u.trust LAN Crypt macOS

EN

utimaco®

Imprint

Copyright 2023	Utimaco IS GmbH
	Germanusstr. 4 D-52080 Aachen Germany
	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
Phone	EMEA +49 800-627-3081
	APAC +81 800-919-1301
	https://support.hsm.utimaco.com/
Internet e-mail	support@utimaco.com

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 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 for macOS

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 largely without user interaction. No special security software needs to be installed on the file server itself.

A security officer can define access authorizations for specific folders and files. Those permissions are summarized in encryption profiles which are stored in a so-called policy file, along with the encryption keys that have been assigned to a user. The policy file is encrypted with a user-specific key and signed by the security officer to protect against malicious modifications. On the endpoint, legitimate users can use decode the encryption profiles along with the assigned keys. Once loaded into the system, they have full access to data encrypted with *u.trust LAN Crypt*. 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 sharing the same encryption profile in their policy file are members of an authorization group. Encryption keys necessary for accessing encrypted files are assigned automatically. Policy files must be deployed to the client for any updates to take effect. As soon as the policy file has been deployed to the client, files can be encrypted or decrypted as soon as they are opened or closed. All forms of organization can be mapped from a LAN model in which users are 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 macOS

The following differences refer to the configuration with {{ site.productName*admin*windows_en}} 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.plist file, which must be created after installation (see Configuration).

A configuration file is necessary because the macOS client itself cannot use Windows group policies. The configuration file contains all necessary settings for the client, such as paths to policy files, certificates, and the user's key file.

Encryption algorithms supported by u.trust LAN Crypt for macOS

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

- AES-256 Bit (XTS-Modus)
- AES-256 Bit (CBC-Modus)
- AES-128 Bit (XTS-Modus)
- AES-128 Bit (CBC-Modus)

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 macOS accepts policies

containing rules with unsupported encryption algorithms. But due to the lack of support, it simply drops such rules.

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 macOS supports the following encryption algorithms for Key Wrapping:

- AES-256 Bit
- 3DES

Note

- When using security tokens or smart cards, make sure the hardware and/or the middleware software supports the selected algorithm.

Encryption

Access to encrypted data

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.

Note

- However, if an SMB share has an "Ignore rule", a user will not be able to open encrypted files contained there, even if the user has the required key.

If a network share is covered by an encryption rule, quick access to the mounted folder is available in the *u.trust LAN Crypt for macOS* menu bar item.

SMB Share Encryption

To ensure the correct encryption of your SMB shares, it is crucial that the paths specified in the encryption rules exactly match the paths of your mount points. If the paths do not match exactly, encryption will not be activated.

Example of a correct match:

Rule: `smb://newhost.newdomain.local/newpath/anotherpath/*.*`

Mount: `smb://newuser@newhost.newdomain.local/newpath`

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.

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 on all local drives.
- Files in folders which are defined in *u.trust LAN Crypt* with an “exclude” or “ignore” rule.

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 his u.trust LAN Crypt Cloud account{:target="_blank"}. Once the registration is completed, all policies and settings set by the security officer will be 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 configuration file

All settings for *u.trust LAN Crypt for macOS* are made via the configuration file config.plist, which must be created after installation. A template is supplied and installed in the directory:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources/
config.plist.template
```

After editing the template, copy it to the location below:

```
~/Library/Application Support/de.{{ site.company_name_small }}.lancrypt/config.plist
```

Mandatory settings in the configuration file

PolicyPath: Mount point to the policy file

In the `<string>` section, enter the path to a mounted network share or local location where the users' policy files (.xml.bz2) are stored.

Example:

```
<key>PolicyPath<key> <string>/Volumes/polices</string>
```

or

```
<key>PolicyPath<key> <string>\\server\share\policies</string>
```

or

```
<key>PolicyPath<key> <string>smb://server/share/policies</string>
```

SOCertLocation: Mount point to the security officer's public certificate

In the `<string>` section, enter the path to a mounted network share or local location where the security officer's public certificates (.cer) are stored.

Example:

```
<key>SOCertLocation</key> <string>/Volumes/certificates</string>
```

or

```
<key>SOCertLocation</key> <string>\\server\share\certificates</string>
```

or

```
<key>SOCertLocation</key> <string>smb://server/share/policies/certificates</string>
```

Optional settings

You can also configure optional settings in the configuration file. These settings are important if, for example, the user login name on macOS differs from the user's name in the *u.trust LAN Crypt* Administration.

UserName: Login name of the user

If the directory username and the local username do not match, `UserName` must be set to the name of the user in the *u.trust LAN Crypt* Administration. Only if the login name and the policy file name are identical, the user can properly work with *u.trust LAN Crypt for macOS*.

CertificatePath: Mount point to the key file (.p12) of the user

After specifying the mount point for the key file (.p12) of the user, *u.trust LAN Crypt for macOS* automatically tries to import a .p12 key file into the user's keyring if the private key of the policy file is not available.

This file must be named after the respective user-login:

[LOGIN_NAME].p12

Note

- If users are to be logged in with a security token or smart card, the whole (`<key>CertificatePath</key>`) entry must be omitted.

DisableCertificateValidation: Disable Certificate Validation

You can specify whether any errors found when checking user certificates are to be ignored.

Example:

```
<key>DisableCertificateValidation</key> <true/>
```

This setting is useful if the validity period of a certificate has expired, and no new certificate is available yet. To ensure that a user can continue to access their encryption profile, the option allows to disable checking of the certificate's validity period. Once the new certificates are available, this setting can be disabled again by changing the parameter for this setting to **false**.

Note

- Alternatively, trust settings can also be configured in Keychain Access. However, ignoring errors that occur during certificate checks always means a reduction in security.

AgentEnvironment: List of environment variables

When using a policy with keywords that should resolve to a specific value, an administrator can do so by specifying them in **AgentEnvironment**.

Example:

```
<key>AgentEnvironment</key> <dict> <key>%Username2%</key> <string>steve</string>
<key>%directory1%</key> <string>finances</string> <key>%directory2%</key>
<string>management</string> </dict>
```

PolicyUpdateInterval: Policy Update-Interval

Time interval between checks for new policies (minutes). If a new policy is available, it will be automatically loaded and applied.

Example:

```
<key>PolicyUpdateInterval<key> <integer>240</integer>
```

Certificates

Before users can access their encryption profile, the corresponding certificate must be available on the Mac. The security officer distributes these certificates to the users along with the corresponding password or PIN to access them. A path where the *u.trust LAN Crypt* Administration stores the user certificates as well as the public certificate (*.cer*) of the Security Officer must be configured. From this path, users then import their **PKCS#12 key file** (their certificate) onto their computer. If the certificates are available at the first logon, the entire process up to PIN entry runs automatically without any user interaction.

Note

- If the login to *u.trust LAN Crypt* fails, errors will be logged to the system log. To filter for *LAN Crypt*, set the subsystem to `de.{{ site.company_name_small }}.lancrypt`. Also enable the "Include Info Messages" and "Include Debug Messages" options in Console. Alternatively, you can also view this information live in Terminal using the following command: `log stream --level debug --predicate 'subsystem == "de.{{ site.company_name_small }}.lancrypt"`
- *u.trust LAN Crypt* verifies the certificates of the user and the public certificate (.cer) from the (Master) Security Officer, who created the policy file. If the certificate contains a "CRL Distribution Point" and no valid CRL is present on the system, *u.trust LAN Crypt for macOS* initially does not trust this certificate. In the user's Keychain, the user can change the trust setting and then assign the setting "Always Trust" for this certificate.

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.

Encryption rules with their assigned keys from 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.

Note

- In order for *u.trust LAN Crypt for macOS* to import the certificates automatically, it is important that the file names of the certificates exported from the Admin Console are not changed.

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 macOS* 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*, the encryption profile stored in the policy file is loaded by *u.trust LAN Crypt for macOS*. If the user holds the proper key, the profile is decrypted end the encryption rules are applied.

Logon with token

Users can also log on to *u.trust LAN Crypt for macOS* 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 certifi-cate is found on a token connected to the system, the user is logged on.

Note

- If users are to be logged in with a security token or smart card, you may not enter a mount point to the user's key file (.p12) in the configuration file.

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 macOS* 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.

Client Status-Information

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

Status

Shows general information about the program status. In addition to information about the active user, the lifetime and update interval of the loaded policy are also displayed.

Rules

This tab lists all active encryption rules.

Keys

This tab list all keys available to the user.

About

This tab shows information about the program version. The instruction manual can also be opened on this page.

Encryption for cloud storage services and network shares.

To add a cloud storage or network share for encryption, click the u.trust LAN Crypt icon in the status bar.

Select the type of storage you want to add (cloud or network). OneDrive and Google Drive are supported for cloud connectivity. After adding your desired storage, a corresponding entry/location will be created in the Finder sidebar, collecting all added file shares.

To remove a network storage, click the status bar icon of u.trust LAN Crypt again and select the eject icon next to the respective network share.

The option to remove a cloud storage connection is located in the settings of *u.trust LAN Crypt for macOS* in the **Accounts** section.

Usage

When browsing the respective folder structure in the Finder, the system creates dataless files for each item found on the user's drive. These dataless files do not occupy space on the device and are downloaded only when the user actively opens a file or uses **Download Now** in the context menu. Downloaded files and modified files that have been successfully synced back to OneDrive/Google Drive can also be removed from the device to free up storage space. This action is also available in the context menu.

To share a file or folder with others, the **Show Online** option in the context menu takes the user to the file or folder in the online view of the respective cloud storage service using the default browser. The user can now use the familiar **Share** functionality here, for example.

Note

- There is no keyword for OneDrive or Google Drive in the *u.trust LAN Crypt* administration. Only relative rules are supported.
- Files that are subject to an encryption rule are encrypted when their content is uploaded to the cloud.
- When the content of encrypted files is downloaded, it is decrypted if the corresponding encryption key is available.
- Every file in OneDrive/Google Drive has a version history. Uploading an encrypted version of a file does not remove its history. It is therefore possible to restore an unencrypted version.
- The supported cloud storage services and *u.trust LAN Crypt for macOS* can work in parallel without any problems. *u.trust LAN Crypt for macOS* can be used as a replacement for the clients of OneDrive and Google Drive.
- Encryption functions are only available when folders are accessed via the *u.trust LAN Crypt* location.

Enable Quick Action extension

u.trust LAN Crypt for macOS comes with a Quick Action extension for quickly viewing file-specific encryption information. For this to work, however, you must first enable the extension within the System Preferences.

To do this, simply follow these steps:

1. Open the **System Preferences**.
2. Now click on **Extensions**.
3. Now select the **Finder** tab on the left and activate the Quick Action extension **Encryption Information**.

To view the encryption information of a file, you can now right-click on it and access it via **Quick Actions**. If files are not subject to any rule and the key is available, they can also be decrypted directly via the encryption information dialog.

Installation

Installing u.trust LAN Crypt for macOS

u.trust LAN Crypt for macOS supports the following versions of macOS:

- **macOS 14 Sonoma**
- **macOS 13 Ventura**

Open the file **{{ site.productName*with*company}}.pkg** and follow the specified installation steps. Apart from that, there are no further settings to be made in the operating system settings.

Uninstalling u.trust LAN Crypt for macOS

Open **Uninstaller.pkg** from the path below and proceed through the dialogs.

```
/Library/Utimaco/u.trust LAN Crypt/Uninstaller.pkg
```

Note

- FileVault must be activated to use u.trust LAN Crypt for macOS
- After uninstalling *u.trust LAN Crypt for macOS*, encrypted files can no longer be decrypted. Uninstalling *u.trust LAN Crypt for macOS* does not decrypt files.

Using "lcutil"

In addition to the program components, a console application ‘lcutil’ is installed. This tool can be useful when solving technical problems. It is installed in the following directory:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources
```

This provides users advanced functions of u.trust LAN Crypt for macOS, which are described below.

Print version information of u.trust LAN Crypt for macOS

To print the version information of u.trust LAN Crypt for macOS, the user must open the terminal and execute the following command:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources/lcutil version
```

Collect logs

You can export all u.trust LAN Crypt for macOS logs to a file (.xz). Certain events can be recorded, evaluated, archived, and checked at any time in this way.

To export all u.trust LAN Crypt for macOS logs in a file, the user must open the terminal and executing the following command:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources/lcutil collect-logs
```

The following events are collected in the log file:

- System log
- Mount table
- Process table
- Version information
- System profiler
- Cached policies
- Config.plist
- Crashdumps
- Information about configured cloud provider accounts

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.de. 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

Last updated 27.03.2024