

Prevent unauthorized access to mobile and stationary endpoint devices by encrypting fixed and external hard disks and removable media easily and transparently with SafeGuard Device Encryption. If a device falls into the wrong hands, the data is unreadable even if the hard disk is removed.

SafeGuard Device Encryption is a 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.

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 offers additional flexibility

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

Benefits

- Unmatched data security
- Protects data on laptops and desktops
- Proven encryption algorithms maximize security and performance
- Suspend-to-disk and hibernation files are encrypted for maximum security

Easy to use

- User-transparent background encryption
- Secure password recovery via phone or web
- Single sign-on to the operating system
- Customized graphical pre-boot login screen
- Biometric fingerprint authentication at pre-boot and Windows logon is possible

Key benefits

Strong, transparent encryption

- » Extensive transparent encryption functionality
- » Full hard disk encryption (NTFS, FAT)
- » Multi-platform removable media encryption
- » Strong, internationally recognized encryption algorithms
- » Secure, encrypted hibernation
- » TPM chip used for random number generation
- » Encrypted data cannot be read even if hard drives are removed from PCs, except by security administrators

Secure user authentication and authorization

- » Pre-boot user authentication via password, cryptographic token or smartcard, or biometrics (single sign-on, keyring access, desktop lock actions supported with tokens/smartcards)
- » Centrally defined, enforced password rules
- » Log-on process prevents password penetration attacks

Greater productivity and ease of use

- » Single sign-on to the operating system
- » Keyring allows for easy sharing of encrypted media within teams
- » High-speed encryption/decryption algorithms ensure no performance degradation
- » Transparent background encryption ensures no work interruptions
- » Challenge/response feature recovers forgotten passwords over phone or web, including web self-help

Keyring secures teamwork

- Secure sharing of encrypted data
- Only authorized users can access the data wherever it is stored
- Facilitates data recovery by administrators

Powerful central control

- Central administration with logs and reports to monitor compliance
- Centrally managed, unattended installations with no user interruptions
- Integration with directory services via LDAP: Microsoft Active Directory®; supports Novell environments
- Grows with your needs with additional SafeGuard Enterprise modules
- SafeGuard Easy customers can easily migrate to SafeGuard Enterprise

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
- Communication with SafeGuard Management Center via advanced XML/SOAP protocols
- Secure Wake-On-LAN allows automated administrative activities (e.g., patch management)
- Deployment options offer flexibility to organizations with centrally managed and non-centrally managed users

¹Successfully 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 2000 (SP 4)
- » Microsoft Windows XP (SP 2, SP 3)
- » Microsoft Windows Vista™ (SP 1, SP 2)

Certifications

- » FIPS 140-2
- » Common Criteria EAL 4 (pending)
- » Aladdin eToken enabled

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

Language Versions

- » English, French, German, Hungarian, Italian, Japanese, Spanish
- » Unicode-based support for other languages

Support for Data Recovery, Imaging and Forensics

- » Lenovo® Rescue and Recovery: secure recovery of encrypted operating systems and data
- » Windows PE 2.0 (recovery operating system)
- » Ready for EnCase (Guidance Software), AccessData and Kroll Ontrack
- » Microsoft Business Desktop Deployment

Multi-Platform Support

- » Multi-platform key management and authentication

For full details, visit www.sophos.com