



Safend Protector CD/DVD Encryption Enforcement

Feature Description

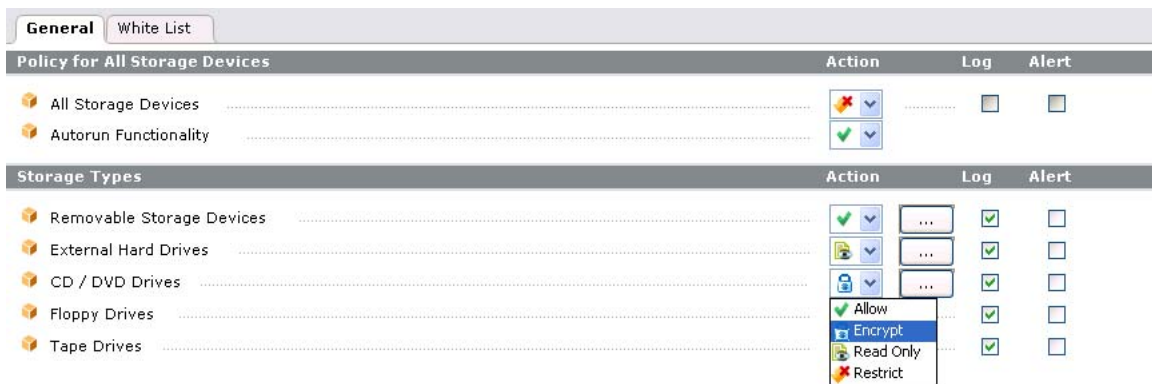
1. Overview

Safend Protector provides the ability to *centrally enforce* CD and DVD encryption using a new mode of encryption – Virtual Volume Encryption. This feature is in addition to Safend Protector's existing ability to encrypt removable storage, and its soon to be available ability to encrypt external hard drives.

As in the case of all of Safend Protector's encryption features, Virtual Volume Encryption uses the FIPS approved AES with a 256-bit key.

2. Centrally Enforced Encryption

Safend CD/DVD encryption allows administrators to mandate the encryption of all the data being transferred off organization endpoints to CD and DVD media, as shown in the following screen capture:



3. What Is an Encrypted Volume?

An encrypted volume is a container into which files and folders are added when the end user wants - or is obligated - to encrypt them. It is created through use of a simple wizard, and once its creation is completed files can be added to it or removed from it (in much the same way files are added to or removed from a compressed archive). Any file or folder subsequently residing in this volume is encrypted.

4. Creating and Using an Encrypted Volume

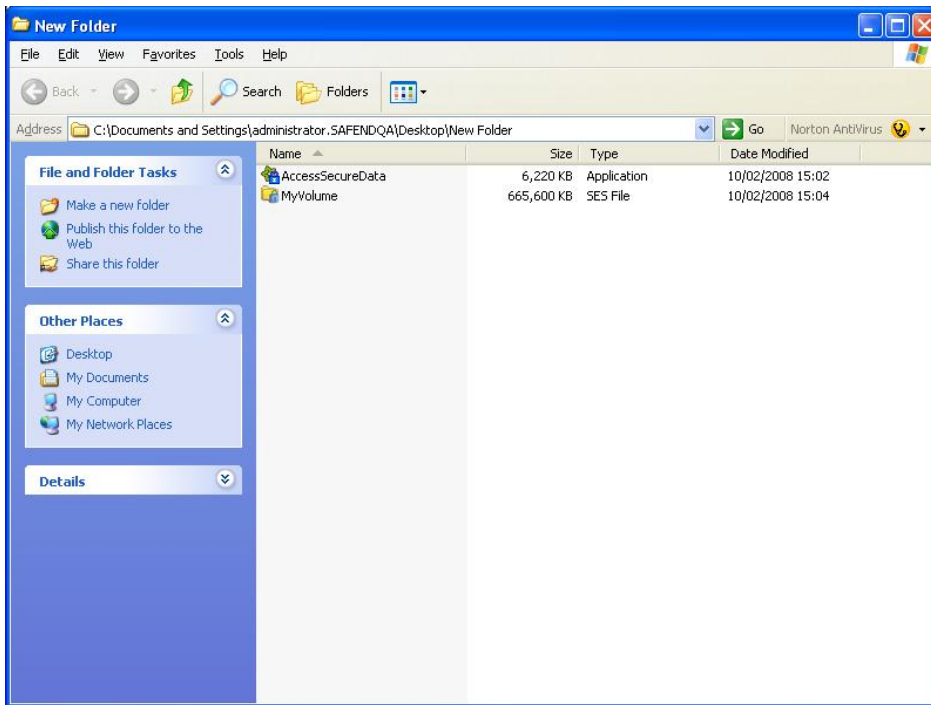
The Encrypted Volume Creation Wizard is initialized using a right click context menu which is added to the machine CD/DVD drive, as shown in the following screen capture:



This wizard enables you to set the destination file, name and required size of the volume:



Once the required parameters have been set, creation of the volume is performed. The encryption procedure creates new files in the destination folder, as shown in the following screen capture:



The following are the newly created files:

- The **Encrypted Volume file** (*.SES) – this is the virtual volume into which files that require encryption are added.
- The **AccessSecureData.exe** utility – this is an application that allows permitted users to access the encrypted volume from machines not protected by Safend Protector Client using a password.

5. Populating and Editing the Encrypted Volume

Files can be added to - or removed from - the Encrypted Volume by clicking the Open Volume button in the wizard step shown in the following screen capture:



When the volume is open, files can be copied to it or removed from it as in any other volume or folder, through Windows Explorer.

Alternatively, you can open the volume at any later time by simply double-clicking the *.ses file, and then adding or removing files as explained above.

6. Using an Encrypted Volume

Once an encrypted volume has been created and the required files added, it can be burned on to a CD/DVD. This option can be enforced through the end user's policy so that he cannot burn files other than encrypted volumes to a CD/DVD medium. In this case, if the user tries to burn unencrypted data to a CD/DVD the following message appears on his screen:



The copying of encrypted volumes to CD/DVD and blocking of unencrypted data can be logged so as to provide an audit trail.

7. Accessing the Encrypted Volume on Non-Company Machines

Safend CD/DVD Encryption is designed to work company-wide. Encrypted devices can be read and used interchangeably on any computer in the organization, without the need to use a password.

The Safend Protector administrator can choose whether or not to allow specific users password-protected access to the data on non-authorized computers. If allowed, each user is able to set his own device password, and use the Safend Protector on a non-company machine.

For these users, the Encrypted Volume Creation Wizard will include the following window, in which they will be able to set the offline access password.



Access to encrypted devices on non-company computers is provided by the AccessSecureData.exe Utility, which is created by the Encrypted Volume Creation Wizard when a user sets an access password for the Virtual Volume. When a user runs this utility on a non-company computer, a window appears, requiring the user to provide the Offline Access password. On entering the correct password, the user gains access to the encrypted data. (Note: this capability will be available in version 3.3 due for release in April 2008).