Data protection with SecureDoc 4.3

There are many ways to protect data, using WinMagic's SecureDoc software can help you protect data, prevent unauthorized copying to a removable device such as USB drive, ...

TipsMake.com - *The problem of losing or losing a laptop while a certain employee goes to work is really disastrous. While most systems use Windows and domain passwords, they are generally not secure enough to protect the data in your computer. But as long as someone has a little bit of computer skills, then your data will be exposed, obviously it's disastrous.*

There are many ways to overcome that problem, using WinMagic's SecureDoc software can help you protect data, avoid unauthorized copying to a removable device such as USB drive, data protection on memory cards and help you safely get rid of corrupted or outdated hard drives (you probably don't want your data to fall into the hands of someone who buys your product (second-hand users))). This article writer also had lost his laptop, so he understood very well at least one of these features.

There are two ways to use SecureDoc, we tried both. First perform the installation on a standalone system, to provide encryption for a separate system. This method should be for users who have to travel a lot and often do not need to connect to the server in the organization. The second way in using SecureDoc is an enterprise solution managed by a server.

The essential step in deploying this software is to install the server version of the product and interact with what a network user can. In the server configuration, the main focus is that the files on the shared drive reside on these servers, so you can use this version in combination with a special, personal user version. If your user disconnects from the network to work completely independently.

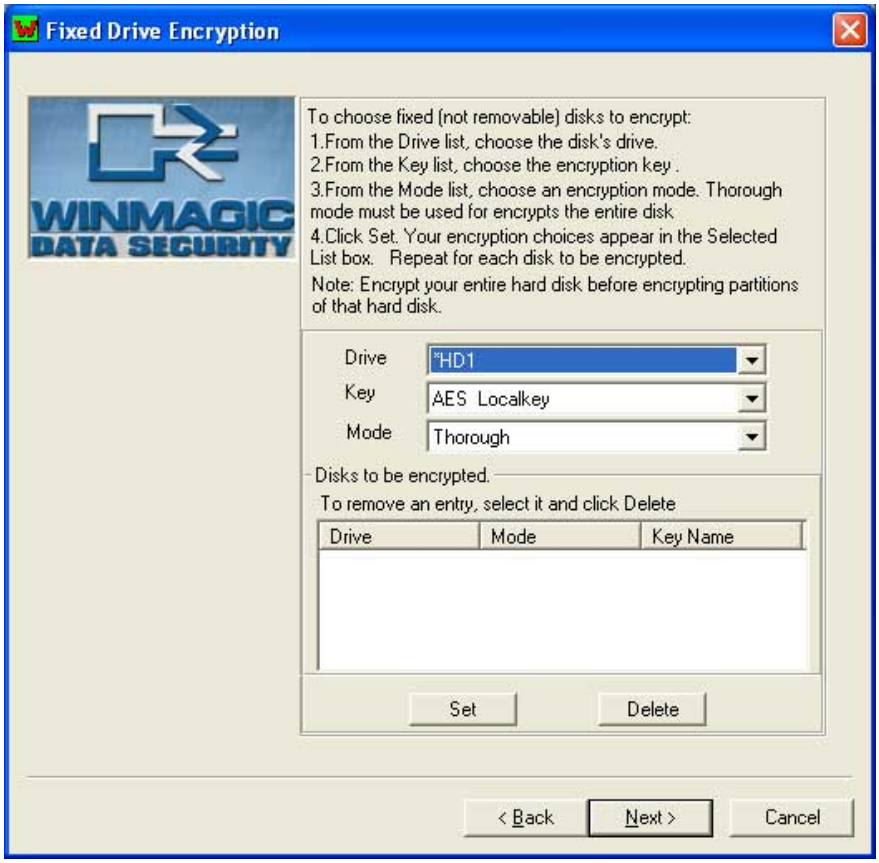

Figure 1: When installing SecureDoc, you can select the drive, key or encryption type you want to use.

Installation and encryption

The installation takes place completely automatically and will take a few minutes. While installing SecureDoc will require you to define a key file, disk password and at least one key (see Figure 1). You can also specify the use of hard cards here with a password. The computer will then reboot and take a few minutes to encrypt the entire disk, ask you to log in and select a key file (if necessary), then access the disc again. There are two events set up in order. The order here is to encrypt the disk, SecureDoc must write to the master boot record (MBR - master boot record). This is a dangerous action, documents often warn that bad disk sectors or other software written into the MBR can cause problems. If you suspect if your hardware is satisfactory, perform some previous checks. This software also does not support dual-boot USB encryption. If you have a Linux partition, you must encrypt that partition separately from within Windows.

System requirements are very responsive: just need a moderate speed processor, 128MB RAM, 128MB of free disk space, Windows Vista operating system, XP SP2 or 2000 SP4. You may also have to install Visual C ++ 2005 Redistributable Package. Perhaps the only downside is that there are too many things for a typical user to read and understand. However, most tasks are completely transparent and easy to understand.

Figure 2: SecureDoc Control Center provides a login using tabs: Password, boot control, disk encryption, customize and Aucit log.

How it works

Under normal use conditions, a computer user will not see any difference between an encrypted computer and an unencrypted computer, except for the initial login process. There are no significant differences in system performance and nothing that users have to do. If users want to copy data from one system to a USB or CD / DVD, the process will be a little different from what they usually use.

Writing data to an external device involves creating a container that will be present on the desktop and in Windows Explorer as a virtual disk. To use this container, users must work with the key and container manager to create, open and close containers.

By default, SecureDoc's configuration wizard will allow you to easily set the key and password. However, this wizard will not allow you to change or restore passwords. With these actions, you can use key management features to manage and recover passwords.

If you are an admin, there are a few things you can do here. For example, if the computer has multiple user accounts, you can add or delete users, passwords and keys. You can also manage startup options between those users.

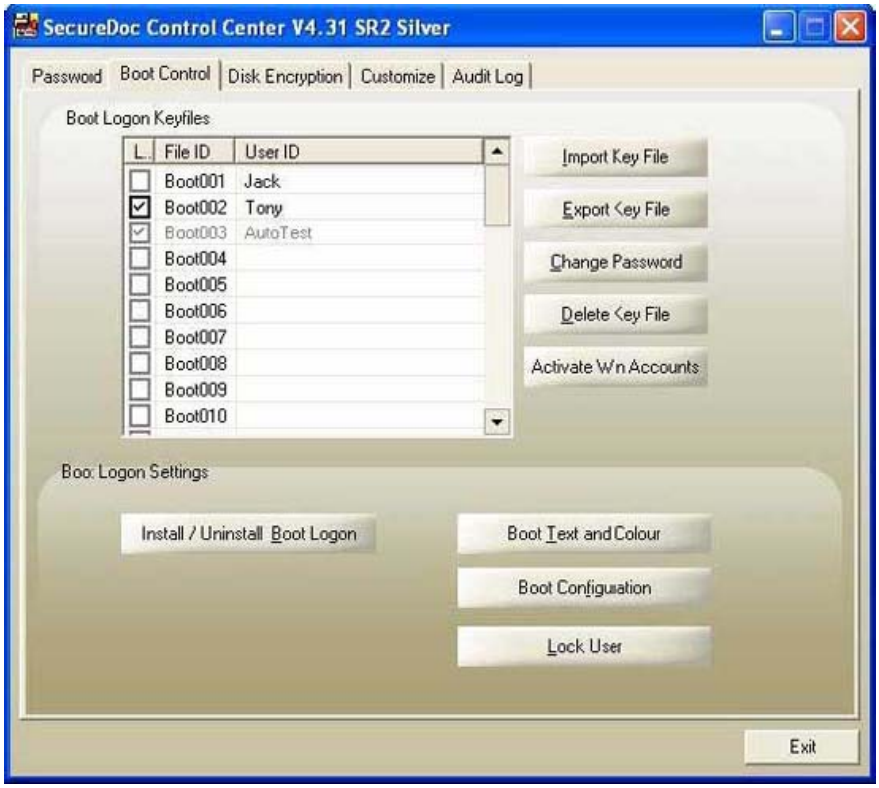

Figure 3: Control Center's boot control tab allows you to manage key files and startup modes for different users

SecureDoc Control Center provides a multi-functional interface for accessing functions. Once installed, you can log in with the disk login password and work in the interface of boot control, disk encryption, customize and log (see Figure 2). Once logged in, you can switch between tabs and perform encryption-related tweaks (see Figure 3).

Users can encrypt files and folders with certain keys. This is useful for emailing documents or other ways that can transmit them on an encrypted environment. You must set up different keys for those objects and manage them in the Control Center. Once you have encrypted a file, this file will have an extension called .SDE, based on this extension you can identify your encrypted documents.

The ability to work from a server is quite smooth. Passwords for individual systems and users are widely available to the server, so when you log in, you won't have to worry about server access passwords. However, if you use a removable device, you still need to create and manage containers.

Security level

SecureDoc products have been validated by AES from the National Institute of Standards and Technology, Level 2 certification according to Information Processing Standards (140-1) and granted by the National Data Security Center itself. US government. Besides support as mentioned above, it also supports smart cards, USB cards and public key infrastructure (PKI).

If your employees have to work outside the corporate network or go on business trips with their laptops, you may encounter two security issues. The first is also the problem that many businesses need is to ensure that access is safe for the corporate network. However, most solutions have not yet been targeted at the loss of

laptops or other devices. Therefore, encryption becomes simpler in the process of use, both for personal solutions as well as for the whole company. This is where you need full disk encryption and SecureDoc is the product you should choose.

Information about product

Product's name:

SecureDoc 4.3

Production company:

WinMagic

Price:

$ 129 per user