

Data Exchange module

Encrypt and 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. Securely share data with team members, business partners and customers. Encrypt files on removable media; files exchanged between removable media, PCs and email attachments¹.

SafeGuard Data Exchange is a functional module of SafeGuard Enterprise—a centralized solution for managing data security in mixed IT environments. Its clients can be managed from the SafeGuard Management Center, keys and certificates can be centrally backed up and administrators can log user activities and create reports.

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
- Audit logs and reports guarantee compliance with internal policies and external regulations
- Centralized key management in mixed environments enables users and administrators to easily share and recover data across groups and devices
- Data/password recovery is compatible with standard forensic and recovery tools, minimizing help desk burden

Secure data sharing and ease of use

- SafeGuard key ring enables transparent sharing of encrypted media between organizational units
- Automatic and transparent 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 are 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
- Mix encrypted and non-encrypted files on the same media
- Simple, intuitive user interface requires minimal user training. User-friendly names for encryption keys. Overlay icon for easy view of encrypted files
- Works consistently in read-write mode across all supported Windows platforms—ideal for heterogeneous environment

Key benefits

- » Fast and transparent encryption of many types of storage media - USB drives, external hard disks, memory cards, rewritable CDs/DVDs, CDs/DVD-ROMs, e-mail attachments¹
- » Protects data on multiple file systems including FAT, FAT32, exFAT, NTFS, CDFS, Joliet
- » Uses the latest Advanced Encryption Standard (AES) algorithm with 256-bit keys
- » Secure key derivation according to PKCS #5
- » Protects against unauthorized storage and import of unencrypted data on mobile storage media
- » Automatic selection of security policies based on media type
- » Key backup and restore with the SafeGuard Management Center

¹With SafeGuard PrivateCrypto

Email encryption with SafeGuard PrivateCrypto

SafeGuard PrivateCrypto is a file encryption and utility that is 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 key rings, enabling data sharing and recovery
- Encrypts all types of files
- Option to create self-extracting encrypted files

Powerful central administration²

- 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. Central backup/restore of SafeGuard Enterprise key ring
- User/computer information imported via integration with directory services e.g., Microsoft Active Directory®
- Efficient data/password recovery minimizing help desk burden
- Detailed logs to monitor compliance
- Devices that have not communicated with the management center at specified intervals can be blocked or locked down via policy while online
- Communication with SafeGuard Management Center² via advanced XML/SOAP protocols

Easy, centrally managed deployments

- Installation packages can be distributed and installed centrally and unattended via standard MSI packages
- Easy rollout over a network—user involvement not required
- Scalable from a few users to a complete company-wide rollout

Non-centrally managed deployments

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.

² The SafeGuard Enterprise Management Center module is required for central administration. For more information visit:

<http://www.sophos.com/products/enterprise/encryption/safeguard-enterprise/management-center/>

System requirements

Operating systems

- » Microsoft Windows 7 (32 and 64 bit)
- » Microsoft Windows Vista (32 and 64 bit; SP 1, SP 2)
- » Microsoft Windows XP (32 bit; SP 2, SP 3)

Certifications

- » Uses FIPS 140-2 validated SafeGuard Cryptographic Engine

Standards and protocols

- » Symmetrical encryption: AES 128/256 bit
- » Asymmetrical encryption: RSA
- » Hash functions: SHA-256, SHA-512
- » Password hashing: PKCS #5
- » 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