trust LAN Crypt keys

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

- Long key name.
- The algorithm used for the key.
- Information about whether the key is enabled.
- Information about who created the key (*Creator*).
- Information about whether the key should be inherited.
- Information about for which group the key was created.
- Information about whether the key is in use.
- Information about the Comment field.

In the default view, all created keys of the respective groups are displayed. By right-clicking on the **All u.trust LAN Crypt keys** node, you can use the context menu to change the view of keys in the right-hand window to view all the specific keys, such as all existing group keys (<GROUPKEY>) and user keys (<USERKEY>).

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 **All u.trust LAN Crypt keys** node and then select *Find a key* from the context menu.

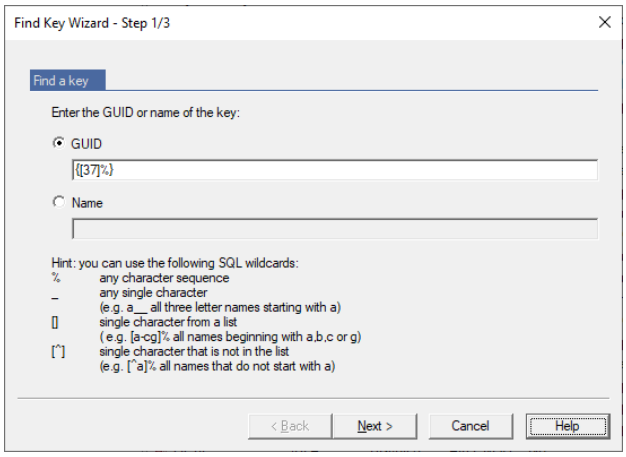
Note: The **Find a key** function is also available for the **Keys for Group** node in every group. To add a key to a group, you also need the right *Copy Keys* for the group the key is in as well as the right Create key for the group the key is to be added to.

If a key does not belong to any group, it will not be displayed to a security officer using the **Find a key** function. Only a Master Security Officer can assign such a key to a group.

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. You can use certain SQL placeholders for this.

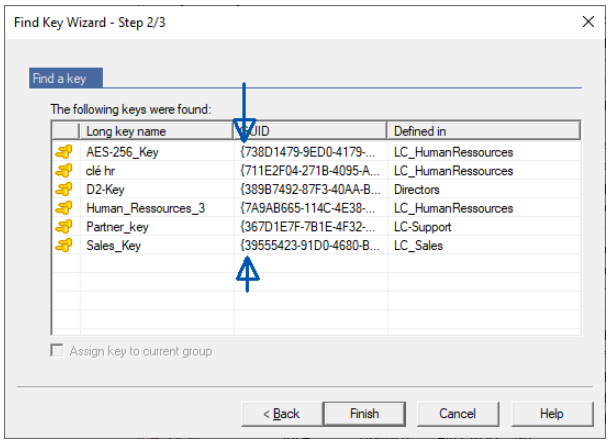
Example:

{[37]%} returns all the keys whose GUIDs start with 3 or 7.



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 key 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 **Keys for Group** of the appropriate current group. You can now use this key in encryption rules.

Note: If you select the **Assign key from the current group** option it is only effective if you called the **Find a key** function from the **Keys for Group** node in a group, and not from the **All u.trust LAN Crypt keys** node. 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 **u.trust LAN Crypt Administration** *user settings* (see "*User settings*" on page 47).

Upon clicking node **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, *u.trust 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 *u.trust LAN Crypt* database:

- Logon name
- Username
- 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. *u.trust 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 *u.trust 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).

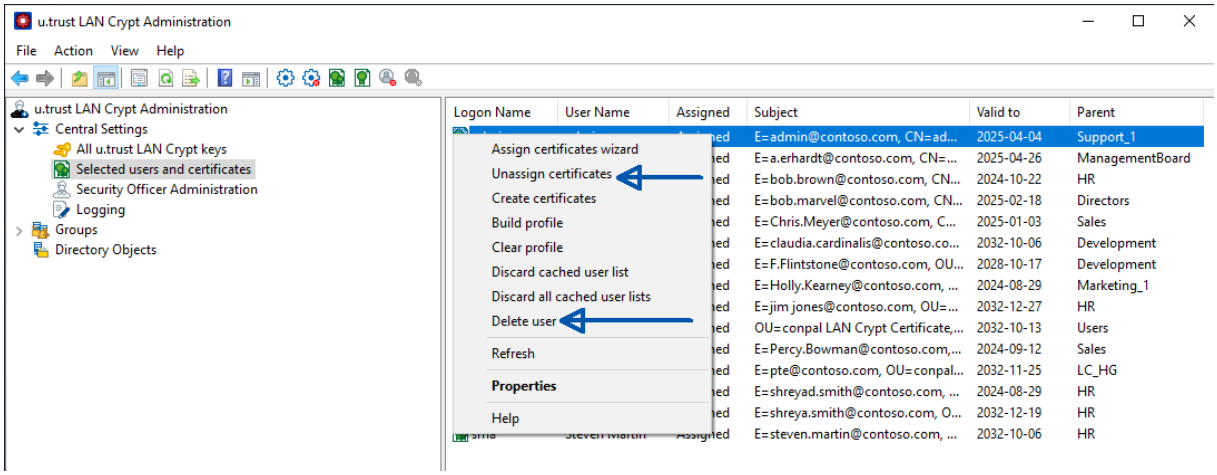
Right-click **Selected users and certificates** node to use all functions of the certificate snap-in that are available for each individual group (see “*Assigning certificates*“ on page 152).

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.

3.7.1 The "Unassign certificates" and "Delete user" menu items of the context menu

For the users displayed in the right dialog box in the **Selected users and certificates** node, the **Unassign certificates** and **Delete user** functions are available via the context menu if you select one or more users. If a user has not yet been assigned a certificate, you can recognize this by the fact that his user icon is displayed "grayed out". Users who already have a valid certificate can be recognized by the fact that their user icon is displayed in “green”.



“Unassign certificates” menu item in the context menu

The **Unassign certificates** menu item is only available for users with a green, yellow, or red user icon. With **Unassign certificates** you can delete the assignment of the certificates for the previously marked users. Afterwards, the color of the user icon changes to "gray" for these. These users then no longer have an assigned certificate.

Notes: If the color of the user icon is displayed in "red", it means that the certificate of this user has expired. On the other hand, if the color of the user icon is "yellow", it means that the certificate of the affected user will expire soon (within the configured warning period).

“Delete User” menu item in the context menu

With **Delete user**, you can delete an existing user from the *u.trust LAN Crypt* database. After you have executed **Delete user**, the user is no longer displayed in the **Selected users and certificates** and also not in the groups of which the user was a member.

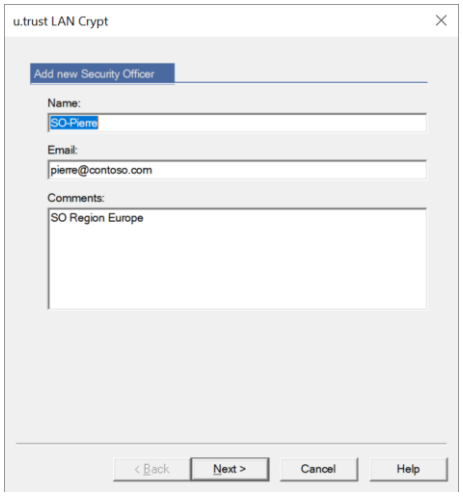
3.8 Creating a Security Officer

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 permissions that define precisely which tasks they can perform. Once Security Officers have been assigned to an organizational unit (an object in *u.trust LAN Crypt* Administration), ACLs can be used to restrict their rights again to suit this particular object.

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

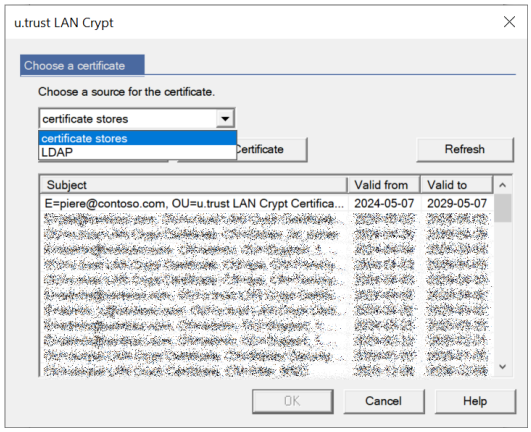
1. To create a new Security Officer (SO), select the node **Security Officer Administration**. To open the initial dialog for creating a Security Officer, click **Add new SO...** in the context menu for this node, or alternatively click **Add new SO...** in the Action menu.

2. In this dialog enter a *Name*, and if necessary, an *email address* and a *comment*. Then click **Next**.



Note: The email address is added to the password log file for certificates generated by *u.trust LAN Crypt*. It can, for example, be used to create a PIN letter via email.

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 permissions. Click the **Browse...** button to select an existing certificate or have one generated by *u.trust LAN Crypt*.



Assigning Certificates using an LDAP source

u.trust 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** node.

Note: If you use *u.trust 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 **Browse ...** button to select an existing signature certificate or have *u.trust LAN Crypt* generate a new one for you.

   Note: If you use *u.trust 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.

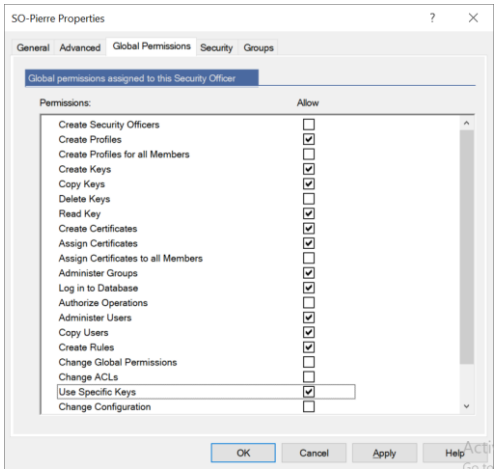
   Note: The system only displays configurations that have been generated for the selected region.

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 permissions required for the selected actions will be set automatically.

   These rights are displayed in the Security Officers properties (double-click a Security Officer to display them) on the **Global Permissions** tab.

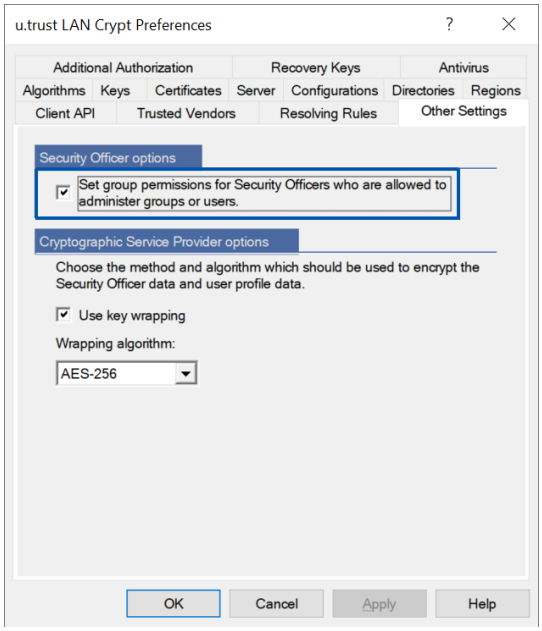
The global permissions can be edited on this page.



In this dialog, if you allow a Security Officer to perform a specific action, they will be automatically granted all the necessary permissions for this action.

Note: In order for a Security Officer to process groups, additional permissions are required (see "*Granting the Security Officer permissions to process the groups*" on page 116.

If a new Security Officer receives the global permission *Administer Groups* or *Administer Users* this way, *u.trust 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 Security Officer 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 user* option can be activated on the **Other Settings** tab in the node **Central Settings**.

9. Click **Finish**.

The new Security Officer is displayed in *u.trust LAN Crypt* Administration.

3.8.1 Granting / editing global permissions

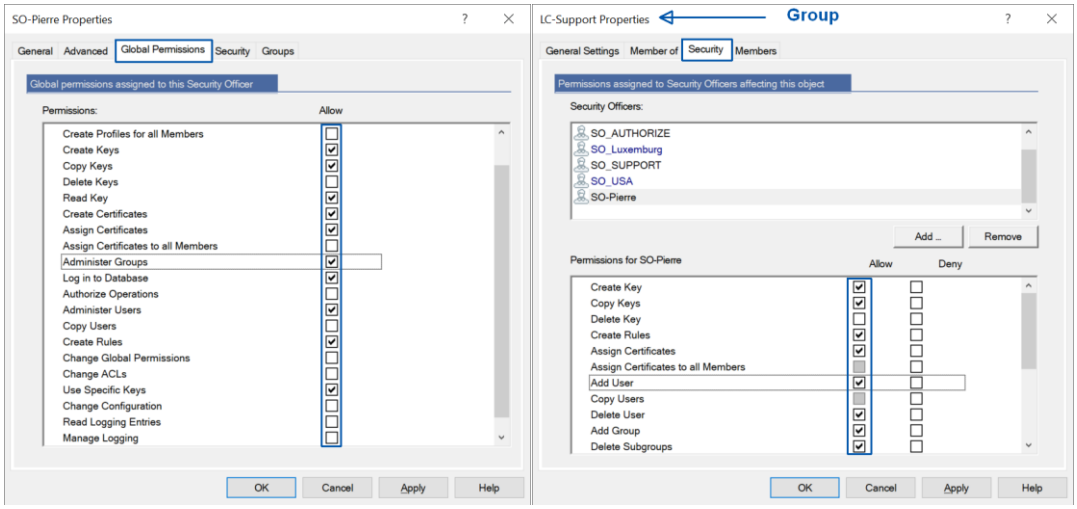
The Security Officer must be granted global permissions. If the **Security Officer Administration** node is selected, all existing Security Officers are displayed in the right-hand console pane. Double-click a Security Officer to open the tabs containing the properties assigned to them.

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

Note: Please note that a Security Officer must also be granted the required group right analogous to the global permission granted to him in each case in order to be able to perform a certain action (see " *Granting the Security Officer permissions to process the groups* " on page 116.

Example:

In order for a Security Officer to be able to import groups and users from directory services, for example, he must also have the group rights "*Add Group*" and "*Add User*" in addition to the global permissions "*Import Directory Objects*", "*Administer Groups*" and "*Administer Users*".



Note: A 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 Officers	The Security Officer has permission to create more Security Officers.
Create Profiles	The Security Officer 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 Security Officer. *Create Profiles* allows the Security Officer to build profiles for users where the Security Officer has the right *Create Profiles* for the user's parent group (see *"Parent group of an user"* on page 113*).* This permission is a prerequisite for assigning values to keys. A Security Officer who only has the permission *Create Keys* 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 Security Officer to create profiles for all users where the Security Officer 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 Security Officer can generate keys in the individual groups. A Security Officer 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 Security Officer must have the *Create Profiles* permission.
Copy Keys	The Security Officer is allowed to copy keys.

Permissions	Description
Delete Keys	The Security Officer can delete keys from individual groups.
Read Keys	The Security Officer can see the data for the individual keys for a group.
Create Certificates	The Security Officer can generate certificates for users.
Assign Certificates	The Security Officer is allowed to assign certificates to the users. The Security Officer 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 Security Officer. *Assign Certificates* allows the Security Officer to assign certificates to users where the Security Officer has the right *Assign Certificates* for the user's parent group (see "*Parent group of an user*" on page 113).
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 Security Officer to assign certificates to all users where the Security Officer has the right *Assign Certificates* for the parent group of the user or *Assign Certificates to all Members* for one of the groups 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.
Administer Groups	The Security Officer can make changes in the groups. Adding sub-groups, moving groups, synchronizing groups, deleting groups.

Permissions	Description
Log in Database	The Security Officer can log on to the *u.trust LAN Crypt* database. The default setting for this permission is active. With this permission a Security Officer can easily make changes to the *u.trust LAN Crypt* database without too much effort (for example, if staff leave the company). This permission 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 *u.trust LAN Crypt*.
Authorize Operations	The Security Officer can participate in actions that require confirmation.
Administer Users	The Security Officer can add users to a group, remove them from a group, and synchronize groups.
Copy Users	The Security Officer is allowed to add (copy) users to groups. This global permission is the prerequisite for setting the permission *Copy Users* for a specific group for a Security Officer. To add a user to a group, the Security Officer must have the permission *Copy Users* on the parent group of the user.
Create Rules	The Security Officer is allowed to generate encryption rules for the users.
Change Global Permissions	The Security Officer can change the global permissions granted to another Security Officer.
Change ACLs	The Security Officer can change the ACL for a group.
Use specific Keys	The Security Officer can use concrete specific keys in encryption rules and can display specific keys in **All u.trust LAN Crypt keys**.
Change Configuration	The Security Officer can change the configuration (paths). This permission is required to display the **Configuration** tab in the **Central settings**, and for the Security Officer to be able to make changes in the **Directories** tab if they are logged on to the database.
Read Logging Entries	The Security Officer can view the settings used for logging and the logged events.

Permissions	Description
Manage Logging	The Security Officer can change the logging settings. They are permitted to archive, delete, and check entries.
Import Directory Objects	The Security Officer can import OUs, groups and users from a directory service and add them to the *u.trust LAN Crypt* database. Before they can import Directory Objects, the Security Officer also needs the *Administer Groups* permission and the *Administer Users* permission. These are set automatically when the *Importing Directory Objects* permission is selected. If a Security Officer 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.
- *u.trust 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 Security Officer has the global permission *Administer group* or *Administer users*. This guarantees that the Security Officer 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 Groups* 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**.

Click **OK** to close the dialog.

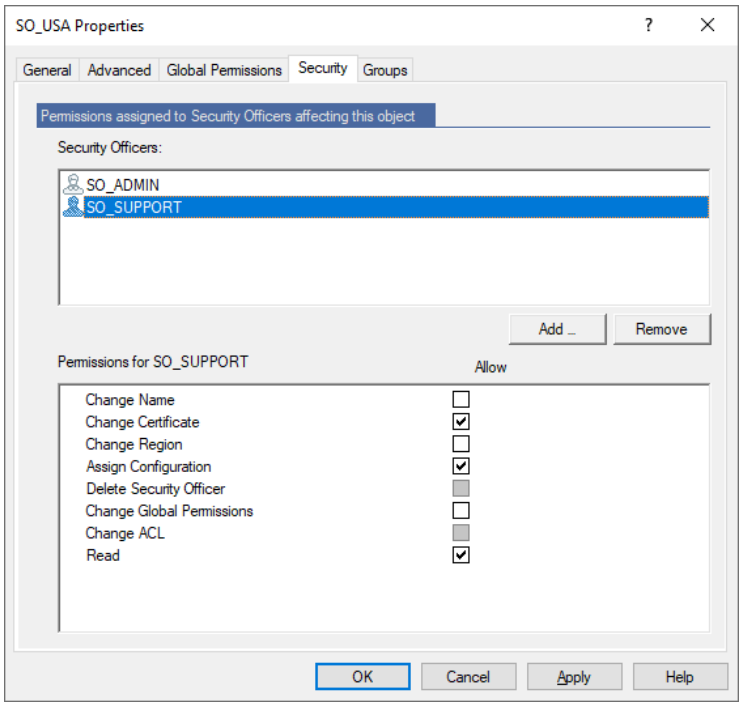
3.8.2 Permissions for changing the settings for a Security Officer

The permissions for changing the settings for a Security Officer can be transferred to other Security Officers. This permission must be specifically granted to a Security Officer.

Note: A Master Security Officer can always change these settings.

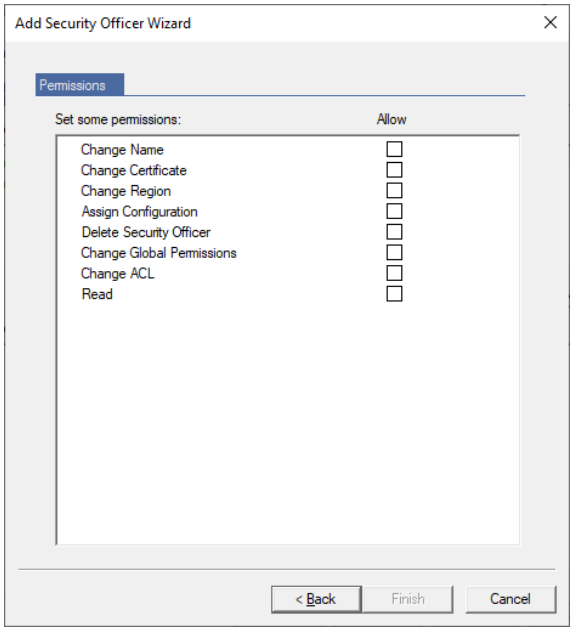
The global permissions a particular Security Officer has determine which permissions they can change for other Security Officers. In addition, several permissions may be required to perform a certain function. For example, if a Security Officer is to be given the permission to delete another Security Officer, this Security Officer must have the global permission *Change ACLs* and *Create Security Officers*.

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



1. Click **Add** to run a wizard for adding a Security Officer. On the first page of the wizard, select the Security Officer you require from the list of existing Security Officers.

2. Click **Next** to display the page on which you specify the current Security Officer's permission to change this object (the Security Officer whose settings are currently being processed).

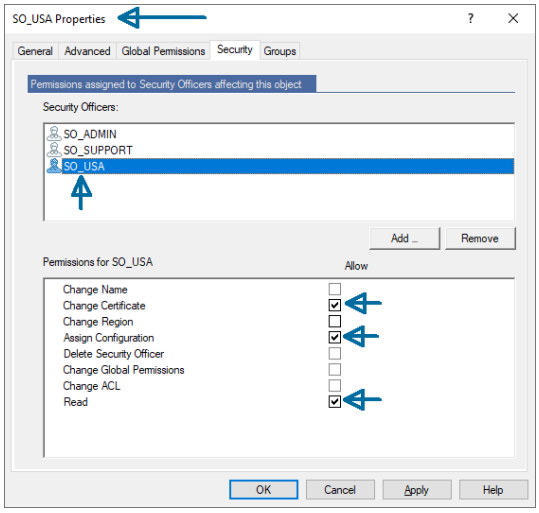


Note: Click **Allow** to select all permissions at once. Click again to deselect all global permissions. The global permission settings specify that disabled rights cannot be granted to the Security Officer (see "*Granding / editing global permissions*" on page 89).

Permissions	Description
Change Name	Allows changes to the name of the Security Officer to whom the permission's owner is assigned.
Change Certificate	Allows changes to the certificate of the Security Officer to whom the owner of the right is assigned.
Change Region	Allows changes to the region prefix of the Security Officer to whom the owner of the right is assigned.
Assign Configuration	Allows changes to the configuration of the Security Officer to whom the owner of the right is assigned.
Delete Security Officer	Allows the Security Officer, to whom the owner of the permission is assigned, to be deleted.
Change Global Permissions	Allows changes to the global permissions of the Security Officer to whom the owner of the permission is assigned.
Change ACL	Allows changes to the global permissions of the ACL to whom the owner of the right is assigned.

Permissions	Description
Read	Displays the Security Officer to whom the owner of the permission is assigned in the node **Central Settings** \ **Security Officer Administration**. This is the prerequisite for all rights that allow this Security Officer 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 Security Officer whose properties are defined here. Before this can happen, that Security Officer must be present in the list of Security Officers that have rights for this object (in this case, that particular Security Officer).



Read

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

Assign Configuration

Allows the Security Officer to assign a different configuration to themselves.

Change Certificate

The prerequisite for this right is **Read** permission. Allows the Security Officer to change their own certificate.

Note: Permissions whose checkbox is grayed out cannot be granted because the selected Security Officer 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 Security Officer.

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

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

In the Security Officers *properties* dialog, select the **Groups** tab. This tab contains two list views:

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

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

Note: You cannot change the rights of a Security Officer in this view. Changing rights is only possible in the properties dialog of a group.

Note: Only groups a Security Officer has rights for (**Allow** or **Deny**) are displayed. Groups for which a Security Officer has inherited rights are not displayed.

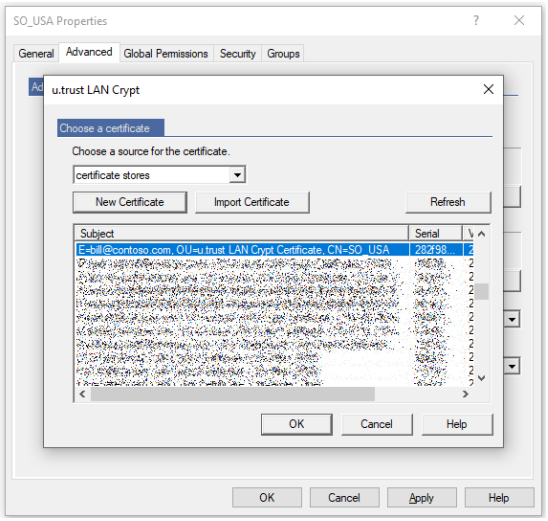
3.8.4 Changing or renewing MSO or SO certificates

The different ways in which you can change or renew an (M)SO certificate is described below:

Variant 1: Via Security Officer Administration

1. Start *u.trust LAN Crypt* Administration and log on as the Master Security Officer. You can also log on as a Security Officer if this Security Officer has the permission to change the certificate for the Security Officers concerned. This can also include the Security Officer themselves, if they have the appropriate permissions and their certificate is still valid.
2. Switch to the **Central settings** node and from there go to the **Security Officer Administration** node.
3. Right-click the Security Officer concerned and select the *Properties* entry from the context menu.
4. Go to the **Advanced** tab.
5. In *Encryption certificate* click the **Browse …** button to select a new encryption certificate for the Security Officer.
6. You can also go to *Signature certificate (optional)* and click **Browse …** to select new signature certificate for the Security Officer.

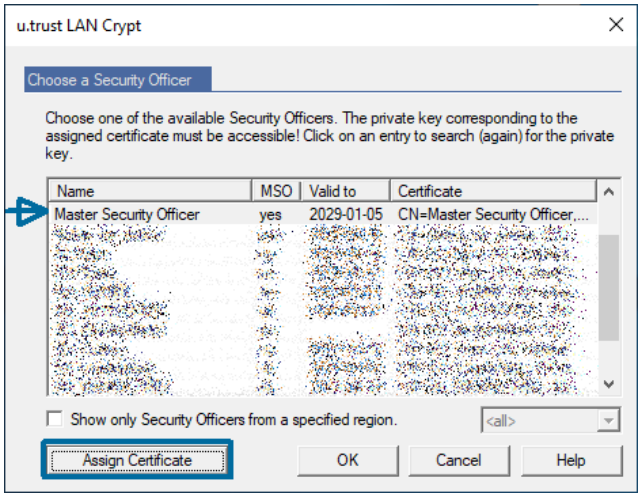
7. Select the preferred certificate or select or create a new certificate. Alternatively, you can import an existing certificate. When you have selected the certificate for the Security Officer, click **OK**.



Note: You can only change Security Officer signature certificates in *variant 1* and not in *variant 2*.

Variant 2: Using the restoration key

1. Start *u.trust LAN Crypt* Administration.
2. In the Security Officer dialog window, select the (M)SO you require.
3. Click the **Assign Certificate** button and follow the instructions in the *Recovery Key Wizard*.



Usually, you should use *variant 1*. *Variant 2* is primarily intended to be an alternative method and should be used if no Security Officer with the appropriate permissions is able to log on to *u.trust 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 Security Officer is regenerated before the old certificate reaches its expiration date. If not, the clients will no longer be able to load the profile.

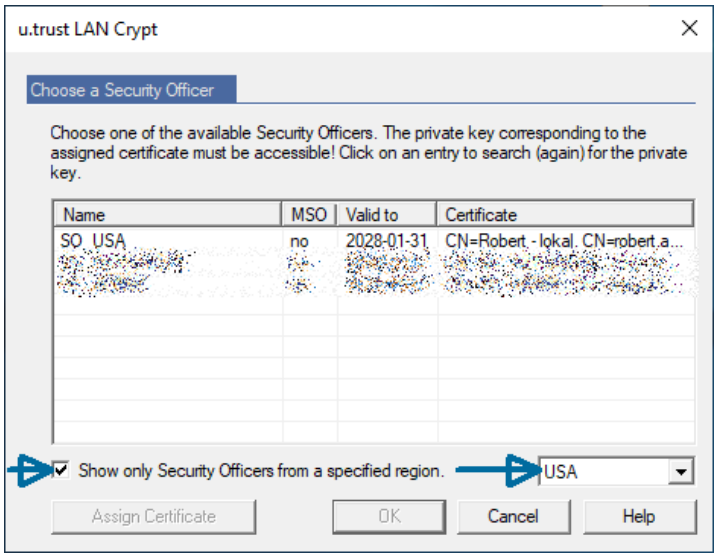
However, you can allow certificates to be assigned with only *additional authorization*. You must remember that this type of assignment will have an effect when Security Officer certificates are changed.

3.9 Logging on to Administration

For logging on to the *u.trust LAN Crypt* Administration Console a Security Officer must have the global permission to *Log in to Database*. Master Security Officers always have this permission since they are automatically granted all available rights.

When you run Administration (*Start/u.trust LAN Crypt Administration/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 *u.trust LAN Crypt* Administration Console.

Recovery Key

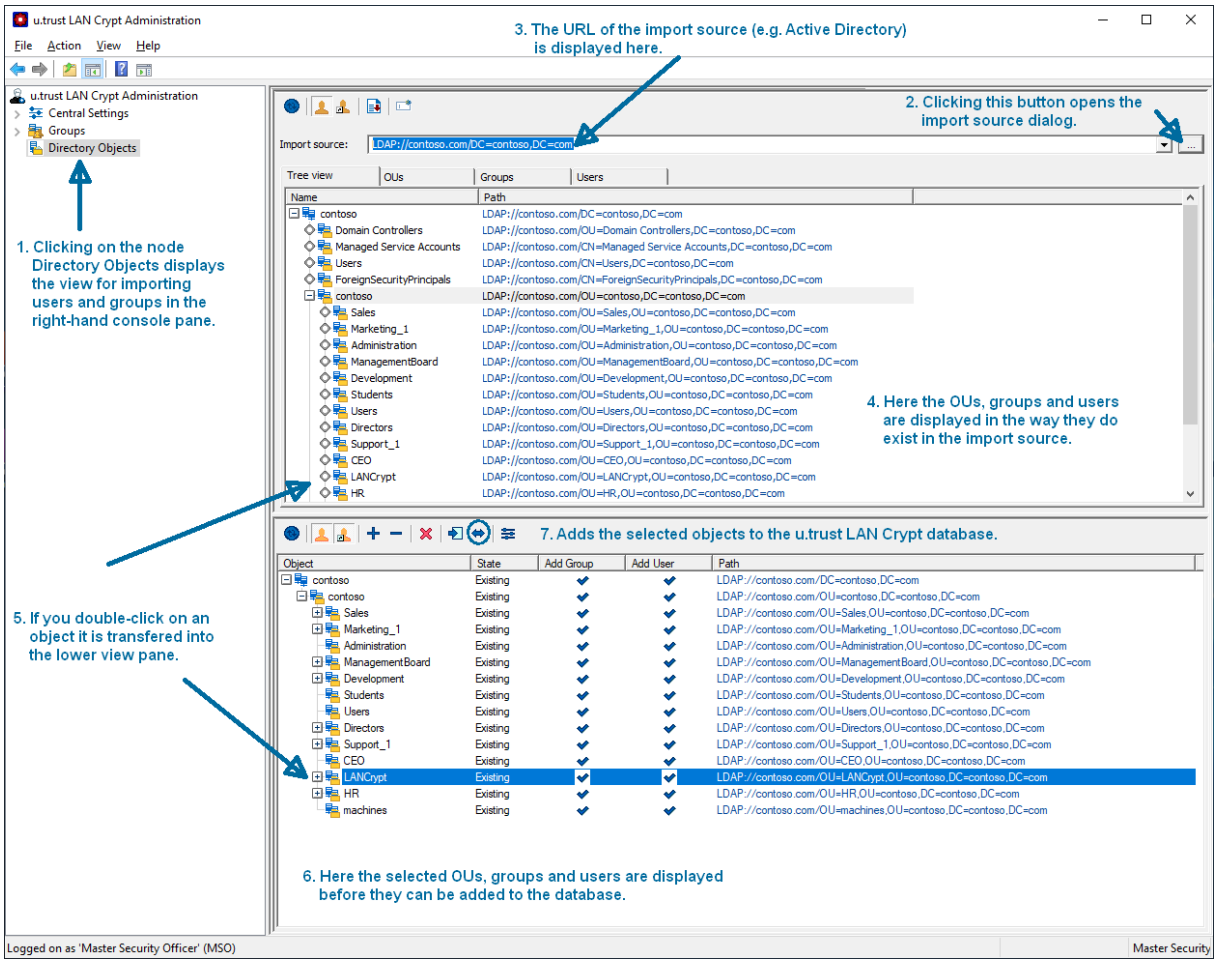
If the key belonging to a Security Officer's certificate has expired, or has been damaged or lost, enter a recovery key to renew the certificate.

Note: If a new certificate is generated during the recovery process, this certificate (and the associated password) is stored in the configured path.

3.10 Importing groups and users

With *u.trust 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 *u.trust LAN Crypt* database, in the right-hand console pane.



Note: If a Security Officer 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 Security Officer has this permission.

Note: For performance reasons, always use the FQDN (**F**ully **Q**ualified **D**omain **N**ame) when calling the import source via LDAP.

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 users are created in the **Groups** and **Directory Objects** nodes in the *u.trust 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 u.trust 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 104).

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 Defines whether the imported object represents a user (USER) or a group (GROUP).
name=	Defines a user’s logon name. This is displayed under *Logon name* in the *u.trust LAN Crypt* Administration console.
display= optional	Allows you to define a username that is not identical to the logon name. This appears as the *Username* in the *u.trust LAN Crypt* Administration console. If no name is specified here, the logon name entered under *name=* is displayed under *Username* in the *u.trust LAN Crypt* Administration console.
mail= optional	Allows you to enter the user’s email address. This is displayed on the Details tab in the user’s properties. **Note:** The email address is added to the password log file for certificates generated by *u.trust LAN Crypt*. For example, it can be used to create a PIN letter via email.

Keywords	Description
members=	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_Utimaco). Enter commas to separate each group member's name from the next.

Note: 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_RS]
type=USER
name=RS
Display=Ralph Smith
Mail=ralph.smith@contoso.com
// my comment ...
[U_PW]
type=USER
name=PW
Mail=pw@contoso.com
[U_JG]
type=USER
name=JG
[U_RL]
type=USER
name=RL
[G_COMPANY]
type=GROUP
name=Company members=G_QA, G_NI, G_FFM, G_HG, U_RL, U_JG, U_PW, U_RS
// my comment ... ...
[G_QA] type=GROUP name=QA members=U_JG, U_PW
[G_PDM] type=GROUP name=PDM members=U_RL, U_RS
```

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 *u.trust LAN Crypt* Database.

 Synchronizes the objects displayed in the bottom right-hand pane with the ones already present in the *u.trust 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 *u.trust 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 synchronization 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 100).

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

When you click **OK** *u.trust 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’s name and password.
2. For LDAP or SSL, specify whether the <Microsoft> or <Novell> implementation is in use.

   Note: Import from a Novell Directory service has not been supported since LAN Crypt version 3.90. Other Novell functionalities are now as well not supported and will not be functional in the administration.
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 u.trust 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 *u.trust 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 *State* column).
  - Whether the logged-on Security Officer has the permission to modify a group (in the *Add Group* column). A red cross show that the Security Officer does not have the permission to add the group. A green tick means that the Security Officer has the permission to *add the group*.
  - Whether the logged-on Security Officer has the permission to add users (in the *Add User* column). A red cross shows that the Security Officer does not have the permission to add users. A green tick means that the Security Officer 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 **Refresh** button. Click **Refresh** 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 *u.trust 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 *u.trust 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 u.trust 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 *u.trust LAN Crypt* Database.

- **New relationships in the directory**

  Displays the objects and memberships that have been added to the *u.trust 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 *u.trust 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 group's 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.
4. 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.

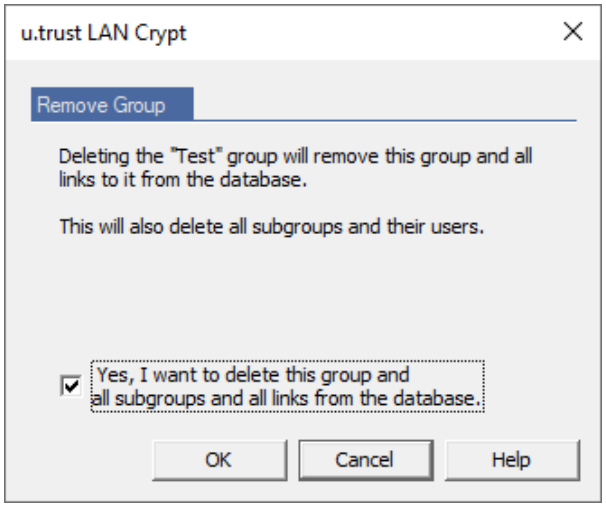
When *Team 1* no longer requires the extra rights, you can remove the shortcut from *Team 2*'s group and generate new policy files again. The members of *Team 1* then no longer have access to Team 2's data.

3.10.5 Deleting groups

You can delete individual groups/OUs and shortcuts to groups/OUs in the *u.trust 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 *u.trust 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 *u.trust LAN Crypt* database.

Before the group is deleted, a dialog is displayed in which you must confirm that you want to delete the group.



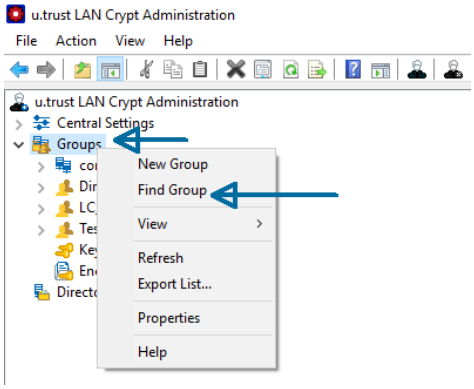
To **delete a shortcut** to a group, click **Delete** in the shortcut's context menu. Only the shortcut is deleted. The group itself is not affected. Before you delete a shortcut, a dialog appears that asks you to confirm that you want to do so.

The context menu of the parent group contains the entry **Remove links** that you use to delete a shortcut.

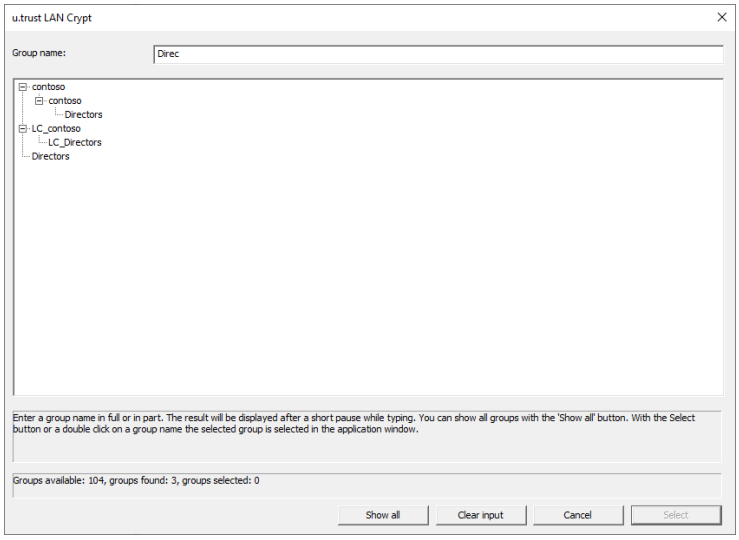
Click **Remove links** to delete all shortcuts to this group. The group itself is not affected.

3.10.6 Find Group

The **Find Group** function helps you to search for a particular group. Right-click the **Groups** node and select **Find Group**.



The following dialog appears:



Enter all or part of the group name you want to find in the **Group name** input field. The result is displayed in the application window after a short pause during the input. By clicking **Show all**, you can also display all groups in the display window. Highlight the group name you were looking for and click **Select** or double-click the group name in the application window to select the group.

Note: The **Find Group** function is only available in the **Groups** main node. However, this function is not displayed in the context menu of any of the groups below it.

3.10.7 Group icons

The OUs and groups are represented by different icons in the *u.trust 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 Security Officers to organizational units

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

The Security Officer 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 u.trust 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 u.trust 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 *u.trust 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 47).

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

- Viewing the properties of a user: Security Officers can view the properties of a user when they have the rights Read and Visible for the parent group of the user.
- Modifying the properties of a user: Security Officers can modify the properties of a user when they have the global permission *Administer Users* and the permissions *Add User* and Delete User on the parent group of the user.
- Creating Profiles: If Create Profiles is set for a group for a Security Officer, the Security Officer is allowed to build profiles for all members of the group, where the group is also the parent object of the group. The Security Officer is not allowed to create profiles for users who are only members of the group and have a different parent group. This requires the permission *Create Profiles for all Members*.
- Assigning Certificates: If *Assign Certificates* is set for a group, the Security Officer is allowed to assign certificates to all members of the group, where the group is also the

parent object of the group. The Security Officer is not allowed to assign certificates to users who are only members of the group and have a different parent group. This requires the permission *Assign Certificates to all Members*.

- Copying Users: When a Security Officer wants to add a user to a group by using properties dialog of a group (on the tab **Members** with the **Add** button), the Security Officer must have the permission *Copy Users* for the parent group of the user.

3.11.2 Allowing a Security Officer to see and edit groups

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 Security Officer. Here, select the *Visible* permission and then click **Finish**. This permission is inherited downwards through the group hierarchy, which means the Security Officer can now view all groups.

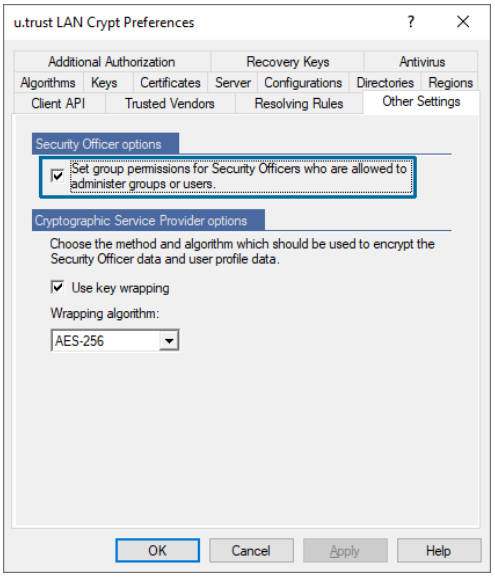
   If the Security Officer logs on to the database with these settings, they can see the entire Administration structure but cannot edit it.
5. In the next step you can now hide (suppress) the groups in the Administration Console you do not want the Security Officer to see because they have no rights to 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 Security Officer.

Note: If a Security Officer 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 a Security Officer **Read** and **View** permissions to a hierarchically superior group so that they can assign rights to subordinate groups without causing any problems.

Note: *u.trust 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 Security Officer has the global permission *Administer Groups* or *Administer Users*. This guarantees that the Security Officer can access (view and/or edit) all groups he is responsible for.

This behavior has to be activated on the **Other Settings** tab in the node **Central Settings**.

Example (Master Security Officer):



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

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

If both the **Visible** permission and the **Read** permission have been assigned to the Security Officer 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 Security Officer can see the contents of the snap-ins but cannot change them.

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

Note: If the Security Officer 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.

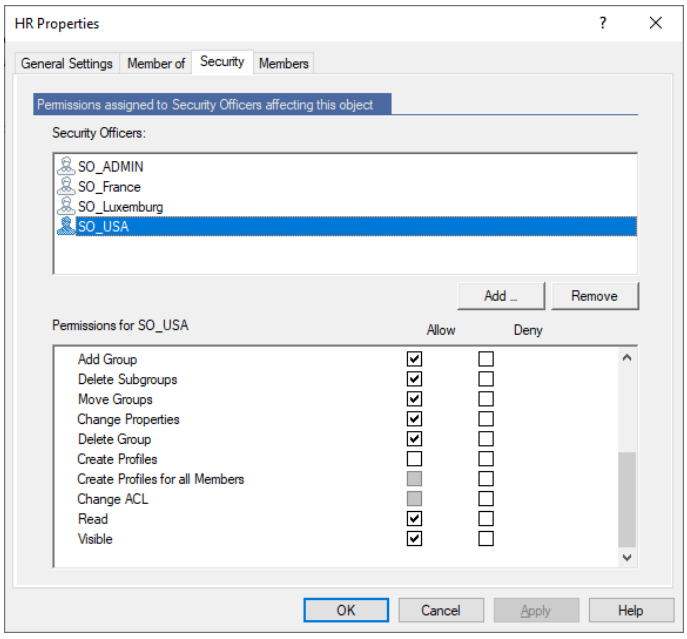
3.11.3 Granting the Security Officer permissions to process the groups

Once you have set up the Security Officer 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 Security Officer, open the *Properties* dialog, and select the **Security** *tab.*

2. Under Security Officers you see all the Security Officers who are assigned to this group. When you select a Security Officer, 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 permissions, have a checkbox that is completely grayed out.

Note: The global permissions settings define which permissions can be assigned to a particular Security Officer. Global permissions are set when the Security Officer is generated.

Note: Click **Allow / Deny** allowing 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.

Note: See also "*Set group permissions for Security Officers who are allowed to administer groups or users*" on page 79.

You can assign the following permissions:

Permissions	Description
Create Key	The Security Officer is allowed to generate keys in the group.
Copy Keys	The Security Officer is allowed to copy keys.
Delete Key	The Security Officer is allowed to delete keys.
Create Rules	The Security Officer is allowed to generate encryption rules for the users.
Assign Certificates	The Security Officer is allowed to assign certificates to the users. The Security Officer is allowed to run the *wizard for assigning certificates*. This permission allows the Security Officer 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 Security Officer to assign certificates to all users in the group: users of whom the 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**.

Permissions	Description
Add User	The Security Officer is allowed to add users to the group manually. This permission is a prerequisite for importing / synchronizing groups and users.
Copy Users	The Security Officer has the permission 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	Security Officers is allowed to use the *Members and certificates for group* snap-in to delete users. This permission is a prerequisite for importing / synchronizing groups and users.
Add Group	The Security Officer 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 Security Officer is allowed to delete the subgroups for this group. This permission is a prerequisite for importing / synchronizing groups and users.
Move Groups	The Security Officer is allowed to move manually created groups in Administration (with *drag & drop*). Imported groups cannot be moved. This permission is a prerequisite for importing / synchronizing groups and users.
Change Properties	The Security Officer is allowed to change a group's properties.
Delete Group	The Security Officer is allowed to delete groups. This assumes that the Security Officer has removed the "*Delete Subgroups*" permission in the group above. This permission is a prerequisite for importing / synchronizing groups and users.

Permissions	Description
Create Profiles	The Security Officer has the permission to run the Profile Resolver and generate policy files for selected users. *Create Profiles* allows the Security Officer 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 Security Officer 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 Security Officer is allowed to change the ACL for the group (for example, by adding another Security Officer).
Read	The Security Officer 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 Security Officer can see the group. Is set in the base node and inherited downwards. If it is refused for the Security Officer, the group is hidden ("*Read*" must also be set to **Deny**).

3. Select the permissions you want to assign to the Security Officer. Click **Apply** to store the settings in the database.

4. If you have assigned other Security Officers to this group, you can now also set up their permissions. To display the permissions set for the Security Officers, select them under *Security Officers*.

Note: Changes to the permissions of a Security Officer for a group only become effective after the relevant Security Officer has logged on to the *u.trust LAN Crypt* Administration again.

3.12 Properties of groups

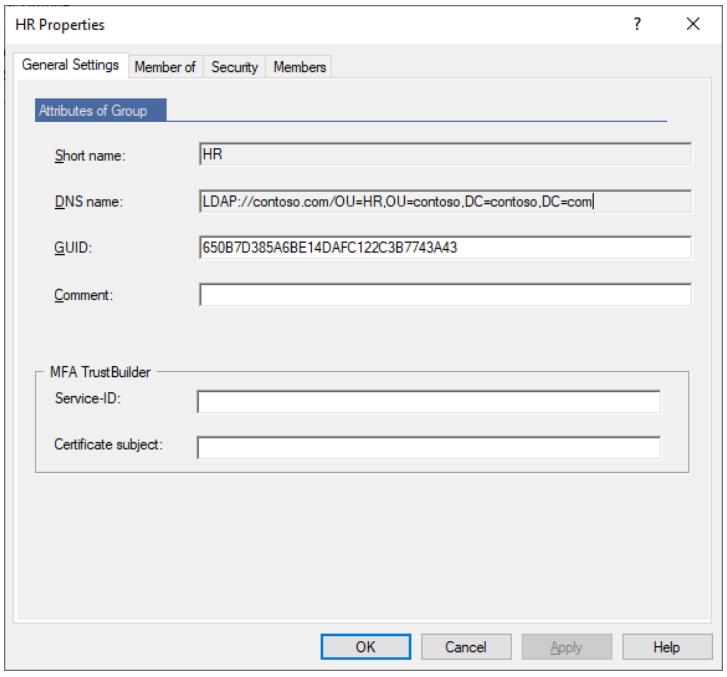
The *Properties* dialog for a group (<Group>/Context menu/Properties) consists of four tabs in which you can edit the properties for a group.

3.12.1 The Properties tab

The **Properties** tab displays the

- Short Name
- DNS Name
- GUID
- Comment
- Service-ID (MFA TrustBuilder)
- Certificate subject (MFA TrustBuilder)

for the group.



TrustBuilder MFA and u.trust LAN Crypt

In the *MFA TrustBuilder* section, you define the specifications for the Multi-Factor Authentification of the users with *TrustBuilder*.

With the support of MFA (**M**ulti-**F**actor **A**uthentification), users can log in to the *u.trust LAN Crypt* Client in a particularly secure manner. The login itself is then performed using a second device (this can be the user's smartphone or tablet, for example). The *TrustBuilder* settings are configured by the Windows or *TrustBuilder* administrator. Please contact them and ask for the required information *Service-ID* and *Certificate subject* for the *MFA TrustBuilder* settings for *u.trust LAN Crypt*.

Enter the required number for the *Service-ID* and the *Certificate subject* ("*@cert.trustbuilder*", the API certificate of the TrustBuilder Service) in the corresponding fields.

Note: In order for the users of this group to be able to use *TrustBuilder MFA*, the profile must be newly built for them (see "*Providing encryption rules – generating policy files*" on page 163). After loading the new profile, the users can perform their login to the *u.trust LAN Crypt* Client via MFA. The user then receives an authentication prompt on his registered *MFA token* (e.g, this can be his smartphone), enters his PIN there and confirms it.

Note: The API certificate of the *TrustBuilder Service* must be installed in the user's certificate store on the *u.trust LAN Crypt* client.

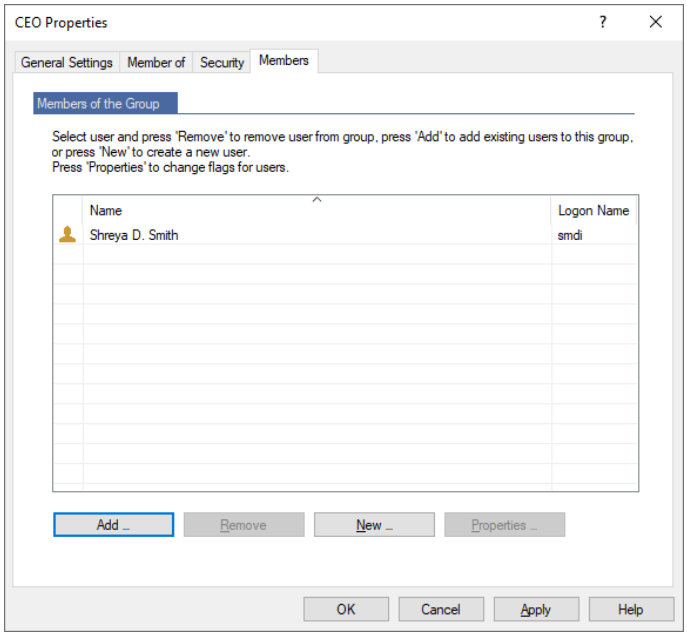
Note: If you define specifications for **M**ulti-**F**actor **A**uthentication (MFA) for a group, these are not inherited downwards. So, you have to define them for each group separately.

3.12.2 The Member of tab

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

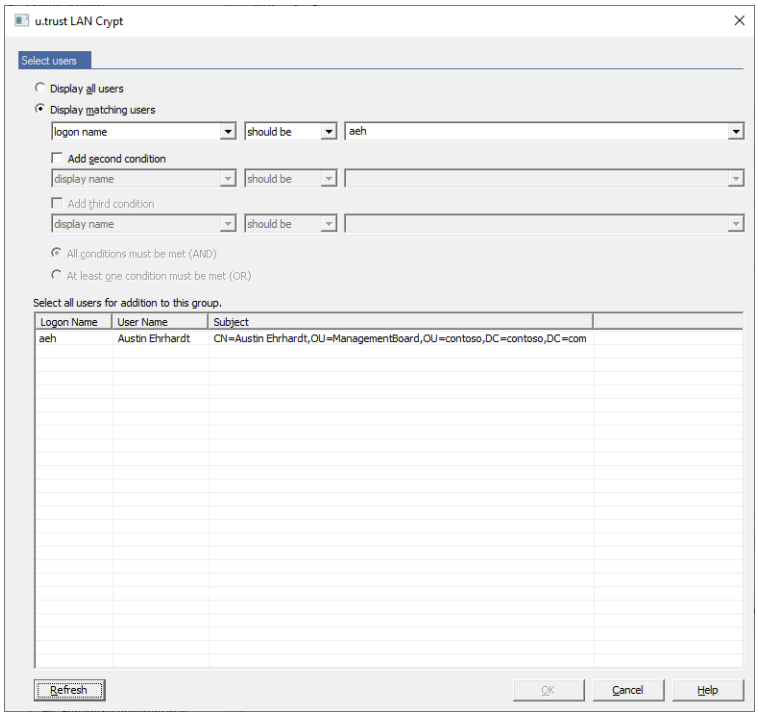
3.12.3 Adding / deleting members

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, *u.trust 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 *u.trust LAN Crypt* database:

- Logon name
- Username
- 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. *u.trust 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 *u.trust 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.

Note: If the user is not a member of any other group, they are deleted from the *u.trust 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.

3.12.4 Adding Security Officers

On the **Security** tab, a (Master) Security Officer can also add Security Officers to the current group and assign them rights to the group (see Chapter 3.11.3 "*Granting the Security Officer permissions to process the groups*" on page 116). The prerequisite for this action is that the Security Officer who wants to add another Security Officer has the **Change ACL** permission.

Note: If the Security Officer adds Security Officers to the group, the Security Officer can assign their own permissions (and only those permissions) to those Security Officers.

A Security Officer 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.

Certificates

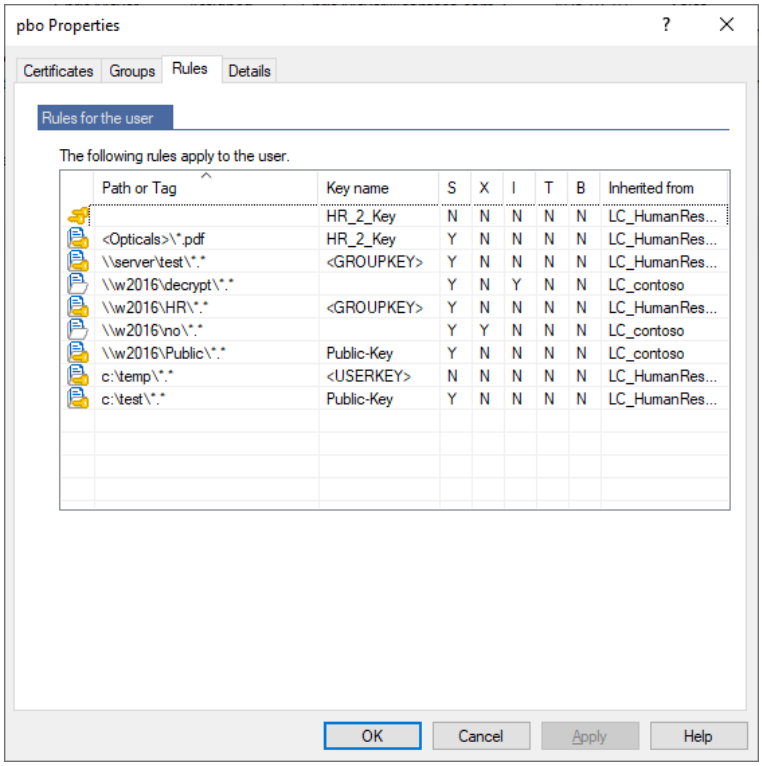
The **Certificates** tab displays all the certificates that are assigned to a user. In this tab you can also create a new *u.trust LAN Crypt* certificate for the user, add a certificate from the certificate store and import a certificate from a file (see *Assigning a certificate to a user* on page 153).

Groups

The **Groups** tab displays the groups in which the current user is a member. Furthermore, you can remove the user's memberships to groups or add new ones as well.

Rules

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.

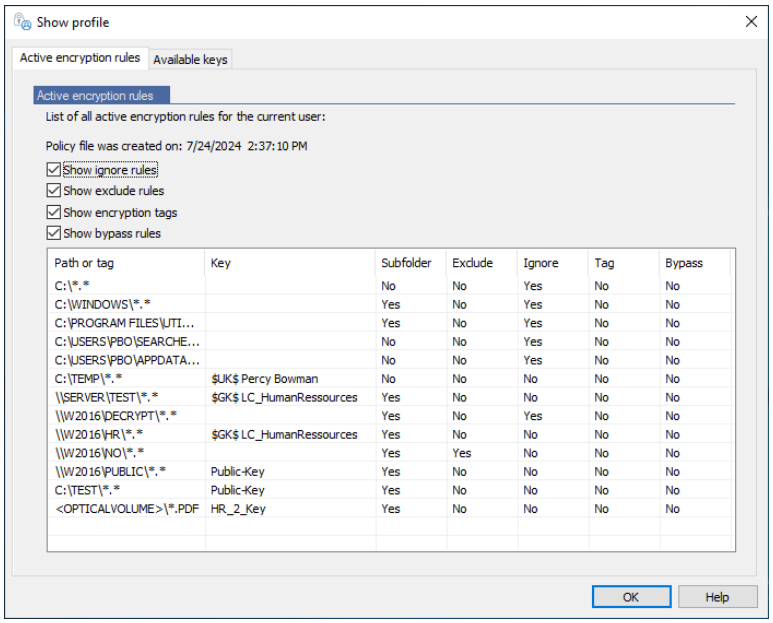


Columns S, X, I, T, B show, which kind of rule it is:

- **S** (sub-directories): sub-directories are included in encryption.
- **X** (exclude path): the path is excluded from encryption.
- **I** (ignore path): the path is ignored by *u.trust LAN Crypt*. For further information, see ”*Generating encryption rules*“ on page 141.
- **T** (tag): the path is used by the *u.trust LAN Crypt* Client API as a predefined encryption tag, see *Encryption tags* on page 150.
- **B** (bypass): the path is defined as a **Bypass Rule**. For further information, see “*Bypass*” on page 146.

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

In the profile view of a user in the *u.trust LAN Crypt* client, you can display this information in the same way:



Details

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

You can enter the user's email address in the *Email Address* input field. The email address is added to the password log file for certificates generated by *u.trust LAN Crypt*. It can, for example, be used to create a PIN letter via email.

Note: User email addresses must not contain any characters above ASCII code 127, and therefore no umlauts. There must not be a period at the beginning and end of the string.

In the section *MFA TrustBuilder* you can define the specifications for the multi-factor authentication for individual users with TrustBuilder.

To do this, contact your System Administrator who is responsible for the administration of TrustBuilder MFA and ask him for the required information. Enter the required number for the Service- and Username-ID and the Certificate subject ("@cert.trustbuilder", the API certificate of the TrustBuilder Service) in the corresponding fields.

For more details on this and how to define this setting for all users of a group, see the **Properties** tab of the respective groups (see "*TrustBuilder MFA and u.trust LAN Crypt*" on page 120).

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

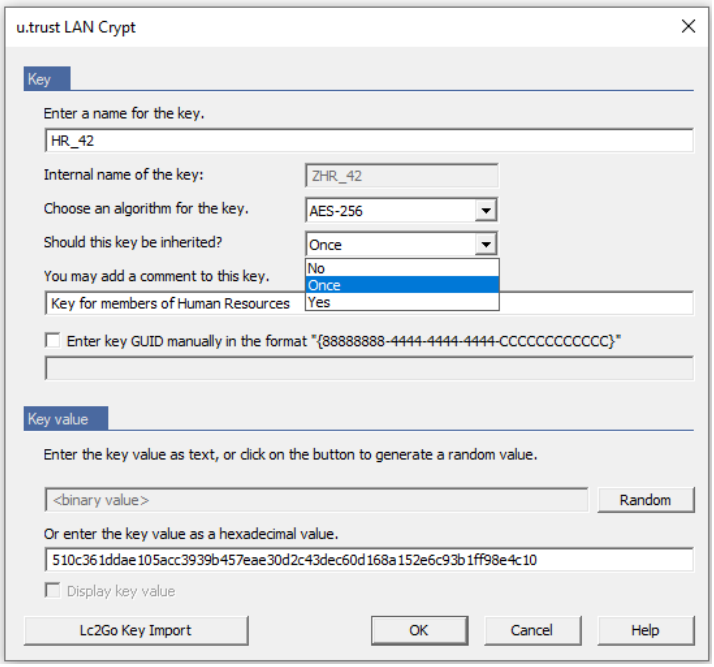
u.trust LAN Crypt's high degree of flexibility means it can easily be adapted to meet any company's security requirements.

Even so, it is very important that a company-wide security strategy has been defined before you create the *u.trust 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 *u.trust 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 **Central Settings \ All u.trust LAN Crypt keys**. However, they cannot be processed there. This view is an overview of the keys used in *u.trust LAN Crypt*. **Keys can only be edited in the groups in which they were created.**

Note: A Security Officer 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 *u.trust 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 *u.trust LAN Crypt* can also sort keys.

  u.trust 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-256, AES-128, 3DES, DES, 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 *u.trust LAN Crypt* installations (see ”*The Keys tab*“ on page 50).

  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. *u.trust 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.

Here you can only see the algorithms that you have made available in the **Central Settings**.

Note: Please always choose a secure algorithm, such as **AES-256** or **AES-128** to encrypt your data, as encryption algorithms such as XOR, IDEA, DES or 3DES are no longer considered secure!

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 u.trust LAN Crypt calculate a value.
9. Click **OK**.

   The new key is displayed in the Administration Console.

3.15.1 Lc2Go Key Import

You can import keys from files encrypted with *Lc2Go*. To do this, click on the **Lc2Go Key Import** button. Then select a file encrypted with *Lc2Go* whose key you want to import to u.trust *LAN Crypt*. If necessary, click **Browse** ("**...**") if you want to select and import the file encrypted with *Lc2Go* from a specific path using the file explorer.

Enter the associated passphrase (the secure password) for that file in the **Passphrase** input field.

The imported *Lc2Go* key is displayed in the Administration Console and can be used for encryption rules.

3.15.2 Specific keys

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

<USERKEY>

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.

Example: 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.

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 the node **Central Settings**, **All u.trust 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 the node **Central Settings**, **All u.trust LAN Crypt Keys**, by clicking on the context menu *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.

Example: A user is imported from Active Directory into the *u.trust 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 *u.trust LAN Crypt* Administration Console and re-import it, *u.trust 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 *u.trust 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\`

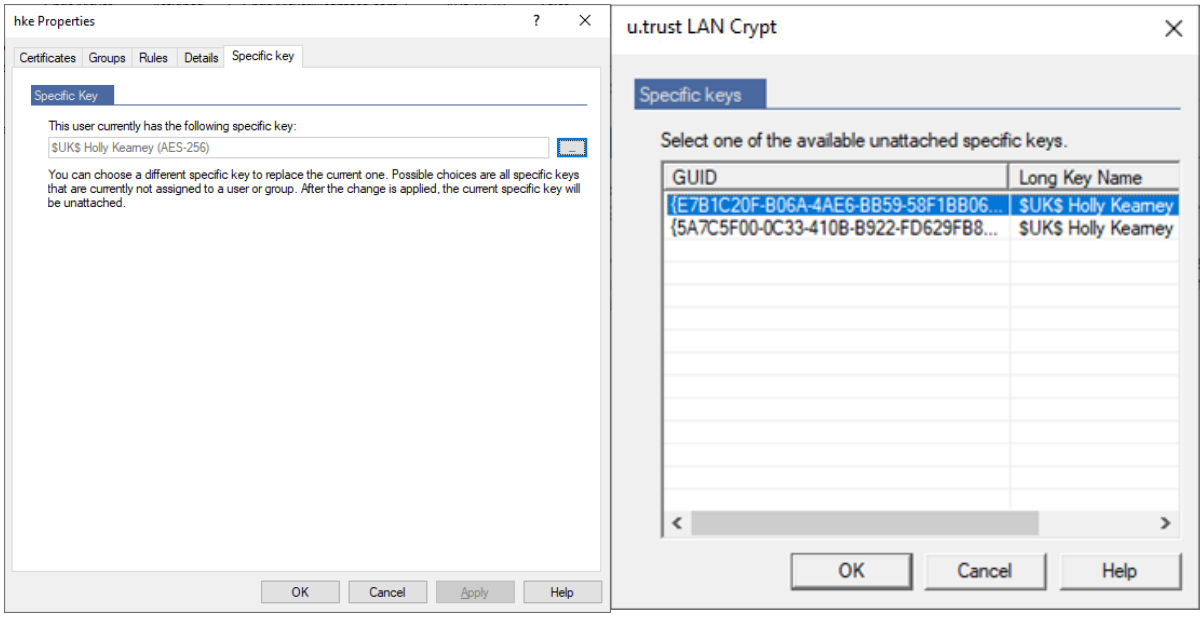
`Utimaco\`

`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.



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 Security Officer 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.

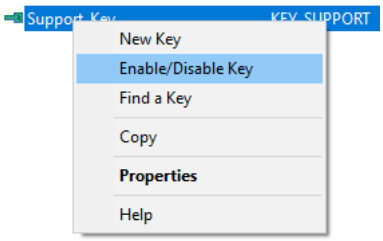
If the current specific key was replaced by a different one, it remains in the database as a non-assigned key.

3.15.3 Making Keys Active/Inactive

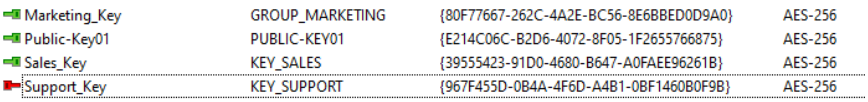
In *u.trust LAN Crypt* you can toggle an existing key to make it inactive. If you do this, this key is no longer available when you define encryption rules.

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 **Enable/Disable Key** 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.

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**

- **Create Keys**

  and

- **Copy Keys**

  in the target group.

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

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 u.trust 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 u.trust 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** permission. The key is actually added to group; it is not a shortcut.

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

3.15.6 Deleting keys from the database

Under the following conditions keys can be actually deleted (under the node **All u.trust 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.

Note: You cannot change the inheritance setting of a key in the **All u.trust LAN Crypt keys** node.

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 *u.trust LAN Crypt*.

Note: To edit a key, the Security Officer must have the group specific **Create Key** permission 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 key value** 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.

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

3.16 Encryption rules

The *u.trust 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.

Note: Please note that in addition to the path specification for an encryption rule, the file pattern must also be specified in the field below. You can also use wildcards (e.g. "*.*") here.

Note: With the new "*multi-policy support*" feature which is available since *u.trust LAN Crypt* version 11.0.0, loading more than one profile file for users is also supported using the u.trust LAN Crypt API. We will be happy to provide you with further information on request. Please contact Utimaco-Support for more details.

The encryption rules defined for a group make up one *u.trust 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 drives, removable media (such as USB flash drives), optical drives, network shares, folders (including sub-folders), 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 *u.trust 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 node **Encryption Rules and Tags**. 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.

The Path, key selection and various options are summarized in a dialog so that an encryption rule can be easily created. Encryption rules can be changed later as required, e.g., if the previously selected algorithm for a key no longer meets the required security requirements. In this case the previously used key (e.g., with IDEA algorithm) could be replaced by a new key with used a higher security algorithm (e.g., AES-XTS 256 bit). After performing an initial encryption, all existing files would then be encrypted with the new key and higher security algorithm.

Note: If a previously used key is to be replaced by another key for an existing encryption rule, the old key must remain in the possession of the user. The old key is then required for the re-encryption of existing encrypted data that is still encrypted with this key. To do this, assign the old key as *key without path* to the respective users (see "*key without path*" on page 148).

Note: Utimaco generally recommends encrypting all data according to AES with a key length of 256 bits. Data that is still encrypted with an outdated algorithm (e.g., DES, 3DES, IDEA, XOR) should definitely be re-encrypted to AES 256 bit as soon as possible for security reasons.

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.

Note: Please note that encryption paths must not be longer than 259 characters.

Relative paths:

u.trust 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"* folder in the ROOT directories.

  For example, these would be the following folders:

  C:\my_data*.*
  D:\my_data*.*
  F:\my_data*.*
  Z:\my_data*.*

- **Entry:** `my_data\*.*`

  encrypts **EVERY** "*my_data"* folder.

  Example:

  C:\company**my_data*.***

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

In both cases all files in the "**my_data**" folders are encrypted.

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

Default folders

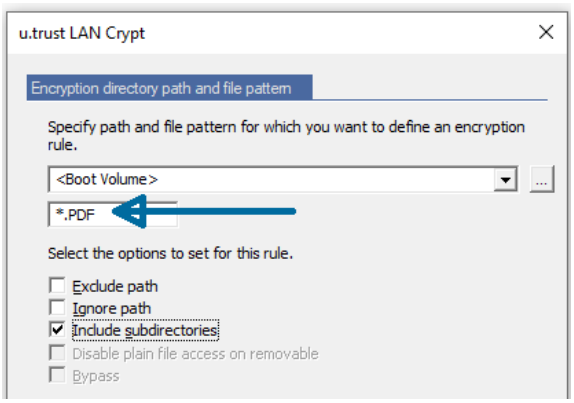
To facilitate the encryption of user specific folders, *u.trust LAN Crypt* supports the default directories predefined by Windows (for example <*Application Data*>, <*Common Documents*>, <*My Documents*> etc.). The Security Officer therefore does not have to consider system-specific variations in client configuration. *u.trust 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.

Boot Volume

By selecting the <*Boot Volume*> option, you can encrypt files located on the system drive (where Windows is also installed). After selecting this option, you can also customize the predefined entry "*.*" (this applies to all files) in the input field as well.

Example:

For example, if only PDF files are to be encrypted on boot volumes, change the entry in the input field as follows:



You can also encrypt additional file types or only specific files (such as "confidential.txt") on the boot volumes. To do this, create another new rule and change the entry in the input field in the same way as described above.

All local drives

The <*All local drives*> option allows you to create a rule that applies only to all locally installed drives. These could be, for example, built-in hard drives (including multiple drives), removable and optical drives.

Opticals

The <*Opticals*> option allows you to create a rule that applies exclusively to optical media. You can thus define that, for example, data burned to a CD, DVD or Blue Ray is always automatically encrypted by *u.trust LAN Crypt*. Only users who are in possession of the corresponding key can then read this data later or share it with each other.

Network Shares

By selecting the <*Network Shares*> option, you can create a rule that applies to all network shares to which the user has access. It does not matter whether the network share is a drive letter or a UNC path.

Removables

By selecting the <*Removables*> option, you can create a rule that applies to all removable devices. For *removables drives*, you can also optionally deny access to plain text files stored there (see “Disable plain file access on removable” on page 143).

Note: Note that <*Removables*> refers to all externally connected storage media (e.g., USB sticks, external hard drives etc.). This then also applies to externally connected optical drives. In addition, removable devices also belong to the local drives.

Local fixed drives

You can create a rule that applies to all locally built-in hard drives by selecting the <*Local fixed drives*> option.

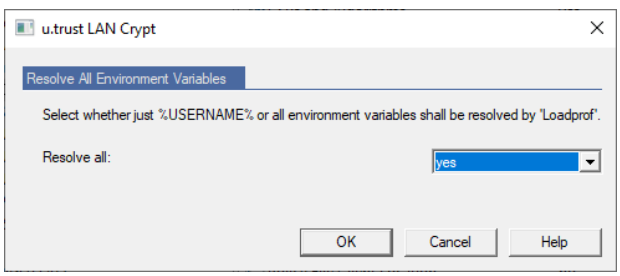
Environment variables

u.trust 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 *u.trust LAN Crypt (*excluding paths of **Bypass Rules**).

Additional folders can be specified in *u.trust LAN Crypt* by entering the environment variable:

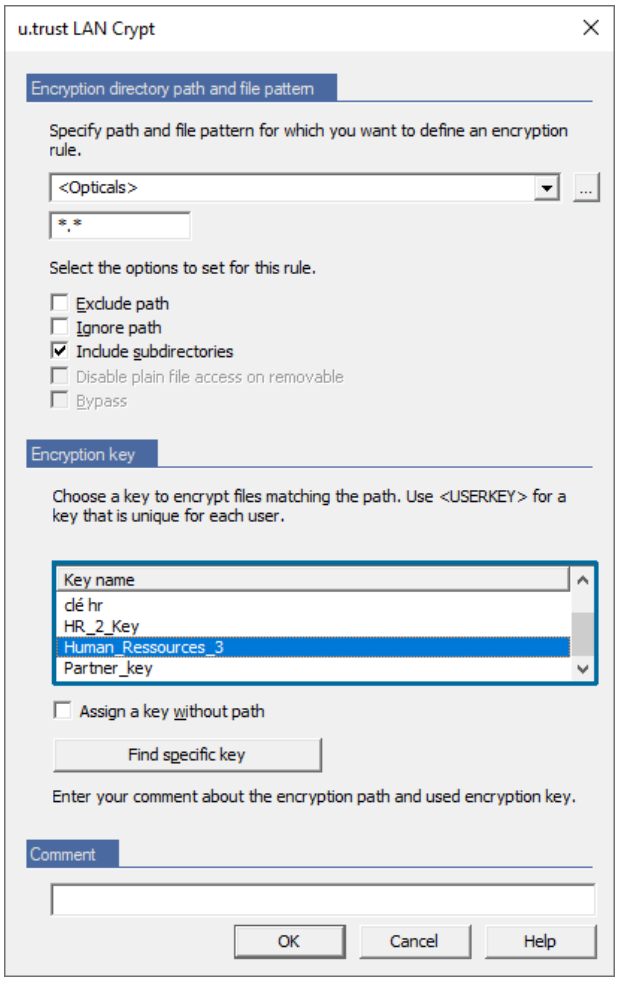
Environment variable:	Example:
%ALLUSERSPROFILE%	C:\ProgramData
%APPDATA%	C:\Users*username*\AppData\Roaming
%LOCALAPPDATA%	C:\Users*username*\AppData\Local
%PUBLIC%	C:\Users\Public
%USERPROFILE%	C:\Users\username

To resolve these environment variables in the *u.trust LAN Crypt* Client, this has to be set in the *u.trust LAN Crypt* Configuration (see chapter “*Resolve all environment variables*“ on page 177).



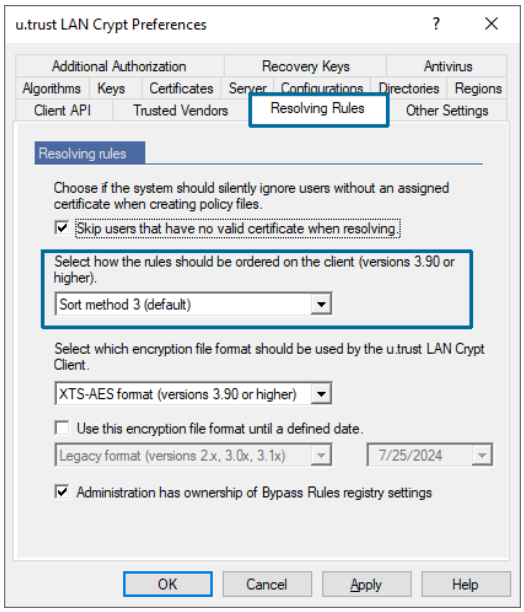
3.16.2 Keys

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, *u.trust LAN Crypt* sorts the encryption rules according to the method you selected on the **Resolving Rules** tab (see "*Sort methods*" on page 52) in the node **Central Settings**:

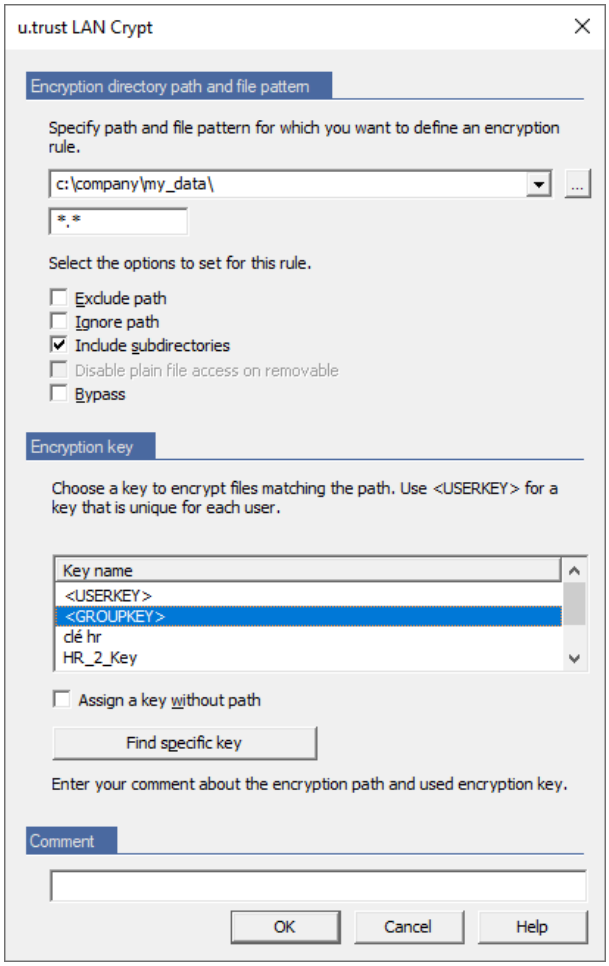


3.16.4 Generating encryption rules

Encryption rules are always generated per group. They consist of a path and a key and are created in the node **Encryption Rules and Tags**. If you are seeking a particular group, you can also use the function **Find Group**.

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* or select one of the predefined templates.

3. If you want the new encryption rule to apply to all files in the selected path, enter "`*.*`" as the file pattern in the input field below. If, on the other hand, you want the new rule to apply only to certain file types, enter "`*.docx`" (for Word files only) or "`*.txt`" (for text files only) as the file pattern there, for example. The use of jokers (*) and wildcards (?) in file names (but not in the rest of the path) is allowed (e.g. "`*.d??`" or also "`*.d*`"). If necessary, click the **Browse button** ("**...**") to select a path.

Alternatively, you can select one of the predefined paths of Windows default folders (e.g., My Documents etc.), local drives, network shares or drive types (e.g., removable, optical etc.) contained in the list box. The correspondingly selected predefined path is then displayed in the input field.

Additional information on the predefined paths can be found at the beginning of this section, starting on page 137.

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 folders with names longer than 8 characters, you must use 8.3 notation to specify the encryption paths.

You must 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.

4. Five options appear under *Encryption directory path and file pattern*:
   - Exclude path
   - Ignore path
   - Include subdirectories
   - Disable plain file access on removable
   - Bypass

Include subdirectories

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

Example:

Entry: `c:\company\my_data\*.* Include subdirectories`

This encryption rule encrypts all the files in:

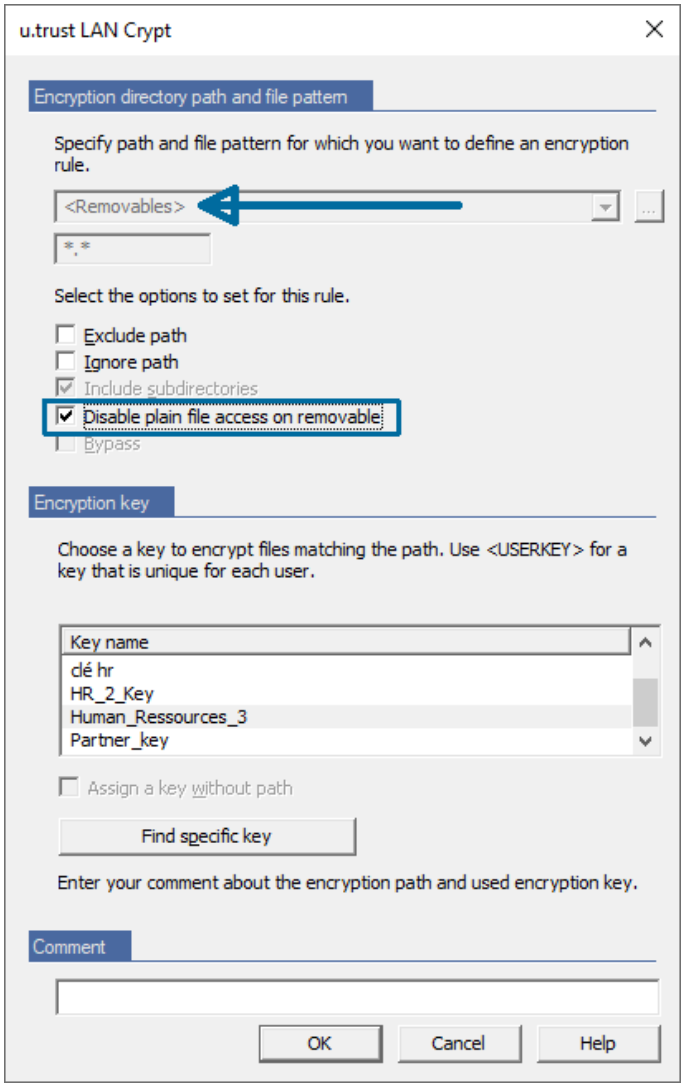
C:\company\my_data

C:\company\my_data\project X

C:\company\my_data\project X\demo

Disable plain file access on removable

This option is only available for encryption rules that have *<Removables>* set as the predefined path. If you have set the **Disable plain file access on removable** option, access to unencrypted files (plain files) stored on removable media (such as for external hard disks, USB sticks, etc.) for which an encryption rule exists is denied. Such files can then neither be read nor opened by the user.



By setting the **Disable plain file access on removable** option, you can, among other things, prevent unauthorized software from being installed from removable media, such as USB sticks.

Note: As soon as you enable this option, the **Include subdirectories** option for the encryption rule is automatically set as well.

Note: You must assign a key to this encryption rule.

Exclude paths

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

This option can be used in an encryption rule to exclude individual files, file types or subfolders of a path for which an encryption rule already exists from encryption. This is achieved by activating the **Exclude path** option in the new encryption rule dialog. This means that the files specified in the encryption rule are not encrypted. You can also change this for existing encryption rules by selecting an existing rule with a double click or via the *Properties* context menu.

Example:

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

First line:

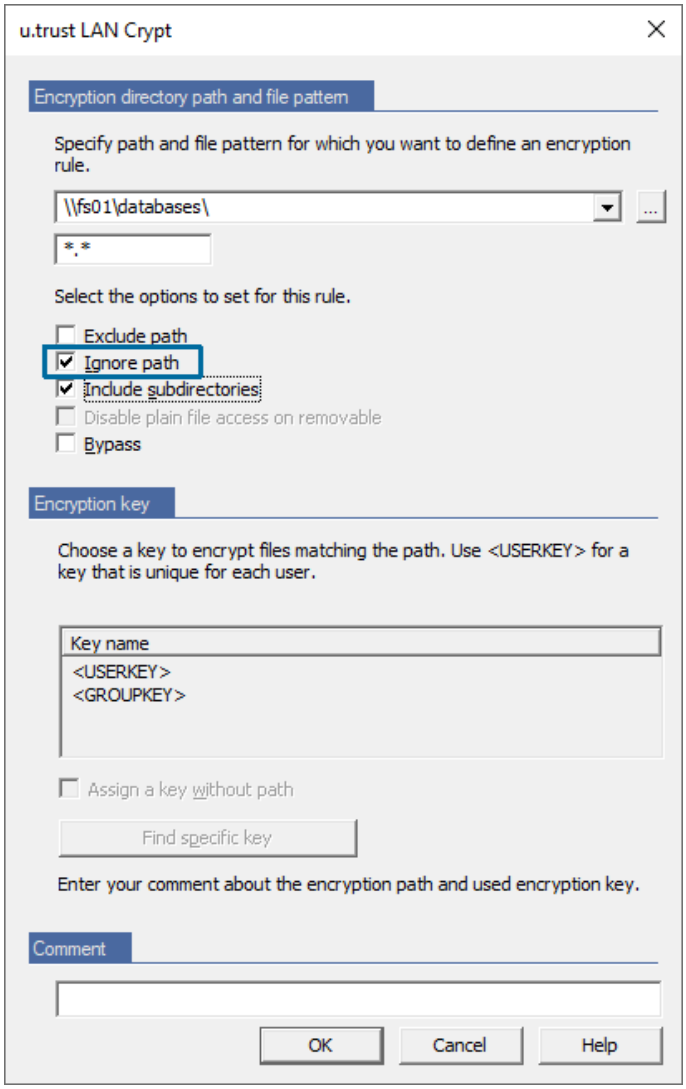
Entry `C:\MYDIR\*.TXT`, **Exclude path**, no key: excludes all files with the file extension `.TXT` in the *MYDIR* folder from encryption.

Second line:

Entry `C:\MYDIR\*.*`, **Exclude path** not selected, encrypts all files in the *MYDIR* folder (**except *.TXT files**) with the specified key.

Ignore path

u.trust LAN Crypt includes the **Ignore path** option. *u.trust 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 folders that are excluded from encryption to see whether or not they are actually encrypted. In this way *u.trust LAN Crypt* can discover whether files in folders of this kind are encrypted or not. You cannot access encrypted data. *u.trust LAN Crypt* simply ignores files in folders for which the **Ignore path** option has been selected! *u.trust LAN Crypt* does not check them, and users can access encrypted files.

Note: At this point we would like to point out that legacy and mini filter drivers sometimes behave differently with the *u.trust LAN Crypt* Client. While the **Ignore path** rule for a folder means that the access protection for files is also deactivated when the mini filter encryption driver is activated, the access protection for files still exists in such folders, if the legacy filter encryption driver is activated (only older *LAN Crypt* clients).

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. The installation location of *u.trust LAN Crypt* or that of Windows itself is also ignored by the encryption. In principle, no files can be encrypted or decrypted in locations for which the **Ignore path** option has been selected. These files are completely ignored by *u.trust LAN Crypt*.

Bypass

With this option you can create a **Bypass Rule** in *u.trust LAN Crypt*. All paths for which such a rule exists are completely ignored by the u.trust *LAN Crypt* mini filter driver. Files located in such paths can neither be encrypted nor decrypted there. In comparison with the **Ignore path** option, file accesses are not monitored at all by the mini filter driver in paths for which a **Bypass Rule** applies.

Note: This function is available at this point only if you have enabled the **Administration has ownership of Bypass Rules registry settings** option in the **Central Settings** node, in the **Resolving Rules** tab (see "*Administration has ownership of Bypass Rules registry settings* on page 55).

Note: Network drive letters and Environment variables are not supported in **Bypass Rules**.

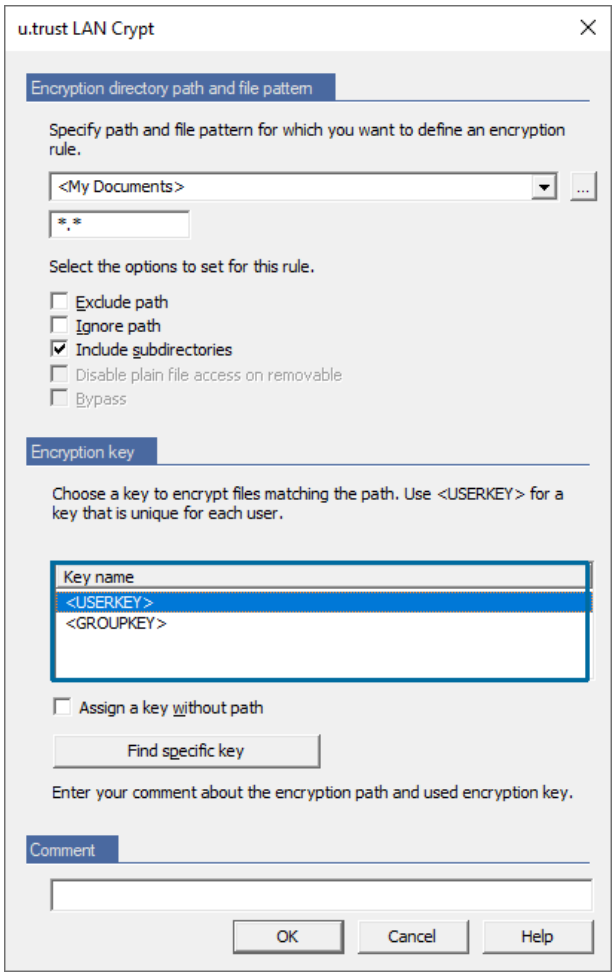
Note: As soon as you enable this option, the **Include subdirectories** option for the encryption rule will also be automatically set as well.

Note: After setting or removing a **Bypass Rule**, you must restart the client computer.

WARNING: Activate this option only if an Utimaco support employee has asked you to do so!

If you want to create an encryption rule with a key, perform the following additional steps:

5. Select a key from the list.



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

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

<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!

Example: 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. A *key without a path* is usually also required to re-encrypt data, and always when there is no longer an encryption rule for this (old) key (see also the note in the section "*Encryption rules* on page 135).

If a key is assigned 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**.

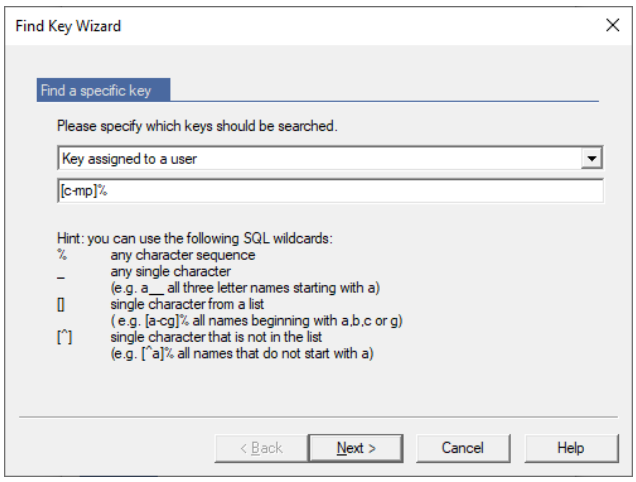
The new encryption rule is displayed in the *u.trust LAN Crypt* Administration.

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

Note: Encryption rules can only be changed in the groups in which they were created.

3.16.5 Find a specific key

Press the **Find 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's name or logon name in the edit field (search condition). To perform a wildcard search, you can use SQL wildcards. For example, "Peter%" finds all keys assigned to users whose user or logon names begin with "Peter").

- **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.

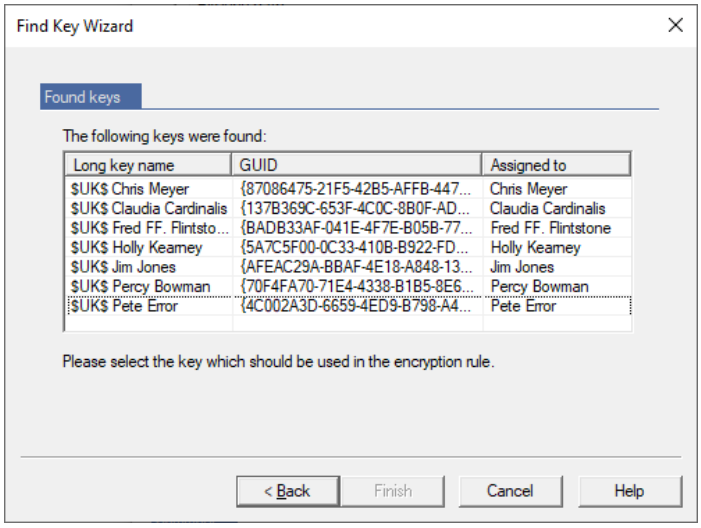
- **Key GUID**

  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's 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 *u.trust LAN Crypt* Client API to encrypt these files. In *u.trust LAN Crypt* Administration, you can define different encryption tags that specify the *u.trust 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.

An example of how to use a reference to a key would be:

```
SGFEAPI encrypt /Tag:CONFIDENTIAL c:\documents\financial-figures.docx
```

Encrypts the financial-figures.docx file in the c:\documents folder using the key associated with the *<CONFIDENTIAL>* tag.

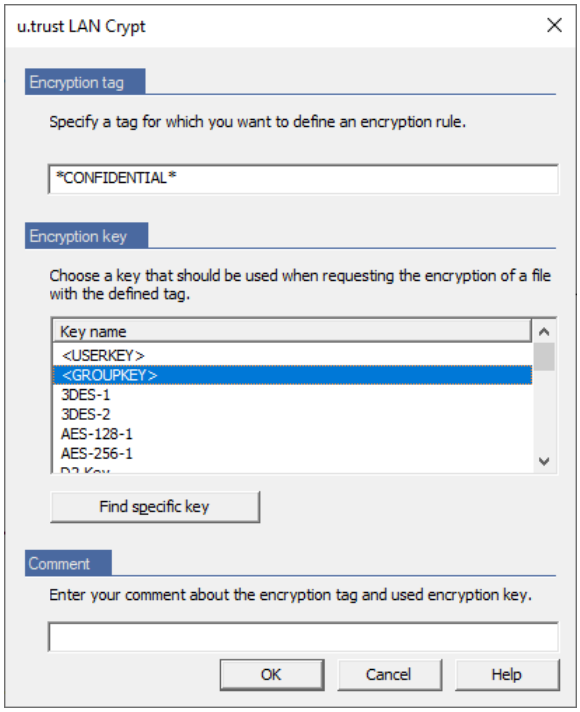
To generate an encryption tag

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.



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

Note: In the default view, only the placeholders for <USERKEY> and <GROUPKEY> and the keys created by a Security Officer are displayed. With the **Find specific key** button you can search and display the specific keys (see previous chapter on page 149).

<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 *u.trust 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 *u.trust LAN Crypt* Administration, via their certificate.

Via the *u.trust LAN Crypt* Administration each user is assigned a certificate (*.p12 file). This file also contains the private key. The private key is protected against unauthorized access by PIN. *u.trust LAN Crypt* writes the corresponding PIN into the password log file (`p12pwlog.csv`). This file should always be specially protected against unauthorized access. To realize this, the (Master) Security Officer on the *u.trust LAN Crypt* Administration could install the *u.trust LAN Crypt* Client application and create an encryption rule for the password log file.

Note: If you install both *u.trust LAN Crypt* components, *Admin Console* and *Client application* on the same computer, they must be of the same version.

Alternatively, you can also use certificates from a PKI. It is recommended that the certificates are already available for use in the certificate store or in 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.

u.trust LAN Crypt has a *Certificate Assignment Wizard* that assigns certificates automatically.

Note: If a Security Officer who create certificates has no permission to change the password log file in the file system, no *u.trust LAN Crypt* certificates can be generated.

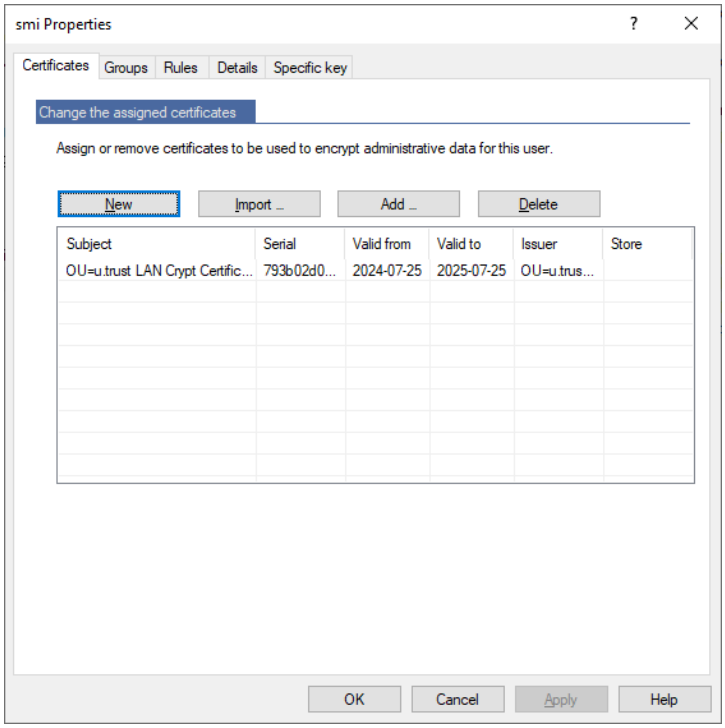
3.18.1 Assigning a certificate to a user

To assign a certificate, proceed as follows:

1. Select **Members and certificates of 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 *u.trust LAN Crypt* to generate a new certificate for the user. If no certificates are available, the *u.trust LAN Crypt* Administration Console can even generate certificates itself. However, only *u.trust LAN Crypt* should use these certificates!

  The certificate it generates is saved as a PKCS#12 file in the default directory (see the **Directories** Tab in the **Central Settings** node).

  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.

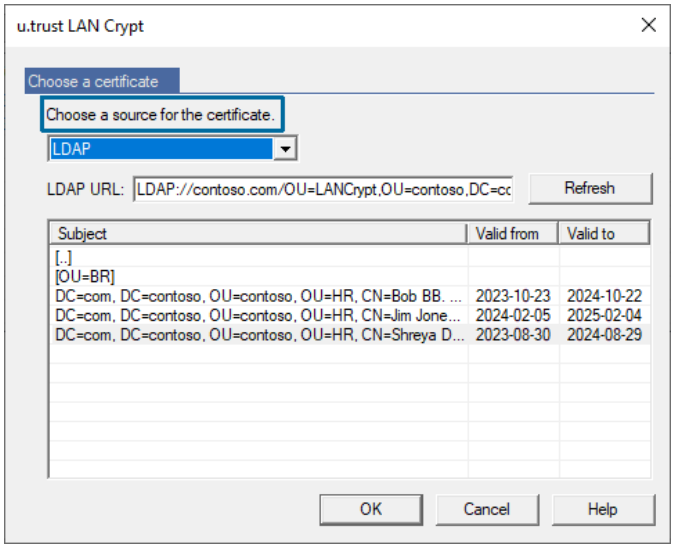
In this case click **Import …** The system opens a dialog in which you can select the required certificate. Then click **OK**, and the system assigns the certificate to the user.

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 …**

Select the source for the certificate:



Assigning Certificates from the certificate store

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

u.trust 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 source for the 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,OU=Sales) on the Server tab in the **Central Settings**.

Note: 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).

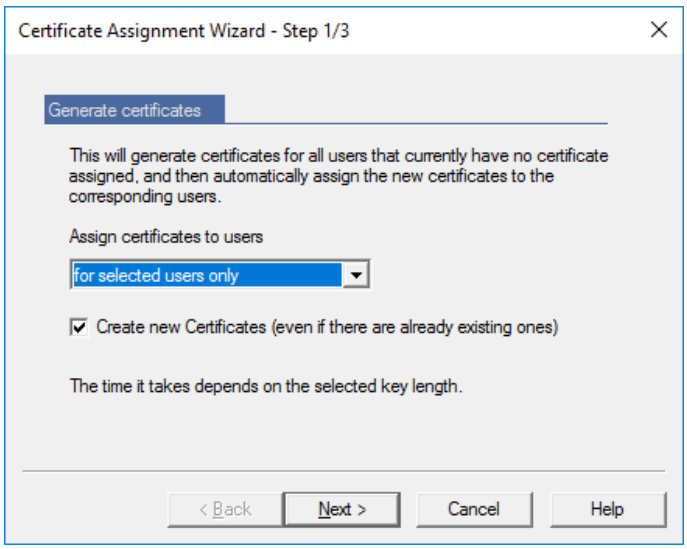
   Note: The Certificate snap-in is available under each user/group node. Here the system only displays the users that are members of the relevant group.

3.18.2 Generating and assigning u.trust 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 **Create Certificates** in the context menu for each *Members and certificates of 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**.



If you check the **Create new Certificates (even if there are already existing once)** option, new certificates will be created for all selected users.

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 *u.trust LAN Crypt* Configuration you specify the folder in which *u.trust 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 *u.trust LAN Crypt* can automatically recognize the user key files.

When *u.trust 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.

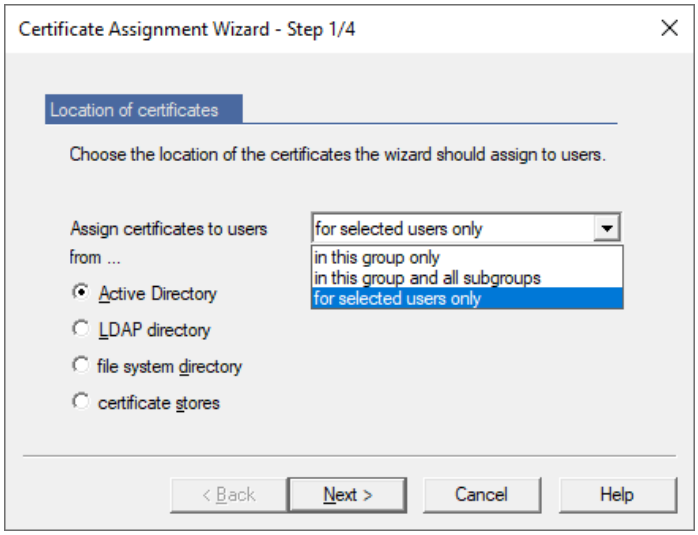
If *u.trust LAN Crypt* finds a **.cer* file that contains the public part of the Security Officer's certificate, it automatically imports it.

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.

3.18.3 Certificate Assignment Wizard

u.trust 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 of 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

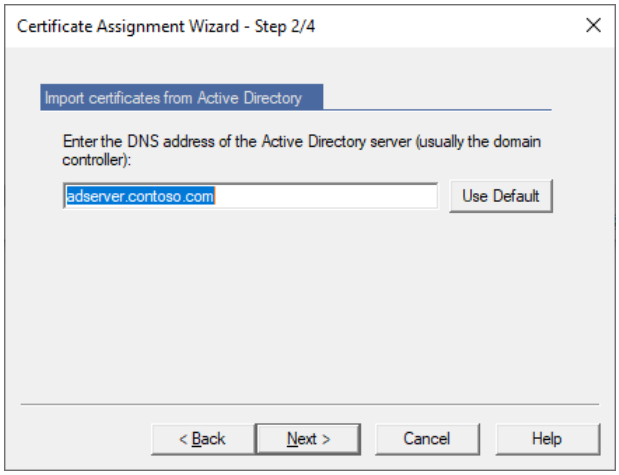
This option is only displayed if one or more users are selected. When you click *Members and certificates of group* under the desired group node in the left-hand console pane, the members of the group are displayed in the right-hand console pane. Selecting the users works the same way as in Windows Explorer (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 to users from the **Active Directory**
- Assign certificates to users from an **LDAP directory**
- Assign certificates to users from a **file system directory**
- Assign certificates to users from the **certificate store**

3.18.3.1 Assigning certificates from the Active Directory

If you have selected the option *Assign certificates to users from Active Directory*, you must enter the name of an Active Directory controller in FQDN form in step 2 (for example: "`adserver.contoso.com`").



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.

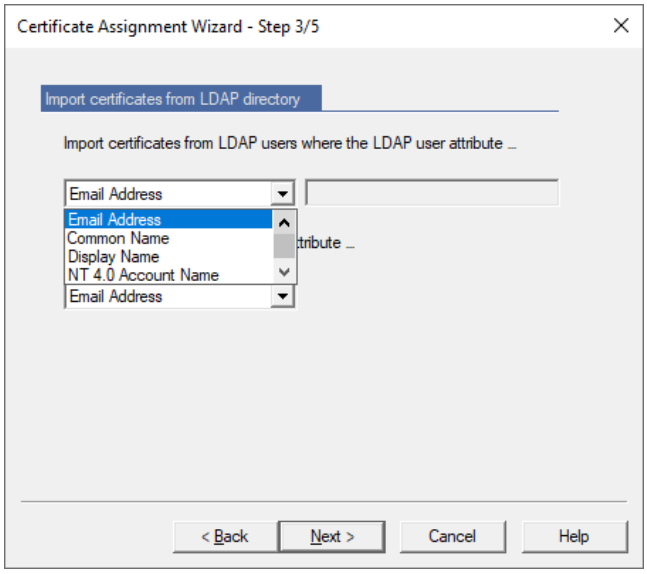
3.18.3.2 Assigning certificates from an LDAP directory

If you select the **Assign Certificates to users 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.

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=COM`
Example 2: `OU=marketing,DC=mydomain,DC=COM`

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 *u.trust LAN Crypt* user.



The following LDAP user properties can be used:

- Email Address
- Common Name (CN)
- Display Name
- NT 4.0 Account Name
- User Principal Name (UPN)
- Surname
- <other>, user-defined attribute

You can specify that these properties match the following *u.trust LAN Crypt* user properties:

- Email Address
- User Name
- Logon Name
- Comment

Select the LDAP user property you want each *u.trust LAN Crypt* user property to correspond to.

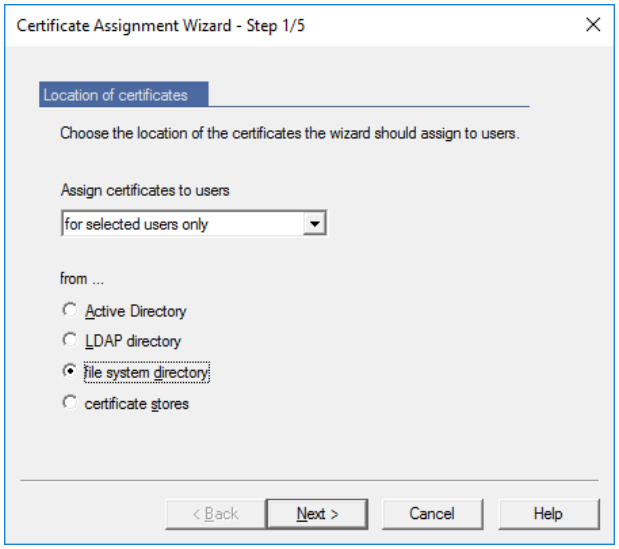
If these properties match, the system imports the LDAP user's certificate and automatically assigns it to the appropriate *u.trust LAN Crypt* user.

Note: To prevent inconsistencies, we recommend that you use the *Email Address* as an assignment criterion, as it is always unique.

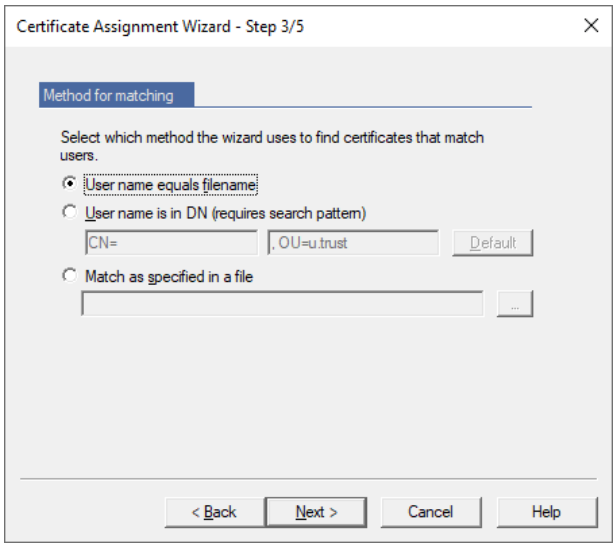
To start the wizard, click **Next**. The system imports and assigns the certificates automatically. It displays a message to confirm that it has successfully assigned the certificates. Click **Finish** to close the wizard.

3.18.3.3 Assigning certificates from a directory

If you select the **Assign certificates to users from a file system 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 *u.trust LAN Crypt* is to use to assign certificates to the users.



- **User name equals filename**

  Select this option, if the file names of the certificate files are identical to the user's name.

  All users that correspond to a file name are assigned to the appropriate certificate.

- **User name is in DN (requires search pattern)**

  If the user's name is contained in the certificate's *Distinguished Name*, *u.trust LAN Crypt* can find it and assign the certificate to the appropriate user. *u.trust LAN Crypt* uses a search pattern to identify the user's 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's name that appears between the two specified character strings in the DN.

  Example:

  In the certificate, the user's name is always present under "CN=".

  (e.g. `CN=DSmith,OU=Utimaco`)

  If you enter `CN=` in the first input field and `OU=Utimaco` in the second input field, LAN Crypt will find the user's name that is located between these two-character strings (in our example, DSmith). 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 Utimaco Smartcard Administration is saved in a file in a pre-defined directory. Utimaco 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:

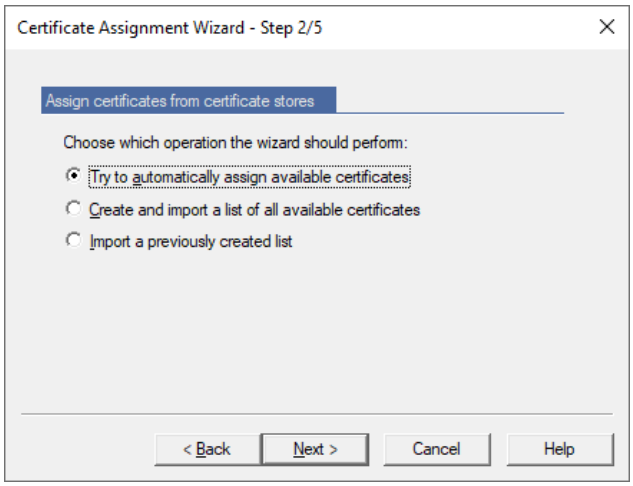
```
Guest;Guest.cer
DSmith;DSmith.cer
....
```

The system assigns the certificates in accordance with the assignment in this file.

Click **Next** to start the wizard and automatically assign the certificates.

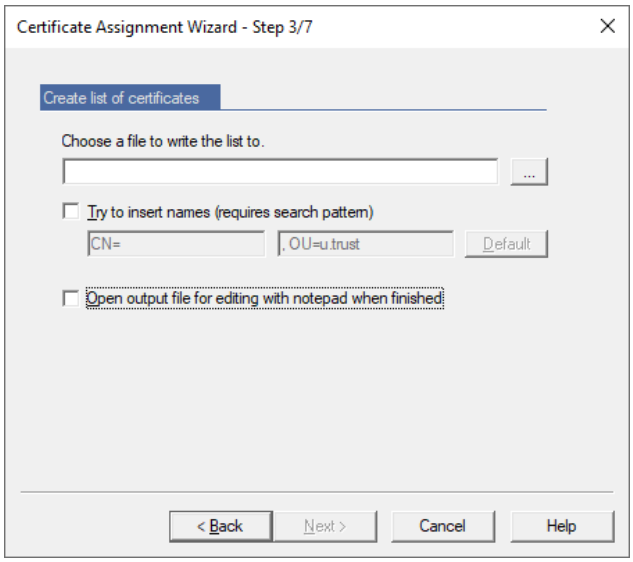
3.18.3.4 Assigning certificates from certificate stores

If you have selected the **Assign certificates to users 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. *u.trust 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.



Choose a file to write the list to.

u.trust LAN Crypt creates a list of all certificates available in the certificate stores. This list contains placeholders for the usernames to which the certificate is to be assigned.

Example:

```
*****; My; OU=u.trust 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 usernames.

If the certificate contains the user's name, you can use the following option:

- **Try to insert names**

  u.trust LAN Crypt can try to recognize a user: if the certificate's *Distinguished Name* (DN) contains the user's name, *u.trust LAN Crypt* can find it and assign the certificate to the appropriate user. *u.trust LAN Crypt* uses a search pattern to identify the user's 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's name that is found between the two specified character strings in the DN.

Example:

In the certificate, the user's name is always present under "CN=".

(e.g. `CN=DSmith,OU=Utimaco`)

If you enter *CN=* in the first input field and enter *OU=Utimaco* in the second input field, *u.trust LAN Crypt* will find the user's name that is located between these two-character strings (in our example, DSmith). The system replaces the placeholder with the user's 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's 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

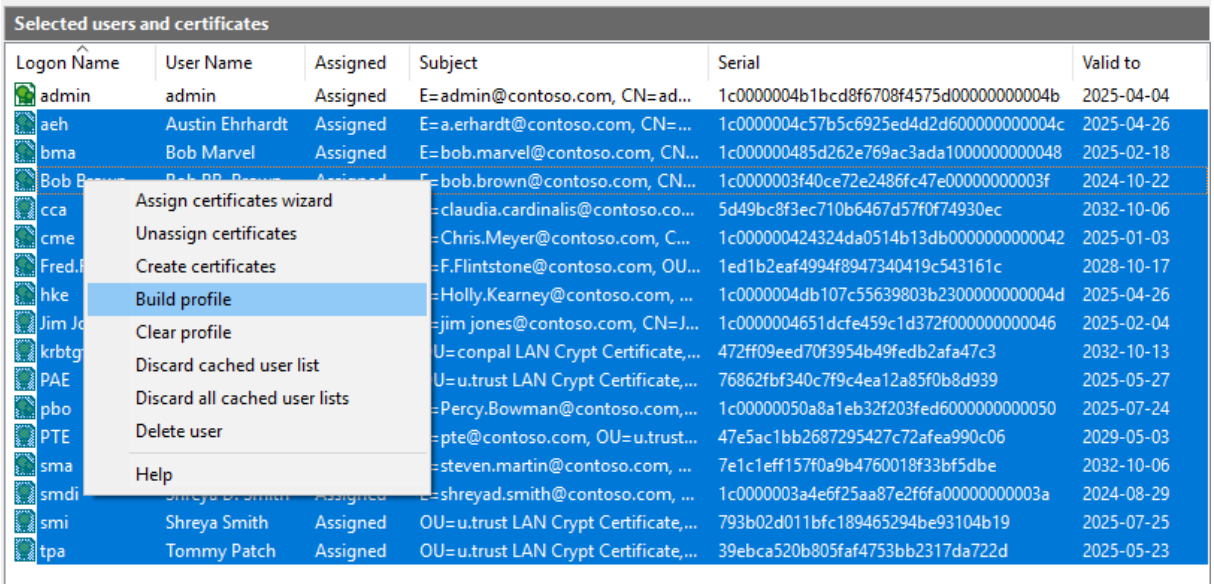
u.trust LAN Crypt saves every profile that has been generated (or changed) in its Administration Database. Here they do not yet have any effect on individual users.

To resolve individual profiles and build the policy files, a *u.trust LAN Crypt* Security Officer must run the *u.trust 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 *u.trust LAN Crypt* Administration console (added new keys, added new rules, *TrustBuilder MFA* ...). 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 profile** 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.

Note: If you choose the **Clear profile** option in the context menu, an empty profile is created for the user. After updating the profile via the *u.trust LAN Crypt* client, this user no longer has any encryption rules and keys available. Access to encrypted data is then no longer possible for this user. You can provide the user with a profile again at any time. Only when the profile is updated again via the *u.trust LAN Crypt* client does he receive his encryption profile with all the rules and keys defined for him and he can work with encrypted data again.

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:**

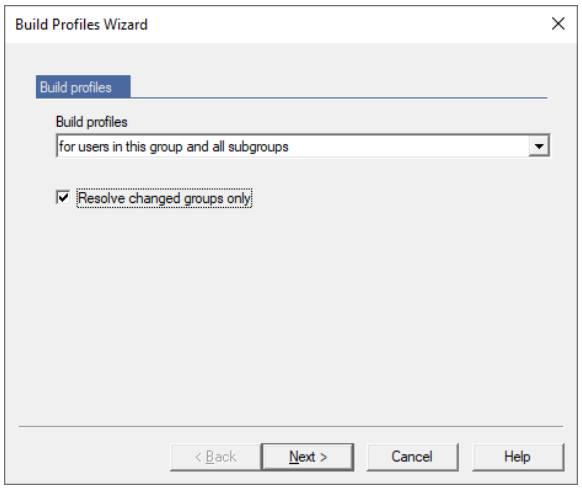
  If *Clear Profile* is started for multiple users. This action cannot be started for an entire group. No certificate checks are necessary.

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 user's 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 of Group** 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's 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 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 u.trust LAN Crypt* **Central Settings** define how profiles are cleared. The process for clearing profiles is similar to the one for building profiles.

3.20 Database logging

u.trust LAN Crypt logs events that are triggered by the *u.trust LAN Crypt* Administration Console in the *u.trust LAN Crypt* database. With *u.trust 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 Security Officer can see the settings for logging and the logged events.
Manage Logging	The Security Officer can change the settings for logging. They are allowed to archive, delete, and check entries.

Basic settings for logging can be made in the *u.trust 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** permission.

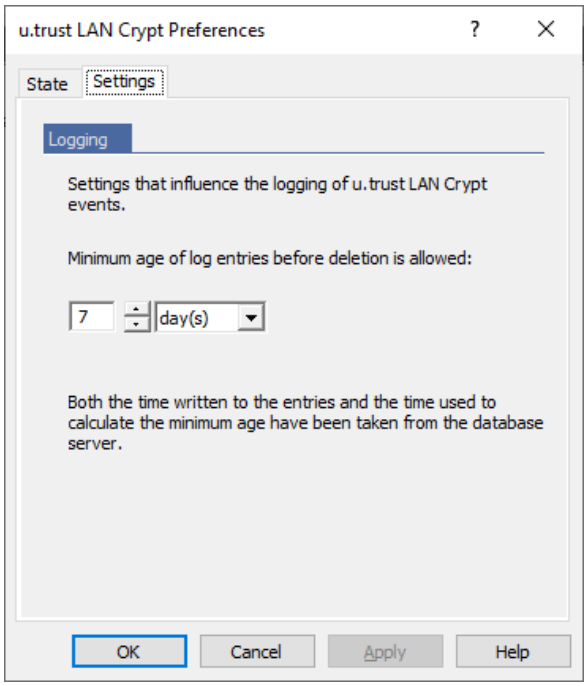
The basic settings can only be made by a Master Security Officer. They can be given additional security by adding a second level of authorization (scenario **Manage Logging**; requires the global permissions **Read Logging Entries** and **Manage Logging**).

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 Security Officer log 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

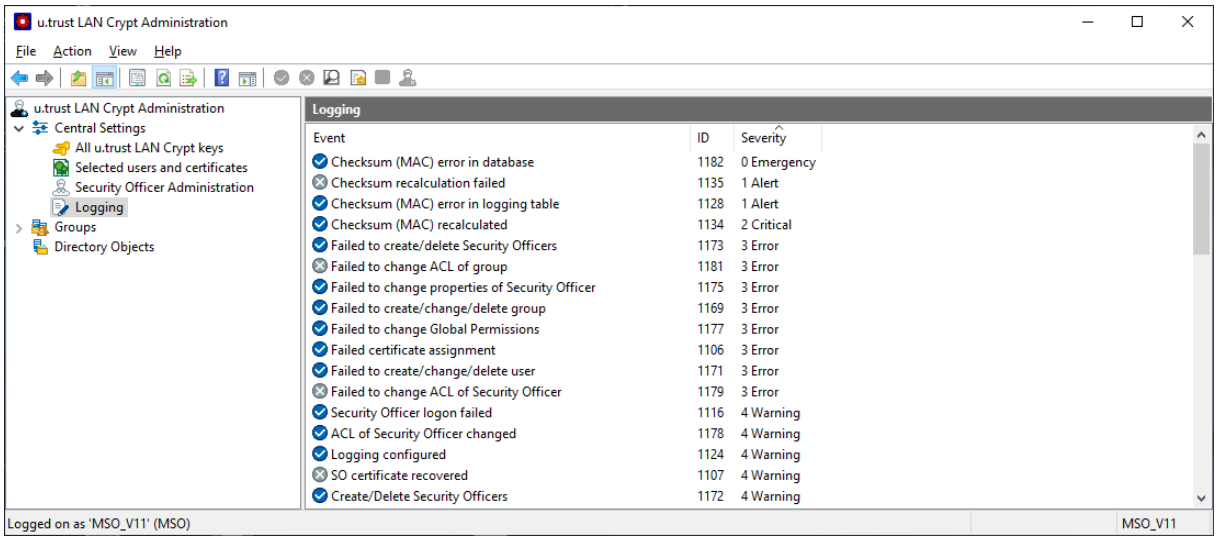
The **Status** tab displays information on how many entries have been logged. If there are several locations, the display is expanded per location. It also shows how many entries have already been archived and whether they can be deleted.

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.

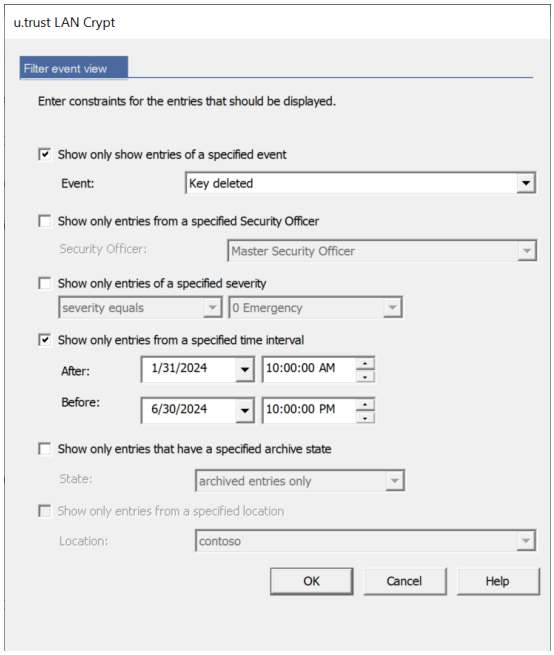
Double-click an entry to display details for that entry.

u.trust LAN Crypt also has a filter in which you can specify conditions for the displayed entries.

3.20.4 Filtering events

The settings for logging can be defined in the **Logging** node. A filter function is available for displaying and exporting the logged events. If the **Logging** node is selected, this can be defined via the context menu (right mouse button) or the **Action** menu via **View and export entries**.

Clicking on **View and export entries** in the **Logging** node opens a 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 (e.g., "*Key deleted*", "*Rule changed*", …).

- **Only show entries from 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. *Severity is less or equal* and *Severity 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 is 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.

Note: Even after executing the **View and export entry's** function, the filter can be defined by clicking the **Filter** button in the **View Events** dialog. Alternatively, this function is also available via the **View** menu and after selecting **Filter**.

3.20.5 Archiving, deleting, checking entries

Note: Security Officers require the global permission **Manage Logging** before they can archive, delete, and check entries.

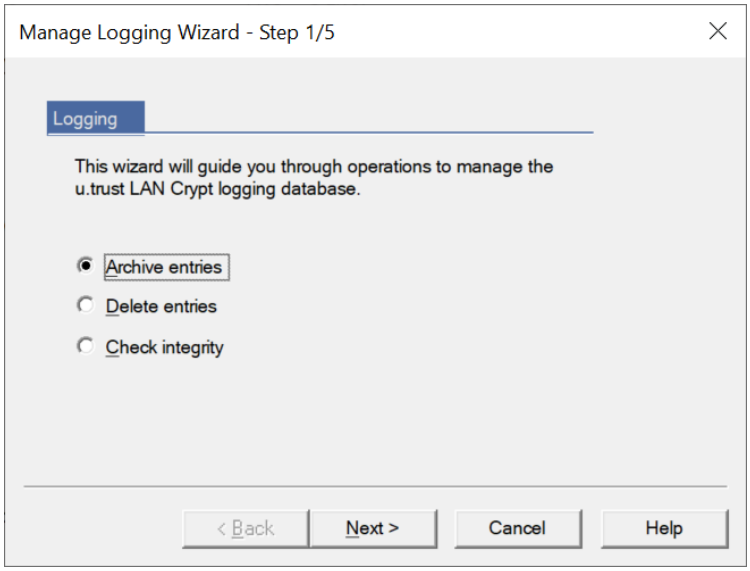
A Security Officer who has the global permission **Manage Logging** can archive, delete, and check logged entries.

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.

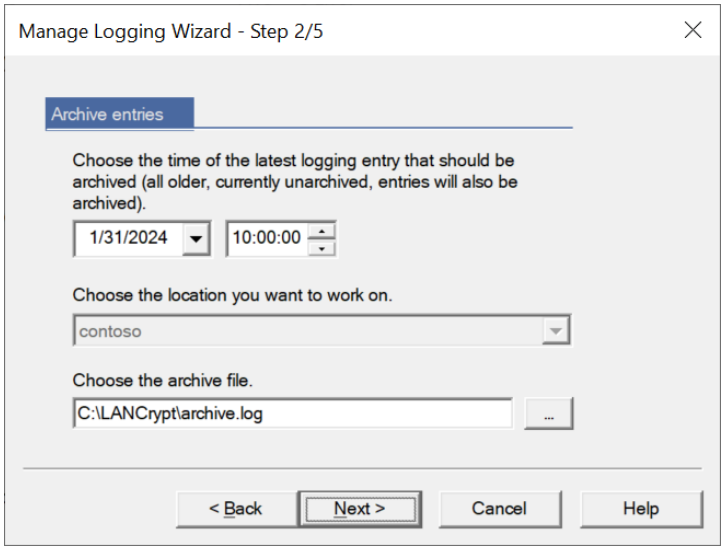
Archiving entries

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. In addition, at this point you can also archive by location (if available).



Note: Different locations are only selectable if you are working with a distributed database. Which locations are selectable at this point depends on how the database is replicated. Only one location is shown in the graphic above. The location is always the entry you defined during the installation of *u.trust LAN Crypt*. This entry cannot be changed afterwards.

- The name of the file in which the entries are to be stored.

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 entries

To delete archived entries, select *Delete entries* and click **Next**.

Please note: Entries that have not yet been archived cannot be deleted.

In the next dialog, specify:

- Date and time of the last entry from which point onwards deletion should take place. All previous log entries before this point in time (even if they have not yet been archived) will be deleted.

  Note: The last possible time depends on the specified minimum age of log entries, which you can define on the **Settings** tab of the **Logging** node.

- 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 integrity

To check the integrity of logged events, select *Check 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.

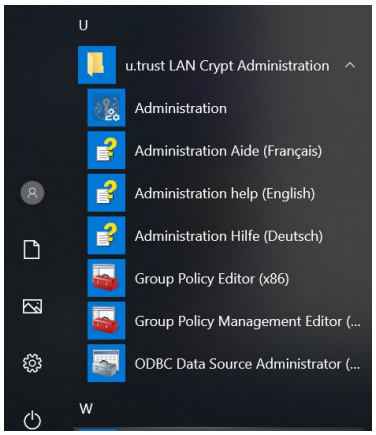
Click **Next**. In the next dialog you can see how many entries have been selected.

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 u.trust LAN Crypt Configuration

Note: Configuration settings must be defined with the 32-bit Group Policy Management Editor (*GPME.msc*) or the 32-bit Local Group Policy Editor (*GPEdit.msc*). Both editors are linked in the Windows Start menu under the folder **u.trust LAN Crypt Administration**. This ensures that the correct version is started.



Note: If you want to configure *u.trust LAN Crypt* group policies for a domain controller from a Windows 11 machine using a snap-in as an administrator, you must install the *u.trust LAN Crypt* administrative template files (see, among other things, the note on this page). On a supported Windows Server system, you can alternatively use the 32-bit Group Policy Management Console (*GPME.msc*) as an administrator.

The following settings are machine-specific or user-specific settings. To edit these settings, you need administrator rights in the domain 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 computer and user 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 / u.trust LAN Crypt*).

Note: As an alternative you can use the administrative template (**.admx* and **.adml*) provided in the \Config folder of your unzipped installation package. The ADMX files must be copied to the "`C:\Windows\PolicyDefinitions`" folder or - if available - to the Central Store. The respective language files (*.ADML), on the other hand, must be copied into the corresponding language sub folder (e.g. "`en-US`"). They will be read and checked for syntax the next time you open the Group Policy Editor. For more information about Administrative Template files, see: `https://learn.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store`

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 *u.trust 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.

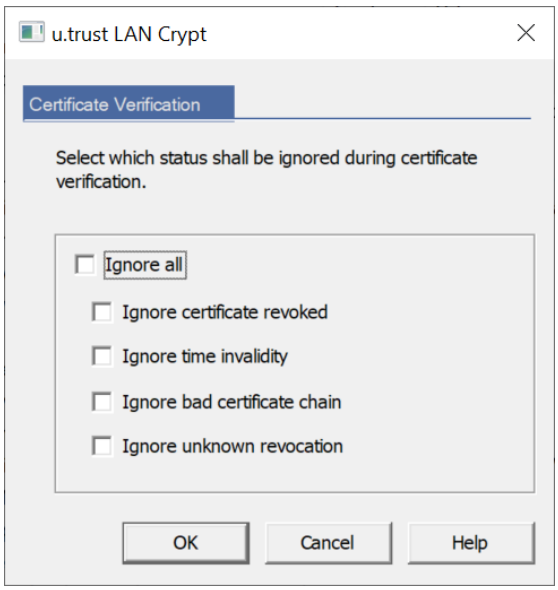
If you want to prevent this, you can specify here that this option is not displayed in the context menu for those files.

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 *u.trust 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 **C**ertificate **R**evocations **L**ist, 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. The *u.trust LAN Crypt* Client does not recognize an unknown revocation status, in accordance with RFC 5280. Therefore, give a different reason for revoking a certificate.

These settings can also be defined under Server Settings. Certificates are verified out both when a Security Officer logs on to the *u.trust LAN Crypt* Administration Console, and when an additional authorization is performed.

4.1.3 Resolve All Environment Variables

u.trust 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. In addition, environment variables could affect different paths depending on the Windows version.

Note: Environment variables are not supported in **Bypass Rules**.

4.1.4 Enabled Menu Entries

Here you can specify which menu options are visible in the *u.trust 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 encryption from being switched off (deactivated) on a client computer.

4.1.5 Default Ignore Rules

As the *u.trust LAN Crypt* driver is always loaded when you boot a workstation, all the files have already been checked to see 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 *u.trust LAN Crypt's* configuration you can configure the *u.trust LAN Crypt* driver to ignore specific drives or folders 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 *u.trust 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 consider that *u.trust 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 folders on the **C** and **D** drives until the user's encryption profile is loaded.

Even if you use *u.trust 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 *u.trust 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.

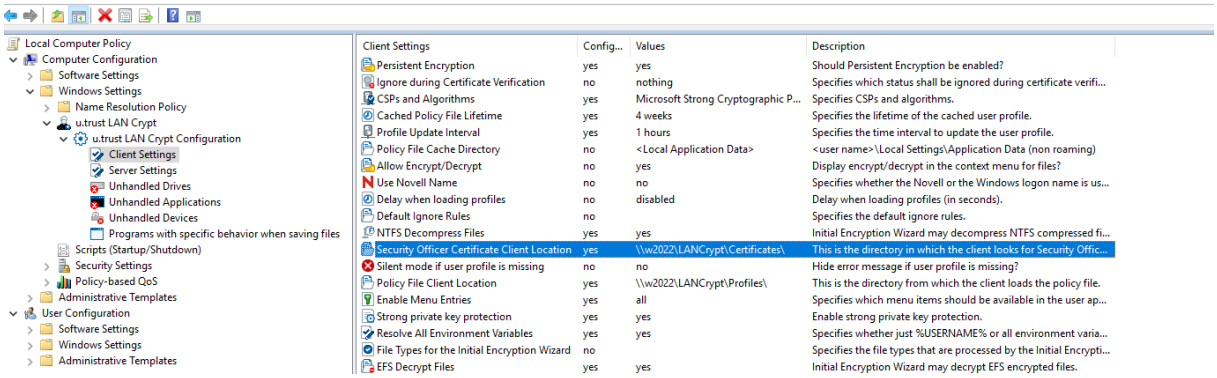
Note: Please note that the entries you define here also include all subfolders.

Note: Please note that during a new installation (not an update) of *u.trust LAN Crypt* the default 'Ignore rule' is predefined with the value "*". As a result, the specific access protection of *u.trust LAN Crypt* is inactive for all paths and files until the user's profile is loaded. Users may delete encrypted files during this period or when they have unloaded their profile. This is true even if they do not have a key for the files stored there.

You can change this, if you define a path for the default 'Ignore rule' (e.g. "C:\Program Files*.*").

4.1.6 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, *u.trust 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.

4.1.7 Key File Client Location

To specify the storage location, select **Client Settings** and, in the right-hand console pane, double-click **Key File Client Location**.

After you specify a path, *u.trust 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 Officer certificates or user certificates are not loaded automatically until the System Administrator has specified the paths.

u.trust LAN Crypt Administration stores both the **.p12* files for users and the public part of Security Officer certificates in the same folder. 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 folders, you must copy them manually into the relevant folders.

4.1.8 Policy File Client Location

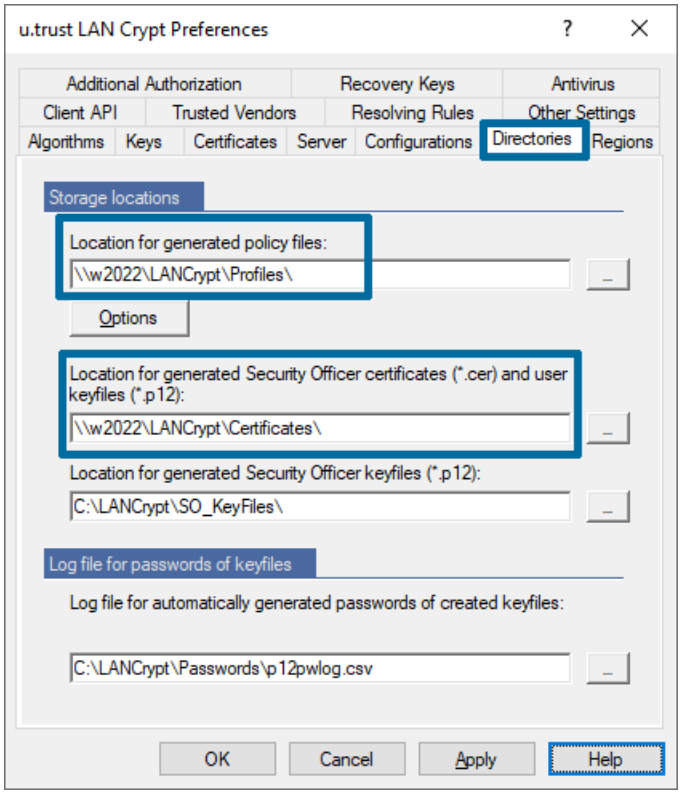
To specify the storage location, select **Client Settings** and, in the right-hand console pane, double-click **Policy File Client Location**.

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 folder in which they were generated by the Security Officer via the *u.trust LAN Crypt* Admin Console. 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.).

The paths entered in the group policy for Security Officer certificates, key files and policy files must match the paths defined in the *u.trust LAN Crypt* Admin Console in the **Central Settings** node, **Directories** tab.



4.1.9 Policy File Cache Directory

To specify the cache storage location, select **Client Settings** and, in the right-hand console pane, double-click **Policy File 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.

If a storage location is specified manually, it must be ensured that this folder also exists on the client computers.

Note: If you want to remove a user from your *u.trust LAN Crypt* environment, you must consider that the local copy remains saved on the computer. As long as this is the case, the user can access data with the rights contained therein.

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 (see "*Clearing Profiles*" on page 167).

4.1.10 Delay when loading profiles

Here, you can specify a period (in seconds) that will pass before the user profile is loaded. This delay is, for example, important if a certificate on 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.

4.1.11 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 folder 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 encryption is started via the Explorer extension "*Encrypt according to profile*", the setting does not have any effect.

Specify the file types in a list separated by semicolons.

Example: `docx;xlsx;pdf;txt`

4.1.12 Cached Policy File Lifetime

u.trust LAN Crypt standard behavior

When a user logs on to Windows, their cached profile will be loaded first. *u.trust 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 *u.trust 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 *u.trust 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 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 period during which policy files are kept in cache and thus remain valid can be specified in days, weeks, or months. In the registry, the value is specified in minutes.

When the specified period expires, *u.trust 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 always use up-to-date policies. On the other hand, you can prevent users from working with the same policy files for an unlimited period since a user can continue working with a cached version of the policy file for an unlimited 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 *u.trust*

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.

4.1.13 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.

Note: When you compress files with NTFS, which have already been encrypted by *u.trust LAN Crypt*, these files can no more decrypted by *u.trust LAN Crypt*. An error message is displayed when trying to decrypt such files. Files that you want to compress with NTFS must not have previously been encrypted with *u.trust LAN Crypt*.

4.1.14 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 *u.trust 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 *u.trust 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.

4.1.15 Profile Update Interval

This setting defines how often *u.trust LAN Crypt* checks for new policy files and updates them if necessary.

For updating policy files *u.trust LAN Crypt* needs access to the network drive on which the policy files are stored. *u.trust 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.

u.trust 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.

The update interval can be specified in minutes, hours, days, and weeks.

Note: *u.trust LAN Crypt* does not allow any update intervals shorter than 15 minutes. If this option is set to **Not configured**, policy files are not updated automatically.

4.1.16 Silent mode if user profile is missing

If the default setting applies, *u.trust 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.

Note: This setting can be particularly helpful in terminal server environments if not all users should work with *u.trust LAN Crypt*.

4.1.17 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. If you set **Persistent Encryption** to **yes**, you can ensure that files remain encrypted even when they are moved or copied.

To deactivate this function, double-click **Persistent Encryption** and select **no** in the list field of **Enable Persistent Encryption**.

4.1.18 Strong Private Key Protection

Here you can specify that the user is prompted for authentication every time the private key is used by *u.trust LAN Crypt*. If you enable this setting, it also applies to the Security Officer (see "*Enable Strong Private Key Protection*" under "*LAN Crypt Administration Settings*" on page 186).

Note: This policy has no effect on previously or manually imported certificates. Enabling this setting will only apply to certificates subsequently imported via *u.trust LAN Crypt*.

4.1.19 Random Number Generator

u.trust LAN Crypt uses an integrated random number generator for secure key generation. Here you can set which algorithm the random number generator should use. The selection affects the security of the generated keys. *BasicRandom* offers good performance with moderate security and is suitable for systems with limited resources and is supported by all earlier *LAN Crypt* versions. *AdvancedRandom* offers a good balance between good entropy and performance. *SuperRandom*, on the other hand, provides significantly higher entropy and is recommended for environments with particularly high security requirements.

Note: *SuperRandom* is only supported from *u.trust LAN Crypt* version 13.0.0.

Select an algorithm for the random number generator from the list:

- BasicRandom
- AdvancedRandom
- SuperRandom

If the random number generator setting is set to **Not configured**, *u.trust LAN Crypt* uses *SuperRandom* by default.

Note: You can set the algorithm for the random number generator in the *Client*- and *Server-Settings* (see "Random Number Generator" in the "*Server Settings*" section on page 187). However, only the same algorithm can be used for both settings. If you change the algorithm for the random number generator in one of the two settings, the change will also be applied to the other setting.

4.1.20 Prevent Plain Files

With this setting you can prevent plain files from being created in defined network paths, on mapped drives or local drives if a *u.trust LAN Crypt* user profile has not yet been loaded, or the user does not have one. Network paths (UNC paths) or local paths can be specified as targets.

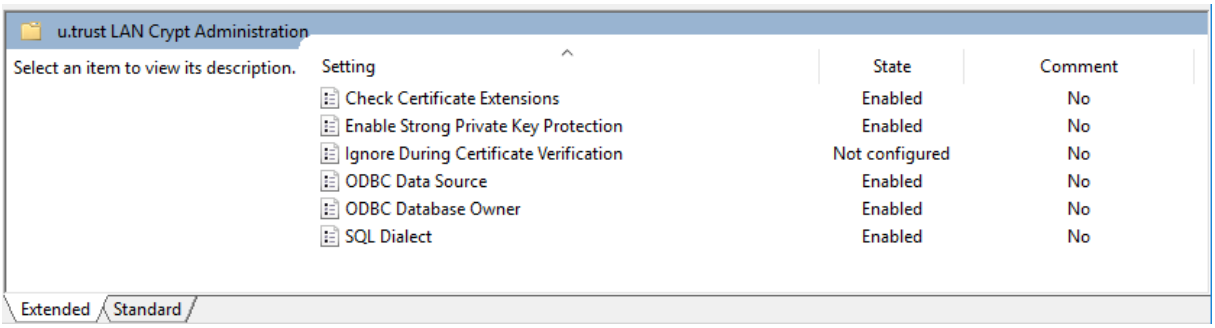
Examples:

```
\\server1.local.intern\share1\
\\server2.extern\share2\
C:\Foldername\
```

Note: Please use only UNC paths for network locations instead of drive letters (see examples above). This ensures the paths work for all users, as drive letters can vary by individual configuration.

4.2 LAN Crypt Administration Settings

Note: You must make these settings for the server. They have no effect on the client computers apart from one exception ("*Enable Strong Private Key Protection*").



However, it is vital that you make these server settings before you start the Administration function for the first time if you do **not** use the standard settings!

4.2.1 Enable Strong Private Key Protection

Here you can specify that the (Master) Security Officer is prompted for authentication every time the private key is used by *u.trust LAN Crypt*. If you enable this setting, it also applies to the clients (see "*Strong Private Key Protection*" under "*Client Settings*" on page 184).

Note: On computers on which you use the *u.trust LAN Crypt ScriptingAPI*, you must deactivate this setting via the group policy. The password query would otherwise always require user interaction when executing a script.

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

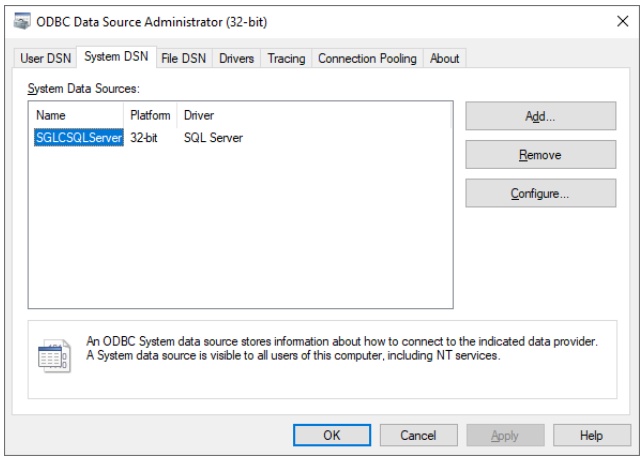
Here you enter the Database Owner to ensure that the database you are using can be addressed correctly.

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.

Attention: 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.



u.trust LAN Crypt uses **SGLCSQL** Server as the default name for the ODBC data source. If you want to use a different name, enter it here before you run *u.trust 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 Random Number Generator

u.trust LAN Crypt uses an integrated random number generator for secure key generation. Here you can set which algorithm the random number generator should use for the *u.trust LAN Crypt* Administration. The selection affects the security of the generated keys. *BasicRandom* offers good performance with moderate security and is suitable for systems with limited resources and is supported by all earlier *LAN Crypt* versions. *AdvancedRandom* offers a good balance between good entropy and performance. *SuperRandom*, on the other hand, provides significantly higher entropy and is recommended for environments with particularly high security requirements.

Note: *SuperRandom* is only supported from *u.trust LAN Crypt* version 13.0.0.

Select an algorithm for the random number generator from the list:

- BasicRandom
- AdvancedRandom
- SuperRandom

If the random number generator setting is set to **Not configured**, *u.trust LAN Crypt* uses *SuperRandom* by default.

Note: You can set the algorithm for the random number generator in the *Server-* and *Client-Settings* (see “Random Number Generator” in the “*Client Settings*” section on page 185).

However, only the same algorithm can be used for both settings. If you change the algorithm for the random number generator in one of the two settings, the change will also be applied to the other setting.

4.2.6 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 the *u.trust LAN Crypt* administration console.

4.2.7 Hash Algorithm

The used Hash Algorithm is only displayed at this point.

4.2.8 Check Certificate Extensions

By default, when *u.trust 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 "*key usage*" property.

However, in **Check Certificate Extensions** you can specify that this check is not carried out, which enables *u.trust LAN Crypt* to use certificates with other properties.

Check Certificate Extensions: **no** permits the use of certificates with other properties.

Note: However, whether or not these types of certificates can be used with *u.trust LAN Crypt* depends on which CSP or KSP 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 *u.trust LAN Crypt*.

4.2.9 Optimize performance for creating policies

You can use this setting to change the performance when creating policy files. By default, when a policy file is created, the temporary policy file is written to the resolver cache directory `%LOCALAPPDATA%\Utimaco\ResolverCache`, copied from there and then deleted.

If set to **Yes**, the temporary policy file is immediately moved to the output directory during profile creation. This improves performance when generating policy files.

Note: If you activate the setting **Optimize performance for creating profiles** and the resolver cache directory and the output directory are located on the same storage medium, the policy files created in the output directory receive the ACL inherited from the resolver cache directory instead of the ACL inherited from the output directory.

If you set this setting to **Not configured** or **No**, when a policy file is created, the temporary policy file is continued to be written to the resolver cache directory by default, copied from there and then deleted.

4.3 Unhandled Drives, Applications and Devices

In *u.trust LAN Crypt* you can specify that drives, applications, and devices (network file systems) are to be "unhandled" (ignored) by *u.trust 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.

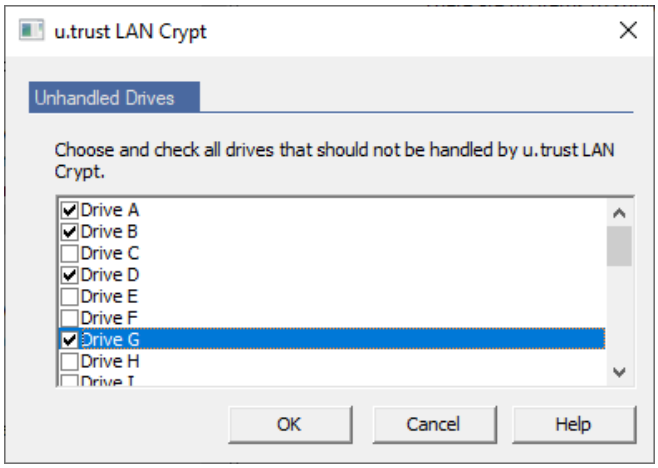
You will find these settings in the **LAN Crypt configuration** node.

Note: As these are machine-specific settings, they do not come into effect until you restart the client computer.

4.3.1 Adding Unhandled Drives

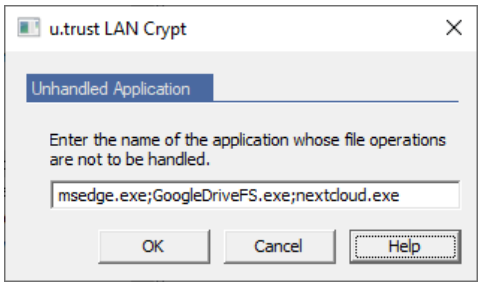
Select **Unhandled Drives** and click **Add unhandled drive(s)** in the context menu.

Select the drives you want *u.trust LAN Crypt* to ignore and click **OK**.



4.3.2 Adding Unhandled Applications

Double-click **Unhandled Applications** in the **Client Settings** to open a dialog in which you can specify unhandled applications.



Typical use:

- Backup programs can be defined as "unhandled" to ensure that they always read and save encrypted data.
- Also, compression programs can be defined as “unhandled” if encrypted files should not be added to an archive unencrypted with such programs.
- Applications that may cause errors when used simultaneously with *u.trust 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.

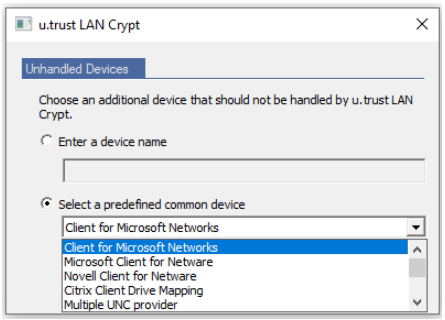
Enter the application’s name and path (if required).

If required, enable the option **Include child processes** and click **OK**.

Note: *u.trust LAN Crypt* already treats certain applications as ”*Unhandled Applications*“ by default. Before you specify an application as ”Unhandled *Application*“, check the *u.trust LAN Crypt* Client user menu via the **Client status** (there in the "*Unhandled*" tab, "Unhandled applications" section), whether this application is already defined there by default.

4.3.3 Adding Unhandled Devices

Double-click **Unhandled Devices** in the *Client Settings* to open a dialog in which you can specify **Unhandled Devices**.



The *Unhandled Devices* dialog displays network file systems and certain types of drives that you can exclude from the *u.trust LAN Crypt* encryption process. For technical reasons you cannot exclude single network drives here.

Note: Security Officers can exclude individual (network) 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.

You can only exclude entire network file systems. The pre-defined devices listed here are:

- Client for Microsoft Networks
- Microsoft Client for Netware
- Novell Client for Netware
- Citrix Client Drive Mapping
- Multiple UNC provider

and the following additional devices by type:

- 1 Boot Volume
- 2 Removables
- 4 Opticals
- 8 Fixed Drives
- 15 All local drives
- 16 Network Shares

Enter the Device(s) name and click **OK**.

Administrators can use tools such as OSR's Device Tree to display the names of file systems currently being used on the system.

5 APPENDIX

5.1 Logging

.... Permissions for 'Security Officer_Utimaco-NI' added. Allowed: 0x86000000 - Denied: 0x0)...

The values after **Allowed:** and **Denied:** show which permissions have actually been modified.

You can use the following tables to interpret the values:

Allowed: 0x86000000

ACL for Security Officer: Read	0x80000000
ACL for Security Officer: Change Certificate	0x02000000
ACL for Security Officer: Change Region	0x04000000
Allowed:	0x86000000

Global permissions of a Security Officer

Permissions	Values
Create Security Officers	0x000001
Create Profiles	0x000002
Create Keys	0x000004
Copy Keys	0x000008
Delete Keys	0x000010
Read Key	0x000020
Create Certificates	0x000040
Assign Certificates	0x000080
Administer Groups	0x000200
Log in to Database	0x000400
Authorize Operations	0x000800
Administer Users	0x001000
Create Rules	0x002000

Permissions	Values
Change Global Permissions	0x004000
Change ACLs	0x008000
Use Specific Keys	0x010000
Change Configuration	0x020000
Read Logging Entries	0x040000
Manage Logging	0x080000
Import Directory Objects	0x100000

ACL for a group

Create Key	0x00000001
Copy Key	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 Security Officers

Permissions	Values
Change Name	0x01000000
Change Certificate	0x02000000
Change Region	0x04000000
Assign Configuration	0x08000000
Delete Security Officer	0x10000000
Change Global Permissions	0x20000000
Change ACL	0x40000000
Read	0x80000000

5.2 Permissions

5.2.1 Global Permissions

Permissions	Description
Create Security Officer	The Security Officer has the global permission to create more Security Officers.
Create Profiles	The Security Officer 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 Security Officer. **Create Profiles** allows the Security Officer to create profiles for users where the Security Officer has the permission **Create Profiles** for the user's parent group. Owning this permission is a prerequisite for assigning values to keys. A Security Officer 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 a specific group. **Create Profiles for all Members** allows a Security Officer to create profiles for all users where the Security Officer 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 Security Officer can generate keys in the individual groups. A Security Officer 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 groups and users. The value itself is generated when policy files are generated. To generate keys with values manually, the Security Officer must have the **Create Profiles** permission.

Permissions	Description
Copy Keys	The Security Officer is allowed to copy keys.
Delete Keys	The Security Officer can delete keys from individual groups.
Read Key	The Security Officer can see the data for the individual keys for a group.
Create Certificates	The Security Officer can generate certificates for users.
Assign Certificates	The Security Officer is allowed to assign certificates to the users. The Security Officer 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 Security Officer. **Assign Certificates** allows the Security Officer to assign certificates to users where the Security Officer has the permission **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 Security Officer to assign certificates to all users where the Security Officer has the permission **Assign Certificates** on the parent group of the user or the permission **Assign Certificates to all Members** on one of the groups 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 Security Officer can make changes in the groups. Adding sub-groups, moving groups, synchronizing groups and deleting groups.

Permissions	Description
Log in to Database	The Security Officer can log on to the *u.trust LAN Crypt* database. The default setting is for this permission is *active*. With this permission a Security Officer 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 *u.trust LAN Crypt*.
Authorize Operations	The Security Officer can participate in actions that require confirmation.
Administer Users	The Security Officer can add users to a group, remove them from a group, and synchronize groups.
Copy Users	The Security Officer is allowed to add (copy) users to groups. This global permission is the prerequisite for setting the permission **Copy Users** for a specific group for a Security Officer. To add a user to a group, the Security Officer must have the permission **Copy Users** on the parent group of the user.
Create Rules	The Security Officer is allowed to generate encryption rules for the users.
Change Global Permissions	The Security Officer can change the global permissions granted to another Security Officer.
Change ACLs	The Security Officer can change the ACL for a group.
Use Specific Keys	The Security Officer can use concrete specific keys in encryption rules and can display specific keys in **All u.trust LAN Crypt keys**.
Change Configuration	The Security Officer can change the configuration (paths). This permission is required to display the **Configuration** tab in the node **Central Settings**, and for the Security Officer to be able to make changes in the **Directories** tab if they are logged on to the database.
Read Logging Entries	The Security Officer can view the settings used for logging and the logged events.
Manage Logging	The Security Officer can change the logging settings. They are permitted to archive, delete, and check entries.

Permissions	Description
Import Directory Objects	The Security Officer can import OUs, groups and users from a directory service and add them to the *u.trust LAN Crypt* database. Before they can import Directory Objects, the Security Officer also needs the **Administer Groups** permission and the **Administer Users** permission. These are set automatically when the **Import Directory Objects** permission is selected. If a Security Officer does not have this permission, the **Directory Objects** 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 Security Officer to whom the owner of the permission is assigned.
Change Certificate	Allows changes to the certificate of the Security Officer to whom the owner of the right is assigned.
Change Region	Allows changes to the region prefix of the Security Officer to whom the owner of the right is assigned.
Assign Configuration	Allows changes to the configuration of the Security Officer to whom the owner of the right is assigned.
Delete Security Officer	Allows the Security Officer, to whom the owner of the permission is assigned, to be deleted.
Change Global Permissions	Allows changes to the global permissions of the Security Officer to whom the owner of the permission is assigned.
Change ACL	Allows changes the ACL of the Security Officer to whom the owner of the permission is assigned.
Read	Displays the Security Officer to whom the owner of the permission is assigned in the node **Central Settings** \ **Security Officer Administration**. This is the prerequisite for all rights that allow the processing of this Security Officer. Is set automatically if a right of that type is selected.

5.2.3 Security Officer permissions for processing the groups

Permissions	Description
Create Key	The Security Officer is allowed to generate keys in the group.
Copy Keys	The Security Officer is allowed to copy keys.
Delete Key	The Security Officer is allowed to delete keys.
Create Rules	The Security Officer is allowed to generate rules for the users.
Assign Certificates	The Security Officer is allowed to assign certificates to the users. The Security Officer is allowed to run the wizard used to assign certificates. **Assign Certificates** allows the Security Officer 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 Security Officer 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 Security Officer is allowed to add users to the group manually. This permission is a prerequisite for importing / synchronizing groups and users.
Copy Users	The Security Officer has the permission to add users from this group to another group. This is only allowed for the members where this group is also the parent object.

Permissions	Description
Delete User	The Security Officer is allowed to use the **Members and Certificates of Group** snap-in to delete users. This permission is a prerequisite for importing / synchronizing groups and users.
Add Group	The Security Officer 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 Security Officer is allowed to delete the sub-groups for this group. This permission is a prerequisite for importing / synchronizing groups and users.
Move Groups	The Security Officer is allowed to move manually created groups in Administration (with "*drag & drop"*). Imported groups cannot be moved. This permission is a prerequisite for importing / synchronizing groups and users.
Change Properties	The Security Officer is allowed to change a group's properties.
Delete Group	The Security Officer is allowed to delete groups. This assumes that the Security Officer has removed the **Delete Subgroups** permission in the group above. This permission is a prerequisite for importing / synchronizing groups and users.
Create Profiles	The Security Officer has the permission to run the Profile Resolver and generate policy files for selected users. **Create Profiles** allows the Security Officer to build profiles for the users in the group where the group is also the parent group.

Permissions	Description
Create Profiles for all Members	This permission requires that the permission **Create Profiles** is set. **Create Profiles for all Members** allows the Security Officer to create profiles for all users in the group: users where the group is the parent group of and also users that are members 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 Security Officer is allowed to change the ACL for the group (for example, by adding another Security Officer).
Read	The Security Officer 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 Security Officer can see the group. Is set in the base node and inherited downwards. If it is refused for the Security Officer, the group is hidden (the permission **Read** must also be denied).

6 Legal notices

Copyright © 2023 - 2026 Utimaco IS GmbH, 2018 - 2023 conpal GmbH, 1996 - 2018 Sophos Limited and Sophos Group. All rights reserved.

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 license where the documentation can be reproduced in accordance with the license 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.

7 Technical Support

You can find technical support for *u.trust LAN Crypt* in any of these ways:

- At https://support.hsm.utimaco.com registered customers with active maintenance contracts get access to downloads, documentation, and knowledge items.

Download the client product documentation for Windows at

- https://help.lancrypt.com/docs/windows/13_0_3/de/ in German language, at
- https://help.lancrypt.com/docs/windows/13_0_3/en/ in English language and at
- https://help.lancrypt.com/docs/windows/13_0_3/fr/ in French language.
- https://help.lancrypt.com/docs/windows/13_0_1/jp/ in Japanese language.

Download the client product documentation for macOS at

- https://help.lancrypt.com/docs/macOS/de/ in German language and at
- https://help.lancrypt.com/docs/macOS/en/ in English language.

Download the product documentation for *iOS* / *iPadOS* at

- https://help.lancrypt.com/docs/ios/de/ in German language and at
- https://help.lancrypt.com/docs/ios/en/ in English language.

Download the product documentation for *Android* at

- https://help.lancrypt.com/docs/android/de/ in German language and at
- https://help.lancrypt.com/docs/android/en/ in English language.

Download the product documentation for *u.trust LAN Crypt 2Go* at

- https://help.lancrypt.com/docs/2Go/de/ in German language and at
- https://help.lancrypt.com/docs/2Go/en/ in English language.

Download the admin product documentation at

- https://help.lancrypt.com/docs/admin/13_0_1/de/ in German language, at
- https://help.lancrypt.com/docs/admin/13_0_1/en/ in English language, at
- https://help.lancrypt.com/docs/admin/13_0_1/fr/ in French language and at
- https://help.lancrypt.com/docs/admin/13_0_1/jp/ in Japanese language.

As a registered maintenance customer send an email to:

support@utimaco.com

including your *u.trust LAN Crypt* software version number(s), operating system(s) and patch level(s), and the text of any error messages.