



## SecureDoc File Encryption

Data Protection for Files, Folders and Network File Shares

- Provides an added security layer for sensitive files and folders
- Delivers fast, transparent encryption for optimized user experience
- Ensures simple, yet comprehensive key management across users and user groups



Data and files containing confidential information should be encrypted and not available elsewhere on the device”

- Office of the CISO, University of Washington

## SFE Benefits

- **Protect sensitive documents**
- **Protect personal files on a shared device or folder**
- **Keeps file usage transparent and fast**
- **Share keys with other authorized in the enterprise,** and thereby share files that are encrypted
- **Avoid business disruptions:** Decryption process does not slow your computer down since, unlike FDE, you don't have to decrypt your programs as well as your files
- **Increase protection against viruses and spyware**

SFE encrypts the individual files, and does not decrypt them until a user with the proper key and rights to view documents tries to access them.

### When a One Size Fits All approach doesn't work

When it comes to data protection, there is no one size fits all solution. Different organizations, departments, and even individuals have differing needs when it comes to protecting the information that they are responsible for. While full drive encryption sets a strong data protection foundation, file-level protection adds an additional layer of protection, often recommended as part of a defense-in-depth security strategy.

Similarly to an office building, full drive encryption ensures your doors are locked to intruders, keeping your valuables mostly secure. Should an intruder be able to somehow bypass the primary security, they'll have quick access to goods simply lying around (financials on a desk; HR documents in an unlocked cabinet; contracts in a pile of banker's boxes). Storing your valuables – your data and files – in a more secure location, and with added protections is a valuable layer of defense.

### An Added Layer of Protection

SecureDoc File Encryption (SFE) is a key component of WinMagic's SecureDoc endpoint data security software. SFE enables users and administrators to encrypt specific files and folders on a device, or on file shares within the network, and can be applied on top of a device already protected by drive encryption. While protecting devices with full drive encryption is important – and always recommended – SFE encrypted files can also reside inside a file server or Network Attached Storage (NAS) that is not encrypted. This flexibility allows you to choose how you manage your data.

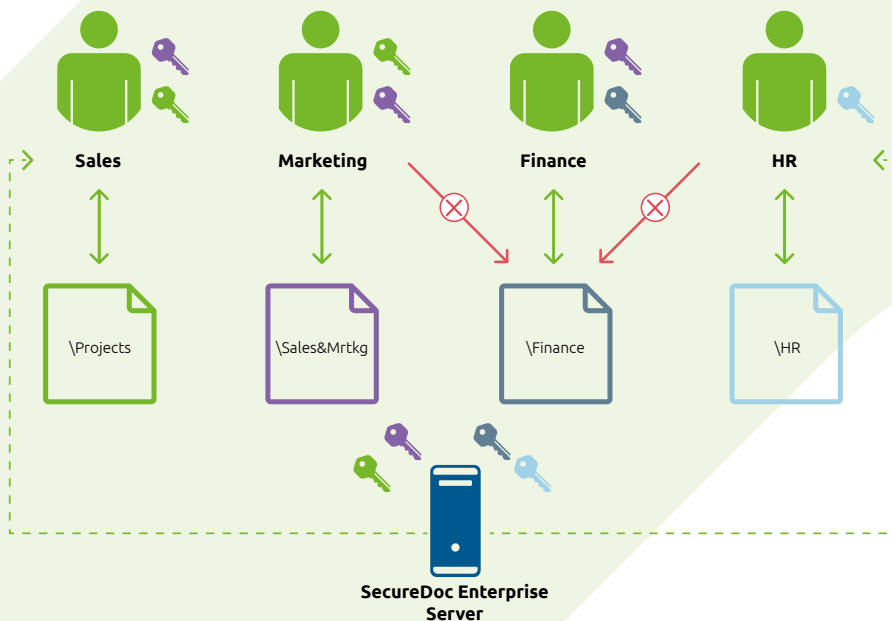
### Policy-Driven Protection

No encryption solution works properly without intelligent key management. Policy-driven rules determine which contents of an In-Policy folder will be encrypted on a file-by-file basis, and limits user access to those with the user key for the individual files. The In-Policy folder is governed by the SecureDoc File Encryption policy set by the administrator. The policy covers all folder contents, from files, to documents, to images, and even subfolders.

If an individual attempts to access a protected file – without the proper rights, they would quickly find that documents are encrypted.

For enterprises seeking to protect highly confidential documents, like a legal document surrounding an acquisition target, HR or financial files, or are simply looking to better manage internal file access in general, SecureDoc File Encryption provides the added layer of protection as part of a defense-in-depth strategy.

## How it Works



## SFE Features

- Uses AES 256-bit encryption
- Synchronizes encryption keys with SecureDoc Enterprise Server
- Permits drag & drop security for easy use
- Each device does not need to encrypt files it puts into a Network File Share
- Supports Multi-factor Authentication
- Visual file overlay icons indicating encryption status and access
- Supports all Windows 8.1 and 10 versions
- Runs in User mode vs. Kernel mode

## Deployment & Administration

Enabling SecureDoc File Encryption in the user profile lays the groundwork for SFE on the client to interact with folders managed by the SFE policies. Until the SFE functionality has been applied, the Server Administrator and users can see the contents of these files in clear text form. To apply and administer SFE, administrators need to create specific encryption keys to protect the folder contents. SFE assigns keys at a user level. User keys can be assigned at an individual level or group level, depending on the type of file being protected. In both cases, only individuals with the correct and matching key for any file, aligned to their AD credentials will be able to open and read a file in clear text. Without the matching user key, the file will remain encrypted.

For file encryption to work efficiently, individual users should also not hold responsibility for encrypting all files. Applying policy-driven protection, any clear text files added to a folder are now able to automatically be encrypted by devices (housekeeping machines), keeping your data safe and secure.

## What are the other benefits in partnering with WinMagic?



### User & Device-Based Authentication

Utilizes wired and wireless pre-boot network authentication to enforce access controls and manage end point devices before the operating system loads.

Reduces the total cost of IT ownership: Cuts password reset time by 75% and PC staging time by 75%.



### Cross-Enterprise, Multiplatform

Easy to use in multi-platform environments, supporting Windows, Mac and Linux.

Synchronizes user credentials across hardware platforms and device types.



### Cloud IaaS Encryption & Key Control

Volume and Full Drive Encryption for your virtualized and cloud workloads. All Keys to sensitive data are controlled by the enterprise, not the cloud service provider.

SecureDoc's CloudSync employs this mindset to ensure that if credentials to the cloud were ever hacked, your customer's data would be unreadable to the would-be attacker.



### BitLocker Management

SecureDoc manages BitLocker with the benefits of lower IT costs and increased IT efficiency.

SecureDoc is platform agnostic, and capable of managing Windows, macOS, Linux and any other current available operating systems, unlike MBAM.