What is u.trust LAN Crypt for Linux?

With 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 ring 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 authorization 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.

Data protection with u.trust LAN Crypt for Linux

u.trust LAN Crypt guarantees that sensitive files can be stored encrypted. 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 run 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 the users via policy files. Policy files contain all rules, access rights, and keys required for encryption. The policy file is protected by a certificate. In order for users to process files encrypted with *u.trust LAN Crypt* on their computers, they must have access to the policy file. By owning the private key belonging to the certificate, the user has access to the policy file in which the encryption profile is stored. In the case of configuration with u.trust LAN Crypt Cloud as administration, the profiles are automatically downloaded and cached when the user logs in.

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

Differences between u.trust LAN Crypt for Windows and u.trust LAN Crypt for Linux

The following differences refer to the configuration with u.trust LAN Crypt Admin for Windows as administration and **not** to the configuration with u.trust LAN Crypt Cloud as administration.

Configuration file substitutes group policy

All settings are made via the config.toml file, which must be created after installation (see Create and configure the configuration file).

A configuration file is necessary because the Linux client itself cannot use Windows group policies. The configuration file therefore contains all settings required by the Linux client, such as the paths where the policy file, the public certificate of the security officer, and the user's key file are stored.

Encryption algorithms supported by u.trust LAN Crypt for Linux

u.trust LAN Crypt for Linux supports the following encryption algorithms:

- AES-256 bit
- AES-128 bit

Note

- Please note in this context that u.trust LAN Crypt for Windows also supports other encryption algorithms (such as "IDEA" or "3DES", etc.). u.trust LAN Crypt for Linux loads all rules from a policy. However, rules that prescribe an unsupported encryption algorithm are dropped.

In case the (master) security officer has activated the "Key Wrapping" option (default setting), security officer data and user profile data are encrypted with a randomly generated session key using the selected algorithm (default: AES). This key is then in turn RSA-encrypted with the public key from the certificate.

u.trust LAN Crypt for Linux supports the following encryption algorithms for Key Wrapping:

- AES-256 bit

Encryption

Access to encrypted files

To be able to read or write encrypted files, a user always needs the key required for this purpose. All keys and encryption rules are assigned to users by the security officer via their policy file.

If the user has the required key with which files are encrypted, he can always open them. This is especially true even if there is no encryption rule in the profile policy for an SMB share and for the directories and files there.

If a network share is covered by an encryption rule, quick access to the mounted folder is available within the *u.trust LAN Crypt for Linux* client.

SMB share encryption

To ensure the correct encryption of your SMB shares, the paths specified in the encryption rules must exactly match the remote path of the mount point, that is, the path to the server, not the local path under which the share is mounted. If the paths do not match exactly, encryption will not be activated.

Before encryption rules can be applied to a network share, the network share must first be mounted in u.trust LAN Crypt for Linux.

To do this, open the Volumes tab in the client. It displays the network shares available on your system as well as those already mounted. Then click Add to mount a network share.

Alternatively, the network share can be mounted in u.trust LAN Crypt for Linux from the terminal using the lancryptctl tool.

Note

- LAN Crypt can only use network drives if they are mounted via a local mount point and appear in the output of the `mount` command. Network drives that have only been connected through a file manager such as Dolphin cannot be used by LAN Crypt.

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.

Configuration with u.trust LAN Crypt Cloud as administration

Login and access with a u.trust LAN Crypt Cloud account

To access his encryption profile, a user must first successfully complete the registration of a u.trust LAN Crypt Cloud account. Once the registration is completed, all policies and settings set by the security officer are assigned to the user account. When the policy file is loaded for the first time, the user is prompted to log in to the u.trust LAN Crypt Cloud using their account details. Upon successful login, the assigned policies are automatically downloaded and stored in the client.

Configuration with u.trust LAN Crypt Admin for Windows as administration

Create and configure the configuration file

All settings for {{ site.productName*linux*en }} are made via the configuration file config.toml. Create this file after installation in the following path:

`/home/<user>/.config/lancrypt/config.toml`

Then add the following parameters to the configuration file:

``` [onprem.general] profile*refresh*interval = 120

[onprem.certificates] storage*path* = *"~/certs" so*cert_path = "~/socerts"

[onprem.profile] storage_path = "~/profiles" ```

| Section | Parameter | Description | Default value |
|---|---|---|---|
| `[onprem.general]` | `profile_refresh_interval` | Interval (in seconds) at which profiles are updated | `120` |
| `[onprem.certificates]` | `storage_path` | Directory for storing the certificates | `~/certs` |
| `[onprem.certificates]` | `so_cert_path` | Directory for storing the public certificates (.cer) of the security officer | `~/socerts` |
| `[onprem.profile]` | `storage_path` | Directory for storing the profile | `~/profiles` |

## Certificates

Before users can access their encryption profile, their **PKCS#12 key file** (their certificate) and the security officer's **public certificate (.cer)** must be present on the computer in the directories defined in the configuration file (see Create and configure the configuration file).

The security officer distributes these certificates to the users, along with the password or PIN needed to unlock the certificate. If the certificates are in place at the first logon, the entire process up to PIN entry runs automatically.

The certificate is checked every time the encryption profile is loaded. If a valid certificate is found, the user is logged on and the encryption rules are applied. Otherwise, the user cannot work with encrypted data.

**Note**

- Do not change the file names of the certificates exported from the Admin Console, otherwise they cannot be imported automatically.
- If errors occur during logon, read the log using the following command:
  `journalctl --user --grep lancrypt`
```

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 policy files are stored in a path defined for this purpose (network share). For *u.trust LAN Crypt for Linux* to find the policy file, the location must be defined in the configuration file. This also applies to the path where the public certificate of the security officer can be found.

When a user logs in to *u.trust LAN Crypt for Linux*, the encryption profile stored in the policy file is loaded. If the user holds the proper key, the profile is decrypted and the encryption rules are applied.

Loading the policy file

u.trust LAN Crypt default behavior

When a user logs in, their cached user profile is loaded first. *u.trust LAN Crypt for Linux* automatically searches for new policy files for the user if the configured policy path or, if used, the u.trust LAN Crypt Cloud is accessible. When a new policy file is found, the cached policy is updated.

The user can start working with encrypted files while *u.trust LAN Crypt* continually checks for new versions of the policy. If the specified policy location is not accessible, the cached profile is used.

In the case of using configuration with u.trust LAN Crypt Cloud as administration, the cached profile is used until the update interval expires. This means that the time limit set in the u.trust LAN Crypt Cloud is used for how long a cached profile is valid before the policies need to be updated.

Loading an updated policy file manually

To reload the policy manually, open the client and click **Reload profile** on the **Status** tab.

Client status information

u.trust LAN Crypt for Linux provides detailed information about its state. The available information is divided into individual tabs as follows:

Status

Shows the current program status, including the logged-on user as well as the lifetime and update interval of the loaded policy.

Volumes

Shows all network shares available for mounting as well as the network shares already mounted in LAN Crypt.

Rules

Lists all encryption rules assigned to the user.

Keys

Lists all keys available to the user.

Events

Shows a chronological log of LAN Crypt activity.

About

Shows product information, including the installed version.

Using "lancryptctl"

In addition to the program components, a console application "lancryptctl" is installed. This tool can be useful when solving technical problems. It provides users with advanced functions of *u.trust LAN Crypt for Linux*, which are described below.

Calling the tool

Call the tool in a terminal using the following syntax:

```
lancryptctl [COMMAND]
```

For an overview of all available commands, use `lancryptctl --help` or `lancryptctl help`. To display the help for an individual command, use `lancryptctl help <COMMAND>`.

Technical support

To access technical support for Utimaco products do the following:

All maintenance contract customers can access further information, such as knowledge base items, at support.Utimaco.com.

As a maintenance contract customer, send an email to technical support at support@Utimaco.com and let us know the version number(s), operating system(s) and patch level of your Utimaco software and, if applicable, the exact wording of any error messages.

Legal notice

Last updated 01.09.2026