

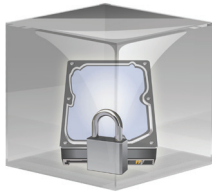


SecureFolder Enterprise

Shared folder encryption for protecting data in use

When it comes to data encryption, most enterprises protect the most vulnerable data, such as sensitive information on mobile devices, first? That's what Full Disk Encryption (FDE) solutions, such as FinallySecure Enterprise, have been developed for. Full Disk Encryption provides power-off protection by encrypting the whole drive rather than requiring the tedious effort of identifying files and folders that need to be encrypted.

Hence, it is imperative to have Full Disk Encryption as the base of your data encryption strategy.



FinallySecure Enterprise



DevicePro



SecureFolder Enterprise



ApplicationPro



CryptionPro

Why Shared Folder Encryption?

The issue with Full Disk Encryption is that it does not protect your data while the Operating System (OS) is up and running. Thus it does not provide any data-in-use (DIU) and data-in-transit (DIT) protection. That's where file and folder encryption solutions come into the picture. The problem is that most file/folder encryption solutions lack the ability to encrypt shared network folders and allow multiple users to access the encrypted folder at the same time. Other issues include lack of resizing support and the non-preservation of the file system structure.

SecureFolder Enterprise, SECUDE's enterprise-grade folder encryption solution has been built to integrate tightly into the Operating System, thus making encrypted folders - so called Safes - behave exactly like an ordinary folder in the file system. SecureFolder Enterprise supports virtualized environments (such as Citrix) and also allows for encryption of data on USB flash drives. The content of entire folders and subfolders can be encrypted and protected from unauthorized users. Thus, the directory structure is preserved to support indexing and backup. Access can be authorized for individual users or user groups in the Microsoft Active Directory. Encryption and decryption take place transparently in the background ensuring a high degree of user acceptance.

Competitive Advantages

Performance & Features

- Support for Windows Distributed File System (DFS)
- Multi-factor authentication & Smart Card Support

Management

- Full integration with Active Directory & LDAP
- Choice of web based console or windows application for management
- Flexible management through web console or API
- Ability to run in standalone mode (backend server optional)
- Seamless integration into existing Identity Management Systems (IDM)

SECUDE GmbH

Sales - Service - Solution - Center
Goebelstrasse 21
64293 Darmstadt
Germany

Tel : +49 6151 828 97 0
Fax : +49 6151 828 97 26

info@secude.com
www.secude.com





SECUDE

Specifications

Operating Systems

Windows XP (32bit)
Windows Vista (32/64bit)
Windows 7 (32/64bit)
Windows Server 2003-2008 R2 (32/64bit)
Citrix Virtual Desktop/ XenApp

LDAP Directories

Microsoft Active Directory 2003/2008
Novell
Siemens DirX
OpenLDAP
etc...

File Servers

All Windows Servers
Novell FileServer
Samba (Linux/Unix)
Netap Server

Authentication Methods

Password
Smart Card (X.509)
X.509 Certificate (PKCS#12 or Microsoft
CAPI)

Encryption Standards

AES (256bit)
RSA

Central Management

Web-based Management Console
Complete Configuration
Active Directory Integration
Reporting & Audit
Role Based
Management of Recovery Keys
LDAP Integration
API for integration into existing management
infrastructure

Related Products

FinallySecure Enterprise
DevicePro
CryptionPro
ApplicationPro

Why SecureFolder Enterprise?

Business processes are increasingly mapped electronically. This makes it essential for companies to ensure data privacy and security. SecureFolder Enterprise protects your sensitive company data with minimal impediment to the end user.

The use of SecureFolder Enterprise ensures:

- **Confidentiality:** The encryption of entire folders protects work group data on file servers.
- **Access Control:** Certificate-based authentication of group members guarantees optimal access protection for centrally stored documents.
- **User Acceptance:** Users need to authenticate themselves only once. They are then given access to all programs in the protected directories via high performance, yet transparent encryption that takes place entirely in the background.

Self-Contained Security Management

The new role-based authorization system elegantly separates the functions of system administration, security management and users. This gives SecureFolder Enterprise clear advantages over other solutions – even sensitive data can be protected effectively from system administrators! All users are securely authenticated with a password, certificates using soft tokens, smart cards, or USB tokens.

The intelligent authorization system in SecureFolder Enterprise combined with certificate-based authentication offers effective protection for security management and for users.

Flexible Administration

SecureFolder Enterprise can be centrally managed. Administering diverse authorizations for numerous employees can often consume a great deal of time and effort, particularly in large organizations. When any employee switches departments, for example, his or her access rights to sensitive data will often change as well. To ease administration, access authorization can be synchronized in a central directory service (corporate directory) in which all certificates are stored.

SecureFolder Enterprise has its own management console to manage encrypted folders centrally (Safes). The management console does not require its own user management and allows direct access of users within the Windows Active Directory Servers (ADS).

Easy Usability

The straightforward and intuitive administration of safes allows for flexible work group definition without compromising security. SecureFolder Enterprise guarantees the strictest security with user friendliness.

Use Cases for SecureFolder Enterprise

- Create encrypted Safe's used by a specific user group, such as HR, to share sensitive documents.
- Integrate encryption into unattended data processing workflows (i.e. data gets exported from an application, temporarily stored (encrypted) in a specific folder before being further processed by another application).
- Created your own encrypted Safe in your computer to protect files, such as financial reports, that should not be accessible to even administrators.

About SECUDE

SECUDE GmbH is a leading global provider of IT data protection and encryption solutions. It represents state-of-the-art security solutions developed by international organizations to provide a holistic approach to security. It not only supports you with high quality, user-friendly solutions that protect the integrity of your data, applications and transactions, but also ensures you access to your secure resources and IT systems. Thus, SECUDE also provides invaluable contribution to your organization's effort towards a growing number of regulatory compliance and industry-specific guidelines. SECUDE has offices in Europe, North America and Asia.