

Data leak prevention, anytime, anywhere...

# Secured eFile



Protecting intellectual property and customer data are top security concerns for any business today. Whether in transit over a network or at rest on your system, encryption helps secure information, minimizing the risk of being altered or accessed by unauthorized internal and external users.

**Secured eFile** enables organizations, teams, and information workers to easily share files and folders securely with individuals and groups. Today customers, business partners, and regulators require stronger and more verifiable measures for protecting sensitive information. At the same time, data access is more distributed causing suppliers and partners to become deeply integrated into many organizations' business processes and IT infrastructures. Continuous sharing of critical data internally and externally creates new security challenges for controlling access to data. Without strong data protection, enterprises may be exposed to significant financial and intellectual property loss, legal penalties, and damage to the brand.

Through the power of the **Simple Encryption Platform**, **Secured eFile** delivers the ability to secure data for individuals and groups without the need to exchange certificates or utilize "phone-based" passwords.

## Key Features

### Simple Encryption Platform integration

The Secured eFile solution can easily be managed through the powerful **SEP Management Console**, empowering the IT Administration to manage licenses, policies, user rights and to manage and set up secure communication groups through drag and drop experience.

### Regulatory Compliance

The **Secured eFile** supports and maintains your regulatory compliance efforts. Centralized policy management is automatically enforced for the end user, ensuring that data stored in files and folders are protected. Your organization can prove that files and folders were encrypted with extensive audit reporting tools.

### Automated Password/Key management

**Secured eFile** comes with automated password/key management that eliminates the password headache for both users and IT administrators.

### Share files and folders on the network

**Secured eFile** can be used to encrypt files and folders on shared network drives where the access to the file or folder is easily decided by the end user through the secured communication group concept.

### System access protection

For enterprises that need an extra layer of security the **Secured eFile** solution offers a System access feature protecting access to the secured data.

### Intuitive workflow

The **Secured eFile** solution empowers the users to encrypt files and folders through intuitive and easy to use drag-and-drop encryption.

### Self-Extracting option

The self-extracting option creates an executable file containing the encrypted content. The recipient of the file simply double clicks on the file name and is then prompted to provide the correct password. The recipient does not need **Secured eFile** on their computer to decrypt the information.

### Share and collaborate around secured data

**Secured eFile** offers the possibility to share and work with encrypted data both internally in your organization and with external parties and customers. Internally it is possible to set up secured groups enabling end users to secure data and then share it on shared network paths, CDs, emails, USB flash drives etc. If a user needs to share data with an external contact there are 3 ways for the external contact to be able to open the encrypted file or folder.

1. The receiver of the data can download a free **Secured eFile Reader**.

2. The receiver can obtain a license and installation package. This is a good alternative for consistent collaboration. The license can be managed using **SEP's** advanced license management system.

3. The third and final way is that it is possible to create self running packages. End users can do this by right hand clicking on an encrypted file or folder and simply choosing to convert to an executable. Then the end user can place the executable on a CD, DVD, USB stick, etc. **Secured eFile** is one of the few solutions on the market where encrypted data can be opened and read from a CD or DVD.

### Automatic Data Compression

Data is automatically compressed up to 5 to 1, thereby increasing the current storage of a 1 gig drive to 5 gigs and a 4 gig drive to a 20 gig capacity

### Secured Recycle Bin

Every user expects data to be available after it has been deleted. **Secured eFile** offers a secured recycle bin located in every secured folder. The secured recycle bin travels with the folder and the user can restore deleted files located in the recycle bin. **Secured files** and folders deleted on the computer will be stored in the standard windows recycle bin secured and can be restored without any problems.

### Brute force protection

The **Secured eFile** solution has a built in brute force protection system which protects the inherent encryption methodology against professional hackers.

### Recovery password

The **Secured eFile** solution comes with a recovery password feature making it possible for business partners and clients to open encrypted files if the password is lost or forgotten.

### Security travels with files and folders

The security and access rights travel with the files and folders as users and groups choose to move or copy data from shared network paths, FTP servers desktops, laptops, servers, USB flash drives, CDs and external hard drives. A fantastic feature with the **Secured eFile** solution is that if you do a backup of the secured file or folder it will be secured on the backup itself.

### User logs

All user actions are logged and this is a perfect tool for organizations that have the need to backtrack encryption actions.

