



EndPoint Encryption

Your Digital Life Insurance

Falcongaze EndPoint Encryption:

- Using exceptionally strong encryption patterns, the application can protect your data wherever they are stored. It provides consistent information security for your PCs, laptops, removable media and portable USB storage devices. Falcongaze EndPoint Encryption can be used to secure any kind of information including employee and customer databases, legal and financial records, intellectual property, etc.
- Rich functionality of the product ensures ultimate protection for your data: pre-boot authentication, encryption of fixed disks (HDD, SSD, etc.) and removable media, as well as any partitions thereof, including system partitions.
- Transparent encryption and decryption processes causing virtually no interruption to users' work or system performance help maintain operational efficiency. Users can access, store, share, and transfer data safely.
- Convenient features for centralized deployment and management. Using these functions, an administrator can install, configure and control smooth operation of the software across a corporate network.

Key Features

- Fixed disk (HDD, SSD, etc.) encryption of desktops or laptops, including system partitions. Full-disk or multi-partition encryption, including system partition (operating system files, swap/ hibernation files).
- Removable media encryption (USB devices, flash drives, CD/DVD).
- Transparent encryption ("on-the-fly") performed in real time – the process is absolutely invisible to the user and has no effect on hardware performance.
- Pre-boot authentication – a password is required before booting an operating system, which minimizes the possibility of unauthorized access to confidential data.
- Authentication with the use of key drives.

Administrator Features

- Setting an administrator password for all user accounts' control, thus helping administrator recover user access in case of user password loss.
- Centralized installation and management of workstations' encryption components.
- Policies to block write access to unencrypted drives, i.e. employees are obliged to encrypt removable drive before copying any information to it.
- Customizable password complexity requirements for security reinforcement.
- Microsoft Active Directory integration that helps to synchronize Active Directory users with the program database and track new or excluded users automatically.
- Flexible user access policy provides different access levels for separate users and user groups.

Client Features

- Option to create and use encrypted containers (virtual encrypted discs).
- Granting rights to reset password to users, however keeping administrator's access to all user data and account settings.
- Using keyfiles alongside with passwords or instead of them.

Encryption Process

- Using the AES, Serpent and Twofish algorithms to encrypt data.
- Support for multiple encryption using several cryptographic algorithms.
- The program supports XTS mode, developed specially for encrypting disk data.

Technical Information

- Protection against «Brute force» attacks (direct password screening) according to PKCS#5 v2 standard.
- Protection against keyloggers using built-in virtual keyboard.
- EndPoint Encryption is optimized for 32-bit (x86) & 64-bit (x64) systems.
- Support for hardware acceleration of AES encryption algorithm (AES_NI and PadLock).
- Deployment and management in the existing infrastructure.