conpal LAN Crypt

Data sheet

conpal LAN Crypt

conpal LAN Crypt is a sustainable enterprise security solution. It persistently protects files from unauthorized access through role-based, client-side encryption.

Remote work

With conpal LAN Crypt, data can be protected regardless of the work location. Whether working from home, on the road or in the office: thanks to the keys and encryption rules assigned to the user, work remains secure without interruption, regardless of the end device used.

Keys are assigned as part of a three-level key concept. This ensures unique assignment to the respective user and enables fast re-encryption of files without computationally intensive processes.

Mobile devices

conpal LAN Crypt is available for all popular mobile devices: iPhone, iPad, Android phones and tablets. The user profile is the same on all devices used. This means that there is no additional administration effort. The user can work without interruption. Clients are available for iPhone/iPad: iOS 15 & 14, iPadOS 15 & 14, Android: 12, 11, 10 & 9.

Two factor authentication

conpal LAN Crypt supports numerous methods for two-factor authentication (2FA) and multi-factor authentication (MFA).

User accounts

conpal LAN Crypt offers unique, personal user accounts for each user.

It is set up exclusively by the responsible SO (Security Officer), and can be additionally secured by a release process. The extensive rights assignment documentation features support regular audit processes.

The ability to assign hierarchical SO roles also supports use in large organizations with multiple locations.

Access control

The system of role-based access rights offered by conpal LAN Crypt guarantees adherence to the "need-to-know" principle. Normal users cannot access data for which there are special access requirements. Data is encrypted at the content level.

When collaborating with other departments, external parties, or partners along the value chain, the role-based approach ensures that the individual work areas are always kept separate. This means that business-critical data never falls into the hands of unauthorized persons.

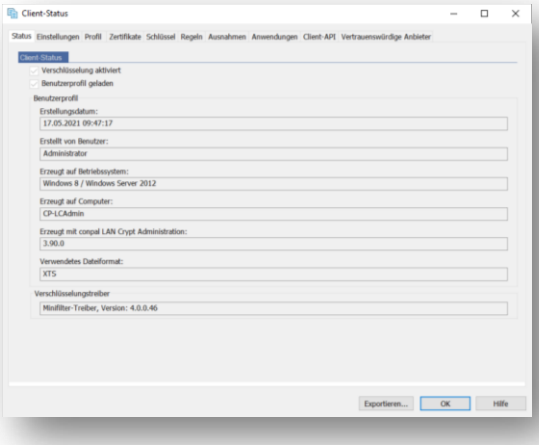
Cryptographic processes

Due to the support of different cryptographic algorithms and methods, the possibility to control key lengths and encryption strength, life cycle defaults and emergency key recovery, conpal LAN Crypt enables a wide range of cryptographic concepts.

Due to the used XTS-AES 256-bit algorithm the encryption is done on the state of the art.

Data-in-motion

The client-side persistent encryption of conpal LAN Crypt ensures that files remain protected on all channels and storage media in transit. They are not visible in plain text at any point. Even when exchanged via cloud platforms, no third party gains access.



External IT-systems

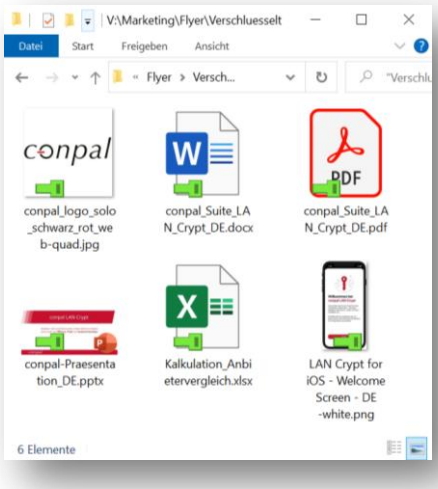
Through file-level encryption, conpal LAN Crypt supports concepts for separating data on shared external IT platforms and prevents unauthorized access. Especially when working with partners along the supply chain, the role-based assignment of keys enables effective concepts for segmenting data.

Especially for the exchange of data with external parties, conpal LAN Crypt 2Go offers the option of password-based encryption. Recipients can decrypt files on all common end devices (Windows, Mac, iPhone, iPad, Android, Linux) or via the web portal www.conpal.de/en/2Go.

Compliance

conpal LAN Crypt supports compliance with legal frameworks such as GDPR (especially art 5.1, 5.2, 30.1, 32.1) and meets the requirements of the technical and organizational measures (TOM) required therein.

conpal LAN Crypt



Technical overview conpal LAN Crypt

conpal LAN Crypt encrypts confidential files persistently. This ensures secure transfer (data in transit) and secure storage (data at rest) of confidential data in all kinds of environments (cloud share, file share, local storage media) in a manner that is sustainable and tamper-proof.

- To the user, the encryption is completely transparent, taking place in the background
- Seamless integration into all enterprise service platforms and third-party tools thanks to its efficient, cutting-edge API architecture
- Authorization is granted by assigning a unique “key group” to a user profile
- Easy implementation of GDPR requirements for internal needs and for the use of mobile media
- Scalable solution, ideal for project teams, departments, companies, or enterprise-wide

System requirements

Administration 64 Bit:

- Windows 11, Windows 10 Pro/Enterprise 19H2 and up Windows Server 2022, 2019, 2016

Clients:

- 64-Bit Windows: Windows 11, Windows 10 Pro/Enterprise 19H2 and up
- Mac: macOS 11 (M1 & Intel), 10.15, 10.14
- iPhone/iPad: iOS 15 & 14, iPadOS 15 & 14
- Android: 12, 11, 10, and 9
- Windows Server 2022, 2019, 2016
- Citrix XenApp 7.18 on Windows Server 2016 and 7.15 LTSR on Windows Server 2016

Databases supported

- Microsoft SQL Server 2019, 2017
- Oracle 19

Algorithms supported

- Encryption: AES 128 Bit und 256 Bit, 3DES 168 Bit, DES, IDEA 128 Bit, XOR
- Certificates: RSA up to 4096 bit, self-generated or involving a PKI, soft certificates, smart cards, tokens
- Recommended algorithms: AES 256
- Recommended encryption format: XTS-AES
- Hash: SHA256

Any questions? Just talk to us!

conpal

You will find further details on our website. We can also make the relevant release notes available to you on request.

Dornhofstraße 69 · 63263 Neu-Isenburg/Germany ·
www.conpal.de
SalesSupport@conpal.de
Phone +49 (0) 6102 / 751 98 0