

Comprehensive protection of your data made easy under one umbrella

Easily deploy, maintain and manage your data security protection transparently



SecureDoc™ is a full-disk encryption solution that is easily configures, deploys and manages your end user security profiles, and associated policies, across PC, Mac and Linux platforms taking advantage of new security technologies entering your enterprise like Opal compliant self-encrypting drives and Intel® Anti-Theft technology. Our pre-boot authentication environment allows for single or multiple factor authentication including password, smartcard, USB token, biometrics, PKI or TPM. Our SecureDoc Enterprise Server (SES) possesses a security policy manager, user / group management system, key management system, user support tools, software distribution tool support and a consolidated audit log.

SecureDoc Enterprise Version – Easy to Configure, Deploy and Manage for enterprise wide deployment of SecureDoc

- Central administration support, allows “silent” installation; in other words, SecureDoc on PC, Mac and Linux clients is installed through the network without any administration on the client machines. Therefore, it is installed quickly and easily, without user intervention, on all client computers.
- Support of both software and hardware based AES encryption for hard drives including Opal compliant hard drives
- Active Directory (AD) user data can be synchronized partially and fully. This increases flexibility and control for administrators. User data can include customized fields; in addition, it can be grouped into folders for easier access, and folders can be assigned to specific administrators for individualized control.
- Access to audit logs is available via the World Wide Web. SES can display audit log history for objects including folders, computers, users, key, packages, and the SES recycling bin. This increases the amount of tracking capability within the system for improved accountability and audit purposes.
- Capacity to bring standalone machines under management of SES, simply by running a new SES package on the client machine. It speeds and simplifies the enterprise deployment process in cases where standalone clients have been deployed earlier.

Extensive Key Management Tools

- Provides centralized management of users, computers, keys and Key files. With SecureDoc, it is easy to create, modify, assign, delete and import keys from files and tokens.
- Facilitates an Account-Based Key Management (WKM) system that makes greater use of the user’s Windows account and permits alternate users to log in to a running, encrypted computer at the Windows Login. SecureDoc can seamlessly disconnect from the previously-logged-in user’s key file, then authenticates to the key file of the newly-logged-on user, completely eliminating the need to reboot the computer to change users.
- Controls client computers remotely, including rebooting or locking them. For example, it can automatically lock out users when no connection to a server surpasses a specified period of time.
- Ensures transactions stored in audit log on client computers can be automatically and securely sent to a central location.



SecureDoc Trusted by the most security-conscious organizations worldwide

- No back door. All recovery features are governed and controlled by your organization, not by WinMagic. Source code validation by third parties and by different governments ensures that no back door exists.
- Conversion tolerates interruption. The initial conversion (to encrypt all sectors of the disk) can tolerate interruption, i.e., power outage without data loss
- User can work with the computer while the conversion takes place in the background.
- Fast conversion. SecureDoc typically converts approximately 30 Gigabytes per hour on a 1.8 GHz Pentium desktop. No noticeable performance loss for encrypted disks.
- Decryption (conversion back to plain text) is possible. This privilege is reserved for administrators only.
- An unlimited number of users can be issued individual key files to access a single computer.
- Supports popular Tablet PCs.
- Compatible with disk defragmentation software, even the Windows built-in utility.
- Compatible with disk imaging software such as Ghost, Drive Image (image and compress encrypted disks) and Rapid Restore (disk and images are always encrypted on the PC).
- Works seamlessly with boot manager utilities such as BootMagic or System Commander.
- Supports different SCSI, RAID controllers, e.g. for servers.
- Disk-lock precludes unauthorized copying of data to floppy disk or other removable drives. Configurable to allow access to only encrypted removable media.
- Fully customizable text and color screen at boot logon. Users can choose the language, text and color (foreground/background) of their preference.
- Comprehensive audit log system that increases the amount of tracking capability within the system for improved accountability and audit purposes.
- Lock/Unlock users at boot time for SecureDoc users, and lock laptops on failed login attempts.
- Support for visually challenged users.
- Unicode Support, English, Japanese, French, Italian, German and Spanish.
- Encryption Header allows more flexibility for sharing encrypted objects. It supports encryption through SecureDoc Key file, with added capabilities such as passwords, or with a supported smart card without key files.
- Increased Hard Drive Support. SecureDoc supports an unlimited number of hard drives and encrypted objects. There is also an increase in disk size support to greater than 2 terabytes (2000 Gigabytes).
- The recovery information for each machine is securely transmitted for storage within the SES server before conversion (encryption) is even completed. The benefit of this is that if the machine is unable to communicate after the first reboot, the user forgets the password or is unable to login to the machine for other reasons, the data on the machine is still recoverable after the first reboot.
- Easier to track down and purge any abandoned devices in the system (i.e. laptops that have been decommissioned, etc.). This enables administrators to free up user licenses for re-use elsewhere in the organization.
- Single client platform that will handle iKey and all other Tokens. This will yield substantial administrative improvements to customers using both iKey and non-iKey tokens for authentication.
- Hosting services ensure that profiles, installation packages and global options within SES console are categorized that enable different companies or regions to be easily organized in different folders in the SES console.
- SecureDoc allows the option of labelling keys utilized for encryption. This feature results in the ability to share access of encrypted objects in a very flexible way. It offers customization such as specifying precisely which user or group of users can or cannot access an encrypted hard disk, floppy disk or other removable disks.
- Support for USB trusted devices like Seagate's Black Armor, IronKey, Sandisk, Kingston, etc. to provide secure & seamless protection for mobile data
- Users can be configured to sign into Windows operating system with only one password. SecureDoc locks computer if the token is removed.
- PIV/CAC card support under Mac Snow Leopard (Mac OS 10.6.x)
- Password expiry and enforcement policies for Mac support.
- Apple's Migration Assistant support, allows migration of data from an encrypted Mac client to non-encrypted Mac client's machine or vice versa.
- Administrators can deploy customized packages to the enterprise. For instance, RME-only packages that encrypt removable media inserted into Mac clients, not the client hard drive. Also, flexibility for administrators to decide whether to provide users with the option to select software or hardware encryption for self-encrypting drives.
- Many more features such as Secure-Wipe, Key File on Token, Automated Token Set-up Wizard, Self-help Key File Recovery, Multi-Processor Support, Auto-Boot Support, and International Keyboard Support



Product Matrix

SecureDoc Products

SecureDoc Full Disk Encryption (FDE)	Protects data-at-rest on the hard drives of desktop and laptop computers.
SecureDoc Enterprise Server	Provides enterprise-class centralized administration and management for SecureDoc-encrypted laptops, desktops and other endpoints.
SecureDoc File Folder Encryption (FFE)	Individual folders and/or files within an encrypted hard drive can be encrypted with their own access rights and restrictions.
SecureDoc Container Encryption	Layered security option, allowing the creation of encrypted sections on hard drives (encrypted or not) and/or removable media. This supports a 'defense in depth' of sensitive data, and offers more granular control over access to the data.
SecureDoc Self Extractor Encryption	Allows you to securely share data with third parties who do not have SecureDoc.
SecureDoc Removable Media Encryption (RME)	Protects sensitive data on CDs, DVDs, USB drives and other removable media by fully encrypting these media on a sector-by-sector basis.
SecureDoc Mobile Edition	Encrypts automatically and transparently data on PDA, Flash Cards, SD Cards and other removable media with no degradation in performance.
SecureDoc for Linux	Protects data-at-rest on the hard drives of Linux desktop and laptop computers.
SecureDoc for Mac	Protects data-at-rest on the hard drives of Mac desktop and laptop computers.

SecureDoc Supported Devices, Operating Systems and External Media

Windows OS, Mobile, and Enterprise Platforms (32 and 64 bit)

Microsoft Windows 7/Vista/XP	Yes
Microsoft Windows 2003, 2000 R2 Standard and Enterprise	Yes
Windows Mobile 5.0	Yes

Linux OS and Enterprise Platforms (32-bit)

OpenSUSE 10.2, 11.0, 11.1	Yes
RedHat Enterprise Linux (RHEL) Desktop, Server 5.3	Yes
Debian 5.0 and Fedora 10	Yes

Mac OS Platforms (32 and 64 bit)

Mac OS X v10.4.x Tiger & Mac OS X v10.5.x Leopard	Yes
Mac OS X v10.6.x Snow Leopard	Yes

Supported Databases

MS SQL Server 2000, 2005, 2008	Yes
MS SQL Server 2005, 2008 Express Edition	Yes

Pre-Boot Authentication Support (Single or Multi-Factor)

TPM (TPM 1.1 and 1.2) and TPM	Yes
Biometrics (UPEK fingerprint)	Yes
Smart Card readers (Including Cryptovision smart cards SP800-73 PIV cards, SP800-78 PIV cards, Gemalto .NET v2+ , and Dell E-Series, USB SCR/SCM 3310 and 3310V2.0, and Crescendo HID C700 (based on JCOP21))	Yes

Removable Media Encryption (RME)

CD/DVD encryption	Yes
USB Tokens Support (Including Gemalto Smart Enterprise Guardian token, BlockMaster SafeStick, IronKey)	Yes

Self Encrypting Drives Support

Seagate's Momentus and Black Armor	Yes
TCG Opal compliant self-encrypting drives (including drives from Seagate, Hitachi, Fujitsu, Toshiba, and Samsung)	Yes

SecureDoc Certification Pedigree

First AES validation from NIST (Certificate #1)	256 bit
FIPS	140-2 Level 2
Common Criteria validation	EAL-4

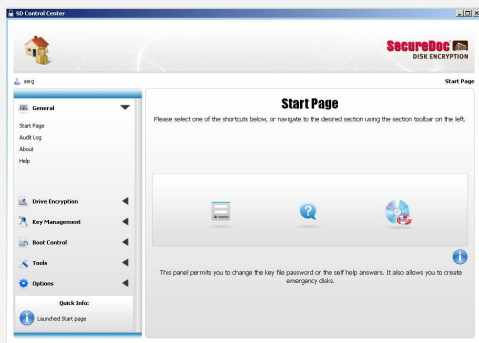
Advantages of Opal Compliant Self-Encrypting Drives (SEDs)

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, therefore becoming instantly activated by SecureDoc and not requiring the hard drive to become initially encrypted in software requiring multiple hours of time to convert into an encrypted drive (protection from the first second).
- 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 overheads).
- 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 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: The Master Boot Record (MBR) is not modified, therefore no kernel driver needed and no conflicts with other software occur.

New Graphical User Interface (Client)



Deploying profiles and policies unique to users and devices in the enterprise

- Ability to associate SecureDoc profiles with users in addition to devices (Windows PCs) as well. Administrators can assign usage policies unique to each user on a machine with multiple SecureDoc accounts.
- SES user and device profiles integration with AD synchronization reduces IT costs and easily deploy IT governance policies per user. It facilitates smoother communication with all SecureDoc clients for greater robustness and scalability.
- Upgrade mechanism support (from older versions of SES) can minimize disruptions in deployment and allow use of old device profiles in addition to the newly added user profiles.

Intel® Anti-Theft Technology (Intel® AT) Support

- SecureDoc FDE, rich PBA with multi-factor authentication and Intel® AT deterrence technologies, add substantial security, manageability and interoperability benefits to the enterprise heterogeneous environments from one management console.
- Intel encrypted data access disable capability can disable user access to the data in a non-destructive manner from SecureDoc Enterprise Server (SES).
- System administrators can restore the users' access to data remotely. It is a simple and inexpensive way to restore a laptop or PC to full functionality. Encryption Data Disable is a recoverable alternative to remote crypto erase, since the latter outcome is irreversible.
- Secures storage of crypto secret that binds the data to the platform.

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 end user, even if the individual attempting to login possesses the correct pre-boot authentication credentials. Encryption Data Disable is a recoverable alternative to remote crypto erase since its outcome is irreversible and not discontinuous. Intel's value-add non-destructive platform disable services can be triggered by:

- Excessive end-user attempts at logging into system (number of allowed attempted 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'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.