GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA VIRTUAL DISK

Encrypted virtual disk

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd_virtual_disk-user_guide-v10

Table of contents

In the documentation, Stormshield Data Security Enterprise is referred to in its short form: SDS.

Preface

This document provides essential information on the use of Stormshield Data Virtual Disk. It describes the functions of Stormshield Data Virtual Disk in its default configuration. You can customize the installation of this component using Stormshield Data Authority Manager. The customization options are the most important in this guide. This guide is for

1. system administrators who want to install Stormshield Data Security.
2. users who want to protect confidential files.

1. Introduction

This chapter describes the features and characteristics of Stormshield Data Virtual Disk.

1.1 Presentation

Stormshield Data Virtual Disk is a security software. It enables you to create encrypted volumes. Encrypted volumes are virtual hard disks in which you can store your confidential data.

An encrypted volume is used like any hard disk volume: you may copy files, start applications that use these files, and install software on your encrypted volume.

Stormshield Data Virtual Disk requires limited memory and CPU resources; files are encrypted on the fly as they are saved, and decrypted at the time they are read.

To install and run Stormshield Data Virtual Disk you need to purchase the appropriate license.

1.2 Key concepts

In this guide, the following terms and concepts are used:

- Creating an encrypted volume is the action of creating a virtual hard disk in which you want to store confidential data. See Section 3.1, "Creating an encrypted volume".
- Mounting an encrypted volume is the action of connecting a virtual hard disk to your workstation and in which you can store confidential data. See Section 3.2, "Mounting an encrypted volume".
- Unmounting an encrypted volume is the action of disconnecting your virtual hard disk from your workstation. See Section 3.3, "Unmounting an encrypted volume".

As a comparison, creating an encrypted volume corresponds to buying a USB token, and mounting/unmounting an encrypted volume corresponds to plugging/unplugging the USB token to your workstation.

- When you create an encrypted volume, you define a list of authorized users: authorized users are the users who can mount/unmount the encrypted volume, and consequently can access the encrypted volume's content. See Section 3.6, "Modifying users list".

As a comparison, authorized users are users you trust giving them your USB token.

In this guide you will meet the term container file:

- The container file is how you see your encrypted volume in Windows Explorer. The encrypted volume is the content of the container file.

As a comparison, the container file is your USB token as it appears in Windows Explorer, whereas the encrypted volume is the content of this USB token.

1.3 Integration into Stormshield Data Security

Stormshield Data Virtual Disk is fully integrated into Stormshield Data Security (public key solutions); this will allow you to use any existing account with previously installed keys and certificates in order to access all the Stormshield Data Security components installed on your computer.

For more information, refer to the *Installation and Implementation guide*.

1.4 Public key encryption

Stormshield Data Security uses the public key encryption technology.

Each correspondent has a pair of keys: a private key and a public key. The private key is carefully kept by its owner. The public key, by contrast, is freely distributed.

This pair of keys is used for encrypting and sharing confidential documents, as explained below.

Stormshield Data Security can use one of the following:

- a unique pair of keys for encrypting and signing
- two different key pairs, one for encrypting, the other for signing
- one key pair for encrypting only or signing only

1.4.1 Encryption

The sender initializes file encryption using either their public key, or the public key of the correspondent(s) if the file is to be sent. The correspondent then uses his private key to decrypt the file. Since the user or correspondent(s) are the only ones who have the private key, they are assured that the data cannot be read by a third party.

1.4.2 Certificates

In order to share encrypted files with correspondents, you need to know the public key of your correspondents.

Public keys are distributed as certificates. A certificate is an electronic document that links a public key to its owner. Stormshield Data Security manages certificates with the X.509 v3 format.

> **IMPORTANT**
> In case of encryption key or certificate renewal, the previous encryption certificate and associated key must be kept in the Stormshield Data Security user account in order to be able to decrypt previously-encrypted files.

For more information on exporting and importing certificates, see the *Installation and Implementation guide*.

1.4.3 Trust

A certificate links a public key to an identity. You can only use the certificate if you trust this link.

If, for example, you want to send an encrypted message to Alice, you must be sure that the certificate actually belongs to Alice. If not, there is a risk that the message has not been encrypted with Alice's real key, but with the key of an impostor who can then decipher your message.

Two techniques enable the trust of a certificate to be established:

- inherited trust is based on the principle that if you trust a certification authority, you implicitly trust the certificates that it distributes.
- explicit trust means that you need to verify the origin of the certificate yourself. One way to do this is to check a parallel source of information (telephone, publication, mail, website, etc.).

1.4.4 Trusted address books

Stormshield Data Security includes a trusted address book: you can use it to insert the certificates of trusted correspondents and authorities.

The management of trusted address books and certificates is described in the *Installation and Implementation guide*.

1.5 A secured connection to Stormshield Data Security

Access to your keys is protected: to be able to use your keys, you must connect to Stormshield Data Security, a process which involves self-authentication, i.e. proving that you are actually the owner of the keys.

Stormshield Data Security provides two authentication methods:

- by password: you enter an identifier and a password
- by smart card or USB token: you enter the secret code of the card – that is the Personal Identification Number (PIN)

For further information, handling user accounts is described in the *Installation and Implementation guide*.

2. Installing Stormshield Data Virtual Disk

This chapter provides information on Stormshield Data Virtual Disk requirements and installation.

2.1 Required configuration

For the required configuration, refer to the section **Compatibility** of the Stormshield Data Security 10.1 Release Notes.

200 MB of disk space are needed for the installation of all the Stormshield Data Security components.

IMPORTANT
Stormshield Data Security is not compatible with the **Fast User Switching** feature.

2.2 Installing Stormshield Data Virtual Disk

Stormshield Data Virtual Disk is a component of Stormshield Data Security.

Stormshield Data Security installation is global. The delivered product contains all the components of the software suite and allows you to install the applications and components you choose, according to the rights contained in the license key.

The installation procedure is described in the *Installation and Implementation guide*. Refer to this guide for further information.

3. Using Stormshield Data Virtual Disk

This chapter describes the functions offered by Stormshield Data Virtual Disk.

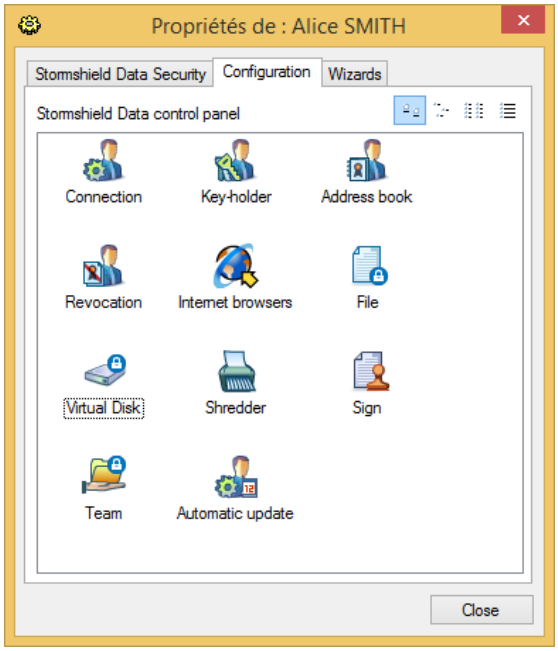
3.1 Creating an encrypted volume

Stormshield Data Virtual Disk enables you to create encrypted (secured) volumes (virtual drives). All of the files on these volumes will be stored securely.

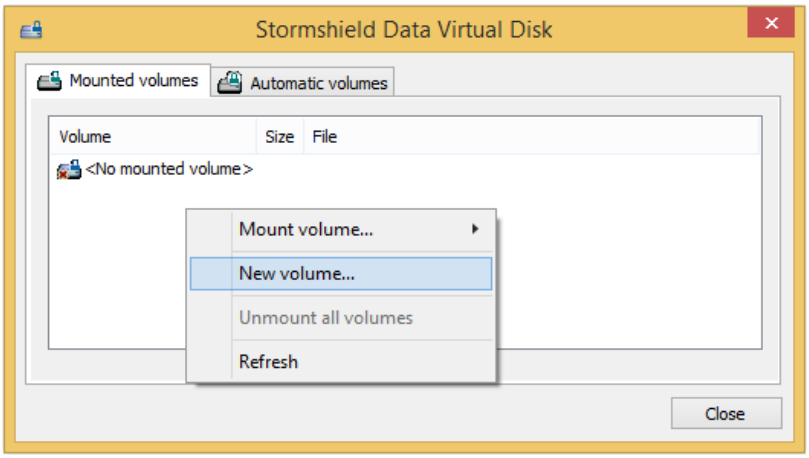
An encrypted volume can be used the same way as a normal hard disk drive. You can copy files on it and start applications that use these files. You can also install software on an encrypted volume.

NOTE
To avoid encrypted volume damage or destruction and thus loss of data contained in the encrypted volume, you must keep a backup copy of the encrypted volume. You should take the same precautions with this virtual volume as you would for a normal physical volume (formatting, error checking, fragmentation, and backup management).

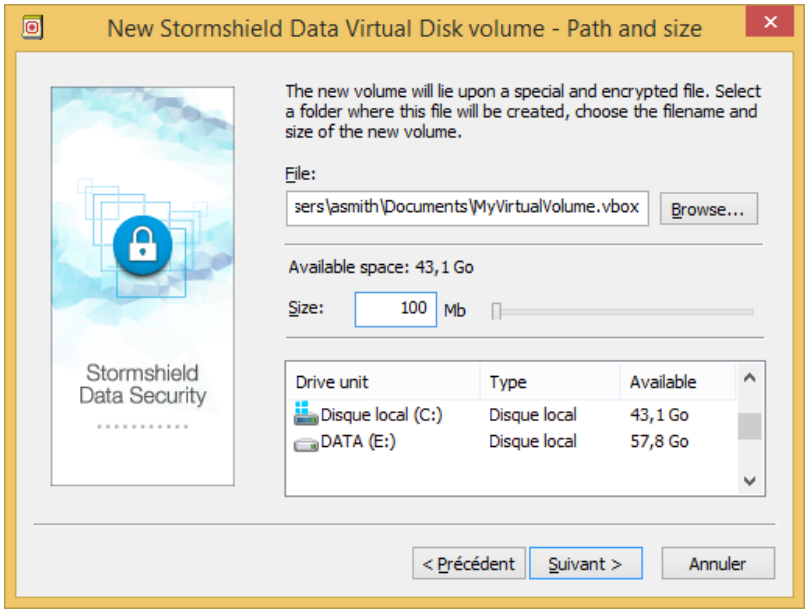
1. From the system tray, right-click the **Stormshield Data Security** menu and click Properties.
2. From the Properties window, select the Configuration tab.
3. Double-click the Virtual Disk icon:



4. From the Stormshield Data Virtual Disk control panel, select the Mounted Volumes tab.
5. In the Mounted Volumes tab, right-click and select New Volume:



6. Following an introduction dialog box, the following dialog box is displayed:



- The File field enables you to define the location and the name of the encrypted volume:
  - The Browse button enables you to select the volume location. The directory in which the volume is created must be previously created.
  - The .vbox extension is automatically added to the volume name.

> **CAUTION**
> If an encrypted volume is locally mounted in a Windows session, all users allowed to open a local session on the workstation will be able to access the content of the encrypted volume. For more information, refer to the section *Using the volume within a Windows multi-session context* of the *Stormshield Data Security Administration guide*.

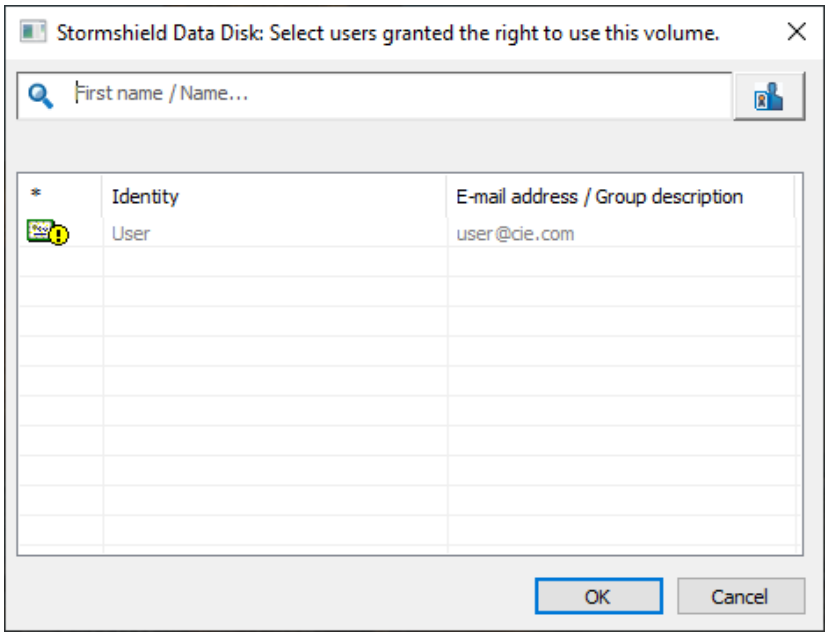
- Specify the volume size in the Size field. You can define the volume size between 1 MB and the maximum available size. The default volume size is 10% of the available space on the drive unit.

IMPORTANT
The maximum size of a Stormshield Data Virtual Disk volume is 2048 GB (2 TB).

NOTE
The real storage capacity of the volume is slightly below the selected volume size because a space is reserved for system files.

7. Click on **Next**.
8. You may want to authorize other users to use the new volume separately. Enter their name in the search field. The search displays users or groups specified in the trusted address book as well as users from the LDAP directory if it is configured.

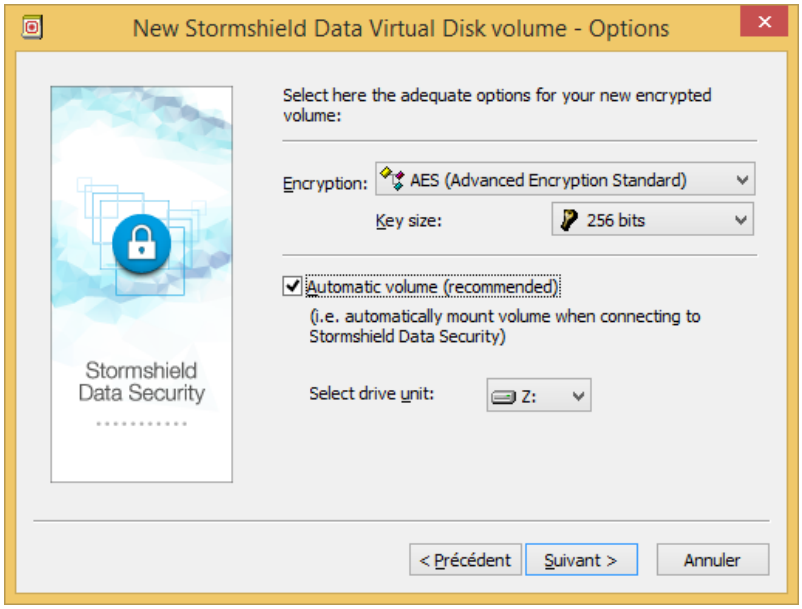
NOTE
Simultaneous use of the volume by different users is not possible. Each allowed user accesses the volume alternately.



NOTE

When the users list is completed, click Next.

9. The following dialog box is displayed:



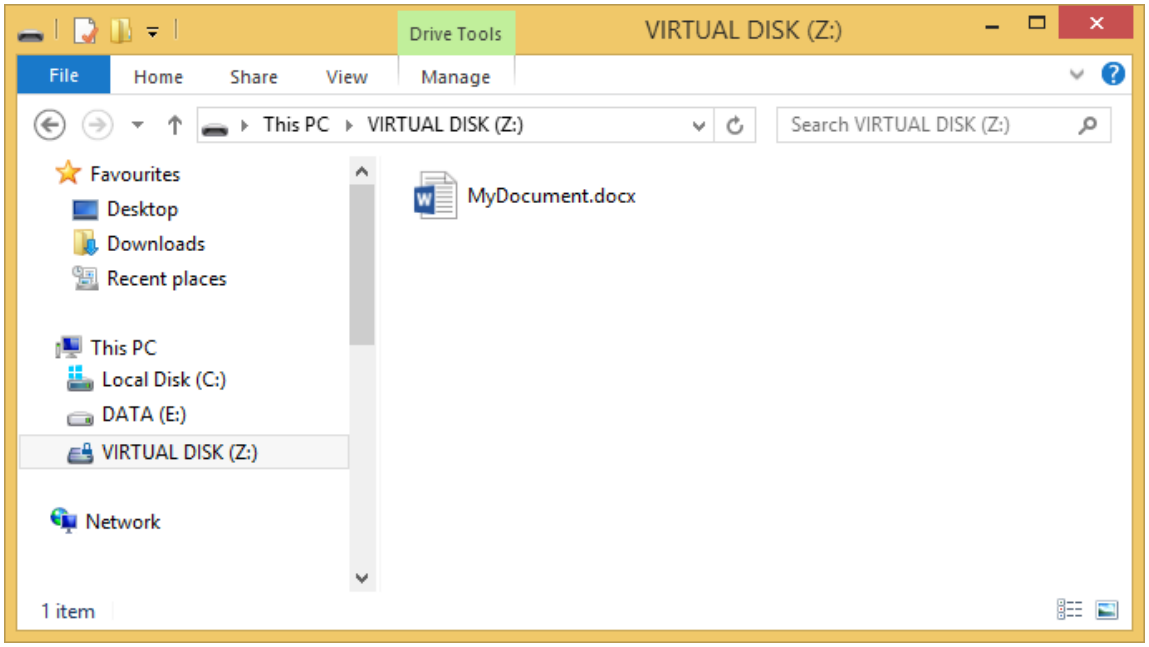
In the dialog box displayed above you must:

- select the encryption algorithm and key strength used to encrypt your new volume. The AES algorithm with a 256 bits key size offers the best protection, with high-standard execution performances;
- indicate if you wish the volume to be mounted automatically each time you connect to Stormshield Data Security;
- select the drive unit mount letter to be used and indicate if the volume must be automatically mounted each time you connect to Stormshield Data Security. The drive letter must not be used by another network drive or USB drive.

10. Click Next to see a summary of the choices you made.

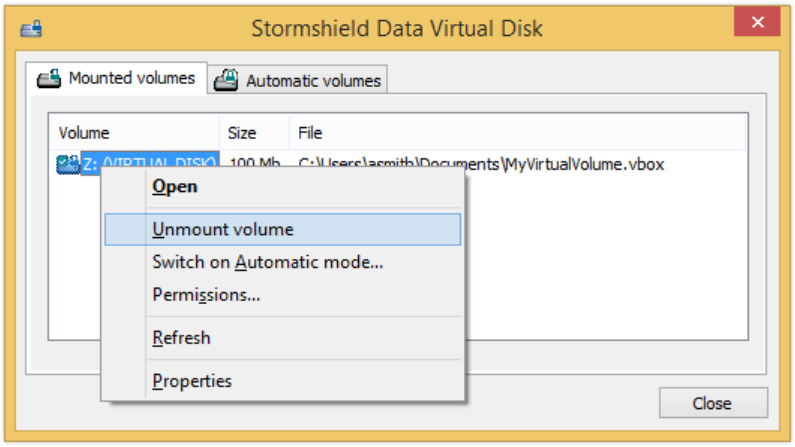
- Click Back to modify your settings.
- Otherwise click Finish to confirm and end the creation of your encrypted volume.

Once the volume creation process is completed, the volume appears whenever you open the Windows Explorer. All files placed on this volume will be encrypted and only authorized users will be able to access the encrypted volume's content.



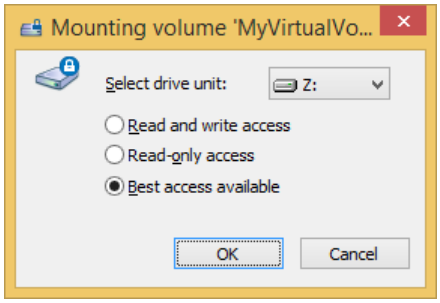
3.2 Mounting an encrypted volume

1. To mount an existing encrypted volume, right-click the Stormshield Data Security menu from the system tray and select Properties.
2. From the Properties window, select the Configuration tab and double-click the Virtual Disk icon.
3. In the dialog box displayed, right-click, then click Mount volume and Browse to select the volume you want to mount. The recently created volumes are listed below Browse and can be mounted by selecting them directly.



NOTE
The Automatic volumes tab enables you to mount an automatic volume if it were unmounted or if the mounting failed.

4. When you select the volume you want to mount, the following dialog box is displayed:



Select the drive unit and the access type:

- Read and write access: the volume has read/write access. This is only possible if the volume is not yet mounted.
- Read-only access: the volume has read access. This is only possible if the volume is not yet mounted with read/write access.
- Best access available:
- The volume will be mounted with read/write access if it is not already mounted.
- The volume will be mounted with read access if it is already mounted with read access.
- An error message is displayed if the volume is already mounted with read/write access.

If the selected drive unit mount letter is busy (for example, a USB token) when mounting the new volume, an error message is displayed, indicating the volume mounting has stopped. Be sure the drive letter is not used by another network drive or USB drive.

NOTE
You can also mount a volume by double-clicking its container file in Windows Explorer and then following the same steps above.

In general, an encrypted volume is mounted to a local workstation. However, an encrypted volume can be mounted to a file server.

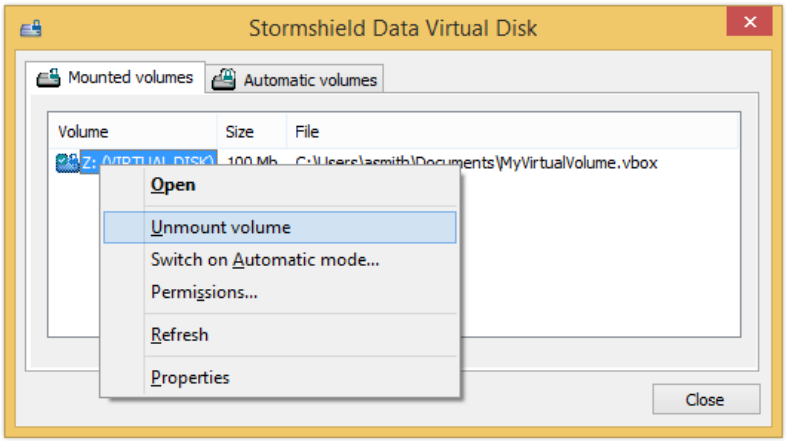
CAUTION
In this case, users with access to the file server can access the encrypted volume's content even if they are not in the list of authorized users.

With Stormshield Data Virtual Disk, only authorized users are users who can mount/unmount an encrypted volume, but if the encrypted volume is mounted to a file server, all users with access to the file server can access the encrypted volume's content.

When an encrypted volume is mounted to a file server, data exchanged between the server and your local workstation is encrypted. Decryption will be done on your local workstation.

3.3 Unmounting an encrypted volume

To unmount an encrypted volume, double-click its container file in Windows Explorer or right-click on it in the Stormshield Data Virtual Disk control panel and click Unmount volume.



NOTE
The list of mounted volumes also includes the automatic volumes.

You can also unmount automatic volumes in the Automatic volumes tab.

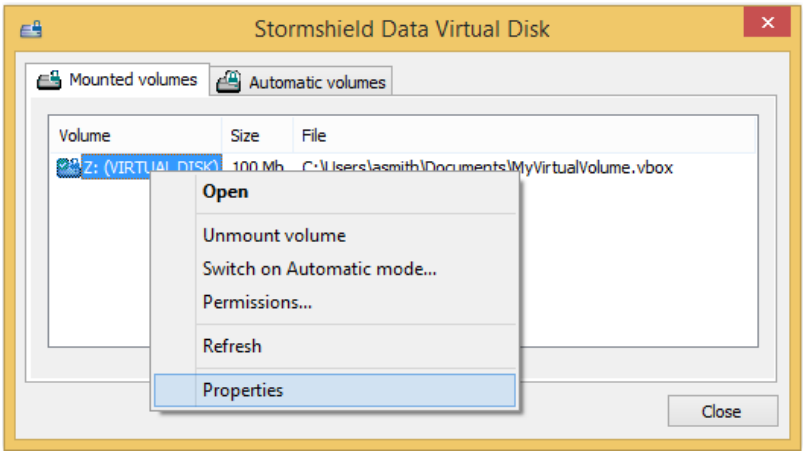
3.4 Accessing encrypted volume properties

There are two ways to access encrypted volume properties:

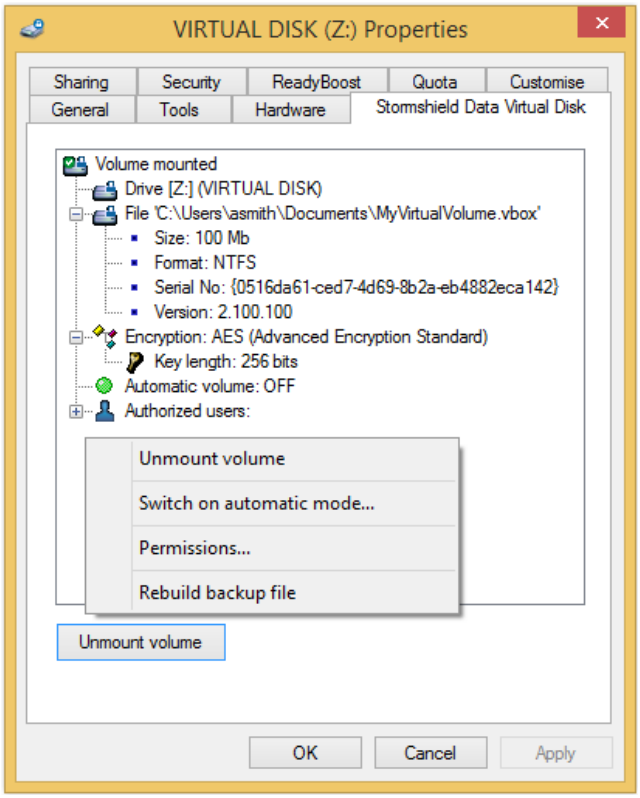
- from the Stormshield Data Virtual Disk control panel (for mounted volumes and automatic volumes)
- from the container file (for unmounted volumes)

3.4.1 From Stormshield Data Virtual Disk control panel

1. Right-click the encrypted volume in the Stormshield Data Virtual Disk control panel, and click Properties.



2. Click the Stormshield Data Virtual Disk tab.

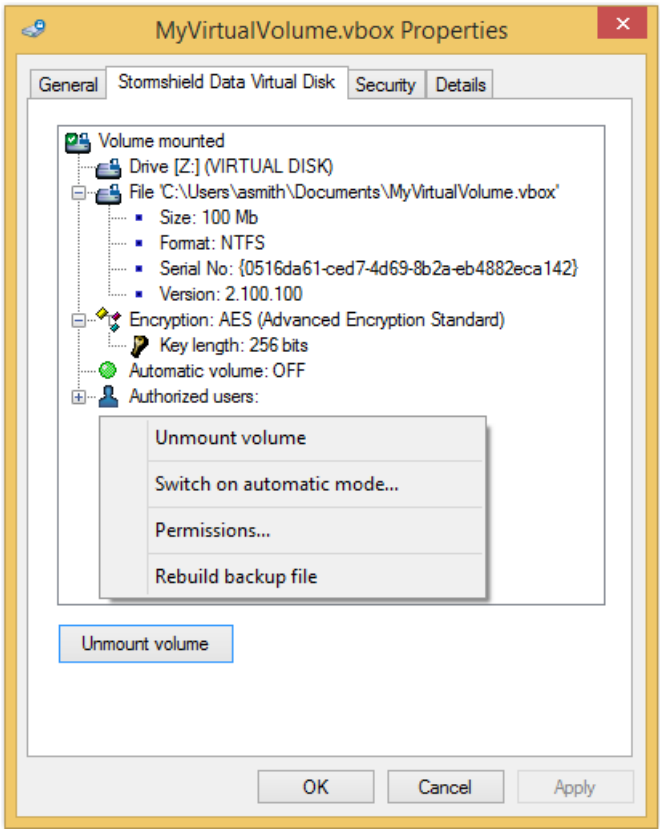


3. By right-clicking in the Stormshield Data Virtual Disk tab, you can:

- Unmount the volume (the Unmount volume button also enables you to unmount the volume)
- Switch volume mode (manual/automatic)
- Modify user access permissions
- Rebuild backup file

3.4.2 From the container file

1. In Windows Explorer, right-click the container file and click Properties.
2. Click on the *Stormshield Data Virtual Disk* tab.



3. By right-clicking in the *Stormshield Data Virtual Disk* tab, you can:

- Mount the volume (the Mount volume button also enables you to mount the volume)
- Switch volume mode (manual/automatic)
- Modify user access permissions
- Rebuild backup file

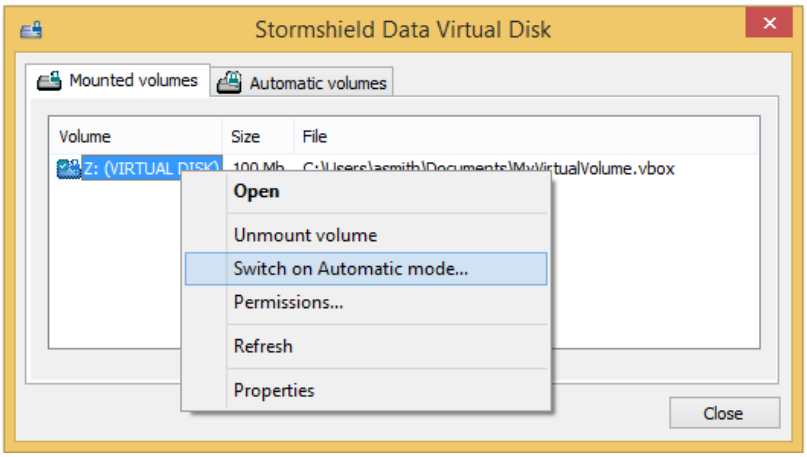
3.5 Automatically mounting encrypted volumes

If you select the automatic volume mounting option, Stormshield Data Virtual Disk automatically mounts your encrypted volumes whenever you connect to Stormshield Data Security. This option can be selected when the volume is created or later on.

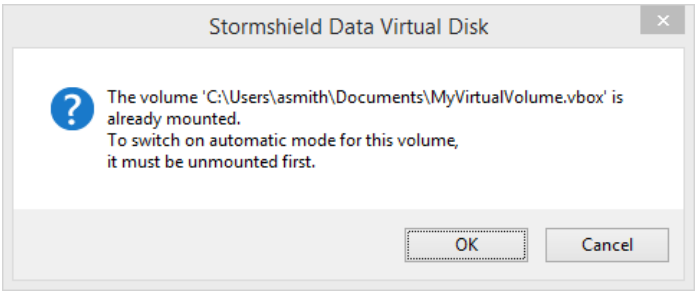
3.5.1 Switching on the automatic mode

To switch on the automatic mode from the Stormshield Data Virtual Disk control panel, the encrypted volume must be mounted.

1. In the Stormshield Data Virtual Disk control panel, right-click the encrypted volume and click Switch on Automatic mode.

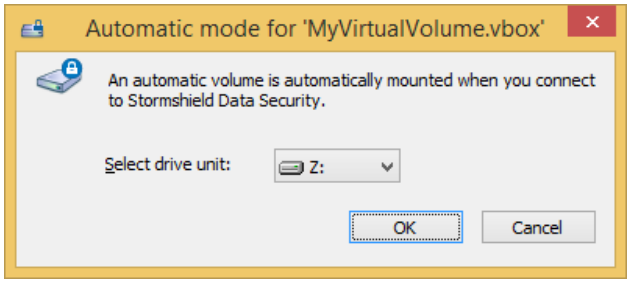


2. When switching on automatic mode, the following message is displayed:



This means that switching to automatic mode requires unmounting the volume. Make sure there are no running applications using files on the volume, and click Yes.

3. Select the drive unit mount letter. By default, the mount letter previously used is selected.



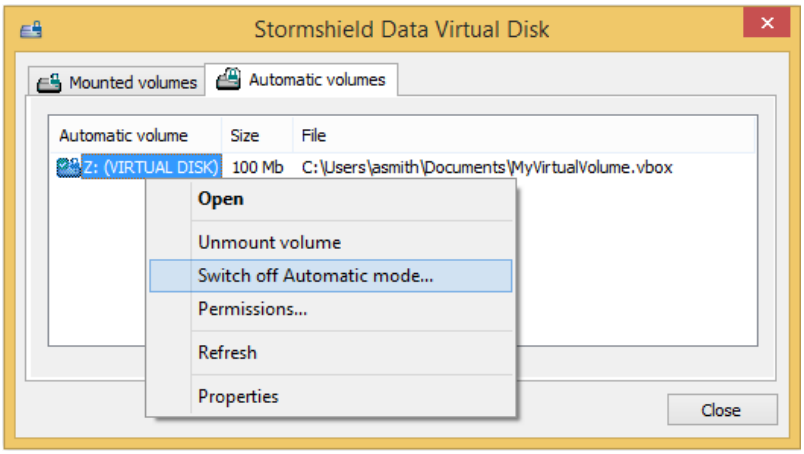
The volume is then unmounted, switched to automatic mode and then re-mounted.

The drive letter must not be used by another network drive or USB drive.

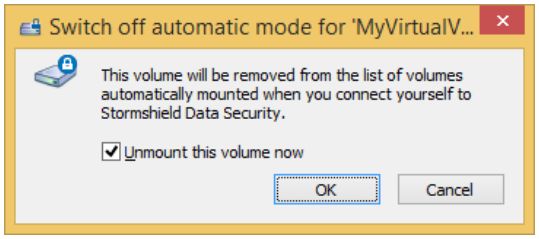
3.5.2 Switching off the automatic mode

To switch off the automatic mode from the Stormshield Data Virtual Disk control panel, the volume can be mounted or unmounted.

1. In the Stormshield Data Virtual Disk control panel, select the Automatic volumes tab.
2. Right-click the encrypted volume and click Switch off Automatic mode.



3. When switching off automatic mode, the following message is displayed:

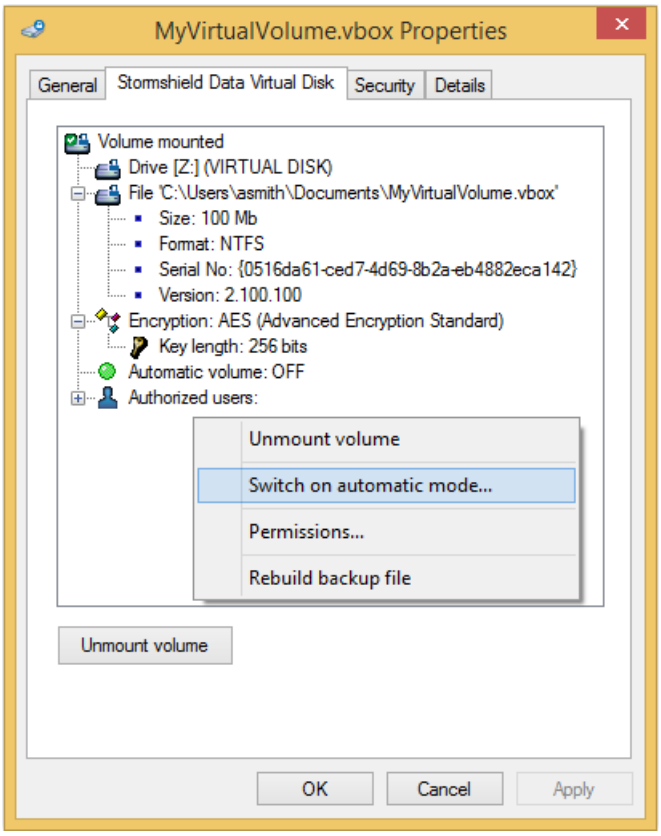


In addition to switching off automatic mode, you can unmount the selected volume by selecting the Unmount this volume now option. Contrarily to the switching on automatic volume procedure, there is no unmounting of the volume during this procedure. Click Yes to validate your choice.

3.5.3 Switching from the container file

You can also switch on/off the automatic mode from the container file. The main advantage is that it is not mandatory to mount the volume to switch it to automatic mode.

1. In Windows Explorer, right-click the container file and click Properties.
2. Click the Stormshield Data Virtual Disk tab.



3. Right-click in the Stormshield Data Virtual Disk tab window and select either Switch on automatic mode or Switch off automatic mode, depending on the original volume mode.

3.6 Modifying users list

Modifying users list implies that the volume is already mounted or is in automatic mode.

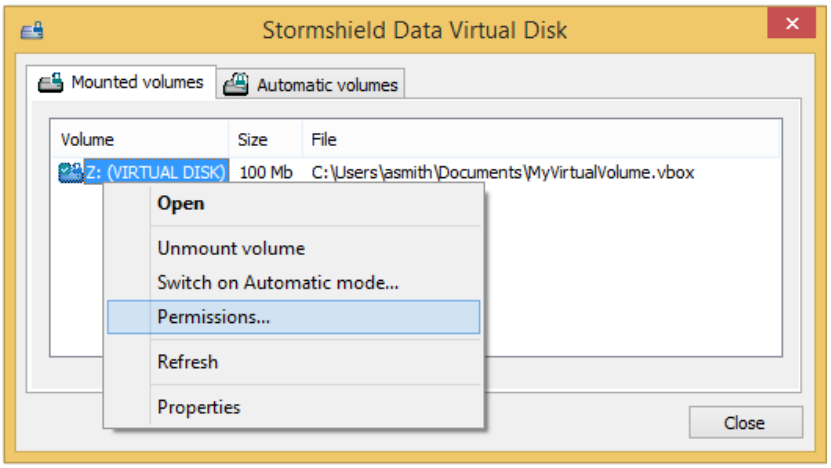
Only the volume owner is authorized to modify the authorized users list.

There are two ways to modify users list:

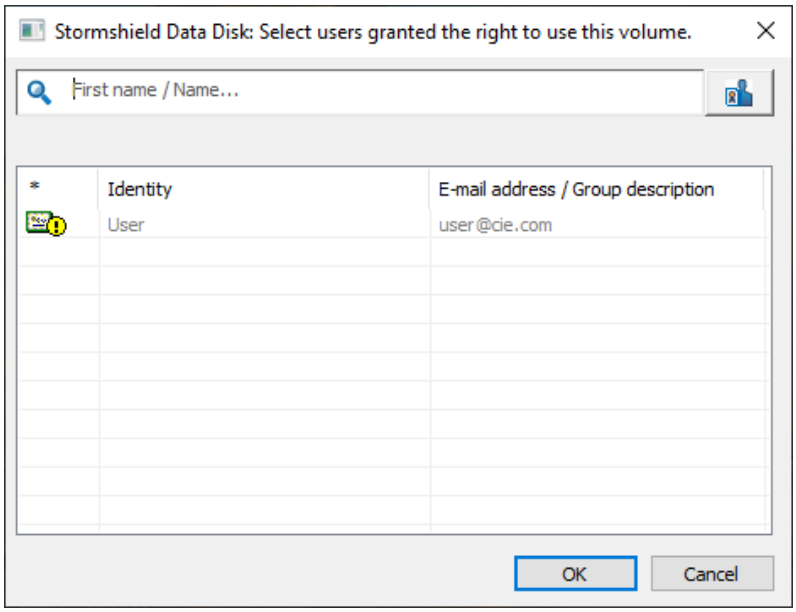
- from the Stormshield Data Virtual Disk control panel (implies that the volume is mounted or is in automatic mode)
- from the container file

3.6.1 From the Stormshield Data Virtual Disk control panel

1. Right-click the volume in the control panel (in the Mounted volumes or in the Automatic volumes tab), and click **Permissions**.

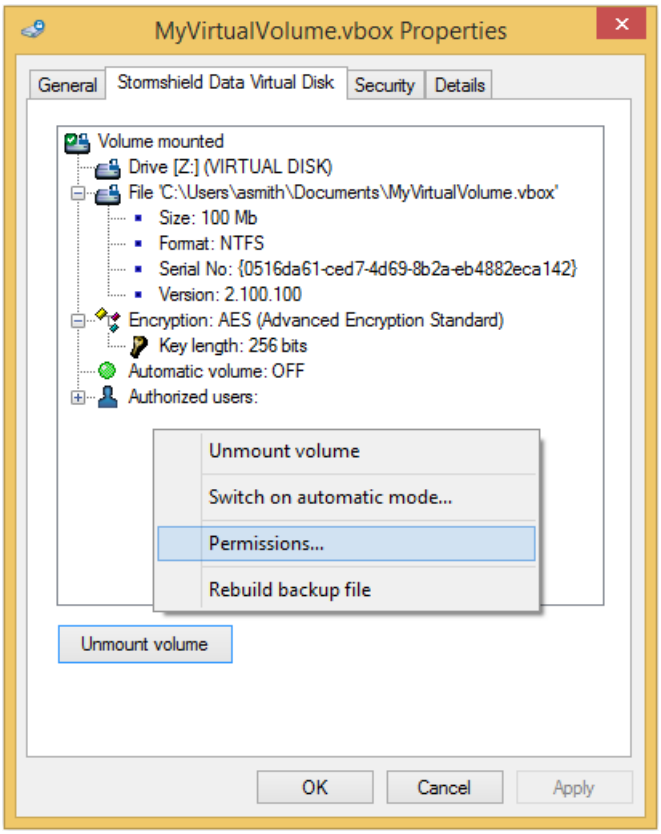


2. You can see the list of users authorized to access the volume. Search for users or groups who will be allowed to access the volume. The search displays users specified in the trusted address book as well as users from the LDAP directory if it is configured.

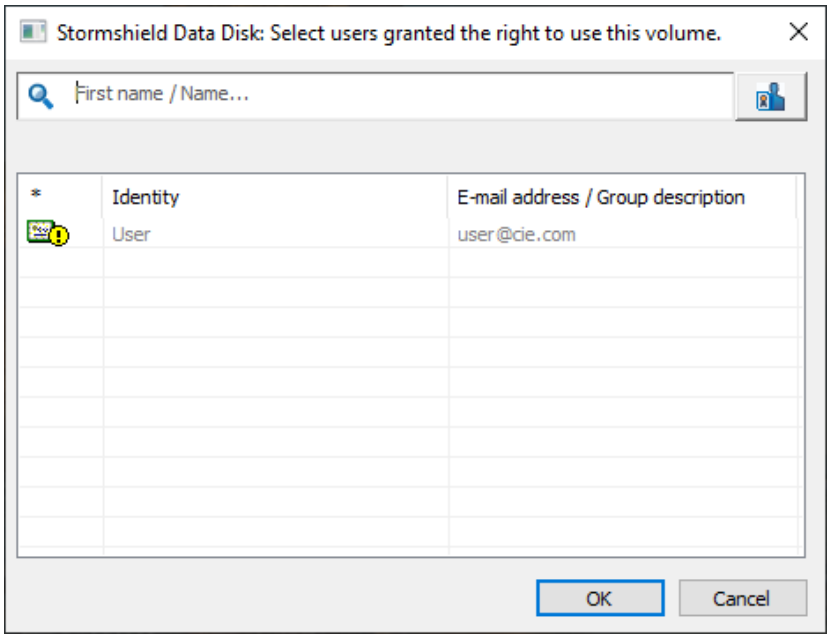


3.6.2 From the container file

1. In Windows Explorer, right-click the container file and click Properties.
2. Click on the *Stormshield Data Virtual Disk* tab.
3. In the *Stormshield Data Virtual Disk* tab, right-click, and then click **Permissions**.



4. You can see the list of users authorized to access the volume. Search for users or groups who will be allowed to access the volume. The search displays users specified in the trusted address book as well as users from the LDAP directory if it is configured.



3.7 Disconnecting from Stormshield Data Security

When disconnecting from your Stormshield Data Security account, all the encrypted mounted volumes are unmounted, even if they are being used by running applications or if some files are open.

Hence it is recommended to close all applications and files before disconnecting from your Stormshield Data Security account.

When reconnecting to your Stormshield Data Security account, only automatically mounted volumes are re-mounted.

3.8 Locking Stormshield Data Security

When locking your Stormshield Data Security account, all the mounted encrypted volumes can no longer be read/write accessed (but they are not unmounted), even if they are being used by running applications or if some files are open.

Hence it is recommended to close all applications and files before locking your Stormshield Data Security account.

3.9 Modifying the volume owner

Following organizational changes, it may be necessary to modify the volume owner.

The new volume owner must be in the list of authorized users. If the new owner is not in the list of authorized users, append it as described in Section 3.6, "Modifying users list" before performing this procedure.

> **NOTE**
> If you want to modify the volume owner but you are not the current volume owner, then you should proceed with a volume recovery.

In this case, it is mandatory that you be an authorized recovery user declared in the Stormshield Data Security account. Refer to the *Installation and Implementation guide* for further information.

More information regarding the volume recovery procedure is available in the *Administration guide*.

Make sure the connected user is the volume owner, and follow these steps to modify the volume owner:

1. Modify the [Disk] section in the *sbox.ini* file. The *sbox.ini* file is typically located in:

C:\Program Files\Arkoon\Security BOX\kernel

The [Disk] section parameters must be defined as follows:

```
[Disk]
ModifyRescueFile = 1
ExpertMode=1
```

The *sbox.ini* file parameters are described in the *Administration guide*.

> **NOTE**
> You do not need to reboot your PC or to disconnect/reconnect to Stormshield Data Security in order to take into account these *sbox.ini* file modifications.

2. Open the folder containing the container file in Windows Explorer: this folder includes the container file (.vbox extension) and another file with the *.vboxsave* extension.
3. Right-click the *.vboxsave* file and click Properties.

4. Select the Stormshield Data Virtual Disk tab and click the + sign on the left of Authorized users to see the complete list of authorized users.
5. Right-click the name of the new volume owner and click Select as new owner.

> **NOTE**
> If the Select as new owner option is not displayed, then the *sbox.ini* file is not correctly modified or saved, or that the current user is not the volume owner.

When the new volume owner is selected, a warning message is displayed in the bottom of the Stormshield Data Virtual Disk tab. It informs you that the list of authorized users in the *.vboxsave* file is different than that of the *.vbox* file.

6. Click the Update volume button to synchronize the users list for the *.vbox* and *.vboxsave* files.
7. Reset the [Disk] section parameters in the *sbox.ini* file to their initial values.

documentation@stormshield.eu