



lenovo®

SecureDoc™ for Lenovo

The Leading Disk Encryption Management Platform for Lenovo Notebooks that Supports Heterogeneous IT Environments

SecureDoc™ is the only solution that truly protects your investment in full disk encryption by supporting emerging technologies such as Intel® Anti Theft and Self-Encrypting Disks already today. The exclusive SecureDoc™ for Lenovo product makes active use of Lenovo's leading ThinkVantage technologies, while being able to integrate additional platforms such as other Windows, Mac OS or Linux endpoints.

Overview

WinMagic is a vendor totally focused on providing the best encryption technology – and this is exactly what you can expect from us. The exclusive SecureDoc™ for Lenovo disk encryption software package allows you to protect and seamlessly manage Windows, Mac OS and Linux clients alike. This enterprise-ready disk encryption solution will not only encrypt your PCs, but also protect your removable media including CD/DVDs, USB thumb drives and SD cards. Lenovo has selected SecureDoc™ as its preferred encryption solution for securing data on laptops – SecureDoc™ for Lenovo is the only solution available that supports the different ThinkVantage technologies such as Biometric Readers, Rescue & Recovery and Hardware Password Manager. SecureDoc™ is an important building block in your efforts to comply with the many privacy and security regulations while meeting the highest security standards confirmed by our FIPS 140-2 Level 2 and Common Criteria EAL-4 certifications. Deploy SecureDoc™ today and be prepared to fully take advantage of new data security technologies entering the enterprise including the activation and management of Opal compliant self-encrypting drives and Intel® Anti Theft Technology.

Key features SecureDoc™ for Lenovo Client:

- Full Disk and File Folder Encryption
- Removable Media Encryption
- Portable and secure USB encryption (no additional software installation or admin access rights required)
- Windows (including Windows 7 64 bit), Mac OS and Linux support
- OPAL Self Encrypting Drives (SED) support
- Support for Lenovo Rescue and Recovery
- Support for built-in UPEK fingerprint sensor for pre-boot authentication
- Support for Hardware Password Manager (January 2011)
- Support for Intel® Anti Theft Technology
- Multi-Language Client available in :
 - o English, Japanese, French, Italian, German, Spanish



WINMAGIC®
DATA SECURITY

Knowing You're Protected



NIST



The Solution

SecureDoc for Lenovo is a scalable Full-Disk Encryption (FDE) software solution that ensures sensitive information stored on laptops across the enterprise are protected against theft and unauthorized access. SecureDoc Pre-boot authentication (PBA) offers single or multiple factor pre-boot authentication methodologies including password, smartcards, popular USB tokens, biometrics, TPM, and PKI. SecureDoc Enterprise Server (SES) functions as a robust and reliable key management system for all your endpoints (running on Windows, Mac OS, Linux), providing a secure central repository for all encryption keys used to protect hard drives, laptops, removable media and other encrypted endpoints.

Key features SecureDoc™ for Lenovo Enterprise Server:

- Support of Windows, Mac OS and Linux clients
- Encryption Key Management
- Dynamic Key Provisioning
- Synchronization with Active Directory
- Password Rules
- Password Recovery Tools (Password Hint, Self Help, Challenge Response)
- Key Labelling
- Auditing capabilities
- Policy based encryption rules
- Easy deployment of client packages through LANDesk, Tivoli, SMS
- Support for Hardware Password Manager (January 2011)



Advantages of Opal Compliant Self-Encrypting Drives (SEDs)

Opal self-encrypting drives are an easy and effective way to deliver a high level of security for digital information.

Key advantages of SEDs are:

- *Quick and easy deployment:* SEDs utilize their own AES encryption, which is utilized by SecureDoc. This allows SEDs to avoid an initial conversion process usually needed to encrypt "normal" hard drives (immediate protection). The in-line encryption algorithm reduces to the hard drive degradation overhead to a negligible amount.
- *Zero performance degradation:* SEDs use their own hardware for encryption, so computing systems do not suffer performance issues (no system processor usage or time delay overhead).
- *Highest Level of Security:* The data encryption key does not leave the drive, hence preventing cooled-RAM attacks and simplifying key management.
- Read Only Pre-Boot Authentication (PBA) area supports single or multi-factor authentication by SecureDoc using drive's secure partition.
- Crypto erase enables instant secure disposal and repurposing of self encrypting-drive, rendering all existing data unintelligible.
- *Transparency and flexibility:* The Master Boot Record (MBR) is not modified, therefore no kernel driver needed and no conflicts with other software.

Advantages of Intel® Anti Theft Technology (Intel AT)

The new generation of notebook PCs with Intel vPro technology include Intel AT Technology. SecureDoc for Lenovo can enable Intel AT to issue a "poison pill" to the notebook should it be identified as lost or stolen. The poison pill will perform a platform disable rendering the laptop's hardware inoperable, and conduct an Encryption Data Disable to lock out the user, even if the individual attempting to login possesses the correct pre-boot authentication credentials. Encryption Data Disable is the recoverable alternative to Remote Crypto Erase since the outcome of the latter is irreversible. Intel's value-add non-destructive platform disable services can be triggered by:

- Excessive end-user attempts at logging into system (number of allowed attempts configurable);
- Laptop missing rendezvous time with the server, thereby issuing a local poison pill;
- A poison pill being issued by the system administrator to the laptop identified as stolen via internet, intranet or 3G.

These methods of PC disablement are non-destructive and can be easily and quickly reversed without harming the platform or affecting the data.



WINMAGIC
DATA SECURITY

WinMagic's SecureDoc full-disk encryption solutions make it simple to protect all data on desktops, laptops, tablets and removable media including USB thumb drives, CD/DVDs, and SD Cards. Compatible with Microsoft Windows 7, Vista, XP, and 2000 as well as Mac and Linux platforms, SecureDoc makes it just as easy to centrally manage and use an encrypted device as an unencrypted device including Seagate and Opal self-encrypting drives. WinMagic is trusted by thousands of enterprises and government organizations worldwide to minimize business risks, meet privacy/regulatory compliance requirements, and protect valuable information assets against unauthorized access. With a full complement of professional and customer services, WinMagic supports over three million SecureDoc users in approximately 43 countries. For more information, please visit www.winmagic.com, call 1-888-879-5879 or e-mail us at info@winmagic.com.