

# SafeGuard® Device Encryption

Strong Data Security for Laptops and Desktops

Datasheet



## Protect your information investment and minimize your risk of data loss with SafeGuard Device Encryption

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 Utimaco's powerful SafeGuard Management Center.

### Central management features include:

- Centralized security policies enforce consistent rules for encryption, authentication, user privileges, or for individuals and groups, on a variety of different devices in mixed IT environments.
- Centralized key management in mixed environments allows 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 helpdesk burden.

### Deployment functionality that 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.

### SafeGuard Enterprise – Your Central Key to Information Protection

## About Utimaco – The Data Security Company.

Utimaco is a leading global provider of data security solutions, enabling mid-to large-size organizations to safeguard their data assets against intentional or accidental data loss, and to comply with privacy laws. Utimaco's complete range of data security solutions provide full 360 degree data protection for data at rest, data in motion and data in use. Utimaco offers its customers comprehensive on-site support via a world-wide network of certified partners and subsidiaries. Utimaco Safeware AG, with headquarters in Oberursel, near Frankfurt, Germany, is listed on the Frankfurt Stock Exchange (ISIN DE0007572406). For more information please visit [www.utimaco.com](http://www.utimaco.com)

## Benefits

### Unmatched data security

- Protects data on laptops and desktops
- Proven encryption algorithms to 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

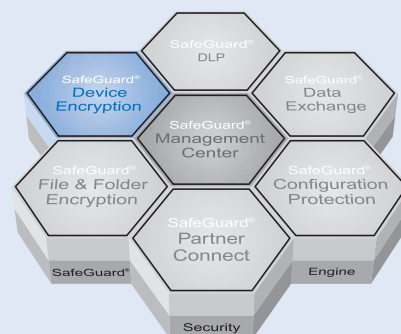
### Keying secures teamwork

- 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 now easily migrate to SafeGuard Enterprise

## SafeGuard® Enterprise



### SafeGuard Device Encryption

is a module of **SafeGuard Enterprise** – a centralized solution for managing data security in mixed IT environments.

**utimaco**<sup>®</sup>  
safe ware

a member of the Sophos Group

# SafeGuard® Device Encryption

## System Requirements

### Operating systems

- Microsoft Windows 2000 (Service Pack 4)
- Microsoft Windows XP (Service Pack 2, Service Pack 3)
- Microsoft Windows Vista™ (Service Pack 1)

### 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
- Data transfer: SOAP, XML, SSL, LDAP

### Language versions

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

### Support for Data Recovery, Imaging and Forensics

- Lenovo® Rescue & 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

- Protects laptops and desktops
  - In combination with SafeGuard Data Exchange also data stored on removable media including USB sticks, memory cards, CDs/DVDs can be protected
- Multi-platform key management and authentication

### Multi-factor authentication: Supported Tokens and Smartcards

- Biometric fingerprint logon:
  - Support for pre-boot and Windows logons. Password/UID is optional
  - Supports Lenovo laptops/desktops with UPEK companion chip or Authentec fingerprint readers
- Supported smartcards, readers, tokens: (Windows XP via PC/SC, PKCS #11, CSP)
  - Smartcards: ActivIdentity®, Siemens, Giesecke & Devrient, Gemalto .NET
  - Tokens: Aladdin® eToken, RSA® SID800, Vasco DIGIPASS 860
  - Smartcard readers: SCM, Gemalto, Omnikey, Kobil mldentity, Axalto Reflex 20V3 PCMCIA
  - Keyboards with integrated smartcard readers from Cherry, Dell®, HP, etc.

For a full list of supported tokens, smartcards and readers please contact your Utimaco representative.

## Key Features/Functionality

### Strong transparent encryption

- Extensive transparent encryption functionality
  - Full hard disk encryption (e.g., 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
- 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 recover forgotten passwords over phone or web, including web self-help

### 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 on-line
- Communication with SafeGuard Management Center via advanced XML/SOAP protocols
- Secure "Wake on LAN" to allow automated administrative activities, e.g., patch management
- Deployment options offer flexibility to organizations with centrally managed and non-centrally managed users

### Easy, centrally managed installation

- Standard MSI installation packages can be distributed from a central source for unattended installations
- Easy roll-out over a network – without involving users

### Logging and reporting

- All client activities/status and security events are logged and stored locally and centrally. Type of logs and storage location are user-defined
- Administrators can filter, view and print log reports on the Management Center console
- Optional standalone "SGNState" tool reports encryption status to external consoles (e.g. LANDesk or Network Access Control (NAC) solutions)

### Unleash the power of SafeGuard Enterprise and migrate your PCs from SafeGuard Easy

- SafeGuard Easy customers can now seamlessly migrate to SafeGuard Enterprise easily via the SafeGuard Device Encryption module.

### Further information

- For more information about Utimaco Safeware and our complete line of SafeGuard solutions, visit: [www.utimaco.com](http://www.utimaco.com). To learn more about all of the modules that comprise SafeGuard Enterprise, visit [www.utimaco.com/sgn](http://www.utimaco.com/sgn)

### Utimaco Safeware Partner:

#### Copyright Information

© 2006-2008 – Utimaco Safeware AG  
SafeGuard® Device Encryption version 5.35

All SafeGuard products are registered trademarks of Utimaco Safeware AG. All other named trademarks are trademarks of the particular copyright holder. Individual functions may have different characteristics according to the different capabilities of the operating systems.



a member of the Sophos Group

[www.utimaco.com](http://www.utimaco.com)

#### EMEA

Utimaco Safeware AG  
Hohemarkstrasse 22  
DE-61440 Oberursel  
Germany  
Phone +49 (61 71) 88-14 44  
info@utimaco.com

#### NORTH & SOUTH AMERICA

Utimaco Safeware Inc.  
10 Lincoln Road  
Foxboro, MA 02035  
USA  
Phone +1 (508) 543-10 08  
sales.us@utimaco.com

#### ASIA PACIFIC

Utimaco Safeware Asia Ltd.  
Unit 602, Stanhope House  
734 King's Road, Quarry  
Bay  
Hong Kong  
Phone +852 25 20 26 08  
info@utimaco-asia.com