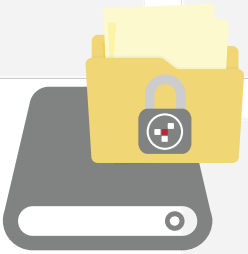
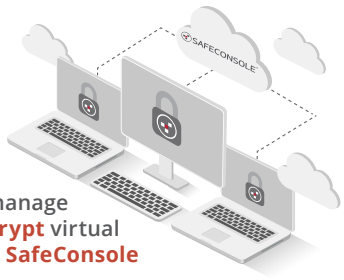
DATALOCKER®
SIMPLY SECURE

SAFECRYPT®
ENCRYPTED VIRTUAL DRIVE

SAFECRYPT®

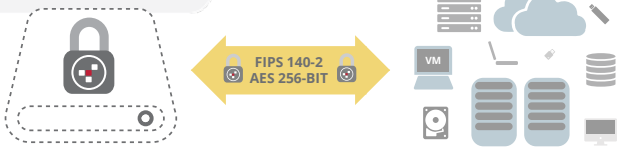




Centrally manage your **SafeCrypt** virtual drives with **SafeConsole**

Encrypted Virtual Drive

Encrypt locally on the **SafeCrypt** virtual drive and point to **ANY** storage location



COMPLETE LOCKDOWN AND AUDITING FOR YOUR SENSITIVE DATA

For companies and individuals, data security is a deciding factor in choosing where to store data. SafeCrypt makes storing your data flexible and secure no matter where you store it, whether it be on a commercial cloud storage service, local storage, or network storage location. SafeCrypt from DataLocker provides a virtual drive secured by FIPS 140-2 validated, military-grade encryption that is storage agnostic and cross-platform compatible. SafeCrypt puts the data encryption in the control of its users as no one except the encrypted volume owner has access to the encryption keys. File activity on the SafeCrypt encrypted volume is audited and available in SafeConsole or can be optionally sent to a SIEM.

CENTRALLY MANAGE YOUR ENCRYPTED VIRTUAL DRIVE

SafeCrypt combines military-grade AES 256-bit encryption with a secure connection to a central management console to protect the contents of the virtual drive. SafeConsole® is a secure online or on-premises management platform able to deploy and apply security policies to SafeCrypt virtual drives with full inventory, audit, and control capabilities for ease and efficiency.

SAFECRYPT MANAGED FEATURES

- **SafeConsole Management:** Customize minimum password requirements for encrypted virtual drives. Allow users to request a password reset, view file activity with geolocation info, and more
- **Fully Compatible:** SafeCrypt works with local files, network drives, external hard drives, flash drives, single-user cloud storage, etc.
- **Advanced Security:** SafeCrypt offers advanced features like encrypted file names, read-only mode, file type restrictions and brute force attack defense

HOW DOES SAFECRYPT WORK?

SafeCrypt utilizes an AES 256-bit mode encryption library to create a virtual drive that automatically encrypts all data saved to it without the need for PKI.

Run SafeCrypt's setup wizard and connect to the SafeConsole management platform using the SafeConsole connection token.

All data saved to the SafeCrypt virtual drive is fully encrypted locally and the encrypted files and file names are automatically synced to your designated location.

SafeCrypt can even be pointed to a local folder to encrypt files anywhere on the local machine.

To access the encrypted files, simply unlock the SafeCrypt drive with your password and open the folder. Your files are decrypted on the fly at your machine.

Admins can set up custom policies within SafeConsole to customize user's functionality of their virtual drives.

TECHNICAL SPECIFICATIONS

CRYPTOGRAPHIC PROCESSES
AES 256-bit / CTR Mode

STANDARDS AND CERTIFICATIONS:
FIPS 140-2 Validated Crypto Engine (Cert #2768)

LICENSE TYPE
1 or 3 year licenses available

SYSTEM COMPATIBILITY
Windows 7 (64bit) or 10 (64bit)
macOS 10.10 - 10.15

PART NUMBERS:
SCM-1, SCM-3, SCM-1R, SCM-3R

A new or existing SafeConsole Account is required in order to utilize and deploy SafeCrypt. A one-time base fee is required for new SafeConsole Accounts. A SafeCrypt license is required for each managed SafeCrypt encrypted virtual drive.

datalocker.com
sales@datalocker.com
+1 855 897 8755 or +1 913 310 9088