

Protect your valuable confidential information stored on USB drives, external hard disks, memory cards and rewritable CDs/DVDs against theft or loss with SafeGuard Data Exchange. Its strong file-based encryption secures files stored on removable media; files exchanged between removable media, PCs and PDAs*; and email attachments*.

SafeGuard Data Exchange can be configured for automation and user transparency, ensuring there is no impact on employee productivity. Its unique keyring feature enables quick, secure data sharing between project team members or across the company. In addition, a portable application offers the capability for external partners to view secured files on PCs without SafeGuard Enterprise installed.

SafeGuard Data Exchange is a functional module of SafeGuard Enterprise, a centralized solution for managing information protection in mixed IT environments. It is centrally managed by Sophos's powerful SafeGuard Management Center module.

Central management features include:

- Centralized security policies enforce consistent rules for encryption, authentication, user privileges, individuals and groups on a variety of different devices in mixed IT environments.
- Centralized key management in mixed environments enables users and administrators to easily share and recover data across groups and devices.
- Audit logs and reports guarantee compliance with internal policies and external regulations.
- Data/password recovery is compatible with standard forensic and recovery tools, minimizing help desk burden.

Deployment functionality that offers additional flexibility

Customers can also deploy encryption to the endpoints without the management center infrastructure. With both central and non-central management options available in SafeGuard Data Exchange, administrators can manage encryption in complex and diverse environments. SafeGuard Data Exchange is available as a standard MSI package for easy, automated deployment.

Benefits

Security

- Fast and transparent encryption of all storage media
- Protects data on FAT, FAT32, exFAT and NTFS file systems
- Uses the latest Advanced Encryption Standard (AES) algorithm with 256-bit keys
- Secure key derivation based on PKCS #5
- Protects against unauthorized storage and import of unencrypted data on mobile storage media
- Key backup and restore with the SafeGuard Management Center

Key benefits

Enhanced security

- » Share data across PCs, removable media, PDAs* and email easily and securely
- » Encrypts USB drives, external hard disks, memory cards, rewritable CDs/DVDs, CDs/DVD-ROMs, PDAs, e-mail attachments*
- » Strong, proven encryption algorithms

Easy to deploy and manage

- » Quick and easy to deploy via Windows Installer or standard software management systems
- » Simple, flexible administration with SafeGuard Management Center
- » Centrally enforced with configurable rules
- » Scalable from a few users to a complete company-wide rollout

Easy to use

- » Transparent background encryption
- » Option to combine encrypted and non-encrypted files on the same storage medium for both fixed and removable media
- » Automatic selection of security rules based on media type
- » Simple, intuitive user interface requires minimal user training
- » Encrypted data can be securely read and modified even on PCs that do not have SafeGuard Enterprise installed
- » User-friendly names for encryption keys

Email and PDA encryption with SafeGuard PrivateCrypto

- SafeGuard PrivateCrypto bundled with the SafeGuard Data Exchange module
- Windows Explorer users: simply right-click on files to encrypt, or encrypt and send as email attachments with Microsoft Outlook, Outlook Express, Lotus Notes and other email clients
- Integrates with SafeGuard Data Exchange's centralized key management, including user keyrings, enabling data sharing and recovery
- Encrypts all types of files
- Option to create self-extracting encrypted files

Greater productivity and ease of use

- Keyring allows sharing of encrypted media between organizational units
- Option for automatic encryption without user intervention
- High level of user acceptance with no additional training or disruption to workflow
- Encrypted files on removable media can be read using the portable application on PCs where SafeGuard Enterprise is not installed; consistent, strong password rules and failed logon delays also available for portable functionality; media passphrase option provides single sign-on to access all files, even when offline, regardless of the key that was used to encrypt the files
- Overlay icon for easy view of encrypted files
- Works consistently in read-write mode across all supported Windows platforms—ideal for heterogeneous environment

Powerful central administration

- Connections to existing directories and domains
- Centrally enforced encryption rules
- Devices that have not communicated with the management center at specified intervals can be blocked or locked down via policy while online, protecting against loss and theft
- Communication with the SafeGuard Management Center via advanced XML/SOAP protocols
- Deployment options offer flexibility to organizations with centrally managed and non-centrally managed users
- Central backup/restore of SafeGuard Enterprise keyring (via API for standalone deployments only)

Easy, centrally managed installation

- Installation packages can be distributed and installed centrally and unattended via standard MSI packages
- Easy rollout over a network—without involving users

* Successfully tested on Windows 7 Release Candidate. Windows 7 final version will be supported in the next release. 64-bit support will be available in the next release.

System requirements

Operating systems (32 bit)¹

- » Microsoft Windows XP (SP 2, SP 3)
- » Microsoft Windows Vista™ (SP 1, SP 2)

Certifications

- » FIPS 140-2

Standards and protocols

- » Symmetrical encryption: AES 128/256 bit
- » Asymmetrical encryption: RSA
- » Hash functions: SHA-256, SHA-512
- » Passwords, padding, PKCS #1, PKCS #5
- » Smartcard/token: PKCS #15, PKCS #11, Microsoft Cryptographic Service Provider (CSP), PC/SC, Kerberos
- » PKI: PKCS #7, PKCS #12, X.509 certificates
- » Data transfer: SOAP, XML, SSL, LDAP

Supported hardware

- » PC with Intel Pentium or compatible processor
- » Supported storage media:
- » Memory cards including CFC, SDC, MMC, SMC, etc.
- » USB memory sticks and hard drives
- » FireWire hard drives
- » CD/DVD-RW
- » Floppy, ZIP, Jazz drives
- » All devices recognized by the OS as storage media