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.

Managed keys

Tapping the **gear icon** in the lower left corner of the application opens the settings menu. Under **Managed keys**, you can view the managed keys of your cloud account. These keys are used by *u.trust LAN Crypt* for Windows, macOS, and Linux to encrypt and decrypt files transparently, based on rules.

Managed keys are also available in the keyring of *u.trust LAN Crypt 2Go*. The **key type** column indicates whether a key is a password-based key or a managed key.

If a file has already been encrypted by a LAN Crypt client using a managed key, you can open it in *u.trust LAN Crypt 2Go*, edit it, and save it in encrypted form again. This requires the corresponding managed key to be present in your keyring.

Managed keys cannot be used to create password-protected files. For this function, *u.trust LAN Crypt 2Go* offers password-based keys only. The difference: password-based keys are derived from a password, managed keys are not.

Note on the Outlook Add-In

- The Outlook Add-In also protects attachments by creating encrypted files with password-based keys. Recipients can open these files with the corresponding password, without having your organization's managed key. This is why the Outlook Add-In uses password-based keys exclusively.
- "Managed" refers to the key type here, not to the storage location. Password-based keys remain password-based even when they are managed in the cloud.

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 inside the application settings.

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, go to the **Application settings** 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

u.trust LAN Crypt 2Go extends Microsoft Outlook with the ability to encrypt attachments before sending.

The Add-In is available in two versions:

Classic Add-In: Installed with the LAN Crypt 2Go Windows client. The LAN Crypt Cloud connection is optional and only used to retrieve and store encryption keys. Central **administration via LAN Crypt Cloud is not required**.

Modern Add-In: Provided through **Microsoft AppSource** and compatible with the latest versions of Outlook on Windows, macOS, and the web application. Central **administration via LAN Crypt Cloud is mandatory**. In addition to retrieving and storing keys, the **Modern Add-In** also enables further administrative functions. For more information on add-in requirements in Exchange and Outlook versions, see Requirements for running Office Add-ins.

> **Note**
>
> - For testing purposes, Outlook web add-ins can also be installed via sideloading. The **manifest XML file** for sideloading can be downloaded from the following link .

Both versions support two encryption modes:

Encrypt On-Demand:

This feature allows attachments to be **encrypted before they are uploaded to the Exchange server**.

To use this feature, the user selects the LAN Crypt 2Go Add-In while composing the email. A window then opens in which an encryption key for the attachments can be selected. The chosen files are then automatically **attached in encrypted form**.

> **Note**
>
> - Due to a technical limitation on Microsoft's side, the **Encrypt on Send** feature of the Modern Add-In is only available if the add-in is **deployed by the organization's administrator** or **manually installed via sideloading**. If the add-in is installed directly from the **Microsoft Marketplace**, the **Encrypt on Send** feature is disabled in Outlook. To enable users to access event-based activation, the Modern Add-In must be centrally deployed by the organization or sideloaded for testing.

Encrypt On-Send:

When sending an email using the **Modern Add-In**, LAN Crypt 2Go automatically checks whether and how unencrypted attachments should be handled. Encryption occurs only under specific conditions:

1. Content is **not encrypted** if …
    - there are no attachments or all attachments are already encrypted,
    - the email is sent only to internal recipients (no external addresses),
    - the user has selected **Unencrypted (Plain)** in the LAN Crypt 2Go sidebar.
2. Content is **automatically encrypted** if …
    - the user selects **Encrypted** in the LAN Crypt 2Go sidebar. In this case, all unencrypted attachments are automatically encrypted with the selected key.
3. The user is **prompted to decide** if …
    - neither option (**Unencrypted (Plain)** nor **Encrypted**) has been selected. When sending the email, a prompt appears asking the user to choose how to handle the attachments.

If no decision is made or the handling of attachments is unclear, the user is notified, and the sidebar with the available options opens automatically.

Unlike the Modern Add-In, when sending an email with the **Classic Add-In**, a dialog box appears every time to select encryption options for attachments.

Note

- Inline images embedded directly in the message body are not encrypted. To ensure the confidentiality of such content, they must be inserted as regular file attachments.
- When using the **Modern Add-In**, the administrator can disable the **Encrypt On-Send** mode within the LAN Crypt Cloud administration. They can also define internal email domains and exclude specific file types from automatic encryption.

Using Registry Keys (Windows Only)

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

HKCU\Software\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

Name	Type	Default Value	Value
			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)	A semicolon-separated string of file extensions for files that should not be encrypted. **Example:** `.txt;.png;.pdf`
`AllowSendUnencrypted`	DWORD	1	This value can be used to force encrypted attachments to external mail domains, thereby ensuring the security of your correspondence. Please note that attachments sent to internal mail domains are still sent in plain text. 1 (or not set) = allow the user to send plain text attachments to external recipients. 0 (and all other values except 1) = force encryption when sending emails to external recipients.

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.

Standalone version

LAN Crypt 2Go now supports the creation of **standalone versions** of the application. A standalone version can be placed on removable media (e.g., USB flash drives) or in cloud-synced folders.

These versions run **without requiring installation** on the host machine and can now be executed on **any machine running the same operating system the standalone version was created on**. All software components and configuration data remain stored alongside the standalone copy.

Note

- No application data is written to the system outside of a generated `readme` file, and a `LAN Crypt 2Go Data` folder stored next to the standalone executable.
- On **Windows**, no information is written to the **Windows Registry**.

Creating a standalone version

To create a standalone version of LAN Crypt 2Go:

1. Open the **Application settings** menu.
2. Select **Create standalone version**.
3. Choose the target folder where the application should be generated.

After the process is complete, the selected folder contains the full **LAN Crypt 2Go standalone application**.

Using a standalone version

Standalone versions of LAN Crypt 2Go store their configuration and keys in an encrypted form protected by a **master password**.

On first launch of the standalone application, the user is asked to define a master password. On subsequent startups, all stored key material and configuration data will remain encrypted until the defined master password is correctly entered.

Changing or resetting the master password

To change the master password, open the **Application settings** while running the standalone version of LAN Crypt 2Go. Under the option **Change application password**, the master password can be changed or reset.

Resetting the master password deletes all stored keys and passwords and will prompt the user at the next application startup to define a new master password.

Restrictions

Since the standalone version does not rely on a system-wide installation, certain features are **not supported**:

- **Outlook add-in** is not available.
- **LAN Crypt Cloud support** is not available.
- On Windows, `.pcrypt` files are **not automatically associated** with the standalone executable.

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

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

At support.Utimaco.com 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

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