u.trust LAN Crypt 2Go

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

What is u.trust LAN Crypt 2Go?

u.trust LAN Crypt 2Go enables secure exchange of confidential data via password-based encryption. Files can be encrypted easily and securely with AES-256 XTS. Either on-demand, using the *u.trust LAN Crypt 2Go* app or transparent via the Outlook for Windows Add-In for attachments shared via email. A web hosted version is also available, which enables encryption and decryption on systems where the product is not installed at all or cannot be installed. The user can individually select the password to be used for the encryption. Passwords have to satisfy a predefined set of requirements and complexity in order to ensure a minimum level of security. Requirements enforced are minimum length of the password, case sensitivity and a mix of alphanumerical and special characters.

Persons who do not know the secret password used for encryption will not have access to the information contained in the file and, when opening a file protected with *u.trust LAN Crypt 2Go*, will see only its encrypted contents.

u.trust LAN Crypt 2Go is a complement to u.trust LAN Crypt clients for Windows and macOS to enable a secure exchange of confidential data also with other persons or external partners who do not use u.trust LAN Crypt yet. Besides Windows and macOS it is also available on Linux (Ubuntu, Debian). On mobile devices like Android and iOS/iPadOS the functionality is part of the respective u.trust LAN Crypt for Mobile App.

u.trust LAN Crypt 2Go is available in English and German language.

Example usage

Imagine that you want to provide an Excel file with confidential financial data to an external marketing agency, which is to create a trendy financial report with attractive graphics. However, the marketing agency does not yet use *LAN Crypt*.

This is how you can securely share the file with your marketing agency:

Encrypt the file (e.g. "Financial report.xlsx") with *u.trust LAN Crypt 2Go*. For this, you can create a new key or use an existing key.

1. Send the encrypted file ("finance report.xlsx.pcrypt") to your marketing agency, e.g. via an insecure email.
2. Tell your contact person at the marketing agency the password that can be used to decrypt the file, e.g. during a telephone conversation.
3. The marketing agency can go to the *u.trust LAN Crypt 2Go* web page to decrypt the encrypted file, without having to install any software. Alternatively, the marketing agency can use *u.trust LAN Crypt 2Go Reader* to decrypt the file locally (Windows only).

   Note

   - *u.trust LAN Crypt 2Go* is compatible with *LAN Crypt*. Therefore, you can encrypt and decrypt files even in folders that have an encryption policy applied by u.trust LAN Crypt. Files remain encrypted at all times!

Installation and upgrade

u.trust LAN Crypt 2Go is available on the following platforms:

- Windows 10 or later (x64)
- macOS 12 or later (Intel, Apple Silicon)
- Debian 11 or later
- Ubuntu 20.04 or later

Individual installation packages are available for the following platforms:

- **lc2go.msi** - Windows (x64)
- **lc2go.dmg** - macOS (Intel, Apple Silicon)
- **lc2go.deb** - Debian, Ubuntu (AMD64)

Note

- A web-based version of *u.trust LAN Crypt 2Go* is hosted on the Utimaco homepage. This version does not require any software to be installed and can be used by anyone who wants to encrypt or decrypt files.

The Windows version of the product has some specifics that differ from other platforms. Firstly, it supports two different installation modes: current user and all users. Secondly, it contains an Add-In for Microsoft Outlook (32-bit and 64-bit), which is only available on the Windows platform.

Installation option: All Users

Per default, installation of *u.trust LAN Crypt 2Go* does not require administrative privileges and can be installed by any user. If installed by a user, the application is installed and will be available exclusively for that user only. Other user accounts on the same system will not have access to the installed product.

Administrative installation of *u.trust LAN Crypt 2Go* will make the product available for all users. For this, you must run the setup in advanced mode and overwrite the parameter MSIINSTALLPERUSER.

For example, run the following command from an elevated Windows Terminal:

```
msiexec /i lc2go.msi MSIINSTALLPERUSER=""
```

This will install the product for all users on the system.

Installation option: Microsoft Outlook Add-In

u.trust LAN Crypt 2Go provides modular installation options allowing customers to tailor installations to their specific needs. The **ADDLOCAL** parameter can be used to select the features to be installed.

Run the following command from an elevated Windows Terminal:

```
msiexec /i lc2go.msi ADDLOCAL=ALL REMOVE=outlook_addin_feature
```

This will install the product itself but will omit installation of the Add-In for Microsoft Outlook.

Uninstall u.trust LAN Crypt 2Go

u.trust LAN Crypt 2Go can be removed from a system at any time. Uninstallation follows standard software removal procedures for each platform.

Note

- After uninstalling *u.trust LAN Crypt 2Go*, password-based encrypted files can no longer be decrypted on the computer. Uninstalling *u.trust LAN Crypt 2Go* does not uninstall *LAN Crypt*.

u.trust LAN Crypt Cloud Support

Using the u.trust LAN Crypt Cloud allows users to securely store their keys in the cloud. This happens automatically and provides access to the keyring from all of the user's devices, across all platforms supported by *u.trust LAN Crypt 2Go*.

Changes to the keyring, whether it's adding, deleting, or renaming a key, are automatically synchronized with the other devices. This ensures that the user always has access to the most up-to-date keys, regardless of which device they are working on.

Signing In and Out

To sign in, tap the **Account icon** in the top right corner of the *u.trust LAN Crypt 2Go* application and select **Sign In**:

If you have password-based keys in your keyring, the user will be asked for permission to upload the keys to the u.trust LAN Crypt Cloud . Permission to upload existing keys is mandatory. If a user does not want existing keys to be uploaded, the keys must be deleted before signing in to the u.trust LAN Crypt Cloud . Note that passwords for password-based keys are not uploaded to the u.trust LAN Crypt Cloud , so the **Show Password** option for keys stored in the u.trust LAN Crypt Cloud is not available.

After clicking on **Sign In**, the user's default browser opens, asking for the login data for the u.trust LAN Crypt Cloud . After entering the login data, a success message is displayed in the browser. This confirms that the login process has been successfully completed and the user now has access to his keys stored in the u.trust LAN Crypt Cloud .

To sign out, follow the same procedure, but select **Sign Out** instead of **Sign In**. After signing out, you will no longer have access to the keys stored in the u.trust LAN Crypt Cloud until you sign in again. This serves as an additional level of security to prevent unauthorized access to your keys.

Inclusion of Managed Keys

The settings menu, which becomes visible after tapping the **Gear icon** in the bottom left corner of the application, now shows a new option called **Managed Keys**. After selecting the **Managed Keys** menu item, the list of the user's asset keys is displayed. These are keys used by LAN Crypt for Windows / macOS to transparently encrypt or decrypt files based on rules about their location in the file system.

u.trust LAN Crypt 2Go now also supports the use of these managed keys for encryption and decryption operations. All keys from the Cloud account's keyring, including managed keys, can be used for encryption and decryption processes.

When you list the keys in the keyring, an additional column for the key type is displayed. This indicates whether a key is a password-based key or a managed key. This makes it easier to identify and manage your keys by providing a clear distinction between the different key types.

Note

- Managed keys are not suitable for protecting attachments through the Outlook Add-In. Their primary function is the encryption and decryption of files at the system level and they are not intended for use in individual applications like Outlook.

Password-based encryption and decryption of files

u.trust LAN Crypt 2Go enables the secure exchange of confidential data through password-protected encryption. With *u.trust LAN Crypt 2Go* (AES 256-bit) you can easily and securely encrypt and decrypt files. LAN Crypt 2GO uses password-generated keys for encryption and decryption, which are stored in a keychain within the application. Users can add new keys, delete old ones or view the passwords used for existing keys at any time.

Note

- Encryption always requires a secure password! It must be at least 8 characters long and contain upper and lower case letters, numbers and special characters.
- The name of the encryption password has no influence on the key used for encryption. The actual key value for encryption is generated separately.

Using the graphical user interface

When opening the app by selecting the *u.trust LAN Crypt 2Go* program icon, the encryption dialog appears. Use the **Select...** button to select the file to be encrypted or decrypted.

To encrypt the file, now select the desired key and finally click **Encrypt**. New keys can be added by the **New Key** button and managed by the **gear icon**.

u.trust LAN Crypt 2Go creates an encrypted copy of the file. Encrypted files get the additional file extension .pcrypt and are clearly recognizable by the graphical document icon.

Note

- The original file is never deleted or overwritten by *u.trust LAN Crypt 2Go*.

When decrypting a file that has been password-encrypted by one of the LAN Crypt products, the system first checks whether the required key is already stored. If this is the case, it is automatically used for decryption. If the required key is not yet available, the key password must be entered to successfully decrypt the file. A key is derived from the entered password and saved, so it can be used for further encryption and decryption.

Note

- When decrypting a file, *u.trust LAN Crypt 2Go* creates an unencrypted copy of the file. It also restores the original file extension of the file by removing the .pcrypt extension.

To view and manage the created keys, click on the **gear icon** and select **Password-based Keys**. Now you will see a listing of the saved keys including information such as their GUIDs. With a **right click** on a key you can now rename it, delete it or view the original password (Windows only).

Using the context menu

If an unencrypted file is opened with **Open with** -> **u.trust LAN Crypt 2Go**, the option to encrypt the document is offered.

An encrypted file is temporarily decrypted in this way and automatically re-encrypted after viewing or editing file.

Using ‘drag and drop’

To encrypt or decrypt a file with *u.trust LAN Crypt 2Go*, you can simply drag the file in question onto the program icon.

View and edit encrypted files

Files can also be edited directly without manual decryption. In this case, the encrypted file is automatically decrypted when opened and then re-encrypted with the corresponding password after editing. The prerequisite for this is that the required key has already been saved or is entered correctly on request.

The respective standard program is used to edit the file (e.g. original .docx files are opened with Microsoft Office by default).

Note

- If an encrypted file is read-only, the temporarily decrypted file is also read-only. This usually results in the respective default program preventing changes to the file.
- To create a decrypted version of a .pcrypt file, you can either use **Save as** within the respective editing program or open *u.trust LAN Crypt 2Go*, select an encrypted file and tap the **Decrypt** button.

Using the Microsoft Outlook Add-in (Windows only)

u.trust LAN Crypt 2Go extends Microsoft Outlook installed on the Windows client with the option to encrypt attachments on the fly. It supports two ways to get an attachment encrypted:

- **On-demand**
- **On-send**

The add-in has built-in logic to help the user to determine when encryption is deemed necessary. Attachments that are included in emails sent to internal recipients only will not be encrypted by default. However, the user can opt to use the **On-demand encryption** option if attachments should be encrypted.

If an email including an attachment is sent to an external recipient, the add-in will prompt the user to have the attachment encrypted before the email is sent. This behavior is intended to prevent sensitive data from being sent to an external partner without adequate protection.

If you create password-based keys in the Outlook Add-In and are signed in to your u.trust LAN Crypt Cloud account, these are automatically transferred to the u.trust LAN Crypt Cloud. This ensures that your newly created keys are immediately available on all your devices. All password-based keys stored in your u.trust LAN Crypt Cloud keyring can be used to protect attachments.

Note

- If there is only a single mail recipient, the same key as last time will be preselected for this recipient.
- If a new key has just been created, this new key will be preselected for encryption.

Encryption ‘On-Demand’

Attachments can be encrypted anytime via the *u.trust LAN Crypt 2Go* add-in in the ribbon bar of the ‘New Email Message’ window. During encryption, the original copy of an attachment is removed from the email and replaced with the encrypted copy.

Encryption ‘On-Send’

The *u.trust LAN Crypt 2Go* add-in is triggered when an email with an attachment is to be sent to an external recipient. A recipient is considered external, when his email domain differs from the sender’s domain (i.e. the part of the email address after the @ is different). Although encryption is suggested, it is not enforced and the user can omit it at his own discretion.

Using Registry Keys (Windows Only)

The Windows version of LAN Crypt 2Go can be configured using the following registry keys:

`HKCU\Software\Policies\conpal\LAN Crypt\2Go`

This key can be edited by users with restricted privileges:

Name	Type	Default Value	Value
`VerboseLogging`	DWORD	0	This value can be used to enable verbose logging, which can be helpful for troubleshooting: 0 = No verbose logging (only info, warning, and error messages are logged) 1 (and all other values) = Verbose logging (includes debug and verbose entries in the log file)

`HKCU\Software\Policies\conpal\LAN Crypt\2Go`

`HKLM\Software\Policies\conpal\LAN Crypt\2Go`

These registry keys cannot be modified by restricted users.

For *u.trust LAN Crypt 2Go* versions 1.0 to 4.0, only the HKEY*CURRENT*USER (**HKCU**) registry hive is supported.

For *u.trust LAN Crypt 2Go* versions 10.0 and newer, if one of the registry keys below is NOT set in the HKEY*CURRENT*USER hive (**HKCU**), the HKEY*LOCAL*MACHINE (**HKLM**) hive is checked as well. This allows administrators to distribute settings for all users (via HKLM) and still supports exceptions for specific users (**HKCU**).

Name	Type	Default Value	Value
`CheckOnSend`	DWORD	1	TThis value can be used to disable the encryption on-send feature: 0 = Send without checking 1 (and all other values) = Check attachments when sending and offer encryption if needed
`InternalMailDomains`	String	(Empty)	A semicolon-separated string of mail domains to be considered as **internal** (= no encryption required). **Example:** `{{ site.company_name_small }}.de; {{ site.company_name_small }}.at`, where all emails to nnn@{{ site.company*name*small }}.de and nnn@{{ site.company*name*small }}.at will not be checked for unprotected attachments. If `InternalMailDomains` is not set, the recipient's email domains are compared with the sender's email domain. Only the sender's email domain is considered **internal**.
`ExcludedAttachments`	String	(Empty)	

Name	Type	Default Value	Value
			A semicolon-separated string of file extensions for files that should not be encrypted. **Example:** `.txt;.png;.pdf`

Note

- For additional information on using registry keys in Windows environments, you can find more details and guidance here{:target="_blank"}.

Using the u.trust LAN Crypt 2Go commmand line tool

With the command line tool of u.trust LAN Crypt 2Go you can encrypt and decrypt files via the command line or the terminal. To do this, open the respective path via the console:

Windows:

```
C:\Users\<Username>\AppData\Local\Programs\conpal\LAN Crypt\2Go\lancrypt.exe
```

macOS:

```
/Applications/LAN Crypt 2Go.app/Contents/Resources/lancrypt.app/Contents/MacOS/lancrypt
```

Linux:

Since the installer automatically adds the command line tool to the search path, there is no need to open a specific path via the console.

Now you can use the application inside the console with the command `lancrypt` and a following statement.

Key management

u.trust LAN Crypt 2Go allows keys to be managed via the console. Keys can be added, deleted, renamed and listed there.

Add key:

```
lancrypt /A key name password
```

or

```
lancrypt /A /F file password
```

Adds a key for further encryption and decryption. With the additional option `/F file` the name of the key, its GUID and further key information are taken from a given file.

Delete key:

```
lancrypt /P /N name
```

or

```
lancrypt /P /G guid
```

Deletes the specified key. With the additional option `/N name` the key to be deleted is identified by its name. With the additional option `/G guid` the key to be deleted is identified by its GUID.

Rename key:

```
lancrypt /R /N name new-name
```

or

```
lancrypt /R /G guid new-name
```

Renames the key. With the additional option `/N name` the selected key is identified by its name and renamed. With the additional option `/G guid`, the selected key is identified and renamed by its GUID.

List key

```
LANCRYPT /L
```

Lists all stored keys.

Note

- While you are signed in to the u.trust LAN Crypt Cloud , command line options for adding, deleting, or renaming keys are not available. However, these functions can be performed through the use of the application.

Encrypt

```
lancrypt /E file /N key name
```

or

```
lancrypt /E file /G keyguid
```

or

```
lancrypt /E file password
```

Encrypts the selected file either with an existing key (identified by either `/N name` or `/G guid`) or with a newly chosen password.

Note

- Encryption always requires a secure password! This must consist of at least 8 characters and contain upper and lower case letters, digits and special characters.
- The name of the encryption password has no influence on the key used for encryption. The actual key value for encryption is generated separately.

Decrypt

```
lancrypt /D file
```

or

```
lancrypt /D file password
```

Decrypts the selected file either automatically with the matching already stored key or with the given password.

Note

- When decrypting with a password, this is not automatically stored in the saved keys.

Decrypt with exported keys

The command line tool now includes an optional parameter `/K` for the decrypt option (`/D`). This parameter specifies the path to a decrypted key export file (in JSON format).

Decrypting a single file

To decrypt a single file, use the `/D` option with the file name and the `/K` option with the path to the key export file:

```
lancrypt /D exportedKeysTest.txt.pcrypt /K exportedKeys.json
```

Decrypting all files in a folder

To decrypt all files in a folder, use the `/D` option with the folder path and the `/K` option with the path to the key export file:

```
lancrypt /D directory /K exportedKeys.json
```

Note

- Decrypting a folder includes all files in its subdirectories.

Technical support

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

At support.Utimaco.de registered customers with active maintenance contracts get access to downloads, documentation and knowledge items.

As a registered maintenance customer, send an email to:

support@Utimaco.de

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

Legal notice

Last updated 31.05.2024