# What is u.trust LAN Crypt?

With transparent file encryption, *u.trust LAN Crypt* enables the exchange of confidential data within authorization groups in small, medium and large organizations. *u.trust LAN Crypt* works without user interaction. It supports the role of a Security Officer (SO), who can restrict the access rights to files encrypted with *u.trust LAN Crypt*. A Master Security Officer (MSO) has the right to manage *u.trust LAN Crypt* or to delegate authorizations. In this way, a hierarchy of Security Officers can be set up that can meet the security requirements in any company.

Encrypted files do not need to be assigned to individual users. Any user who has the required key can work with an encrypted file. This allows administrators to create logical user groups that can share access and work with encrypted files. This process can be compared to a kind of key bunch as used in daily life. *u.trust LAN Crypt* equips users and user groups with a key ring, whose individual keys can be used for different folders or files.

Each time a user moves a file to an encrypted folder, the file is encrypted on that user's computer. If another user in the same privilege group reads the file from the folder, it is transferred in encrypted form. The file is only decrypted on the recipient's computer. The user can edit it there. Before the file is transferred back to the encrypted folder, it is encrypted again.

Unauthorized users may be able to access these encrypted files (only from workstations without *u.trust LAN Crypt*), but without the corresponding *u.trust LAN Crypt* authorization they will only see their encrypted content. This way the file always remains protected, even if no access protection is defined in the file system itself, the network is attacked or the employees do not follow the security guidelines of the organization.

## Data protection with u.trust LAN Crypt

*u.trust LAN Crypt* guarantees that sensitive files can be stored encrypted on file servers and workstations. Likewise, the transmission in networks (LAN or WAN) is protected, as the encryption and decryption are carried out in the main memory of the user's workstation. On the workstations, all encryptions and decryptions are transparent and largely without user interaction. No special security software needs to be installed on the file server itself.

A Security Officer can define different access rights for folders and files. These rights are summarized in encryption profiles for the users. Encryption profiles are distributed to users via policy files. Policy files contain all rules, access rights, and keys required for transparent encryption. The policy file is protected by a certificate. In order for users to process data encrypted with *u.trust LAN Crypt* on their computers, they must have access to the policy file. By possessing the private key belonging to the certificate, the user has access to the policy file where the encryption profile is stored.

*u.trust LAN Crypt* enables users to be divided into different authorization groups. All *u.trust LAN Crypt* users who have saved the same encryption profile in their policy file are members of an authorization group. You do not have to worry about encryption or key exchange. You only need to be able to access the policy files so that the files can be transparently encrypted or decrypted as soon as they are opened or closed. All forms of organization can be mapped from a LAN model in which the users are administered centrally to a distributed model in which users only use notebooks.

Since version 4.03, the *u.trust LAN Crypt* mini filter driver can also process files that are encrypted with *SafeGuard Enterprise* (Fileshare). Decryption of such files is not necessary. The respective keys of *SafeGuard Enterprise* must only be migrated to *u.trust LAN Crypt* using a key export and key import tool.

**Note**

- In this context, please also note that files that are encrypted with *SafeGuard Enterprise Fileshare* and then edited with *u.trust LAN Crypt* can then no longer be read by *SafeGuard Enterprise Fileshare*!
- 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*.

## SafeGuard Enterprise: File encryption migration

SafeGuard Enterprise is a security suite from Sophos, consisting of several modules. Data Exchange (DX), Cloud Storage (CS), and File Encryption (FE) all provide file-level encryption. However, the entire software suite is being discontinued, putting users at risk of losing access to their encrypted documents. Migrating from one security product to another can be a hassle and an added risk, especially if the process involves decrypting the data. However, this is not the case when migrating to u.trust LAN Crypt.

u.trust LAN Crypt and Sophos SafeGuard Enterprise are fully compatible. They share the same technical foundation and file-encryption subsystem. Consequently, files encrypted in SafeGuard Enterprise are fully compatible with and can be read natively by u.trust LAN Crypt. The encryption keys are specific to each installation, and only those need to be migrated.

**Step 1: Export Keys from SafeGuard Enterprise**

The keys used to encrypt files are unique for each SafeGuard Enterprise installation. Sophos provides a simple tool that allows for easy export of all encryption keys used in SafeGuard Enterprise for encrypting files. All keys are conveniently copied into a single package.

**Step 2: Import Keys to u.trust LAN Crypt**

The keys, now available in a separate package, can easily be imported into any existing u.trust LAN Crypt system. Once imported, the u.trust LAN Crypt installation has all it needs to access files that have been encrypted with SafeGuard Enterprise.

**Step 3: Update Policy / Assign Keys**

Assign the newly imported keys to all users who need access to files encrypted by SafeGuard Enterprise. These keys enable users to read files that have been encrypted by any SafeGuard file encryption module in the past. This also applies to files that have been encrypted by SafeGuard Enterprise after the key import.

**Step 4: Access Safeguard Enterprise Files**

The u.trust LAN Crypt Client shares its technical foundation with SafeGuard Enterprise. Once the keys have been deployed to the client, it can read all files that have been encrypted with any of the SafeGuard Enterprise file encryption modules – DX, CS, FS. There's no need to decrypt a single file. No matter how long ago a file was encrypted, u.trust LAN Crypt can read it.

Full file-level compatibility allows for smooth migration. Even if parts of the company still use SafeGuard Enterprise, all encrypted files they create can be read by anyone who has already migrated to u.trust LAN Crypt.

**Note**

- If you have installed *SafeGuard Enterprise* and plan to migrate to *u.trust LAN Crypt*, please contact the u.trust LAN Crypt support. Further information is available at https://utimaco.com/file-encryption-migration-five-easy-steps-safeguard-enterprise.

# Encryption

## Transparent encryption

For the user, transparent encryption means that all data stored in encrypted form (in encrypted folders or drives) is automatically decrypted in main memory as soon as it is opened by an application (such as Office). When the file is saved, it is automatically re-encrypted. Transparent encryption covers all file operations. Because all processes run in the background, users don't notice when they work with encrypted files.

**Note**

- *u.trust LAN Crypt* cannot encrypt files, for which **NTFS compression** or **EFS encryption** is used under the NTFS file system of Windows. However, the wizard for initial encryption offers the possibility to decompress or decrypt NTFS-compressed and/or EFS-encrypted files during initial encryption, if an encryption rule exists. The files are then encrypted by *u.trust LAN Crypt* according to the encryption rules. Whether the user has the possibility to decompress NTFS-compressed files or to decrypt EFS-encrypted files, if necessary, must be determined by the Security Officer in advance.

Encryption does not depend on folders, but only on encryption rules. The encryption works as follows:

- All files for which an encryption rule exists are automatically encrypted.
- When files are moved or copied to an encrypted folder, they are encrypted according to the encryption rule defined for that folder. The Security Officer can define several encryption rules for different file types or file names located in the same folder via the *u.trust LAN Crypt* Administration. For example, you can encrypt Word files with a different rule than Excel files, even though both files are located in the same folder.
- When you rename encrypted files, they remain encrypted (unless another encryption rule or no encryption rule exists for the new file name or extension).
- If a user copies or moves encrypted files to a location where the previous encryption rule no longer applies, they are automatically decrypted.

  **Note**

  - This does not apply if a user moves files to another folder within the same network share. In this case, the files remain encrypted, even if no encryption rule exists.
- If the Security Officer or System Administrator has enabled the **Persistent Encryption** feature via the *u.trust LAN Crypt* Group Policy (GPO), encrypted files remain encrypted even if they are moved or copied to another folder or location for which no encryption rule exists (e.g., on an USB stick).
- If a user copies or moves encrypted files to a location that has an encryption rule, the files are first decrypted and then encrypted using the other key defined for that location.

### Access to encrypted data

If there is no key and no Encryption Rule in a user's encryption policy for a specific folder, the user is not allowed to access the encrypted files in that folder. The user is not allowed to read, copy, move, rename, delete, etc. any encrypted file in that folder.

If the user has the key with which the files are encrypted, he can open them even if his encryption profile for that location or folder does not include an encryption rule.

**Note**

- Starting with LAN Crypt Administration Windows version 13.0.0, encryption in the CBC-uIV format is available. Older Classic LAN Crypt Clients (prior to version 13.0.0) do not recognize this format and therefore cannot decrypt the affected files. Please ensure that you always use the latest client version.

**Integration of u.trust LAN Crypt 2Go**

Files that have been password encrypted by *u.trust LAN Crypt 2Go* can be opened and edited with *u.trust LAN Crypt for Windows* since version 4.2.0. This requires that the required key exists within the user's encryption policy.

After viewing or editing the file, it can still be freely encrypted and decrypted with the same key by *u.trust LAN Crypt 2Go* and all other *u.trust LAN Crypt* applications that support *u.trust LAN Crypt 2Go* or password-based encryption and decryption.

**Rename or move a folder**

For performance reasons *u.trust LAN Crypt* does not change the encryption status when moving whole folders within a drive via Windows Explorer. This means that no encryption, un-encryption or re-encryption occurs when moving a whole folder.

If the files in such folders were encrypted, they will remain encrypted under the new folder name or in the new location. If the user has the corresponding key, he can work with these files as usual.

The behavior is different when moving files or folders to another partition or to USB storage devices for which no encryption rule has been set. If the *u.trust LAN Crypt* feature **Persistent Encryption** is not activated, the files will be decrypted when moved to such media. If the Security Officer or the System Administrator has activated **Persistent Encryption** for the clients, the files remain encrypted.

**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.

**Secure move**

*u.trust LAN Crypt* supports the secure moving of files and folders. When moving files through *u.trust LAN Crypt*, the files are encrypted, decrypted or re-encrypted at the new location according to the applicable encryption rules. Afterwards the source files are securely deleted.

This function is available via the entry **u.trust LAN Crypt** -> **Secure move** in the Windows Explorer context menu of *u.trust LAN Crypt*. Via a dialog you can then select where the files should be moved to.

**Explicit decryption of files**

To decrypt a file, you only need to copy or move it to a folder without encryption rules. The file is then automatically decrypted.

Prerequisites:

- a corresponding encryption profile is loaded
- the user has the required key
- the active encryption profile does not contain an encryption rule for the new location
- **Persistent Encryption** is not active

**Note**

- *u.trust LAN Crypt* can also encrypt offline folders in Windows. However, problems can occur in connection with virus scanners. More detailed information about known problems with virus scanners can be found in the version information of the *u.trust LAN Crypt* Client.

**Delete encrypted files**

When your encryption rule is loaded, you can delete any encrypted file for which you have a key.

**Note**

- Actually, deleting files is about moving the files to the Windows Recycle Bin. To ensure the highest security standard, the files encrypted with *u.trust LAN Crypt* remain encrypted even in the recycle bin. No key is necessary to empty the recycle bin.

**Files and folders excluded from encryption**

The following files and folders are automatically excluded from encryption, even if an encryption rule has been defined for them:

- Files in the *u.trust LAN Crypt* installation folder.
- Files in the Program Files and Program Files (x86) folders.
- Files in the Windows installation folder.
- Files in the Windows.old folder.
- Policy file cache.

The location is specified in the *u.trust LAN Crypt* Administration and is displayed in the **Profile** tab of the dialog **Status**.

- Root directory of the system drive. Subfolders are not excluded.
- Indexed Locations (search-ms).
- Files in folders which are defined in *u.trust LAN Crypt* with an exclude or ignore rule.

**Persistent encryption**

For *u.trust LAN Crypt* a Security Officer or System Administrator can configure the **Persistent Encryption** via a *u.trust LAN Crypt* Group Policy (GPO). Files are normally only encrypted if they are subject to an encryption rule.

For example, if a user copies an encrypted file to a folder for which no encryption rule is defined, the file is decrypted in the destination folder. However, if **Persistent Encryption** is enabled, files remain encrypted even if they are moved or copied to another location for which no encryption rule is defined.

Security Officers or System Administrators can set this behavior via a *u.trust LAN Crypt* Group Policy (GPO). If **Persistent Encryption** is deactivated, files are decrypted if they are copied or moved to a location for which there is no encryption rule. In this way, files can be decrypted, e.g., to be sent as an email attachment. However, it would be better to leave **Persistent Encryption** enabled and instead copy such files to a folder that has an ignore or exception rule. In this way, the protective function of **Persistent Encryption** could continue to be maintained and at the same time there could be a storage location in which users could explicitly decrypt files, for example to send them as e-mails.

The following rules apply to **Persistent Encryption**:

- 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* in a location not covered by an encryption rule, the file will be stored decrypted.
- 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**.

**Note**

- Persistent Encryption uses the Windows Tunneling Cache. If a thread opens an encrypted file and then creates a file with the *same name* within the tunneling interval (default: 15 s), the new file will be encrypted automatically, regardless of the target path and even if no encryption policy exists for that location. This behavior is system-dependent and should be considered when using LAN Crypt.

#### Persistent encryption vs. encryption rule

**Persistent Encryption** ensures that an encrypted file retains its encryption state, i.e., the original encryption key. This works well with **Persistent Encryption** if the file is copied or moved to a folder without an encryption rule. However, if the file is copied or moved to a location that has a different encryption rule, that encryption rule takes precedence over **Persistent Encryption**. The file is then converted according to the encryption rule for that location, using the encryption algorithm (for example, AES) and key defined for that location.

#### Persistent encryption vs. ignore path rule

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

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

#### Persistent encryption vs. exclude path rule

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

### Limitations on persistent encryption

**Persistent Encryption** has some limitations.

#### Files that are supposed to remain plain are encrypted

### Unencrypted files are copied to multiple locations with and without applying encryption rules.

- If an unencrypted file is copied to several locations at the same time, with one location having an encryption rule applied, all copies of that file might be encrypted too.
- If an unencrypted file is copied to an encrypted location the file is added to the encryption tool's internal list. When a second copy of the file is created, the encryption tool finds the file name in its list and also encrypts the second copy.

### Create a file with the same name after accessing an encrypted file

- If an encrypted file is opened (accessed) and a new file with the same name is created shortly afterwards, the newly created file is encrypted with the same key as the first file.
- This only applies if the same application / thread is used for reading the encrypted file as well as creating the new one.

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

#### Files are not encrypted

### Multiple copies of a file are created

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

**Client API and encryption tags for DLP products**

If a **Data Loss Prevention** (DLP) product identifies data that needs to be encrypted, it can use the *u.trust LAN Crypt* Client API to encrypt these files. In *u.trust LAN Crypt* Administration (see Admin help), 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.

## Deactivating / activating transparent encryption

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

**Note**

- The settings, which functions or elements can be selected via the user menu, can be set by the Security Officer or System Administrator via the *u.trust LAN Crypt* Group Policy (GPO). This way the client can be configured in such a way that the user cannot deactivate the transparent encryption.

In comparison, disabling **Persistent Encryption** causes encrypted files to be decrypted when they are copied / moved to a location or folder where no encryption rule exists. The rule-based automatic encryption and decryption function for folders and files (see Transparent Encryption) remains in effect when you deactivate **Persistent Encryption**. The configuration of the **Persistent Encryption** is also done by the Security Officer or System Administrator via a *u.trust LAN Crypt* Group Policy (GPO).

If you have the **Persistent Encryption** feature enabled, encrypted files remain encrypted even if they are copied or moved to a location or folder without an encryption rule. If you use **Persistent Encryption** , it is not necessary to disable transparent encryption before copying encrypted files to another location. **Persistent Encryption** ensures that files remain encrypted even if they are accidentally moved to another folder or if the user forgets to disable encryption before moving or copying. You must restart your computer for any changes made to the **Persistent Encryption** (enabled or disabled) to take effect.

**Note**

- If **Persistent Encryption** is enabled and a user moves or copies a file to a folder to which an *Ignore* or *Exclude rule* applies, this will result in the file being decrypted. Also note that changing the **Persistent Encryption** setting requires a restart of the client computer. The previously defined setting remains valid until the computer is restarted.

## Transparent encryption and file-compression tools

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

If **Persistent Encryption** is enabled, the files will not be compressed in encrypted form. However, the archive file itself remains encrypted and can only be read by a user who has the necessary key. A prerequisite for this is, however, that archive files are also subject to an encryption rule.

However, if you also want to use compression programs to pack encrypted files into an archive file, transparent encryption must be disabled before using such programs. This procedure is usually only necessary if no encryption rule exists for the archive file to be created.

However, if such an encryption rule exists, the files within the created archive file would be unencrypted, but the archive file itself would be encrypted according to the encryption rule defined for this purpose, and thus securely protected against unauthorized access.

Another way to ensure that files are packed into an archive file in encrypted form is to define compression programs as an *unhandled application*. If necessary, this can be configured by the Security Officer (MSO / SO) or System Administrator via the *u.trust LAN Crypt* Group Policy (GPO).

## Cloud synchronization

Major cloud synchronization applications, including Microsoft OneDrive, Google Drive, Nextcloud and BoxDrive, are configured to automatically register themselves upon installation. By default, these applications, along with any associated child processes, are prevented from accessing the contents of encrypted files.

If you wish to extend this restriction to additional cloud applications and their child processes, preventing them from reading encrypted file contents, you can do so by making modifications to the system registry as described below:

Key: `HKLM\SYSTEM\CurrentControlSet\Services\cplcdt2\Parameters`

Setting: `IgnoredCloudSyncApps`

Type: `REG_MULTI_SZ`

## Initial encryption and explicit encryption

After *u.trust LAN Crypt* has been installed, you need to perform initial encryption process. During this process, all files are encrypted using the loaded encryption profile. This initial encryption can be performed using:

- the *u.trust LAN Crypt* system tray icon, see User application
- *u.trust LAN Crypt* Explorer extensions, see Explorer extensions
- the **lcinit.exe** tool, which also supports Unattended mode, see Initial encryption in Unattended mode

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

**Note**

- During initial encryption, the files are displayed lexicographically sorted.

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

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

### The initial encryption wizard

The initial encryption tool, **lcinit.exe** , offers a wizard with a graphical user interface. This wizard supports

- encrypting, decrypting and re-encrypting files
- checking the encryption status of files -even in folders and subfolders

You can start this **wizard**

- by clicking the Taskbar icon
- by going to `Start/u.trust LAN Crypt Client/Initial encryption`
- by double-clicking on **lcinit.exe** in the *u.trust LAN Crypt* Program folder.

**Note**

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

#### Performing initial encryption

**Step 1:** Start the wizard, see User menu.

**Step 2:** Select the Perform initial encryption option in Step 1 / 5.

**Step 3:** Click **Next**. **Step 4:** Now define how files are to be handled in Step 2 / 5.

- **Encrypt files in accordance with profile:** If you select this option, the files will be encrypted according to the rules contained in the user's profile (default setting). If the system finds already encrypted files, they will be ignored.
- **Re-encrypt files in accordance with profile:** If you select this option, files encrypted with a different key than the one defined in the profile will (also) be decrypted and encrypted with the correct key.

  **Note**

  - A prerequisite for this procedure is that the key which has been used for encrypting the file(s) in the first place is contained in the user's profile.

**Step 5:** Click **Next**. **Step 6:** Now specify in step 3 / 5 the drives, folders and subfolders that you want to include in the initial encryption or decryption process. Folders that are specified in the rules can be selected with the **Profile Rules** button.

Selected drives and folders are marked with a check mark. A checkmark with an additional "+" sign next to a folder indicates that there are other subfolders in the folder that are not being processed, that means, where no encryption/encryption of files is performed. If these are also to be processed, they must also be marked with a check mark by a mouse click.

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

Click **Advanced** to access extra options:

**Note**

- The settings which can be changed by the user depend on the configuration of the *u.trust LAN Crypt* Client. The Security Officer defines the configuration centrally.

- **Decrypt EFS encrypted files if necessary:** Select this option to decrypt and re-encrypt EFS encrypted files. Note an encryption rule must apply to them. If you do not select this option, the Initial Encryption Wizard will ignore EFS encrypted files. They will not be re-encrypted by *u.trust LAN Crypt*, even if an encryption rule has been specified for them.
- **Decompress NTFS compressed files if necessary:** Select this option to decompress NTFS compressed files and encrypt them. Note an encryption rule must apply to them. If you do not select this option, the Initial Encryption Wizard will ignore NTFS compressed files. They will not be encrypted, even if an encryption rule has been specified for them.
- **Decrypt/re-encrypt files encrypted with several keys:** Select this option to re-encrypt files that were encrypted with several keys. The files are encrypted with one key only. Note an encryption rule must apply to them.

  **Note**

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

- **Include only the following file types:** Select the file types to which you want to restrict the initial encryption process (for example .docx, .pdf, txt). This setting only applies to files for which an encryption rule exists. If there are files of different types in the folder, they will not be

processed during initial encryption. They will only be encrypted when the user opens and saves them. To specify several file types, use a list separated by semicolons.

**Step 7:** Click **Next**. **Step 8:** Now define which files are to be included in the initial encryption report in Step 4 / 5. For the initial encryption report the user can select between the following options:

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

**Step 9:** Click **Next**. The **Result** of the encryption, the **key name** of the key used and the encryption algorithm will be shown for each file in Step 5 / 5.

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

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

**Step 10:** Click **Finish**. The wizard will be closed.

#### Verifying encryption state

**Step 1:** Start the wizard.

**Step 2:** Select the **Verify encryption states** option in Step 1 / 5.

**Step 3:** Click **Next**.

**Step 4:** Select all the drives and folders you want to verify in Step 2 / 5.

**Step 5** Select drives and folders by marking with a tick.

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

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

Click **Advanced** to restrict the verification to specific file types:

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

**Step 6:** Click **Next**.

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

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

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

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

#### Decrypting files

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

To decrypt files:

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

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

**Note**

- *u.trust LAN Crypt* only decrypts files for which no encryption rule applies.

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

1. Enable **Encrypt files in accordance with profile:** All files are encrypted according to the new encryption.
2. Enable **Re-Encrypt files in accordance with profile:** If files are to be encrypted with a different key according to the new rules, they will be re-encrypted.
3. Enable **Decrypt files with selected keys** and then select **all keys:** Encrypted files, for which no longer any encryption rule exists, will be decrypted. *u.trust LAN Crypt* only decrypts files for which no encryption rule exists. Therefore, selecting all keys will not cause any problems.

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

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

**Initial encryption in unattended mode**

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

**Command line syntax:**

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

**Parameters:**

**Start path**

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

**%Profile**

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

**Note**

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

**/s**

Includes all subfolders from the start path.

**/h or /?**

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

**-DIgnoreDirectory**

Ignores this folder.

**/Tv**

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

**/Te**

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

**/Tr**

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

**/Td**

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

**/Tdk**

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

**Note**

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

**/Dc**

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

**/De**

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

**/Dm**

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

**+Ffiletype**

If you specify file types with this option (e.g., +Ftxt+Fdocx), only files of the relevant type are processed. This setting only affects files for which an encryption rule exists.

If a folder also contains files of a different file type, that is not specified with this option, they are not taken into account during initial encryption. They will only be encrypted when the user opens and saves them.

**Example:** The file "*123.pdf*" is not encrypted because files of the type "PDF" in the above example are not to be encrypted in the initial encryption. If the user opens this file, e.g., with a PDF editor, and saves this file in the same folder, the file is encrypted. The file is also encrypted if the user copies such a file out of this folder and then copies it back in. However, this is only possible if the encryption rule defined for the folder also applies to files of the type "PDF".

**/V0**

Verbose mode 0: No reporting.

**/V1**

Verbose mode 1: Lists error messages.

**/V2**

Verbose mode 2: Lists modified files.

**/V3**

Verbose mode 3: Lists all files.

**/V4**

Verbose mode 4: Lists plain files.

**/E**

Stop on error.

**/X**

Initial encryption without displaying a window.

**/LLogfile**

Writes output to the specified file.

**Note**

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

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

lcinit.exe D:\data /S /V4
```

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

---

# Policies

## Certificates

Before users can access their encryption profile, the corresponding certificate must be available on the computer. The Security Officer distributes these certificates to the users. Users then import the certificate to their own machines. If the certificates are available at the first logon, the entire process runs without any user interaction.

*u.trust LAN Crypt* has an option for importing certificates automatically, when the encryption profile is loaded for the first time. In this case, the Security Officer configures the system so that *u.trust LAN Crypt* can find a certificate file during logon and starts importing the certificate automatically. The user is prompted once to enter the PIN for the PKCS#12 key file.

**Note**

- The (Master) Security Officer is responsible for distributing the PIN required to import a certificate automatically to the users.

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

**Note** If users attempt to log on to *u.trust LAN Crypt* and their logon fails, they receive an error message to tell them why they were unable to log on.

Special encryption rules included in the *u.trust LAN Crypt* encryption profiles give users access to encrypted data. These rules define exactly which files in particular directories have to be encrypted by each key. A user's encryption profile only needs to be loaded and encryption and decryption takes place in the background (transparently).

The user is unaware of the encryption / decryption tasks being performed.

**Note**

- CA certificates are only accepted as correct if they are stored in the certificate store under "Trusted Root Certification Authorities". *u.trust LAN Crypt* however imports CA certificates, which can be contained in PKCS#12 key files, together with the user certificates into the folder "My Certificates-Certificates". To avoid error messages, CA certificates in the certificate store must be moved manually to "Trusted Root Certification Authorities". If you use certificates generated by *u.trust LAN Crypt*, such a step is not necessary.

### Smartcard readers

As the use of certificates is handled by using Cryptographic Service Providers (CSPs) and Key Storage Providers (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 Cryptographic Service Provider (CSP) or Key Storage Provider (KSP) are correctly installed and operational!

**Note**

- Please also note that Cryptographic Service Providers (CSP) for key operations by u.trust LAN Crypt are now only supported in conjunction with Shims that make them accessible as Key Storage Providers (KSP)

## Loading the policy file

#### *u.trust LAN Crypt* default behavior

When a user logs on to Windows, their cached profile is loaded first. *u.trust LAN Crypt* checks whether a new policy file is available for the user by establishing a connection to the specified location of the policy file (network drive or webserver). If a new policy file is found, the cached user profile is updated.

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 specified location is not accessible, the user works with the cached user profile until it can be updated.

**Note**

- *u.trust LAN Crypt* verifies the certificates of the user and the (Master) Security Officer. If the certificates contain a CRL Distribution point and no valid CRL is present in the system, Windows tries to import the CRL from the specified address. If a firewall is installed you may see a message that a program (*loadprof.exe*) is trying to establish a connection to the Internet. In some cases, also the download of the user profile may cause this message.

#### Behavior defined by Security Officers

The Security Officer can modify the default behavior using central settings. Security Officers can specify for how long the cached policy is valid on client computers. They can define update intervals for the policy files. The settings defined by the Security Officer are shown in the **Profile** tab of the **Client-Status** dialog, see *The Client-Status dialog*.

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

When the specified time period expires *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 is unloaded. The user can no longer access encrypted data.

The policy file is updated and loaded again, when a valid policy file is available (for example at the next logon with a connection to the client location for policy files). The user can access encrypted data again. The counter for the duration of cache storage is reset.

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

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

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

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

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

#### Policy files are not cached

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

## Logon to u.trust LAN Crypt

*u.trust LAN Crypt* encryption profiles are created by a Security Officer, in accordance with the company's security policy, and then stored in policy files. An encryption profile can only be loaded, if the user owns the corresponding certificate.

The path of the policy file is written to a client machine's registry by the System Administrator or Security Officer. This is done via a *u.trust LAN Crypt* group policy. When a user logs on to *u.trust LAN Crypt*, the encryption profile, which is stored in the policy file, is loaded onto the client machine. *u.trust LAN Crypt* Client loads the policy files from the defined location (e. g. a network share) and checks, whether the user is allowed to load it, by verifying user's certificate.

#### Logon with token

Users can also log on to *u.trust LAN Crypt* using a token. A prerequisite for this logon method is that the user's *u.trust LAN Crypt* user certificate is stored on the token. If the user certificate is found on a token connected to the system, the user is logged on.

When using tokens for logging on, *u.trust LAN Crypt* may try to load a policy file before the token can be identified by the operating system. In this case, a message is displayed indicating that the user certificate could not be found, although the token is connected to the system.

The user has to load the policy file manually via the user application in the toolbar -> **Load encryption rules**. The token is identified and the user is logged on. To avoid this, a delay for loading the profiles can be specified in **Configuration** (setting **Delay when loading profiles** ).

---

# User application

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

**Green:** Encryption rules loaded and transparent encryption activated.

**Yellow:** Encryption rules loaded, but transparent encryption deactivated.

**Red:** No profile loaded.

## User menu

Right-click on the key icon to open the *u.trust LAN Crypt* user menu offering the following options:

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

**Note**

- The menu commands available depend on the configuration of the *u.trust LAN Crypt* Client. The Security Officer defines the configuration centrally.

**Load encryption rules/Update encryption rules**

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

**Clear encryption rules**

This option prevents access to encrypted data. This is a security option that secures encrypted data against unauthorized access when the workstation is unattended. Note the use of the private key must be secured with a password. Otherwise, the profile could be reloaded by using the **Load encryption rules** command.

**Deactivate / Activate Encryption**

Toggles transparent encryption on and off. Deactivating encryption is used if files are to remain encrypted when they are moved or copied to a folder where no encryption rule is valid. With active encryption, the files would be decrypted if they were copied to this type of folder.

If, for example, an encrypted file is attached to an e-mail, it would be decrypted automatically, if transparent encryption were active. If transparent encryption is deactivated, the encrypted file can be sent as an e-mail attachment.

**Note**

- If the System Administrator has activated the Persistent Encryption function, encrypted files remain encrypted even if they are copied or moved to a location for which no encryption rule has been specified.

**Show profile** Displays the encryption rules and the keys contained in the encryption information in two tabs.

The *Active Encryption Rules* " tab contains an overview of the valid rules for the logged-in user. In addition, the following options are available to the user: *Show Ignore Rules*, *Show Exclude Rules*, *Show Encryption Tags* and *Show Bypass Rules*.

The *Available keys* tab page lists all the keys that are available to the current user.

**Client-Status**

The **Client-Status** option uses several tabs to display detailed information about the current status of the *u.trust LAN Crypt* Client, see The Client-Status.

**Initial encryption**

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

**Close**

Closes the *u.trust LAN Crypt* User Application.

**About**

Displays information about your current version of *u.trust LAN Crypt*.

**Note**

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

## The Client-Status dialog

The **Client-Status** option displays several tabs that provide information on the encryption settings for a user's machine.

These are:

**Status**

This tab shows whether the user profile has been loaded and encryption is active. It also displays detailed information on the policy file (creation date, Security Officer who created the file etc.).

If the user profile has been loaded, encryption is also active. However, the encryption can also be (temporarily) disabled when the user profile has been loaded, see "User menu, command **Deactivate / Activate encryption**".

**Settings** This tab provides information on the settings that currently apply to the client. These settings are defined centrally and refer to encryption, system tray icon and the settings for the **Initial Encryption Wizard**. Among other details this tab shows whether **Persistent Encryption** has been activated as well as the menu options to be available on the client computers.

**Profile** This tab shows the settings for the user profile.

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

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

**Rules** This tab lists all the encryption rules that apply to the current user.

**Unhandled** This tab provides information about unhandled applications, disk drives and devices. It also lists the active ignore and bypass rules of the current user.

*u.trust LAN Crypt* treats certain applications as 'unhandled applications' by default. These applications are also shown on this tab.

**Applications** This tab shows programs that require a special approach by *u.trust LAN Crypt* due to their behavior.

**Antivirus software**

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

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

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

**Export** button

Use the **Export** button to export the current client settings to an XML file. This way, support teams can be easily provided with important configuration information.

## Explorer extensions

The *u.trust LAN Crypt* Explorer Extensions offer the following features:

- Encryption according to profile (files, folders and drives);
- Explicit encryption and decryption of files, folders and drives;
- Easy control of the encryption state of your data.

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

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

**Green Key:** The file is encrypted and the user has access to the key.

**Red Key:** The file is encrypted and the user does not have access to the key.

**Gray Key:** A gray key indicates that the file is plain (unencrypted) but should be encrypted in accordance with an encryption rule in the loaded profile.

**Yellow Key:** If a yellow key is displayed, the file is encrypted, but the transparent encryption is currently deactivated.

**Yellow Key with question mark:** The user does not have sufficient access rights so *u.trust LAN Crypt* is not able to determine the encryption state.

**Note**

- No key symbols are displayed for files that have the offline attribute set (for example, for physically non-existent files).
- Key symbols are also added to the files in Windows Explorer itself. If an encryption rule exists for entire drives or folders, these are also marked with a key symbol. There, keys in different colors also show the encryption status.

**Menu options for folders**

**Encryption state**

This option displays a list of all files in this folder and their encryption state (colored keys). Only files on the first folder level are displayed. To display files in a subfolder, first go to that subfolder. In Explorer, folders for which an encryption rule exists can be recognized by a key icon.

**Encrypt according to profile**

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

**Encrypt**

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

**Note**

- If an encryption rule exists for files in a folder and not all of these files are (already) encrypted according to the rule, an error message may occur during encryption after marking the directory or folder and selecting the *Encrypt* option.

**Example:** Mark a folder in which at least one of the files contained therein has an encryption rule with e. g. "Key-1", select another Key, e. g. "Key-2", via the *Encrypt* option and click **Ok**.

**Note**

- For folders that already have an encryption rule, encrypt them using the "*Encrypt according to profile*" option instead. Alternatively, you can also encrypt the files using the *u.trust LAN Crypt* user menu Initial encryption.

**Decrypt**

This option decrypts all the files on the first folder level. Therefore, all relevant keys need to be available in the active encryption profile. If a key is missing, the files that use that key remain encrypted.

**Secure move**

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

**Secure delete**

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

**Menu options for individual files**

**Encryption state**

This option shows the file's encryption status. For encrypted files, a popup information box shows the key used to encrypt them along with additional information about whether the user is entitled to use this key.

If another user is logged on, but is not entitled to use this key, the GUID appears in the info box instead of the key name.

You can identify encrypted files in Explorer by the small green key icon shown next to them. If the user clicks on **Folder Options** -> **View** , they can specify whether or not the file encryption status and the folder encryption status are to be displayed for their profile. The changes they make to these settings do not become effective until they log off and then log on again.

**Encrypt according to profile**

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

**Encrypt**

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

**Note**

- If an encryption rule exists for files in a drive or folder and not all files are (already) encrypted according to this rule, an error message may occur during encryption after marking several files and selecting the *Encrypt* option.

**Example:** Mark a folder in which at least one of the files contained therein has an encryption rule with e. g. "Key-1", select another Key, e. g. "Key-2", via the *Encrypt* option and click **Ok**.

**Note**

- For folders that already have an encryption rule, encrypt them using the "*Encrypt according to profile*" option instead. Alternatively, you can also encrypt the files using the *u.trust LAN Crypt* user menu Initial encryption.

**Decrypt**

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

**Secure move**

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

**Secure delete**

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

**Note**

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

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

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

**Encryption information**

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

---

# Terminal server

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

## Firewall

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

## Installation in a terminal server environment

The installation of the LAN Crypt Client on a terminal server is generally the same as on regular Windows systems. However, when LAN Crypt is used in a RemoteApp environment (application virtualization), additional steps are required to ensure that **LoadProf** is executed only within the RemoteApp context rather than globally for the entire session.

### Installation in a RemoteApp environment (application virtualization)

#### Preparation before setup

Before starting the installation package, the existing entry for *loadprof.exe* must be removed. Open the Registry Editor and delete the entry in the following key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Appsetup
```

If *loadprof.exe* appears in this value, remove it completely.

#### Installation with Transform File (.mst)

To run the installation package, a transform file (.mst) must be created and included.

> **Note**
>
> - Please note that the .mst file must be created manually.

In this transform file, the private property **TerminalServer** must be set to **1** so that the setup installs correctly in terminal server mode.

#### Example installation command with transform file:

```
msiexec /i LCClient.msi /qn [additional parameters] TRANSFORMS="C:\Transform_File.mst"
```

This configuration ensures correct startup behavior in RemoteApp scenarios.

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

## Restrictions

#### Citrix

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

# Installation and upgrade

**Note**

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

**Step 1:** Double-click on one of the **LCClient.msi** file in the *u.trust LAN Crypt* Install folder of your unzipped installation package.

**Step 2:** Click **Next**.

The License Agreement dialog is displayed.

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

**Step 4:** Click **Next**.

The **Destination Folder** dialog is displayed.

**Step 5:** Select where to install *u.trust LAN Crypt*.

**Step 6:** Click **Next**.

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

**Step 7:** In this dialog, you select which components of *u.trust LAN Crypt* Client are to be installed.

- *Typical*: Installs the most commonly used application functions of *u.trust LAN Crypt* Client.
- *Complete*: Complete client installation, including the Client API.
- *Custom*: Lets the user select the different components.

**Step 8:** Select **Custom** and click **Next**.

The following components can be installed:

**User Application**

Installs the *u.trust LAN Crypt* user application, see User application.

**Shell Extension**

Installs the *u.trust LAN Crypt* Explorer Extensions.

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

**Client API**

Used to access *Utimaco* File Encryption functionality through an API.

**Note**

- You must install the Client API to enable DLP products to access data using the *u.trust LAN Crypt* Client API.

**Network Filter**

Used to access *Utimaco* File Encryption functionality through an API.

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

**Note**

- Please note that *u.trust LAN Crypt* from version 4.1.0 no longer supports legacy filter drivers. All encryption and decryption operations are performed exclusively via the new more up-to-date and future-proof mini filter driver technology.

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

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

**Note**

- To apply all settings, you must restart the computer.

## Unattended installation

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

The Install directory of your installation CD includes the *.msi-file* that is required for unattended installation of the client components.

f

## Components to install

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

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

**Example:**

AddLocal= **ALL** installs all available components.

## Command line syntax

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

**Mandatory parameters:**

**/I**

Specifies the installation package to be installed.

**/QN**

Installation without user interaction (unattended setup).

Name of the .msi-file: **LCClient.msi**

**Syntax:**

```
msiexec /i \<path\>\LCClient.msi /qn AddLocal=\<component1\>,\<component2\>,...
```

**Optional parameters**

```
/Lvx\* \<path + filename\>
```

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

**AddLocal=**

```
AddLocal= ALL
```

Installs all available components.

```
AddLocal= LanCrypt
```

Does not install any of the available components.

```
AddLocal= UserApplication
```

Installs the *u.trust LAN Crypt* user application.

```
AddLocal= NetworkFilter
```

Installs a driver that helps improve the performance of network accesses.

```
AddLocal= ClientAPI
```

Installs the *u.trust LAN Crypt* Client API. This will be used to access *Utimaco* File Encryption functionality through an API.

```
AddLocal= ShellExtensions
```

Installs the *u.trust LAN Crypt* Explorer Extensions.

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

**NOOVERLAY=**

**(Only works for new installations, not for version upgrades)**

```
NOOVERLAY=0
```

Enables overlay icons for files and folders.

```
NOOVERLAY=1
```

Disables overlay icons for files and folders.

**Note**

- Users can enable overlay icons after installation. If the users click on **Folder Options** -> **View** they can specify whether or not the file encryption status and the folder encryption status are to be displayed for their profile. The changes they make to these settings do not become effective until they log off and then log on again.

**Productlanguage=**

Installs the MSI language package for the *u.trust LAN Crypt* Client in a specific language, regardless of the existing language setting on the computer. This set language is then used for the installation itself and also for later changes by the setup wizard of *u.trust LAN Crypt*. The following language settings are currently supported via the installation parameter "Productlanguage=".

```
Productlanguage=1031
```

Installs the German MSI language package for the *u.trust LAN Crypt* Client

```
Productlanguage=1033
```

Installs the English MSI language package for the *u.trust LAN Crypt* Client

```
Productlanguage=1036
```

Installs the French MSI language package for the *u.trust LAN Crypt* Client.

**RESET_CONFIGURATION=**

```
RESET_CONFIGURATION=1
```

Resets all existing LAN Crypt Client configurations in the Windows Registry. All previous settings will be permanently deleted. All default registry keys are created during installation.

**ONEDRIVE=**

```
ONEDRIVE=1
```

Activates the support of Microsoft OneDrive for the respective user for which the setup is intended.

**Examples:**

```
msiexec /i C:\Install\LCClient.msi /qn AddLocal=ALL
```

A complete installation of *u.trust LAN Crypt* is performed. The program is installed in the default installation directory (`\<System drive\>:\Program Files\Utimaco\u.trust LAN Crypt`).

```
msiexec /i C:\Install LCClient.msi /qn AddLocal=UserApplication,ShellExtensions
Productlanguage=1033
```

The installation of *u.trust LAN Crypt* is executed. The program is installed in the default installation directory (`\<System drive\>:\Program Files\Utimaco\u.trust LAN Crypt`) with the user application, explorer extensions and English MSI language package, but without the Client API.

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

**Note**

- Please note that the installation program will be aborted if the line after the parameter "AddLocal=" remains empty or a parameter is entered incorrectly there.

## Removing u.trust LAN Crypt Client

You can only remove the *u.trust LAN Crypt* Client if you have Windows administrator privileges.

Select Start -> *Settings* -> *Apps*. Double click on **u.trust LAN Crypt Client** in the list of Apps and click on the **Uninstall** button. In the following dialog click again on the **Uninstall** button. The *u.trust LAN Crypt* Client is uninstalled. Restart your computer afterwards.

**Note**

- Sometimes the required *Visual C++ runtime libraries* are not (or no longer) installed on some client computers. Because of this missing component, *u.trust LAN Crypt* cannot be uninstalled on these computers. An error message during the uninstallation then indicates that there would be a problem with the Windows Installer package. In this case you have to install the required *Visual C++ runtime libraries* on the affected client computer. You can find them at the following URLs:

https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170

https://aka.ms/vs/17/release/vc_redist.x86.exe

https://aka.ms/vs/17/release/vc_redist.x64.exe

After you have successfully installed the required *Visual C++ runtime libraries* on the client computer, it should be possible to uninstall *u.trust LAN Crypt* again without errors.

**Note**

- Encrypted files can no longer be decrypted after *u.trust LAN Crypt* Client has been removed.

**Note**

- Do not install *u.trust LAN Crypt* Client again immediately after you have removed it. You must reboot the machine at least once before you install it again.

## Uninstallation Without User Interaction

**Prerequisite:** The MSI package that needs to be uninstalled must be present on the system.

Example:

```
msiexec /X {00000000-0000-0000-0000-000000000000} /qn /norestart
```

This command uninstalls the MSI package with the ProductCode {00000000-0000-0000-0000-000000000000} in silent mode and prevents the system from restarting.

**Command Line Options:**

**/X {ProductCode}**

The ProductCode of the MSI package to be uninstalled. The ProductCode can be extracted from the MSI file itself.

**/qn**

Executes the uninstallation in silent mode, without displaying any user interface to the user.

**/norestart**

Prevents a system restart after the uninstallation.

# Custom error messages in LAN Crypt Client

LAN Crypt Client offers the option of storing individual messages for specific error messages. This allows you to expand on the standard messages with your own notes, for example with a reference to IT support.

**Note**

- Currently, adding your own information is only supported for error messages related to **loading profiles (LoadProf)**.

## Setup

The user-defined texts are stored in the following registry path:
'HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client'

For each error message to be added, a separate subdirectory must be created in the format: 'Client-MsgId-'

The `<error code>` corresponds to the error code of the error message in question. For error code **1056**, for example, the path is:
'HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client\Client-MsgId-1056'

**Note**

- The error code can be identified via the linked document (subject to change) or by reproducing the error.

Messages can be stored in different languages within this registry. The language and country code is used as the name of the entry (`de-DE`, `de-AT`, `en-US`, etc.).

The respective value contains the message to be appended. Please note that the message must not exceed **a maximum of 1000 characters**. If this length is exceeded, the message will not appear in the error message.

# Integrating documentation in an environment without internet access

If LAN Crypt is used in an environment without access to the public internet, the client’s integrated links to the online help will not function. To still provide a direct link to local or internal documentation, the following registry value can be set:

```
HKLM\SOFTWARE\Policies\conpal\LAN Crypt\HelpURL
```

This setting allows you to specify an alternative help file, such as the local PDF documentation.The registry value must be set to an absolute URL path that is accessible from the client system (e.g., "https://intranet.local/docs/lancrypt_help.pdf").

# Compatibility with Cloud Services

LAN Crypt supports the encryption of files stored on cloud-based platforms, providing an additional layer of protection against unauthorized access - even by the operators of the cloud services themselves. Cloud providers such as Microsoft, Google, and similar platforms typically offer additional capabilities, such as collaborative document editing or content-based file search. Since these services cannot access the contents of encrypted files, such features are unavailable for files protected by LAN Crypt. The encrypted data is subject to a particularly high level of protection and therefore cannot be processed by these services.

## Microsoft 365 Services Not Compatible

The following Microsoft 365 features require content-level analysis and therefore cannot be used with files encrypted by LAN Crypt:

- Mail flow rules, including anti-malware and anti-spam checks that require access to attachments
- Microsoft Delve
- eDiscovery
- Content search and indexing

### * Office Web Apps, including collaborative document editing

# Reporting Security Vulnerabilities

Utimaco recognizes that strong security is built through collaboration. We are committed to working responsibly and constructively with customers, security professionals, security researchers, and the broader community to identify and address vulnerabilities.

We welcome and encourage responsible reporting of vulnerabilities. Every report we receive is treated with diligence and urgency, and we aim to acknowledge submissions promptly, communicate responsibly throughout the investigation process, and share relevant updates (Security Advisories and patches) as they become available.

If you discover a vulnerability, we encourage you to report it urgently and securely to the Utimaco PSIRT (Product Security Incident Response Team) who will address the report with urgency.

Any vulnerability report must be submitted encrypted, using PGP encryption, thereby preventing critical information from being accidentally disclosed.

## (Step 1) Prepare Your Report

Include as much detail as possible to help us understand and reproduce the issue:

```
Short summary of the vulnerability Description of the vulnerability Affected
product(s), version(s), and configuration Describe product environment Operating System
used. Step-by-step reproduction instructions Possible Root cause. Proof-of-concept
code, screenshots, or logs (if available) Potential impact and suggested remediation
(optional) Your contact information for follow-up and public PGP encryption key.
```

Any reports will be handled strictly confidentially, and no personal data will be shared with third parties

## (Step 2) Encrypt Your Email with PGP

To protect sensitive information, you must encrypt your report using our PGP public PSIRT key before sending it.

1. Import our PSIRT public key (provided below) into your PGP/GPG tool.
2. Encrypt Vulnerability report using this key
3. Submit email to PSIRT@utimaco.com with encrypted attachment.
4. Optionally, sign your message with your own PGP key so we can verify authenticity.

## PSIRT Contact

**PSIRT team:** PSIRT@Utimaco.com

**PGP fingerprint:** 77F3 05F8 11AF 228B 7623 33E5 DA5F 264E A9C1 64CB

**PGP Key:** Download

---

# Technical Support

**To access technical support for Utimaco products do the following:**

All maintenance contract customers can access further information and/or knowledge base items at the following link support.Utimaco.com. As a maintenance contract customer, send an email to technical support using the support@Utimaco.de email address and let us know the exact version number, operating system and patch level of your Utimaco software and, if applicable, a detailed description of any error messages you receive or applicable knowledge base items.

# Legal notice

Copyright © 2024 - 2026 Utimaco IS GmbH, 2018 - 2024 conpal GmbH, 1996 - 2018 Sophos Limited and Sophos Group. All rights reserved. conpal®, AccessOn® and AuthomaticOn® are registered trademarks of conpal GmbH.

All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid 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.

---

**Last updated 21.09.2026**