



Safend Protector 3.3

Virtual Volume Encryption

Feature Description

1. Overview

Safend Protector version 3.3 broadens the product's encryption capabilities by including a new mode of encryption – Virtual Volume Encryption. This new feature is added to Safend Protector's removable storage encryption to provide end users with the ability to encrypt data on CD/DVD media and external hard drives. It also enables them to selectively encrypt data on their internal 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. What Is an Encrypted Volume?

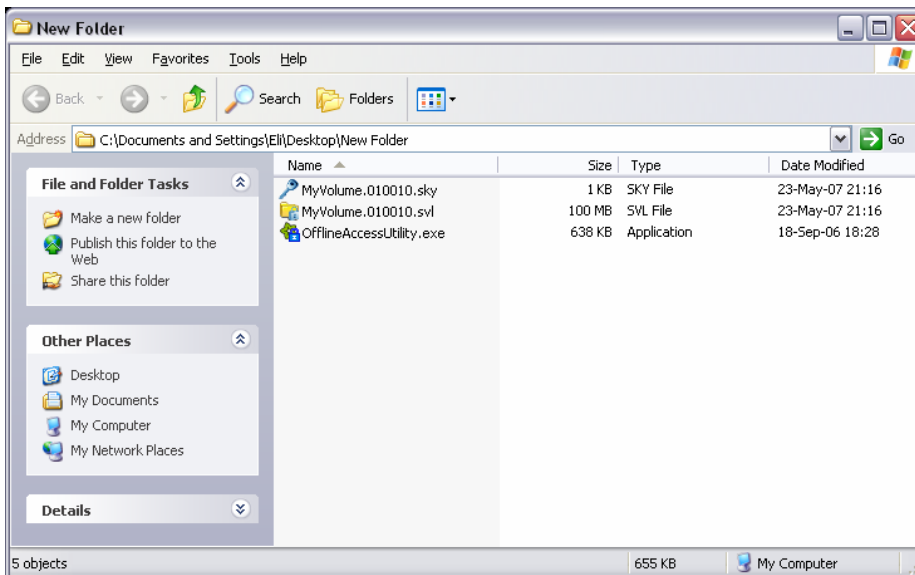
An encrypted volume is a container into which files and folders are added when the end user wants - or is obligated - to encrypt them. It is created through use of a simple wizard, and once its creation is completed files can be added to it or removed from it (in much the same way files are added to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

3. Creating and Using an Encrypted Volume

The Encrypted Volume creation wizard enables you to set the destination file, name and required size of the volume, as shown in the following screen capture:



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** (*.svl) – this is the virtual volume into which files that require encryption are added.
- The **Key file** (*.sky) – this file must always be kept and copied together with the Encrypted Volume file in order to read and edit the encrypted volume.
- The **Offline Access Utility** file (OfflineAccessUtility.exe) – this program enables authorized end users to access the Encrypted Volume on non-organizational computers.

4. 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 *.svl file, and then adding or removing files as explained above.

5. Using an Encrypted Volume

Once an encrypted volume has been created and the required files added, it can be used to meet several needs:

- Burning the Encrypted Volume 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:



- Copying the Encrypted Volume to an **external hard drive**
- Leaving the Encrypted Volume as a container on the end-user's **internal hard drive** to be used for securing his folders and files.

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

6. Offline Access to an Encrypted Volume

The user's policy may allow access to the encrypted volume on non-organizational computers. In this case, the encrypted volume creation wizard allows the user to set an offline access password and provides her with a utility which will enable decryption of the volume using the password*.

*This feature will be available in version 3.4