

Device Encryption module

Prevent unauthorized access to laptops and desktops with full disk encryption that is transparent and easy to use. If a SafeGuard encrypted PC 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. (Please refer to the SafeGuard Enterprise Management Center datasheet for information on central management.

Strong, transparent encryption

- Extensive transparent encryption functionality
- Full hard disk encryption (NTFS, FAT, FAT32)
- Strong, standardized encryption algorithms
- Secure, encrypted hibernation
- Encrypted data cannot be read even if hard drives are removed from PCs, except by security administrators
- High-speed encryption/decryption algorithms

Secure power-on 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*
- Single sign-on to the operating system
- Centrally defined, enforced password rules
- Multi-user pre-boot environment with audit trails
- Dynamic addition/removal of registered users from the pre-boot environment via policy updates
- Hardened log-on process, which prevents password penetration attacks
- User-friendly graphical pre-boot login screen that is customizable
- Service accounts allow administrators to securely access PCs while end users retain ownership

Key benefits

- » Unmatched data security with proven encryption algorithms, which maximizes security and performance
- » Encryption of swap and hibernation files for complete security
- » User-transparent background encryption, which ensures work without interruptions
- » Higher end-user productivity with secure password recovery via phone or the local self-help option
- » Convenience and speed for end users with single sign-on to the operating system from the pre-boot stage
- » User-friendly graphical pre-boot login screen that is customizable
- » Stronger security with biometric fingerprint authentication at pre-boot; tokens and smartcards also supported
- » Broad, comprehensive data security when deployed in conjunction with the other SafeGuard Enterprise modules

* Please refer to the SafeGuard Enterprise Technical White Paper for a detailed list of supported smartcards, tokens and biometrics (Lenovo fingerprint readers supported).

Secure recovery of passwords, data and forensics

- Challenge/response over the phone with the help desk for recovery of forgotten passwords
- Local self-help to recover forgotten passwords during pre-boot without calling the help desk or the need for an internet connection
- Secure and quick access to encrypted disks on other systems for emergency data access or recovery with automated key reassignments enabled by SafeGuard keyring management
- External boot option with Windows PE (e.g., for recovering broken operating system configurations on encrypted disks)
- Ready for EnCase (Guidance Software), AccessData and Kroll Ontrack (access requires user or administrator cooperation)
- Support for Microsoft Business Desktop Deployment and Computrace
- Integration with Lenovo Rescue and Recovery for secure recovery of encrypted operating systems and data

Centralized administration

- Centrally enforced encryption policies
- User/computer information imported via integration with directory services (e.g., Microsoft Active Directory)
- 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 Center via advanced XML/SOAP protocols
- Automated administrative activities (e.g., patch management) enabled by Secure Wake-On-LAN
- Centralized key management for data recovery and sharing

(The SafeGuard Enterprise Management Center module is required for central administration. Please refer to its datasheet.)

Easy, centrally managed installation

- Installation packages can be distributed and installed centrally and unattended via standard MSI packages.
- Network rollout is easy—user involvement is not required.

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 cryptography
- » Common Criteria EAL-3+
- » Aladdin eToken enabled

Standards and protocols

- » Symmetrical encryption: AES 128/256 bit
- » Asymmetrical encryption: RSA
- » Hash functions: SHA-256, SHA-512
- » Password hashing: PKCS #5, PKCS #12
- » 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, Italian, Japanese, Spanish
- » Unicode-based support for other languages

For full details, visit www.sophos.com