



u.trust LAN Crypt Protection for Business-Critical Data — Convenient. Reliable. Secure.



Utimaco
u.trust LAN Crypt









u.trust LAN Crypt in a Nutshell

Convenient, reliable, and secure protection for business-critical data

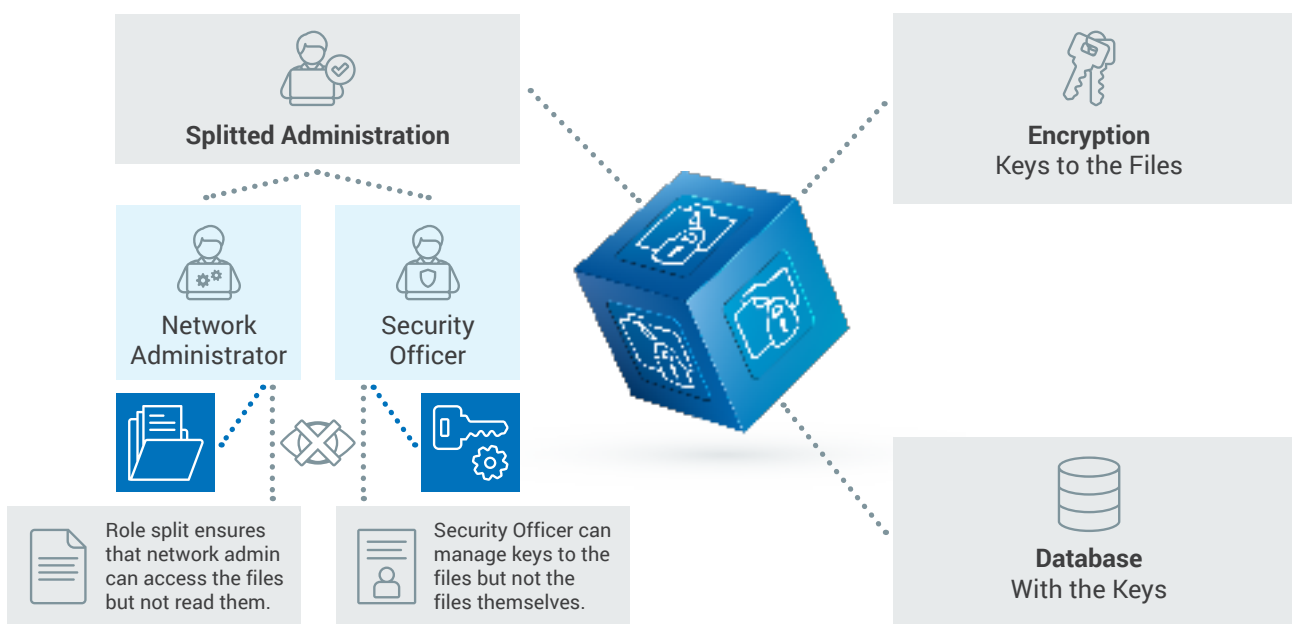
Utimaco's u.trust LAN Crypt is a software-based data encryption solution. It protects your data against unauthorized internal and external access regardless of the storage location by transparently encrypting all files according to the policy framework.

u.trust LAN Crypt is adding the extra-layer of security to your data. With its role-based access rights management it enables you to avoid unauthorized external access (e. g. by attackers or external consultants with administrative rights) as well as internal access (e. g. by network administrators) within your organization. Given that, it is the ideal solution to ensure compliant data management. Furthermore, the cryptographic keys used to encrypt your data are solely stored in a central data base or in the key ring at the users' local machine so you are 100% independent from the (cloud) providers you may use.

With u.trust LAN Crypt you will benefit from:

<p>Role-based encryption of sensitive and business-critical data</p> 	<p>Protection against unauthorized internal and external data access</p> 	<p>Fulfillment of individual security policies and compliance rules</p> 
<p>Cross-platform and transparent data access – no changes in your employees' working routine</p> 	<p>u.trust LAN Crypt 2Go: Password-based encryption for secure data sharing with external parties</p> 	<p>Appropriate evidence for companies and authorities</p> 

Basic Architecture



Key Features

Role-based encryption of sensitive and business-critical data

With u.trust LAN Crypt, all your company data is fully encrypted and can only be accessed and decrypted by users with corresponding access rights. You can flexibly decide which user groups are allowed to access which kinds of data. Your employees won't notice any difference in their working routine: Encryption rules are set up by the security officer and are transparent to the users.

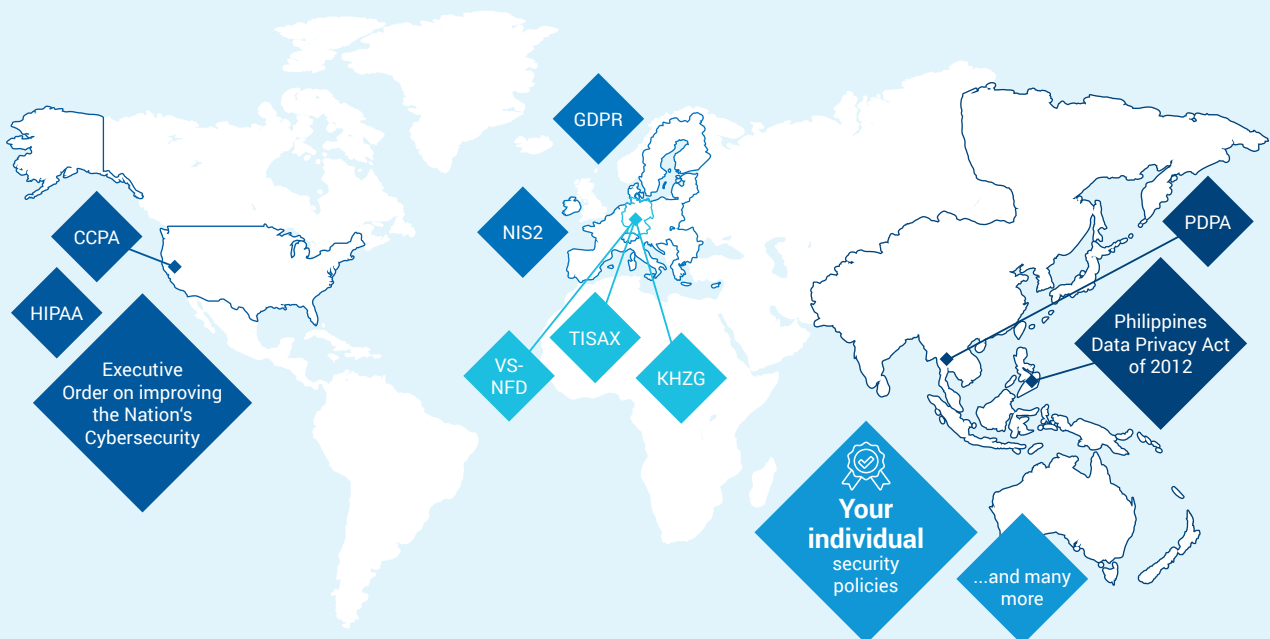
Protects against unauthorized internal and external data access

The persistent encryption protects your confidential files against unauthorized external or internal access. Furthermore, u.trust LAN Crypt uses a strict role split approach: The network administrator can access and manage files and the security officer manages keys and security policies. This ensures a complete separation of network administration and security management.

Helps fulfilling local compliance rules and achieving your company's security policies

With its persistent encryption method and role-based access management, u.trust LAN Crypt helps fulfilling the most important data protection rules and regulations, e. g.

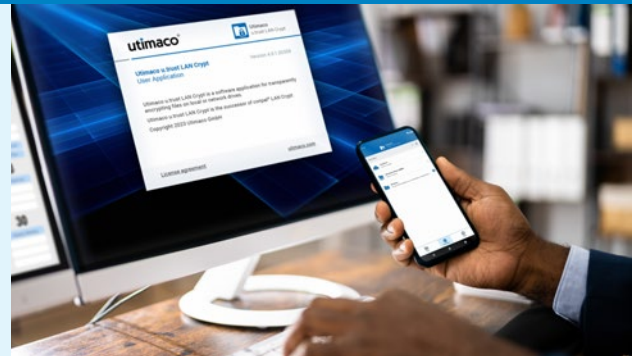
- **GDPR** (EU)
General Data Protection Regulation
- **CCPA** (CA, USA)
California Consumer Privacy Act
- **TISAX** (DE)
Trusted Information Security Assessment Exchange
- **HIPAA** (USA)
Health Insurance Portability and Accountability Act
- **KHZG** (DE)
Krankenhauszukunftsgesetz
- **Executive Order on improving the Nation's Cybersecurity** (USA)
- **Philippines Data Privacy Act of 2012** (PH, APAC)
- **PDPA** (TH, APAC)
Personal Data Protection Act
- **NIS2 Directive** (EU)
- **Your individual security policies**



u.trust LAN Crypt provides the **appropriate evidence for companies and authorities** to fulfill data protection policies.

Protects Data at Rest and Data in Motion while granting cross-platform and transparent access

All files are encrypted and decrypted directly at the users' endpoint (e. g. PC/Laptop, Tablet, Smartphone, Terminal Server) regardless of the storage location (e. g. Cloud, Data Center, USB device, local drive). This ensures that data remains encrypted when transferred and cannot be captured. As decryption and encryption happen unnoticed in the background, there is no visible change for your employees' working routines or any noticeable impact on the performance of your systems.



u.trust LAN Crypt 2Go: Password-based encryption for secure sharing with external parties

u.trust LAN Crypt additionally allows the secure sharing of external documents with a password. Users can simply set a password for a certain file and share it with people outside their organization. The recipients can then decrypt it with the corresponding password.

This is ideal for organizations who work on sensitive projects with other companies e.g. external consultants. Only one party needs to have u.trust LAN Crypt installed.

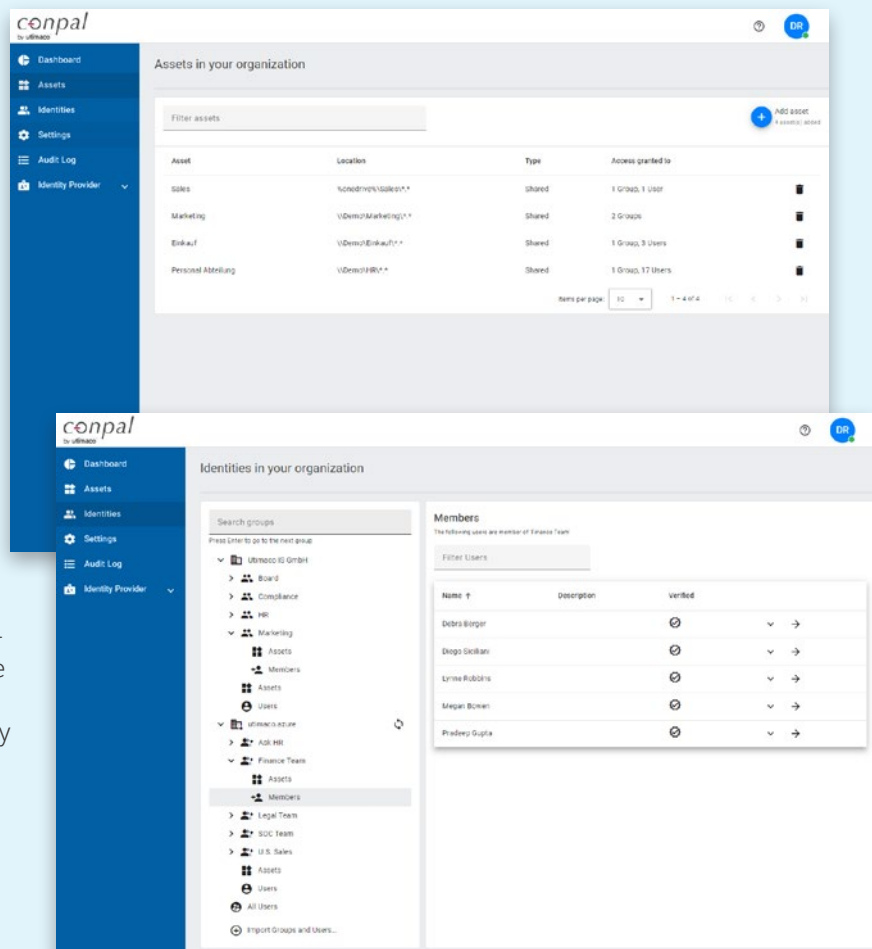
Optional: Managed in the u.trust LAN Crypt Cloud

u.trust LAN Crypt is available to be managed in the Cloud. In the Cloud platform, administration of u.trust LAN Crypt is easy to use even for administrators without technical knowledge.

In 3 simple steps you will be guided through the setup:

1. Define assets
2. Define identities
3. Distribute access permissions

You can be up and running in less than 5 minutes. Administration is completely platform-independent – no back-end installation required. Manage and monitor from a single dashboard that gives you visibility into devices, users, and other information – a powerful tool for passing compliance audits.



Technical Details

Technical Requirements

Client 64 Bit



Windows 10 Pro/Enterprise

- 1809 (LTSC)
- 20H2
- 21H2
- 21H2 (LTSC)
- 22H2

Windows 11 Pro/Enterprise

- 21H2
- 22H2

Windows Server

- 2019
- 2022

Supported Citrix Environments

- Citrix Virtual Apps and Desktop 7 1912 LTSR CU2 on WS 2019

macOS

- 10.15 Catalina
- 11 Big Sur (M1 & Intel)
- 12 Monterey
- 13 Ventura

Administration 64 Bit



- Windows 10 Pro/Enterprise*
- Windows 11 Pro/Enterprise*
- Windows Server*

Mobile Operating Systems



- Android 10, 11, 12, 13
- iOS / iPadOS 15, 16

* See client versions for supported versions

Supported Media and Platforms



Media

- Network drives
- Local hard disks
- CD / DVD
- USB
- Flash drives
- Memory cards

Platforms

- Microsoft Terminal Server
- Virtual Machines
- OneDrive
- Azure SQL
- Dropbox
- Google Drive
- MS Azure (e.g. Clients, Azure, DB)

Supported Databases



Microsoft SQL Server

- 2019
- 2022

Oracle Database

- 19

Supported Algorithms



Encryption

- AES 128 Bit and 256 Bit
- 3DES 168 Bit
- DES
- IDEA 28 Bit
- XOR

Certificates

- RSA up to 4096 Bit
- Self-generated or via involvement of a PKI
- Softcertificates
- Smartcards
- Tokens

Recommended algorithm

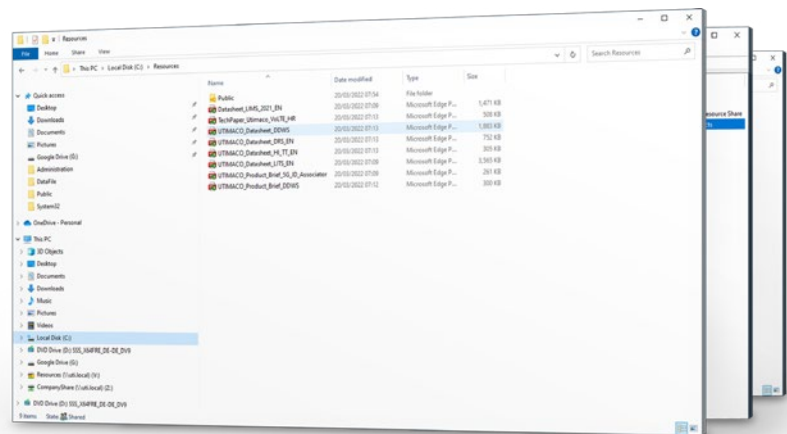
- AES-256

Recommended encryption format

- XTS-AES

Hash

- MD5
- SHA256



About Utimaco

Utimaco is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

Utimaco develops on-premises and cloud-based hardware security modules, solutions for key management, data protection, and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. Utimaco is one of the world's leading manufacturers in its key market segments.

550+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of Utimaco's high-security products and solutions.

Find out more on utimaco.com



Headquarters Aachen, Germany



Headquarters Campbell, USA



Contact us



EMEA

Utimaco IS GmbH

📍 Germanusstrasse 4
52080 Aachen,
Germany

☎ +49 241 1696 200

✉ info@utimaco.com

Americas

Utimaco Inc.

📍 900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

☎ +1 844 UTIMACO

✉ info@utimaco.com

APAC

Utimaco IS Pte Limited

📍 6 Temasek Boulevard
#23-04 Suntec Tower Four
Singapore 038986

☎ +65 6993 8918

✉ info@utimaco.com

For more information about Utimaco® products, please visit:

utimaco.com

© Utimaco IS GmbH 02/24 – Version 1.7

Utimaco® is a trademark of Utimaco GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

Creating Trust in
the Digital Society

utimaco®