What is u.trust LAN Crypt 2Go Reader?

u.trust LAN Crypt 2Go Reader enables the secure exchange of confidential data by decrypting password-protected data.

u.trust LAN Crypt 2Go Reader is a complement to the *u.trust LAN Crypt* Clients. The application allows easy decryption of all files password-encrypted by LAN Crypt applications, so that files can be easily decrypted even by people and organizations that do not yet use one of the LAN Crypt products.

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

Note

- *u.trust LAN Crypt 2Go Reader* is closely related to the LAN Crypt 2Go client, but only supports file decryption!
- Both products (*u.trust LAN Crypt 2Go* and *u.trust LAN Crypt 2Go Reader*) can be installed and uninstalled independently.

Example usage

Imagine you want to provide an external marketing agency with several Excel files containing confidential financial data encrypted with one of the LAN Crypt products. You also receive a password to decrypt the files.

Now you can use *u.trust LAN Crypt 2Go Reader* to decrypt the given files with the received password.

Installation and upgrade

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

- **Windows 10** or later (x64)

Individual installation packages are available for the following platforms:

- **lc2go.msi** - Windows (Intel-x64)

Installation

u.trust LAN Crypt 2Go Reader supports two different installation modes: Current User and All Users.

Installation option: All users.

By default, the installation of *u.trust LAN Crypt 2Go Reader* does not require administrator privileges and can be performed by any user. If the installation is performed by one user, the application will be installed so that it is only available to that user. Other user accounts on the same system will not have access to the installed product.

The administrative installation of *u.trust LAN Crypt 2Go Reader* makes the product available to all users. To do this, you must run Setup in Advanced mode and override the MSIINSTALLPERUSER parameter.

Run the following command from a Windows terminal with elevated privileges:

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

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

Uninstall u.trust LAN Crypt 2Go Reader

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

Note

- After uninstalling *u.trust LAN Crypt 2Go Reader*, encrypted files on the computer can no longer be decrypted. Uninstalling *u.trust LAN Crypt 2Go Reader* does not uninstall any other product from *u.trust 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 Reader*.

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 Reader* 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.

Decrypting password protected files

Using the graphical user interface

When opening the app by selecting the *u.trust LAN Crypt 2Go Reader* program icon, the decryption dialog will appear. Use the **Select...** button to select the file to decrypt or drag in the desired file.

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 Reader* creates an unencrypted copy of the file. It also restores the original file extension of the file by removing the .pcrypt extension.

Using the context menu

u.trust LAN Crypt 2Go Reader adds its own commands to the context menu of files. These are displayed when you right-click on a file. Files can be decrypted directly from the context menu.

Using drag-and-drop

Simply drag the file you want to encrypt or decrypt onto the program icon of *u.trust LAN Crypt 2Go Reader*.

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.

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

Technical support for Utimaco products can be accessed as follows:

At support.Utimaco.com maintenance contract customers get access to further information, such as knowledge items.

As a maintenance contract customer send an email to technical support:

support@Utimaco.de

and include the version number(s), operating system(s) and patch level of your Utimaco software as well as the exact wording of error messages, if applicable.

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