conpal LAN Crypt

Smart
High-security
Persistent
encryption

Protection of sensitive data for enterprise organizations

Agile data requires flexible encryption

Companies often store sensitive, business-critical data such as company reports, personnel data and customer information largely unprotected in electronic form.

It can be stored locally, on external storage media, on-premise or in the cloud – with significantly increased risks.

As there is an increasing tendency to "cloudify" when managing (sensitive) data, applications and system environments in the course of the "mobilization" of user devices (such as notebooks, tablets, smartphones, etc.), the risks of improper use, data theft and loss of control increase exponentially. Furthermore, most protective measures are aimed at external threats, whereas internal IT risks are often neglected.

However, the potential damage from improper use of confidential company data is the same. It is essential to have a security solution that adapts to the requirements of enterprise environments and grants access to sensitive data only to authorized users throughout the organization.
Encrypted content should always be encrypted persistently to ensure complete protection across different platforms.

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

Separation of roles

conpal LAN Crypt provides for the strict separation of administrator and security roles so that data security policies can be enforced rigorously.

- System administration is carried out by the administrator, as before, but without the authority to decrypt files
- Security personnel are responsible for key management and defining access policies for individuals or groups
- Security personnel define individual access rights for work groups or individual users in accordance with the security policies

conpal LAN Crypt

Data security

conpal LAN Crypt is the sustainable enterprise security solution that systematically prevents unauthorized access to sensitive data.

- Tested and proven security algorithms
- User authentication via X.509 certificates

Security administration

Thanks to its sophisticated administration concept, integrating conpal LAN Crypt into your IT security architecture is quick and uncomplicated.

- Cost-efficient solution designed for easy installation without additional administration infrastructure
- Integrated recovery processes for access to encrypted data in emergency situations

User convenience

- No changes are necessary to the working environment or work practices
- Optimized performance for encryption and decryption of protected data on a client

System requirements

Client 64 Bit

- Windows 10 1803 (RS4), 1809 (RS5), 1903 (19H1), 1909 (19H2), 2004 (20H1), 2009 (20H2) Pro/Enterprise
- Windows Server 2012 R2, 2016, 2019
- Citrix XenApp 7.18 on Windows Server 2016 and 7.15 LTSR on Windows Server 2016

Administration 64 Bit

- Windows 10 Build 1803, 1809, 1903, 1909, 2004 Pro/Enterprise
- Windows Server 2012, 2012 R2, 2016, 2019

Databases supported

- Microsoft SQL Server 2012 SP4, 2016 SP2, 2017, 2019
- Oracle 12
- Oracle 19

Media and Platforms supported

- Media: Network drives, local hard disks, optical media, USB, flash drives and memory cards
- Platforms: Microsoft Terminal Server, virtual machines, OneDrive, Azure SQL, Dropbox, Google Drive, MS Azure (e.g. clients, Azure DB)

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
Fax: +49 (0) 6102 / 751 98 99