

SOPHOS

SafeGuard® Private Disk 2.50 help

Document date: March 2011



Contents

- 1 Overview..... 2
- 2 Getting started..... 6
- 3 SafeGuard PrivateDisk main application 14
- 4 SafeGuard PrivateDisk Portable..... 31
- 5 Use cases - examples 33
- 6 Central administration 38
- 7 SafeGuard PrivateDisk OLE Automation Interface 44
- 8 Technical Support..... 47
- 9 Legal notices 48

1 Overview

1.1 What is SafeGuard® PrivateDisk?

SafeGuard PrivateDisk securely and transparently protects sensitive files on notebooks and desktop computers, no matter where they are located (on a local hard disk, removable media, or network file servers), while never forcing the user to think about security.

Secure Virtual Disk Technology - the electronic safe

It is achieved by defining "secure virtual disks", which are logical disks that encrypted their data and then store it in large files (volume files). Our Secure Virtual Disk Technology solution combines user-friendly encryption with simultaneous protection of several files in one secure virtual disk. This Secure Virtual Disk Technology creates an "electronic safe" on the computer, which protects the precious electronic data (e-assets).

To open the electronic safe, the user only has to log on to the virtual disk and can then work with their encrypted data. Data is encrypted automatically when it is stored on this virtual disk. Also, files are decrypted automatically when they are opened for everyday work. The user has no need to worry about encrypting data.

1.2 Benefits

Virtual disk encryption combines benefits from both file encryption and disk encryption technologies:

- Encryption is transparent (performed automatically).
- File data and metadata (directory information) are encrypted.
- When a user is working with encrypted content, data is decrypted only in RAM, not on disk.
- Not all data on a partition has to be encrypted.

1.2.1 Virtual disks

A virtual disk acts like an additional drive on the computer but, unlike a physical disk, a virtual disk stores its data inside a single (large) file. For example, for a 100 MB virtual disk, a 100 MB file (the so-called volume file) is needed on one of the physical disks.

Volume files can reside on all available drives, for example on removable media (floppy disks, CD-ROMs, DVDs, ZIP disks, USB memory sticks, or flash memory cards), on fixed disks and even on network drives.

All sector write and read operations are encrypted and decrypted. Therefore all file data and directory information within a virtual disk is encrypted with the same encryption key, using the state of the art AES algorithm.

Security lies in how the disk is protected. Without access rights to the disk, users may be able to delete whole virtual disk volume files (if access is not prevented) and they might be able to read the encrypted data, but they could never read the plain (unencrypted) data, or even the directory structure stored within the volume file.

SafeGuard PrivateDisk protects the disk key by using a password (PKCS#5) as well as by public/private key pairs from certificates. Users can open a secure virtual disk either by knowing the passphrase for that disk or by owning the private key of one of the certificates (stored in files or on smartcards) associated with the disk.

1.3 Keys from the SafeGuard Enterprise Key Ring

SafeGuard PrivateDisk also allows you to use keys from the SafeGuard Enterprise key ring besides passwords and certificates for accessing PrivateDisk drives. If SafeGuard Enterprise is installed on the computer, all keys contained in the user's key ring (keys created centrally by SafeGuard Enterprise or keys created locally on the SafeGuard Enterprise Client) can be used.

Thereby, for example several user can be granted access to the same PrivateDisk drive (for example on a network share). For accessing the PrivateDisk drive, only the key used to create the PrivateDisk drive has to be available on the users' computers. However, this is only possible, if Version 2.30 or a newer Version of SafeGuard PrivateDisk is used on both computers.

Note: Please note that the same key (e.g. a SafeGuard Enterprise group key) has to be available on both computers. If you use a SafeGuard Enterprise key which is not included in the user's key ring, the user cannot access the PrivateDisk drive.

If you use a locally created SafeGuard Enterprise key, you have to provide the user who is to access the PrivateDisk drive with the key passphrase. Upon opening the archive the recipient will be prompted automatically to enter the passphrase.

1.4 Platforms

SafeGuard PrivateDisk is available for:

- Windows XP 32-bit
- Windows Vista 32-bit
- Windows Vista 64-bit
- Windows 7 32-bit
- Windows 7 64-bit

1.5 Versions

Personal Edition

The Personal Edition is ideal for single users and small offices. It contains no central administration functionality.

Enterprise Edition

Beside this version of SafeGuard PrivateDisk, which is optimized for personal use and small offices, we also supply an Enterprise Edition of this product which is ideal for larger companies that want to deploy software and administer centrally. The Enterprise Edition contains all the features of the Personal Edition plus:

- Central and easy configuration using Windows policies in a similar way to other SafeGuard products and Windows itself.
- It checks Certificate Revocation Lists (CRLs) when evaluating certificates.

Since SafeGuard PrivateDisk is installed using Windows Installer, unattended installation can be performed using standard Windows mechanisms.

It is possible to upgrade from the Personal Edition to the Enterprise Edition of the product, but not vice versa.

Demo version

A demo version of SafeGuard PrivateDisk is available at <http://www.sophos.com/products/enterprise/encryption/safeguard-privatedisk/>.

It can be downloaded free of charge.

This is a fully functional Personal Edition for evaluation purposes that works for 30 days without limitation. After that, disks can only be mounted for read access until the product is purchased via the Sophos webshop. A splash screen is shown, additionally, as long as the product has not been purchased.

Upgrade demo version

If you want to upgrade from a demo version to a full version of SafeGuard PrivateDisk, you only need to install the new version over the existing demo version. The demo version can be upgraded to all other versions.

1.5.1 Upgrade to version 2.50

There is no problem upgrading from your existing version to version 2.50. You can still use the new version to use (the volume files on) existing PrivateDisk drives.

Note: Starting with version 2.00 SafeGuard PrivateDisk uses the AES-256 algorithm by default, while older versions used AES-128 (and did not support AES-256). If you would like to use Version 2.50 to generate volume files that can also be used by older versions of SafeGuard PrivateDisk, you must select the encryption algorithm AES-128, and no other encryption algorithm, when you set up the PrivateDisk. PrivateDisk drives that use AES-256 cannot be used together with older versions.

2 Getting started

2.1 Certificates

SafeGuard PrivateDisk allows you to use certificates, including public/private key pairs, instead of passwords. Once a certificate is assigned to a secure virtual disk, it can be used for authentication. Only the owner of the certificate has access to the private key of the certificate and can use it to log on to the virtual disk. Similarly to passwords, certificates can be assigned user or administrator rights.

Below you will find some important information if certificates are being used:

SafeGuard PrivateDisk uses the Microsoft Crypto API for certificate functionality only. Virtual disk encryption itself is performed using our implementations of AES and SHA-1.

SafeGuard PrivateDisk supports all Cryptographic Service Providers (CSPs), e.g. Microsoft Enhanced CSP.

To gain the highest security level we recommend that you use strong CSPs such the Microsoft Strong Cryptographic Service Provider (requires Windows XP or Microsoft High Encryption Pack). These CSPs allow 4096 bit key length and provide strong encryption algorithms (such as 3DES).

Some prerequisites for using certificates with SafeGuard PrivateDisk:

- The certificate must contain a public key.
- For you to access a secure virtual disk using certificates, the private key for the assigned certificate has to be available.
- Only certificates from the *Current User's Personal*, **Address Book** and **Other People** certificate stores and from the **Personal** certificate store of the *Local Computer* are listed. Certificates in other locations are not recognized by SafeGuard PrivateDisk!
Certificates can be imported and organized using the *Certificate* management console snap-in.
- To add a certificate to a virtual disk, only the public key is used. No knowledge of the private key is needed. The private key remains the property of the owner of the certificate and only that person is then able to open the virtual disk.

We recommend that you have the certificates available before starting to install SafeGuard PrivateDisk. This way they are immediately displayed in the *Add Certificates* dialog after SafeGuard PrivateDisk has been installed, and can be assigned to any virtual disk.

Note: SafeGuard PrivateDisk does not administer certificates. Certificates can be administered using a company's own PKI infrastructure or by using trust centers.

2.1.1 Certificate verification

Certificates have to meet certain requirements to be used with SafeGuard PrivateDisk:

- SafeGuard PrivateDisk checks a certificate's validity period. Expired certificates can be used to mount PrivateDisks, but they cannot be assigned to PrivateDisks.
- SafeGuard PrivateDisk checks the critical extensions of certificates. Certificates with unknown critical extensions cannot be assigned to PrivateDisks. In the Enterprise Edition you can change this default reaction within the administrative template.
- Signature certificates cannot be assigned to PrivateDisks. In the Enterprise Edition you can change this default reaction within the administrative template.

Enterprise Edition

- In the Enterprise Edition of SafeGuard PrivateDisk you can perform extended certificate verification. This means that certificates will only be accepted after a complete check of their certificate chain. If necessary, a Certificate Revocation List (CRL) will be downloaded over the network from the issuer of the certificate. If the certificate cannot be checked, access to the PrivateDisk is denied. Extended certificate verification is deactivated by default.
Note: A network connection may be necessary to evaluate a CRL. If this connection cannot be established, access will be denied although the certificate may be valid.
- In the Enterprise Edition, a preferred CSP can be defined in the administrative template. Whenever a user tries to use passwords for authentication, or certificates from a different CSP, they will see a warning message telling them that the preferred CSP offers better security.

2.1.2 Smartcard Reader

Since Cryptographic Service Providers enable certificates to be used, smartcards are automatically supported when you are using a smartcard CSP. It is therefore possible to log on to virtual disks using certificates on smartcards.

If you want to use certificates on smartcards for logging on to a virtual disk please ensure you have installed the smartcard reader and the appropriate Cryptographic Service Provider properly!

2.2 Installation

Note: It is only possible to install SafeGuard PrivateDisk if you are logged on to the operating system with administrator rights.

If you have downloaded the program from the internet, run the downloaded file.

If you have been sent a CD, insert it into your CD-ROM drive. Installation usually starts automatically (if not please run the .exe file or the .msi file in the `Install` directory of your installation CD.)

An installation wizard guides you through the very simple steps to install SafeGuard PrivateDisk.

Please select **I accept the license agreement** in the *Licence Agreement* dialog. Otherwise it is not possible to install SafeGuard PrivateDisk!

SafeGuard PrivateDisk is ready to use immediately after installation.

2.2.1 Tray icon

SafeGuard PrivateDisk places an icon in the Windows Task Bar. You can right-click the icon to display a menu for

- starting the main application (**PrivateDisk**)
- starting the *New Disk Wizard* (**New Disk**)
- importing existing disks (**Import Disk**)
- mounting and unmounting disks (**Mount** or **Unmount**)
- specifying certain settings for SafeGuard PrivateDisk (**Options**).
This is only possible if you are logged on to the system as administrator.

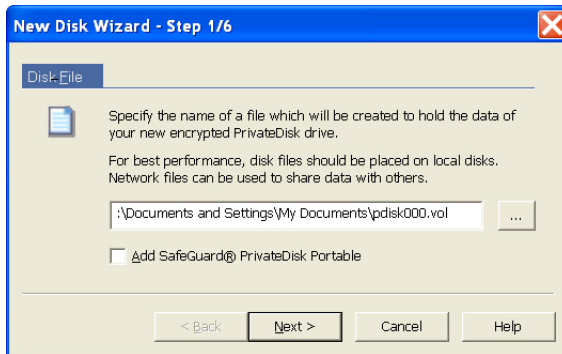
The SafeGuard PrivateDisk main application can also be started by selecting **Start/Program/Sophos/SafeGuard PrivateDisk**.

2.3 Quick start

After installation, use SafeGuard PrivateDisk's *New Disk Wizard*, which helps you create a secure virtual disk in 6 easy steps.

Afterwards the virtual disk you have created can be used like an additional drive on your system. Data in the new drive is encrypted and decrypted automatically.

To create a new secure virtual disk, right-click the SafeGuard PrivateDisk icon in the Windows task bar and click **New Disk**. The *New Disk Wizard* runs.



1. Specify the location and name of the file that holds the data of your new encrypted SafeGuard PrivateDisk drive. The file extension `.vol` specifies your new volume file.

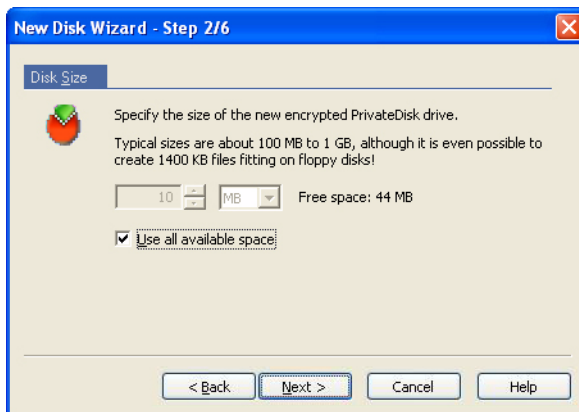
The paths for the creation of the PrivateDisk drives can be restricted by central settings. If you try to create a drive at restricted location, a message will be displayed stating the paths allowed.

- **Add SafeGuard PrivateDisk Portable**

If you activate this option, SafeGuard PrivateDisk Portable will be copied in addition to the `.vol` file to the media.

Using SafeGuard PrivateDisk Portable PrivateDisk drives can be opened on computers without SafeGuard PrivateDisk being installed.

Click **Next**.



- Specify the size of your new SafeGuard PrivateDisk drive. Typical sizes are about 100 MB to 1 GB.

- **Use all available space**

If you select this option, SafeGuard PrivateDisk uses all disk space available on the selected drive for the new PrivateDisk drive.

The available disk space is shown under *Free space*.

The maximum size of a PrivateDisk drive can be restricted by a central setting. If you try to create a bigger drive, a message will be displayed stating the maximum size for PrivateDisk drives.

Click **Next**.

Note: The size of virtual disks cannot be changed after creation. To get more space, a new virtual disk must be created and data from the original disk must be copied to the new disk.



- Select the drive letter for your new SafeGuard PrivateDisk drive. The drive will be displayed like any other local disk. The **Automatic** drive letter option automatically uses the next free drive letter. Click **Next**.



- Choose a file system for your SafeGuard PrivateDisk drive. The drive will be formatted automatically. Click **Next**.

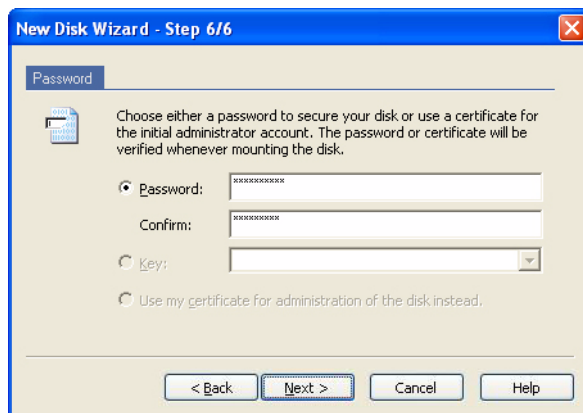
Note: Users who are logged on to the operating system who have NO administrator rights can only choose FAT as the file system for the secure virtual disk.



5. Select an encryption algorithm for the new disk drive. You can choose between AES-128 and AES-256.

Note: Starting with version 2.00 SafeGuard PrivateDisk uses the AES-256 algorithm by default, while older versions used AES-128 (and did not support AES-256). If you would like to use Version 2.30 to generate volume files that can also be used by older versions of SafeGuard PrivateDisk, you must select the encryption algorithm AES-128, and no other encryption algorithm, when you set up the PrivateDisk. PrivateDisk drives that use AES-256 cannot be used together with older versions.

Click Next.

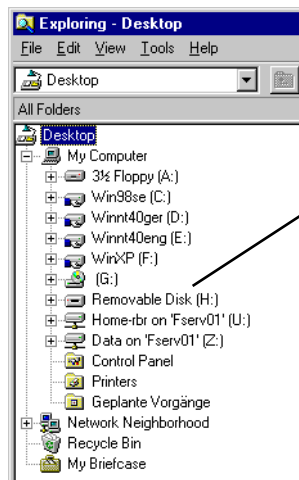


6. Choose:

- **an administrator password** for your new SafeGuard PrivateDisk drive and confirm it.
The password will be verified each time you mount the disk.
- **a key from the SafeGuard Enterprise key ring**
If SafeGuard Enterprise or SafeGuard RemovableMedia is installed on your computer, you can use a key from the relevant key ring. This key will be used for creating and logging on to a PrivateDisk volume. An additional password is not necessary.
- **Use my certificate for administration of the disk instead**
If this option is activated, the certificate of the user is added instead of the administrator password. This option is only activated if a certificate (private key) is available.
If more than one certificate is available, a dialog is displayed in which you must select a certificate.

7. Click **Finish**.

The system creates the new secure virtual disk on your hard disk.



When mounted, the new secure virtual disk is visible like any other of your system's disk drives, and can be used in the same way. Data is encrypted and decrypted automatically.

Unmounting the disk (right click in Explorer) closes the disk and removes it from the list of available drives.

2.4 Unattended installation

Unattended Setup means setup with no user interaction. It is a way for you to install SafeGuard PrivateDisk on a large number of machines using an automated procedure.

The `Install` directory of your installation CD contains the `sgpd100.msi` file which is necessary for any unattended installation.

2.4.1 Command line syntax

To perform an unattended installation you must run `msi exec` with certain parameters.

Mandatory parameters:

`/I`

Specifies the installation package to install.

`/QN`

Installation without user interface (unattended setup)

Name of the `.msi` file: `sgpd100.msi`

Syntax:

```
msiexec /i <path>\sgpd100.msi /qn
```

Optional parameter:

`/L* <path + filename>`

Logs all warnings and all error messages in the location specified at `<path + filename>`.

EXAMPLE:

```
msiexec /i C:\Install\sgpd100.msi /qn
```

As a result the system performs a complete installation of SafeGuard PrivateDisk. The program is installed in the default installation directory (`<System drive>\Program Files\Sophos`). The `msi` file resides in the `Install` directory on the C drive.

3 SafeGuard PrivateDisk main application

The SafeGuard PrivateDisk main application can be started by right-clicking the icon in the Windows task bar and clicking **PrivateDisk** or by selecting it from the Windows programs folder (Start/Programs/Sophos/SafeGuard PrivateDisk).



The left-hand side of the main application window displays a list of all available secure virtual disks.

If a disk is selected, the right-hand side of the main application window displays the details of the disk that is selected in the disk list. If no disk is selected, for example after the application has been started, the system displays a welcome screen with information about basic tasks (creating new secure virtual disks, importing disks).

You can select a disk and press the **Del** key on the keyboard (or click *Edit/Remove from List*) to remove that disk from the list of available disks. The volume file is still available and can be imported into the list of available disks again.

To really delete a disk (or, in fact, the volume file), unmount it first, select it and click *Edit/Delete*. The system displays a dialog warning you that all data stored on the disk will be destroyed. If you confirm by clicking **Yes**, the system deletes the volume file.

3.1 Toolbar and menu commands

SafeGuard PrivateDisk includes a toolbar that contains buttons for the most important commands:



- **New:**
Starts the wizard for creating a new virtual disk.
- **Mount:**
Mounts the selected virtual disk.
- **Unmount:**
Unmounts the selected virtual disk.
- **Passwords:**
Displays the *Change Disk Password* dialog in which you can change/set passwords (administrator and user password) for the virtual disks.
- **Certificates:**
Displays the *Disk Certificates* dialog in which you can assign and modify certificates for a virtual disk.
- **Options:**
Changes the program settings. This option is available only for system administrators.
- **Help:**
Opens the SafeGuard PrivateDisk online help.
- All these commands can also be found in the different menus (*File, Edit, View, Tools, Help*).

Alternatively you can click the SafeGuard PrivateDisk icon in the Windows task bar to access the most important functions (and to start the main SafeGuard PrivateDisk application).

3.2 Information about the selected disk

If a disk is selected in the list of available secure virtual disks, the right-hand part of the main windows displays detailed information about the selected disk:

- **Name:**

Every virtual disk can have a symbolic name. The default name is the disk file name without path information. It can be changed in this disk information dialog.

To change the name of the disk, change the name in the edit field and press Enter. The new name is displayed in the list of available files. It only applies in this list! In the Windows Explorer each virtual disk is displayed as: `Removable Disk (drive letter)`!
- **Status:**

Shows the current status of the virtual disk.

 - **Mounted:** The virtual disk is mounted and available.

In brackets the system also displays the access rights with which the disk is mounted (Administrator, User or Read Only).
 - **Not mounted:** The virtual disk is not mounted.
 - **File not found:** The specified volume file does not exist (e.g. if the file has been renamed, moved or deleted).
 - **Not a PrivateDisk volume file:** The file is not a valid SafeGuard PrivateDisk volume file.
 - **Access is denied:** Access to the volume file is denied, e.g. by NTFS rights.
- **Disk File:**

Displays the location and name of the volume file that stores the encrypted data for the virtual disk.
- **Drive Letter:**

Displays the current drive letter of the virtual disk and provides a place for you to change it. Drive letters can either be fixed (from A to Z) or can be set to **Automatic**. In this case the system uses the next free drive letter when it mounts the virtual disk.

Drive letters can be changed by the user at any time. Changes become effective the next time the virtual disk is mounted.

Therefore, if you change the drive letter, the system displays a dialog, asking if you now want to remount the disk. Click **Yes** to make changes effective immediately.

■ **Startup:**

Defines when and how the selected virtual disk should be mounted. The following options are available:

■ **Mount manually**

The disk is not mounted automatically. The user has to mount the disk every time they want to use it.

■ **Mount after user logged on to the system**

The disk is mounted automatically when the user logs on to the operating system.

Note: If you select the option **Mount after user logged on to the system**, you must also select the option **Automatic Login At Startup** on the General page of the settings dialog.

■ **Mount when volume file is accessible**

The disk is mounted automatically when the drive for the virtual disk's volume file becomes available. This option is for virtual disks on network drives and plug&play drives.

■ **Mount when smartcard is inserted**

The disk is mounted automatically after inserting a smartcard.

Note: If you select the option **Mount when smartcard is inserted**, you must also select a smartcard reader on the Smartcard page of the settings dialog.

■ **Attributes:**

Here you can specify mount options for the virtual disk.

■ **Read only:**

If you select this option, the disk is mounted for read only access, even if the user has read/write access privileges to the volume file.

With write access a virtual disk can only be mounted by a single user. The **Read Only** attribute can be used to give more than one user simultaneously access to a secure virtual disk.

Changes made by the user with write access will be visible to the other users after a short delay.

■ **Fixed Disk:**

If this option is selected, SafeGuard PrivateDisk simulates a hard disk, and not a removable disk - the drive icon in the Windows Explorer differs accordingly.

This option has to be activated to make a virtual disk shareable.

Drives can only be shared if you are logged on with administrator rights.

■ **Disk Size:**

Displays the size of the selected virtual disk.

In addition to the size, the system displays the algorithm that is used for encryption.

Note: Drives that have been encrypted with AES-256 cannot be used in SafeGuard PrivateDisk versions older than 2.00.

- **Passwords:**

Under **Passwords** you can see which passwords have been set for the virtual disk. A secure virtual disk may have one administrator password, or one administrator password and one user password, or only one user password, if a certificate with administrator rights is assigned to the disk.

- **Certificates:**

Under **Certificates** you can see a list of all certificates associated with the virtual disk. For every certificate additional information is given about privileges (user or administrator) and access (read only or read/write).

It is only possible to edit the list of assigned certificates with administrator privileges for a virtual disk (see above).

3.3 Creating a new virtual disk

New disks can be created in the following ways:

- Click the **New PrivateDisk** button in the *Welcome* dialog.
- Click the **New** button in the SafeGuard PrivateDisk toolbar.
- Choose **New** from the *File* menu.
- Click **New Disk** after right-clicking the SafeGuard PrivateDisk icon in the Windows task bar.

In every case the *New Disk Wizard* runs and guides you through the steps for creating the disk.

3.4 Mounting and unmounting disks

Before you can access a secure virtual disk, the disk has to be mounted. To be able to mount a disk, a user must have a password for the disk or has to own the private key of a certificate assigned to the virtual disk or the SafeGuard Enterprise key used for creating the drive has to be available to the user.

To mount/unmount a disk manually:

- Select the disk in the disk list and click the **Mount/Unmount** button in the SafeGuard PrivateDisk toolbar.
- Select the disk in the disk list and click **Mount/Unmount/Unmount All Disks** from the *Edit* menu.
- Click the SafeGuard PrivateDisk icon in the Windows task bar. When you select **Mount/Unmount** the system displays a list of disks from which you can choose one to mount/unmount.
- Select the volume file in the Windows Explorer and click **Mount/Unmount** in the SafeGuard PrivateDisk context menu.

You will be prompted for a password or PIN if needed.

If a user cannot log on to a virtual disk because another user is already logged on, the name of the user who is already logged on is displayed as a hint.

If a virtual disk cannot be unmounted because of an application that has references to the disk, the user can choose one of the following options:

- **Retry**
Logs off the user after the user has closed the appropriate application or file.
- **Force dismount**
Logs off the user, even if the virtual disk is in use.
Warning:
this may lead to loss of unsaved data!
- **Cancel**
The user remains logged on to the virtual disk.

Beside mounting a disk manually, SafeGuard PrivateDisk offers different logon methods to disks, including **Automatic Login at Startup**, **Single Login**, **Mount when smartcard is inserted**, , etc. Please see the appropriate sections for more information.

3.5 Importing a Virtual Disk

If you want to use a virtual encrypted disk which is not already in the list of available disks, use the **Import Disk** command in the *File* menu to import it to the list of available disks.

A dialog is displayed in which you can select the volume file. Select the file and click **Open**. The disk is added to the list of available virtual disks.

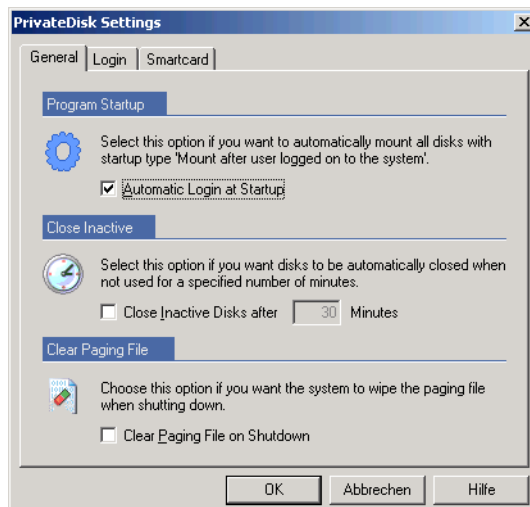
3.6 SafeGuard PrivateDisk settings

SafeGuard PrivateDisk offers certain settings with which you can adapt it to suit your personal needs. These settings can be found in the *PrivateDisk Settings* dialog. Open the *PrivateDisk Settings* dialog by clicking the **Options** button of the toolbar in the SafeGuard PrivateDisk main application (or clicking **Options** in the *Tools* menu). Alternatively, open the *PrivateDisk Settings* dialog by right-clicking the icon in the Windows task bar and clicking **Options**.

The *PrivateDisk Settings* dialog contains three different pages:

3.6.1 General page

The *General* page contains general options that specify the behavior of SafeGuard PrivateDisk.



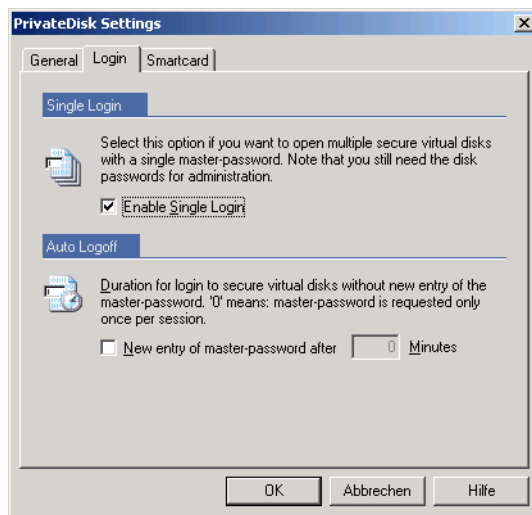
- **Automatic Login at Startup:**

If you select this option, all disks with startup type Mount after user logged on to the system are mounted automatically when the user logs on to the operating system.

Depending on the settings, dialogs may pop up prompting the user to enter the disk passwords, or a single dialog box in which the user must enter the single login password.

- **Close Inactive Disk After:**
If you select this option, all mounted disks are closed when they have not been used for the specified number of minutes.
- **Clear Paging File On Shutdown:**
Since the paging file might contain sensitive data, SafeGuard PrivateDisk offers an option for emptying it when the system is shut down.
If this option is activated, the paging file is wiped on shutdown and is therefore no longer a potential security risk.

3.6.2 Login page



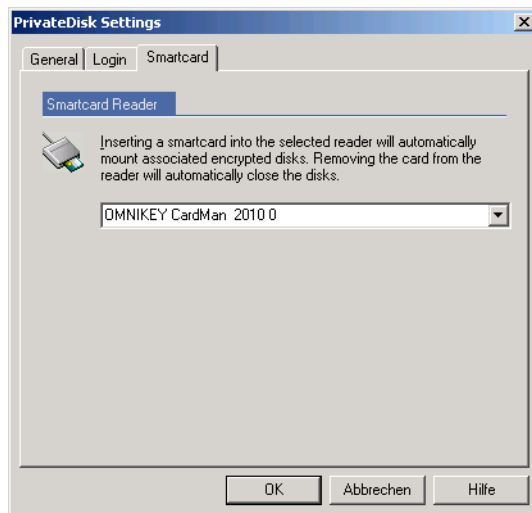
- **Enable Single Login:**
If a user wants to use more than one virtual encrypted disk, SafeGuard PrivateDisk asks for the passwords of all these disks, one after the other.
For this purpose SafeGuard PrivateDisk includes a Single Login feature that works with a master password. If you select this option, a master password is used to securely store the passwords for the virtual disks. The user then only has to enter this single master password instead of all virtual disk passwords.
The passwords for the virtual disks are remembered as soon as they are entered by the user the first time the Single Login feature has been enabled.
To change the Single Login password you can use the Tools/Change Single Login Password menu option.
To prevent repeated prompts for the master password, the Single Login password is saved in memory for a configurable time.
- **New entry of master password after**
If you select this option you can specify a duration (in minutes) after which the Single Login password is cleared from memory.

Note: The single login feature is not available for login with certificates.

3.7 Smartcard page

When a smartcard is inserted in the card reader, virtual disks with startup type **Mount when smartcard is inserted** are mounted automatically.

When a smartcard is removed, all virtual disks configured with startup type **Mount when smartcard is inserted** are unmounted.



To use this feature of SafeGuard PrivateDisk, you must specify the card reader that SafeGuard PrivateDisk is to use. Select the corresponding card reader in the drop-down menu on the *Smartcard* page.

3.7.1 The LDAP page

This dialog is only available in the Enterprise Version.

When you are assigning certificates to a PrivateDisk drive SafeGuard PrivateDisk enables you to use an LDAP search to find particular users.

The settings for this search are displayed in this dialog. Usually they cannot be changed here, since they are defined via an administrative template in central Administration. The options in this dialog can only be changed by a user who is logged on to SafeGuard PrivateDisk with administrator rights.

Searching for a specific certificate (for example, by using the e-mail address in the certificate) allows this certificate's user to access a PrivateDisk drive because the drive is assigned to their certificate.

When a certificate is assigned these settings can be made or changed locally even if the user does not have administrator rights.

3.8 Passwords and certificates

A virtual disk can have exactly one administrator password and one user password (either with read/write access or with read access only).

Additionally, certificates can be assigned to virtual disks.

While only two passwords can be assigned to a virtual disk, SafeGuard PrivateDisk allows up to 32 certificates to be assigned for authentication purposes.

Similarly to passwords, certificates can also be assigned user rights (read/write or read access only) or administrator rights.

3.8.1 Access to secure virtual disks

Logon with passwords

Access to a virtual disk can be granted by specifying a password. For each disk SafeGuard PrivateDisk allows you to use three kinds of passwords, but only one of the user passwords can be assigned to a virtual disk in addition to the administrator password:

- **Administrator password:**

This is the initial password for every new virtual disk. Using a virtual disk's administrator password you can specify one user password for the disk, reset the user password (even if it is not known), modify the administrator password and also add certificates to the disk, or remove them (see below).

Note: It is also possible to use certificates that have administrative rights.

When a new virtual disk is created, a certificate for these administration tasks can also be specified!

- **User password with read/write access:**

This user password enables a user to mount the disk and access data within the disk.

- **User password with read only access:**

This user password enables a user to mount the disk but only allows them to read the content of the disk.

Logon with certificates

Using passwords for virtual disk access is optional. Certificates can be used in addition to, or instead of, passwords.

Up to 32 certificates can be associated with each virtual disk. In this case the system uses the public key from within the certificate for encoding the disk encryption key. Only the owner of the certificate has access to the private key of the certificate and can use it to log on to the virtual disk.

Similarly to passwords, certificates can also be assigned user rights (read/write or read only access) or administrator rights.

Logging on to virtual disks using certificates has several benefits:

- Administrators using the administrator password for a virtual disk can easily assign users to it, using the available public part of the user's certificate.
- It is not necessary to create and distribute initial passwords.
- As with passwords, certificates can be added either as users (may access the data either for read only or read/write access) or administrators (are allowed to change the passwords and the assigned certificates).
- Before a user can add certificates to a virtual disk, or remove them, they must first authenticate themselves as administrator for the disk (either using the administrator password or by owning one of the administrator certificates assigned to the virtual disk).

Single logon

When multiple virtual disks are in use, users must authenticate themselves separately to all virtual disks. When passwords are in use, the user must remember and enter all necessary passwords. Not only is this inconvenient when many disks are being used, but it also tempts people into using the same password for all their virtual disks, which creates a security risk.

To overcome this difficulty, SafeGuard PrivateDisk includes a Single Login feature which remembers the passwords of virtual disks for the user. Passwords are stored in encrypted form in the Registry and are used automatically when the user mounts a virtual disk. A master password (Single Login password) is used to secure the list of passwords. The user therefore only has to remember and enter this Single Login password.

Automatic logon/logoff

SafeGuard PrivateDisk can be configured to automatically mount virtual disks after the user logs on to the operating system. Of course, it first prompts the user to supply the necessary passwords or certificates.

Virtual disks are closed automatically when a user logs off. Additionally, virtual disks can be closed automatically after a specified time of disk inactivity.

Smartcard support

SafeGuard PrivateDisk also supports the use of certificates stored on smartcards. Logon to secure virtual disks is performed using their private key, stored on the inserted smartcard.

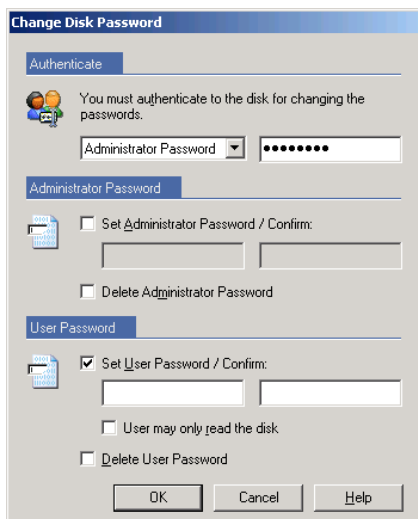
SafeGuard PrivateDisk reacts to the insertion and removal of smartcards and is able to automatically mount and unmount virtual disks:

- When a smartcard is inserted, all virtual disks configured with startup type **Mount when smartcard is inserted**, are mounted automatically.
- When a smartcard is removed, all virtual disks authenticated by a certificate from the smartcard are unmounted.

Note: SafeGuard PrivateDisk does not administer certificates. Certificates can be administered using a company's own PKI infrastructure or by using trust centers.

3.8.2 Editing passwords

If you need to edit passwords, you can use the SafeGuard PrivateDisk *Change Disk Password* dialog. To open this dialog click **Passwords** in the toolbar or select **Change Password...** in the *Edit* menu.



In this dialog you can:

- **Set/Change the Administrator Password**
To change the administrator password, the user must be the administrator of the disk involved (either by knowing the old administrator password or owning one of the administrator privilege certificates associated with the disk).
- **Set/Change the User Password**
To change the user password, the user must be able to log on to the virtual disk (either by knowing the old user password, or the current administrator password, or by owning one of the administrator privilege certificates associated with the disk).

- **Delete the User Password**

To delete the user password, the user must be the administrator of the disk involved (either by knowing the administrator password or owning one of the administrator privilege certificates).

To change the administrator password you must authenticate yourself to the disk using the administrator password for the disk:

- Select **Administrator Password** in the Authenticate section of the dialog and enter the administrator password.
- Select the **Set Administrator Password** option.
- Enter a new administrator password and confirm it.

Note: If a certificate with administrator privileges is used (by selecting **Certificate** in the drop-down list of the Authenticate section) an administrator password can also be deleted by selecting the appropriate option. The disk can then only be administered by someone who owns a certificate that has administrator privileges.

You can set and change a user password in the same way.

If you authenticate yourself to the disk using the user password, it is only possible to change the user password.

You can only set a user password for the virtual disk or delete the user password if you have administrator rights (either through the administrator password or a certificate that has administrator rights).

3.8.3 Password delay

After the user enters an incorrect password their next logon attempt will be delayed. The delay increases from 2 seconds to 5, to 10, and to a maximum of 20 seconds. The actual delay is remembered individually for the last 10 disks used in SafeGuard PrivateDisk.

3.8.4 Assigning certificates

Access to virtual disk can also be granted by assigning certificates (up to 32) to the virtual disk.

Note: If there are multiple users, it is not possible to open the same virtual disk volume files for read and write access simultaneously. If groups of users want to have access to a single virtual disk at the same time, they must open this disk for read-only access.

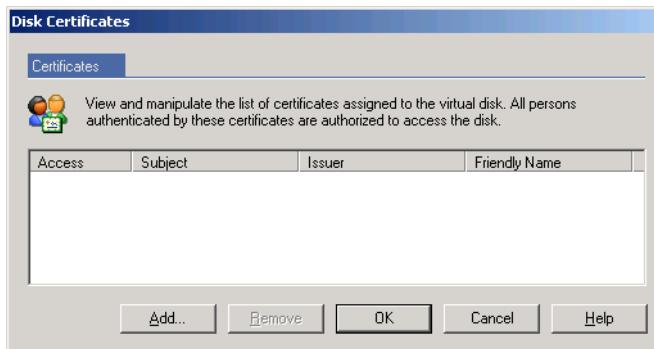
Similarly to passwords, SafeGuard PrivateDisk distinguishes between the following:

- Administrator Certificates
- User Certificates
- User Read Only Certificates

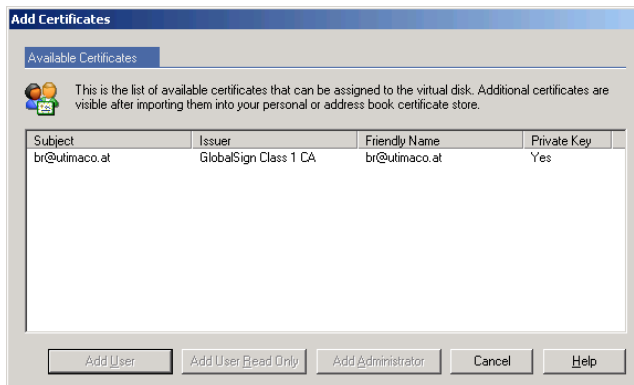
Note: Before you can assign certificates to a virtual disk you must first authenticate yourself to the disk with the administrator password or an existing administrator certificate.

To add certificates to a virtual disk:

1. Click **Certificates** in the toolbar or select **Certificates...** in the *Edit* menu.
2. Enter the administrator password for the virtual disk and click **OK**.
The system displays the *Disk Certificates* dialog.



3. All certificates currently assigned to the virtual disk are displayed in this dialog.
4. To add certificates, click the **Add** button.
The system displays the *Add Certificates* dialog.



5. The system displays a list of available certificates that can be assigned to a disk.

Note: Only certificates from the **Current User's Personal**, **Address Book** and **Other People** certificate stores and from the Personal certificate store of the Local Computer are listed. Certificates in other locations are not recognized by SafeGuard PrivateDisk!

Using LDAP to find a certificate

If you want to assign a certificate that is not yet held in these certificate stores, SafeGuard PrivateDisk provides a way to use an LDAP search to find a certificate. LDAP search settings can be defined centrally, and appear under Options on the LDAP page.

- To search for a certificate, click **Search certificates** in the *Add certificate dialog*. The *LDAP Search* dialog opens.
- Click the **Search** button. SafeGuard PrivateDisk lists all the certificates it finds using the search data you entered (connection data and search filter).
Filters are defined so that you can search for specific data in a certificate (for example, e-mail address). For example, if you use the e-mail address to search for a particular certificate, you are prompted to enter the e-mail address of the person whose certificate you want to assign to the PrivateDisk disk drive.
You can also use different data to search for a certificate. You are prompted to enter different required information, depending on which filters the administrator has defined. Please note that you must enter this data (for example, cn - Common Name) exactly as it appears in the certificate.
- In the bottom part of the dialog, SafeGuard PrivateDisk displays all the certificates that match your search criteria. It only shows certificates that can be used with SafeGuard PrivateDisk.
- Mark the certificate you require and click on **Add** to transfer it to the list of available certificates, where you can now assign it a disk drive. The public part of the certificate is copied to the certificate store.

Changing the LDAP search

Click on the **Extended** button to display the LDAP settings so you can change them. These settings should only be changed by an administrator because they require extensive LDAP knowledge.

However, a "normal" user may also need to change the filter that is used. For example, a variety of filters can be defined and then used to search by e-mail address or by the certificate's Common Name. You can select one of the predefined filters displayed under **Filter**. If you delete the **Filter** line in this dialog, the system displays all the certificates found in the specified LDAP directory service. This may be helpful if, for example, you do not know exactly how the data you are looking for is written (user name in certificate, Common Name, e-mail address, etc.). You can then select the certificate you require from the list. Please note that this procedure may result in a very long list of certificates!

Saving settings

If you change the settings in the LDAP Search dialog, you can save them and reload them again by clicking one of these buttons, which are located at the top, on the right. When you save the settings you must define a name for these settings. You can use this name to identify these settings again later. When you are loading settings you can then select the settings you want from a list.

6. Select a certificate from the list, and click one of these settings, depending on which rights you want to grant to the user associated with the certificate:
 - Add User
 - Add User Read Only
 - Add Administrator
7. The certificate is displayed in the list of certificates assigned to the virtual disk. Under *Access* you can see the access right for this particular certificate.

3.8.5 Deleting certificates assigned to a disk

To delete certificates assigned to the disk:

1. Click **Certificates** in the toolbar or select **Certificates...** from the **Edit** menu.
2. Enter the administrator password for the virtual disk or use your certificate for authentication and click **OK**.

The system displays the *Disk Certificates* dialog.
3. To remove a certificate from the list, select it and click **Remove**.

The owner of the certificate no longer has access to this virtual disk.

3.9 SafeGuard Enterprise keys

SafeGuard Enterprise keys can be used for mounting a PrivateDisk drive. If a key ring exists, the SafeGuard Enterprise keys will be offered for selection when creating a drive using the SafeGuard Private Disk Wizard.

If a SafeGuard Enterprise key is assigned to the drive, only this key will be used for mounting the PrivateDisk drive. An additional password is not required. If the key exists on the computer, it will be used automatically for mounting the PrivateDisk drive. If option *Mount after user logged on to the system* is enabled for the drive, the mounting procedure will be carried out transparently. The drive is available after logging on to Windows.

Local keys

SafeGuard Enterprise differentiates between keys which are created centrally and distributed to the users automatically and keys which are created locally on the client computers. Local keys have a passphrase for accessing them.

Local keys can also be used for mounting PrivateDisk drives. If the key exists on the computer, it will be automatically used for mounting the drive.

If the local key is not available on the computer, the user will be prompted to enter the passphrase.

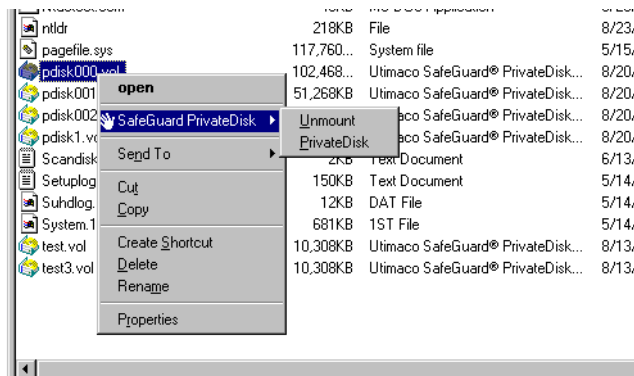
If a user who does not have the local key of the PrivateDisk drive is to be granted access to the volume, the user has to be provided with the key passphrase.

3.10 Windows Explorer extensions

SafeGuard PrivateDisk adds a menu item called *SafeGuard PrivateDisk* to the Windows Explorer context menu.

Depending on the selected file or disk in the Windows Explorer, the following commands are available:

- If you right-click a volume file (.vol), the system displays a menu item for mounting/unmounting the virtual disk (depending on its status) and for starting the main application.
- If you right-click a volume file (.vol) which is not already added to the list of available disks in the SafeGuard PrivateDisk main application, the system displays an **Import** command in the context menu. Click **Import** to add the virtual disk to the list of available virtual disks in the main SafeGuard PrivateDisk application.



4 SafeGuard PrivateDisk Portable

Using SafeGuard PrivateDisk Portable you can access PrivateDisk drives even if SafeGuard Private Disk is not installed on the computer.

This is achieved by a specific program (PDPortable.exe) that is copied to removable media. You can select an option for copying SafeGuard PrivateDisk Portable to the removable media when creating a PrivateDisk drive.

When connecting the removable media to a computer without SafeGuard Private Disk you cannot access the PrivateDisk drive. However, after starting SafeGuard PrivateDisk Portable you can select the PrivateDisk drive and after entering the password for this drive you will be granted read access to the encrypted files.

You cannot add files to the PrivateDisk drive using SafeGuard PrivateDisk Portable. However, you can save files from the PrivateDisk drive to a different file location. In this case, the files will be saved unencrypted at the new location.

4.1 Opening PrivateDisk drives

To open a PrivateDisk drive:

1. To start SafeGuard PrivateDisk Portable double-click `PDPortable.exe`.
2. Click **File > Open** and select the PrivateDisk drive.
3. Enter the password for the PrivateDisk file.

Note: For exchanging data using this method, the password has to be communicated to the recipient of the SafeGuard PrivateDisk drive.

4. SafeGuard PrivateDisk Portable now displays the drive and its contents. A functionality similar to Windows Explorer is available now.
5. You can open files by double-clicking them.

4.2 Extracting files

To extract files from a PrivateDisk drive:

1. Select the file(s).
2. Click **Edit > Extract**.
3. Select a file location for the file(s).
4. Click **Save**.

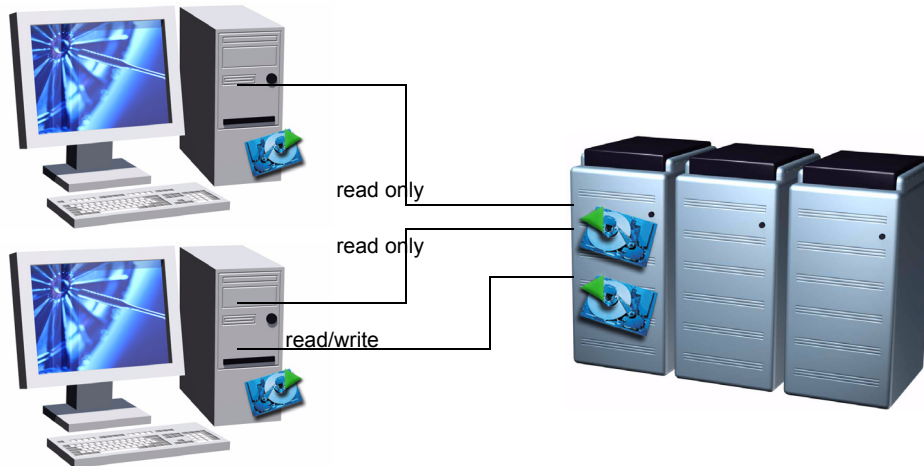
5 Use cases - examples

SafeGuard PrivateDisk is an easy to use solution for securing files on workstations, notebooks, file servers and terminal servers. In the sections that follow you will find some examples of the most typical scenarios for securing confidential data with SafeGuard PrivateDisk.

5.1 Workstation user

Virtual disks for workstation users are typically created on local fixed drives or on network locations. SafeGuard PrivateDisk guarantees confidentiality, even when data is being exchanged over a network, so a workstation user only has to open the secure virtual disk on the file server. SafeGuard PrivateDisk only needs to be installed on the workstations. It is not necessary to install SafeGuard PrivateDisk on the file server. The file server only stores the secure virtual disks.

Our example shows two workstations on a network, and a file server. On the file server, two secure virtual disk volume files are stored. One of the virtual disks is used by multiple client machines, so it is opened for read access only. The second virtual disk is opened by a single client machine, so the client has read and write access.



Benefit from using SafeGuard PrivateDisk:

- Users can store confidential data on server machines securely.
- Users can have simultaneous read access to virtual disks.
- Data transmitted between clients and servers is always encrypted, since encryption and decryption is performed by the client machines.
- No additional CPU capacity is needed on server machines since encryption is performed by the workstations.

- Administrators of server machines have no access to the confidential data if they are not authorized to open the virtual disks. This enables security administrator and system administrator tasks to be kept separate, for example.
- A security administrator can create centrally located virtual disk volume files.
- Volume files on server machines can easily be included in the company's server backup plan.

Note: Since access to a secure virtual disk is controlled like access to a single file, multiple users cannot access a secure virtual disk simultaneously (open it with read **and** write access). If a virtual disk is mounted by a user with read/write rights, the disk cannot be mounted by any other user. To give multiple users simultaneous access to a secure virtual disk, they must all mount it for read access only.

Simultaneous read/write access to secure virtual disks

Virtual encrypted disks can be shared with network users like normal drives. So if SafeGuard PrivateDisk is installed on a server machine, this machine can share its open virtual disks with network users. Client machines can mount these shared virtual disks like standard network resources. User groups can then have concurrent full (read and write) access to shared encrypted virtual disks.

Please note:

- Access to shared virtual disks is only protected using operating system functions (by a password or user credentials). Clients do not need to authenticate themselves to the virtual disks.
- Data between servers and clients is transmitted in clear (unencrypted) text since decryption is performed on the server machine. VPN software can be used to secure the connection.
- The virtual disks must be opened on the server by an authorized person.

5.2 Mobile user

The biggest security threat for notebook users is theft. Although SafeGuard PrivateDisk cannot protect notebooks from being stolen, it can be used to ensure that confidential data cannot be read by outsiders.

Our example shows a notebook with one local secure virtual disk and a second virtual disk on CD-ROM (e.g. containing internal product price lists, etc.). Data can be updated between headquarters and the mobile user in a secure way by using virtual volume files on CD-ROM. Only authorized users can open the virtual disk (with a password or by owning the private key of an assigned certificate) and read its contents.



Benefit from using SafeGuard PrivateDisk:

- Confidential data on the local hard disk is protected when the notebook is turned on, as well as if it is lost or stolen.
- For unauthorized persons the secure virtual disk looks like a normal file, and the directory structure is also hidden from them.
Confidential data is even protected against people who have physical access to the notebook provided the password needed to open the secure virtual disk is not known, and the private key of any assigned certificates is properly protected.
- Confidential data can be made secure without having to encrypt the whole hard disk or entire partitions.
- Volume files for secure virtual disks can be easily stored on hard disks, network drives and removable media (floppy disks, ZIP disks, CD-ROMS, USB memory sticks, etc.).
- Volume files for secure virtual disks can be exchanged securely over insecure channels such as e-mail.

5.3 Terminal servers

SafeGuard PrivateDisk can be installed on terminal servers. To ensure privacy between the terminal server users, a secure virtual disk is visible only to the user who has opened that virtual disk.

Benefit from using SafeGuard PrivateDisk:

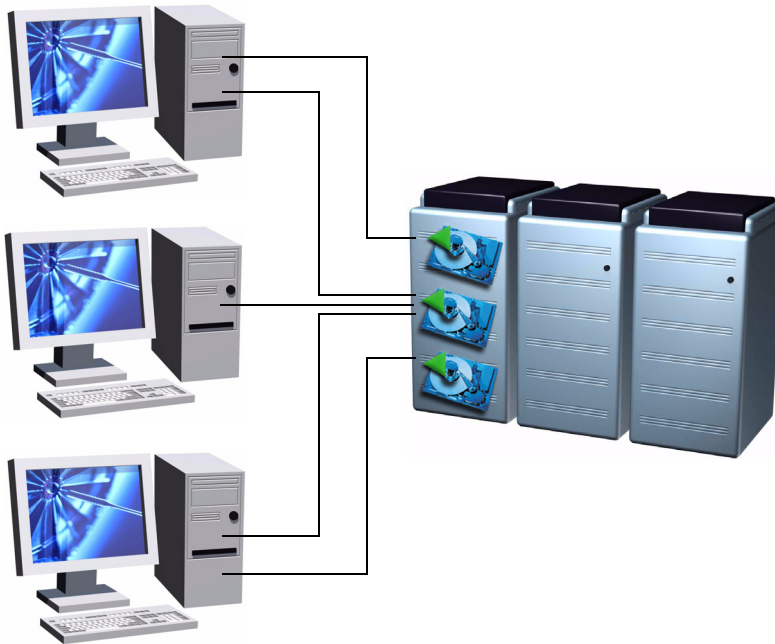
- Users can work with confidential data which is not accessible to the system administrator of the terminal server machine.
- Secure virtual disks are visible only to authorized users. If one user opens a virtual disk, it is only visible to other users if they also open the same virtual disk.

Example:

User USER 1 opens a secure virtual disk as drive X.

USER 2 does not see USER 1's drive X but can also open the same secure virtual disk. USER 2 could even open a different encrypted virtual disk as drive X.

- Multiple users can share read and write access to a single secure virtual disk. **This allows groups of users to work simultaneously on the same virtual disks!**
- Data transferred between the terminal server and its clients is secured by means of the terminal server protocol.
- Only the terminal server machines have to be administered (software installation etc.)



The figure shows a terminal server environment in which two of three users have secure virtual disks and all users also share another virtual disk.

Note: Although multiple terminal server users may simultaneously use a secure virtual disk, the disk may have different drive letters for each terminal server session, depending on the client machine and session configuration. For instance, the shared secure virtual disk in the example might be drive D on the first machine and drive E on the second.

5.4 Encrypted backups

SafeGuard PrivateDisk can be used for encrypted backups.

This is achieved by copying the files to be backed up to a virtual encrypted disk, and then saving the virtual disk volume file to the backup media.

When virtual disk volume files are in use on networks, a backup of the network servers automatically includes the encrypted virtual disk content.

Benefit from using SafeGuard PrivateDisk:

- Confidential data is stored securely on backup media.
- The backup administrator does not have access to confidential data.

5.5 Fast user switching

SafeGuard PrivateDisk supports Windows XP's "Fast User Switching" technology. Since the Windows XP fast user switching feature is based on terminal server technology, using SafeGuard PrivateDisk with fast user switching on Windows XP is comparable to using the software on a terminal server. This offers enhanced flexibility when several users use files and computers simultaneously.

Benefit from using SafeGuard PrivateDisk:

- Virtual encrypted disks are visible and accessible only to authorized users, e.g. if one user opens a virtual disk, this is not visible to other users.
- One user's virtual disks stay open while the PC is switched to another user, but they cannot be read by this user. This allows applications to continue accessing encrypted data in the background.

6 Central administration

6.1 Product configuration and policy

The Enterprise Edition of SafeGuard PrivateDisk is shipped with an administrative template (sguard.adm) that can be used to create policy files (if no Active Directory is available) or group policy objects (for Active Directory) for users and computers. The administrative template sguard.adm is stored in the ADM subdirectory of the installation directory. The policies contain settings for all SafeGuard PrivateDisk options. Additionally they enable specific lists of virtual disks available to the users to be defined, and also the creation of an initial virtual disk upon logging in for the very first time.

Policies created by the system administrator are deployed automatically by the operating system when users log on to the domain server or Active Directory.

Since users in an IT environment usually do not have administrative privileges they cannot change the product settings.

6.1.1 Administrative template sguard.adm

To use the administrative template for SafeGuard PrivateDisk, open the Group Policy Editor and add the administrative template.

Afterwards the system displays a *SafeGuard...* node for computer configuration and user configuration.

For computer configuration the administrative template contains nearly the same settings as the SafeGuard PrivateDisk application's Settings dialog, except for password restrictions.

Note: For settings which are not described in this chapter in detail, refer to the the relevant Properties dialog of the Administrative Template. The settings are explained there.

System Policy Editor:

SafeGuard PrivateDisk

Group Policy Editor (Active Directory)

Computer Configuration\
Administrative Templates\
SafeGuard\
PrivateDisk

- **General**

- **Automatic Login to Virtual Disks**
- **Automatic Unmount of Inactive Virtual Disks**
- **Preferred CSP**

When you are using certificates for authentication you can specify your preferred "Cryptographic Service Provider" (CSP), e.g. a specific smartcard CSP. The CSP name must be part of the CSP's name from the registry. The friendly name is used for presenting messages to the user and is optional.

- **Login**

- **Single Login**

- **Smartcard**

- **Smartcard Reader**

Warning! The name of the smartcard reader is case sensitive!

- **LDAP**

In this tab page you can define settings that can be used to search for a certificate using LDAP. The system displays these settings on the LDAP page, in the Options dialog, and also displays them at the start of the search for assigning a certificate. It is not possible to change these settings in the Options dialog (unless the user is logged on with administrator rights), however it is possible to change them when assigning the certificate.

- **Host**

In the **Host** field, enter the domain name or IP address of the LDAP server.

- **Port**

In the **Port** field, enter the TCP port that is to be used to set up the connection. If you leave this field empty, the default port 389 will be used.

- **Protocol Version**

Here, select the version of the protocol that is to be used from the list.
The default is version 3.

- **Anonymous**

If this option is selected, the system attempts to set up an anonymous connection to the host.

If you do not want the connection to be anonymous, enter valid access data for the LDAP server when you are setting up the connection.

- **Authentication**

Here you can specify the required type of authentication to the LDAP server. The default is GSS (Generic Security Services).

The parameters below affect the search in the LDAP structure.

- **Base**

Here you can specify the node in the LDAP structure from which the system searches for the certificate. This enables you to restrict the search to one part of the tree structure, so certificates can be found more quickly (example: only search in one particular OU (organizational unit)).

You must specify the node from which the system begins the search.

- **Filter**

In the Filter list input field you can define a filter for searching for a certificate. When the user is assigning the certificate they are only shown certificates that match the filter. This is, for example, a way to search for the Common Name or E-mail address in a specific certificate.

Filter syntax:

A filter consists of a description (Filter name), the actual filter definition (which states the criteria used for the search, for example: "cn=") and an optional parameter list.

In the variable part of the filter definition, enter "%s" (for example: "cn=%s"). The search queries this %s parameter. The user is prompted to enter the appropriate information. In the filter the system replaces the parameter with the value entered by the user.

In the parameter list, a parameter name can be set for each placeholder in the filter definition. The system displays the parameter name to the user when it prompts them to enter their value so that they can see what type of information they are required to enter.

If you enter parameter names, separate them with a comma.

Enter the filter name, filter definition and parameter list in quotation marks, and separate them with a comma.

If you enter several filters, separate them with a hyphen.

When the user is assigning a certificate they can select the filter that is to be used from a list of filter names.

Example:

"E-mail search","mail=%s","E-mail address"

If the "E-mail search" filter is selected for finding a certificate, the user is prompted to enter the e-mail address of the user that is being searched for (the system displays E-mail address in the dialog). The system displays all certificates that contain the relevant e-mail address.

Note: The user must enter the required information in exactly the same way as it is contained in the certificate. The e-mail address itself is useful for that purpose since it is usually known and used by the user. If, however, cn=%s is used, for example, the user must know exactly how the Common Name is entered in the certificate.

- **Attribute**

Here you must enter the attribute that is used to save each of the user's certificates in the directory service. Usually this will be the LDAP `usercertificatesattribute`.

The default is `usercertificates`. Only one attribute can be set.

- **Time limit**
Time limit for the search in seconds. A value of 0 means "no limit". For example: 30.
- **Quantity limit**
Maximum number of found certificates that the system displays, and so can be assigned. A value of 0 means "no limit". For example: 10.
- **Password Restrictions**
 - **Minimum Length**
Here you can define a minimum password length for newly-created virtual disks. Specify the desired password minimum length (1 to 32 characters). The default password length is 4.
- **Certificate Verification**
 - **CRL Check**
If you select this option, certificates will only be accepted after a complete check of their certificate chain. Note: if necessary, a Certificate Revocation List (CRL) will be downloaded from the issuer (CA) of the certificate.
 - **Allow certificates with Unknown Critical Extensions**
Select this option if you want to allow certificates even if they contain a critical extension unknown to the SafeGuard PrivateDisk software. It will then be possible to assign certificates of this kind.
 - **Allow signature certificates**
Select this option if you want to allow certificates with key usage "Signature".

The following settings are available for user configuration:

```
User Configuration\  
Administrative Templates\  
SafeGuard\  
PrivateDisk
```

- **User Rights**
 - **Create Disk**
Creating virtual disks on the machine must be explicitly permitted. Select this option to allow the user to create their own virtual disks.
 - **Tray Icon**
If this option is not selected, the SafeGuard PrivateDisk icon is not displayed in the Windows task bar.

■ Virtual Disks

■ Mandatory Disk

Virtual disks assigned to a user through this policy setting are called mandatory disks. Settings for mandatory disks cannot be changed by the user, and mandatory disks cannot be removed from the list of available disks. This way, administrators in companies can ensure that specific virtual disks are always available to particular users.

The entry specifies a single virtual disk, using the format:

```
<volume file>|<name>|<drive letter>|<options>
```

If the next unused drive letter is to be used automatically when the disk is mounted (see page 16, **Automatic** option), ensure the <drive letter> is left blank.

Example: `c:\mandatory001.vol|MandatoryDisk||L)`

Startup options (you can only select one at a time):

L ... mount on user logon

P ... mount on device arrival (plug and play)

C ... mount on smartcard arrival

Additional options:

R ... mount for read access only

S ... fixed disk (see page 17)

Example:

```
c:\mandatory001.vol|MandatoryDisk|Z|LR
```

The volume file `mandatory001.vol` resides on drive C and is displayed as `MandatoryDisk` in the SafeGuard PrivateDisk list of available disks. Drive Letter Z is assigned to the virtual disk. The disk is mounted when the user logs on (L) and is mounted only for read access (R).

To create a virtual disk for the user automatically, see **Initial Virtual Disk**.

Note: Even if the specified volume file does not exist it is still displayed in the list of available virtual disks. If it is created later it can be used as intended.

■ Recovery Certificate

Here you can enter the serial number of a certificate that is assigned automatically, with administrator privileges, to virtual disks created by users. This ensures that you always have access to every virtual disk.

The serial number must be entered as a sequence of hex numbers.

Note: Data protection can be ensured by keeping the private key of the recovery certificate in a secure place (e.g. stored on smartcard or floppy disk in a safe).

- **Initial Virtual Disk**

- **Initial Virtual Disk**

- The initial virtual disk file is created automatically if the user logs on to the system and the disk does not already exist.

- **Add the user's certificate**

- If you select this option, the user's certificate is added to the disk that is created automatically. By default this option is inactive.

Note: When the secure virtual disk is created on the users computer a certificate is only added if the private key is available! If more than one certificate is available to the user, a dialog is displayed when the disk is created, in which the user must select a certificate.

- **LDAP**

- **Filter used**

- Here you can specify a search filter which the user is offered by default when they search for a certificate via LDAP. In the input field you must enter the name of the filter as it appears in Computer Configuration.

- You can only set a filter that has been defined in Computer Configuration.

7 SafeGuard PrivateDisk OLE Automation Interface

SafeGuard PrivateDisk exports an OLE automation server (pdole.exe) that can be used for using the software programmatically from within all applications that are compatible with Windows scripting. This includes the Windows Scripting Host (supporting Visual Basic Scripting, JavaScript, Perl, etc.) as well as MS Office applications, web pages and programming environments such as Visual Basic, Visual C++ and many more.

The COM object class exported is named PrivateDisk.Application. For scripting compatibility, it exports an IDispatch interface with the following properties and commands.

7.1 Properties

If you change the properties of a PrivateDisk.Application object, this only affects subsequent operations to this individual object, and does not change the settings of other objects.

NoGui Boolean	This option can be set to <i>True</i> if absolutely no GUI should be shown. In this case, neither dialog boxes nor message boxes are displayed. By default this option is set to <i>False</i> . The system therefore prompts for passwords, if they are not already passed as command parameters, and displays message boxes with descriptive text if errors occur. If the "NoGui" property is set to <i>True</i> but a user action is required (e.g. entering a password), the whole operation is canceled and an appropriate error code is displayed.
---------------	---

7.2 Commands

This is the list of commands that can be called for the PrivateDisk.Application object. Parameters in brackets are optional. See below for descriptions of the individual parameters:

NewDisk volume, size, (path), (fileys), (admpwd), (usrpwd)	Creates a new virtual disk. The disk is mounted automatically after creation. Returns <i>True</i> if successful, or else <i>False</i> .
MountDisk volume, (pwd), (pwdtype), (readonly)	Mounts a virtual disk, identified by its volume file name. The virtual disk must already be present in the user's list of disks. If readonly is set to <i>True</i> , the virtual disk is mounted for read access only. Returns <i>True</i> if successful, or else <i>False</i> .
ImportDisk volume, (path)	Adds a virtual disk to the user's list of disks. Returns <i>True</i> if successful, or else <i>False</i> .

UnmountDisk volume (forced)	Unmount a virtual disk. If forced is set to <i>True</i> , the virtual disk is always unmounted, even if it is still being used by applications. Returns <i>True</i> if successful, or else <i>False</i> .
UnmountAllDisks (forced)	Tries to unmount all currently mounted virtual disks. If forced is set to <i>True</i> , the virtual disk is always unmounted, even if it is still being used by applications. Returns <i>True</i> if successful, or else <i>False</i> .
GetDiskInfo volume, (path), (mounted), (readonly)	Collects information about the state of a virtual disk. Only the <volume> parameter is used as input. All other values are output parameters and filled by this function, if specified. Returns <i>True</i> if successful, or else <i>False</i> .
GetErrorText	If there is an error, you can call this function to display the reason for the error as plain text.

7.2.1 Parameters

volume	Disks are identified by their volume file names. The symbolic disk name cannot be used for this purpose since it is not unique.
size	Disk size in kBytes. The value is adjusted to the next multiple of 4 kB, which is the cluster size for SafeGuard PrivateDisk virtual disks.
path	Describes the drive letter for a virtual disk. For drive letters, specify a string such as "X" or "X:". To choose the next free drive letter, leave the parameter empty.
filesys	Identifies the file system for a new virtual disk. Possible values are "FAT" and "NTFS". The default value is "FAT".
usrpwd	Specifies the user password for a new disk.
admpwd	Specifies the administrator password for a new disk. If the administrator password is not specified here, the user is prompted for an administrator password when the disk is created.
pwd	The password for login to a virtual disk. This can be either the user password or the administrator password or even a PIN for a cryptographic service provider (see <pwdtype> parameter below). If this parameter is left empty, the system attempts to log on to the virtual disk with certificates. The user is prompted for a password, if necessary.

pwdtype	This integer value selects the method of authentication used when a disk is being mounted. It is only used when the <pwd> parameter is set: 0 (or empty) ... the <pwd> parameter is the administrator password 1 ... the <pwd> parameter is the user password 2 ... the <pwd> parameter is the PIN for a certificate login ("silent" connect)
mounted	This value is set to <i>True</i> if the disk is mounted, or else <i>False</i> .
readonly	This value is set to <i>True</i> if the disk is mounted for read only access, or else <i>False</i>

7.3 Example Script

You will find an example script (`demo.vbs`) in the `SafeGuard PrivateDisk` subdirectory of your SafeGuard PrivateDisk Installation directory. You can run the script for demonstration purposes.

8 Technical Support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk forum at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>
- Download the product documentation at <http://www.sophos.com/support/docs/>
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

9 Legal notices

Copyright © 2000 - 2011 Sophos Group. All rights reserved. SafeGuard is a registered trademark of Sophos Group.

Sophos is a registered trademark of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.