conpal LAN Crypt

Persistent
Highly secure
Scalable

macOS

Product version: 1.0.0
Document date: July 2021

TABLE OF CONTENTS

1 What is conpal LAN Crypt? 3

1.1 Data protection with conpal LAN Crypt 3

1.2 Differences between conpal LAN Crypt for Windows and macOS 4

2 Encryption 5

2.1 Transparent Encryption 5

2.1.1 Access to encrypted data 5

2.1.2 Explicit decryption of files 6

2.1.3 Files and folders excluded from encryption 6

2.2 Transparent encryption and file-compression tools 6

3 Configuration 6

3.1 Create configuration file 6

3.1.1 Entries of the configuration file 8

3.1.2 Reload configuration file 11

3.2 Certificates 11

3.3 Loading the policy file 12

3.3.1 *conpal LAN Crypt* default behavior 12

3.3.2 Load updated policy file manually 13

3.4 Logon to conpal LAN Crypt 13

3.4.1 Logon with token 13

4 Installation 14

4.1 Removing conpal LAN Crypt for macOS 17

5 Functions of the console application “lcutil” 18

5.1 Print version information of conpal LAN Crypt for macOS 18

5.2 Collect logs 18

6 Technical support 19

7 Legal notices 20

1 What is conpal LAN Crypt?

With transparent file encryption, *conpal LAN Crypt* enables the exchange of confidential data within authorization groups in small, medium and large organizations. *conpal 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 *conpal LAN Crypt*. A master security officer (MSO) has the right to manage *conpal 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. *conpal 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 *conpal LAN Crypt*), but without the corresponding *conpal 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.

1.1 Data protection with conpal LAN Crypt

conpal 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 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 user decode the encryption profiles along with the assigned keys. Once loaded into the system, they have full access to data encrypted with *conpal LAN Crypt*.

conpal LAN Crypt enables users to be divided into different authorization groups. *All conpal 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 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 users are administered centrally to a distributed model in which users only use notebooks.

1.2 Differences between conpal LAN Crypt for Windows and macOS

Configuration file substitutes group policy

The client version *of conpal LAN Crypt for macOS* does not have a user menu in version 1.0.0. All settings are made via the `config.plist` file, which must be created after installation (see "Create configuration file") on page 6.

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

Encryption algorithms supported by conpal LAN Crypt for macOS

conpal LAN Crypt for macOS supports the following encryption algorithms:

- AES-256 bit (XTS mode)
- AES-256 bit (CBC mode)
- AES-128 bit (XTS mode)
- AES-128 bit (CBC mode)

Note: Please note in this context that *conpal LAN Crypt* for Windows also supports other encryption algorithms (such as "IDEA" or "3DES", etc.). If the Security Officer creates encryption rules that (also) apply to *conpal LAN Crypt for macOS*, only the above-mentioned AES encryption algorithms may be used.

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.

conpal LAN Crypt for macOS supports the following encryption algorithms for Key Wrapping:

- AES-256 bit
- 3DES

Note: If you are using security tokens or smart cards, please make sure that they or the middleware used in this context also supports the algorithm you have selected. If this is not the case, select another compatible algorithm as an alternative.

2 Encryption

2.1 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: *conpal LAN Crypt for macOS* version 1.0.0 currently cannot encrypt or decrypt local files on the Apple computer itself. *conpal LAN Crypt for macOS* can encrypt and decrypt files on SMB shares. All drives on which files are encrypted or decrypted first have to be mounted on the Apple computer. Using the Finder window, you can mount the desired drives or SMB shares.

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

- All files for which an encryption rule exists for, 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 *conpal 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 encrypted files are renamed, they remain encrypted. If a different encryption rule is applicable to the newly chosen filename, the file gets encrypted according to this rule. However, a rename operation will never result in a decryption of the file.
- If a user copies encrypted files to another folder within the same SMB share or to another SMB share that does not have an encryption rule, the files are automatically decrypted. If files are moved within the same SMB share, they remain encrypted. **This also applies to folders for which an "Exclude" or "Ignore" rule exists** (see Administrator's Manual, section "Generating encryption rules").

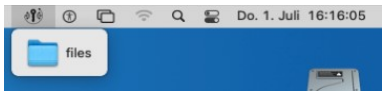
2.1.1 Access to encrypted data

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.

To access encrypted files in quick access, users have to click on the key symbol of *conpal LAN Crypt for macOS* at the top right of your desktop. Then click on the folders shown there. All encrypted SMB shares are listed and can be opened after 30 seconds.



2.1.2 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
- and the active encryption profile does not contain an encryption rule for the new location.

2.1.3 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 *conpal LAN Crypt* with an “*exclude*” or “*ignore*” rule.

2.2 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. To retain protection provided by encryption it is recommended to have target folder or file used for compressed storage covered by an encryption rule.

3 Configuration

3.1 Create configuration file

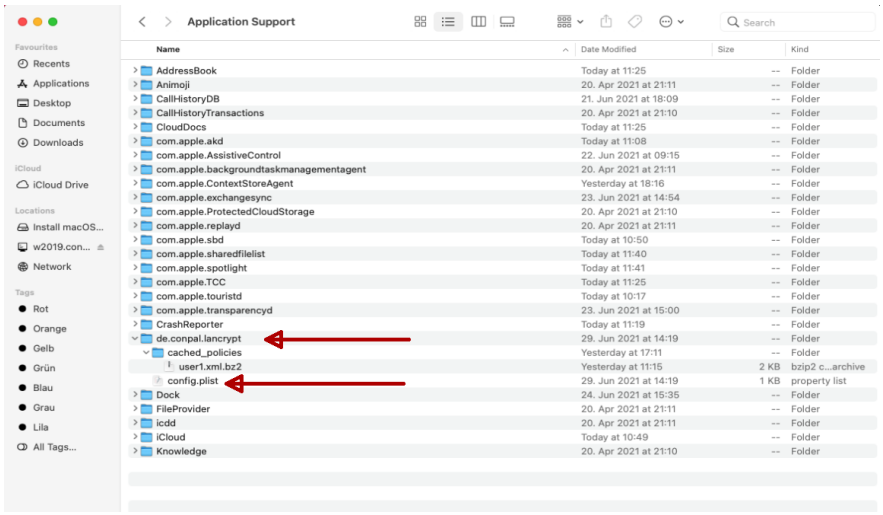
All settings for *conpal LAN Crypt for macOS* are made via the configuration file `config.plist`, which must be created after installation. This file contains all settings required for *conpal LAN Crypt for macOS*, such as the paths where the policy files (*.bz2*), the public certificates (*.cer*) of the (Master) Security Officer and the key files of users (*.p12*) are stored, so that *conpal LAN Crypt for macOS* can find them. A PLIST template is supplied and installed in the directory:

`/Library/conpal/LAN Crypt/useragent.app/Contents/Resources/config.plist.template`.

It is recommended to use this file as a template and configure the individual options as required.

Once created, this file must be copied to the folder below:

`~/Library/Application Support/de.conpal.lancrypt/`



The configuration file of *conpal LAN Crypt for macOS* is structured as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <!-- Mandatory; Mountpoint for a share where policies are located -->
        <key>PolicyPath</key>
        <string>/Volumes/share/policies</string>

        <!-- Mandatory; Mountpoint for a share where the SO certificate is located -->
        <key>SOCertLocation</key>
        <string>/Volumes/share/keys</string>

        <!-- Optional; Only needed if the username on the machine differs from the username in the policy -->
        <key>UserName</key>
        <string>LANCryptUser</string>

        <!-- Optional; Mountpoint for a share where certificates are located -->
        <key>CertificatePath</key>
        <string>/Volumes/share/keys</string>

        <!-- Optional; When set to true, for every connected network share a mountpoint will be created -->
        <key>AutoMountAllNetworkShares</key>
        <true/>

        <!-- Optional; When set to true, certificates will not be validated -->
        <key>DisableCertificateValidation</key>
        <false/>

        <!-- Optional; Additional keywords used when expanding keywords in the policy -->
        <key>AgentEnvironment</key>
        <dict>
            <!-- will expand %custom_key% in rule to custom_value -->
            <key>custom_key</key>
            <string>custom_value</string>
        </dict>
    </dict>
</plist>
```

3.1.1 Entries of the configuration file

1. Mount point to the policy file (<key>policypath<key>).

In the <*string*> section, enter the network share where the users' policy files *(.xml.bz2*) are stored.

Example:

```
<key>Policypath<key>
<string>/Volumes/lancrypt/Profile</string>
```

2. Mount point to the security officer's public certificate (<key>SOCertLocation</key>).

In the <*string*> section, enter the network share where the security officer's public certificates (*.cer*) are stored.

Example:

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

Note: It is essential to enter the mount points to the policy file (*.bz2*) and to the public certificates (*.cer*) of the security officers in the configuration file.

Optional settings of the configuration file

You can also make additional optional settings in the configuration file. These settings are important if, for example, the user login name on the mac computer differs from the user's name in the *conpal LAN Crypt* Administration.

3. Login name of the user (<key>UserName</key>)

The attribute for the login name has a special meaning. *conpal LAN Crypt* names the policy files according to the login name of the user. Only if the login name and the policy file name are identical, the user can log in to *conpal LAN Crypt for macOS*. Since the user login name on the mac computer could be different, you must enter the name matching the policy file in the configuration file. Only then *conpal LAN Crypt for macOS* can load the correct policy file.

4. Mount point to the key file (.p12) of the user (<key>CertificatePath</key>)

After specifying the mount point for the key file (*.p12*) of the user, *conpal 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 called "*Login Name.p12*" so that it can be recognized by the relevant user.

Note: If users are to be logged in with a security token or smart card, the whole (<key>Certificate-Path</key>) entry has to be omitted.

5. Auto-mount all network shares (<key>AutoMountAllNetworkShares</key>)

If you set the associated parameter to "**true**", *conpal LAN Crypt for macOS* will automatically provide all currently connected and all SMB shares that will be connected in the future for transparent file encryption.

Example:

```
<key>AutoMountAllNetworkShares</key>
<true/>
```

In the example above, all mounted SMB shares will be automatically mounted as LCFS shares. *conpal LAN Crypt for macOS* can then access these mounted shares.

Note: Support for relative paths requires a mount-point to begin with. If this option is set to "**false**", the system will not automatically create mountpoints for SMB shares. Hence if their policy does not include explicit rules using full path names, rules based on relative paths won't be applied. In that case, paths in encryption rules must always be defined as absolute paths.

Example:

```
\\server\my_data\*.*
```

6. Disable Certificate Validation (<key>DisableCertificateValidation</key>)

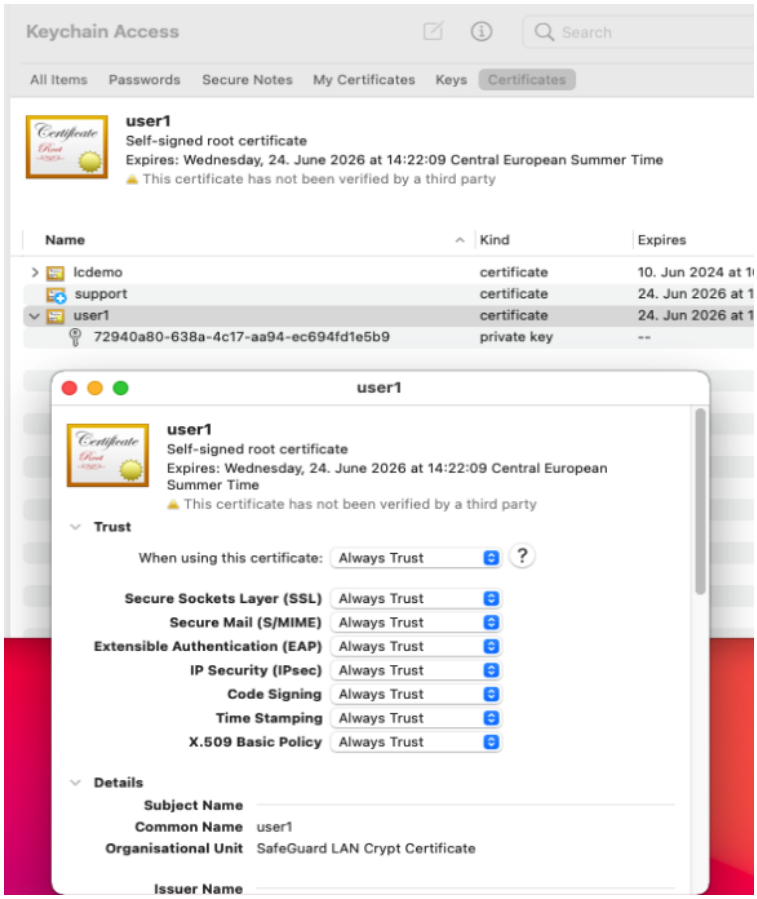
You can specify whether any errors found when checking user certificates are to be ignored.

Example:

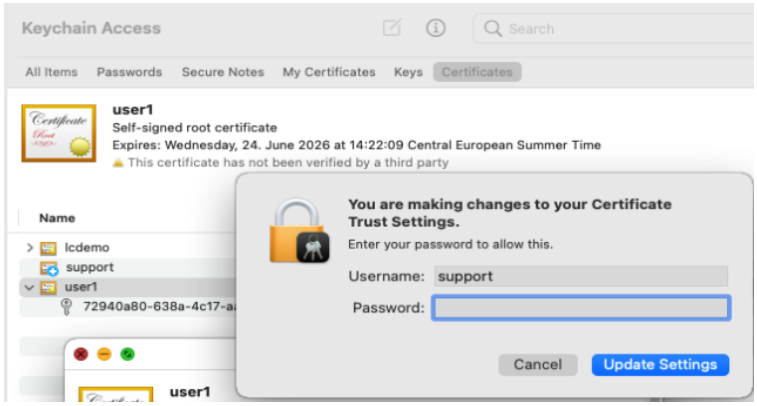
```
<key>DisableCertificateValidation</key>
<true/>
```

This setting is useful if the validity period of a certificate has expired and no new certificate is not yet available. To ensure that a user can continue to access their encryption profile, the option allows to disable checking of the certificate's validity period. As a result, the same certificate, which has actually expired, can still be used. Once the new certificates are available, this setting can be disabled again by changing the parameter for this setting to "**false**".

Note: Alternatively, you can also manually set its trust setting via the *Keychain Access* and thus, for example, **Always Trust** a certificate.



Note: Changes of trust settings always require explicit authorization via login.



Note: Ignoring errors that occur during certificate checks always means a reduction in security.

7. Use environment variables (<key>AgentEnvironment</key>)

Here you can define environment variables that you have used for encryption rules in policy files. So that these can also be resolved accordingly by the mac computer, you must assign the appropriate values or names to these environment variables.

Beispiel:

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

Note: There is no limit to the number of environment variables that you can define in the section *<key>AgentEnvironment</key>*.

3.1.2 Reload configuration file

To reload a changed configuration file ("*config.plist*"), the user must open the terminal and execute the following command there:

```
launchctl unload /Library/LaunchAgents/de.conpal.lancrypt.useragent.plist
&& launchctl load /Library/LaunchAgents/de.conpal.lancrypt.useragent.plist
```

The modified configuration file is then reloaded without the user having to log off from the mac computer and log on again, or the mac computer having to be restarted.

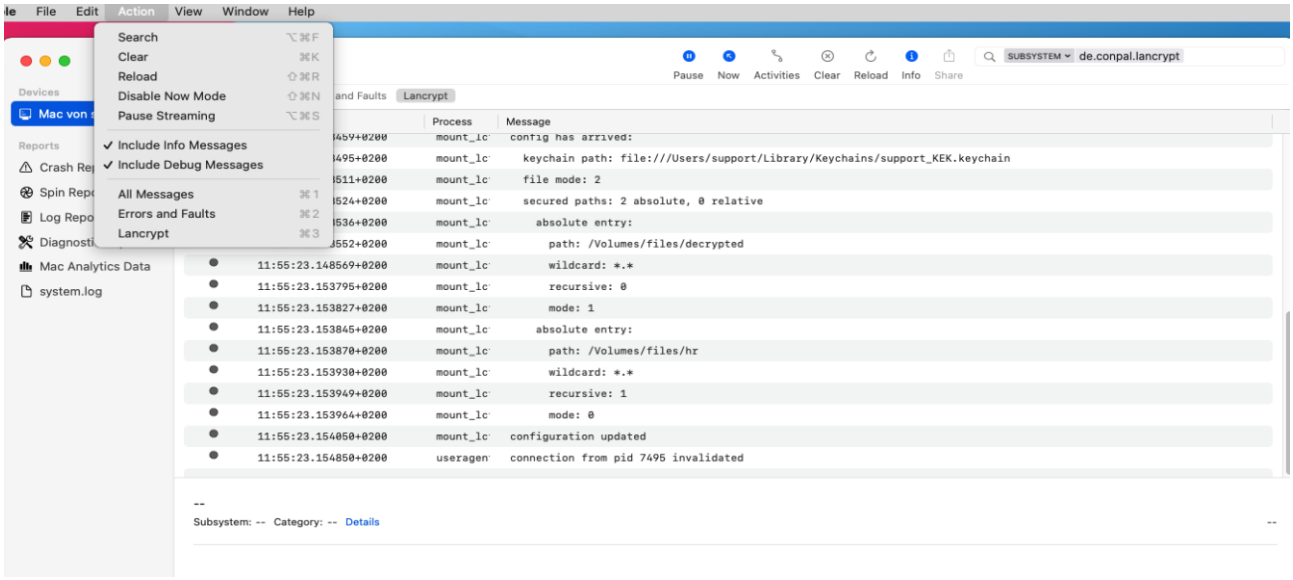
3.2 Certificates

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 and also provide them with the password or PIN to access their certificates. For this purpose, the administrator must create the configuration file "*config.plist*" on the mac client. There you have to enter the path where the *conpal LAN Crypt* Administration stores the user certificates as well as the public certificate *(*.cer*) of the Security Officer (see conpal LAN Crypt Administration manual, "***Central Settings***", "***The Directory tab***"). 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.

conpal 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 *conpal 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: If the login to *conpal LAN Crypt* fails, they will be displayed in the mac console under the filter "`subsystem de.conpal.de.lancrypt`" in the respective log entries. Also enable the "Include Info Messages" and "Include Debug Messages" options in the console. Alternatively, you can also view this information live in a terminal. This requires the following entry in the terminal:

```
sudo log stream --level debug --predicate 'subsystem == "de.conpal.lancrypt"'
```



The certificate is checked every time the encryption profile is loaded. If a valid certificate is found, the user is logged on to *conpal 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 *conpal LAN Crypt* and their logon fails, they receive an error message to tell them why they were unable to log on.

Encryption rules with their assigned keys from the *conpal 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. The rules can be changed at any time and at will by the *conpal LAN Crypt* (Master) Security Officer (MSO/SO). For example, files can also be re-encrypted with a different key.

3.3 Loading the policy file

3.3.1 *conpal LAN Crypt* default behavior

When a user logs in to his mac computer, their cached user profile is loaded first. *conpal LAN Crypt* checks if a new policy file is available for the user by establishing a connecting to the specified location of the policy file (SMB share). If a new policy file is found, it is used to update the cached one.

The user can start working with encrypted files while *conpal LAN Crypt* continually checks for new versions of the policy. If the specified location is not accessible, the cached profile is used till an updated version becomes available.

Note: *conpal 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, *conpal LAN Crypt for macOS* initially does not initially 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.

3.3.2 Load updated policy file manually

The Security Officer provides the user with his policy file. If this policy file is updated by the Security Officer, this updated version is only loaded when the user logs off from his mac computer and then logs on again or restarts his computer. In some cases, however, it may be useful for the user to be able to update their updated policy file without having to log off.

To do this, the user must open the terminal on his mac computer and then run the following command:

```
/Library/conpal/LAN\ Crypt/useragent.app/Contents/Resources/lcutil reload-policies
```

After running this command, the user's policy file will be reloaded.

3.4 Logon to conpal LAN Crypt

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

3.4.1 Logon with token

Users can also log on to *conpal LAN Crypt for macOS* using a token. A prerequisite for this logon method is that the user’s *conpal 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.

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.

4 Installation

Note: You need administrator rights to install *conpal LAN Crypt for macOS*.

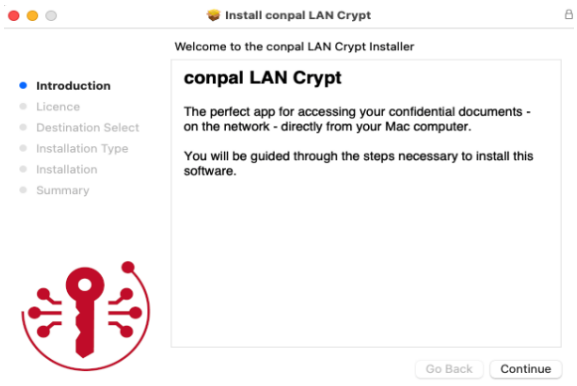
conpal LAN Crypt for macOS supports the following versions of macOS:

- v11 Big Sur
- v10.15 Catalina
- v10.14 Mojave

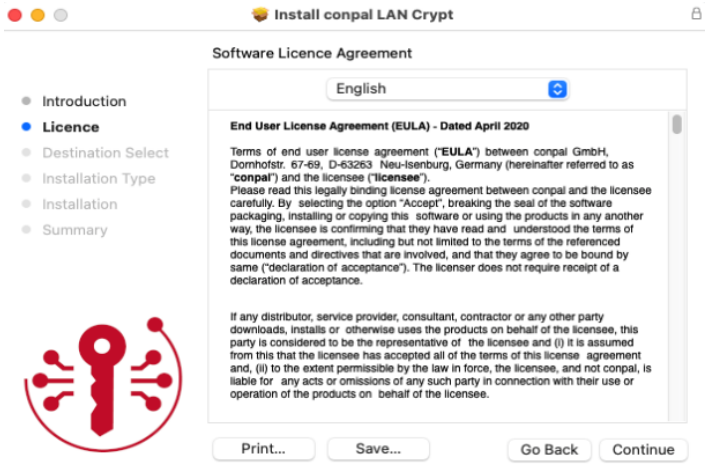
Double click on the file **conpal LAN Crypt.dmg**.

The following dialog is displayed:

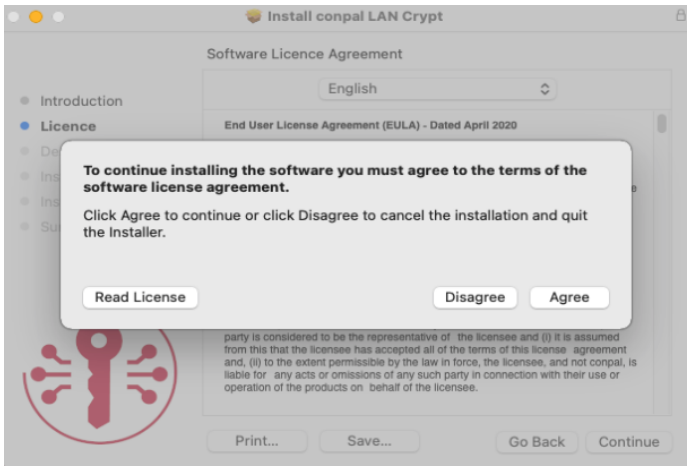
Double click on **conpal LAN Crypt.pkg**.



The **End User License Agreement (EULA)** dialog is displayed.



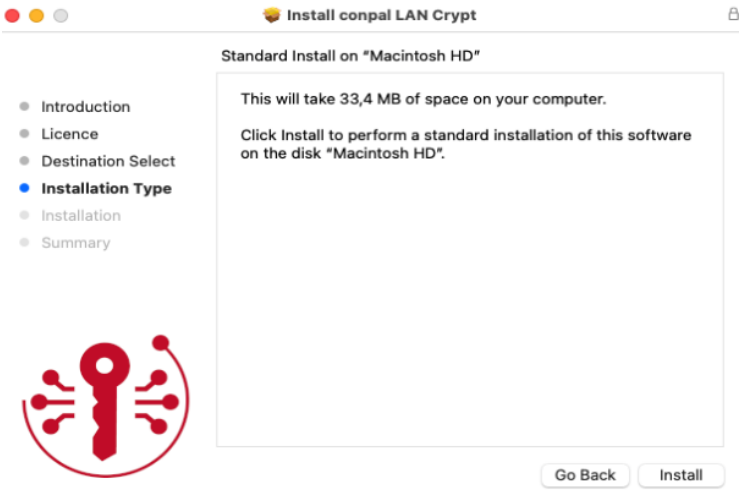
Click on **Continue**.



Then click **Agree**.

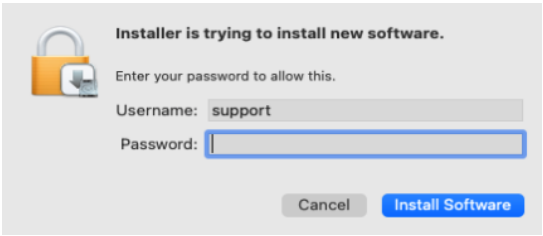
Note: If you do not accept the software license agreement and press **Disagree**, *conpal LAN Crypt for macOS* cannot be installed.

If you have accepted the software license agreement, the following dialog is displayed:



Click on **Install**.

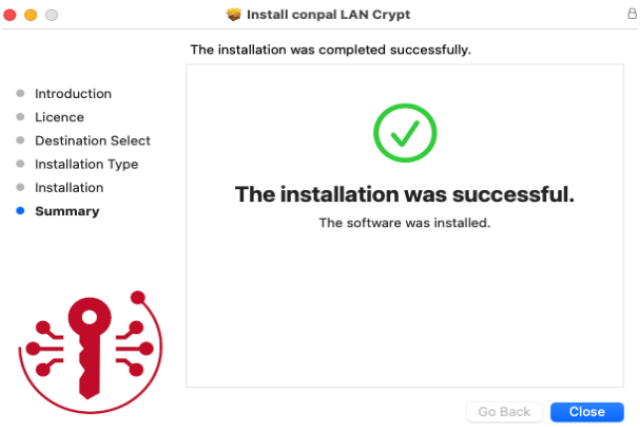
You receive a warning message that an installer is trying to install new software:



Log in as an administrator with your associated username and password and click **Install Software**.

conpal LAN Crypt for macOS will then be installed on your mac computer.

If the installation is successful, a dialog appears in which you can click on **Close** to complete the installation process.



4.1 Removing conpal LAN Crypt for macOS

You can only remove *conpal LAN Crypt for macOS*, if you are logged on with administrator rights.

Click **Uninstaller.pkg** in the path given below.

```
/Library/conpal/LAN Crypt/Uninstaller.pkg
```

conpal LAN Crypt for macOS will be uninstalled.

Note: After uninstalling *conpal LAN Crypt for macOS*, encrypted files can no longer be decrypted from the mac computer. Uninstalling *conpal LAN Crypt for macOS* does not decrypt files.

5 Functions of the console application “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/conpal/LAN Crypt/useragent.app/Contents/Resources
```

This provides users advanced functions of *conpal LAN Crypt for macOS*, which are described below:

5.1 Print version information of conpal LAN Crypt for macOS

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

```
/Library/conpal/LAN\ Crypt/useragent.app/Contents/Resources/lcutil version
```

5.2 Collect logs

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

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

```
/Library/conpal/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 and
- config.plist

6 Technical support

You can find technical support for conpal products in any of these ways:

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

Download the client product documentation for windows at

- https://docs.lancrypt.com/de/client/lc_400_hdeu.pdf in German language, at
- https://docs.lancrypt.com/en/client/lc_400_heng.pdf in English language and at
- https://docs.lancrypt.com/fr/client/lc_400_hfra.pdf in French language.

Download the client product documentation for macOS at

- https://docs.lancrypt.com/de/client/lc_macOS_100_hdeu.pdf in German language and at
- https://docs.lancrypt.com/en/client/lc_macOS_100_heng.pdf in English language.

Download the admin product documentation at

- https://docs.lancrypt.com/de/admin/lc_401_ahdeu.pdf in German language, at
- https://docs.lancrypt.com/en/admin/lc_401_aheng.pdf in English language and at
- https://docs.lancrypt.com/fr/admin/lc_401_ahfra.pdf in French language.

As a registered maintenance customer send an email to

support@conpal.de

including your conpal software version number(s), operating system(s) and patch level(s), and the text of any error messages.

7 Legal notices

You find copyright information on third party suppliers in the 3rd Party Software document in your product directory.