SecureDoc Enterprise V6.5

User Guide

WINMAGIC®
DATA SECURITY

Many products, software and technologies are subject to export control for both Canada and the United States of America. WinMagic advises all customers that they are responsible for familiarizing themselves with these regulations. Exports and re-exports of WinMagic Inc. products are subject to Canadian and US export controls administered by the Canadian Border Services Agency (CBSA) and the Commerce Department's Bureau of Industry and Security (BIS). For more information, visit WinMagic's web site or the web site of the appropriate agency.

Acknowledgements

This product includes cryptographic software written by Antoon Bosselaers, Hans Dobbertin, Bart Preneel, Eric Young (eay@mincom.oz.au) and Joan Daemen and Vincent Rijmen, creators of the Rijndael AES algorithm.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.OpenSSL.org/).

WinMagic would like to thank these developers for their software contributions.

Contacting WinMagic

WinMagic
5600A Cancross Court
Mississauga, Ontario, L5R 3E9

toll free: 1-888-879-5879
phone: (905) 502-7000
fax: (905) 502-7001

Sales: sales@winmagic.com

Marketing: marketing@winmagic.com

Human Resources: hr@winmagic.com

Technical Support: support@winmagic.com

For information: info@winmagic.com

For billing inquiries: finance@winmagic.com

Who Should Read this Document

This document explains how to use SecureDoc in an enterprise environment and is intended for either end users or administrators. It describes features available in all SecureDoc editions, with edition-specific features clearly labelled. Note that some features may not be available in some environments, or to some users.

This document assumes a basic working knowledge of Windows-based computer systems. It explains only SecureDoc-specific procedures: you may also need to consult separate documentation, such as that provided by a token manufacturer.

Chapter 1

Introduction to SecureDoc

About SecureDoc

SecureDoc stops unauthorized users from gaining access to confidential data on your notebook or desktop computer or on your removable media (USB drive, CD, and/or DVD). Once SecureDoc is installed and set up on your computer, you and other users must be authenticated (using password, hardware token/smart card, biometric, or PKI) before even attempting to log on to Windows: this is called Pre-Boot Authentication (PBA).

SecureDoc is installed automatically on your computer and configured by your administrator.

As a SecureDoc user, you have access to WinMagic's MagicSync product, which allows you to encrypt and securely share files that are stored in a cloud storage provider. See the separate MagicSync online help.

About Boot Logon

Boot Logon is the SecureDoc mechanism that performs Pre-Boot Authentication. Whether or not you see Boot Logon as well as your normal Windows logon depends on how SecureDoc has been configured. You can choose the language used for Boot Logon: right-click on the SecureDoc icon in the system tray and choose SecureDoc Language Selection, then choose the language to be used for the client interface, Boot Logon, or both.

SecureDoc’s Encryption Features

In addition to allowing you to encrypt your fixed disk, you can use SecureDoc to encrypt:

- removable media (USB, CD, DVD), encrypted either automatically or manually, for individual or shared use (see “Working with Removable Media” on page 42)
- individual files and folders locally, on a network, or on a USB device, using File and Folder Encryption (see “Using File and Folder Encryption” on page 50)

SecureDoc performs full disk encryption for fixed and removable media. This provides the most secure and comprehensive protection for data. However, file and folder encryption has a useful role to play in a comprehensive strategy for data-at-rest encryption. It is effective in protecting data files in transit, securing information sharing, and defending against internal threats.

By shielding data files in transit — file transfers, e-mail attachments, etc. — File and Folder Encryption provides a strong complement to full disk encryption, particularly when the functions are integrated under a single management scheme.

About the SecureDoc Interface

Launch the SecureDoc interface from **Start > SecureDoc Control Center**.

You use the SecureDoc interface to encrypt removable media as well as to perform encryption management tasks.

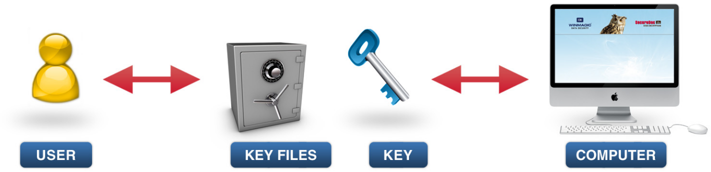
Use the navigation pane on the left of the screen to choose a function to perform. Click groups to expand them, then click the function’s name. The corresponding data screen appears in the right pane.

Encryption Terms and Concepts

Using SecureDoc doesn’t require detailed knowledge about encryption and how it works. However, it is useful to understand some basic terms and concepts.

Keys and Key Files

Like a physical key, an *encryption key* is used to lock and unlock secured information. Encryption keys are stored in key files (you can think of them as the key ring that holds your keys). To access encrypted media, you need to log on to the key file containing the key used to encrypt the media.



The key file identified during encryption of your fixed disk is your "default" key file.

A key file can contain multiple keys, and the same key can exist in multiple key files. For example, you might want to share with other users the key used to encrypt removable media, but not the key used to encrypt your fixed disk. If you have both keys in the same key file, you would create (or acquire) key files for the other users and copy (import) the removable media key from your key file into the other key files. Alternatively, you could have different key files for different purposes, logging onto each key file as needed.

More About Key Files

Key files have a .DBK extension (juser.dbk, sdadmin.dbk, etc.) and are protected by a password or token.

You can store key files in a variety of locations, such as your computer's hard disk, removable media, or a token. As long as your removable media is kept in a secure location, storing key files on removable media provides more security than storing them on the hard disk. With key files on removable media, a hacker who has access to a computer does not have access to the keys used to encrypt it. Their only option is to attack and break the encryption algorithm — a nearly impossible task.

Key files are, themselves, encrypted.

Key files can be further protected with a certificate or protection key stored on a token or smart card.

About the Encryption/Decryption Process

During encryption, data is read, encrypted, then written back on the same sector. Once this process is complete, any data *read* is automatically and transparently decrypted, and any data *written* is automatically and transparently encrypted.

Note: *Initial encryption is called "conversion".*

Once a file is accessed, it is decrypted in memory. If this file is saved elsewhere other than the encrypted area, it remains in plain text. For example, if you open a file on your encrypted hard drive and save it to an unencrypted network folder, the network version is not encrypted.

Password Rules

Password rules can be used to ensure that passwords are secure (for example, are made up of a mixture of numbers and letters, are changed regularly). Password rules apply to a specific key file. For more about passwords, see See "Appendix A: Password Rules" on page 59.

Key File Privileges

Key files are associated with specific privileges that determine what the user of that key file can and cannot do. Privileges fall into two basic categories: user and administrator (admin). SecureDoc features are available only to someone who logged on to the computer using a key file that has administrator privileges. Key files created through the Key File Wizard are admin key files.If your computer was encrypted by someone else, you may have a user key file, which enables you to read and write to encrypted disks, and change the password of your key file, but nothing else.

Note: *Users who log in with a user key file can create new key files for their personal use and have all administrator privileges for those key files. However, these key files do not contain the key used to encrypt the hard disk and so can be used only for removable media.*

Administrator key files may contain the encryption keys for multiple users, such as those in a department or division. This ensures that administrators, on behalf of the enterprise, can always access data encrypted by users. This is an important safety precaution in case a user leaves the company without decrypting information, or without leaving their encryption keys and passwords behind.

Note: *You can lock specific users even if they have a valid key—see "Creating Backup Key File" on page 21.*

About Recovery Media

If anything happens to the computer's master boot record (MBR), and the Boot Logon screen is missing, the computer could be left inaccessible. Recovery media has been created for you.

Recovery media is specific to the individual computer: do not use recovery media unless you are sure it was created on your computer.

Note: *Because recovery media requires no password or token to access it, it presents a large security risk. Keep recovery media in a secure location at all times.*

Keep your recovery media updated, or you could encounter problems with restoring data. SecureDoc prompts you to create recovery media every time the SecureDoc space is modified, such as when Boot Logon is updated. You can create recovery media any time from the Control Center.

Note: *Special recovery media is needed for self-encrypting drives (SEDs) — see "Recovery Media for Self Encrypting Drives (SEDs)" on page 36.*

About Password Recovery

SecureDoc provides several mechanisms for allowing you to recover a lost password:

- A password hint can be defined for a key file and revealed at Boot Logon and when logging on to Control Center.This feature may have been configured for you.
- Self-help password recovery can be defined for a key file. This uses a series of questions and answers gathered at encryption time or when a key file using self-help password is being managed. If the password is forgotten, the user can answer the questions again and, if successful, gain access to a protected computer.This feature may have been defined for you. Administrator-supported password recovery is also available.

Chapter 2

Accessing an SD-Protected Computer

Using Boot Logon

Depending on your configuration, you may or may not see SecureDoc's PreBoot Authentication screen, Boot Logon, before you log on to Windows. If Auto Login has been configured for you, you will have to log on to Windows only once: for all subsequent times, after you authenticate to Boot Logon, your Windows environment launches.

You can use Boot Logon to:

- establish a wireless connection
- log on to an encrypted device
- perform administrative tasks
- recover a forgotten password (see See "Recovering from a Lost Password" on page 34)
- change your password (See "Changing a Key File Password" on page 34)

Note: *If you are unable to logon, you may be able to press F3, then click* ***Save Log****. You will be prompted to save a log file that you can then share with your administrator for troubleshooting purposes*

Connecting Wirelessly

You may be able to connect to the SecureDoc Enterprise Server to authenticate, following these steps. This feature is not available for Windows 8.

1. At the Boot Logon screen, click the wireless icon 📶. A new screen opens.
2. If you have connected wirelessly before, you will see your previous choices: select the appropriate choice and click **Connect**, then click **Back** to return to the Boot Logon screen so you can enter your username/password.
   If this is your first time connecting wirelessly, or if previous wireless settings are not appropriate, follow the steps below.
3. Choose your **Wireless Adapter Type**, then click **Scan** to scan for available wireless networks. Information about the found networks appears on the screen.
4. When you see your wireless network, select it and, if necessary, click **Settings** to make any changes to your network settings.
5. Click **Connect** to connect to your wireless network. A new screen opens.
6. Enter your wireless access **Password** and click **Save**. Once you are connected, you should see a prompt telling you that you are connected.
7. Click **Return** to go back to the SecureDoc Boot Logon screen.
8. Enter your username/password and press Enter or click **Login**. If the username/password matches the one stored in the SES database, your computer continues to load Windows.

If you enter an inaccurate password, you may see a password hint. If you forgot your password, click **Forgot Password?** and follow the appropriate password recovery steps.

Logging On

If desired, choose the language of the SecureDoc interface from the list.

Enter the userID and password provided to you and press ENTER or click **Login**. The userID is not case-sensitive. Depending on configuration, you may be able to press ENTER in the UserID field to use a default userID.

If the key needed to access the protected computer is stored on removable media, or in a different key file, enter the full path to the key file's location (removable media will need to be inserted) as well as the key file name/username. If you protected your key file with a token or Smart Card, or if the key file is stored on a token, you are prompted to insert the token or Smart Card.

Note: *The key file(user ID) name must be in DOS format ("8.3"). If your key file is on a USB drive, be sure that the device is detected in DOS.*

If login is successful, your computer continues to load Windows.

If you enter an inaccurate password, you may see a password hint. If you forgot your password, click **Forgot Password?** and follow the appropriate password recovery steps.

Note: *The* 🖧 *icon indicates your connection status to the network (a red dot indicates you are not connected, a green dot indicates a connection exists).*

Accessing Administrative Functions

Press F3 to show additional functions:

- Configuration (use to modify boot configuration; most of these settings should be changed only in consultation with WinMagic Technical Support, or to uninstall SecureDoc - see See "Removing SecureDoc From Your System" on page 41)
- Save Log (use to save information related to login attempts for troubleshooting purposes)
- Information (use to see details about your Network Interface Controller and any SES-related messages)

Note: *By default, your SecureDoc account will be locked after 15 failed login attempts. Another user can login to your locked computer, but you will need administrative help to unlock it for your use. Your installation may use a different value. You can change the value if you wish. See "Changing Maximum Number of Failed Logins" on page 31.*

Identifying Your Keyboard (Tablets Only)

Click ⌨ to choose a different keyboard.

Note: You can also change the keyboard layout in the Control Center (see "Using Specialized Devices" on page 24).

Using the V4 Boot Logon

SecureDoc includes two Boot Logon versions. If Boot Logon fails, reboot and press the "a" key while the computer boots up. That will invoke the V4 version of Boot Logon instead.

To avoid having to manually invoke the V4 version in the future, you can set SecureDoc to use the V4 version of Boot Logon all the time: see "Choosing V5 or V4 Loader" on page 29.

Entering a Temporary Password (Single Sign-on and Password Synchronization)

If your ActiveDirectory administrator has changed your password and provided you with a temporary one, you will need to re-establish the password synchronization between Windows and SecureDoc.

If you reboot your machine after receiving a temporary password:

1. You will see the SecureDoc login again.
2. Enter your original key file password: the login will fail.
3. Enter it again: you will see the Windows Login (including the **Use cached Credentials** option, to be used if the computer is temporarily not on the network, for Vista/Win 7).
4. Enter your temporary password and, when prompted, enter a new password.
5. When you reboot again, you will be able to access Windows without specifying a password.

If you simply lock after receiving a temporary password:

1. Enter your temporary password in the Windows Login: the login will fail and the computer will lock.
2. Switch users.
3. The SecureDoc Login screen appears, as it did when you first booted an encrypted computer.
4. Enter your original key file password: the login will fail.
5. Enter it again: you will see the Windows Login and can proceed as normal.

Chapter 3

Using SecureDoc

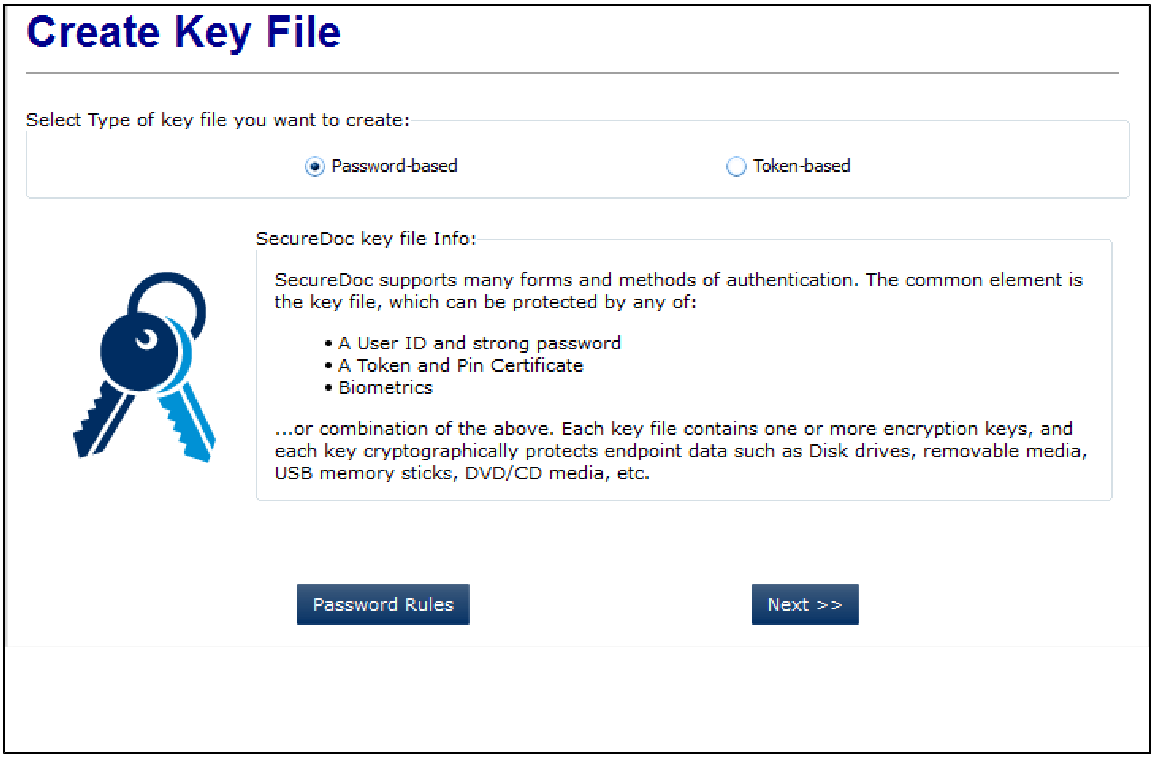
Choosing a Language

You can choose the language used for the SecureDoc interface: right-click on the SecureDoc icon in the system tray and choose SecureDoc Language Selection, then choose the language to be used for the client interface, Boot Logon, or both.

Creating Key Files

Creating Key Files with Control Center

1. In Control Center, click **Key Management**, then **Create key file**.
2. Choose whether to create a password-based or token-based key file.



Create Key File

Select Type of key file you want to create:

● Password-based ○ Token-based

SecureDoc key file Info:

SecureDoc supports many forms and methods of authentication. The common element is the key file, which can be protected by any of:

- A User ID and strong password
- A Token and Pin Certificate
- Biometrics

...or combination of the above. Each key file contains one or more encryption keys, and each key cryptographically protects endpoint data such as Disk drives, removable media, USB memory sticks, DVD/CD media, etc.

3. To set the password rules for this key file, click **Password Rules**. (For more about password rules, see See "Appendix A: Password Rules" on page 59.)

Token-Based Key Files

1. If you choose **Token-based**, you are prompted for token information. Choose the token type slot and slot. Choose from the available methods for protection (see See "Appendix B: Protection Methods" on page 61).

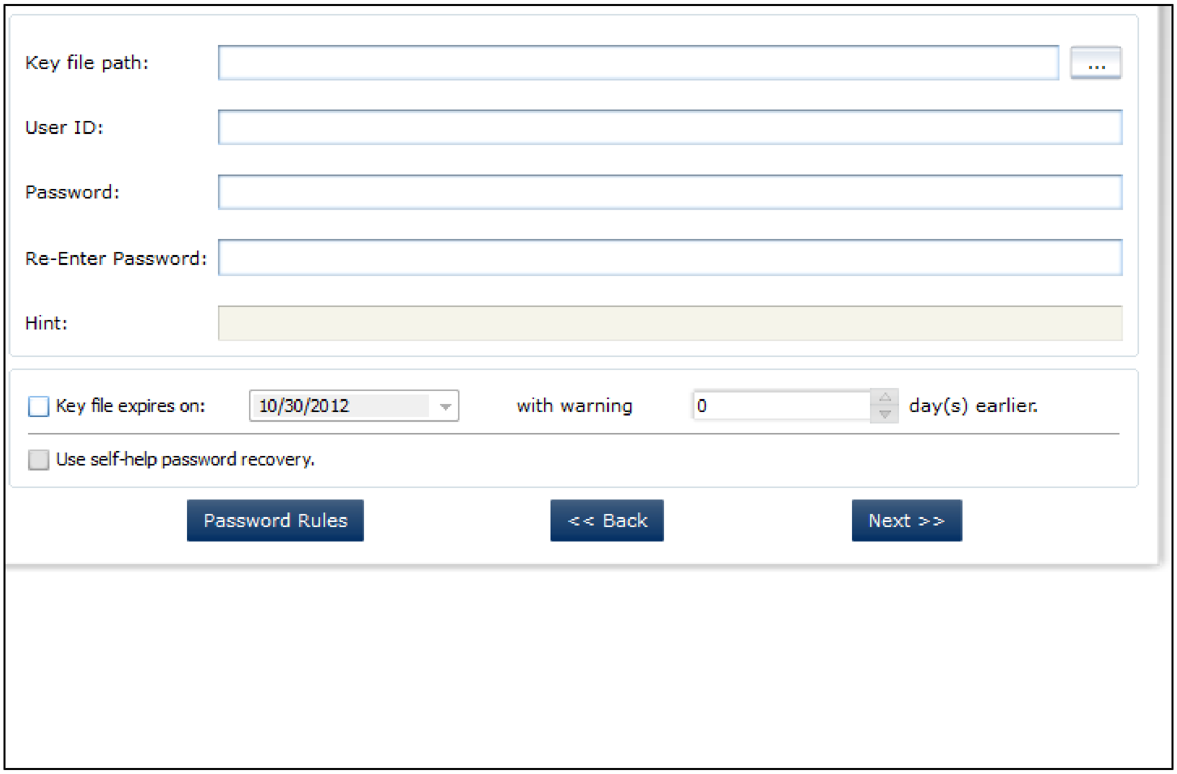
Note: *Password fields and options appear once a token is selected.*

2. Enter the token password and choose whether or not you want a user password used in addition to the token password to gain access to the encrypted computer.
3. Click **Login Token**, then click **Next**. The **Object Label** field appears.

4. From the **Object Label** list, choose the key from the token that you want to use for encryption. Click **Next** and follow the steps as for password-based key files in “Password-Based Key Files” on page 14.

Password-Based Key Files

1. If you choose **Password-based**, when you click **Next** you are prompted to enter the key file details.



Key file path:

User ID:

Password:

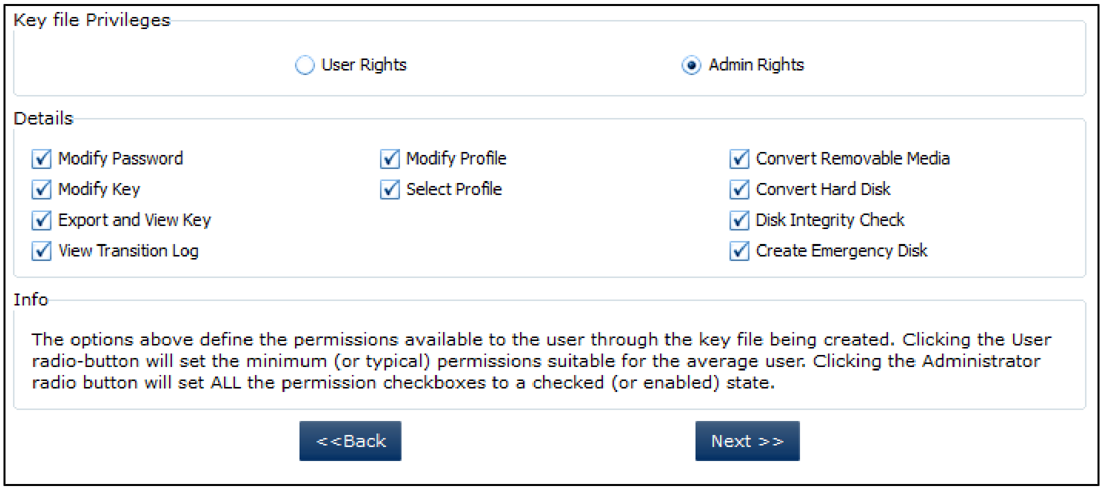
Re-Enter Password:

Hint:

□ Key file expires on: 10/30/2012 with warning 0 day(s) earlier.

□ Use self-help password recovery.

2. Click ... and browse to the location where you want to create your key file, entering a key file name.
3. Enter a **User ID** and password (in both the **Password** and **Re-Enter Password** fields) to be used for accessing the key file. The User ID is a maximum of 64 characters, and not, by default, case-sensitive. The password should be a strong password that satisfies the password rules you established earlier.
4. If your password rules included enabling the password hint, enter a **Hint** that you can display if you forget your password. Be sure the hint does not contain enough information for an illegitimate user to guess your password. Click **Password Rules** and make sure that **Disable password hint** is cleared.
5. To have the key file expire by a certain date, check the **Key File Expires On** option and choose the expiry date and the number of days prior to that date that a warning will appear when that key file is used.
6. To use self-help password recovery for a forgotten password, first click **Password Rules** again and choose how many questions should be answered and the minimum total length of the answers. Then check the **Use self-help password recovery** option: you are prompted to acknowledge the need to enter self-help answers. Click **OK** and answer the appropriate number of questions.
7. Click **Next**.



Key file Privileges

○ User Rights ● Admin Rights

Details

☑ Modify Password
☑ Modify Key
☑ Export and View Key
☑ View Transition Log
☑ Modify Profile
☑ Select Profile
☑ Convert Removable Media
☑ Convert Hard Disk
☑ Disk Integrity Check
☑ Create Emergency Disk

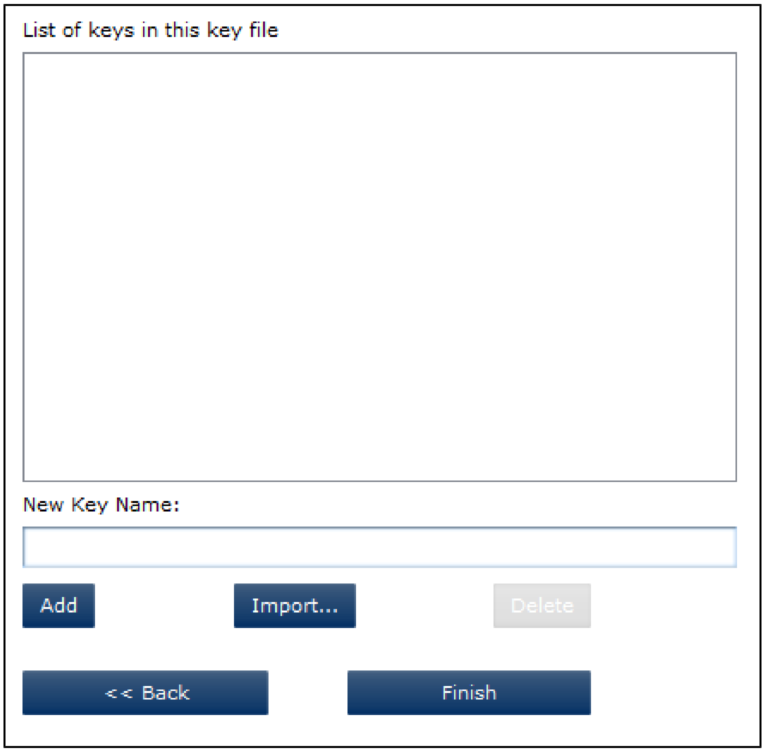
Info

The options above define the permissions available to the user through the key file being created. Clicking the User radio-button will set the minimum (or typical) permissions suitable for the average user. Clicking the Administrator radio button will set ALL the permission checkboxes to a checked (or enabled) state.

8. You are prompted to choose whether the key file should have user or administrator rights, and the specific rights for the key file.

Privilege	Key File Allows
Modify Password	Use of SecureDoc to change the key file password. User key files have only this privilege.
Modify Key	Use of Key Manager to generate, delete, and import keys and to make key file backups. Automatically enables the Export and View Key privilege.
Export and View Key	Use of Key Manager to work with encryption keys, copy a key file to a floppy disk, and to export keys to other key files. Automatically enables the Modify Key privilege.
View Transaction Log	Viewing of the SecureDoc audit log (see “Viewing the Audit Log” on page 39).
Modify Profile	Use of Control Center to set up disk access profiles which control or monitor read/write access to both encrypted and non-encrypted disks. See “Controlling Access to Computer Disks” on page 25. Automatically enables the Select Profile privilege.
Select Profile	Application of disk access profile. See “Controlling Access to Computer Disks” on page 25. Automatically enables the Modify Profile privilege.
Convert Removable Media	Ability to decrypt/encrypt removable media. See“Working with Removable Media” on page 42. Users must also be granted “administrative” rights in Windows.
Convert Hard Disk	Enables administrative user to use the Control Center to decrypt/encrypt hard disks. Users must also be granted “administrative” rights in Windows. Automatically enables the Disk Integrity Check and Create Emergency Disks privileges.
Disk Integrity Check	Continued use of SecureDoc if the *disk integrity* check fails, The Disk integrity check process checks the computer’s boot files to make sure they have not been tampered with, or corrupted, on boot-up.
Create Emergency Disk	Use of the Control Center to create an emergency disk (recovery media) to restore the Master Boot Record. See “Creating Recovery Media” on page 36.

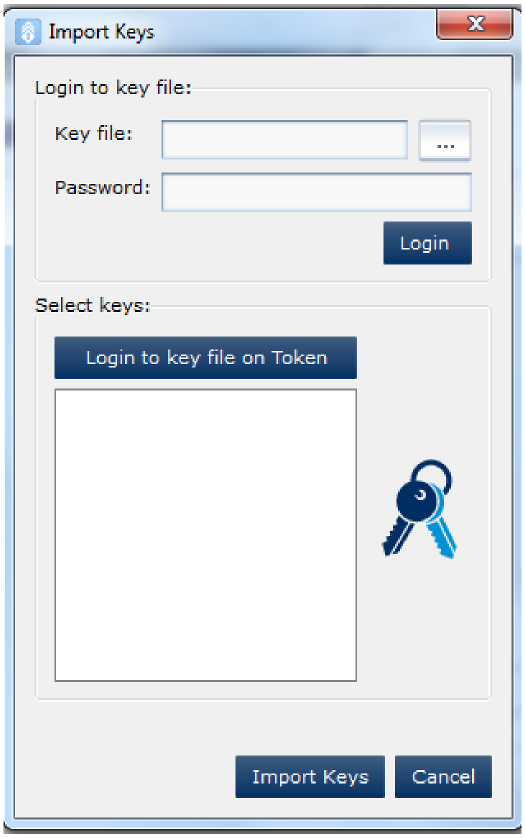
9. Make your selections and click **Next**.



10. Add keys to the key file:

- To create a key and add it to the key file, enter a key name in the **New Key Name** field and click **Add**.
- To import a key from another key file, click **Import**.

  Click ⋯ and browse to the location of the key file containing the key you want to import, enter the **Password** and click **Login**. A list of keys in that key file appears. Select the key(s) to be imported and click **Import Keys**. The selected key(s) are added to the key file's list.



__Note:__ If Boot Logon has not yet been installed, you need to log out of Control Center and log in again to see the added key.

11. Click **Next**, then **Finish**. A prompt tells you the key file was created.

Managing Key Files

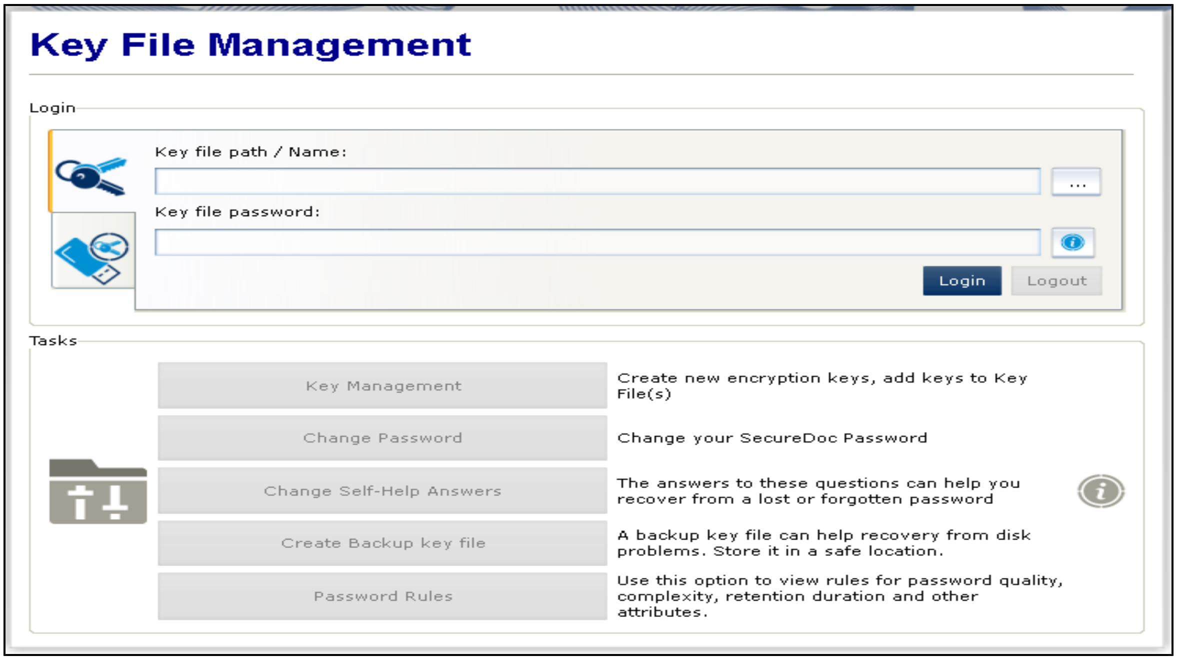
You can manage key files from Control Center. Management of password-based and token-based key files differs.

Managing Key Files

1. In Control Center, click **Key Management**, then **Key file Management**.

2. To manage a password-based key file, click the 🔑 tab, identify and enter the password for the key file you want to manage, and click **Login.**

   To manage a token-based key files, click the 🔑 tab, choose the appropriate token type and slot, enter teh **Password**, and click **Login**.



Key File Management

Login

Key file path / Name:

Key file password:

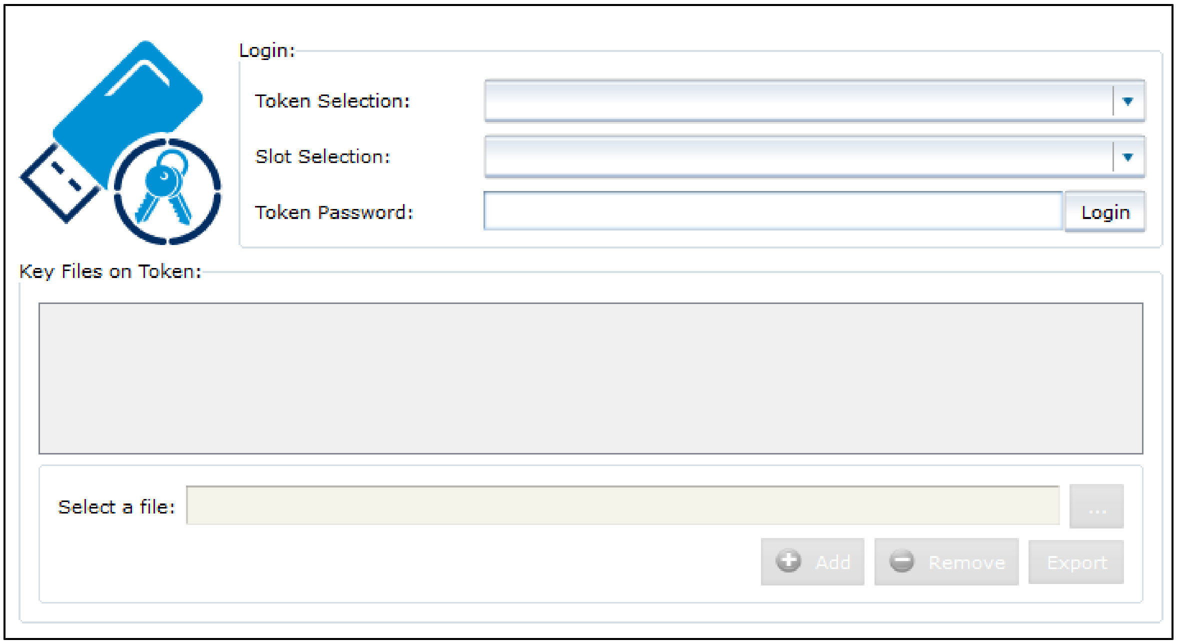
Tasks

Key Management	Create new encryption keys, add keys to Key File(s)
Change Password	Change your SecureDoc Password
Change Self-Help Answers	The answers to these questions can help you recover from a lost or forgotten password
Create Backup key file	A backup key file can help recovery from disk problems. Store it in a safe location.
Password Rules	Use this option to view rules for password quality, complexity, retention duration and other attributes.

3. Choose from the following actions:
   - To add keys to the key file, click **Key Management** and follow the procedures in “Adding Keys to An Existing Key File” on page 20).
   - To change the key file’s password, click **Change Password** or **Change Token Password** and follow the steps as in “Changing a Key File Password” on page 34.
   - To change the key file’s self-help recovery answers, click **Change Self-Help Answers** and follow the steps in “Changing Your Self-Help Answers ” on page 35.
   - To create backup key file, click **Create Backup key file** and follow the steps in see “Creating Backup Key File” on page 21.
   - To view (but not change) password rules, click **Password Rules**. See “Appendix A: Password Rules” on page 59 for more details.

Managing Key Files on a Token

1. In Key Manager or Control Center, click **Key Management**, then **Token key file Management**.

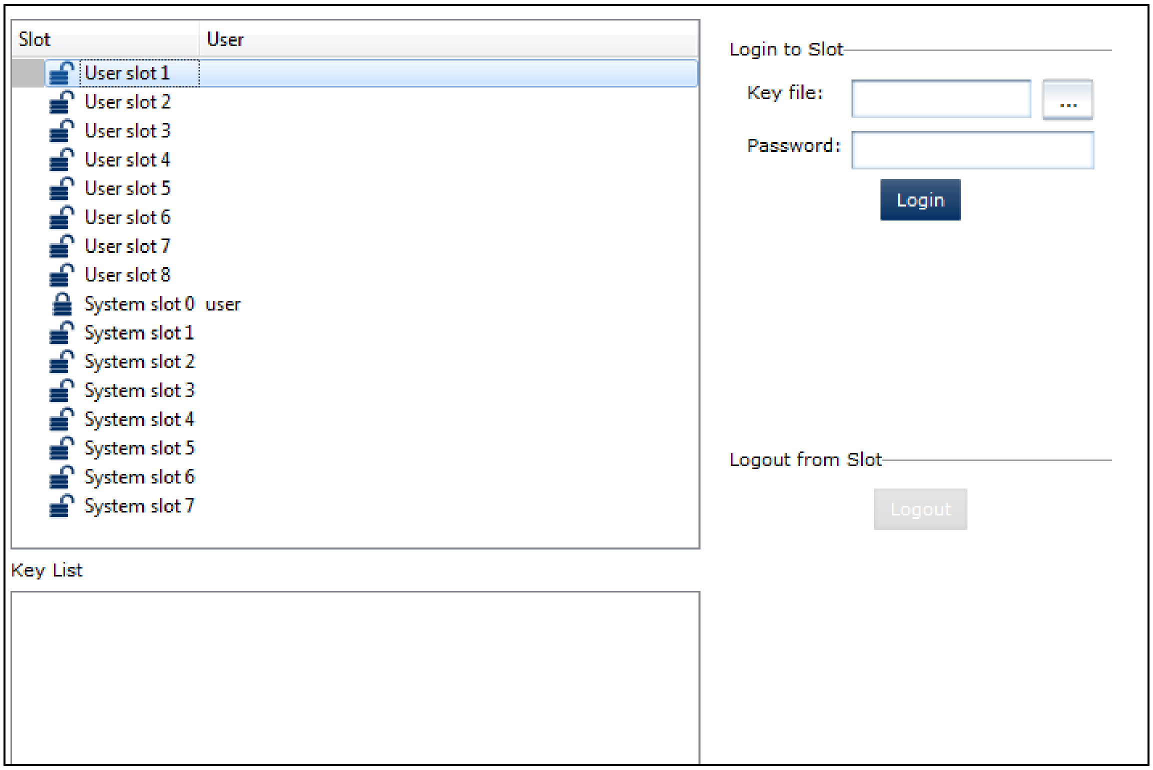


2. Choose the appropriate token type and slot, enter the **Password**, and click **Login**. A list of the key files on that token appear.
3. To add a key file, click **Add**.
   To remove a key file, click **Remove**.
   To export a key file, click **Export**.

Managing Other Key Files

Use this function if you have multiple key files on your computer, and want to control what slot they belong in.

1. In Control Center, click **Key Management**, then **Additional Key files**.



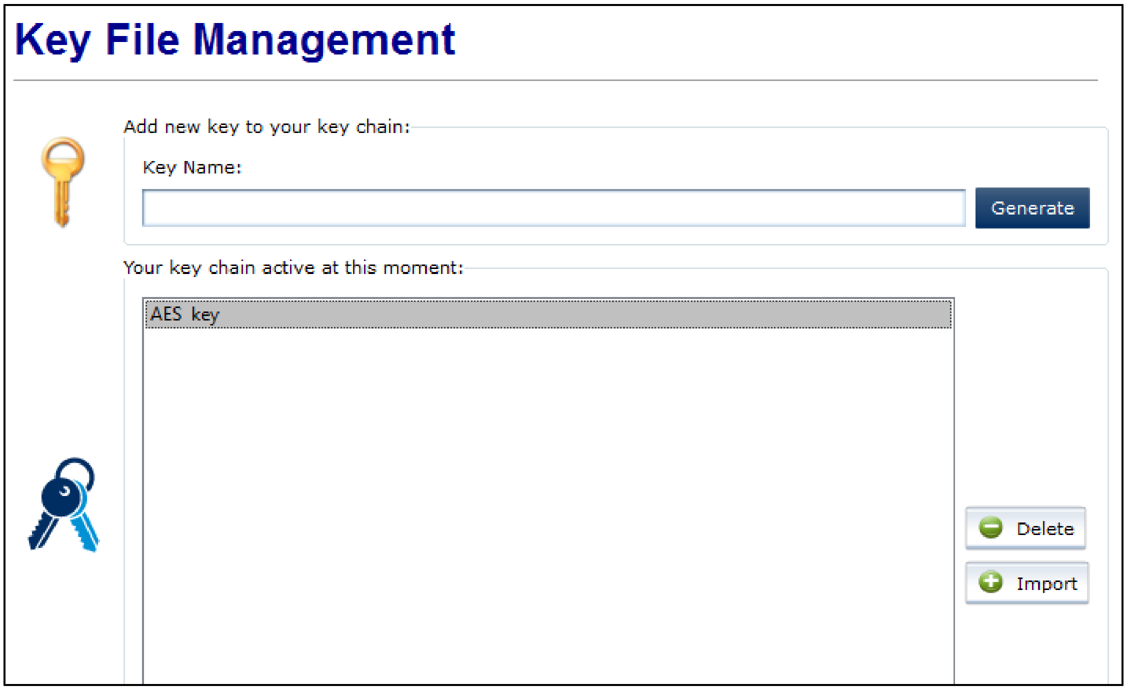
Slot	User
User slot 1	
User slot 2	
User slot 3	
User slot 4	
User slot 5	
User slot 6	
User slot 7	
User slot 8	
System slot 0	user
System slot 1	
System slot 2	
System slot 3	
System slot 4	
System slot 5	
System slot 6	
System slot 7	

2. To remove a key file from its current slot, select it and click **Logout**.
   To add a key file to a slot, select the slot, navigate to the **Key file**, enter the password, then click **Login**.

Adding Keys to An Existing Key File

You can either create new keys for an existing key file, or import keys from another key file.

1. In Control Center, click **Key Management**, then **Key file Management**.
2. Locate and log on to the key file you want to manage, and click **Login**.
3. Click **Key Management**. A new screen appears, showing the keys currently in the key file.


Key File Management
Add new key to your key chain:
Key Name:
Generate
Your key chain active at this moment:
AES key
Delete
Import

- To create a key and add it to the key file, enter a key name in the **Key Name** field and click **Generate**.
- To remove a key from the key file, select it and click **Delete**.

  Note: *Deleting a key that is used to access encrypted media will make that media inaccessible.*

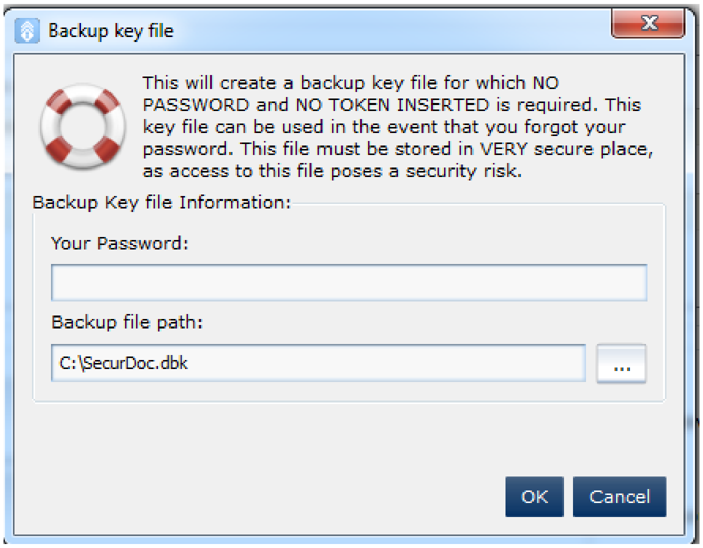
- To import a key from another key file, click **Import**.

  Click ... and browse to the location of the key file containing the key you want to import, enter the **Password** and click **Login**.
  A list of keys in that key file appears.
  Select the key(s) to be imported and click **Import Keys**. The selected key(s) are added to the key file's list.

Creating Backup Key File

A backup key file can be used if you forget your password or make an error when changing your password. The backup contains your encryption keys and requires no password or token to gain access, so it must be kept safe and secure at all times.

1. In Control Center, click **Key Management**, then **Key file Management**.
2. Locate and log on to the key file you want to manage, and click **Login**.
3. Click **Create Backup key file**. A new screen appears.



This will create a backup key file for which NO PASSWORD and NO TOKEN INSERTED is required. This key file can be used in the event that you forgot your password. This file must be stored in VERY secure place, as access to this file poses a security risk.

Backup Key file Information:

Your Password:

Backup file path: C:\SecurDoc.dbk

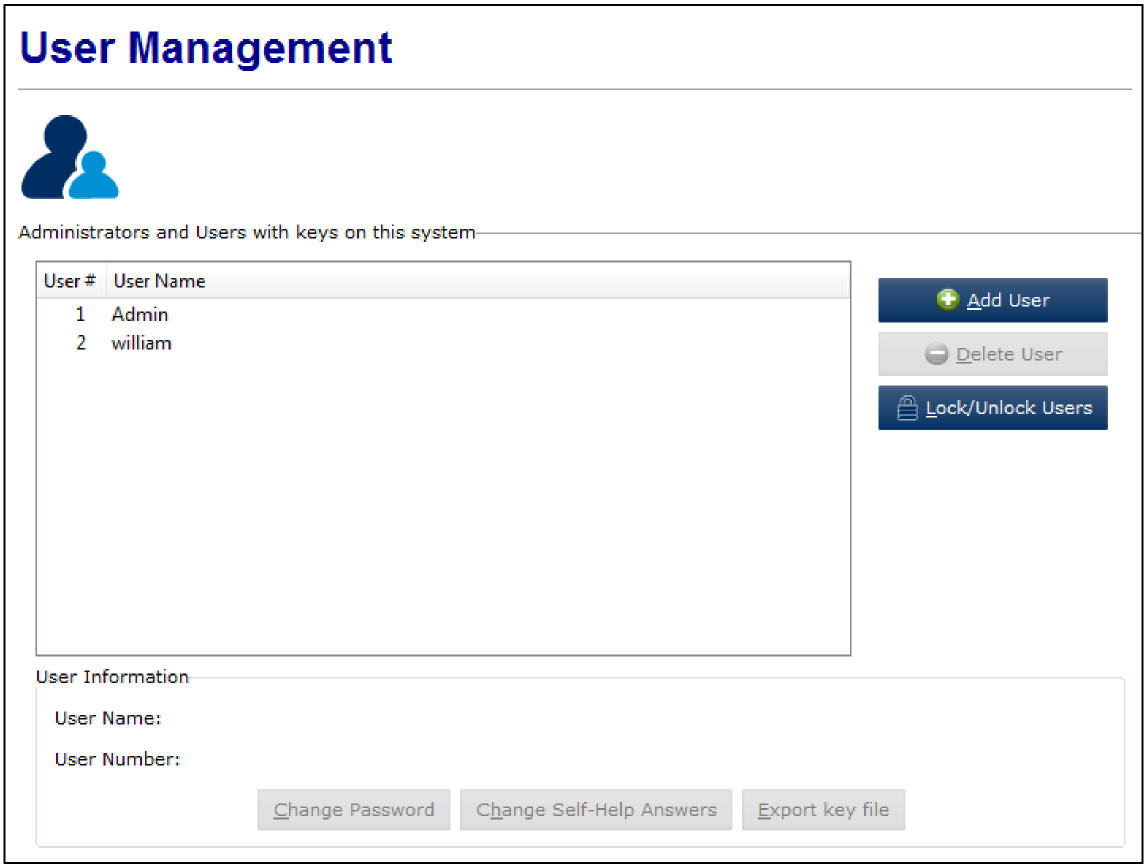
4. Enter the password for the key file again.
5. Choose a location and file name (by default, the file is called Securdoc.dkb).
6. Click **OK**.

Note that a backup key file is not the same thing as a copy: a copy requires the key file password to access.

Managing Users

Use this function to add users (accounts and key files) to your computer and to the Control Center features, change their password or self-help answers, or lock the key files so they cannot access the computer.

In the Control Center, click **Boot Control**, then **User Management**.



User Management

Administrators and Users with keys on this system

User #	User Name
1	Admin
2	william

User Information

User Name:

User Number:

Changing a User’s Key File Password

You can change the password of the key file of any user: select it in the User Management screen and click **Change Password**, then follow the instructions in “Changing a Key File Password” on page 34.

Changing a User’s Self-Help Password Recovery Answers

You can change the self-help password recovery answers, if any, for any user:, select it in the User Management screen and click **Change Self-Help Answers**, then follow the instructions in “Changing Your Self-Help Answers ” on page 35.

Adding Users to This Computer

1. To add a user (existing key file), in the User Management screen, click **Add User.**
2. Click … and navigate to the user’s key file. Optionally, click **Get User Information**.
3. Click **Add**.

Deleting Users From This Computer

1. To remove a user (existing key file), select it in the User Management screen and click **Delete User.**
2. User information appears: to confirm the deletion, click **Delete**. Note that the key file itself is not deleted.

Preventing Users from Accessing This Computer

You may want to lock certain users out from having access to this computer, even if they still have valid keys (for instance, if someone has left the company). Use this function to create a list of users to be locked out. These users, at boot time, see a message that tells them they cannot log on.You can create the list of users to lock out, but the list does not take effect unless you choose to enable it in this screen. You cannot add the key file you are logged in with to the "locked" list.

To lock out a user:

1. In the User Management screen, click **Lock User**. The lock user screen appears, with the lock list enabled and the name of the selected user in the first field.
2. To add the user to the locked list, click **Lock**. If a user name does not appear in the first field, you can type it in the field, then click **Lock**.
   If necessary, click **OK** and select another user, clicking **Lock** to display the lock user screen again and clicking **Lock** to add the selected user to the list.
3. To have the list take effect, be sure that **Enable Locked Users List** is checked when you click **OK**.

Exporting A User's Key File

This function creates a copy of a user's key file.

1. In the User Management screen, select the user (key file) you want to export, then click **Export key file**.
2. You are prompted to choose the destination for the exported file.

Sharing Encrypted Files with Other Users

Enterprise users can, depending on configuration, share files (and folders) from a fully encrypted disk with other users.

1. Right-click on selected files or folders and choose **SecureDoc SFX**.
2. When prompted, enter a password.
3. Give the resulting zip file to another user, along with the password. That user can extract decrypted versions of the files in the compressed file.

Using Specialized Devices

Specialized Keyboards

Use this function if you have an atypical keyboard layout.

1. In the Control Center, click **Boot Control**, then **Advanced Settings**.
2. Click the Keyboard Layout tab.
3. If appropriate, check **Non-standard keyboard** and choose what layout to map it to.
4. To automatically retrieve the Windows keyboard layout while installing Boot Logon, check **Automatically get...**.
5. To use a foreign keyboard, check **Foreign keyboard support**.

Note: *You can also choose a different keyboard at preboot (see "Using Boot Logon" on page 11).*

Tablet PC

Use this function if your computer is a Tablet computer, and you want to use the Tablet's on-screen keyboard for SecureDoc functions. You must also use the V4 bootloader: see "Choosing V5 or V4 Loader" on page 29.

1. In the Control Center, click **Boot Control**, then **Advanced Settings**.
2. Click the Tablet PC tab.
3. From the **Tablet PC support** list, choose the appropriate manufacturer. If your manufacturer and model are not listed, the on-screen keyboard may not be supported (this means that, if you do not have a physical keyboard, you cannot use SecureDoc).
4. Click **Apply**.

PCMCIA Reader

If Boot Logon has problems locating a PCMCIA reader in a laptop, it may be an addressing problem. You may need to change the PCMCIA I/O address on their laptop to the default address D0000000 to help SecureDoc detect it. You then need to do the following:

1. In the Control Center, click **Boot Control**, then **Advanced Settings**.
2. Click the General Settings tab.
3. Check **Change PCMCIA I/O Address if zero**.
4. Click **Apply**.

Controlling Access to Computer Disks

About Disk Access Control

You can lock or monitor different functions performed on the different disks (both encrypted and not encrypted) on your computer. You can monitor, but not lock, your boot disk, using one or all of the following control options.

Setting	Description
Lock	*Lock* means to restrict access in specific ways. You cannot lock the first (boot) drive or the system drive of the disk where SecureDoc resides. You should not lock disks to which Windows and other applications may need to write. For removable media, "lock" means limiting the ability to work with the removable media: if the media is not locked, the user can encrypt, continued interrupted conversion, and decrypt the media (potentially exposing sensitive data). When you lock media, you can choose the specific restriction.
Monitor	*Monitor* means to notify the user when someone tries to access the drive. A warning message that the file is being accessed pops up immediately to any user currently logged in and to the user who triggered the monitored event.
Log Write Access	*Log Write Access* means to track writing to media in a log file. The log file is called `wr.log` and resides in the UserData folder of SecureDoc. It contains the date the data was written and to which file, the sector modified, and the name of the logged on user.

Disk access control can be used, for example, to:

- block all write access to a USB drive, thereby preventing data from leaving the device or preventing data being written to it while on the Internet
- block read/write access to a USB drive, thereby preventing others from loading software onto the machine.

This function protects against accidents rather than malicious attacks. If a disk is not encrypted, restricting access to it is not enough — a user could still boot from removable media and bypass the restriction altogether.

Setting up Disk Access Control

Disk Access Control is defined as a profile. SecureDoc comes with a default profile which applies the profile settings determined by your administrator.

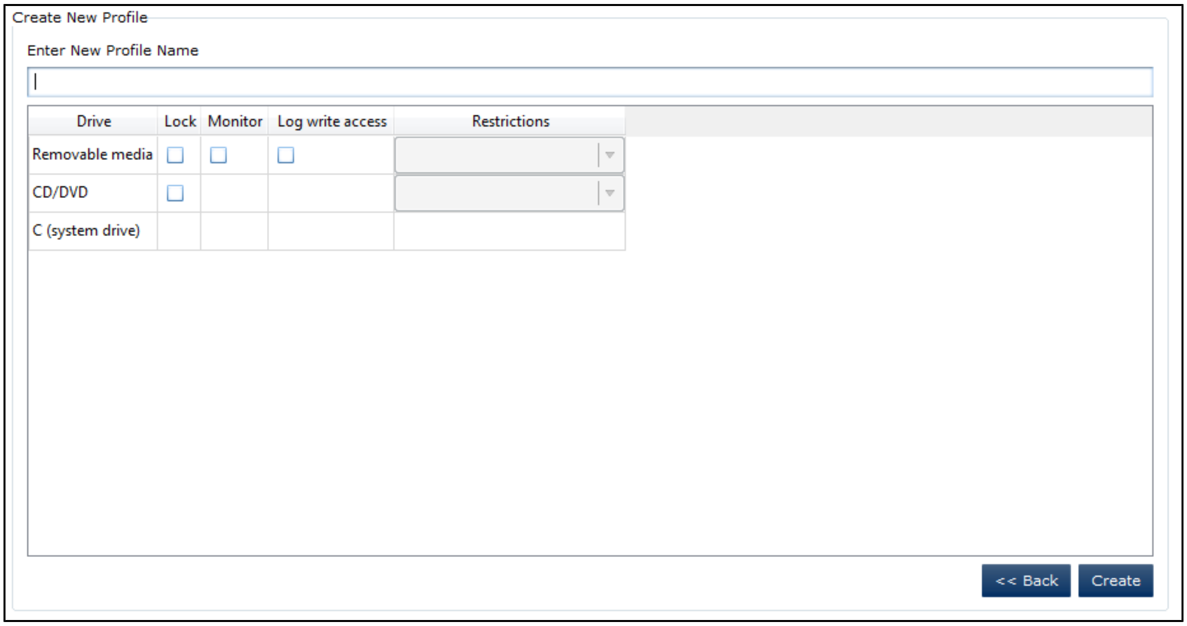
To modify the default profile:

1. From the Control Center, click **Tools**, then **Disk Access Control**.
2. On the Profile Options tab, click **Edit**.
3. Follow the instructions as for a new profile.

To create a profile:

1. From the Control Center, click **Tools**, then **Disk Access Control**.

2. On the Profile Options tab, click **Create New Profile**.



Create New Profile

Enter New Profile Name

Drive	Lock	Monitor	Log write access	Restrictions
Removable media	□	□	□	
CD/DVD	□			
C (system drive)				

3. Enter a name for the profile.
4. On the appropriate row, click one or more control option(s) to be applied. For example, click in the **Monitor** column of the removable media row to monitor access to removable media.

   Note: *For users of BlackArmor devices,* ***do not lock*** *those devices.*

   If you chose **Lock**, choose a restriction from the **Restrictions** drop-down list in the appropriate row. The effect of a condition is shown in the following table:

Restriction	Access to Non-Encrypted Disks	Access to Encrypted Disks
Read Only, unless Encrypted	read only	full
No Access, unless Encrypted	none	full
Read Only Access	read only	read only
No Access	none	none

   Note: *Locking write access to an NTFS file system drive will lock both reading and writing, since even opening a document on an NTFS drive will write information to the drive.*

5. Click **Create**.
6. To activate the profile, on the Current Profile tab, click **Select a Different Profile**, then choose it from the list.

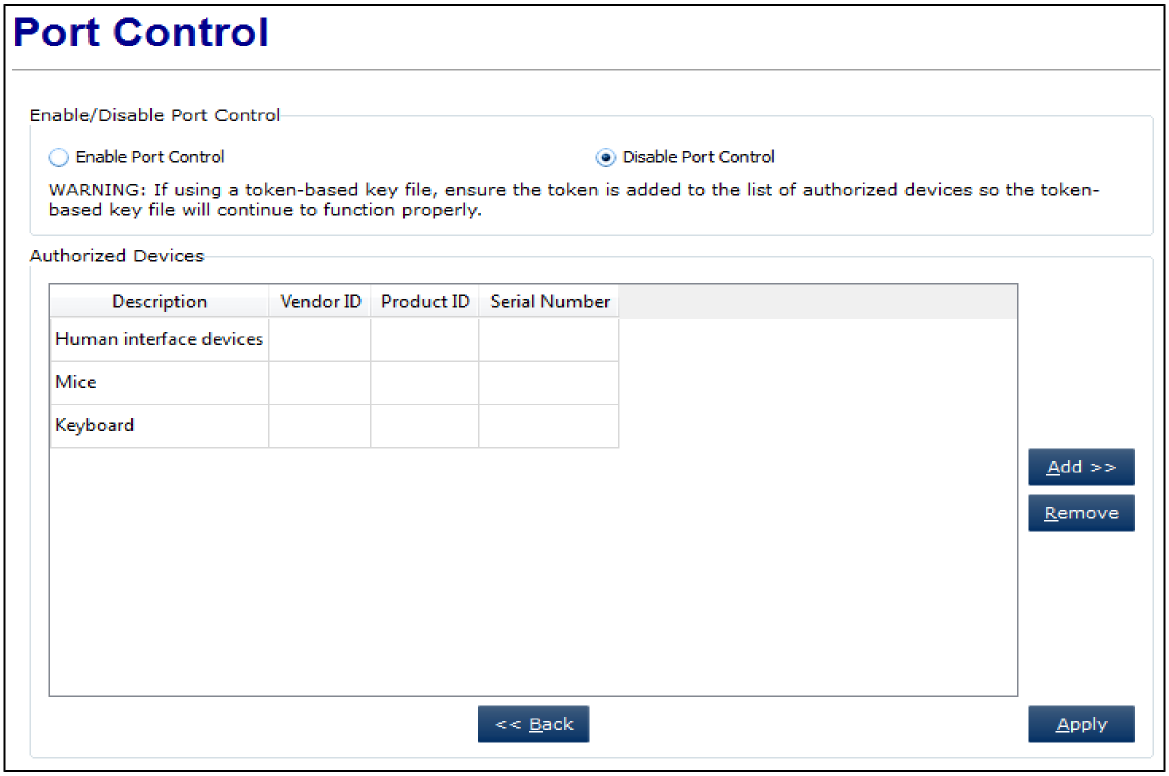
Controlling Use of USB Devices on Computer

You can choose to block all but specific authorized USB devices from being used with your computer. This feature is required for USB storage devices attached to ports: if you enable Port Control, such devices are locked by default until they are authorized through Port Control.

Note: *If you are using a token-based key file and want to use the Port Control feature, you must add your token to the list of authorized devices.*

1. From the Control Center, click **Tools**, then **Port Control**.

2. Click **Install** (necessary only the first time you use this feature). You are prompted to reboot.
3. After rebooting, return to the Port Control screen and click **Manage**. A new screen appears.



Port Control

Enable/Disable Port Control

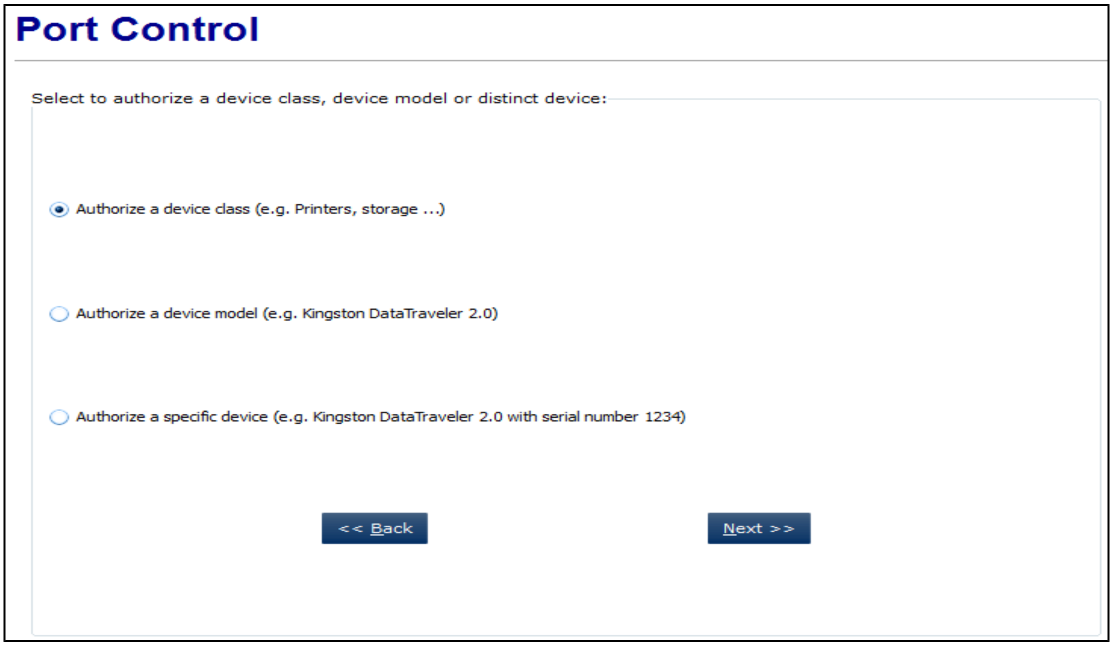
○ Enable Port Control ● Disable Port Control

WARNING: If using a token-based key file, ensure the token is added to the list of authorized devices so the token-based key file will continue to function properly.

Authorized Devices

Description	Vendor ID	Product ID	Serial Number
Human interface devices			
Mice			
Keyboard			

4. If necessary, click **Enable Port Control**.
5. Click **Add**.
6. You are prompted to choose an authorization method.



Port Control

Select to authorize a device class, device model or distinct device:

● Authorize a device class (e.g. Printers, storage ...)

○ Authorize a device model (e.g. Kingston DataTraveler 2.0)

○ Authorize a specific device (e.g. Kingston DataTraveler 2.0 with serial number 1234)

If you choose this authorization…	When you click Next you need to…
device class	Choose a class of devices (e.g. modems). Note that if you then also authorize specific devices, those devices must be of an authorized class in order to be accessible.
device model	Choose from the list of currently and/or previously connected devices to authorize. Authorization is based on the device's vendor ID and product ID. Note that more than one device could have the same IDs as the one you are intending to authorize.
specific device	Choose from the list of currently and/or previously connected devices to authorize. Authorization is based on the device's vendor ID, product ID, and serial number. This uniquely identifies the device.

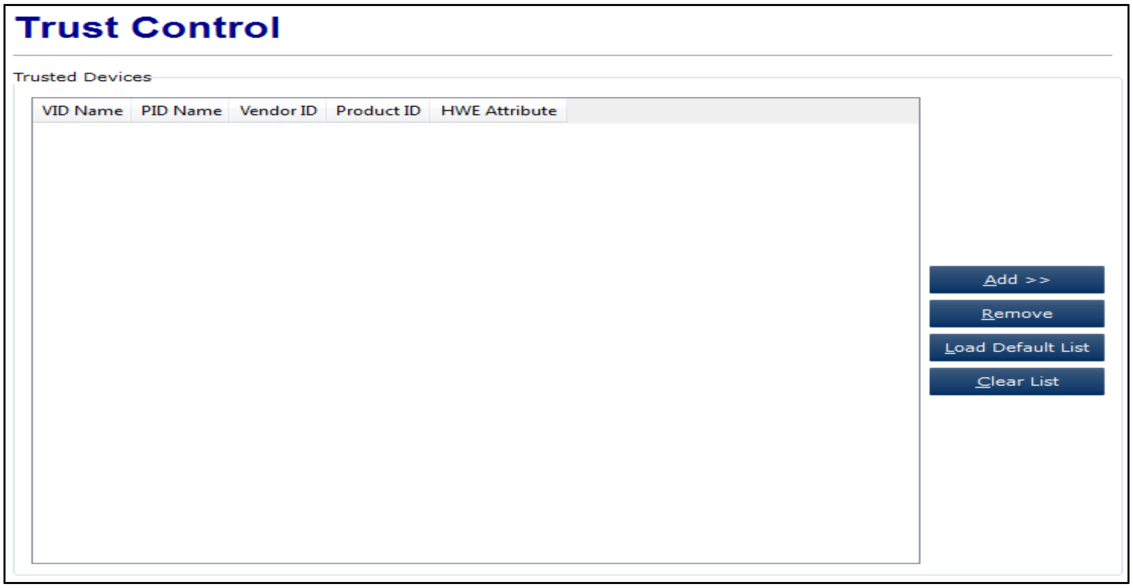
7. Each authorized item is listed on the Port Control screen. You can remove an authorized device if necessary: select it and click **Remove**.
8. When Port Control has been configured to your satisfaction, click **Apply**.

You can disable and/or uninstall Port Control if necessary.

Trust Control

If using Disk Access Control, you can prevent the use of all but specific SEDs on your computer.

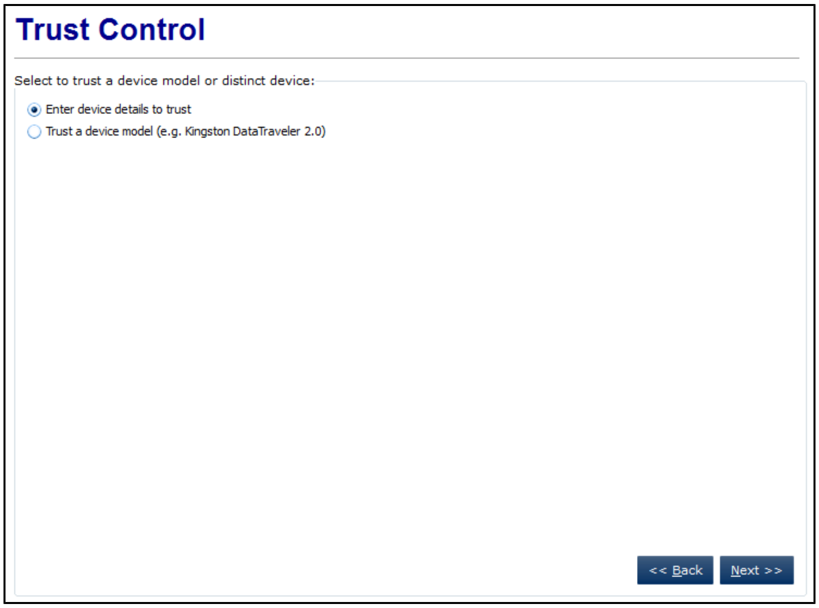
1. From the Control Center, click **Tools**, then **Trust Control**.


Trust Control

Trusted Devices

VID Name	PID Name	Vendor ID	Product ID	HWE Attribute

2. To load the default list, click **Load Default List**. The list is populated with information provided by WinMagic. You can add to this list, remove an item from the list, or clear the entire list.
   To add a specific item, click **Add**. You are prompted to either enter the device details or trust a device model.



Trust Control

Select to trust a device model or distinct device:

● Enter device details to trust

○ Trust a device model (e.g. Kingston DataTraveler 2.0)

3. If you select **Enter device details to trust**, when you click **Next** you are prompted to enter identifying information about the device.
   If you select **Trust a device model**, when you click **Next** you see a list of the device models currently connected to your computer. Select a model and click **Add Selected Device Model**.

Simplifying Login

Synchronizing Passwords

You can choose to synchronize your Windows and SecureDoc key file passwords, so that changes made to either password are automatically made to the other one.

1. In the Control Center, click **Options**, then **General**.
2. Check **Synchronize SecureDoc with Windows password**.
3. Optionally, also check **Synchronize with matching windows Accounts only** to have password synchronization done only if the name of your Windows account is the same as your SecureDoc account name (name of the key file you use to access your encrypted computer).
4. Click **OK**.

Customizing Boot Logon

Making Usernames Case-Sensitive

By default, the username you enter at Boot Logon is not case-sensitive. If you want to make it case sensitive:

1. In the Control Centre, click **Boot Control**, then **Advanced Settings**.
2. On the General Settings tab, choose **User ID is case sensitive**.
3. Click **Apply**. The next time you reboot, the username will require you to enter it considering the case.

Choosing V5 or V4 Loader

SecureDoc includes two Boot Logon versions. By default, SecureDoc is configured to use the V5 loader and, if it fails, use the V4 loader as fallback. If you consistently find the V4 version is needed for your computer (this is rare), you can set SecureDoc to use the older (V4) version of Boot Logon all the time.

Note: *Consult with your administrator before choosing to use the V4 boot loader. It does not support all Enterprise features.*

1. In the Control Centre, click **Boot Control**, then **Advanced Settings**.
2. On the General Settings tab, choose **Use V4 Boot Loader only**.
3. Click **Apply**. The next time you reboot, the V4 Boot Logon will be used.

This function is also available from the Boot Logon Configuration screen: at Boot Logon, press F3, click **Configuration**, then set **Switch back to PBA** to "Yes".

Note: *You can also use this feature to force use of V5 boot loader exclusively or to use the V4 boot loader and V5 as an upgrade (before Boot Logon loads, press "a" to switch to the V4 loader).*

Using UEFI Driver Hook

This option permits the SD Client Administrators to enable / disable the driver binding for UEFI devices. By leaving this option disabled, SecureDoc's own logic will be used to manage such devices, which will work better for devices that do not have full implementations of Driver Binding.

By enabling this option, the assumption is that the devices receiving this profile will have full implementations of Driver Binding for UEFI. UEFI driver binding is special protocol, providing functions for starting and stopping drivers, as well as a function for determining whether a given driver can manage a particular controller.

Note: *By default, the UEFI driver hook is not enabled.*

1. In the Control Centre, click **Boot Control**, then **Advanced Settings**.
2. On the **General Settings** tab, select the **Use UEFI driver hook** checkbox.

Masking Key Input

By default, the user name entered at Boot Logon and answers to any self-help password recovery questions are shown in plain text, while the password is shown in asterisks. You can choose to have all user input to Boot Logon masked.

1. In the Control Centre, click **Boot Control**, then **Advanced Settings**.
2. On the General Settings tab, choose **Mask key file input**.
3. Click **Apply**. The next time you reboot, the masking will be used.

Boot Text and Color

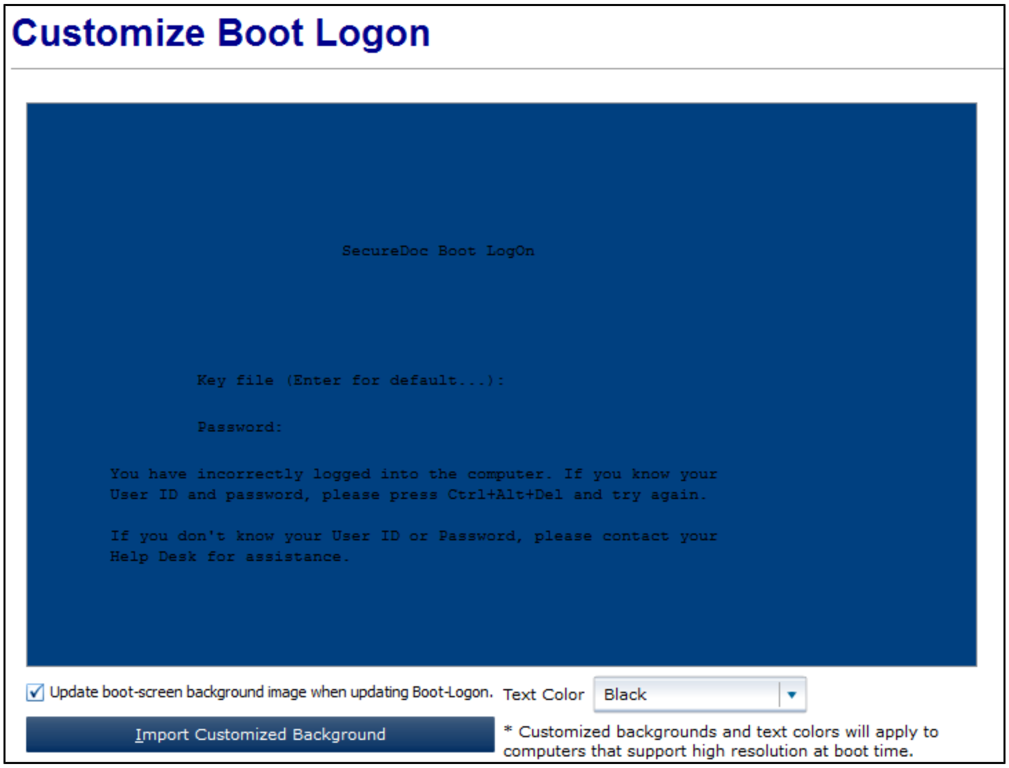
Boot text and color options control the way Boot Logon appears. These options enable you to customize Boot Logon to reflect your personal preferences.

If you plan to use a customized background, the graphic file needs to meet these requirements:

- 24 bit bitmap (.bmp) format
- 1024 x 768 pixels
- when zipped (SecureDoc zips the file for you), no larger than 0.5MB (you will be warned if your file exceeds this size)

Only computers with a high resolution monitor (the most common type) will display the customized logo — other monitors will shown the default Boot Logon display.

1. In the navigation pane, click **Boot Control**, then **Boot Text and Color.**



Customize Boot Logon

```
SecureDoc Boot LogOn

Key file (Enter for default...):

Password:

You have incorrectly logged into the computer. If you know your
User ID and password, please press Ctrl+Alt+Del and try again.

If you don't know your User ID or Password, please contact your
Help Desk for assistance.
```

☑ Update boot-screen background image when updating Boot-Logon. Text Color: Black

Import Customized Background

* Customized backgrounds and text colors will apply to computers that support high resolution at boot time.

2. Choose a text color. The results are previewed.
3. Optionally, click **Import Customized Background** and browse to the location of a graphic file to use as the background for the Boot Logon screen. (See file requirements above.) Check **Update boot-screen background image when updating Boot Logon**: the new background will appear at the next Boot Logon.

Changing Maximum Number of Failed Logins

By default, SecureDoc sets a maximum of 15 failed logins (to Boot Logon). After that maximum number is reached, the key file is automatically locked, regardless of its permissions. An administrator key or password recovery needs to be used to unlock the device. Any time a successful login of another key file takes place, the locked key file will be unlocked and the count begins again. If you want to change the default number:

1. From the Control Center, click **Boot Control**, then **Advanced Settings**.
2. Change the value of **Maximum number of failed logins**.
3. Click **OK**.

Use of Token

If your key file is on a token, you can have Boot Logon look on the token, rather than the hard disk. Optionally, you can have Boot Logon remember the key file on the token last used.

1. From the Control Center, click **Options**, then **General**.
2. Check **Default to use "Key file Token" at boot logon**.
3. Optionally, check **If using "Key file Token" option, remember key file to be used next time.**
4. Click **OK**.

Converting a Key File to TPM Protection

1. From the Control Center, click **Options**, then **General**.

2. Check the **Use TPM chip, if available** option.
3. Reboot your computer and log in as usual to Boot Logon.
4. When you log on to Windows, you will see a message indicating your key file has been successfully converted to TPM protection.
5. From now on, when you access Boot Logon, you will see an indication that it is accessing TPM.

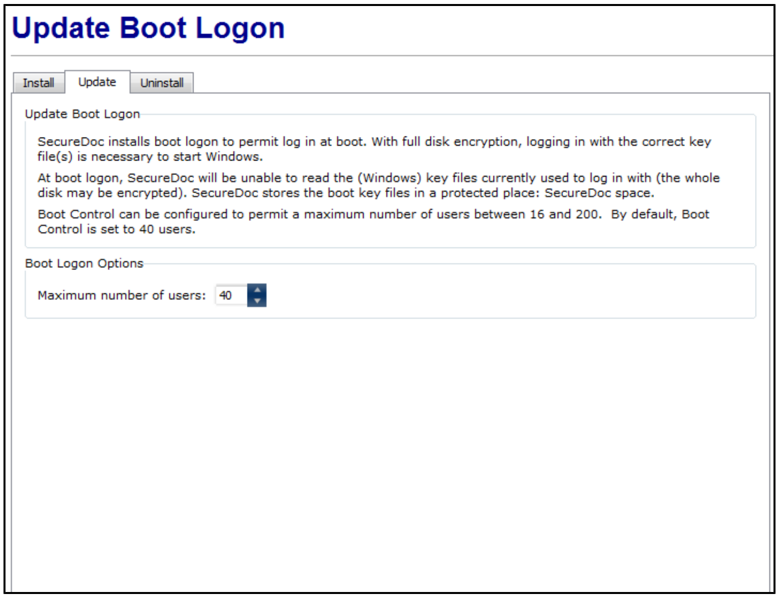
Hiding SecureDoc Icon from System Tray

1. From the Control Center, click **Options**, then **Advanced Options**.
2. Check the **SecureDoc icon will not appear in system tray** option.

Controlling Number of Users of Boot Logon

Use this function to change the maximum number of users of Boot Logon on this machine

1. In the navigation pane, click **Boot Control**, then **Install/Uninstall Boot Logon**, then the Update tab.



Update Boot Logon

SecureDoc installs boot logon to permit log in at boot. With full disk encryption, logging in with the correct key file(s) is necessary to start Windows.

At boot logon, SecureDoc will be unable to read the (Windows) key files currently used to log in with (the whole disk may be encrypted). SecureDoc stores the boot key files in a protected place: SecureDoc space.

Boot Control can be configured to permit a maximum number of users between 16 and 200. By default, Boot Control is set to 40 users.

Boot Logon Options

Maximum number of users: 40

2. Choose the number of users (key files) you want to have access to this computer.
3. Click **Update**. You are prompted to update your recovery media: insert the media used originally during encryption (it will be overwritten with updated information).

Updating Boot Logon

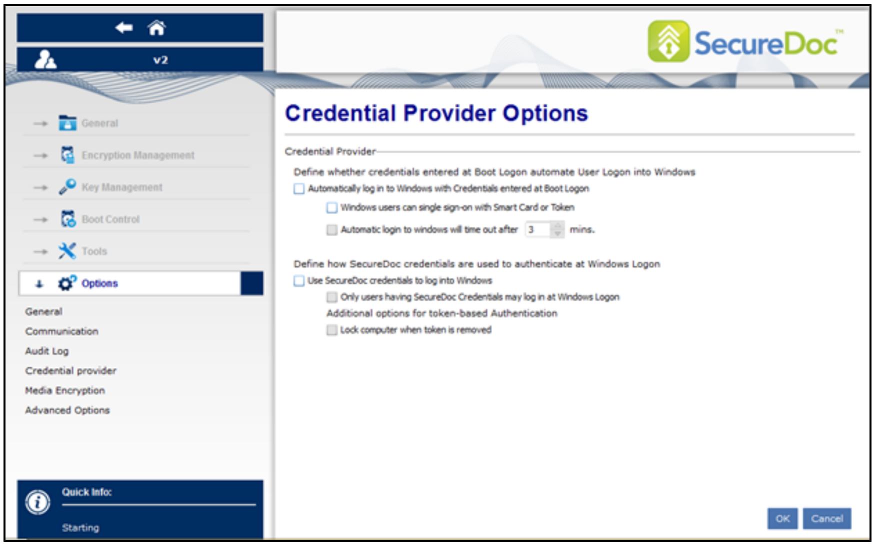
Use this function to change the maximum number of users of Boot Logon on this machine.

1. From the Control Center, click **Boot Control**, then **Install/Uninstall Boot Logon**, then the Update tab.
2. Choose the number of users (key files) you want to have access to this computer.
3. Click **Update**. You are prompted to update your recovery media: insert the media used originally during encryption (it will be overwritten with updated information).

Credential Provider Options

Options in the Credential Provider tab affect the way Boot Logon functions on all Vista/Windows 7/Windows 8 client devices that are controlled by the settings encapsulated within the device profile.

To access the Credential Provider Options screen, open the SecureDoc Control Center, select Options tab on the left menu, then click Credential provider.



Credential Provider Options

Credential Provider

Define whether credentials entered at Boot Logon automate User Logon into Windows

☐ Automatically log in to Windows with Credentials entered at Boot Logon

☐ Windows users can single sign-on with Smart Card or Token

☐ Automatic login to windows will time out after 3 mins.

Define how SecureDoc credentials are used to authenticate at Windows Logon

☐ Use SecureDoc credentials to log into Windows

☐ Only users having SecureDoc Credentials may log in at Windows Logon

Additional options for token-based Authentication

☐ Lock computer when token is removed

Setting Credential Provider Options

The following table describes the options:

Options	Description
Automatically log in to Windows with credentials entered at boot logon	Check to have Windows login information stored so that logging into boot logon automatically logs users into Windows as well (single sign-on). Set the amount of time to wait before timing out automatic login.
Automatically log in to Windows will time out after x mins (Optional)	Automatically login to windows will time out after x mins.
Windows users can single sign-on with Smart Card or Token	This functionality allows you to permit and manage Single Sign-on (SSO) when using Smart-Cards or Tokens. Having authenticated with a Smart Card or Token, the user's underlying credentials will be accessed and utilized to complete the single sign-on process, transitioning the user into the Windows desktop directly without requiring further authentication.
Use SecureDoc Logon credentials to log into Windows	Only users having SecureDoc credentials may login at Windows login
Lock computer when token is removed (token-based keyfiles)	Check to ensure that only users with SecureDoc credentials can access the system. – check to have SecureDoc screen lock take effect whenever the token is removed and to require users to insert their token to dismiss screen lock.

Chapter 4

Maintenance Troubleshooting

Windows 8 Refresh/Reset Behavior

Windows 8 Refresh/ Reset will have different behaviors with SecureDoc.

- Refresh in Windows - Encrypted refresh, machine is still encrypted.
- Reset in Windows - Encrypted Reset. Machine is still encrypted after reset.
- Reset to Plain Text - This can be done by pressing F11 at PBU, and clicking yes on the following page. At this point the machine will remove PBU.
    - It will load Windows Recovery > WinRE > User can reset to plain text

Recovering from a Lost Password

If your administrator has set up your key file for password recovery, when you click **Forgot Password?** you may see one or two new buttons offering ways to recover the password.

Self-Help Password Recovery

1. Click **Self-Help Answer**.
2. Answer the correct answers to the questions that appear, using the answers you used when you created the key file.

    Note: *The text you type may be visible, or may appear as asterisks, depending on the option setting (see "Masking Key Input" on page 30).*

3. Click **Login**. The answers are compared to those you gave at installation or changed since then (see "Changing Your Self-Help Answers " on page 35). If you answered any of the questions incorrectly, you are returned to the screen to try again. If you successfully answered all of the questions, Windows starts up as normal. You are immediately required to assign a new password and password hint.

Challenge-Response Password Recovery

1. Contact your SES administrator and answer the password recovery questions they ask you.
2. Reboot, enter your user ID, then click **Forgot Password?** and **Challenge Response**.
3. A new screen opens.
4. Read your administrator the challenge text you see. The administrator will read you a response number.
5. Enter the response number in the **Respons**e field and click **Login**. If the response number is entered correctly, your computer continues to boot.
6. Once the operating system loads, you are prompted to change your password.

Using Rescue and Recovery (Lenovo Devices)

If you use this utility to create a custom disk image that includes a service partition, that service partition must be at least twice as large as the required contents to allow Rescue and Recovery to back up the partition. If there is not enough space available in the service partition, the Rescue and Recovery backup process will warn you that the available disk space is insufficient for the backup. If this happens, accept the warning: all partitions will be successfully backed up, except the service partition.

Changing a Key File Password

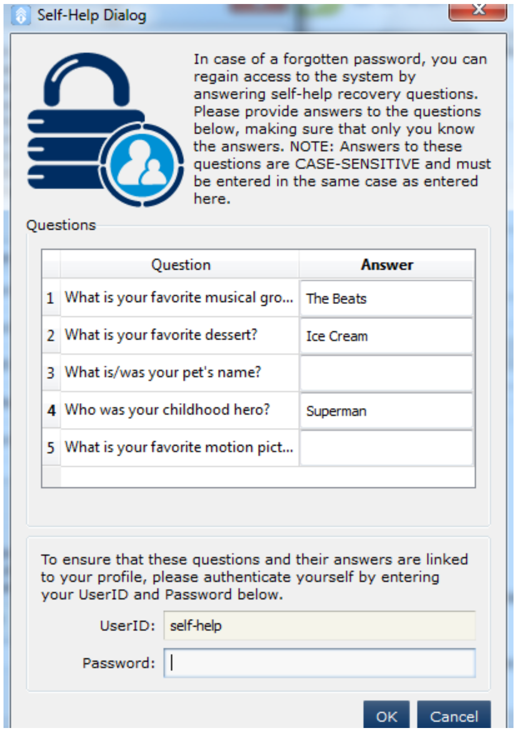
This function applies only to key files to which you are logged on.

1. In the Control Center, click **General**, then **Start Page**, then (available only when Boot Logon has been installed).
   or
   In the Control Center, click **Boot Control**, then **User Management**, select a user and click **Change Password.**
   The Change Key file Password screen appears.
   or
   From Boot Logon, check **Change Password**.
2. Enter your **Old Password** to the current key file, then enter and confirm the **New Password**.
3. If the key file was created using password rules that allow a password hint, enter or change a **Password Hint** that can help you recall a password.
   To view the password rules in effect for your key file, click **Password Rules**.
4. Click **OK**.

Changing Your Self-Help Answers

This function is available only to key files set up for self-help answers, and to which you are logged on.

1. In Control Center, click **General**, then **Start Page**.
   or
   In the Control Center, click **Boot Control**, then **User Management**, select a user with a key file that has self-help answers in it and click **Change Self-Help Answers.**
2. Click . The Self Help screen appears, showing only the questions to which an answer was originally given.
3. Click in any row to enter a new answer. Note that whether or not those answers appear in plain text depends on the option setting (see “Masking Key Input” on page 30).



Self-Help Dialog

In case of a forgotten password, you can regain access to the system by answering self-help recovery questions. Please provide answers to the questions below, making sure that only you know the answers. NOTE: Answers to these questions are CASE-SENSITIVE and must be entered in the same case as entered here.

Questions

	Question	Answer
1	What is your favorite musical gro...	The Beats
2	What is your favorite dessert?	Ice Cream
3	What is/was your pet's name?	
4	Who was your childhood hero?	Superman
5	What is your favorite motion pict...	

To ensure that these questions and their answers are linked to your profile, please authenticate yourself by entering your UserID and Password below.

UserID: self-help

Password:

4. Enter the UserID and password for the key file.

5. The answers you gave at installation are displayed. Click in the answer field and enter a new answer. Keep in mind that answers are case-sensitive: when recovering your password, you will need to enter answers exactly as entered here.
6. Click **OK**.

Working with Recovery Media

Creating Recovery Media

1. In Control Center, click **General**, then **Start Page**, then + (available only once Boot Logon has been installed).
   or
   In Control Centre, click **Drive Encryption**, then **Create Recovery Media**.
2. You are prompted to specify the path where the recovery media will be created.

Using Recovery Media

WinMagic has never experienced a case when recovery media was needed (probably because hard disks are very reliable and SecureDoc does not let applications overwrite its information). However, we have experienced improper use of recovery media, such as using outdated media or media created for another computer, in which case the boot disk is no longer accessible. We strongly recommend you contact WinMagic Technical Support before using the emergency disk.

To use recovery media, insert it and change your BIOS settings to boot from the USB.

Note: *It is vital that the recovery media used in this procedure was created for the specific machine on which this procedure will be performed.*

Recovery Media for Self Encrypting Drives (SEDs)

Note: *For SED users only.*

You must have the Create Emergency Disk privilege to perform the following function.

To export:

1. In Control Center, click **Boot Control**, then **Import/Export FDE Recovery Info**, then the Export tab.
2. Browse to the location where the recovery information is to be stored and enter/confirm the password. You will need the password to import the key file, which contains the files HWEkeyfile.dbk and SDHWE.enc.

To import:

1. In Control Center, click **Boot Control**, then **Import/Export FDE Recovery Info**, then the Import tab.
2. Browse to the location where the recovery information is stored and enter the password.

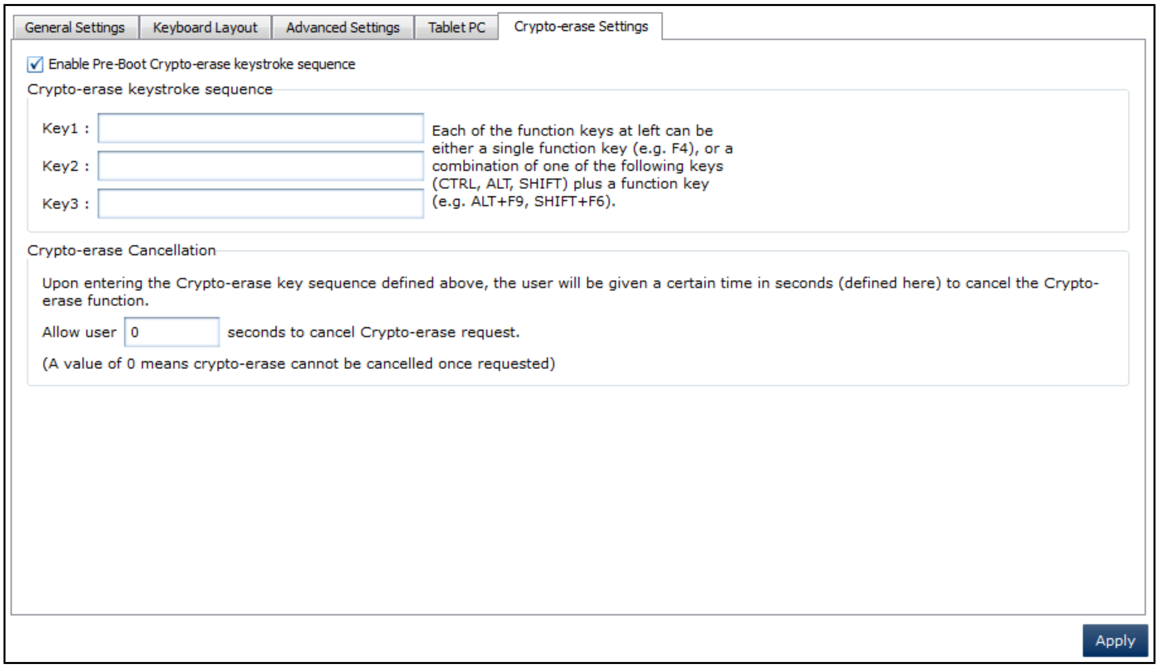
Working with Crypto-Erase

About Crypto-Erase

Note: *Crypto-erasing a device removes the encryption keys from it, **rendering it inaccessible**.*

Setting up Crypto-Erase

1. In Control Center, click **Boot Control**, then **Advanced Settings**.
2. On the Crypto-erase Settings tab, check **Enable Pre-Boot Crypto-erase keystroke sequences**.



☑ Enable Pre-Boot Crypto-erase keystroke sequence

Crypto-erase keystroke sequence

Key1 :

Key2 :

Key3 :

Each of the function keys at left can be either a single function key (e.g. F4), or a combination of one of the following keys (CTRL, ALT, SHIFT) plus a function key (e.g. ALT+F9, SHIFT+F6).

Crypto-erase Cancellation

Upon entering the Crypto-erase key sequence defined above, the user will be given a certain time in seconds (defined here) to cancel the Crypto-erase function.

Allow user 0 seconds to cancel Crypto-erase request.

(A value of 0 means crypto-erase cannot be cancelled once requested)

3. Specify the three key strokes to be used for this purpose. Supported keys are Function keys (F1, F2, etc.), alone or in conjunction with the Shift, Ctrl, or Alt key. For example, the sequence could be SHIFT+F1, CTRL+F2 and F3.
4. To allow time to cancel the Crypto-erase function, enter the number of seconds of delay before the Crypto-erase will be carried out. During this time, if the sequence is re-entered, the Crypto-erase is cancelled.
5. Click **Apply**.

Crypto-Erasing Your Computer

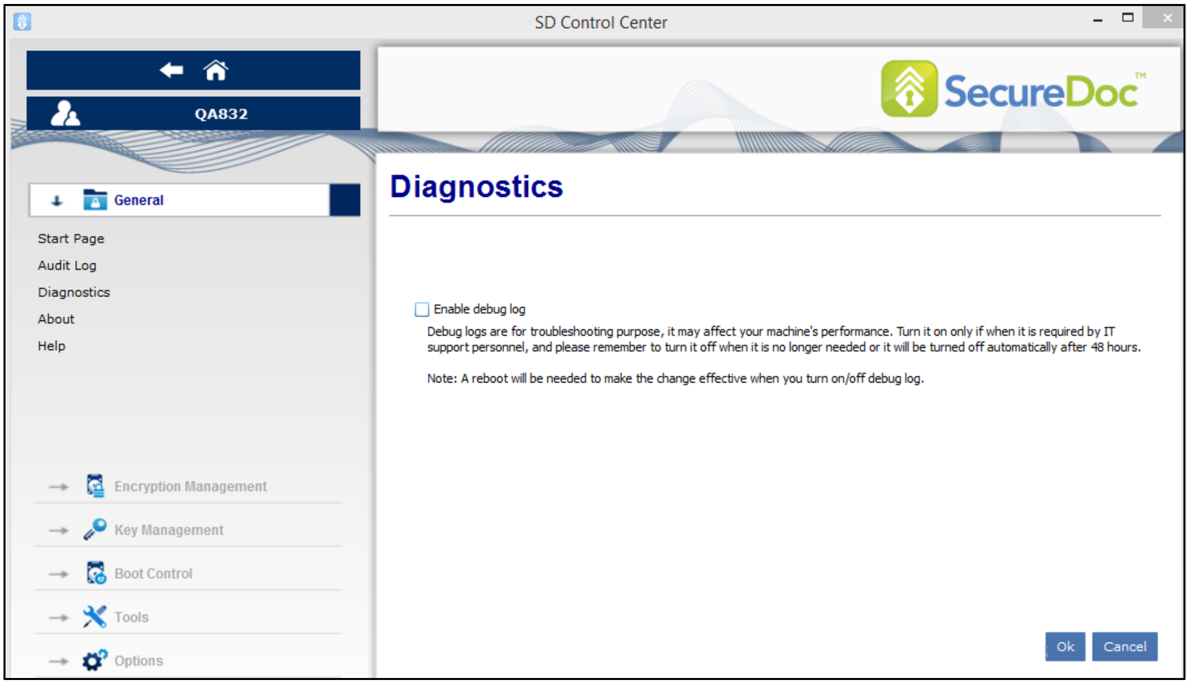
At pre-boot or after Windows has started, you can Crypto-erase your computer by pressing the defined key sequence. This takes effect immediately. If done at pre-boot, login will be denied. If done after Windows has started, Windows will crash as soon as the sequence is entered. Depending on your settings, you may be able to cancel the Crypto-erase.

Crypto-Erasing a SED

1. In Control Center, click **Drive Encryption**, then **Encryption Management**.
2. Select the box representing the SED you plan to crypto-erase.
3. Click **Crypto-Erase**.

Diagnostics

The "Diagnostics" screen in SecureDoc Control Center provides a regular (non-admin) user with the ability to enable detailed logging in the SecureDoc Client environment. This will normally only be needed when requested by WinMagic SecureDoc technical support, to provide detailed log information for analysis. Once enabled, because of the additional load that detailed logging places on the computer, this feature is designed to disable itself automatically after 48 hours, on the assumption that two days of detailed log information should normally provide adequate additonal information to aid in troubleshooting.



Diagnostics

□ Enable debug log

Debug logs are for troubleshooting purpose, it may affect your machine's performance. Turn it on only if when it is required by IT support personnel, and please remember to turn it off when it is no longer needed or it will be turned off automatically after 48 hours.

Note: A reboot will be needed to make the change effective when you turn on/off debug log.

Enabling Debug Logs

1. Open SD Control Center.
2. Select the **General** tab on the left menu.
3. Select the **Diagnostics** tab. The Diagnostics screen appears.
4. Select the **Enable debug log** checkbox.
5. Click **OK**.

> ***Note:*** *A reboot will be needed to make the change effective when you turn on/off this checkbox.*

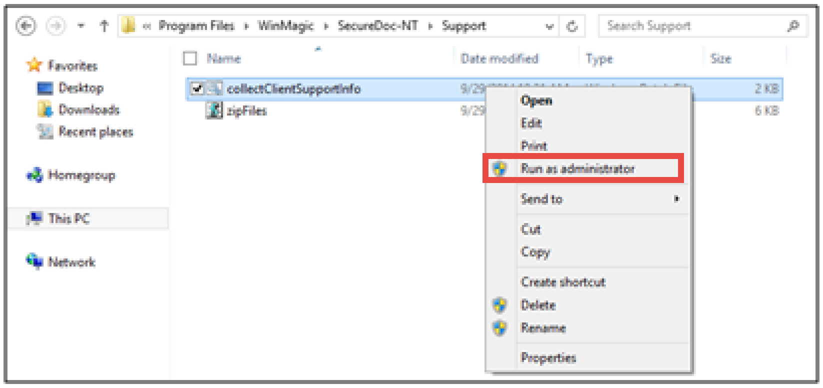
Collecting Support Information and Logs

There may be occasions where, when seeking assistance from WinMagic Technical Support, a support member may request detailed device-level logs to aid in trouble-shooting issues on a given device. SecureDoc offers an easy way to aggregate these logs, after which they can be sent to WinMagic Technical Support.

There exists a batch file named `collectClientSupportInfo.bat` in folder *C:\Program Files\WinMagic\SecureDoc-NT\Support*. This file allows the end-users (upon SES Administrator request) to collect automatically aggregated device-level detail logs. These logs may be required by WinMagic Support to troubleshoot issues on that device.

To collect support information and logs:

1. Go to *C:\Program Files\WinMagic\SecureDoc-NT\Support*.
2. Right-click on the `collectClientSupportInfo.bat` file.
3. Select Run as administrator. A file called `<name>_wmSupportFile.zip` file is created at desktop. The `<name>` is a placeholder for the name of the current user, so this will be replaced with e.g. johndoe_wmSupportFile.zip



Viewing the Audit Log

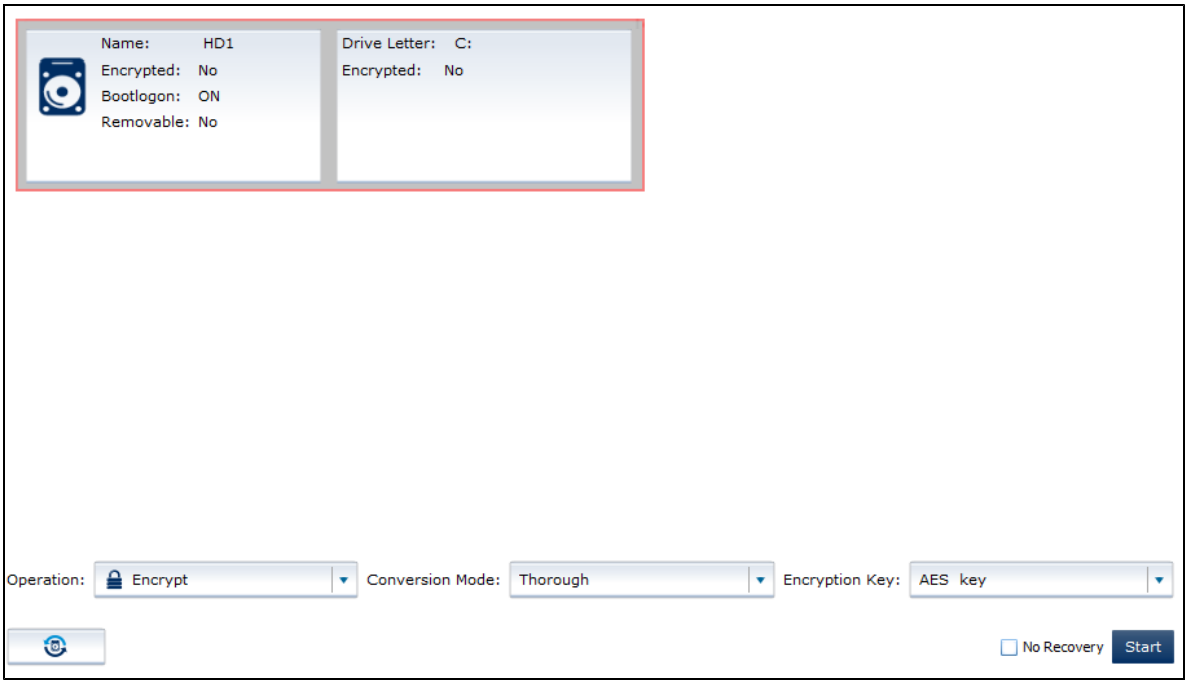
The audit log records actions done in the Control Center, including logging in, installation, and encryption tasks.

1. In the Control Center, click **General**, then **Audit Log**.
2. View the log. You can sort the information by clicking on the column heading.
3. To export the audit log's contents, click **Export Audit File** and choose the location of the exported log.

Viewing Encryption Status

Use this function to get a quick view of all the drives (fixed and removable) you have access to, their encryption status, and whether or not they have Boot Logon installed. You may also be able to use this function to encrypt or decrypt a fixed drive or removable media, or to re-encrypt a fixed disk. Encrypting a fixed disk that is already encrypted does not encrypt the disk twice, but decrypts it and then re-encrypts it with the new key.

In the navigation pane, click **Drive Encryption**, then **Encryption Management**. You see a new screen, with a box for each drive (fixed or removable media) on your computer.



Name: HD1
Encrypted: No
Bootlogon: ON
Removable: No

Drive Letter: C:
Encrypted: No

Operation: Encrypt
Conversion Mode: Thorough
Encryption Key: AES key

The list of drives available for you to encrypt or decrypt uses the following conventions:

- encrypted disks have an "e", and the name of the key used to encrypt them following their name

- hard disks are named HD1, HD2, and so on
- partitions are identified by their drive letter (C:, D:, and so on)

Note: *If you do not see a piece of removable media after you have inserted it, click the refresh button* ⟳.

If you check "No Recovery", then no recovery data is created during the encryption process. This speeds up the encryption process. This option is useful if you need to quickly encrypt a new disk.

Do not select this option if the disk contains critical data.

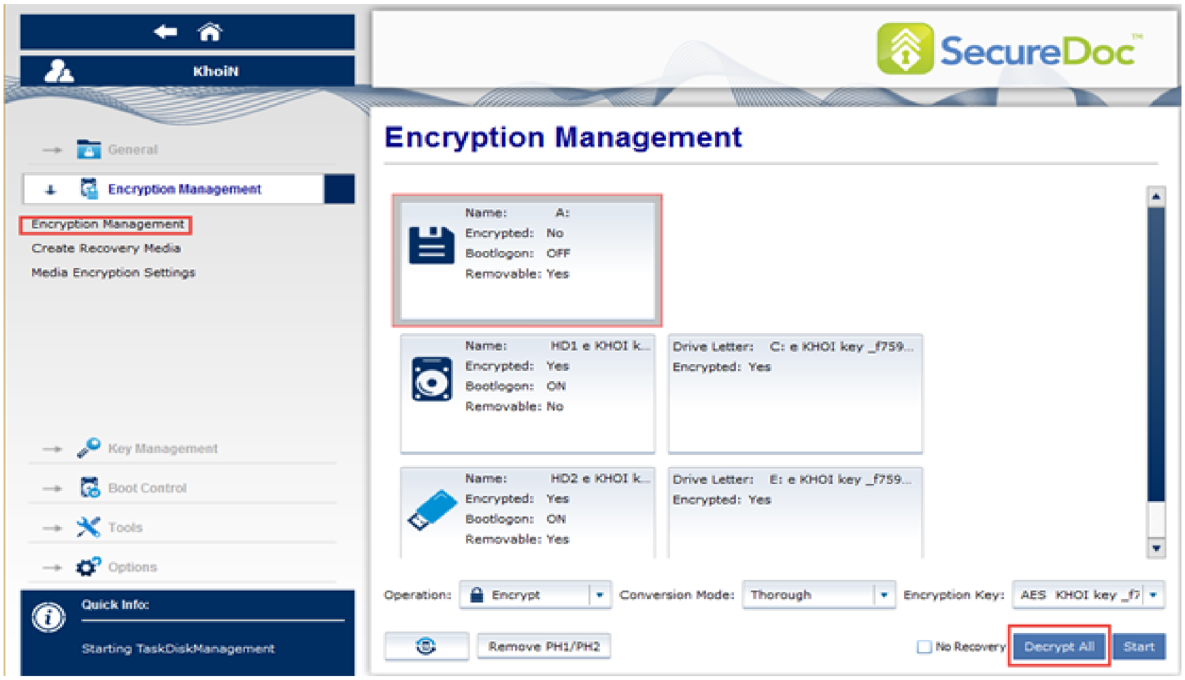
The default setting for this option is set in the installation package. This option is applied for the initial encryption of the disk.

Decrypting / Encrypting ALL Disks

This feature allows the users with Administrator rights to decrypt/encrypt all the device's disks in a single process.

To decrypt/encrypt ALL discs:

1. Open SD Control Center.
2. Select the **Encryption Management** tab.
3. Select the **Decrypt All / Encrypt All** button located at the bottom right of the window. A confirmation message, "*All disks have been set for decryption. SecureDoc Control Center will now terminate*", will appear.
4. Click **OK**.



Encryption Management

Name: A:
Encrypted: No
Bootlogon: OFF
Removable: Yes

Name: HD1 e KHOI k...
Encrypted: Yes
Bootlogon: ON
Removable: No

Drive Letter: C: e KHOI key _f759...
Encrypted: Yes

Name: HD2 e KHOI k...
Encrypted: Yes
Bootlogon: ON
Removable: Yes

Drive Letter: E: e KHOI key _f759...
Encrypted: Yes

Operation: Encrypt
Conversion Mode: Thorough
Encryption Key: AES KHOI key _f7

□ No Recovery

Deleting Temporary Files (PH1/PH2)

This option allows users to delete the temporary files (PH1/PH2) that are generated during encryption process. If the encryption process is disrupted for any reason (e.g. computer shutdown), these PH1/PH2 files will be stored in the respective disks / USBs and may prevent them from being encrypted.

To delete the temporary files, click the **Remove PH1/PH2** button located in the **Encryption Management** screen.

Getting More Information about SecureDoc Control Centre

To view the version and other details, in the Control Center, click **General**, then **About**.

To view online help, in the Control Center, click **General**, then **Help**.

Removing SecureDoc From Your System

Note: *User-created files, including key files, and the SecureDoc folder will not be deleted automatically by these processes.*

To completely remove SecureDoc from your computer:

1. Decrypt all encrypted drives.
2. Uninstall Boot Logon:
   in the Control Center, click **Boot Control**, then **Install/Uninstall Boot Logon**, then the Uninstall tab
   or
   from Boot logon, press F3, click **Configuration**, then click **Uninstall**.
3. Uninstall SecureDoc using the Windows Control Panel.
4. Delete the default folder for SecureDoc Disk Encryption, e.g. C:\Program Files\WinMagic\SecureDoc-NT.

Chapter 5

Working with Removable Media

About Encrypting/Decrypting Removable Media

You can choose to encrypt removable media either using full disk encryption (all contents of the media will be encrypted) or container encryption (only the files and folders you place in a container on the removable media will be encrypted).

Your system may have been configured to automatically encrypt all USB devices and/or removable media, either with or without waiting for a response from you. Consult your administrator for guidance.

You can protect removable media either with a password or a key.

If you use a key, the key used to encrypt removable media may be any of the following:

- the key used to encrypt your hard disk (recommended only if the removable media will either not be shared, or will be shared only with users who you also allow access to your hard disk)
- a specific key you select and may have shared with others (by creating their own key file and importing the key into it)
- the key chosen by your administrator, which may or may not be shared with others (your machine may be set to automatically encrypt)

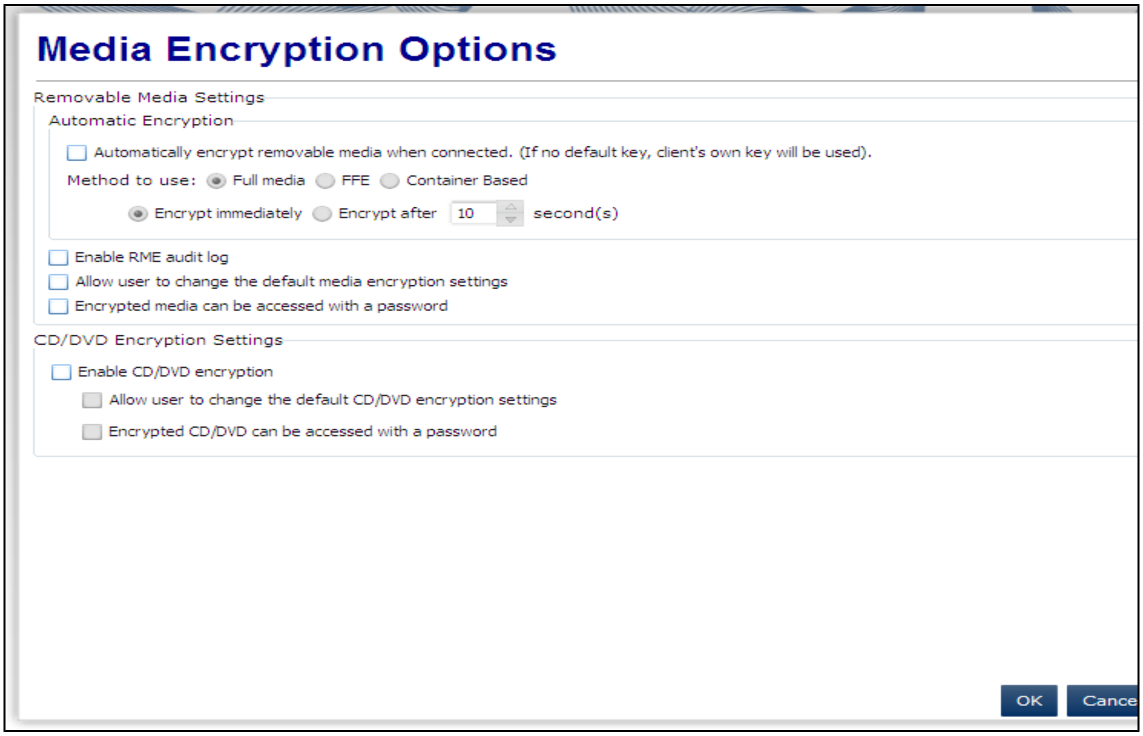
You can allow access to removable media in any of the following ways:

- only to individuals who have the encryption key used to encrypt it and who can login to the key file holding that key
- only to individuals who know the appropriate password
- only to individuals who have access to the certificate you specified at encryption time
- only to individuals with either access to the certificate or who know the appropriate password

Other individuals will need either SecureDoc or the free WinMagic MediaViewer application (along with access to the necessary key or password) to view encrypted removable media.

Setting Removable Media Options

1. On the Control Center, click **Options**, then **Media Encryption**.



Media Encryption Options

Removable Media Settings

Automatic Encryption

□ Automatically encrypt removable media when connected. (If no default key, client's own key will be used).

Method to use: ● Full media ○ FFE ○ Container Based

● Encrypt immediately ○ Encrypt after 10 second(s)

□ Enable RME audit log

□ Allow user to change the default media encryption settings

□ Encrypted media can be accessed with a password

CD/DVD Encryption Settings

□ Enable CD/DVD encryption

□ Allow user to change the default CD/DVD encryption settings

□ Encrypted CD/DVD can be accessed with a password

2. To automatically encrypt removable media with the key you are logged on to when the media is inserted, check the **Automatically encrypt...** option. This option is required for container encryption.
3. Choose the type of encryption you want to use (note that "FFE" encryption is not available). If you choose **Container-based**, specify the percentage of available free space on the removable media that the container is to use. Note that even with a setting of 100%, there will be space available for the media viewer that allows the encrypted media to be accessed on a machine without SecureDoc installed.
4. To enable the removable media audit log, check **Enable RME audit log**. The log is stored locally as USBLogTxt.txt under the SecureDoc installation folder.
5. To be able to override these settings for individual pieces of media, check **Allow user to change the default media encryption settings**. Optionally, check **Encrypted media can be accessed with a password**: you can override this setting on the Media Encryption Settings screen (see “Configuring Removable Media Encryption Settings” on page 43) if necessary.
6. To enable encryption of CDs/DVDs, check **Enable CD/DVD encryption** and **Allow user to change the default CD/DVD encryption settings**. Optionally, check **Encrypted CD/DVD can be accessed with a password**: you can override this setting on the Media Encryption Settings screen (see “Configuring Removable Media Encryption Settings” on page 43) if necessary.
7. Click **OK**.

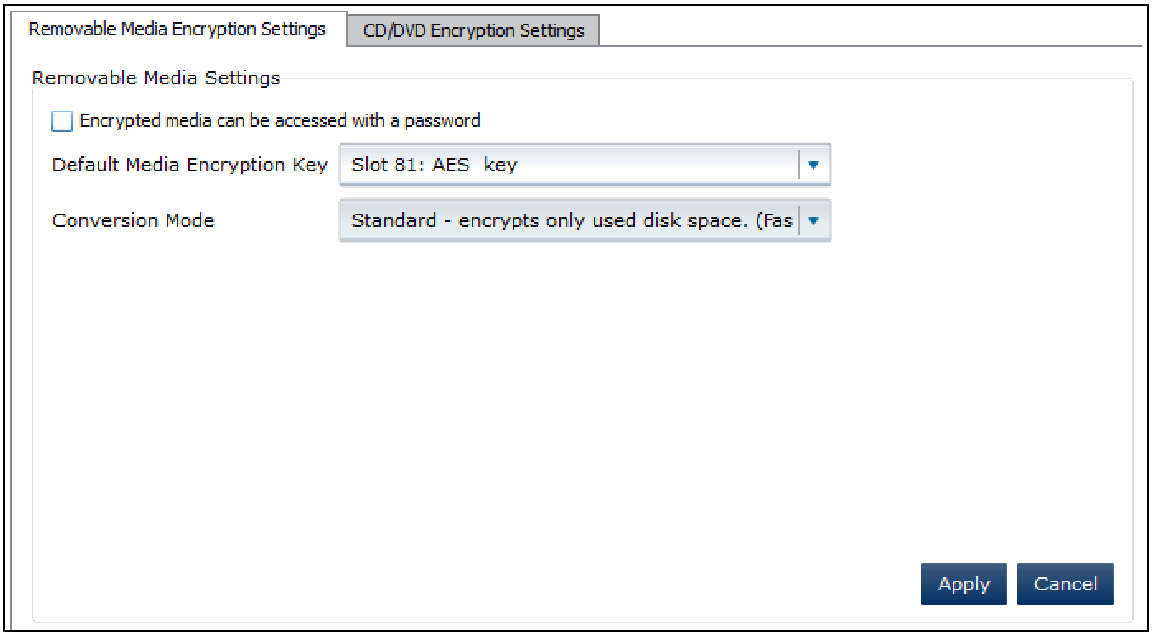
Configuring Removable Media Encryption Settings

Use this function to control encryption of specific removable media and/or CD/DVD. This function is available only once you have enabled it (see “Setting Removable Media Options” on page 42) and provides a way of temporarily overriding the general removable media settings.

Log on to Control Center with the key file containing the key to be used for removable media.

Removable Media Encryption Settings

1. In the Control Center, click **Drive Encryption**, then **Media Encryption Settings**. You see a new screen.


Removable Media Encryption Settings
CD/DVD Encryption Settings
Apply
Cancel

Removable Media Settings

□ Encrypted media can be accessed with a password

Default Media Encryption Key: Slot 81: AES key

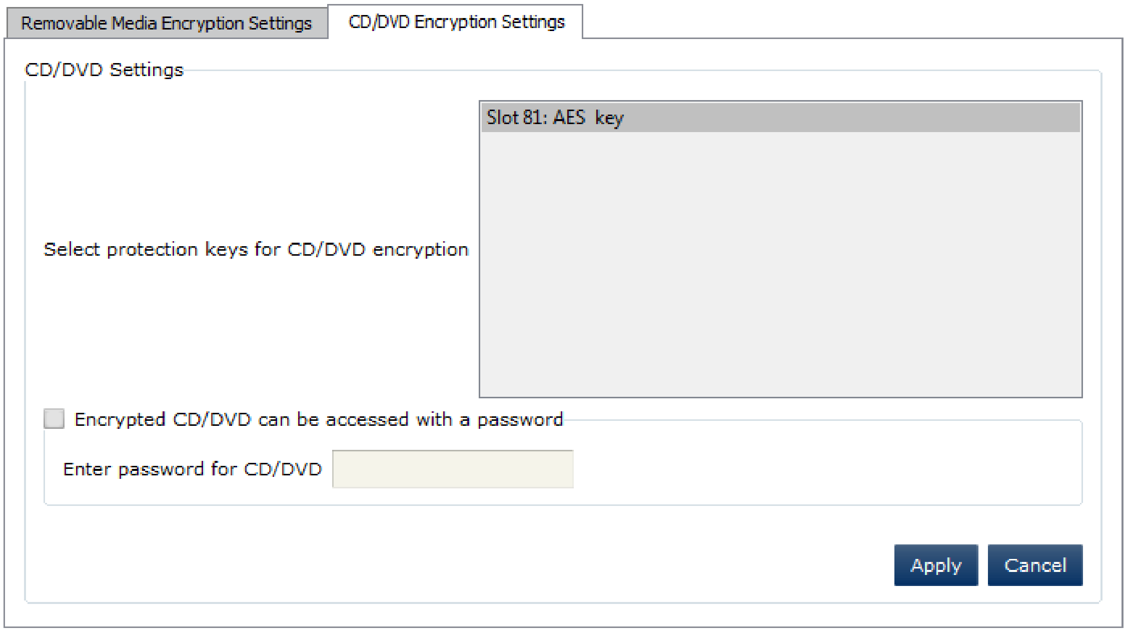
Conversion Mode: Standard - encrypts only used disk space. (Fas

2. Click the Removable Media Encryption Settings tab.
3. Choose how you want users to be able to handle encrypted removable media created on this machine:
   - To have encrypted removable media available only to those who are logged in to a device with SecureDoc installed on it, and who have access to the key used to encrypt the removable media, clear the **Encrypted media can be accessed with a password** option.
   - To have encrypted removable media available to anyone who is logged in to a device with SecureDoc or SecureDoc MediaViewer installed on it, and who knows the password, check the **Encrypted media can be accessed with a password** option (you are prompted for the password when encrypting media). You will need to share this password with other users but those users do not need the encryption key itself.
4. Choose the key and mode to be used to encrypt removable media (it is advisable not to use the key that is used to encrypt your bootable disk) for these purposes.
5. Click **Apply**.

CD/DVD Encryption Settings

Use this function to define the key to be used to encrypt CDs/DVDs. Encryption occurs automatically whenever CDs/DVDs are burned. This option is available only if CD/DVD encryption is enabled (see “Setting Removable Media Options” on page 42).

1. In the Control Center, click **Drive Encryption**, then **Media Encryption Settings**.
2. Click the CD/DVD Settings tab.



Removable Media Encryption Settings | CD/DVD Encryption Settings

CD/DVD Settings

Select protection keys for CD/DVD encryption: Slot 81: AES key

□ Encrypted CD/DVD can be accessed with a password

Enter password for CD/DVD

3. Choose a key to be used for the encryption (it is advisable not to use the key that is used to encrypt your bootable disk).
4. Choose how you want to be able to access encrypted CD/DVDs created on this machine:
   - To have encrypted CDs/DVDs available only to those who are logged in to a device with SecureDoc installed on it, and who have access to the key used to encrypt the removable media, clear the **Encrypted CD/DVD can be accessed with a password** option.
   - To have encrypted CDs/DVDs usable to anyone using a SecureDoc-encrypted device and who has the appropriate password, check the **Encrypted CD/DVD can be accessed with a password** option and enter a password. For security reasons, the CD/DVD password will be erased when the computer is rebooted. Every time you turn on your computer and burn a CD/DVD, you need to enter the password again (or a new password). You may will need to share this password with other users.
5. Click **Apply**.

Working with Removable Media (FDE)

If Automatic Encryption is Enabled

If automatic encryption is enabled (this may have been set up by your administrator), when you insert removable media you will be prompted depending on how this function has been set up. You may be:

- able to remove the media before encryption occurs
- prompted to enter the password for the key used to encrypt the media
- prompted to enter a password that will allow the encrypted media to be accessed on a machine without SecureDoc

If removable media is not set to encrypt automatically, you can encrypt or decrypt it from either the Control Center or Windows Explorer.

CD/DVDs will be encrypted at the same time they are burned.

Working with Removable Media (FDE) Using Control Center

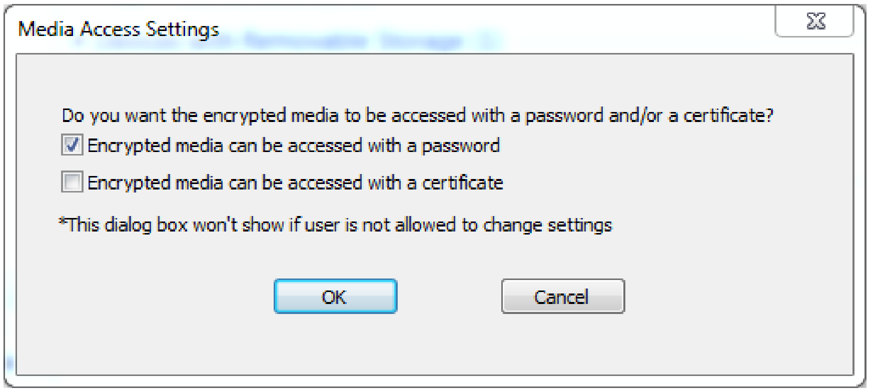
1. Insert the removable media into your computer.
2. Log on to the Control Center using a key file containing the key you want to use to encrypt the removable media.
3. In the Control Center, click **Drive Encryption**, then **Encryption Management**.
4. Select the box for the removable media.

5. Choose the Encrypt **Operation**.
6. Choose a **Conversion Mode** mode (see “Introduction to SecureDoc” on page 8).
7. Choose the **Encryption Key** to be used (one of the keys in the key file to which you are logged in).

Note: *If encryption of the removable media is interrupted, and the media is accessible via password, the password will not be applied, although it can use the Encryption Management feature of the Control Center to apply a password to the encrypted media later.*

Working with Removable Media (FDE) From Windows Explorer

1. Using Windows Explorer, navigate to the removable media you want to encrypt, right-click on it and choose **Encrypt Media**.
2. You are prompted to choose whether to encrypt the removable media with a password (you will be prompted for the password before encryption), a certificate, both, or neither.



Media Access Settings

Do you want the encrypted media to be accessed with a password and/or a certificate?

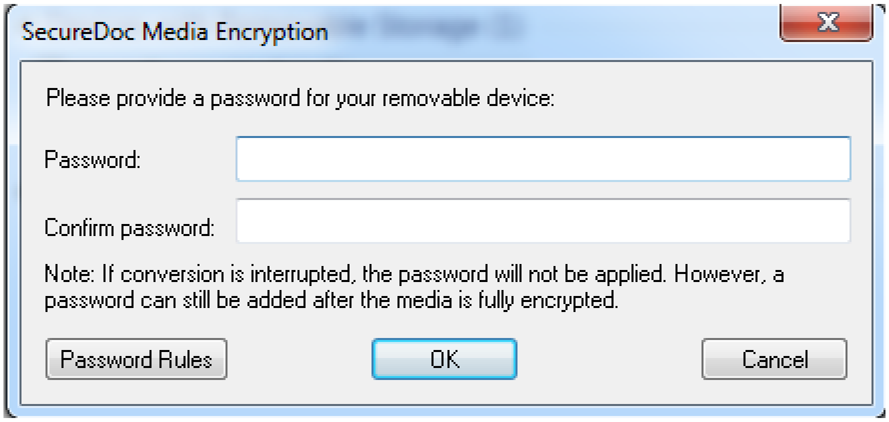
☑ Encrypted media can be accessed with a password

□ Encrypted media can be accessed with a certificate

*This dialog box won't show if user is not allowed to change settings

3. You are prompted to confirm the encryption request.
4. What happens next depends on the choices made:

   - If you chose neither password or certificate protection, encryption begins immediately.
   - If you chose to protect the removable media with a password, you are prompted to choose the password.



SecureDoc Media Encryption

Please provide a password for your removable device:

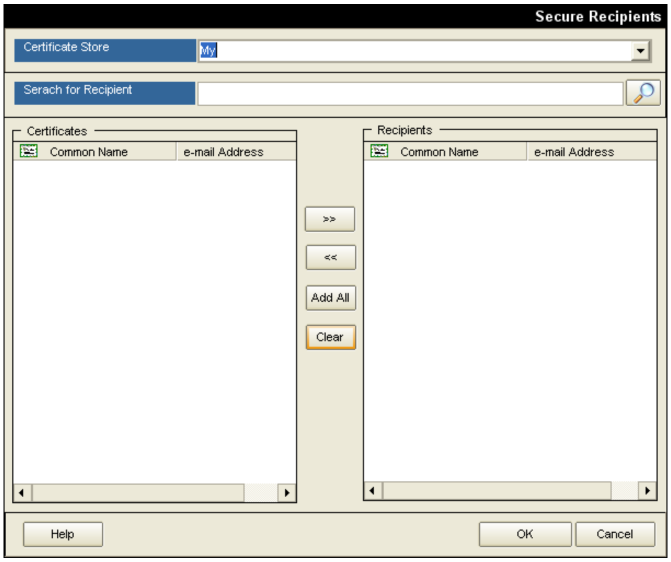
Password:

Confirm password:

Note: If conversion is interrupted, the password will not be applied. However, a password can still be added after the media is fully encrypted.

> ***Note:*** *To see the password rules in effect for this password, click* **Password Rules**.

   - If you chose to protect the removable media with a certificate, you are prompted to choose the certificate from those stored on your machine: choose the appropriate Certificate Store to display the certificates in that store, then add them to the **Recipients** list.



Certificate Store: My

5. If encryption is interrupted, the password (if used) may not be assigned. If this happens, when encryption is complete you can use the Encryption Management feature of the Control Center to apply a password to the encrypted media.

Decrypting Removable Media

Do one of the following:

- In Windows Explorer, right-click on the encrypted removable media and choose **Decrypt Media**. You are prompted to confirm (Windows 32 only).
- In the Control Center Encryption Management screen, select the removable media's box and choose the Decrypt **Operation**.

> ***Note:*** *In order to improve user experience when needing to decrypt media, SecureDoc uses the "fast decryption" option, which in this case means that all sectors that contain data will be decrypted back into Clear-text, but any sectors that are marked as not containing data will remain encrypted (since those sectors are considered to not contain data). This will substantially shorten the time required to decrypt sparsely used media by not requiring the decryption of sectors that do not contain "live" data.*

Accessing Encrypted Removable Media

You must have SecureDoc or the free WinMagic MediaViewer application installed to work with encrypted removable media.

When you insert the encrypted removable media in your computer, you may be prompted for the password of the key used to encrypt it. If the encryption was done using PKI and you have the appropriate public certificate, you will not be prompted for a password.

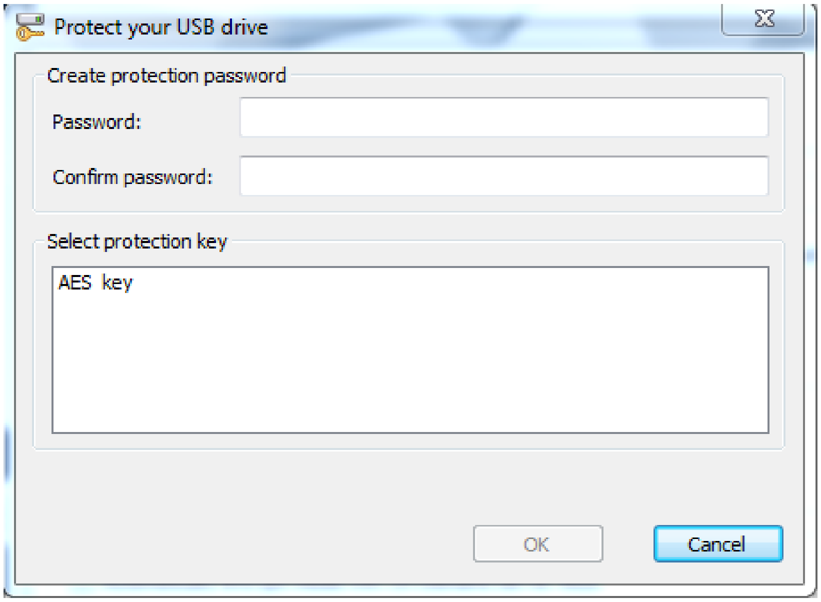
Working with Removable Media Container Encryption

If Automatic Encryption is Enabled

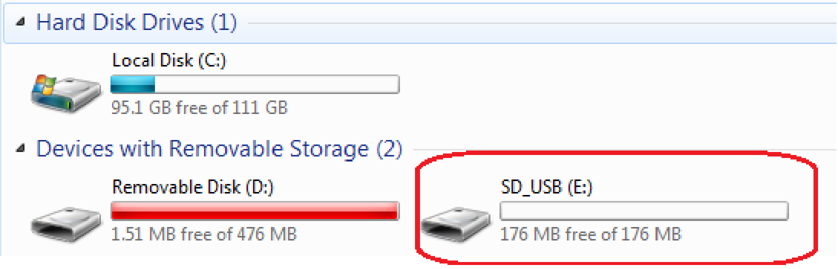
If automatic encryption for container is enabled (this may have been set up by your administrator), when you insert removable media you will be prompted for a password that will allow access to the container from a machine that does not have SD. If a key has not already been associated with the container, you will also be prompted to choose a key.

Creating the Container

When removable media container encryption is enabled, the first time you insert removable media in your computer you will be prompted to create a container.



1. Enter a password (used to access the contents of the container from a computer that does not have SecureDoc installed). Note that the password you set must follow password rules.
2. Choose a key (used to access the contents of the container from a computer that has SecureDoc installed).
3. Click **OK**.
4. Encryption of the container begins (a progress bar is shown).
5. The container is automatically mounted and shown as a separate drive in Windows Explorer.



Mounting and Unmounting Container

Right-click on a container and choose **Un-mount**. The container is closed and only the unencrypted portion of the USB is listed in Windows Explorer.

To mount it again, right-click and choose **Mount encrypted container**.

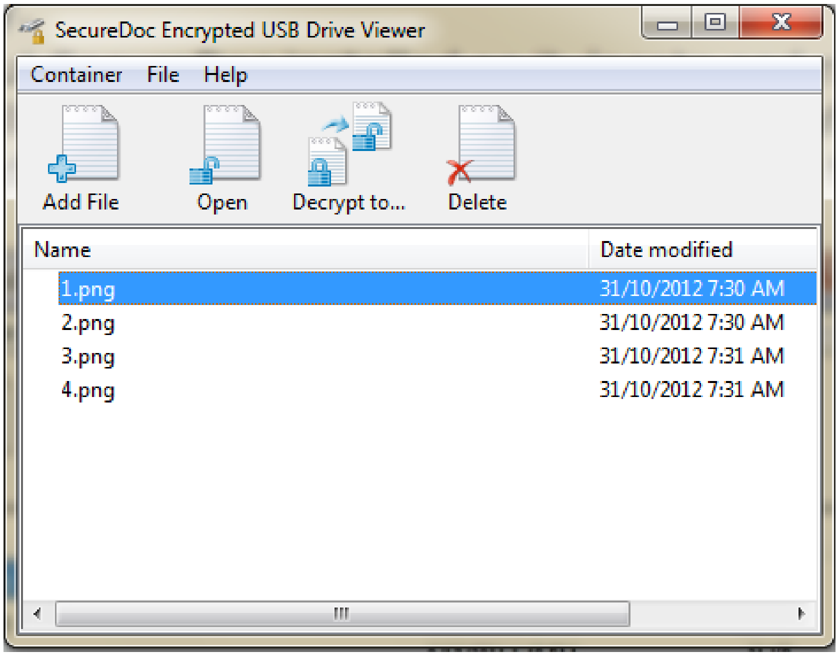
Decrypting Contents of Container

Move or copy files out of the container.

Accessing Container Contents

On a computer with SecureDoc installed, simply insert the USB key. If you are not logged on to a key file containing the key used to encrypt the container, you are prompted for that key.

On a computer without SecureDoc installed on it, locate and run the RMCE Viewer.exe (this was automatically created on the unencrypted portion of the USB when the container was created). The container contents are shown in the viewer window.



Name	Date modified
1.png	31/10/2012 7:30 AM
2.png	31/10/2012 7:30 AM
3.png	31/10/2012 7:31 AM
4.png	31/10/2012 7:31 AM

- To add a file to the container, click **Add**.
- To open a file, select it and click **Open**. Any changes you make to the file are saved back to the encrypted container.
- To decrypt a file, select it and click **Decrypt to**, then choose the destination for the decrypted file.

Removing a Container

Note: *Be sure to back up any data from the encrypted container that you want to retain. Once you remove an encrypted container, all data in that container is lost and cannot be recovered.*

1. Browse the removable media to locate the folder _$SDCE. If you cannot see it, set your folder options to show hidden files, folders, and drives.
2. Delete the folder. All data in the container will be lost.

Viewing the Removable Media Log

If the RME audit log is enabled, this log file tracks removable media functions for removable media under full disk encryption, container encryption, and/or for removable media under file and folder encryption.

The log shows the user who performed the operation, the operation type (create/delete/write/rename), and other useful information.

To view the log, open the USBLogTxt.txt file, located in the SecureDoc installation folder.

Chapter 6

Using File and Folder Encryption

About SecureDoc File and Folder Encryption

Note: *Enterprise users may not have access to this feature or may have a local or networked folder encrypted automatically. Consult your administrator to find out what File and Folder Encryption features have been configured for you.*

Overview

SecureDoc File and Folder Encryption is installed along with SecureDoc, and can be used whether or not your computer has its hard disk encrypted and whether or not Boot Logon has been installed. You will need a key file, however.

This feature can be used to protect folders on the local disk, using any encryption key on the computer.

Once a folder is protected, all users who could normally see the folder can see what files it contains, but to do anything with the folder or its contents, users need both:

- access rights in Windows to the folder
- to be logged in to a key file containing the key used to encrypt the folder.

File and Folder Encryption Rules

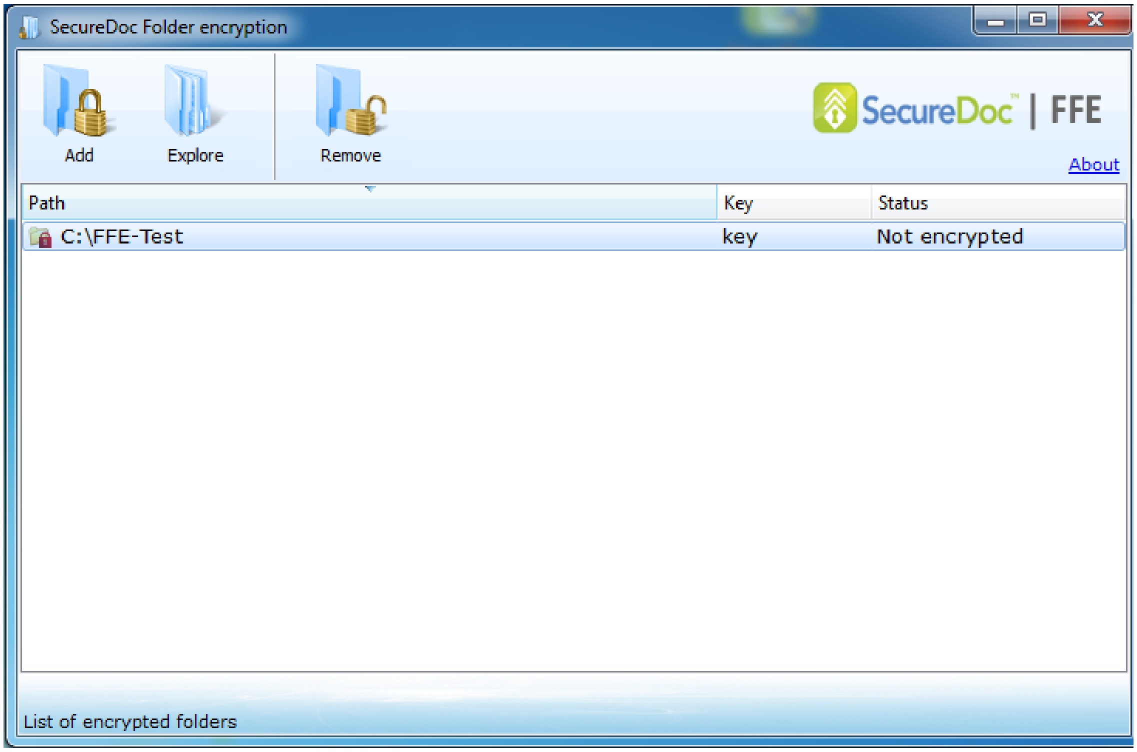
The following general rules apply to SecureDoc File and Folder Encryption:

- Encrypting a folder encrypts everything currently in that folder.
- Anything moved, copied to, or created in an encrypted folder is encrypted automatically.
- If a child folder of an encrypted parent is copied or moved to a parent folder encrypted with another key, the child folder becomes encrypted by that parent's key.
- An encrypted folder or file *copied* or *moved* to an unencrypted location becomes decrypted.

Note: *The above rules do not apply if the movement is within the same partition. If a file or folder is moved from one part of a partition to another part of the same partition, the file's encryption status will not change.*

Encrypting Folders

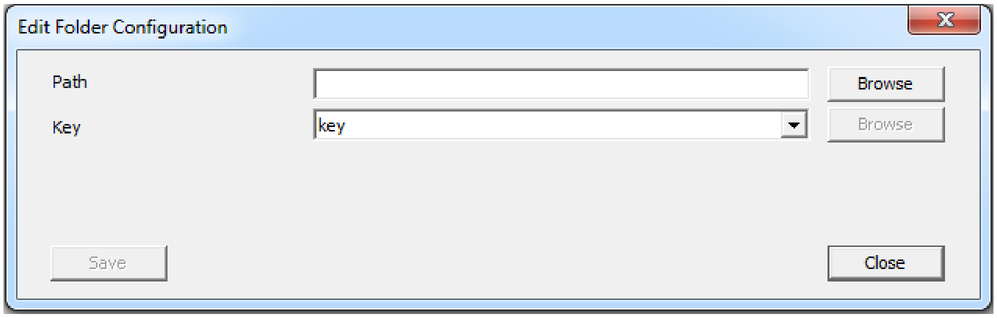
1. Right-click on the SecureDoc icon in the Windows task bar and choose **SecureDoc Folder Encryption**.



Path	Key	Status
C:\FFE-Test	key	Not encrypted

List of encrypted folders

2. A list of folders that are currently protected is shown. For Enterprise users, these may have been configured by your administrator.
3. Click **Add** and navigate to the folder you want to encrypt, choosing the key to be used,



Path:

Key: key

4. To have the change take effect, reboot.

Note: *The SecureDoc Folder Encryption screen shows the status of the folder encryption: encrypted, encrypting, or "unknown" (reboot has not been done).*

Decrypting Folders

Before you remove encryption from a folder, it is advisable to move the files in it to a new, unencrypted folder. To remove encryption from the folder, select it and click **Remove**, then reboot.

Chapter 7

Advanced Functions

This chapter lists features that are to be used only under specific circumstances.

Options for Use Only in Consultation with SES Administrator

The following options should be used only in consultation with the SES administrator:

- Custom Error Message (Options > General)
- Allow to login the boot key file automatically (Boot Control > Advanced Settings > General Settings tab)
- Enable traditional boot logon (Boot Control > Advanced Settings > General Settings tab)
- Simplified sign-on (Boot Control > Advanced Settings > General Settings tab)
- Automatically continue interrupted encryption (Boot Control > Advanced Settings > General Settings tab)
- Communication screen, Audit Log, Certificate Validation (Options)
- On-Demand Key Provisioning and On-Demand Key Requests (Options > Media Encryption)
- Advanced Options (Options)

Options for Use with WinMagic Technical Support

The following options should be used only in consultation with WinMagic technical support:

- MBR access mode (Boot Control > Advanced Settings > General Settings tab)
- Virtual MBR (Boot Control > Advanced Settings > General Settings tab)
- Special BIOS mode (Boot Control > Advanced Settings > General Settings tab)
- Special Y mode (Boot Control > Advanced Settings > General Settings tab)
- all options on the Advanced Settings tab of the Boot Control screen

Chapter 8

For Users of BlackArmor Devices

Introduction

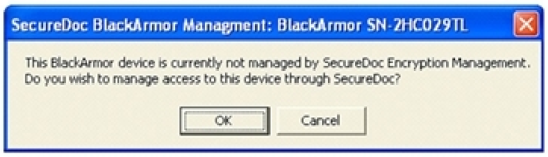
BlackArmor devices are factory-encrypted. You can use SecureDoc to manage such devices, complementing the initial password, if any, assigned to the device with one associated with a digital key.

You can choose to manage BlackArmor devices either automatically or manually:

- Automatic management protects the device with the key you are currently logged on to SecureDoc with or, in an SES environment, the personal key assigned to you. If you are not using Boot Logon, you must create a key for these purposes and log in to it for automatic management to work.
- Manual management protects the device with the key of your choice. The most typical reason for manually managing a device is to share it with others. You may want to create a shared or group key and use it for such purposes.

Automatic Management

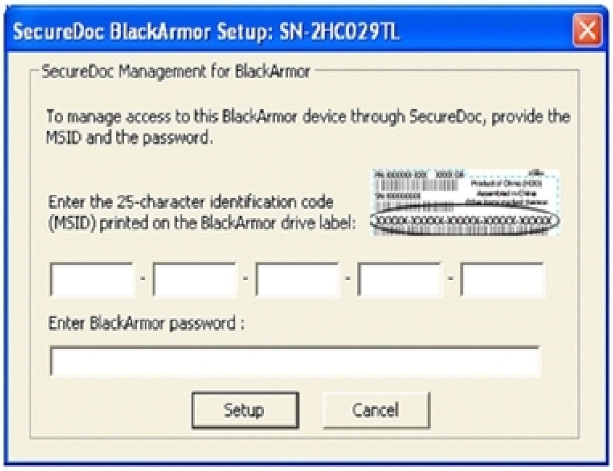
1. Insert the BlackArmor device in the computer. A new screen appears.



SecureDoc BlackArmor Managment: BlackArmor SN-2HC029TL

This BlackArmor device is currently not managed by SecureDoc Encryption Management.
Do you wish to manage access to this device through SecureDoc?

2. Click **OK**. A new screen appears.



SecureDoc BlackArmor Setup: SN-2HC029TL

SecureDoc Management for BlackArmor

To manage access to this BlackArmor device through SecureDoc, provide the MSID and the password.

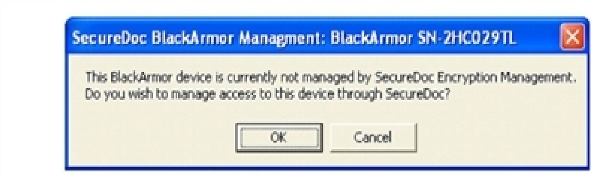
Enter the 25-character identification code (MSID) printed on the BlackArmor drive label:

Enter BlackArmor password :

3. Enter the MSID (located on the back of the BlackArmor device).
4. If the device is in the manufactured state (no password has even been assigned), the password field is disabled.
   If the device has been managed by Maxtor, or was managed by SecureDoc but that management has been removed, enter the most recent password used to manage the device.
5. Click **Setup**. A confirmation message appears.

Manual Management

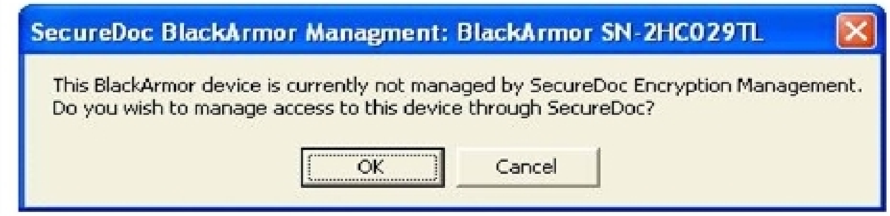
1. Insert the BlackArmor device in the computer. A new screen appears.



SecureDoc BlackArmor Managment: BlackArmor SN-2HC029TL

This BlackArmor device is currently not managed by SecureDoc Encryption Management.
Do you wish to manage access to this device through SecureDoc?

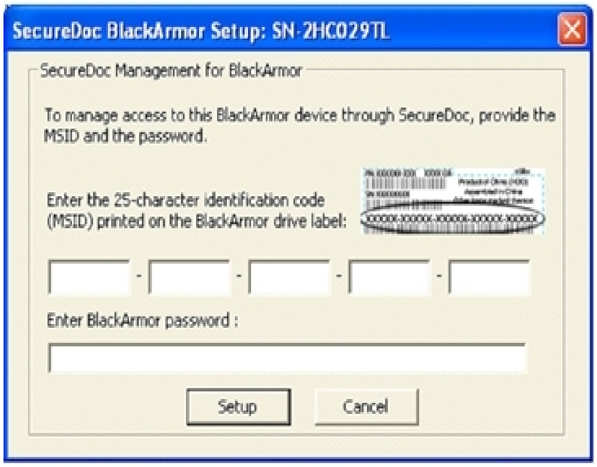
2. Click **Cancel**.
3. Open the Encryption Management screen (in the Control Center, click **Drive Encryption**, then **Encryption Management**).
4. Select the BlackArmor device. It will be named HD2, HD3, or something similar (the hard disk is always named HD1).
5. From the **Action** list, choose **Manage BlackArmor device with key**, then choose the encryption key.
6. Click **Start**. A new screen appears.



SecureDoc BlackArmor Managment: BlackArmor SN-2HC029TL

This BlackArmor device is currently not managed by SecureDoc Encryption Management.
Do you wish to manage access to this device through SecureDoc?

7. Click **OK**.
8. A new screen appears.



SecureDoc BlackArmor Setup: SN-2HC029TL

SecureDoc Management for BlackArmor

To manage access to this BlackArmor device through SecureDoc, provide the MSID and the password.

Enter the 25-character identification code (MSID) printed on the BlackArmor drive label:

Enter BlackArmor password :

9. If the device is in the manufactured state (no password has even been assigned), the password field is disabled.
   If the device has been managed by Maxtor, or was managed by SecureDoc but that management has been removed, enter the most password used to manage the device.
10. Click **Setup**. A confirmation message appears.

Sharing the BlackArmor Device

If you have used a group key to manage the BlackArmor device, that key can unlock the device on any SecureDoc computer that received the group key.

To share the device with computers that do not already have the key used to manage it:

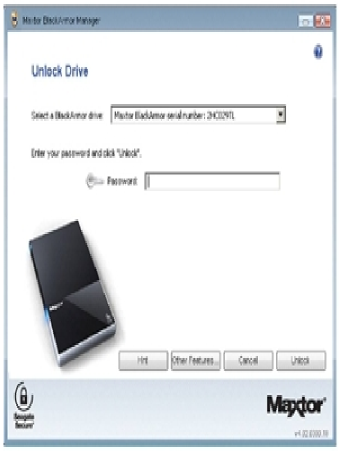
1. Copy the key file whose key manages the device to the computers that are to share that device.

2. On each computer that is to share the device, add the key file (see “Adding Users to This Computer” on page 23)

Using the Managed Device

Once the device has been set up for SecureDoc management, when it is inserted into a SecureDoc machine where the user is logged in to the key used to manage the device, it is automatically unlocked (without a password being required). It may be necessary to wait for up to 30 seconds for the device to be unlocked.

When a SecureDoc-managed device is inserted into a machine without SecureDoc, the password for the key used to manage the device needs to be entered in the Maxtor Manager screen.



Select a BlackArmor drive: Maxtor BlackArmor serial number: 2HC029TL

Enter your password and click "Unlock".

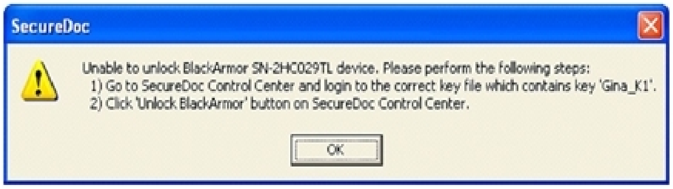
Password:

Handling Unexpected Events

If you attempt to use the BlackArmor device on a machine that does not have SecureDoc on it, you need to know the password for the device. Since normally SecureDoc simply unlocks the device, you may have forgotten this password. To solve this issue:

1. Return to the machine with SecureDoc on it and change the password.
2. Return to the machine without SecureDoc on it and insert the device.
3. When prompted, enter the newly created password.

   If you lose the shared key used to manage the BlackArmor device, you can request it from your SES administrator.
4. SecureDoc will report the name of the key when the device is inserted. For example:



Unable to unlock BlackArmor SN-2HC029TL device. Please perform the following steps:
1) Go to SecureDoc Control Center and login to the correct key file which contains key 'Gina_K1'.
2) Click 'Unlock BlackArmor' button on SecureDoc Control Center.

5. Ask your administrator for the key and copy it to your machine, then add it to your computer (see “Adding Users to This Computer” on page 23).
6. Re-insert the device. It will unlock automatically.

Removing Device from SecureDoc Management

1. Before you begin, be sure you know the password associated with the key file controlling the device. This may either be the password given when the key was created, or the password as changed following the procedure above.
2. Open the Encryption Management screen (in the Control Center, click **Drive Encryption**, then **Encryption Management**).

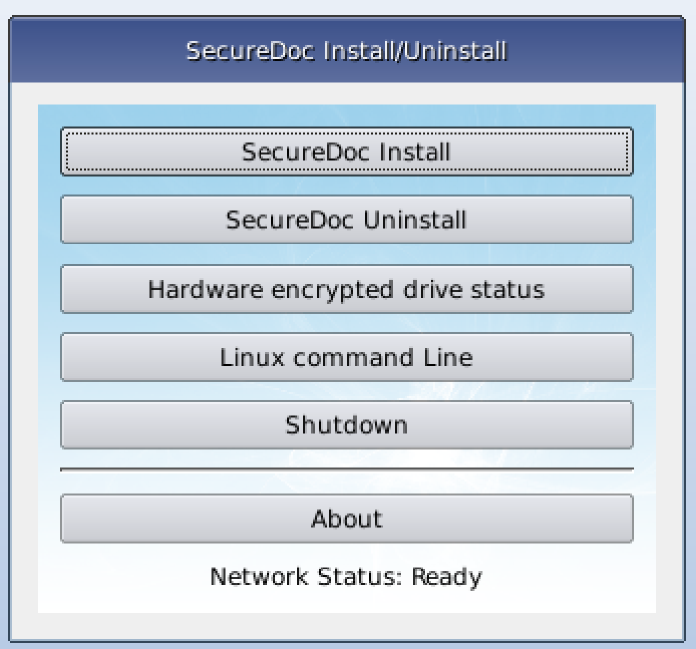
3. Insert the BlackArmor device.
4. Select the device.
5. From the **Action** list, choose **Remove BlackArmor device from SecureDoc management** and click **Start**.
6. A confirmation message appears.

Chapter 9

SecureDoc OSA Users

Installing SecureDoc

1. Boot the SED device from USB or from the PXE server (check with your administrator for which to use).
   The SecureDoc Install/Uninstall screen opens, showing the available menu of options.



Note: *SecureDoc OSA supports English only.*

2. Wait for the Network Status (at the bottom of the screen) to read "Ready".
3. Click **SecureDoc Install**. SecureDoc OSA will try to copy the configuration files locally. If copying fails, you can try this process several times: if it continues to fail, there may be a problem with file/network sharing. Consult your system administrator.
4. If copying is successful, a Registration Computer Form screen opens. Enter the user name provided by your administrator.
5. Modify other field as needed and click **Submit**.
6. You see a confirmation or error messages.
7. Depending on your password rules, you may be prompted to change the initial password.

Encryption will start. A SecureDoc installation in Progress screen will be visible until the installation is completed (approximately 5 minutes).

Changing Your Password

1. At PBA, check the **Change password** option, then enter your username and password and press Enter.
2. You will be prompted to enter a new password (and to confirm it).
3. Click **Save**. A confirmation message appears.
4. Click **OK**.

Uninstalling SecureDoc

1. At PBA, enter your username and password but press F8 (instead of Enter).
   The SecureDoc Boot Configuration Menu opens.
2. Click **Uninstall**.
   You are prompted to confirm.
3. Click **Yes**.
   The screen will remain open for a minute, then the computer will power off. When it restarts, you will no longer see PBA.

Appendix

Appendix A: Password Rules

Password Security Policy

The goal of a policy enforced when passwords are created or changed is to prevent certain types of attack on protected devices. Here are some common attacks:

- Guess Attack — may be successful if personal information like phone number, license plate number, pet's name, etc. is used as a password. Such a password may be easily guessed by anyone who has access to this information.
- Brute Force Attack — may be successful if the password is too short, allowing an attacker to try all possible combinations in a feasible time.
- Dictionary Attack — may be successful if the password is a word of a real language, geographical name, name of a person, etc. Modern information technologies provide capability to find equivalents of such passwords for known authentication mechanisms.

The following rules help prevent these attacks:

- Password must be at least 8 characters long (protects against Brute Force Attack).
- Password must contain at least one character that is a lower-case letter, upper-case letter, digit, or special character (protects against Brute Force and Dictionary Attacks).
- Password hint feature must be disabled (protects against Guess Attack).
- Self-Help Password Recovery feature must be disabled (protects against Guess Attack).

Configure your password rules and key file options so they enforce this policy.

Password Rules Screen

Password Composition

1. In the **Contain at least** area, specify the minimum number of characters and type of characters to be used in a password. Click the arrows or type the appropriate values. Note that:
   - numeric characters are the numbers 0 - 9
   - non-alphanumeric characters are any character except A - Z, a - z, and 0- 9. Non-alphanumeric characters include #,?, !, @, and so on.
2. In the **Contain at most** area:
   - Specify the maximum number of repeated characters allowed in a password. A value of 0 means any number of consecutive characters is allowed—for example, "passsssword" would be allowed. A value of 1 means no consecutive characters are allowed—for example, "password" would not be allowed. A value of 2 means no more than two consecutive letters are allowed—for example, the password "passsword" would not be allowed. However, "PASSsword" would be allowed, because the third "s" is a different case.
   - Specify the maximum number of consecutive characters allowed in common between the old password and a new one. For example, if you specify a maximum of 2 consecutive characters, and the old password was "PASSWORD", a new password of "WORLDMAP" would not be allowed, because there are three consecutive characters ("WOR") in the old and new password. However, "WoRLDMAP" would be allowed, because the "o" is a different case.

General Options

Use these options to set up password expiry. Causing passwords to expire after a period of time increases security since it requires passwords to be changed at regular intervals (people tend to choose from a limited set of possible passwords that may be easily guessed by someone familiar with that person's patterns, or may write down or share their password). Setting password expiry options diminishes these risks.

1. If you are acting as administrator to several users of this computer, to require users to change their password when they first log on to SecureDoc, check the **Change initial password** option. Note that users must have the Modify Password privilege to do this.
2. To set a minimum number of days for which a password must be kept, enter a value in the **Password must be retained for** field. You will be prompted for a new password after that number of days. Alternatively, set **Password will expire in** and indicate the number of warning days. You will be prompted for a new password after that number of days. If you also check the **Enforce password expiry** option, however, the key file will permanently expire when its password expires. Uses will need access to a different key file containing the appropriate encryption key to access media encrypted using the expired key file: use with caution in a single-user environment.

Password Recovery Options

1. To prevent password hints from being available, check the **Disable Password Hint** option.
2. Set the minimum total length of characters used in answers to self-help authentication questions in the **For self-help password recovery…** field.
3. Set the minimum number of questions a user must answer for self-help password recovery in the **For self-help password recovery…** field.

Other Options

1. Set the **Maximum number of passwords to be saved** in the key file's password history. New passwords are checked against the key history file to prevent any duplicates from being created. For example, if you set the history to 5, any new password cannot have been used in the past 5 times the password was changed.
2. If you are using token-based key files, enter a value in the **After a token-based key file's password…** field. When doing password recovery on a token-based key file, a password-based key file is created and used in place of the token-based key file. This option determines how long the user can use the password determined by this process before having to run password recovery again or switch to using a token.

Note: *The password for the actual token can only be changed after the token is authenticated and only if the token vendor supports this functionality. Password rule settings apply to all key files created after the settings have been modified.*

Appendix B: Protection Methods

Method	Description
Method 1: Use Token RSA Keys	SecureDoc uses the RSA keys on the token to protect the key files. During login, SecureDoc uses the entered password to log in to the token. SecureDoc uses the on-token RSA private key to decrypt and encrypt data. Note that you can change the token's password using third-party card management or PKI software; SecureDoc does not have to know that the password has been changed. As long as the entered password can login to the correct token with the correct RSA private key, you can log in to SecureDoc. If the card has been lost and the card management software can create another card and place the same encryption RSA keys on it, you can use the new token to login to the SecureDoc key file.
Method 2: Token contains PIN	If the token does not have encryption capability, use this method. The token is used to store a "strong" PIN of 256 bits, generated randomly at the time of creation. The PIN is used to access the key file. During login, SecureDoc uses the entered password to log in to the token and obtain the PIN stored in the token to access SecureDoc key files. This method changes the tokens, thus is not recommended if the enterprise relies on other third-party card management or PKI systems to manage tokens. For password recovery, the key file cannot be recreated. You need to initialize a new token and create a new key file including the encryption key used to encrypt the user's computer.
Method 3: Use Certificate on token	During login, SecureDoc uses the RSA private key on the token as in method 1. Unlike in method 1, SecureDoc uses the certificate stored on the token to perform the RSA public key encryption. The token must contain the certificate but it doesn't have to have the public key. For password recovery, you only need to initialize a new token, make sure the private key from the MS CA is created on the card, and give the user the new card. The user can then restore their old token-based key file because the token you gave them contains the private key that can decrypt their original key file.
Method 4: Use Certificate on file	During login, SecureDoc uses the RSA private key on the token as in method 1. Unlike in method 1 and 3, SecureDoc uses the certificate from a file. This token-based key file does not need the token to be present. This is the preferred method for creating key files for an enterprise with PKI systems. A SecureDoc administrator can create key files for thousands of users without having to have the tokens or the password to the tokens. If you use this method, the interface changes to enable you to browse to the certificate file.
Method 5: Use Symmetric Keys	Some tokens can use secret keys instead of RSA keys. You can use these secret keys to protect the key file as well. SecureDoc needs the token inserted when creating the key file. During login, SecureDoc uses the entered password to log in to the token and uses the on-token secret key to access the SecureDoc key file.

Method	Description
Method 6: Use certificate from Windows Store	Windows may store certificates in a particular folder. If you use this method, users are prompted to chose from the list of certificates stored on their Windows computer.

Appendix

Glossary

Term	Definition
admin key file	A key file with full privileges for an encrypted device, including the ability to create additional key files.
Algorithm	A detailed sequence of actions to perform some task (named after a Persian mathematician, Al-Khawarizmi). Technically, an algorithm must reach a result after a finite number of steps, thus ruling out brute force search methods for certain problems. The term is also used loosely for any sequence of actions which may or may not terminate.
Auto Login	SecureDoc Client function that requires users to log on to Boot Logon, after which SecureDoc Client automatically logs on to the SecureDoc Client Screen Lock and the Windows Login.
Boot #	Each key file enabled on an individual device is assigned a number in Boot Control. This number can be used to select the key file to be used at Boot Logon.
Boot Logon	SecureDoc Client application that authenticates users to key files before giving them access to an encrypted device. Also known as "pre-boot authentication prompt".
Control Center	SecureDoc Client application used on client computers to perform SecureDoc Client management functions, such as changing a password.
conversion	Synonym for process of encrypting a full disk.
Crypto-erase	Remove the encryption key from an encrypted device, rendering it inaccessible. Aka "zeroize".
disk	Includes local or network disk, RAIDs and magneto optical drives.
disk access profile	Settings to control or monitor read/write access to both encrypted and non-encrypted disks.
disk integrity check	The process that checks the computer's boot files to make sure they have not been tampered with, or corrupted, on boot-up. Depending on the user's privileges, the user may or may not be able to proceed if disk integrity is in doubt.
emergency disk	Used to restore Boot Logon on a client computer. This would be necessary if something happens to the computer's MBR and Boot Logon is missing, leaving the computer inaccessible. The files for this disk are returned from the client computer on receipt of installation package.The "disk" can be any removable media except a diskette: USB stick, CD, etc.
encryption key	The mechanism used to encrypt/decrypt a user's disks or removable media. Can act on a set of disks, a single partition, a single disk, etc. Can be assigned to different users in different forms (e.g. to user A in a key file, to user B in a smart card, to user C in a USB device, and to user

Term	Definition
	D in a key file protected by user D's Entrust profile). Must be stored in a key file.
fixed disk	See "disk".
GINA	Graphical Identification and Authentication. SecureDoc Client replaces Window's GINA with its own.
key file	Contains the encryption keys, user privileges, password rules, and other information for a specific user. Can be stored on a token. Encrypted itself and protected using a password or token.
MBR	Master Boot Record of a computer.
password hint	A hint to help the user recall their password. Should not contain the password itself, and should not contain enough information that someone other than the authorized user could guess. (For example, "name of your first pet".) This option is checked and cleared in password rules.
Password Recovery	Process of enabling users with a lost or forgotten password to regain access to their PC. Once user is validated through answers to *challenge questions*, they can continue to boot and log on to Windows, but are immediately prompted to specify a new password.
Protection Key	Key that identifies which administrators have administrative access to which encryption keys.
removable media	Refers to USB/firewall drives, CD/DVDs, flash and SD cards, and PCMCIA, Jaz and Zip drives.
Screen Lock	SecureDoc Client function that uses a screen saver for added security. The screen saver requires users to log on to their key file or, for token-based key files, to insert their token, to continue working with the computer.
SED	Self-encrypting hard disk with embedded hardware encryption functionality. See WinMagic web site for details on which of these drives are supported.
SecureDoc Client Control Center	See Control Center
self-help password recovery	Function that enables users to recover, without administrator help, from a lost password or token.
strong password	A password that is difficult for a person or program to guess. Passwords are made strong by being long (no shorter than eight characters) and including a mixture of alphabetic and numeric characters, mixing cases as desired. It is important to not have a password that corresponds to a recognizable word or phrase, particularly a user's name or login ID. The password also should be able to be remembered by the user, to avoid writing passwords down.
token	In security terms, a physical device, such as a "smart card".
zeroize	Remove the encryption key from an encrypted device, rendering it inaccessible. Aka "Crypto-erase".

Appendix

Index