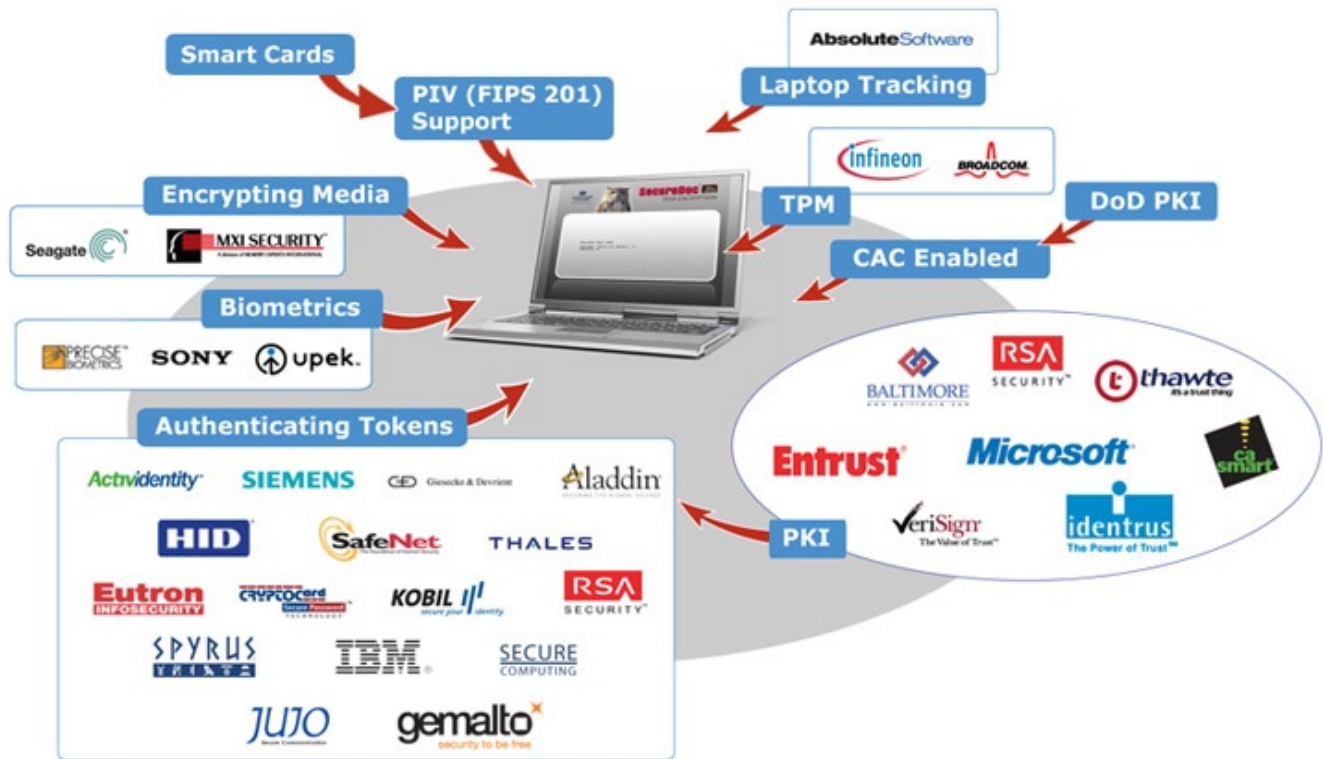


1-, 2- or even 3- Factor User Authentication at PRE-BOOT



The most secure and versatile disk encryption software

A commercially available full-disk encryption software application designed specifically to run transparently with Windows Vista/XP/2000/2003. While thoroughly encrypting all residual data, temporary files, paging files, and hidden partitions, SecureDoc utilizes the AES 256-bit encryption algorithm to encrypt the entire hard-drive where every byte is encrypted.

It is superior to other encryption products and technologies in its robustness and reliability. It offers many exciting new features including the ability to run disk utility applications like "ghost" on drives that may or may not have bad sectors. SecureDoc is the only disk encryption solution offering integration with popular tokens and PKI truly at PRE-BOOT time – where secure user authentication should take place! SecureDoc offers dual and triple factor authentication for ultimate security and flexibility (password / hardware token / biometrics / smart card).

Integrates with USB Tokens and Smart cards

SecureDoc offers dual and triple factor authentication for ultimate security and protection (password, tokens, and biometrics). It works with ActivCard, Aladdin, Datakey, Eutron, Kobil, Rainbow, and other industry leading suppliers of tokens.

Encrypts Removable Media

Easily encrypts floppy, Zip, Jazz drives, USB drives, PCMCIA, memory sticks, Firewall drives as well as flash drives such as IBM MicroDrive PC-card, and now includes CD/DVD encryption.

Enterprise Version – Easy to Configure, Deploy and Manage

For enterprise wide deployment of SecureDoc:

- Central Administration allows "silent" installation, installs and set up user's PC's through the network without any administration on the client PCs.
- Central Database lets the administrator manage users and keys. The central administrator has access to all PCs, guaranteed to be able to recover data in case the employee leaves the company.
- Remote one-time password key recovery allows user to log on to use the PC if the user forgets the password. Help desk can issue a one-time key unlock password on a challenge-response way so an attacker would not be able to access the PC even if the attacker intercepts all transmitted data.

Single Sign On

Users can be configured to sign into Windows operating system with only one password.

Protected Multi-Users for Shared Computers

An unlimited number of users can be issued individual keys to access a single computer. Users can easily choose the method of securing their computer utilizing a password-only and/or token integration.

Role & Identity-Based Key Labeling

SecureDoc allows the option of labeling 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.

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 30 Gigabytes per hour on a 1.8 G 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.



- Password Rules assist users in password preparation, thus readily conforming to in-house security policies and practices.
 - Single Sign-On with Windows. SecureDoc locks computer if the token is removed.
 - Supports popular Tablet PCs.
 - Supports standby and hibernation modes in Windows Vista/XP/2000/2003.
 - 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.
 - Removable Media Encryption including DVD/CD's, USB thumb drives, Encryption support for floppy, Zip, Jaz, as well as the IBM MicroDrive PC card.
 - 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.
 - Lock/Unlock users at boot time for both SecureDoc users and failed login attempts.
 - Support for visually challenged users.
 - Unicode Support, Spanish, German, Italian, Chinese, Taiwanese, and other western languages.
 - Encryption Header allows for more flexibility for sharing encrypted objects. It supports encryption through the conventional 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).
 - Many more features such as *Secure-Wipe *File & Folder Encryption *Key File on Token *Automated Token
- Set-up Wizard *Self-help Key File Recovery *Multi-Processor Support *Auto-Boot Support *International Keyboard Support

WinMagic has been an innovator and thought leader where all, if not most, of the advancements in Full-Disk Encryption has come from our pioneering results.

Enterprise-wide Deployment and Management through the SecureDoc Enterprise Server (SES)

Contributions to the market place in the last 5+ years:

- First AES validation from NIST (Certificate #1)
- First and only FIPS 140-1 Level 2 certification
- Common Criteria validation
- The ONLY disk encryption (FORTEZZA version) certified by the NSA for SECRET data for US Government agencies
- The only disk encryption to support DoD Common Access Card smartcard, and even pass the PKI enable interoperability test at Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC)
- Common Criteria validation
- Chosen for the Support of HSPD-12 initiative by US State Department and Homeland Security in 2005 (First and Only Biometrics support for HSPD-12)
- Smartcard and PKI at pre-boot since 2000
- First to support Windows 2000 in 2000, first to support VISTA in 2006
- First to support disk utilities such as imaging software on encrypted disks (others use to say it's impossible)
- First to denounce "master password" so that "Master password" is no longer used as a feature in disk encryption market.
- First to use scalable DBMS like SQL for centralized management of disk encryption
- Only one to support drives with non-standard 512 byte sectors such as MO drives.
- First to support removable media encryption with comprehensive features since 1998
- Use key file, key labeling, applying crypto standard, crypto API even between internal components. Ready for "standard disk encryption".
- Early support for hibernation in 2003
- Support TPM 1.1 since 2005. Now supporting TPM 1.1 and 1.2 – at pre-boot

Simple, Streamlined Deployment

- Quickly and easily install SecureDoc, without user intervention, on all client computers
- Encryption keys automatically assigned and information returned to SES for centralized management of users, computers, keys and key files.
- Automatic addition of administrator key to key file, ensuring administrator access to encrypted client computers

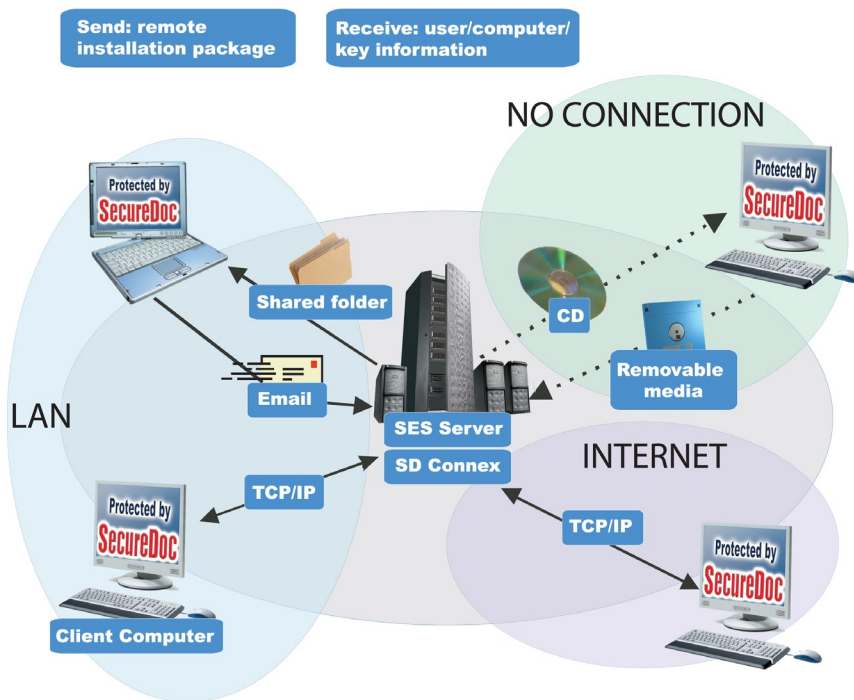
Extensive Management Tools

- Ability to remotely control client computers, including rebooting or locking them
- Easily create, modify, assign and delete keys
- Import keys from files and tokens
- Users can be grouped into folders for easier access: folders can be assigned to specific administrators for individualized control
- Active Directory user data can be synchronized automatically as it changes
- User data can include customized fields
- Transactions stored in audit log on client computers and automatically and securely sent to central location
- Ability to automatically lock out users when connection to server lost for specified period of time
- Encryption status of client computers shown in management interface

Password Rule Enforcement

- Password rules, including length and detailed composition, set by administrators and enforced for users
- Password update frequency can be configured
- Variety of Password-Recovery Options
- Self-help password recovery based on user response to an unlimited number of authentication questions
- Remote one-time challenge-and-response password unlock

SES: The different connection methods



SecureDoc Enterprise Server (SES) can:

- Easily configure user / group profiles
- Conveniently deploy and manage profiles
- Import users and certificates from Active Directory or any LDAP server
- Deploy SecureDoc on client computers using PKI certificates (Certificate Authority-CA serves)

Other Products in the SecureDoc family

- Compartmental SecureDoc divides ONE computer into two or three totally independent compartments with different levels of security. It's the first software-only, cost-effective solution for home/work, secret and non-secret levels of a Secure Computer.
- SecureDoc Mobile Edition encrypts automatically and transparently data on PDAs, Flash cards, SD Cards and other removable media, with no degradation in performance. It's powerful, user-friendly and indispensable protection of sensitive data on the go.

Easy and comprehensive Deployment and Management on thousands of client computers over:

- LAN
- WAN
- Intermittent network connection
- Or no network connection at all (CD)



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.