



SecureDoc™ - Enterprise Ready Disk Encryption

*Comprehensive Encryption For All Of Your
Data-At-Rest Security Needs*

WinMagic's SecureDoc facilitates greater synergies in Assets and Data protection together with Seagate Secure™ and Intel® Anti-Theft Technology



Advantages of Seagate Self-Encrypting Drives

Seagate self-encrypting drives are an easy and effective way to deliver a high level of security for digital information. Hard drives featuring Seagate Secure™ technology combine capacity, reliability and comprehensive security capabilities to provide powerful data protection.

Key Advantages:

Zero performance degradation: Seagate self-encrypting drives use their own hardware for encryption, so the user does not suffer performance issues as with software encryption. There is no system processor usage or time delay overhead.

Highest Level of Security:

- Data encryption key does not leave the drive, which helps prevent cooled-RAM attack and simplifies key management.
- Read Only Pre-Boot Authentication (PBA) area supports multi-factor authentication by Independent Software Vendors (ISV) 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: At power-up, when authentication takes place in pre-boot, user enters authentication credentials for the drive to verify. If authentication is successful, the drive retrieves original MBR (Master Boot Record) to load whatever OS has been stored on the drive. Therefore, the MBR is not modified and no kernel driver is needed resulting in 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® Anti-Theft Technology. Intel® AT offers the option of activating hardware-based client-side intelligence to secure the PC and/or data if a notebook is lost or stolen. Intel's non-destructive platform disable capability can be triggered by:

- Hardware timer expiring – Intel AT hardware-based timers help identify unauthorized access to the system.
- Local & remote poison pill (via LAN/WLAN and Broadband Technologies) - Renders the PC inoperable by blocking the OS from booting and minimizes the potential of a stolen notebook being used.
- Local & remote platform reactivation through Intel AT rapid reactivation mechanisms.



WINMAGIC®
DATA SECURITY

Knowing You're Protected



WinMagic's SecureDoc Solution

WinMagic develops scalable Full Disk Encryption (FDE) software solutions that ensure sensitive information stored on laptops across the enterprise are protected against theft and unauthorized access. In providing strong pre-boot authentication, SecureDoc offers one integrated management console to manage Intel AT technology embedded on PC clients while supporting the heterogeneous components of these clients including self-encrypting drives, removable media, and utilities like password recovery tools. SecureDoc disk encryption provides a complete comprehensive solution for securing data-at-rest on laptops. SecureDoc key features include:

SecureDoc Enterprise Server (SES):

- Robust and reliable encryption key management system
- Secure central repository for all encryption keys used to protect hard drives
- Key Labeling
- Dynamic Key Provisioning
- Synchronization with Active Directory
- Password Rules
- Password Recovery
- Auditing Capabilities
- Configure, deploy and manage Windows and Mac clients under one management console

SecureDoc Client:

- Support of self-encrypting drives: Seagate and Opal drives
- Pre-boot authentication (PBA): Single and multiple factor authentication, including password, smartcards, popular USB tokens, biometrics, TPM, and PKI
- Removable Media Encryption (USB thumb drive; CD/DVD)
- Password Recovery Tools (Password Hint, Self Help, Challenge Response)

Advantages of Intel AT combined with WinMagic's SecureDoc:

WinMagic's SecureDoc leverages the best of Intel AT under one enterprise management console. Delivering a superior notebook security solution that brings together the combined benefits of Intel AT and SecureDoc. Hence, one server management console that handles data-at-rest encryption in a heterogeneous fashion including notebooks embedded with Intel AT. Key advantages of the synergies include:

- Intel hardware-based theft deterrence capabilities: Substantial security, manageability and interoperability benefits including FDE, rich PBA with multi-factor authentication.
- Encrypted Data Access Disable: Disable user access to data in a non-destructive manner from SecureDoc Enterprise Server (SES). Even if the user (for example, a terminated employee) still has valid credentials and moves the drive to another machine, the user will not be able to access the data.
- System admin can restore users' access to data remotely. It is a simple and inexpensive way to restore notebook or PC to full functionality. Encryption Data Disable is a recoverable alternative to remote crypto erase since its outcome is irreversible.
- Secure storage of crypto secret that binds the data to the platform.



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.