What is u.trust LAN Crypt for iOS / iPadOS?

u.trust LAN Crypt for iOS / iPadOS enables users to work with their encrypted data remotely, by using their mobile devices, such as smartphones or tablets.

With transparent file encryption on Windows / macOS, Utimaco LAN Crypt enables the secure exchange of confidential data within authorization groups in small, medium and large organizations. Numerous companies, business organizations and the public administration in Germany and worldwide are already relying on Utimaco LAN Crypt.

A Security Officer (SO) determines centrally, which files and storage locations should be protected by Utimaco LAN Crypt and defines which users are allowed to have access to specific data by setting one, or several encryption rules. As an example, the Security Officer (SO) can ensure that all Word documents in a specific file storage path are encrypted, by creating an encryption rule on the defined path, e.g., `\\Servername\Files\*.docx`. As soon as this rule is transferred to the client computer via a policy file, created with the Utimaco LAN Crypt Administration console, all Word documents in this path will be encrypted from now on. Additionally, you can combine one or more encryption rules to one encryption profile.

This applies to all files, independently of where the files are stored. You can access all Utimaco LAN Crypt encrypted files that are either stored locally, on a network storage or on a remote storage (e.g., cloud storage). A user can easily access the same Utimaco LAN Crypt encrypted files, that are also available on his workstation computer.

u.trust LAN Crypt for iOS / iPadOS enables users to use their mobile devices, such as iPhone or iPad, to work with their encrypted data.

This release of *u.trust LAN Crypt for iOS / iPadOS* allows the user to open, edit and save encrypted files and access them per se and moreover extends the usual Utimaco LAN Crypt security infrastructure by using certificates (.p12 files) and policy files (.xml.bz2) on mobile devices.

u.trust LAN Crypt 2Go

With the new built-in u.trust LAN Crypt 2Go you can also encrypt and decrypt files based on passwords. This allows you to easily and securely exchange information with other people, such as your business partners or even external employees.

SafeGuard Enterprise: File encryption migration

SafeGuard Enterprise is a security suite from Sophos, consisting of several modules. Data Exchange (DX), Cloud Storage (CS), and File Encryption (FE) all provide file-level encryption. However, the entire software suite is being discontinued, putting users at risk of losing access to their encrypted documents. Migrating from one security product to another can be a hassle and an added risk, especially if the process involves decrypting the data. However, this is not the case when migrating to u.trust LAN Crypt.

u.trust LAN Crypt and Sophos SafeGuard Enterprise are fully compatible. They share the same technical foundation and file-encryption subsystem. Consequently, files encrypted in SafeGuard Enterprise are fully compatible with and can be read natively by u.trust LAN Crypt. The encryption keys are specific to each installation, and only those need to be migrated.

Step 1: Export Keys from SafeGuard Enterprise

The keys used to encrypt files are unique for each SafeGuard Enterprise installation. Sophos provides a simple tool that allows for easy export of all encryption keys used in SafeGuard Enterprise for encrypting files. All keys are conveniently copied into a single package.

Step 2: Import Keys to u.trust LAN Crypt

The keys, now available in a separate package, can easily be imported into any existing u.trust LAN Crypt system. Once imported, the u.trust LAN Crypt installation has all it needs to access files that have been encrypted with SafeGuard Enterprise.

Step 3: Update Policy / Assign Keys

Assign the newly imported keys to all users who need access to files encrypted by SafeGuard Enterprise. These keys enable users to read files that have been encrypted by any SafeGuard file

encryption module in the past. This also applies to files that have been encrypted by SafeGuard Enterprise after the key import.

Step 4: Access Safeguard Enterprise Files

The conpal LAN Crypt client shares its technical foundation with SafeGuard Enterprise. Once the keys have been deployed to the client, it can read all files that have been encrypted with any of the SafeGuard Enterprise file encryption modules – DX, CS, FS. There's no need to decrypt a single file. No matter how long ago a file was encrypted, u.trust LAN Crypt can read it.

Full file-level compatibility allows for smooth migration. Even if parts of the company still use SafeGuard Enterprise, all encrypted files they create can be read by anyone who has already migrated to u.trust LAN Crypt.

Note

- If you have installed *SafeGuard Enterprise* and plan to migrate to *u.trust LAN Crypt*, please contact the u.trust LAN Crypt support. Further information is available at www.conpal.de/en/sgn-migration-en.

Which iOS / iPadOS-Versions are supported?

u.trust LAN Crypt for iOS / iPadOS supports iOS 16/ iPadOS 16 and newer versions.

u.trust LAN Crypt for iOS / iPadOS is available in German and English.

Supported encryption algorithms for file encryption

Supported encryption algorithms for file encryption

u.trust LAN Crypt for iOS / iPadOS 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)

Supported encryption algorithms for key wrapping

u.trust LAN Crypt for iOS / iPadOS supports the following encryption algorithms for key wrapping:

- AES-256
- AES-192
- AES-128
- Supported, but not recommended: 3DES, 3DES TWO KEY, DES, RC4

  Note

  - With key wrapping (default setting), the transport key of the Security Officer data and the user profile data will be encrypted with a randomly generated session key, using the selected algorithm (AES is used by default). This key, on the other hand, is then RSA-encrypted using the public key from the certificate.
  - Please note that in comparison to u.trust LAN Crypt for Windows, the algorithm "RC2" is not supported by *u.trust LAN Crypt for iOS / iPadOS*. If the key wrapping for your policy file is set to this algorithm, the policy file cannot be used with *u.trust LAN Crypt for iOS / iPadOS*. In that case, you have to change the key wrapping encryption algorithm and choose an algorithm that is supported. (e.g., AES-128).

General preparations and setup

For security reasons, the Utimaco LAN Crypt app requires a passcode to be set for the device. When the app becomes active, it checks for the presence of a device passcode and if it finds that the device is not protected, it blocks usage until a device passcode has been set. Never use an easy-to-guess passcode, such as "1234" or "000000". Only with a secure passcode you can prevent unauthorized access to your confidential data, in case your device is lost or stolen. In general, Utimaco recommends to erase the policy file and certificate on your Apple device, if the device is not in use for a longer period of time, or if you exchange your device for a new one (see Deleting policy file and user certificate).

Note

- When the device passcode is turned off, the user certificate password is removed and must be re-entered after the device passcode is turned on again.

Providing the configuration data

After leaving the *u.trust LAN Crypt for iOS / iPadOS* welcome screen, you will be prompted to provide the configuration data:

- Import your policy file
- Import your user certificate

Note

- If SMB shares are used to distribute configuration files, the settings view shows an additional Network section. This allows to clear or enter the SMB credentials. When deleting the SMB credentials, downloaded configuration files are deleted as well.

Managing encryption keys

Managed keys and password-based keys can be both found within the settings. Managed keys originate exclusively from the given policy file, whereas password-based keys can be freely created, renamed and deleted inside the related settings. Renaming a key does not change the generated key used for encryption.

Note

- Password-based keys can also be created within the action of encrypting a file. These keys are then automatically added to the saved list of password-based keys.
- By successfully decrypting a file with a password-based key, the used key will also be automatically added to the saved list of password-based keys.
- Passwords used for generating password-based keys can also still be inspected after they have been created.

Policies

What are Utimaco LAN Crypt policy files?

A Security Officer (SO) centrally defines via the Administration of Utimaco LAN Crypt which files and storage locations are to be protected by Utimaco LAN Crypt with encryption and also which users have access to which of these data. For this purpose, the Security Officer creates one or more encryption rules for the user. Each individual encryption rule consists of an encryption path, a key and an encryption algorithm. Utimaco LAN Crypt policy files contain all encryption rules, that the user requires, in order to be able to work with encrypted data. For the user to be able to use the policy file, he/she needs a certificate, which will be provided to him/her as a key file (.p12 file) by the Utimaco LAN Crypt Security Officer. The key file contains the certificate and the private key of the user. The access to the key file is secured by a password. The user will receive the password through his Security Officer.

Automated import with LAN Crypt Cloud

If the Security Officer (SO) performs administration via the LAN Crypt Cloud, policy files and user certificates are automatically loaded. For this to happen, the user simply needs to be logged into the client with the appropriate LAN Crypt account. The login function can be accessed by tapping the profile icon in the top right corner of the application.

Manual import of policy files

Open the *u.trust LAN Crypt for iOS / iPadOS* App on your mobile device. Tap the **gear icon** at the bottom of the app to open the settings. Tap **Import your policy** and select the location that contains the policy file. The policy file will then be imported into the application.

Manual import of certificates

Open the *u.trust LAN Crypt for iOS / iPadOS* App on your mobile device. Tap the **gear icon** at the bottom of the app to open the settings. Tap the **Import your user certificate** and choose the location that contains the certificate key file (.p12 file). Into the dialog box, enter the password of your certificate, that you have received from your Security Officer. Once you have entered the correct password, the certificate and its associated private key will be stored in the application's certificate store.

Note

- *u.trust LAN Crypt for iOS / iPadOS* also supports referencing multiple user certificates in the policy file. In order to be able to use the policy file, the user must have at least one of the certificates that have been issued to him and whose public key is used to encrypt the policy file, and of course he must also have imported it.

Display certificate details

Open the app *u.trust LAN Crypt for iOS / iPadOS* on your mobile device. Then tap on the **user icon** in the LAN Crypt history (file browser) in the app in the upper right corner to open the settings view. There, tap on the selection **User Certificate**. The next dialog will show you more details about this certificate, such as the Subject and the Serial Number. If the certificate is not trusted, this is also indicated at this point.

Rolling out policy files and certificates using MDM

In addition to the app, you can use a Mobile Device Management (MDM) solution to deploy the individual configuration (policy file and certificate) for the mobile devices in addition to the app itself. If you do not have a Mobile Device Management (MDM) solution at your disposal, the configuration data (policy file and certificate) must be imported by each user manually, as described above.

Settings

Configuration data is a list of key+string tuples. Files must be provided as Base64-encoded strings, via URL, hosted on a HTTPS or SMB server. The following configuration keys are offered by LAN Crypt:

Operation Mode

operation_mode: Can be used to restrict the configuration options of the app **(STRING)**.

- Possible values:
  - `"cloud"`: Only LAN Crypt Cloud administration can be used.
  - `"classic"`: Only LAN Crypt on-premise administration (usage of policy files) can be used.
  - No value: Cloud or on-premise administration options are available.

Note

- If *operation_mode* is empty or has an undefined value and one of the MDM configurations are set (*policy_url*, *policy_blob*, *usercert_url*, *usercert_blob*, *admcert_url*, *admcert_blob*), `"classic"` is enforced by the app.

Policy

policy_blob: Policy XML or XML.bz2 file as Base64-encoded **(STRING)**.

policy_url: URL to a policy XML or XML.bz2 file **(STRING)**.

User Certificate / P12 file

usercert_blob: Certificate PKCS-12 file as Base64-encoded **(STRING)**.

usercert_url: URL to a certificate PKCS-12 file **(STRING)**.

Security Officer Certificate

admcert_blob: Security Officer Certificate (.cer) file (DER encoded) as Base64-encoded **(STRING)**.

admcert_url: URL to a Security Officer Certificate (.cer) file (DER encoded) **(STRING)**.

Default Key

default_key_guid: GUID of the key that must be used for encryption of new files **(STRING)**.

Note

- If this key is set, the user is not allowed to change the encryption key (forced encryption key). However, he can always use a password-based key for encryption (which results in an encrypted copy of the original file).

Samba Credentials

smb_username: If one of the policy or user cert settings refers to a SMB location, the user name for the SMB connection can be configured with this key **(STRING)**.

Note

- If the value is not set, the user is asked to enter the user name. Due to security reasons, the password for the SMB connection has always to be entered by the user.

Certificate Validation

cert_validation: Enables the certificate validation. Validation is disabled if setting is missing **(BOOLEAN)**.

Note

- The validation is disabled if the setting is missing.

Rules

- Managed settings cannot be changed or overruled by the user.
- URLs must be hosted on HTTPS servers with a valid SSL certificate. You can verify this by entering the URL in a browser on the mobile device (e.g., Chrome, Safari). If the file can be shown, the URL will also work as configuration value.
- If both BLOB and URL are supported for a setting, the BLOB has priority.
- If the data BLOB or URL of a setting is invalid, an error is shown.
- When using URLs for SMB shares, username and passwords will be ignored (use smb_username instead) (`smb://localfileserver/certificates/sepp.p12`) format: `smb://<host>/<share>/<folders>/<filename>`
- There are no documented maximum lengths for configuration strings but size of the strings should not be bigger than a few kilobytes.

WARNING - Intune and Base64-encoding of strings for iOS configuration data:

- When using Microsoft Intune and providing Base64-encoded strings: use XML configuration file format, as strings otherwise are cut by Intune without warning and incomplete data will be pushed to the device.

Deleting policy file and user certificate

Deleting the policy file

Open the *u.trust LAN Crypt for iOS / iPadOS* app on your iPhone or iPad. Within the *u.trust LAN Crypt for iOS / iPadOS* app, tap the **user icon** in the right top corner of the LAN Crypt Recents screen (file browser), to open the settings. On the right side, next to the policy file tap the Trash icon. Then tap **Delete**, if you really want to delete your policy file. Tap **Cancel**, if you do not want to continue deleting your policy file.

Deleting the user certificate

Open the *u.trust LAN Crypt for iOS / iPadOS* app on your iPhone or iPad. Then tap the **user icon** in the upper right corner of the LAN Crypt history (file browser) to access the settings. From there, tap the Trash icon to the right of the user certificate. Then tap **Delete**, if you really want to delete your user certificate. Tap **Cancel**, if you do not want to continue deleting your user certificate.

Open, edit, encrypt, decrypt and share files

u.trust LAN Crypt for iOS / iPadOS provides access to files that are stored locally on the mobile device, or on remote storage systems. The access to remote storage systems (e.g., on OneDrive or Google Drive), via the file browser, is protected by iOS sandbox security. The iOS sandbox security provides protected remote access, over file browsers, that are provided by apps installed on the device. Thus, a user can, for example, use the *u.trust LAN Crypt for iOS / iPadOS* app to access data stored on OneDrive, provided that the OneDrive app is installed on your device. The access to Google Drive happens in a similar manner, if the associated app is installed on the mobile device.

How to access encrypted data?

There are various ways how you can access files using your iPhone or iPad. This can be done within the *u.trust LAN Crypt for iOS / iPadOS* app via the file browser or from there via a proprietary app for cloud storage (such as OneDrive). With *u.trust LAN Crypt for iOS / iPadOS* you can open encrypted and unencrypted files, edit them and save them encrypted. If the file was already encrypted, it will be encrypted even after editing. You can use your preferred apps to modify files, e.g., Microsoft Office can be used to edit documents, presentations, and spreadsheets. The document preview has an **Edit** button. This can also be used to forward a file to a third-party apps.

Open encrypted file

To open an encrypted file, use the Utimaco LAN Crypt app, browse to the location that contains the encrypted file and tap the file to open it. This file is then opened and decrypted directly via the integrated viewer of the Utimaco LAN Crypt app on your iPhone or iPad. For this purpose, *u.trust LAN Crypt for iOS / iPadOS* QuickLook framework. All files always remain in the secure sandbox of the Utimaco LAN Crypt app when displayed and are therefore always optimally protected. On the storage location itself, however, this file remains encrypted. All encryption and decryption processes only occur on the mobile Apple device itself.

> **The QuickLook framework for iOS has limited editing support for certain file types:**
>
> - ***PDF and image files:*** Mark-up support. Tap the pen-tip icon in the navigation bar when viewing the file.
> - ***Video files:*** Rotation and Trimming support. Tap the rotate or trim button in the navigation bar when viewing the file. Tapping the Done button saves the changes back to the original file.

Edit files with third-party apps

1. Tap the **Edit** button in the document preview.
2. Document preview is closed and the iOS share screen comes up. Select your application of choice.
3. The third-party app comes up and presents the document. Work with the app as usual.
4. When the third-party app writes the changes, *u.trust LAN Crypt for iOS / iPadOS* makes sure that the changes are written to the original location, e.g., being uploaded to a cloud storage provider.

Display file encryption information

A badge icon in the right top corner of the thumbnail indicates if a file can be opened:

- **green key:** The file is encrypted and can be accessed.
- **gray key:** The file is plain and can be accessed.
- **red key:** The file is encrypted and can not be accessed (the key is not available or the used encryption algorithm is not supported on mobile).
- For more information long-press a file to open the context menu. There you can select the option **Encryption Info**.
- The **Encryption Info** dialog now shows you the following information about the file:
- **Encryption State:** Indicating if the file is encrypted or not.
- **Key name:** The name of the key used for encryption (only shown for encrypted files).

- **Key Id:** The GUID of the key used for encryption (only shown for encrypted files).
- **Key availability:** Indicating if the key is available in the policy (only shown for encrypted files).
- **Supported on Mobile:** Indicating if the used encryption algorithm is supported on the device (only shown for encrypted files where the algorithm is not supported).

Encrypt a file with a key from the policy file

To encrypt a file, first navigate to the location where the file is stored using the integrated file browser in the *u.trust LAN Crypt for iOS / iPadOS* app. **Long-press** the file you want to encrypt. The context menu appears. Then tap the **Encrypt** option there. In the next dialog you can decide with which method you want to encrypt the file. In the middle part of the dialog your available keys are displayed. If a default encryption key was set up for you, it is marked there. Select the key you want to use to encrypt the file. Then tap **Done** in the upper right corner. The file is encrypted with the previously selected key.

Note:

- If no default encryption key was set up for you, you can change the encryption key from the list by tapping on another available key. In that case, the file will be encrypted using that key instead of the previous selected key.
- Unlike the encryption using a password-based key, the encryption with a key from the police file will encrypt the file in-place which makes the file inaccessible to read without the used key.

Encrypt and share as password-protected file (u.trust LAN Crypt 2Go)

If you want to share a password-protected file, navigate to the location where the file is stored using the integrated file browser in the *u.trust LAN Crypt for iOS / iPadOS* app. **Long-press the file** you want to encrypt. The context menu appears. Tap the **Encrypt** option there. Then tap the **Share as password-protected** file slider so that it is highlighted in green. Now you can either select a previously used password or create a new password for encryption. By creating a new password in this way, the password will automatically be saved on device and can be used to further encrypt and decrypt files. Password-based keys can also be found and edited in the settings menu. In the next dialog, select the app you want to use to share the file in encrypted form, or alternatively tap Save to Files, if you want to save the file in encrypted form to a folder in the iCloud for example. Using AirDrop, you can also share the encrypted file with a nearby device via Wi-Fi or Bluetooth.

Note:

- The encryption requires a secure password! This must be at least 8 characters long and contain upper- and lower-case letters, numbers and special characters. The password used for the key can still be inspected later on in the settings.
- The name given to the encryption password does not have any impact on the key used for encryption. The actual key value for encryption is generated separately.
- Unlike the in-place encryption using a key from the police file, the encryption with a password-based key will not manipulate the original file and will instead create an encrypted copy of the file to then share.

Decrypt and share a file

To decrypt a file, first navigate to the location where the encrypted file is stored using the integrated file browser in the *u.trust LAN Crypt for iOS / iPadOS* app. Long-press the file you want to decrypt. The context menu appears. Then tap the **Decrypt** option there. If the file is a password-protected file, an additional dialog may be displayed at this point. In this case, enter the required password in the Enter password field. In the next dialog, select the app you want to use to share the file decrypted or, alternatively, tap **Save to Files**, if you want to save the file decrypted to a different location. After that, tap **Save** in the top right corner. The file is shared decrypted or saved decrypted in the previously selected location.

Note:

- If you choose the same location, another dialog will ask you if you want to replace the existing file.
- By successfully decrypting a file with a password-based key, the used key will automatically be added to the saved list of password-based keys. The list of

password-based keys can be found and edited in the settings. The password used for the password-based key can also be accessed there.

Logging

u.trust LAN Crypt for iOS / iPadOS has a Verbose Logging feature. The usage of this feature is only intended for error analysis and should only be enabled if you encounter any errors or issues with the *u.trust LAN Crypt for iOS / iPadOS* app.

Verbose logging

Open the *u.trust LAN Crypt for iOS / iPadOS* app on your iPhone or iPad. Within the *u.trust LAN Crypt for iOS / iPadOS* app, tap the **user icon** in the right top corner of the LAN Crypt history (file browser), to open the settings. Move the slider to the right to **enable** the Verbose Logging feature. The Verbose Logging feature is enabled once the area around the slider button is colored green. Take the necessary steps to reproduce the error, to create the log files.

Note:

- In no case will the log files reveal sensitive information!

Send logs

By using the **Send Logs** feature, you can send the log files, for analysis purposes, to the Utimaco support team by e-mail. To send the log files, tap the **share icon**, that appears to the right of **Send Logs**. Then select the app you use for your email communication. The log file will be attached as a compressed file (.zip) and sent to the team at support@Utimaco.de. To disable the **Verbose Logging** feature, move the slide button back to the left.

Compatibility with Cloud Services

LAN Crypt supports the encryption of files stored on cloud-based platforms, providing an additional layer of protection against unauthorized access - even by the operators of the cloud services themselves. Cloud providers such as Microsoft, Google, and similar platforms typically offer additional capabilities, such as collaborative document editing or content-based file search. Since these services cannot access the contents of encrypted files, such features are unavailable for files protected by LAN Crypt. The encrypted data is subject to a particularly high level of protection and therefore cannot be processed by these services.

Microsoft 365 Services Not Compatible

The following Microsoft 365 features require content-level analysis and therefore cannot be used with files encrypted by LAN Crypt:

- Mail flow rules, including anti-malware and anti-spam checks that require access to attachments
- Microsoft Delve
- eDiscovery
- Content search and indexing
- Office Web Apps, including collaborative document editing

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

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.com. 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

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