digitronic®
.net

HiCrypt™

The new generation of data encryption

What is HiCrypt™?

HiCrypt™ encrypts data on network drives and ensures that only the group of people in possession of the corresponding key can view the confidential data. The software is installed in just a few minutes, runs silently in the background and is very easy to use.

All-round protection even in the home office

No matter from where you access the data: whether from the company network or via VPN in the home office, with HiCrypt™ you hold the key to the confidentiality of your data yourself. It doesn't matter whether the data is on a Windows share or a WebDAV drive in the cloud.

Confidentiality through separation of powers

HiCrypt™ key management is performed only by persons who are exclusively responsible for the confidentiality of the data contents (e.g. CEO). Administrators can prepare drives to be encrypted for use, but do not need to have authorization to view the data. This protects them in case of suspicion.

HiCrypt™

- ✔ collaborative work on encrypted shares possible
- ✔ central rollout and management capabilities
- ✔ integrated user management
- ✔ disaster recovery capabilities
- ✔ full control over permissions
- ✔ separation of authority through decoupled access rights
- ✔ fully scalable: for small, medium and large enterprises

Our promise as a manufacturer

All solutions from our company have been developed on the basis of concrete requirements and needs from practice. The solutions therefore already include many individual configuration options. As a manufacturer, however, we are also happy to work with you to develop customizations that best meet your specific requirements.

Contact

digitronic®
computersysteme gmbh
Oberfrohnaer Str. 62
09117 Chemnitz

+49 371 81539 0
sales@digitronic.net
www.digitronic.net

HiCrypt™
The new generation of data encryption

Functionality & Features

Which HiCrypt™ suits you?

The HiCrypt™ family includes **HiCrypt™ Professional** and **HiCrypt™ Enterprise Services**.
You decide which one is right for you.

How HiCrypt™ works:

Management Studio, Initial Encryption, ...

Feature summary:	HiCrypt™ Enterprise Services	HiCrypt™ Professional
Working together on encrypted shares	✔	✔
Central rollout and management option	✔	✔
Restoring individual files from a backup	✔	✔
Support for individual password policies	✔	✔
Protection of administrators in case of suspicion	✔	✔
Integrated user administration	✔	✔
Token support*	✔	✔
Connection to existing user administration	✔	✖
Workflow-Integration	✔	✖
Script-based control possible	✔	✖
Central management of all encrypted shares	✔	✖
Convenient SSO on encrypted shares	✔	✖
Initial Encryption	✔	✖

* Which tokens are supported you can read under https://www.digitronic.net/en/encryption/#info -> Notes

https://www.digitronic.net/en/encryption

HiCrypt™

The new generation of data encryption

Technical details - HiCrypt™ Professional

Supported operating systems

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7 or later (x86 und x64)

Supported encryption algorithms

- AES 256
- Blowfish 448
- IDEA 128

Installation format

- Product Key: Installation programme (EXE)
- Floating License: Microsoft Installer (MSI)

Space requirement on the main disk

about 50 MB

Software requirements

- Microsoft .NET-Framework 4.6

License types

- **Single user license:**
  For the single user license, we offer a product key (license key) that can be used for activation on any number of systems (depending on the offer). One installation with one (simultaneous) user can be licensed at a time. A transfer of licenses is made possible by uninstallation (incl. deactivation).

- **Terminal server license:**
  With the terminal server license, there is also a product key, which, however, must be generated with the number of users to be logged on simultaneously (depending on the offer). Here, simultaneous users on one system are licensed.

- **Floating license:**
  One copy of the software can be installed on multiple devices. However, only as many software instances as there are floating licenses can be used simultaneously. For verification, the software establishes a connection to the WIBU license server.

- **Volume license ("Golden Key"):**
  The volume license is bound to the customer's Windows domain and can thus be used as often as desired.

Further information

Requirements at your site

- network drive
- when using the floating license:
  - Setup of a license server
    - WIBU CodeMeter with Soft- or Hardwaredongle

Included in delivery

- the installation package for HiCrypt in EXE or MSI format.
- the licence required for the respective licensing (product key or licence dongle)

Documentations and test download

➔ https://www.digitronic.net/en/encryption/

HiCrypt™

The new generation of data encryption

Technical details - HiCrypt™ Enterprise Services

Supported operating systems
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7 or later (x86 und x64)

Supported encryption algorithms
- AES 256
- Blowfish 448
- IDEA 128

Licensing system
- Floating licence (WIBU CodeMeter with software or hardware dongle)

Installation format
- Floating License: Microsoft Installer (MSI)

Space requirement on the main disk
about 50 MB

License types
- **Floating license:**
  One copy of the software can be installed on multiple devices. However, only as many software instances as there are floating licenses can be used simultaneously. For verification, the software establishes a connection to the WIBU license server.

Software requirements
- Microsoft .NET-Framework 4.7
- Microsoft VC Redistributable 2015 Update 3
- CodeMeter Runtime auf allen Systemen

Other requirements
- Microsoft SQL Server 2012 / 2014 / 2016
- (ODBC driver required)
- File server
- Optional: User directory

Further information

Requirements at your site
Administrator(s) for the following areas:

- network drive
- database
- domain
- file server
- clients / virtual clients
- optional: firewall admin

In addition, a global admin password administrator is required as this role must be assigned during initial setup.

Included in delivery
- the installation packages for all HiCrypt Enterprise Services components (Client, Studio, Service, Agent) as MSI package.
- the setups for the necessary prerequisites (.NET Framework, cmdlets for the supplied scripts, Codemeter Runtime for the licence server, Codemeter Runtime for all other systems, ODBC drivers, etc.)
- a schema for creating the necessary tables and structures on the (SQL) database
- registry entries that are needed (adjustments are required)
- configuration files (in "raw form", must be adapted to AD)
- licence dongle

Documentations and test download

➔ https://www.digitronic.net/en/encryption/

digitronic®.net